# SAP Business Application と SAP HANA Database ソリューション

NetApp Solutions SAP

NetApp
August 01, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/netapp-solutions-sap/index.html on August 01, 2025. Always check docs.netapp.com for the latest.

# 目次


SAP Business Application と SAP HANA Database ソリューション . . . 1
ベストプラクティス . . . 2
『 SAP HANA on NetApp AFF Systems with FCP Configuration Guide 』 . . . 2
『 SAP HANA on NetApp AFF Systems with Fibre Channel Protocol 』を参照してください . . . 2
VMware vSphere を使用した SAP HANA . . . 3
アーキテクチャ . . . 4
ストレージのサイジング . . . 8
インフラのセットアップと設定 . . . 14
追加情報の参照先 . . . 52
履歴を更新します . . . 53
『 SAP HANA on NetApp AFF Systems with NFS Configuration Guide 』 . . . 53
『SAP HANA on NetApp AFF Systems with NFS』-構成ガイド . . . 53
アーキテクチャ . . . 56
ストレージのサイジング . . . 61
インフラのセットアップと設定 . . . 66
追加情報の参照先 . . . 96
履歴を更新します . . . 97
『 SAP HANA on NetApp ASA Systems with FCP Configuration Guide 』 . . . 98
『 SAP HANA on NetApp ASA Systems with Fibre Channel Protocol 』を参照してください . . . 98
VMware vSphere を使用した SAP HANA . . . 99
アーキテクチャ . . . 99
ストレージのサイジング . . . 103
インフラのセットアップと設定 . . . 108
追加情報の参照先 . . . 143
履歴を更新します . . . 144
『 SAP HANA on NetApp FAS Systems with NFS Configuration Guide 』 . . . 144
『SAP HANA on NetApp FAS systems with NFS Configuration Guide』 . . . 144
アーキテクチャ . . . 147
ストレージのサイジング . . . 152
インフラのセットアップと設定 . . . 158
追加情報の参照先 . . . 190
履歴を更新します . . . 190
『 SAP HANA on FAS Systems with FCP Configuration Guide 』を参照してください . . . 191
『SAP HANA on NetApp FAS Systems with Fibre Channel Protocol』構成ガイド . . . 192
アーキテクチャ . . . 193
ストレージのサイジング . . . 198
インフラのセットアップと設定 . . . 204
追加情報の参照先 . . . 244
履歴を更新します . . . 245

バックアップ、リストア、ディザスタリカバリ 247
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 247
TR-4926：『SAP HANA on Amazon FSX for NetApp ONTAP - Backup and Recovery with SnapCenter 』 247
Amazon FSX for ONTAP を使用したバックアップとリカバリ 247
SnapCenter アーキテクチャ 252
SnapCenter 構成 258
SnapCenter バックアップ処理 274
データボリューム以外のボリュームのバックアップ 284
リストアとリカバリ 291
SnapVault を使用したバックアップレプリケーション 299
追加情報の参照先 314
SnapCenter を使用した SAP HANA のバックアップとリカバリ 315
TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』 315
SnapCenter アーキテクチャ 320
SnapCenter SAP HANA Backup 解決策 の略 321
SnapCenter の概念とベストプラクティス 325
このレポートで使用するラボのセットアップ 344
SnapCenter 構成 346
SnapCenter の初期設定 347
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 360
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 379
データベースのバックアップ 384
ブロック整合性チェック 393
リストアとリカバリ 397
高度な設定と調整 452
追加情報およびバージョン履歴の参照先 460
SnapCenter、SnapMirror Active Sync、VMware Metro Storage ClusterによるSAP HANAのデータ保護と高可用性 462
SnapCenter、SnapMirror Active Sync、VMware Metro Storage ClusterによるSAP HANAのデータ保護と高可用性 462
SAP HANAの高可用性の概要 463
セツテイノカイヨウレイ 466
HANAシステムのプロビジョニングとインストール 467
SnapMirrorのアクティブな同期設定 475
SnapCenter 構成 481
SnapCenter バックアップ処理 486
SnapCenterノリストアトリカハリ 489
SAPシステムの更新処理 491
SnapCenterデータボリューム以外のボリューム 491
フェイルオーバーのシナリオ 493

追加情報とバージョン履歴 . . . 497
VMware VMFSおよびNetApp ASAシステムを使用したSnapCenterによるSAP HANAデータ保護 . . . 498
VMware VMFSおよびNetApp ASAシステムを使用したSnapCenterによるSAP HANAデータ保護 . . . 498
このドキュメントで使用したラボのセットアップ . . . 498
HANAシステムのプロビジョニングとインストール . . . 499
HANA構成 . . . 506
SnapCenter 構成 . . . 507
バックアップ処理 . . . 514
リストア処理とリカバリ処理 . . . 517
SAP システムリフレッシュ . . . 521
追加情報とバージョン履歴 . . . 531
BlueXP Backup and Recovery for SAP HANA - バックアップ先としてのクラウドオブジェクトストレージ . . . 532
BlueXP Backup and Recovery for SAP HANA - バックアップ先としてのクラウドオブジェクトストレージ . . . 532
BlueXP Backup and Recovery for SAP HANAの設定 . . . 534
SAP HANA BlueXPのバックアップのリストア . . . 552
追加情報とバージョン履歴 . . . 555
SnapCenter を使用した SAP HANA システムレプリケーションのバックアップとリカバリ . . . 556
TR-4719 ：『 SAP HANA System Replication - Backup and Recovery with SnapCenter 』 . . . 556
ストレージ Snapshot バックアップと SAP システムレプリケーション . . . 557
SAP システムレプリケーションの SnapCenter 設定オプション . . . 559
リソースグループを使用した SnapCenter 4.6 の設定 . . . 560
単一のリソースを使用する SnapCenter 構成 . . . 571
もう一方のホストで作成されたバックアップからのリストアとリカバリ . . . 584
追加情報の参照先 . . . 589
バージョン履歴 . . . 589
Azure NetApp Files を使用した SAP HANA ディザスタリカバリ . . . 589
TR-4891 ：『 SAP HANA disaster recovery with Azure NetApp Files 』 . . . 589
ディザスタリカバリ解決策の比較 . . . 592
SAP HANA を使用した ANF のクロスリージョンレプリケーション . . . 596
ディザスタリカバリのテスト . . . 608
ディザスタリカバリフェイルオーバー . . . 621
履歴を更新します . . . 632
TR-4646 ：『 SAP HANA Disaster Recovery with Storage Replication 』 . . . 632
TR-4711 ：『 SAP HANA Backup and Recovery Using NetApp Storage Systems and Commvault Software 』 . . . 633
SnapCenterとSAP ASEデータベースの統合 . . . 633
はじめに . . . 633
追加情報とバージョン履歴 . . . 646
IBM DB2データベース用のSnapCenter統合 . . . 647
はじめに . . . 647

セツテイノカイヨウレイ 648
デモ環境 648
追加情報とバージョン履歴 655
SAP MaxDBデータベースのSnapCenter統合 656
はじめに 656
セツテイノカイヨウレイ 656
デモ環境 657
ソフトウェアバージョン 657
MaxDBボリューム設計 657
データベースM02を保護する手順 658
ホストの前提条件 658
データベースの前提条件–バックアップテンプレートの作成、ログバックアップの有効化 659
sap-lnx25をホストするためのSnapCenterエージェントの配備 659
データベースM02のSnapCenterリソース構成の作成 660
システムM02をリカバリする手順 667
インスタンスM02のリカバリ 667
追加情報とバージョン履歴 673
ライフサイクル管理 674
Ansibleを使用したNetApp SAP Landscape Managementの統合 674
TR-4953：『NetApp SAP Landscape Management Integration using Ansible』 674
SAPシステムのクローニング、コピー、更新のシナリオ 674
システムの更新、コピー、クローニングのユースケース 675
Ansibleを使用して、NetApp SAP LaMaを統合 678
実装例 678
SAP LaMaプロビジョニングワークフロー-クローンシステム 684
SAP LaMaによるワークフローのプロビジョニング解除-システムの破壊 692
SAP LaMaプロビジョニングワークフロー-コピーシステム 695
SAP LaMaプロビジョニングワークフロー-システムの更新 699
プロバイダスクリプトの設定とAnsibleのプレイブック 701
まとめ 714
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 715
TR-4667：『Automating SAP HANA System Copy and Clone Operations with SnapCenter 』 715
SAPシステムのコピー、更新、クローニングのシナリオ 717
システムの更新とクローニングのユースケース 718
サポートされるインフラとシナリオ 721
SnapCenter を使用したSAPシステムの更新ワークフローの概要 722
SnapCenter を使用したSAPシステムのクローニングワークフローの概要 724
ストレージSnapshotバックアップを使用したSAP HANAシステムの更新処理に関する考慮事項 725
自動化スクリプトの例 730
SAP HANAシステムをSnapCenter で更新 733
SnapCenter によるSAPシステムのクローニング 758

追加情報およびバージョン履歴の参照先 771
Libelle SystemCopyによるSAPシステムのコピー処理の自動化 771
TR-4929：Libelle SystemCopyによるSAPシステムのコピー処理の自動化 771
LSCおよびSnapCenter でSAP HANAシステムが更新されます 774
LSC、AzAcSnap、およびAzure NetApp Files を使用してSAP HANAシステムが更新されます 788
追加情報およびバージョン履歴の参照先 800
解決策概要 802
SB-3978 ：『 Lifecycle Management for SAP HANA 』 802
SB-3965: SAP HANAのバックアップとリカバリ 802
課題 802
主要なソリューション・コンポーネント 802
SB-3968: SAP HANAの災害復旧 802
課題 802
主要なソリューション・コンポーネント 802
SB-4292：AnsibleによるSAP自動化 803
解決策の概要 803
まとめ 806
追加情報の参照先 806
バージョン履歴 807
SB-4293：AlpacaとNetApp SnapCenterによる
SAPシステムのコピー、更新、クローニングのワークフローの自動化 807
解決策の概要 807
まとめ 812
追加情報の参照先 812
バージョン履歴 812
SB-4294：AvantraとNetApp SnapCenterによる
SAPシステムのコピー、更新、クローニングのワークフローの自動化 812
解決策の概要 812
まとめ 816
追加情報の参照先 817
バージョン履歴 817
法的通知 818
著作権 818
商標 818
特許 818
プライバシーポリシー 818

# SAP Business Application と SAP HANA Database ソリューション

# ベストプラクティス

## 『 SAP HANA on NetApp AFF Systems with FCP Configuration Guide 』

『 **SAP HANA on NetApp AFF Systems with Fibre Channel Protocol** 』を参照してください

NetApp AFF 製品ファミリーは、 TDI プロジェクトの SAP HANA との使用が認定されています。このガイドでは、FCP のこのプラットフォーム上の SAP HANA に関するベスト プラクティスについて説明します。

Marco Schoen 、ネットアップ

はじめに

NetApp AFF AシリーズおよびAFF Cシリーズ製品ファミリーは、Tailored Data Center Integration（TDI；テーラードデータセンター統合）プロジェクトでSAP HANAとの使用が認定されています。

この認定は、次のモデルで有効です。

- AFF A150、AFF A20、AFF A250、AFF A30、AFF A400、AFF A50、AFF A70、AFF A1K、AFF A90 、AFF A900、AFF A800
- AFF C250、AFF C30、AFF C400、AFF C60、AFF C800、AFF C80
- ASA A250、ASA A400、ASA A800、ASA A900
- ASA C250、ASA C400、ASA C800

NetApp AFFおよびASA CシリーズにはNetApp ONTAP 9.13.1以降が必要です

SAP HANA 向けのネットアップ認定ストレージソリューションの一覧については、を参照してください "認定およびサポートされている SAP HANA ハードウェアディレクトリ"。

本ドキュメントでは、 Fibre Channel Protocol （ FCP ；ファイバチャネルプロトコル）を使用した AFF 構成について説明します。

このホワイトペーパーで説明している構成は、 SAP HANA に必要な SAP HANA KPI と、 SAP HANA に最適なパフォーマンスを達成するために必要です。ここに記載されていない設定または機能を変更すると、原因のパフォーマンスが低下したり、予期しない動作が発生したりする可能性があります。変更は、ネットアップのサポートから助言された場合にのみ実施

NFS システムと NetApp FAS システムを使用する AFF システムの構成ガイドは、次のリンクから入手できます。

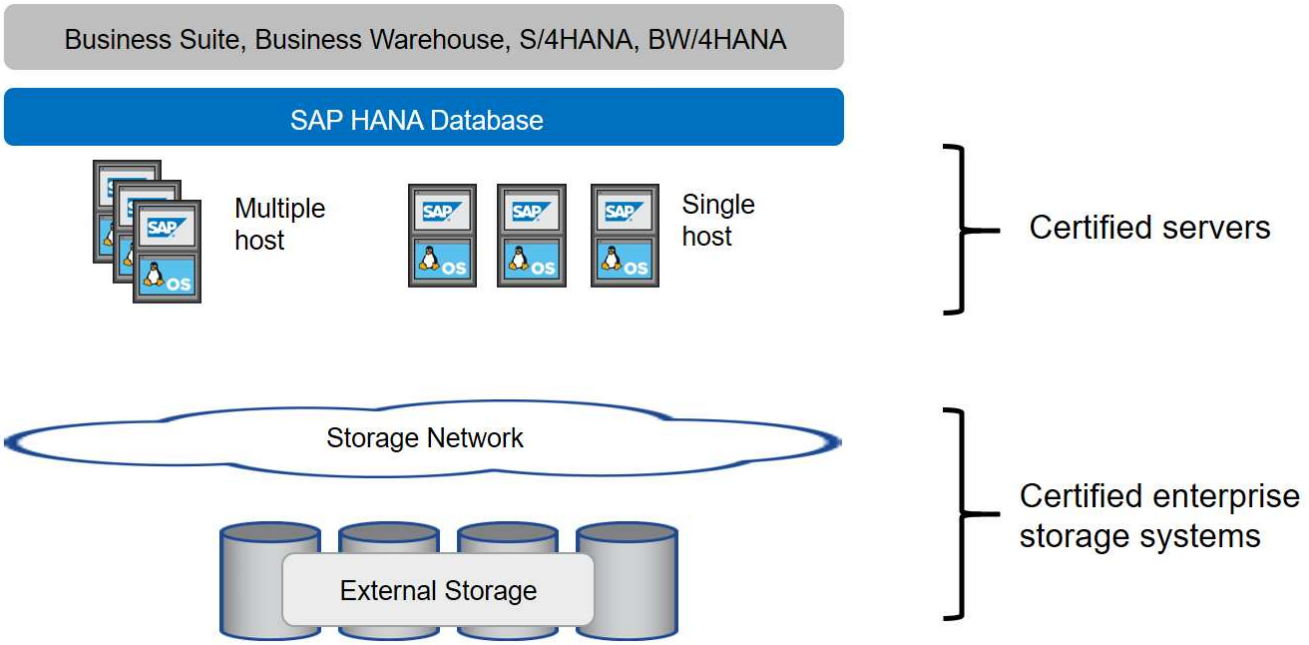
- "FCP を使用した NetApp FAS システムでの SAP HANA"
- "FCP 搭載の NetApp ASA システム上の SAP HANA"

- "NFS を使用した NetApp FAS システムでの SAP HANA"
- "NFS を使用した NetApp AFF システムでの SAP HANA"

SAP HANA マルチホスト環境では、 SAP HANA ホストのフェイルオーバー時にフェンシングを提供するために、標準の SAP HANA ストレージコネクタが使用されます。オペレーティングシステムの構成ガイドラインと、 HANA 固有の Linux カーネルの依存関係については、必ず該当する SAP ノートを参照してください。詳細については、を参照してください "SAP Note 2235581 – SAP HANA Supported Operating Systems 』"。

**SAP HANA** テーラードデータセンター統合

NetApp AFF ストレージシステムは、 NFS （ NAS ）プロトコルと FC （ SAN ）プロトコルの両方を使用した SAP HANA TDI プログラムで認定されています。これらは、シングルホスト構成とマルチホスト構成のどちらでも、 SAP Business Suite on HANA 、 S/4HANA 、 BW/4HANA 、 SAP Business Warehouse on HANA など、最新の SAP HANA シナリオに導入できます。SAP HANA との使用が認定されているサーバは、ネットアップ認定のストレージソリューションと組み合わせることができます。次の図に、アーキテクチャの概要を示します。




生産性の高いSAP HANAシステムを実現するための前提条件と推奨事項の詳細については、次のリソースを参照してください。

- "『 SAP HANA Tailored Data Center Integration Frequently Asked Questions 』"

## VMware vSphere を使用した SAP HANA

ストレージを仮想マシン（ VM ）に接続する方法はいくつかあります。推奨される方法は、ストレージボリュームと NFS をゲストオペレーティングシステムから直接接続することです。このオプションについては、を"NFS を使用した NetApp AFF システムでの SAP HANA"参照してください。

raw デバイスマッピング（ RDM ）、 FCP データストア、または FCP を使用する VVol データストアもサポートされます。どちらのデータストアオプションも、本番環境で使用するためにデータストアに格納する SAP HANA データボリュームまたはログボリュームは 1 つだけです。

SAP HANA での vSphere の使用の詳細については、次のリンクを参照してください。

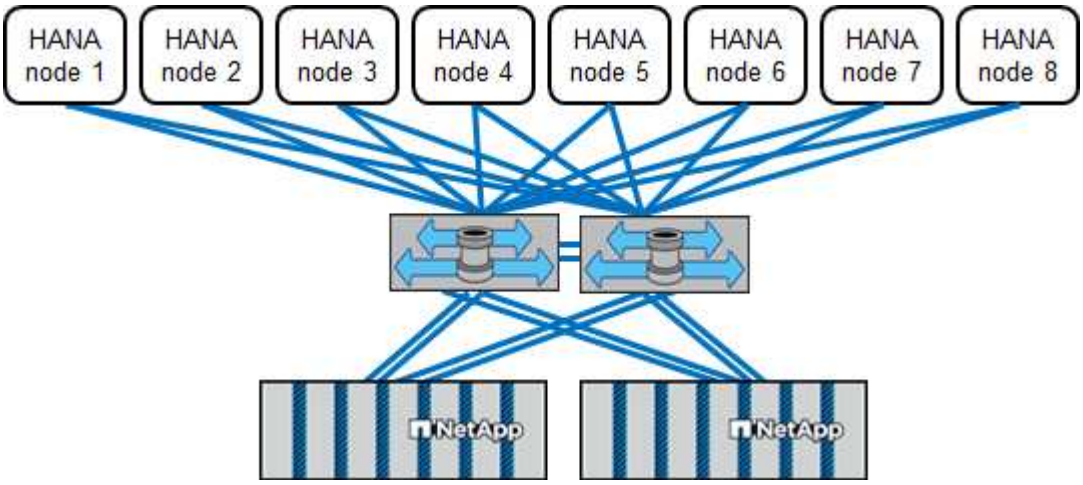
- "SAP HANA on VMware vSphere - 仮想化 - コミュニティ Wiki"
- "『SAP HANA on VMware vSphere Best Practices Guide』"
- "2161991 - VMware vSphere 設定ガイドライン - SAP One Support Launchpad （ログインが必要）"

## アーキテクチャ

SAP HANA ホストは、冗長 FCP インフラとマルチパスソフトウェアを使用してストレージコントローラに接続されます。スイッチまたはホストバスアダプタ（ HBA ）で障害が発生した場合に、耐障害性に優れた SAP HANA ホスト / ストレージ接続を実現するには、冗長 FCP スイッチインフラが必要です。すべての HANA ホストがストレージコントローラ上の必要な LUN にアクセスできるように、スイッチで適切なゾーニングを設定する必要があります。

AFF システム製品ファミリーのさまざまなモデルをストレージレイヤで混在させることができるため、拡張が必要になったり、パフォーマンスや容量のニーズが異なる場合があります。ストレージシステムに接続できる SAP HANA ホストの最大数は、 SAP HANA のパフォーマンス要件と、使用されているネットアップコントローラのモデルによって定義されます。必要なディスクシェルフの数は、 SAP HANA システムの容量とパフォーマンスの要件によってのみ決まります。

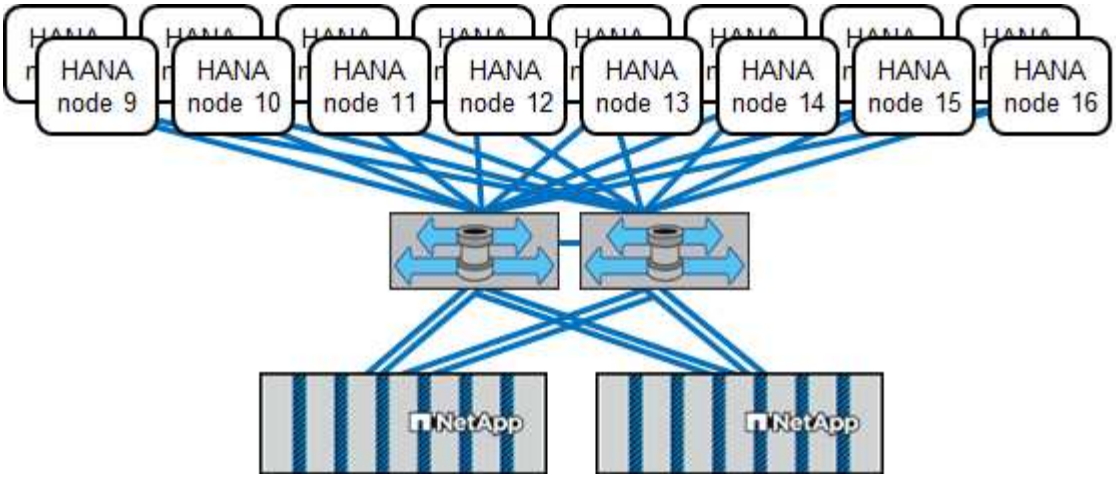
次の図は、 8 台の SAP HANA ホストをストレージ HA ペアに接続した構成例を示しています。



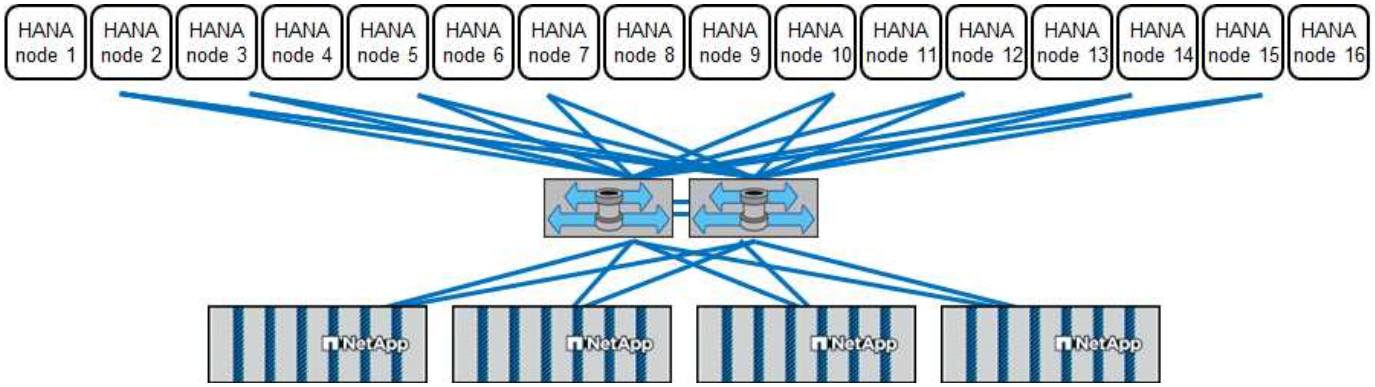

このアーキテクチャは、次の 2 つの側面で拡張できます。

- 既存のストレージに SAP HANA ホストとストレージ容量を追加で接続することで、ストレージコントローラが現在の SAP HANA KPI を満たす十分なパフォーマンスを提供する場合
- 追加の SAP HANA ホスト用にストレージ容量を追加したストレージシステムを追加する

次の図は、追加の SAP HANA ホストをストレージコントローラに接続した場合の構成例を示しています。この例では、 16 台の SAP HANA ホストの容量とパフォーマンスの要件を満たすために、さらにディスクシェルフが必要です。合計スループット要件に応じて、ストレージコントローラへの FC 接続を追加する必要があります。




次の図に示すように、導入した AFF システムとは関係なく、認定済みのストレージコントローラを追加することで、 SAP HANA 環境を拡張して希望するノード密度に合わせることもできます。




**SAP HANA** のバックアップ

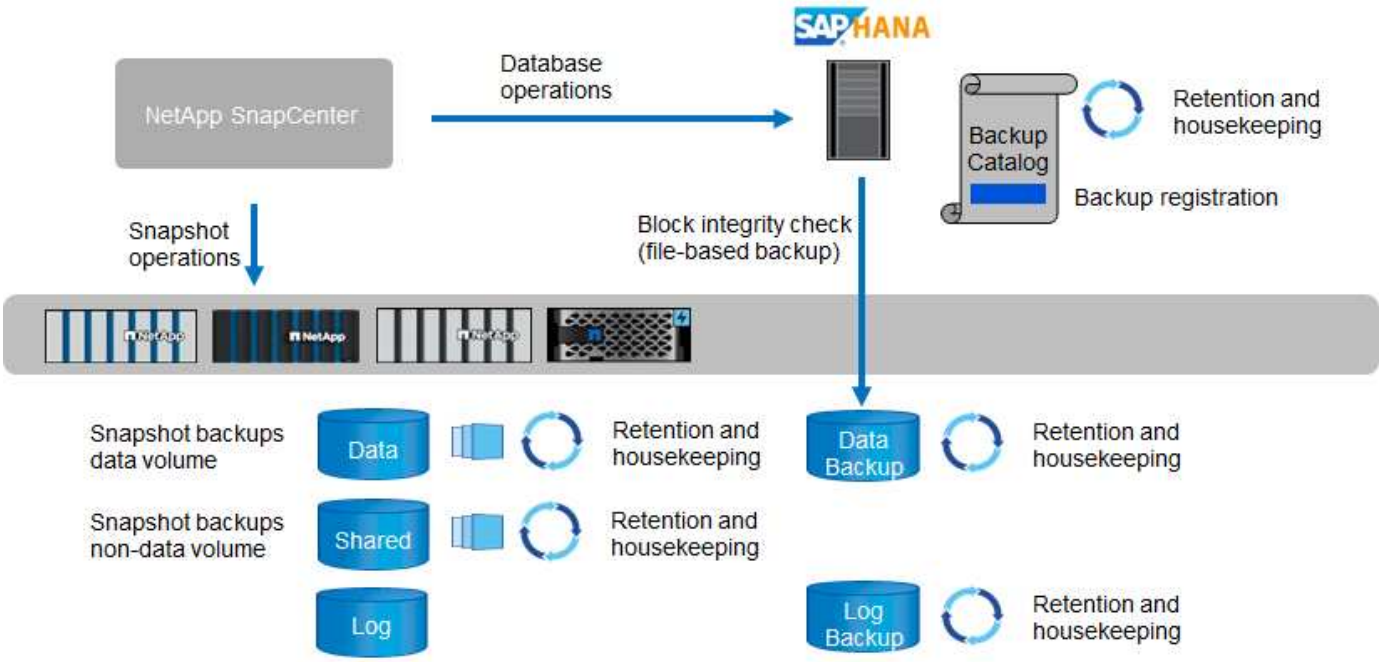
すべてのネットアップストレージコントローラに搭載された ONTAP ソフトウェアは、動作中にパフォーマンスに影響を与えることなく SAP HANA データベースをバックアップするための組み込みメカニズムを提供します。ストレージベースの NetApp Snapshot バックアップは、 SAP HANA の単一コンテナ、および単一のテナントや複数のテナントを使用する SAP HANA MDC システムで使用可能な、完全にサポートされた統合バックアップ解決策です。

ストレージベースの Snapshot バックアップは、 NetApp SnapCenter Plug-in for SAP HANA を使用して実装されます。これにより、 SAP HANA データベースに標準で搭載されているインターフェイスを使用して、整合性のあるストレージベースの Snapshot バックアップを作成できます。SnapCenter は、各 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。そのため、 SnapCenter で作成されたバックアップは、リストア処理とリカバリ処理用に直接選択できる SAP HANA Studio または Cockpit 内に表示できます。

NetApp SnapMirror テクノロジを使用すると、 1 つのストレージシステムで作成された Snapshot コピーを、 SnapCenter で制御されるセカンダリバックアップストレージシステムにレプリケートできます。その後、プライマリストレージ上のバックアップセットごと、およびセカンダリストレージシステム上のバックアップセットごとに、異なるバックアップ保持ポリシーを定義できます。SnapCenter Plug-in for SAP HANA は、不要なバックアップカタログの削除を含め、 Snapshot コピーベースのデータバックアップとログバックアップの保持を自動的に管理します。また、 SnapCenter Plug-in for SAP HANA では、ファイルベースのバックアップを実行することで、 SAP HANA データベースのブロック整合性チェックを実行できます。

次の図に示すように、 NFS マウントを使用して、データベースログをセカンダリストレージに直接バックア

ップできます。




ストレージベースの Snapshot バックアップは、従来のファイルベースのバックアップに比べて大きなメリットをもたらします。これには次のような利点がありますが、これらに限定されるわけではありません。

- 高速バックアップ（数分）
- ストレージレイヤでのリストア時間（数分）が大幅に短縮され、バックアップの頻度も高まり、 RTO が短縮されます
- バックアップとリカバリの処理中、 SAP HANA データベースのホスト、ネットワーク、またはストレージのパフォーマンスが低下することはありません
- ブロックの変更に基づいて、スペース効率と帯域幅効率に優れたセカンダリストレージへのレプリケーションを実行します

SAP HANAのバックアップとリカバリの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-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"。

### SAP HANA ディザスタリカバリ

SAP HANA ディザスタリカバリは、 SAP HANA システムレプリケーションを使用してデータベースレイヤで実行するか、ストレージレプリケーションテクノロジを使用してストレージレイヤで実行できます。次のセクションでは、ストレージレプリケーションに基づくディザスタリカバリソリューションの概要について説明します。

SAP HANAディザスタリカバリ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-4646 ：『 SAP HANA Disaster Recovery with Storage Replication 』"。

#### SnapMirror に基づくストレージレプリケーション

次の図は、ローカルDRデータセンターへの同期SnapMirror Active Syncと、リモートDRデータセンターへのデータ複製に非同期SnapMirrorを使用する3サイトのディザスタリカバリソリューションを示しています。SnapMirrorActive Syncにより、サイト全体の障害発生時でもビジネスサービスは継続して稼働し、セカンダリコピー（RPO=0、RTO=0）を使用してアプリケーションを透過的にフェイルオーバーできま

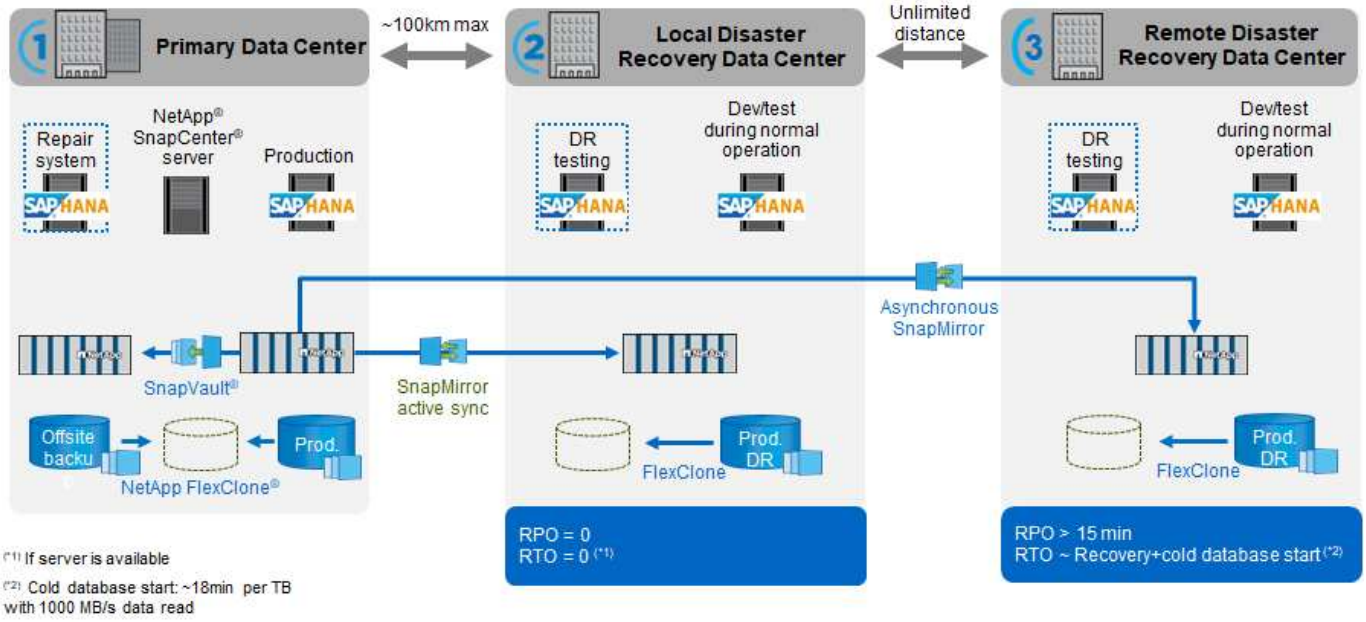
す。SnapMirrorActive Syncでは、フェイルオーバーを開始するために手動による介入やカスタムスクリプトは必要ありません。ONTAP 9.15.1以降では、SnapMirrorアクティブ同期で対称アクティブ/アクティブ機能がサポートされます。対称アクティブ/アクティブ：双方向同期レプリケーションにより、保護されたLUNの両方のコピーからの読み取りおよび書き込みI/O処理を有効にし、両方のLUNコピーがローカルでI/O処理を処理できるようにします。

詳細については、を参照してください "ONTAPでのSnapMirrorアクティブ同期の概要"。

非同期 SnapMirror レプリケーションの RTO は、主に DR サイトで HANA データベースを起動し、データをメモリにロードするのに必要な時間によって決まります。1000Mbps のスループットでデータが読み取られることを前提とし、 1TB のデータをロードするには約 18 分かかります。

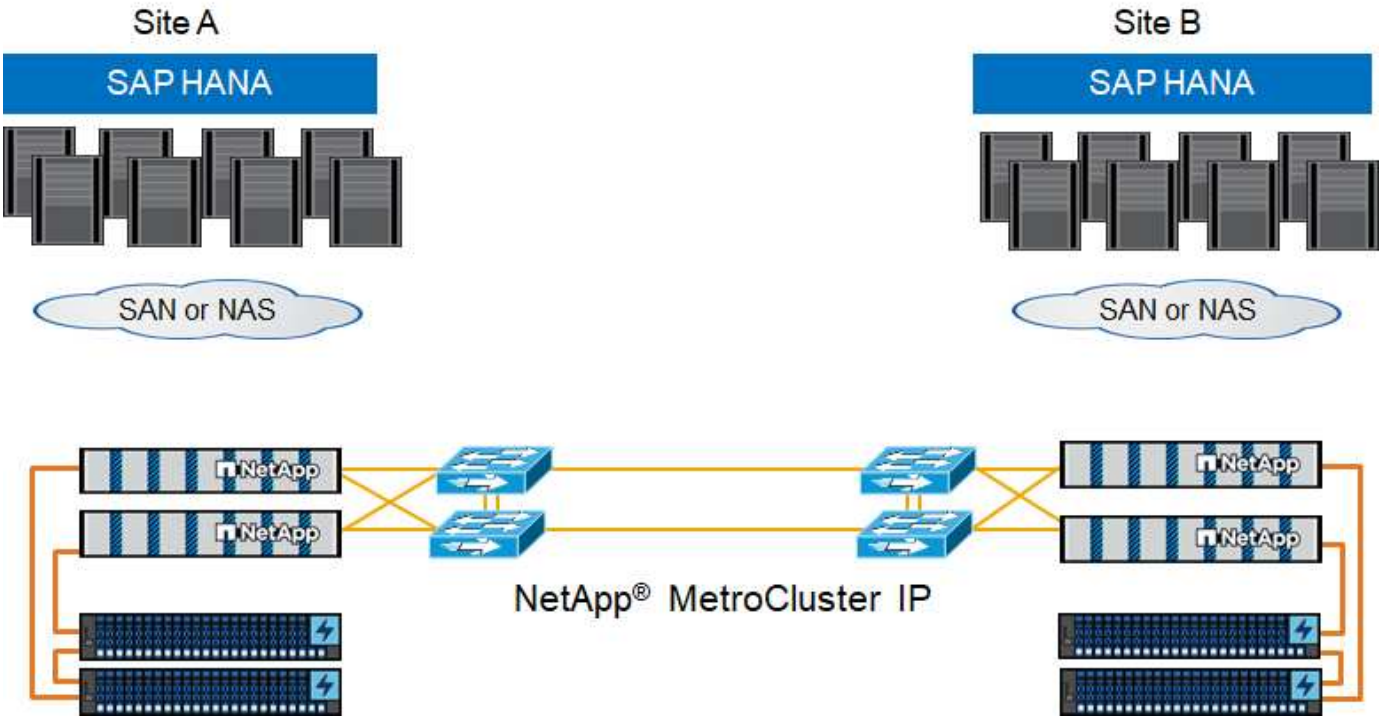
DR サイトのサーバは、通常運用時に開発 / テストシステムとして使用できます。災害が発生した場合は、開発 / テスト用システムをシャットダウンし、 DR 本番用サーバとして起動する必要があります。

どちらのレプリケーション方法でも、 RPO と RTO に影響を与えることなく DR ワークフローテストを実行できます。FlexClone ボリュームはストレージ上に作成され、 DR テストサーバに接続されます。




**NetApp MetroCluster** に基づくストレージレプリケーション

次の図は、解決策の概要を示しています。各サイトのストレージクラスタがローカルで高可用性を実現し、本番環境のワークロードに使用されます。各サイトのデータはもう一方のサイトに同期的にレプリケートされ、災害のフェイルオーバー時に使用できます。




## ストレージのサイジング

次のセクションでは、 SAP HANA 用のストレージシステムのサイジングに必要なパフォーマンスと容量に関する考慮事項の概要を説明します。

ストレージのサイジングプロセスをサポートし、適切なサイズのストレージ環境を構築するには、ネットアップまたはネットアップパートナーの営業担当者にお問い合わせください。

### パフォーマンスに関する考慮事項

SAP では、ストレージの主要パフォーマンス指標（ KPI ）の静的なセットが定義されています。これらの KPI は、データベースホストのメモリサイズや SAP HANA データベースを使用するアプリケーションに関係なく、すべての SAP HANA 本番環境に対して有効です。これらの KPI は、シングルホスト環境、マルチホスト環境、 Business Suite on HANA 環境、 Business Warehouse on HANA 環境、 S/4HANA 環境、および BW/4HANA 環境で有効です。したがって、現在のパフォーマンスサイジングアプローチは、ストレージシステムに接続されているアクティブな SAP HANA ホストの数にのみ依存します。

ストレージパフォーマンス KPI は、本番用 SAP HANA システムにのみ必須ですが、すべての HANA システムに実装できます。

SAP はパフォーマンステストツールを提供します。このツールは、ストレージに接続されたアクティブな SAP HANA ホストのストレージシステムパフォーマンスを検証するために使用する必要があります。

ネットアップは、特定のストレージモデルに接続できる SAP HANA ホストの最大数をテストして事前に定義しました。さらに、本番環境ベースの SAP HANA システムに必要なストレージ KPI を実現しています。

ディスクシェルフで実行できる SAP HANA ホストの最大数と、 SAP HANA ホストごとに必要な SSD の最小数は、 SAP パフォーマンステストツールを実行して決定されています。このテストでは、ホストの実際のストレージ容量要件は考慮しません。また、必要な実際のストレージ構成を決定するために、容量要件を計算す

る必要があります。

#### SAS ディスクシェルフ

12Gb SAS ディスクシェルフ（ DS224C ）では、次のような固定ディスクシェルフ構成を使用してパフォーマンスのサイジングを行います。

- 12 本の SSD を備えたハーフ搭載のディスクシェルフです
- 24 本の SSD を搭載したフル搭載のディスクシェルフです

どちらの構成もアドバンストドライブパーティショニング（ ADPv2 ）を使用します。ハーフ搭載のディスクシェルフは、最大 9 台の SAP HANA ホストをサポートします。フル搭載のシェルフは、 1 台のディスクシェルフで最大 14 台のホストをサポートします。SAP HANA ホストは、両方のストレージコントローラ間で均等に分散する必要があります。

DS224C ディスクシェルフは、 SAP HANA ホストの数をサポートするため、 12Gb SAS を使用して接続する必要があります。

6Gb SAS ディスクシェルフ（ DS2246 ）は、最大 4 台の SAP HANA ホストをサポートします。SSD と SAP HANA ホストは、両方のストレージコントローラ間で均等に分散する必要があります。次の図は、ディスクシェルフあたりでサポートされる SAP HANA ホストの数を示しています。

| | **24** 本の **SSD** をフル搭載した **6Gb SAS** シェルフ（ **DS2246** | **12Gb SAS** シェルフ（ **DS224C** ）には、 **12** 本の **SSD** と **ADPv2** をハーフ搭載しています | **12Gb SAS** シェルフ（ **DS224C** ）では、 **24** 本の **SSD** と **ADPv2** をフル搭載しています |
|---|---|---|---|
| ディスクシェルフあたりの SAP HANA ホストの最大数 | 4. | 9. | 14 |

この計算は、使用しているストレージコントローラには依存しません。ディスクシェルフを追加しても、ストレージコントローラでサポートできる SAP HANA ホストの最大数は増加しません。

#### NS224 NVMe シェルフ

1つのNVMe SSD（データ）は、使用する特定のNVMeディスクに応じて、最大2/5のSAP HANAホストをサポートします。SSDとSAP HANAホストは、両方のストレージコントローラ間で均等に分散する必要があります。AFFシステムとASAシステムの内蔵NVMeディスクについても同様です。

ディスクシェルフを追加しても、ストレージコントローラでサポートできる SAP HANA ホストの最大数は増加しません。

混在ワークロード

SAP HANA とその他のアプリケーションワークロードを、同じストレージコントローラ上または同じストレージアグリゲート内で実行することはできません。ただし、ネットアップのベストプラクティスとして、 SAP HANA ワークロードを他のすべてのアプリケーションワークロードから分離することを推奨します。

SAP HANA ワークロードとその他のアプリケーションワークロードを、同じストレージコントローラまたは

同じアグリゲートに導入することもできます。その場合は、混在ワークロード環境内で SAP HANA に対して適切なパフォーマンスが確保されていることを確認する必要があります。また、 Quality of Service （ QoS ；サービス品質）パラメータを使用して、 SAP HANA アプリケーションに対する他のアプリケーションの影響を制御し、 SAP HANA アプリケーションのスループットを保証することも推奨します。

SAP HCMT テストツールを使用して、他のワークロードにすでに使用されている既存のストレージコントローラで、追加の SAP HANA ホストを実行できるかどうかを確認する必要があります。SAP アプリケーションサーバは、 SAP HANA データベースと同じストレージコントローラやアグリゲートに安全に配置できます。

### 容量に関する考慮事項

SAP HANA の容量要件の詳細な概要については、を参照してください "SAP ノート 1900823" ホワイトペーパー。

> 複数の SAP HANA システムで構成される SAP 環境全体の容量サイジングは、ネットアップの SAP HANA ストレージサイジングツールを使用して決定する必要があります。ストレージのサイジングプロセスを検証し、適切なサイズのストレージ環境を構築するには、ネットアップまたはネットアップパートナーの営業担当者にお問い合わせください。

### パフォーマンステストツールの設定

SAP HANA 1.0 SPS10 以降、 I/O 動作を調整し、使用中のファイルシステムとストレージシステムのデータベースを最適化するためのパラメータが導入されています。SAP のテストツールでストレージのパフォーマンスをテストするときは、 SAP のパフォーマンステストツールにもこれらのパラメータを設定する必要があります。

ネットアップは、最適な値を定義するため、パフォーマンステストを実施しました。次の表に、 SAP テストツールの構成ファイルで設定する必要があるパラメータを示します。

| パラメータ | 価値 |
| --- | --- |
| max_parallel _io_requests と入力します | 128 |
| async _read_submit | オン |
| async ： write_submit_active | オン |
| async_write_submit_bblocks | すべて |

SAP テストツールの設定の詳細については、を参照してください "SAP ノート 1943937" HWCCT （ SAP HANA 1.0 ）および "SAP ノート 2493172" HCMT/HCOT 用（ SAP HANA 2.0 ）。

次の例は、 HCMT/HCOT 実行プランに変数を設定する方法を示しています。

```
…
{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
      },
```

```
      {
         "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
         "Name": "DataAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
```

```
per completion queue",
          "Name": "DataExtMaxParallelIoRequests",
          "Value": "128",
          "Request": "false"
       }, …
```

これらの変数はテスト構成に使用する必要があります。これは通常、 SAP が HCMT/HCOT ツールを使用して提供する事前定義された実行計画の場合です。次に、 4k ログの書き込みテストの例を示します。

```
…
       {
          "ID": "D664D001-933D-41DE-A904F304AEB67906",
          "Note": "File System Write Test",
          "ExecutionVariants": [
             {
                "ScaleOut": {
                   "Port": "${RemotePort}",
                   "Hosts": "${Hosts}",
                   "ConcurrentExecution": "${FSConcurrentExecution}"
                },
                "RepeatCount": "${TestRepeatCount}",
                "Description": "4K Block, Log Volume 5GB, Overwrite",
                "Hint": "Log",
                "InputVector": {
                   "BlockSize": 4096,
                   "DirectoryName": "${LogVolume}",
                   "FileOverwrite": true,
                   "FileSize": 5368709120,
                   "RandomAccess": false,
                   "RandomData": true,
                   "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                   "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                   "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                   "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                   "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                   "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                   "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                   "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                   "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
                }
             },
…
```

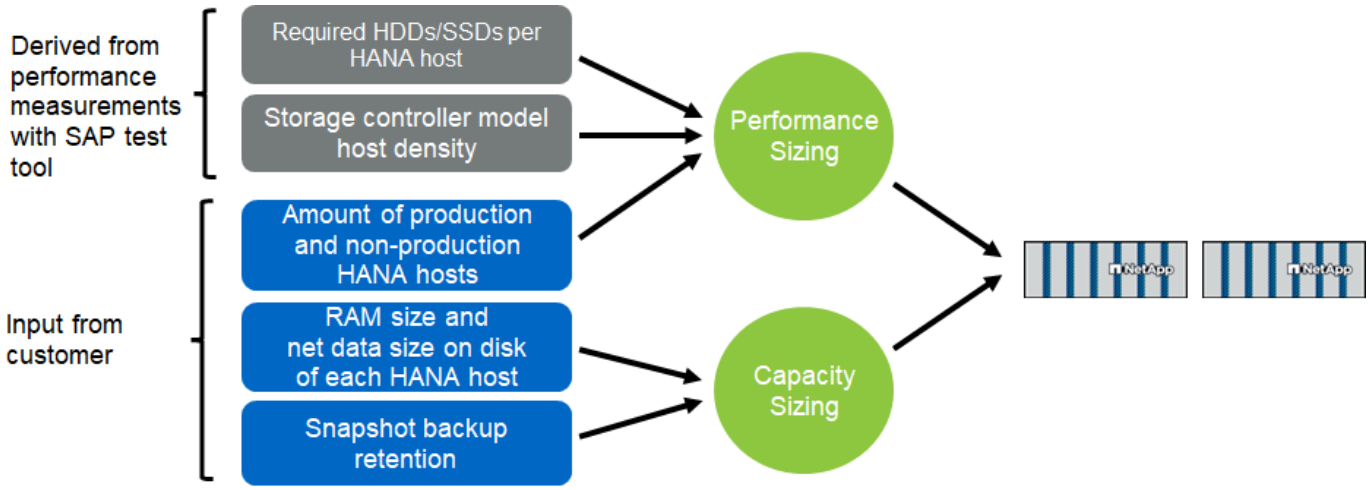
ストレージサイジングプロセスの概要

各ストレージモデルの HANA ホストあたりのディスク数と SAP HANA ホストの密度は、 SAP HANA テストツールを使用して決定されています。

サイジングプロセスでは、本番用および非本番用の SAP HANA ホストの数、各ホストの RAM サイズ、ストレージベースの Snapshot コピーのバックアップ保持期間などの詳細が必要です。SAP HANA ホストの数によって、必要なストレージコントローラとディスクの数が決まります。

RAM のサイズ、各 SAP HANA ホストでのディスク上の正味データサイズ、および Snapshot コピーのバックアップ保持期間は、容量サイジングの際に入力として使用されます。

次の図に、サイジングプロセスの概要を示します。




## インフラのセットアップと設定

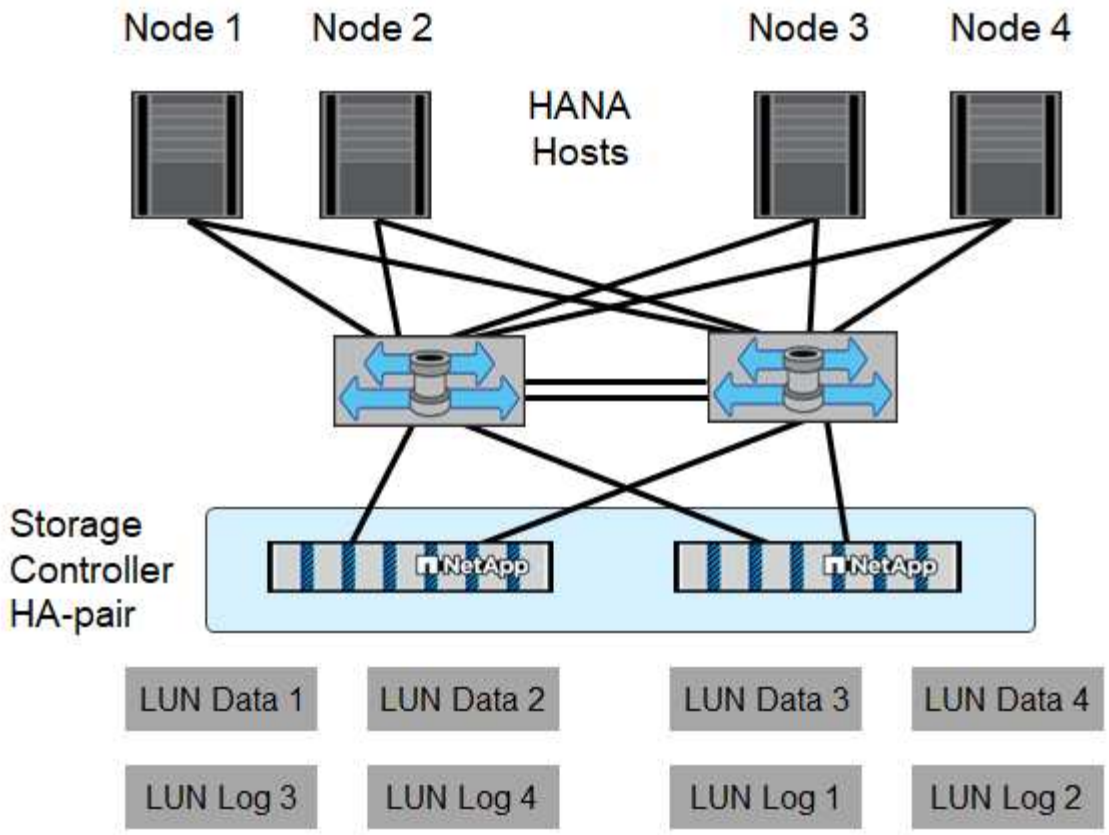
以降のセクションでは、 SAP HANA インフラのセットアップと構成のガイドラインについて説明し、 SAP HANA システムのセットアップに必要なすべての手順について説明します。ここでは、次の設定例を使用します。

- SID=FC5のHANAシステム
  - Linux 論理ボリューム マネージャー (LVM) を使用した SAP HANA の単一ホストと複数ホスト
  - SAP HANA マルチパーティションを使用する SAP HANA シングルホスト

### SAN ファブリックのセットアップ

各 SAP HANA サーバには、最低 8Gbps の帯域幅の冗長 FCP SAN 接続が必要です。ストレージコントローラに接続された各 SAP HANA ホストでは、少なくとも 8Gbps の帯域幅をストレージコントローラで設定する必要があります。

次の図は、 4 台の SAP HANA ホストを 2 台のストレージコントローラに接続した場合の例を示しています。各 SAP HANA ホストには、冗長ファブリックに接続された 2 つの FCP ポートがあります。ストレージレイヤでは、各 SAP HANA ホストに必要なスループットを提供するために、 4 つの FCP ポートが構成されます。




スイッチレイヤのゾーニングに加えて、ストレージシステム上の各 LUN を、この LUN に接続するホストにマッピングする必要があります。スイッチ上のゾーニングはシンプルにします。つまり、すべてのホスト HBA がすべてのコントローラ HBA を認識できるゾーンセットを 1 つ定義します。

### 時刻の同期

ストレージコントローラと SAP HANA データベースホストの間で時刻を同期する必要があります。そのためには、すべてのストレージコントローラとすべての SAP HANA ホストに同じタイムサーバを設定します。

### ストレージコントローラのセットアップ

ここでは、ネットアップストレージシステムの構成について説明します。プライマリのインストールとセットアップは、対応する Data ONTAP のセットアップガイドおよび設定ガイドに従って実行する必要があります。

#### ストレージ効率

SSD 構成の SAP HANA では、インライン重複排除、ボリューム間インライン重複排除、インライン圧縮、インラインコンパクションがサポートされています。

#### **NetApp FlexGroup**ボリューム

NetApp FlexGroup Volumeの使用はSAP HANAではサポートされていません。SAP HANAのアーキテクチャ上、FlexGroup Volumeを使用してもメリットはなく、パフォーマンスの問題が発生する可能性があります。

#### NetAppボリュームとアグリゲートの暗号化

SAP HANAでは、NetApp Volume Encryption（NVE）とNetApp Aggregate Encryption（NAE）の使用がサポートされています。

#### Quality of Service の略

QoSを使用すると、共有コントローラ上の特定のSAP HANAシステムまたはSAP以外のアプリケーションのストレージスループットを制限できます。

本番環境と開発/テスト

1つのユースケースは、開発システムとテストシステムのスループットを制限して、混在環境で本番システムに影響を与えないようにすることです。サイジングプロセスでは、非本番システムのパフォーマンス要件を決定する必要があります。開発 / テスト用のシステムは、通常、 SAP で定義されている本番用システム KPI の 20~50% の範囲で、パフォーマンス値を低くしてサイジングすることができます。ストレージシステムのパフォーマンスに最も大きな影響を与えるのは、大きな書き込みI/Oです。そのため、QoSスループットの上限を、データボリュームとログボリュームの対応する書き込みSAP HANAストレージパフォーマンスKPI値の割合に設定する必要があります。

共有環境

もう1つのユースケースは、負荷の高い書き込みワークロードのスループットを制限することです。特に、レイテンシの影響を受けやすい他の書き込みワークロードにこれらのワークロードが影響しないようにするためです。このような環境では、非共有のスループットの上限QoSグループポリシーを各Storage Virtual Machine（SVM）内の各LUNに適用して、個 々 のストレージオブジェクトの最大スループットを指定した値に制限することを推奨します。これにより、1つのワークロードが他のワークロードに悪影響を及ぼす可能性が低くなります。

そのためには、SVMごとにONTAPクラスタのCLIを使用してグループポリシーを作成する必要があります。

```
qos policy-group create -policy-group <policy-name> -vserver <vserver
name> -max-throughput 1000MB/s -is-shared false
```

SVM内の各LUNに適用されます。次の例では、SVM内の既存のすべてのLUNにポリシーグループを適用します。

```
lun modify -vserver <vserver name>  -path * -qos-policy-group  <policy-
name>
```

この作業はSVMごとに行う必要があります。QoSポリシンググループの名前は、SVMごとに異なる名前にする必要があります。新しいLUNの場合は、ポリシーを直接適用できます。

```
lun create -vserver <vserver_name> -path  /vol/<volume_name>/<lun_name>
-size <size> -ostype <e.g. linux>  -qos-policy-group <policy-name>
```

特定のLUNの最大スループットとして1000MB/秒を使用することを推奨します。アプリケーションがより多くのスループットを必要とする場合は、LUNストライピングを備えた複数のLUNを使用して、必要な帯域幅を提

供する必要があります。このガイドでは、セクションで、Linux LVMをベースとしたSAP HANAの例を紹介します"ホスト セットアップ"。

> この制限は読み取りにも適用されます。そのため、SAP HANAデータベースの起動時間やバックアップに必要なSLAを満たす十分な数のLUNを使用します。

#### NetApp FabricPool

SAP HANA システムのアクティブなプライマリファイルシステムには、 NetApp FabricPool テクノロジを使用しないでください。これには ' データとログ領域のファイル・システムと '/hana/shared-file システムが含まれますそのため、特に SAP HANA システムの起動時に、予測不可能なパフォーマンスが発生します。

FabricPool や SnapMirror デスティネーションなどのバックアップターゲットで、 Snapshot のみの階層化ポリシーと SnapVault を併用できます。

> FabricPool を使用してプライマリストレージで Snapshot コピーを階層化するか、バックアップターゲットで FabricPool を使用すると、データベースまたはシステムクローンの作成や修復などのその他のタスクのリストアとリカバリに必要な時間が変わります。この点を考慮して、全体的なライフサイクル管理戦略を計画し、この機能を使用している間も SLA が満たされていることを確認してください。

FabricPool は、ログバックアップを別のストレージ階層に移動する場合に適しています。バックアップの移動は、 SAP HANA データベースのリカバリに要する時間に影響します。したがって 'tiering-minimum-cooling-days オプションは ' ローカルの高速ストレージ階層にログ・バックアップを配置する値に設定する必要がありますこの値は ' リカバリに日常的に必要なログ・バックアップがローカルの高速ストレージ階層に配置されます

### ストレージを設定する

以下に、必要なストレージ構成手順の概要を示します。各手順の詳細については、以降のセクションで説明します。このセクションでは、ストレージハードウェアがセットアップされており、 ONTAP ソフトウェアがすでにインストールされていることを前提としています。また、ストレージ FCP ポートと SAN ファブリックの接続がすでに確立されている必要があります。

1. の説明に従って、正しいディスク・シェルフ構成を確認します[ディスクシェルフの接続]。
2. の説明に従って、必要なアグリゲートを作成して設定します[アグリゲートの構成]。
3. の説明に従って、Storage Virtual Machine（SVM）を作成しますStorage Virtual Machine の設定。
4. の説明に従って、論理インターフェイス（LIF）を作成します[論理インターフェイスの構成]。
5. セクションの説明に従って、HANAサーバーのワールドワイド名（WWN）を持つイニシエータグループ（igroup）を作成します。 [イニシエータグループ] 。
6. セクションの説明に従って、アグリゲート内にボリュームとLUNを作成して構成します。 "単一ホスト設定"単一のホストまたはセクション内"複数ホストのセットアップ"

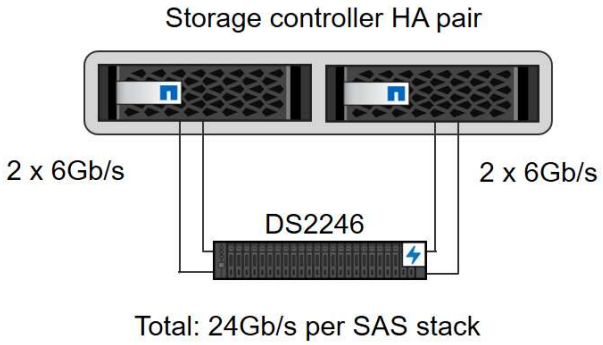
### ディスクシェルフ接続

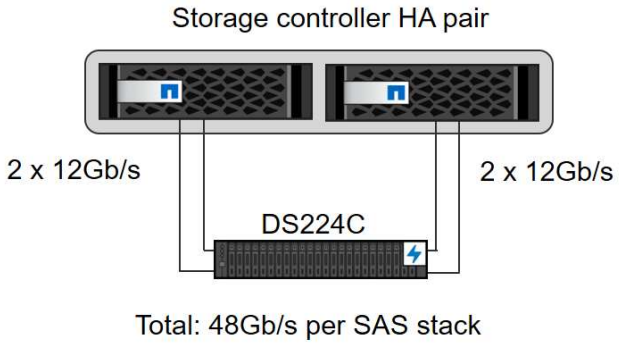
#### SAS ベースのディスクシェルフ

次の図に示すように、 1 つの SAS スタックに最大 1 台のディスクシェルフを接続して、 SAP HANA ホストに必要なパフォーマンスを実現できます。各シェルフ内のディスクは、 HA ペアの両方のコントローラに均等

に分散する必要があります。ADPv2 は、 ONTAP 9 および DS224C ディスクシェルフで使用されます。

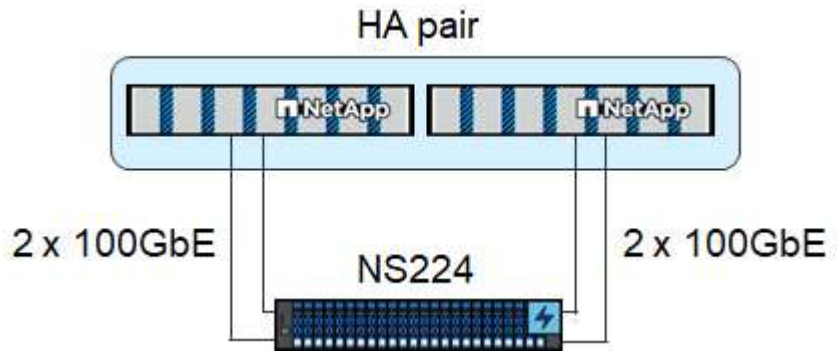
ディスクシェルフ DS224C では、クワッドパスの SAS ケーブルも使用できますが、必須ではありません。




**NVMe**ベースのディスクシェルフ

次の図に示すように、NS224 NVMeディスクシェルフは、コントローラごとに2つの100GbEポートで接続されます。各シェルフ内のディスクは、HAペアの両方のコントローラに均等に分散する必要があります。ADPv2 は、 NS224 ディスクシェルフにも使用されます。

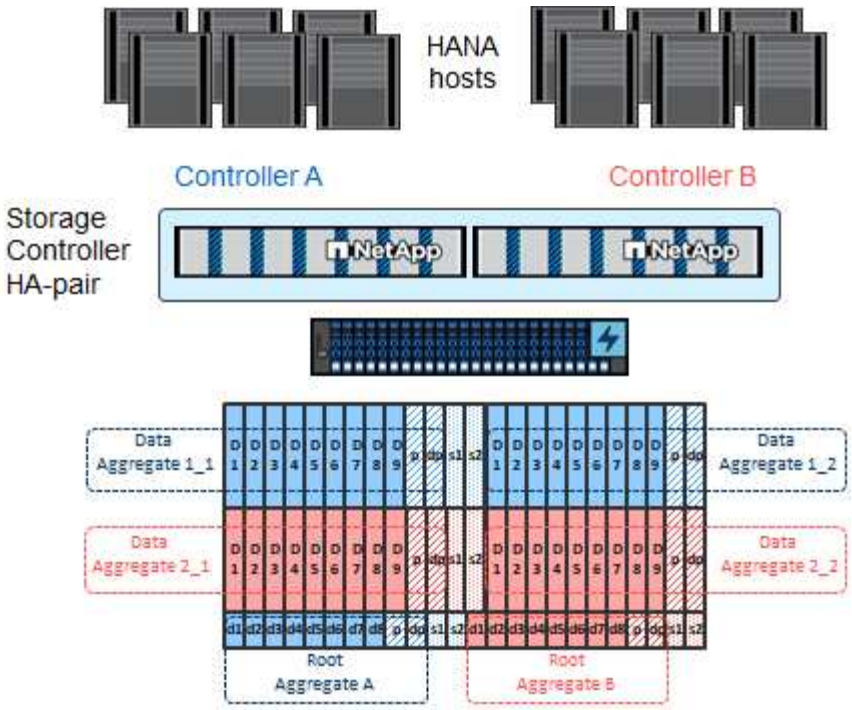



アグリゲートの構成

一般に、使用するディスクシェルフやディスクテクノロジ（ SSD または HDD ）に関係なく、コントローラごとに 2 つのアグリゲートを設定する必要があります。この手順は、使用可能なすべてのコントローラリソースを使用できるようにするために必要です。

2024年8月以降にリリースされたASAシステムでは、この手順は自動的に実行されるため必要ありません。

次の図は、 ADPv2 を使用した、 12Gb の SAS シェルフで稼働する、 12 台の SAP HANA ホストの構成を示しています。6 台の SAP HANA ホストが各ストレージコントローラに接続されています。各ストレージコントローラに 2 つずつ、合計 4 つのアグリゲートが構成されています。各アグリゲートには、 9 つのデータパーティションと 2 つのパリティディスクパーティションを含む 11 本のディスクが構成されます。各コントローラで、 2 つのスペアパーティションを使用できます。




**Storage Virtual Machine** の設定

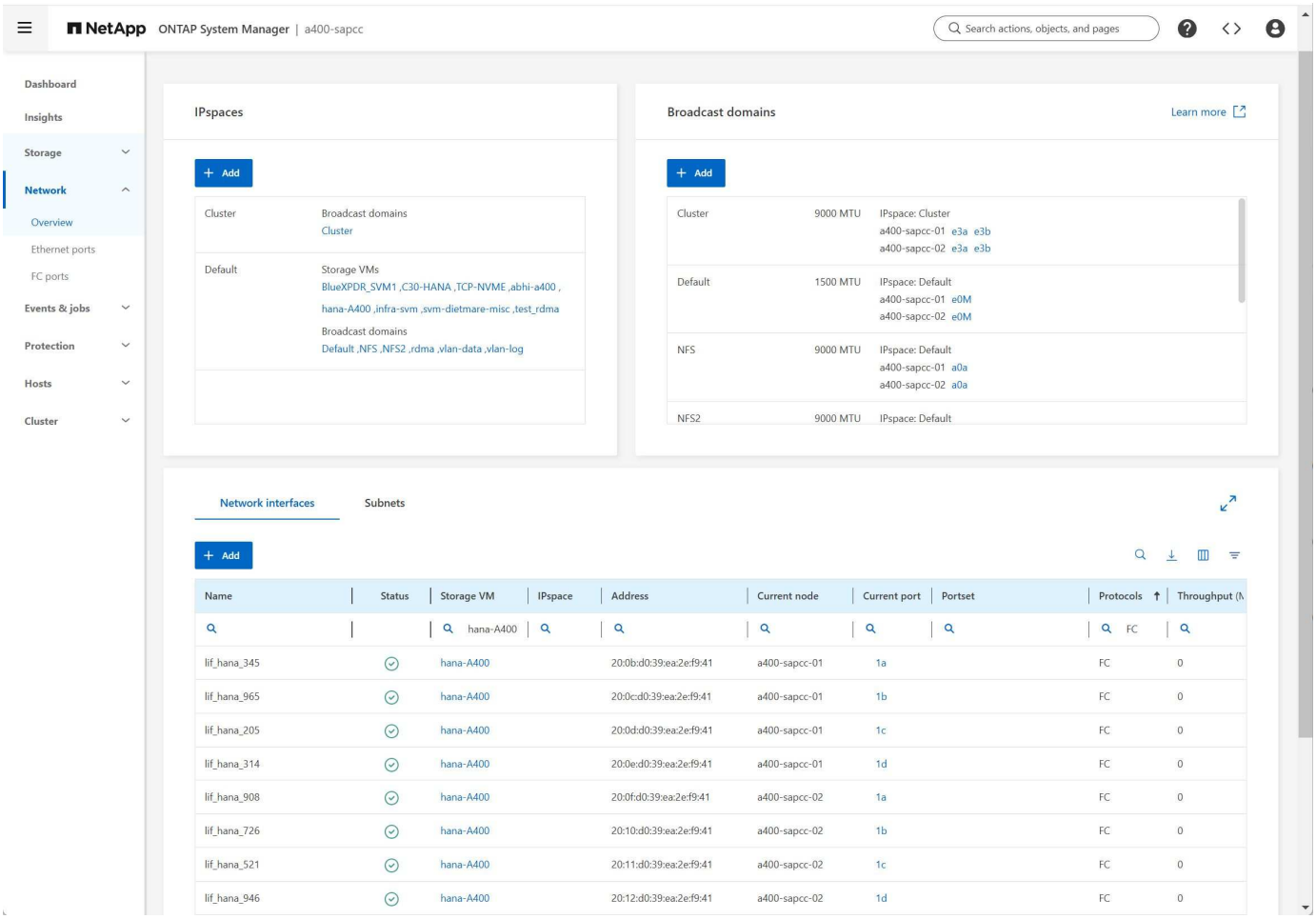
SAP HANA データベースを使用する複数の SAP ランドスケープでは、単一の SVM を使用できます。SVM は、社内の複数のチームによって管理される場合に備え、必要に応じて各 SAP ランドスケープに割り当てることもできます。

新しい SVM の作成時に自動的に作成されて割り当てられた QoS プロファイルがある場合は、この自動作成されたプロファイルを SVM から削除して、 SAP HANA に必要なパフォーマンスを確保します。

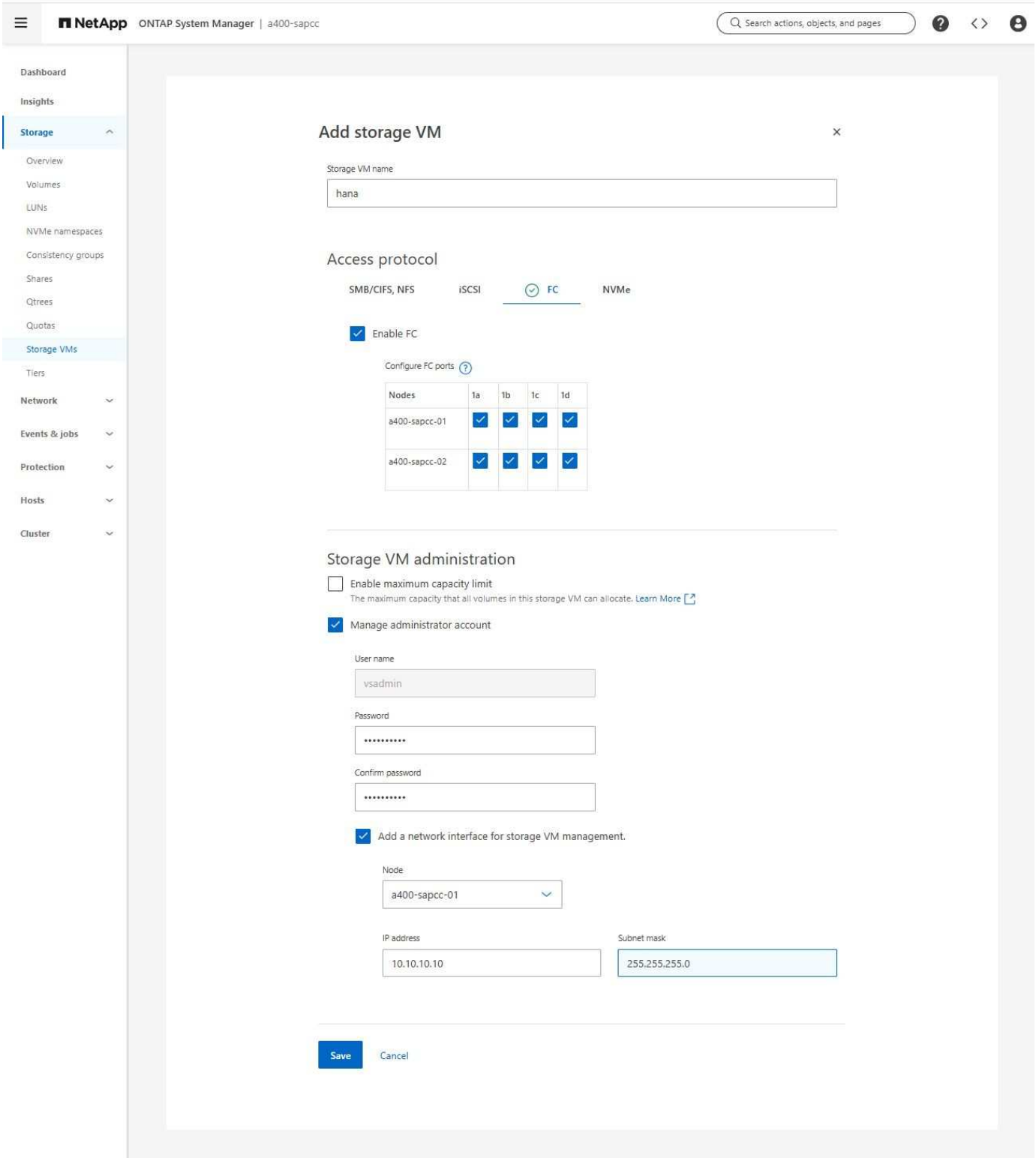
```
vserver modify -vserver <svm-name> -qos-policy-group none
```

論理インターフェイスの構成

ストレージクラスタ構成内に、 1 つのネットワークインターフェイス（ LIF ）を作成して専用の FCP ポートに割り当てる必要があります。たとえば、パフォーマンス上の理由から 4 つの FCP ポートが必要な場合は、4 つの LIF を作成する必要があります。次の図は、SVMに設定された8つのLIFのスクリーンショットを示しています。




ONTAP System Managerを使用したSVMの作成時には、必要なすべての物理FCPポートを選択でき、物理ポートごとに1つのLIFが自動的に作成されます。




イニシエータグループ

igroup は、サーバごとに、または LUN へのアクセスを必要とするサーバのグループに対して設定できます。igroup の構成には、サーバの World Wide Port Name （ WWPN ）が必要です。

「 anlun 」ツールを使用して次のコマンドを実行し、各 SAP HANA ホストの WWPN を取得します。

```
stlrx300s8-6:~ # sanlun fcp show adapter
/sbin/udevadm
/sbin/udevadm

host0 ..... WWPN:2100000e1e163700
host1 ..... WWPN:2100000e1e163701
```

この `sanlun`ツールはNetApp Host Utilitiesに含まれており、各SAP HANAホストにインストールする必要があります。詳細については、セクションを参照してください。"ホストのセットアップ："

igroupは、ONTAPクラスタのCLIを使用して作成できます。

```
lun igroup create -igroup <igroup name> -protocol fcp -ostype linux
-initiator <list of initiators> -vserver <SVM name>
```

シングルホスト

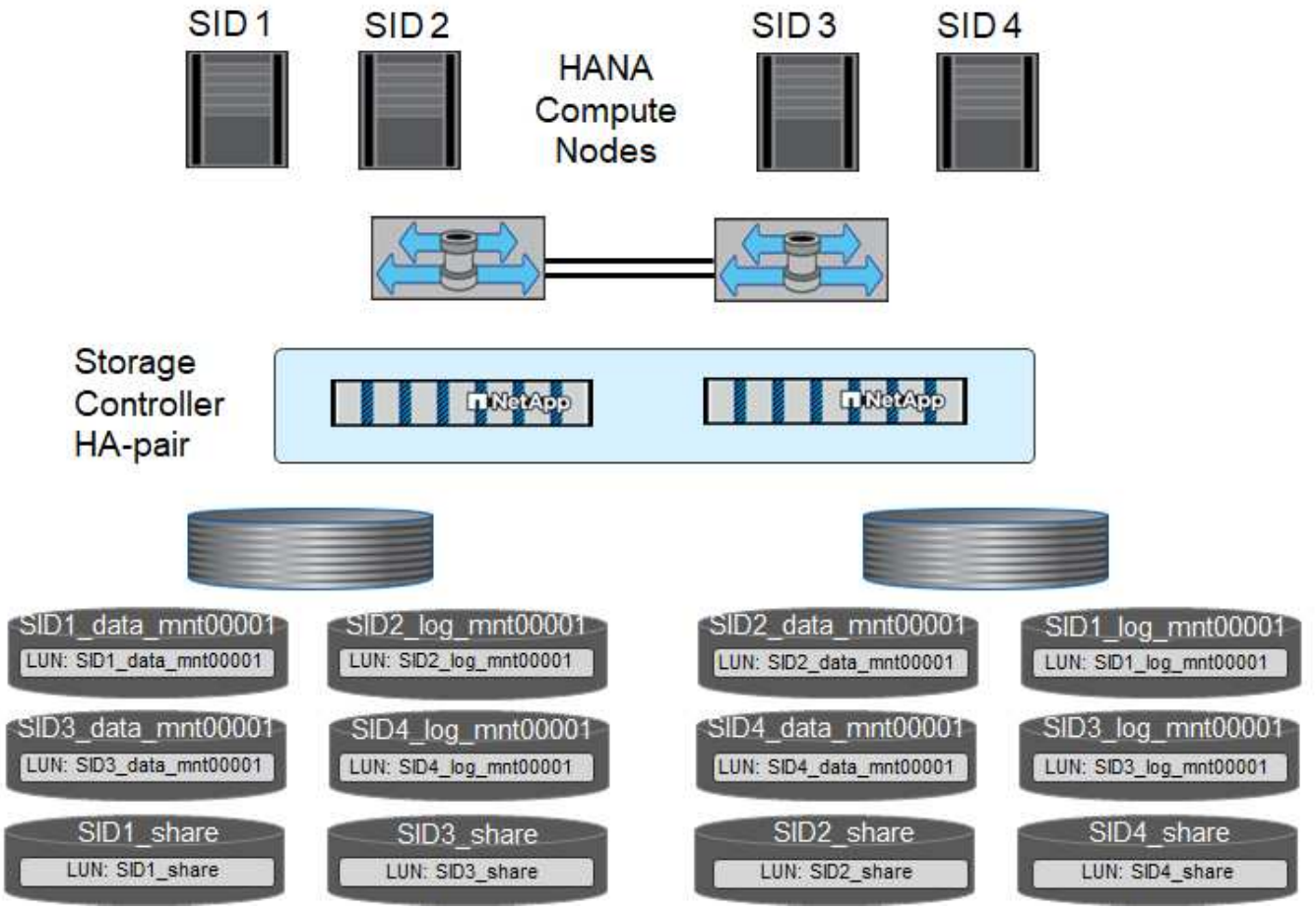
シングルホスト

## このセクションでは、SAP HANAシングルホストシステムに固有のNetAppストレージシステムの構成について説明します。

### SAP HANA シングルホストシステムのボリュームと LUN の構成

次の図は、 4 つのシングルホスト SAP HANA システムのボリューム構成を示しています。各 SAP HANA システムのデータボリュームとログボリュームは、異なるストレージコントローラに分散されます。たとえば、ボリューム「 ID1_data_mnt00001 」がコントローラ A で設定され、ボリューム「 ID1_log_mnt00001 」がコントローラ B で設定されているとします各ボリューム内で 1 つの LUN が構成されます。

HA ペアのうち、 1 台のストレージコントローラのみを SAP HANA システムに使用する場合は、データボリュームとログボリュームを同じストレージコントローラに保存することもできます。




各 SAP HANA ホストには、データボリューム、ログボリューム、「 /hana/shared 」のボリュームが構成されています。次の表は、 4 台の SAP HANA シングルホストシステムを使用した構成例を示しています。

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| システム SID1 のデータ、ログ、および共有ボリューム | データボリューム：SID1_data_mnt00001 | 共有ボリューム：SID1_shared | – | ログボリューム：SID1_log_mnt00001 |
| システム SID2 のデータボリューム、ログボリューム、および共有ボリューム | – | ログボリューム：SID2_log_mnt00001 | データボリューム：SID2_data_mnt00001 | 共有ボリューム：SID2_shared |
| システム SID3 のデータ、ログ、および共有ボリューム | 共有ボリューム：SID3_shared | データボリューム：SID3_data_mnt00001 | ログボリューム：SID3_log_mnt00001 | – |
| システム SID4 のデータボリューム、ログボリューム、および共有ボリューム | ログボリューム：SID4_log_mnt00001 | – | 共有ボリューム：SID4_shared | データボリューム：SID4_data_mnt00001 |

次の表に、シングルホストシステムのマウントポイント構成例を示します。

| LUN | SAP HANA<br>ホストのマウントポイント | 注 |
| --- | --- | --- |
| SID1_data_mnt00001 | /hana/data SID1/mnt00001 のように指定します | /etc/fstab エントリを使用してマウントされます |
| SID1_log_mnt00001 | /hana/log/s1/mnt00001 | /etc/fstab エントリを使用してマウントされます |
| SID1_shared | /hana/shareed/SID1 | /etc/fstab エントリを使用してマウントされます |

ここで説明する構成では ' ユーザ SID1adm のデフォルトのホーム・ディレクトリが格納されている /usr/sap/SID1 ディレクトリがローカル・ディスク上にありますディスク・ベースのレプリケーションを使用した災害復旧セットアップでは、すべてのファイル・システムが中央ストレージ上にあるように、 /usr/sap/SID1 ディレクトリの「 ID1_shared 」ボリューム内に追加の LUN を作成することを推奨します。

**Linux LVM** を使用した **SAP HANA** シングルホストシステムのボリュームと **LUN** の構成

Linux LVM を使用すると、パフォーマンスを向上させ、 LUN サイズの制限に対処できます。LVM ボリュームグループの各 LUN は、別のアグリゲートおよび別のコントローラに格納する必要があります。次の表に、ボリュームグループごとに 2 つの LUN を使用する例を示します。

SAP HANA KPI を満たすために複数の LUN で LVM を使用する必要はありませんが、使用することをお勧めします。

| 目的 | コントローラ **A**<br>のアグリゲート **1** | コントローラ **A**<br>のアグリゲート **2** | コントローラ **B**<br>のアグリゲート **1** | コントローラ **B**<br>のアグリゲート **2** |
| --- | --- | --- | --- | --- |
| LVM ベースのシステムのデータ、ログ、および共有ボリューム | データボリューム：SID1_data_mnt00001 | 共有ボリューム：SID1_shared log2 ボリューム：SID1_log2_mnt00001 | data2 ボリューム：SID1_data2_mnt00001 | ログボリューム：SID1_log_mnt00001 |

ボリュームのオプション

次の表にリストされているボリューム オプションは、SAP HANA に使用されるすべてのボリュームで検証および設定する必要があります。

| アクション | **ONTAP 9** |
| --- | --- |
| Snapshot コピーの自動作成を無効にする | vol modify – vserver <vserver-name> -volume <volname> -snapshot-policy none と指定します |
| Snapshot ディレクトリの可視化を無効にします | vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false |

**CLI** を使用して **LUN** を作成し、**LUN** をイニシエータ グループにマッピングする

このセクションでは、LVM と LVM ボリューム グループごとに 2 つの LUN を使用する SID FC5 の SAP HANA 単一ホスト システムに対して、ONTAP 9 のコマンド ラインを使用した構成例を示します。

1. 必要なボリュームをすべて作成します。

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. すべての LUN を作成します。

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. FC5 のシステム ホストに属するすべてのポートのイニシエーター グループを作成します。

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb -vserver hana
```

4. 作成したイニシエータグループにすべての LUN をマッピングします。

```
lun map -path /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
```



複数のホスト

## このセクションでは、SAP HANAマルチホストシステムに固有のNetAppストレージシステムの構成について説明します。

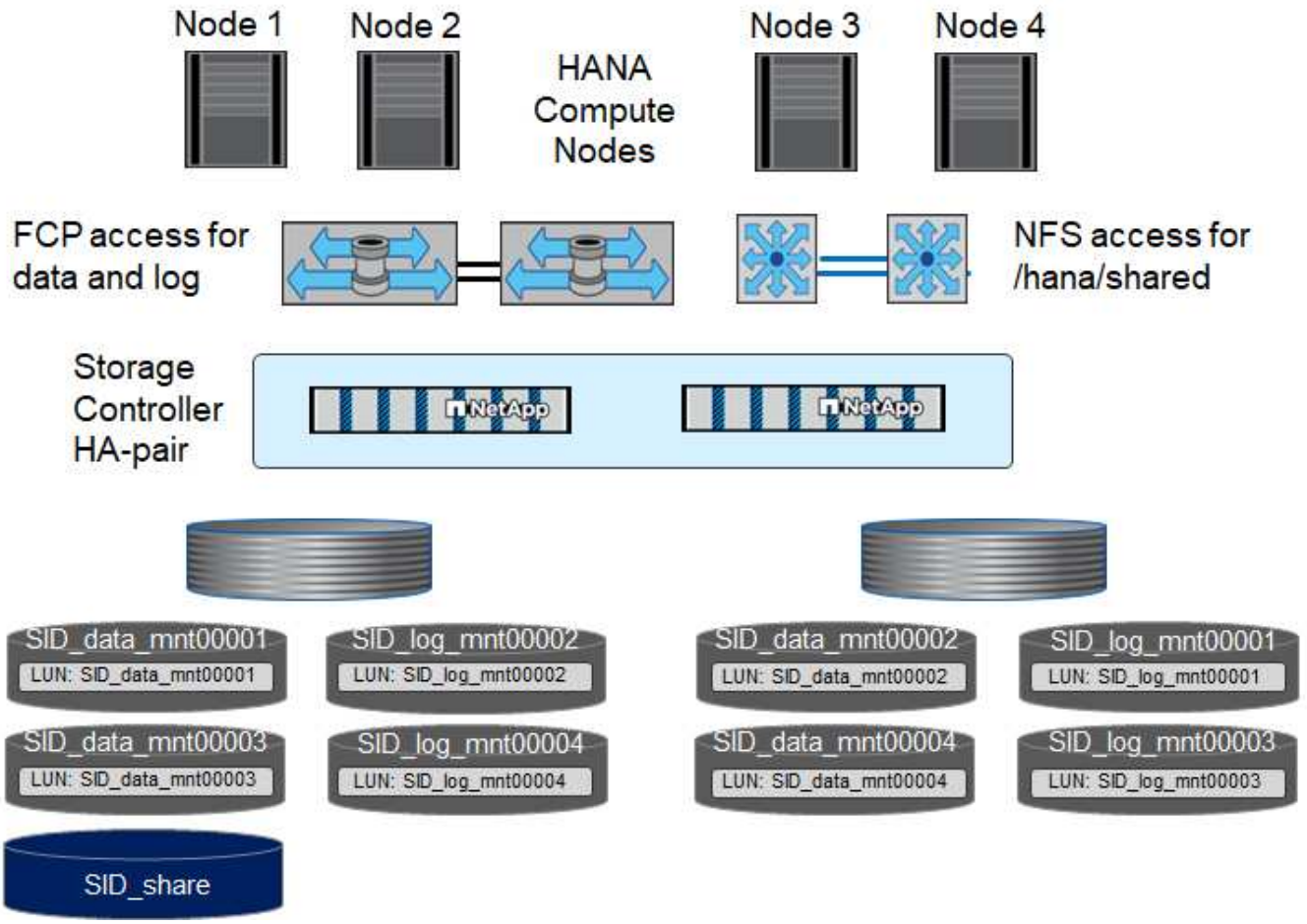
### SAP HANA マルチホストシステムのボリュームと LUN の構成

次の図は、 4+1 のマルチホスト SAP HANA システムのボリューム構成を示しています。各 SAP HANA ホストのデータボリュームとログボリュームは、異なるストレージコントローラに分散されます。たとえば、ボリューム「 `S ID_data_mnt00001 」はコントローラ A に設定され、ボリューム「 S ID_LOG_mnt00001 」はコントローラ B に設定されています各ボリュームに 1 つの LUN を設定します。

「 /hana/shared 」ボリュームは、すべての HANA ホストからアクセスできる必要があり、 NFS を使用してエクスポートされます。「 /hana/shared 」ファイルシステムには特定のパフォーマンス KPI がありませんが、 10Gb のイーサネット接続を使用することを推奨します。

HA ペアのうち、 1 台のストレージコントローラのみを SAP HANA システムに使用する場合は、データボリュームとログボリュームを同じストレージコントローラに保存することもできます。

NetApp ASAシステムは、プロトコルとして NFS をサポートしていません。 NetAppは、追加のAFFまたはFASシステムを使用することを推奨しています。 `/hana/shared`ファイルシステム。




各 SAP HANA ホストには、 1 個のデータボリュームと 1 個のログボリュームが作成されます。「 /hana/shared 」ボリュームは、 SAP HANA システムのすべてのホストで使用されます。次の表に、 4+1 のマルチホスト SAP HANA システムの構成例を示します。

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| ノード 1 のデータボリュームとログボリューム | データボリューム： SID_data_mnt00001 | – | ログボリューム： SID_log_mnt00001 | – |
| ノード 2 のデータボリュームとログボリューム | ログボリューム： SID_log_mnt00002 | – | データボリューム： SID_data_mnt00002 | – |
| ノード 3 のデータボリュームとログボリューム | – | データボリューム： SID_data_mnt00003 | – | ログボリューム： SID_log_mnt00003 |
| ノード 4 のデータボリュームとログボリューム | – | ログボリューム： SID_log_mnt00004 | – | データボリューム： SID_data_mnt00004 |
| すべてのホストの共有ボリューム | 共有ボリューム： SID_shared | – | – | – |

次の表に、アクティブな SAP HANA ホストが 4 台あるマルチホストシステムの構成とマウントポイントを示

します。

| **LUN** またはボリューム | **SAP HANA** ホストのマウントポイント | 注 |
|---|---|---|
| LUN ： SID_data_mnt00001 | /hana/data/SID/mnt00001 | ストレージコネクタを使用してマウント |
| LUN ： SID_log_mnt00001 | /hana/log/sid/mnt00001 | ストレージコネクタを使用してマウント |
| LUN ： SID_data_mnt00002 | /hana/data/sid/mnt00002 | ストレージコネクタを使用してマウント |
| LUN ： SID_log_mnt00002 | /hana/log/sid/mnt00002 | ストレージコネクタを使用してマウント |
| LUN ： SID_data_mnt00003 | /hana/data/sid/mnt00003 | ストレージコネクタを使用してマウント |
| LUN ： SID_log_mnt00003 | /hana/log/sid/mnt00003 | ストレージコネクタを使用してマウント |
| LUN ： SID_data_mnt00004 | /hana/data/sid/mnt00004 | ストレージコネクタを使用してマウント |
| LUN ： SID_log_mnt00004 | /hana/log/sid/mnt00004 | ストレージコネクタを使用してマウント |
| ボリューム： SID_shared | /hana/shared にアクセスします | NFS と /etc/fstab のエントリを使用して、すべてのホストにマウントされます |

上記の構成では、ユーザ SIDadm のデフォルトのホームディレクトリが格納されている /usr/sap/SID のディレクトリは、各 HANA ホストのローカルディスクにあります。ディスク・ベースのレプリケーションを使用した災害復旧の設定では、各データベース・ホストが中央ストレージ上のすべてのファイル・システムを持つように、 /usr/sap/SID ファイル・システムの「 S ID_shared 」ボリュームに 4 つのサブディレクトリを追加作成することを推奨します。

**Linux LVM** を使用した **SAP HANA** マルチホストシステムのボリュームと **LUN** の構成

Linux LVM を使用すると、パフォーマンスを向上させ、 LUN サイズの制限に対処できます。LVM ボリュームグループの各 LUN は、別のアグリゲートおよび別のコントローラに格納する必要があります。

SAP HANA KPIを満たすために複数のLUNを組み合わせるためにLVMを使用する必要はありませんが、推奨されます。

次の表に、 2+1 の SAP HANA マルチホストシステムのボリュームグループあたり 2 つの LUN の例を示します。

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| ノード 1 のデータボリュームとログボリューム | データボリューム： SID_data_mnt00001 | ログ 2 ボリューム： SID_log2_mnt00001 | ログボリューム： SID_log_mnt00001 | data2 ボリューム： SID_data2_mnt00001 |

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| ノード 2 のデータボリュームとログボリューム | ログ 2 ボリューム：SID_log2_mnt00002 | データボリューム：SID_data_mnt00002 | data2 ボリューム：SID_data2_mnt00002 | ログボリューム：SID_log_mnt00002 |
| すべてのホストの共有ボリューム | 共有ボリューム：SID_shared | – | – | – |

ボリュームのオプション

次の表に示すボリュームオプションは、すべての SVM で検証および設定する必要があります。

| アクション | |
|---|---|
| Snapshot コピーの自動作成を無効にする | vol modify – vserver <vserver-name> -volume <volname> -snapshot-policy none と指定します |
| Snapshot ディレクトリの可視化を無効にします | vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false |

**LUN** 、ボリュームを作成し、 **LUN** をイニシエータグループにマッピングします

NetApp ONTAP System Managerを使用してストレージボリュームとLUNを作成し、それらをサーバとONTAP CLIのigroupにマッピングすることができます。このマニュアルでは、CLIの使用方法について説明します。

**CLI** を使用して **LUN** 、ボリュームを作成し、 **igroup** に **LUN** をマッピングします

このセクションでは、コマンドラインを使用した ONTAP 9 と、 SID FC5 を使用した 2+1 の SAP HANA マルチホストシステムで、 LVM ボリュームグループごとに 2 つの LUN を使用した構成例を示します。

1. 必要なボリュームをすべて作成します。

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00002  -aggregate aggr2_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data_mnt00002  -aggregate aggr2_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00002  -aggregate aggr2_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_data2_mnt00002  -aggregate aggr2_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. すべての LUN を作成します。

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data_mnt00002/FC5_data_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00002/FC5_log_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. システム FC5 に属するすべてのサーバのイニシエータグループを作成します。

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator
10000090fadcc5fa,10000090fadcc5fb,10000090fadcc5c1,10000090fadcc5c2,1000
0090fadcc5c3,10000090fadcc5c4 -vserver hana
```

4. 作成したイニシエータグループにすべての LUN をマッピングします。

```
lun map -path /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_data_mnt00002/FC5_data_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log_mnt00002/FC5_log_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002  -igroup HANA-FC5
```

#### SAP HANA Storage Connector API

ストレージコネクタは、フェイルオーバー機能を備えたマルチホスト環境でのみ必要です。マルチホスト構成では、 SAP HANA に高可用性機能が提供されるため、 SAP HANA データベースホストはスタンバイホストにフェイルオーバーできます。

この場合、障害が発生したホストの LUN には、スタンバイホストからアクセスして使用されます。ストレージコネクタは、一度に 1 つのデータベースホストだけがストレージパーティションにアクティブにアクセスできるようにするために使用されます。

ネットアップストレージを使用した SAP HANA マルチホスト構成では、 SAP が提供する標準のストレージコネクタが使用されます。『 SAP HANA Fibre Channel Storage Connector Admin Guide 』は、への添付ファイルとして提供されています "SAP ノート 1900823"。

ホストのセットアップ

ホストをセットアップする前に、 NetApp SAN Host Utilities をからダウンロードしておく必要があります "ネットアップサポート" HANA サーバにインストールします。ホスト・ユーティリティのマニュアルには、使用する FCP HBA に応じてインストールする必要がある追加ソフトウェアの情報が記載されています。

また、使用している Linux バージョンに固有のマルチパス構成に関する情報も記載されています。このドキュメントでは、 SLES 12 SP1 以降および RHEL 7 で必要な設定手順について説明します。2 以降。を参照してください "『 Linux Host Utilities 7.1 Installation and Setup Guide 』"。

マルチパスを設定します

SAP HANA マルチホスト構成のすべてのワーカーホストとスタンバイホストで、手順 1~6 を実行する必要があります。

マルチパスを設定するには、次の手順を実行します。

1. 各サーバで Linux の「 re scan-scsi-bus.sh -a' 」コマンドを実行して、新しい LUN を検出します。
2. 実行 `sanlun lun show`コマンドを実行し、必要なLUNがすべて表示されていることを確認します。次

の例は、 `sanlun lun show` 2つのデータLUNと2つのログLUNを持つ2+1マルチホストHANAシステムのコマンド出力。出力には、LUNと対応するデバイスファイル（LUNなど）が表示されます。 `FC5_data_mnt00001`デバイスファイル `/dev/sdag`各 LUN には、ホストからストレージ コントローラへの FC パスが 8 つあります。

```
sapcc-hana-tst:~ # sanlun lun show
controller(7mode/E-Series)/                                    device
host                  lun
vserver(cDOT/FlashRay)        lun-pathname                     filename
adapter    protocol   size    product
------------------------------------------------------------------------
---------------------------------------
svm1                          FC5_log2_mnt00002                /dev/sdbb
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdba
host21     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001                /dev/sdaz
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001                 /dev/sday
host21     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002               /dev/sdax
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002                /dev/sdaw
host21     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001               /dev/sdav
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001                /dev/sdau
host21     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002                /dev/sdat
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdas
host21     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001                /dev/sdar
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001                 /dev/sdaq
host21     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002               /dev/sdap
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002                /dev/sdao
host21     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001               /dev/sdan
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001                /dev/sdam
host21     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002                /dev/sdal
host20     FCP        500g    cDOT
```

```
svm1                            FC5_log_mnt00002              /dev/sdak
host20     FCP         500g     cDOT
svm1                            FC5_log2_mnt00001             /dev/sdaj
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001              /dev/sdai
host20     FCP         500g     cDOT
svm1                            FC5_data2_mnt00002            /dev/sdah
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00002             /dev/sdag
host20     FCP         1t       cDOT
svm1                            FC5_data2_mnt00001            /dev/sdaf
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001             /dev/sdae
host20     FCP         1t       cDOT
svm1                            FC5_log2_mnt00002             /dev/sdad
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00002              /dev/sdac
host20     FCP         500g     cDOT
svm1                            FC5_log2_mnt00001             /dev/sdab
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001              /dev/sdaa
host20     FCP         500g     cDOT
svm1                            FC5_data2_mnt00002            /dev/sdz
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00002             /dev/sdy
host20     FCP         1t       cDOT
svm1                            FC5_data2_mnt00001            /dev/sdx
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001             /dev/sdw
host20     FCP         1t       cDOT
```

3. 実行 `multipath -r`そして `multipath -ll`デバイス ファイル名のワールドワイド識別子 (WWID) を取得するコマンド。

この例では、8 つの LUN があります。

```
sapcc-hana-tst:~ # multipath -r
sapcc-hana-tst:~ # multipath -ll
3600a098038314e63492b59326b4b786d dm-7 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
```

```
  `- 21:0:6:2 sdan 66:112 active ready running
3600a098038314e63492b59326b4b786e dm-9 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
3600a098038314e63492b59326b4b786f dm-11 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
3600a098038314e63492b59326b4b7870 dm-13 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
3600a098038314e63532459326d495a64 dm-6 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
3600a098038314e63532459326d495a65 dm-8 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
3600a098038314e63532459326d495a66 dm-10 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
```

```
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
3600a098038314e63532459326d495a67 dm-12 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

4. /etc/multipath.conf ファイルを編集し 'WWID とエイリアス名を追加します

> 出力例は '2+1 マルチホスト・システムの 4 つの LUN のエイリアス名を含む /etc/multipath.conf ファイルの内容を示しています使用可能な multipath.conf ファイルがない場合、「 multipath-T 」 /etc/multipath.conf を実行して作成できます。

```
sapcc-hana-tst:/ # cat /etc/multipath.conf
multipaths {
                multipath {
                wwid    3600a098038314e63492b59326b4b786d
                alias   svm1-FC5_data2_mnt00001
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786e
                alias   svm1-FC5_data2_mnt00002
        }
        multipath {
                wwid    3600a098038314e63532459326d495a64
                alias   svm1-FC5_data_mnt00001
        }
        multipath {
                wwid    3600a098038314e63532459326d495a65
                alias   svm1-FC5_data_mnt00002
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786f
                alias   svm1-FC5_log2_mnt00001
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b7870
                alias   svm1-FC5_log2_mnt00002
        }
        multipath {
                wwid    3600a098038314e63532459326d495a66
                alias   svm1-FC5_log_mnt00001
        }
        multipath {
                wwid    3600a098038314e63532459326d495a67
                alias   svm1-FC5_log_mnt00002
        }


}
```

5. 「 multipath -r 」コマンドを実行して、デバイスマップをリロードします。
6. すべての LUN 、エイリアス名、およびアクティブパスとスタンバイパスを一覧表示するには、「マルチパス -ll 」コマンドを実行して構成を確認します。



次の出力例は、 2 つのデータ LUN と 2 つのログ LUN を持つ 2+1 マルチホスト HANA システムの出力を示しています。

```
sapcc-hana-tst:~ # multipath -ll
hsvm1-FC5_data2_mnt00001 (3600a098038314e63492b59326b4b786d) dm-7
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
svm1-FC5_data2_mnt00002 (3600a098038314e63492b59326b4b786e) dm-9
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
svm1-FC5_data_mnt00001 (3600a098038314e63532459326d495a64) dm-6
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
svm1-FC5_data_mnt00002 (3600a098038314e63532459326d495a65) dm-8
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
svm1-FC5_log2_mnt00001 (3600a098038314e63492b59326b4b786f) dm-11
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
```

```
svm1-FC5_log2_mnt00002 (3600a098038314e63492b59326b4b7870) dm-13
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
svm1-FC5_log_mnt00001 (3600a098038314e63532459326d495a66) dm-10
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
svm1-FC5_log_mnt00002 (3600a098038314e63532459326d495a67) dm-12
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

単一ホスト設定

単一ホスト設定

# この章では、LINUX LVM を使用した SAP HANA 単一ホストのセットアップについて説明します。

### SAP HANA 単一ホストシステムの LUN 構成

次の表に示すように、 SAP HANA ホストで、ボリュームグループと論理ボリュームを作成してマウントする必要があります。

| 論理ボリューム / LUN | SAP HANA<br>ホストのマウントポイント | 注 |
|---|---|---|
| lv ： FC5_data_mnt0000 -vol | /hana/data/FC51/mnt00001 | /etc/fstab エントリを使用してマウントされます |
| lv ： FC5_log_mnt00001 -vol | /hana/log/FC5/mnt00001 | /etc/fstab エントリを使用してマウントされます |

| 論理ボリューム / **LUN** | **SAP HANA**<br>ホストのマウントポイント | 注 |
| --- | --- | --- |
| LUN：FC5_shared | /hana/shareed/FC5 | /etc/fstab エントリを使用してマウントされます |

説明した構成では、 `/usr/sap/FC5`ユーザー FC5adm のデフォルトのホーム ディレクトリが格納されているディレクトリは、ローカル ディスク上にあります。ディスクベースのレプリケーションによる災害復旧設定では、 NetAppは、 `FC5_shared`のボリューム `/usr/sap/FC5`すべてのファイルシステムが中央ストレージ上に存在するようにディレクトリを作成します。

**LVM** ボリュームグループと論理ボリュームを作成

1. すべての LUN を物理ボリュームとして初期化します。

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001
```

2. 各データパーティションとログパーティションのボリュームグループを作成します。

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
```

3. データパーティションとログパーティションごとに論理ボリュームを作成します。ボリュームグループごとに使用されている LUN の数（この例では 2 つ）と同じストライプサイズを使用し、データの場合は 256K 、ログの場合は 64k を使用します。SAP では、ボリュームグループごとに 1 つの論理ボリュームのみがサポートされます。

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. その他すべてのホストで、物理ボリューム、ボリュームグループ、およびボリュームグループをスキャンします。

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

これらのコマンドでボリュームが見つからない場合は、再起動する必要があります。

論理ボリュームをマウントするには、論理ボリュームをアクティブ化する必要があります。ボリュームをアクティブ化するには、次のコマンドを実行します。

```
vgchange -a y
```

ファイルシステムの作成

すべてのデータおよびログ論理ボリュームと hana 共有 LUN に XFS ファイル システムを作成します。

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs /dev/mapper/svm1-FC5_shared
```

マウントポイントを作成する

必要なマウント ポイント ディレクトリを作成し、データベース ホストの権限を設定します。

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod –R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod –R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

ファイルシステムをマウント

システム起動中にファイルシステムをマウントするには、 `/etc/fstab`設定ファイルに必要なファイルシステムを追加し、 `/etc/fstab`設定ファイル:

```
# cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/FC5_log_mnt00001-vol /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/FC5_data_mnt00001-vol /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
```



データ LUN とログ LUN の XFS ファイルシステムは 'relatim' および inode64' マウントオプションを使用してマウントする必要があります

ファイルシステムをマウントするには、 `mount –a`ホストでコマンドを実行します。

# 複数ホストの設定

この章では、2+1 SAP HANA マルチホストシステムのセットアップを例として説明します。

## SAP HANA マルチホストシステムの LUN 構成

次の表に示すように、 SAP HANA ホストで、ボリュームグループと論理ボリュームを作成してマウントする必要があります。

| 論理ボリューム（ **LV** ）またはボリューム | **SAP HANA** ホストのマウントポイント | 注 |
|---|---|---|
| lv ： FC5_data_mnt00001 -vol | /hana/data FC5/mnt00001 のように指定します | ストレージコネクタを使用してマウント |
| lv ： FC5_log_mnt00001 -vol | /hana/log/FC5/mnt00001 | ストレージコネクタを使用してマウント |
| lv ： FC5_data_mnt00002 -vol | /hana/data FC5/mnt00002 のように指定します | ストレージコネクタを使用してマウント |
| lv ： FC5_log_mnt00002 -vol | /hana/log/FC5/mnt00002 | ストレージコネクタを使用してマウント |
| ボリューム: FC5_shared | /hana/shared にアクセスします | NFS と /etc/fstab のエントリを使用して、すべてのホストにマウントされます |

説明した構成では、 `/usr/sap/FC5`ユーザー FC5adm のデフォルトのホーム ディレクトリが格納されているディレクトリは、各 HANA ホストのローカル ディスク上にあります。ディスクベースのレプリケーションによる災害復旧設定では、 NetAppは、以下の4つの追加サブディレクトリを作成することを推奨しています。 `FC5_shared`のボリューム `/usr/sap/FC5`ファイル システムを作成して、各データベース ホストのすべてのファイル システムを中央ストレージ上に配置します。

## LVM ボリュームグループと論理ボリュームを作成

1. すべての LUN を物理ボリュームとして初期化します。

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001
pvcreate /dev/mapper/hana-FC5_data_mnt00002
pvcreate /dev/mapper/hana-FC5_data2_mnt00002
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001
pvcreate /dev/mapper/hana-FC5_log_mnt00002
pvcreate /dev/mapper/hana-FC5_log2_mnt00002
```

2. 各データパーティションとログパーティションのボリュームグループを作成します。

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_data_mnt00002 /dev/mapper/hana-FC5_data_mnt00002
/dev/mapper/hana-FC5_data2_mnt00002
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
vgcreate FC5_log_mnt00002 /dev/mapper/hana-FC5_log_mnt00002
/dev/mapper/hana-FC5_log2_mnt00002
```

3. データパーティションとログパーティションごとに論理ボリュームを作成します。ボリュームグループごとに使用されている LUN の数（この例では 2 つ）と同じストライプサイズを使用し、データの場合は 256K 、ログの場合は 64k を使用します。SAP では、ボリュームグループごとに 1 つの論理ボリュームのみがサポートされます。

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. その他すべてのホストで、物理ボリューム、ボリュームグループ、およびボリュームグループをスキャンします。

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

これらのコマンドでボリュームが見つからない場合は、再起動する必要があります。

論理ボリュームをマウントするには、論理ボリュームをアクティブ化する必要があります。ボリュームをアクティブ化するには、次のコマンドを実行します。

```
vgchange -a y
```

ファイルシステムの作成

すべてのデータおよびログ論理ボリュームに XFS ファイル システムを作成します。

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_data_mnt00002-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs FC5_log_mnt00002-vol
```

マウントポイントを作成する

必要なマウント ポイント ディレクトリを作成し、すべてのワーカー ホストとスタンバイ ホストの権限を設定します。

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod -R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod -R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

ファイルシステムをマウント

マウントするには `/hana/shared`システム起動時にファイルシステムを使用する `/etc/fstab`設定ファイルに、`/hana/shared`ファイルシステムに `/etc/fstab`各ホストの構成ファイル。

```
sapcc-hana-tst:/ # cat /etc/fstab
<storage-ip>:/hana_shared /hana/shared nfs rw,vers=3,hard,timeo=600,
intr,noatime,nolock 0 0
```

すべてのデータファイルシステムとログファイルシステムは、 SAP HANA ストレージコネクタを使用してマウントされます。

ファイルシステムをマウントするには、各ホストで「 mount – a 」コマンドを実行します。

**SAP HANA** の **I/O** スタック構成

## SAP HANA 1.0 SPS10 以降、 I/O 動作を調整し、使用中のファイルシステムとストレージシステムのデータベースを最適化するためのパラメータが導入されています。

ネットアップは、最適な値を定義するため、パフォーマンステストを実施しました。次の表に、パフォーマンステストから推定した最適な値を示します。

| パラメータ | 価値 |
| --- | --- |
| max_parallel _io_requests と入力します | 128 |

| パラメータ | 価値 |
| --- | --- |
| async _read_submit | オン |
| async ： write_submit_active | オン |
| async_write_submit_bblocks | すべて |

S12 までの SAP HANA 1.0 では、 SAP ノートに記載されているように、 SAP HANA データベースのインストール時にこれらのパラメータを設定できます "2267798 – Configuration of the SAP HANA Database During Installation Using hdbparam 』で説明されています"。

また、パラメータは、 SAP HANA データベースのインストール後に「 hdbparam 」フレームワークを使用して設定することもできます。

```
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_read_submit=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

SAP HANA 2.0 以降 'hdbparam' は廃止され ' パラメータは global.ini` ファイルに移動されますパラメータは、 SQL コマンドまたは SAP HANA Studio を使用して設定できます。詳細については、 SAP ノートを参照してください "2399079 ： HANA で hdbparam の除去 2"。パラメータは 'global.ini` ファイル内で設定することもできます

```
SS3adm@stlrx300s8-6: /usr/sap/SS3/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

SAP HANA 2.0 SPS5 以降では、「 setParameter.py 」スクリプトを使用して正しいパラメータを設定します。

```
fc5adm@sapcc-hana-tst-03:/usr/sap/FC5/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

**SAP HANA** ソフトウェアのインストール

## このセクションでは、シングルホストシステムとマルチホストシステムに SAP HANA をインストールするために必要な準備について説明します。

### シングルホストシステムへのインストール

SAP HANA ソフトウェアのインストールでは、シングルホストシステムについて行う追加の準備作業はありません。

### マルチホストシステムへのインストール

インストールを開始する前に 'global.ini` ファイルを作成して 'SAP ストレージ・コネクタの使用を有効にしますSAP ストレージコネクタは、インストールプロセス中にワーカーホストで必要なファイルシステムをマウントします。global.ini` ファイルは '/hana/shared ファイル・システムなど ' すべてのホストからアクセス可能なファイル・システムで使用できる必要があります

マルチホストシステムに SAP HANA ソフトウェアをインストールする前に、次の手順を実行する必要があります。

1. データ LUN およびログ LUN の次のマウント・オプションを global.ini` ファイルに追加します
   - 「データとログファイルシステム」の「 relatime 」と「 inode64 」です
2. データパーティションとログパーティションの WWID を追加します。WWID は '/etc/multipath.conf' ファイルに設定されているエイリアス名と一致している必要があります

   次の出力は、SID=FC5 の LVM を使用した 2+1 のマルチホスト セットアップの例を示しています。

```
sapcc-hana-tst-03:/hana/shared # cat global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/FC5
basepath_logvolumes = /hana/log/FC5
[storage]
ha_provider = hdb_ha.fcClientLVM
partition_*_*__prtype = 5
partition_*_data__mountOptions = -o relatime,inode64
partition_*_log__mountOptions = -o relatime,inode64
partition_1_data__lvmname = FC5_data_mnt00001-vol
partition_1_log__lvmname = FC5_log_mnt00001-vol
partition_2_data__lvmname = FC5_data_mnt00002-vol
partition_2_log__lvmname = FC5_log_mnt00002-vol
sapcc-hana-tst-03:/hana/shared #
```

SAP hdblcm インストール ツールを使用して、ワーカー ホストの 1 つで次のコマンドを実行してインストールを開始します。オプションを使用し `addhosts`て、2番目のワーカー（sapc-hana-tst-06）とスタンバイホスト（sapc-hana-tst-07）を追加します。

準備したファイルが格納されているディレクトリ `global.ini`は( --storage_cfg=/hana/shared`、CLIオプションに含まれてい `storage_cfg`ます）。

使用する OS のバージョンによっては、 SAP HANA データベースをインストールする前に Python 2.7 をインストールする必要があります。

```
./hdblcm --action=install --addhosts=sapcc-hana-tst
-06:role=worker:storage_partition=2,sapcc-hana-tst-07:role=standby
--storage_cfg=/hana/shared/

AP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
```

```
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1
(1.015.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
```

```
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip


SAP HANA Database version '2.00.073.00.1695288802' will be installed.

Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------------
---------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version
2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
  9     | epmmds          | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
4.203.2321.0.0

Enter comma-separated list of the selected indices [3,4]: 2,3
```

3. 選択したすべてのコンポーネントが、すべてのワーカーホストとスタンバイホストにインストールされていることを確認します。

**SAP HANA** シングルホストシステムのデータボリュームパーティションを追加します

SAP HANA 2.0 SPS4 以降では、追加のデータボリュームパーティションを構成できます。この機能を使用すると、 SAP HANA テナントデータベースのデータボリュームに複数の LUN を設定し、単一 LUN のサイズやパフォーマンスの制限を超えて拡張することができます。

SAP HANA KPI を達成するために複数のパーティションを使用する必要はありません。単一の LUN にパーティションが 1 つあると、必要な KPI が満たされます。

データボリュームに複数の個別の LUN を使用することは、 SAP HANA シングルホストシステムでのみ可能です。SAP HANA マルチホストシステムに必要な SAP ストレージコネクタは、データボリュームに対して 1 つのデバイスのみをサポートします。

データボリュームのパーティションはいつでも追加できますが、 SAP HANA データベースの再起動が必要になる場合があります。

#### 追加のデータボリュームパーティションの有効化

追加のデータボリュームパーティションを有効にするには、次の手順を実行します。

1. global.ini` ファイル内に次のエントリを追加します

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

2. データベースを再起動して機能を有効にしてください。SAP HANA Studio でパラメータを global.ini` ファイルに追加する際に Systemdb 設定を使用すると、データベースが再起動されなくなります。

#### ボリュームと **LUN** の構成

ボリュームと LUN のレイアウトは、 1 つのデータボリュームパーティションを持つ単一のホストのレイアウトに似ていますが、ログボリュームとして別のアグリゲートに追加のデータボリュームと LUN が格納され、残りのデータボリュームも同じです。次の表は、 2 つのデータボリュームパーティションを持つ SAP HANA シングルホストシステムの構成例を示しています。

| コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|
| データボリューム： SID_data_mnt00001 | 共有ボリューム： SID_shared | データボリューム： SID_data2_mnt00001 | ログボリューム： SID_log_mnt00001 |

次の表に、 2 つのデータボリュームパーティションを持つシングルホストシステムのマウントポイント構成の例を示します。

| **LUN** | **HANA** ホストのマウントポイント | 注 |
|---|---|---|
| SID_data_mnt00001 | /hana/data/SID/mnt00001 | /etc/fstab エントリを使用してマウントされます |
| SID_data2_mnt00001 | /hana/data2/SID/mnt00001 | /etc/fstab エントリを使用してマウントされます |
| SID_log_mnt00001 | /hana/log/sid/mnt00001 | /etc/fstab エントリを使用してマウントされます |
| SID_shared | /hana/shared-SID を指定します | /etc/fstab エントリを使用してマウントされます |

ONTAP システムマネージャまたは ONTAP CLI を使用して、新しいデータ LUN を作成します。

ホストの設定

ホストを設定するには、次の手順を実行します。

1. 追加のLUNのマルチパスを設定します。 "ホスト セットアップ" 。
2. HANA システムに属する追加の各 LUN に XFS ファイルシステムを作成します。

```
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana-FC5_data2_mnt00001
```

3. 追加のファイル・システム /s を '/etc/fstab 構成ファイルに追加します

> データとログ LUN の XFS ファイルシステムは 'relatim' および inode64' マウントオプションを使用してマウントする必要があります

```
stlrx300s8-6:/ # cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/hana-FC5_log_mnt00001 /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/hana-FC5_data_mnt00001 /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/hana-FC5_data2_mnt00001 /hana/data2/FC5/mnt00001 xfs
relatime,inode64 0 0
```

4. マウントポイントを作成し、データベースホストに権限を設定します。

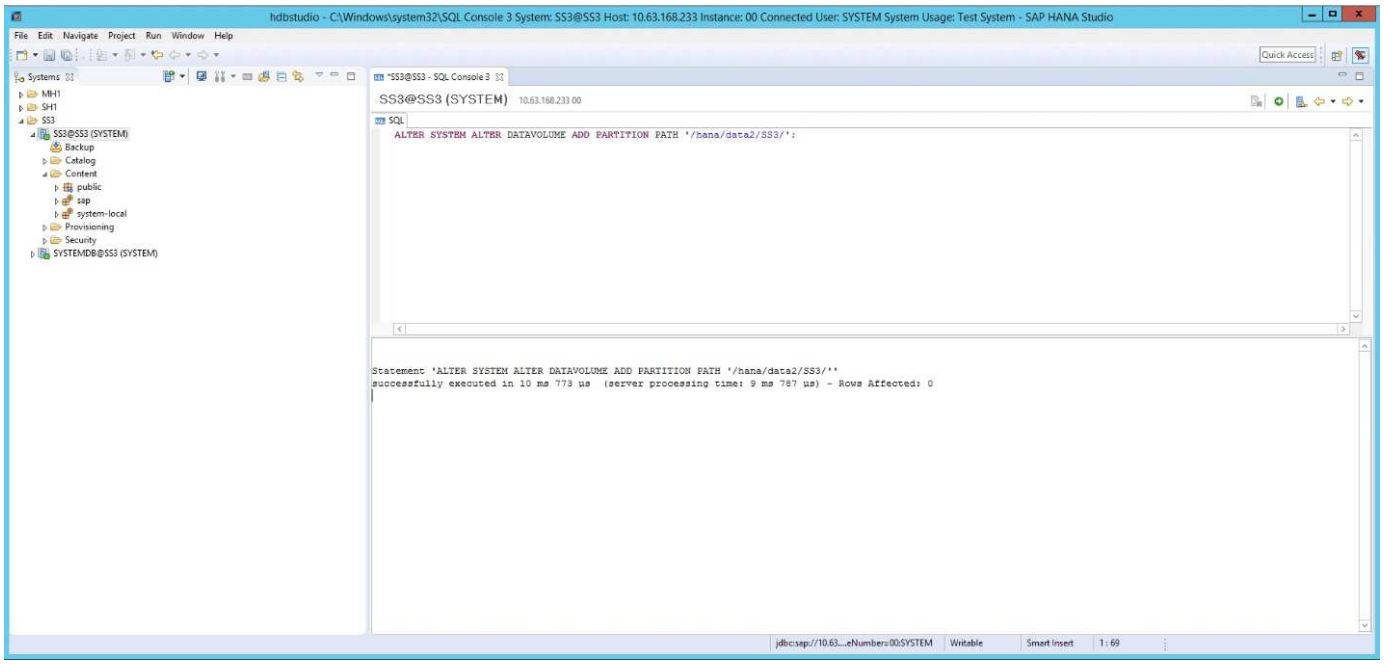
```
stlrx300s8-6:/ # mkdir -p /hana/data2/FC5/mnt00001
stlrx300s8-6:/ # chmod -R 777 /hana/data2/FC5
```

5. ファイルシステムをマウントし、「 mount – a 」コマンドを実行します。

データボリュームパーティションを追加しています

データボリュームパーティションをテナントデータベースに追加するには、テナントデータベースに対して次の SQL ステートメントを実行します。追加する LUN のパスはそれぞれ異なります。

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```




## 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。

- "SAP HANA ソフトウェアソリューション"
- "TR-4646 ：『 SAP HANA Disaster Recovery with Storage Replication 』"
- "TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"
- "TR-4667：『Automating SAP HANA System Copy and Clone Operations with SnapCenter 』"
- ネットアップドキュメントセンター

  "https://www.netapp.com/support-and-training/documentation/"
- SAP HANA 向け SAP 認定エンタープライズストレージハードウェア

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"
- SAP HANA のストレージ要件

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"
- 『 SAP HANA Tailored Data Center Integration Frequently Asked Questions 』

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"
- SAP HANA on VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"
- 『SAP HANA on VMware vSphere Best Practices Guide』

"https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

履歴を更新します

この解決策の初版以降には、次の技術的な変更が加えられています。

| 日付 | 概要を更新します |
| --- | --- |
| 2015年10月 | 初期バージョン |
| 2016年3月 | 容量のサイジングを更新しました |
| 2017年2月 | 新しいネットアップストレージシステムとディスクシェルフ ONTAP 9 の新機能 SLES12 SP1 および RHEL 7.2 の新しい SAP HANA リリース |
| 2017年7月 | マイナーアップデート |
| 2018年9月 | 新しいネットアップストレージシステム新しい OS リリース（ SLES12 SP3 および RHEL 7.4 ）では、 SAP HANA 2.0 SPS3 のマイナーアップデートが追加されています |
| 2019年11月 | 新しいネットアップストレージシステムと NVMe シェルフ新しい OS リリース（ SLES12 SP4 、 SLES 15 、および RHEL 7.6 ）では、マイナーアップデートが追加されています |
| 2020年4月 | 新しい AFF ASA シリーズストレージシステムでは、 SAP HANA 2.0 SPS4 以降に複数のデータパーティション機能が導入されています |
| 2020 年 6 月 | 追加情報オプションの機能に関するマイナーアップデート |
| 2021年2月 | 新しいネットアップストレージシステムをサポートする Linux LVM （ SLES15SP2 、 RHEL 8 ） |
| 2021年4月 | VMware vSphere 固有の情報を追加しました |
| 2022年9月 | 新しいOS -リリース |
| 2023年8月 | 新しいストレージシステム（AFF Cシリーズ） |
| 2024年5月 | 新しいストレージシステム（AFF Aシリーズ） |
| 2024年9月 | 新しいストレージシステム（ASA Aシリーズ） |
| 2024年11月 | 新しいストレージシステム |
| 2025年2月 | 新しいストレージシステム |
| 2025年7月 | マイナーアップデート |

# 『 SAP HANA on NetApp AFF Systems with NFS Configuration Guide 』

## 『SAP HANA on NetApp AFF Systems with NFS』-構成ガイド

NetApp AFF AシリーズおよびAFF Cシリーズ製品ファミリーは、Tailored Data Center Integration（TDI；テーラードデータセンター統合）プロジェクトでSAP HANAとの使用が認定されています。このガイドでは、NFS 用のこのプラットフォーム上の SAP HANA

# のベスト プラクティスについて説明します。

Marco Schoen 、ネットアップ

この認定は、次のモデルで有効です。

- AFF A150、AFF A20、AFF A250、AFF A30、AFF A400、AFF A50、AFF A70、AFF A1K、AFF A900 、AFF A90、AFF A800
- AFF C250、AFF C30、AFF C400、AFF C60、AFF C800、AFF C80

> NetApp AFF CシリーズにはNetApp ONTAP 9.13.1以降が必要です

SAP HANA 向けのネットアップ認定ストレージソリューションの一覧については、を参照してください "認定およびサポートされている SAP HANA ハードウェアディレクトリ"。

本ドキュメントでは、 NFS プロトコルバージョン 3 （ NFSv3 ）または NFS プロトコルバージョン 4 （ NFSv4.1 ）の ONTAP 設定要件について説明します。

> NFSバージョン3または4.1のみがサポートされます。NFSバージョン1、2、4.0、4.2はサポートされていません。

> このホワイトペーパーで説明している構成は、 SAP HANA に必要な SAP HANA KPI と、 SAP HANA に最適なパフォーマンスを達成するために必要です。ここに記載されていない設定または機能を変更すると、原因のパフォーマンスが低下したり、予期しない動作が発生したりする可能性があります。変更は、ネットアップのサポートから助言された場合にのみ実施

FCP を使用する NetApp AFF システム、および NFS または FCP を使用する FAS システムの構成ガイドは、次のリンクから入手できます。

- "FCP を使用した NetApp FAS システムでの SAP HANA"
- "NFS を使用した NetApp FAS システムでの SAP HANA"
- "FCP 搭載の NetApp AFF システム上の SAP HANA"
- "FCP 搭載の NetApp ASA システム上の SAP HANA"

次の表に、 SAP HANA データベースの構成に応じた、 NFS バージョン、 NFS ロック、および必要な分離実装についてサポートされる組み合わせを示します。

SAP HANA シングルホストシステム、またはホストの自動フェイルオーバーを使用しない複数のホストでは、 NFSv3 と NFSv4 がサポートされます。

ホストの自動フェイルオーバーを有効にした SAP HANA マルチホストシステムでは、サーバ固有の STONITH （ SAP HANA HA/DR プロバイダ）実装の代わりに NFSv4 ロックを使用した場合に、ネットアップは NFSv4 のみをサポートします。

| **SAP HANA** のサポート | **NFS** バージョン | **NFS** ロック | **SAP HANA** の **HA/DR** プロバイダ |
|---|---|---|---|
| SAP HANA シングルホスト、ホストの自動フェイルオーバーを使用しない複数のホスト | NFSv3 | オフ | 該当なし |
| | NFSv4 | オン | 該当なし |
| ホストの自動フェイルオーバーを使用する SAP HANA マルチホスト | NFSv3 | オフ | サーバ固有の STONITH の実装は必須です |
| | NFSv4 | オン | 必要ありません |

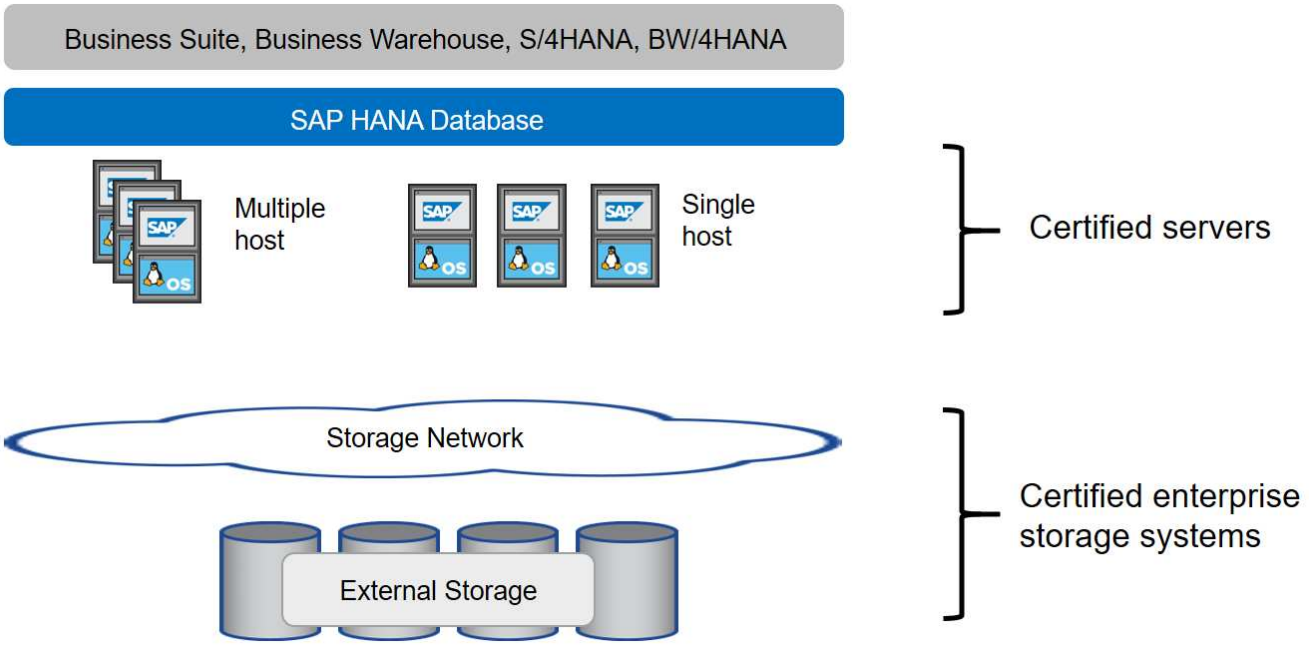
サーバ固有の STONITH 実装については、このガイドでは説明していません。そのような実装については、サーバのベンダーにお問い合わせください。

このドキュメントでは、物理サーバ上および VMware vSphere を使用する仮想サーバ上で実行される SAP HANA の構成に関する推奨事項について説明します。

オペレーティングシステムの構成ガイドラインと、 HANA 固有の Linux カーネルの依存関係については、該当する SAP ノートを参照してください。詳細については、『 SAP note 2235581 ： SAP HANA Supported Operating Systems 』を参照してください。

**SAP HANA** テーラードデータセンター統合

NetApp AFF ストレージコントローラは、 NFS （ NAS ）プロトコルと FC （ SAN ）プロトコルの両方を使用した SAP HANA TDI プログラムで認定されています。これらは、シングルホスト構成とマルチホスト構成のどちらでも、 SAP Business Suite on HANA 、 S/4HANA 、 BW/4HANA 、 SAP Business Warehouse on HANA など、最新の SAP HANA シナリオに導入できます。SAP HANA との使用が認定されているサーバは、ネットアップ認定のストレージソリューションと組み合わせることができます。次の図に、 SAP HANA TDI のアーキテクチャの概要を示します。




本番用SAP HANAシステムの前提条件と推奨事項の詳細については、次のリソースを参照してください。

- "『 SAP HANA Tailored Data Center Integration Frequently Asked Questions 』"

**VMware vSphere** を使用した **SAP HANA**

ストレージを仮想マシン（ VM ）に接続する方法はいくつかあります。推奨される方法は、ストレージボリュームと NFS をゲストオペレーティングシステムから直接接続することです。このオプションを使用しても、ホストとストレージの構成が物理ホストと VM で同じになることはありません。

NFS データストアと NFS を使用する VVol データストアもサポートされます。どちらの場合も、本番環境で使用するデータストアに格納する必要があるのは、 1 つの SAP HANA データボリュームまたはログボリュームだけです。

このドキュメントでは、ゲスト OS から NFS への直接マウントを使用する場合の推奨セットアップについて説明します。

SAP HANA での vSphere の使用の詳細については、次のリンクを参照してください。

- "SAP HANA on VMware vSphere - 仮想化 - コミュニティ Wiki"
- "『SAP HANA on VMware vSphere Best Practices Guide』"
- "2161991 - VMware vSphere 設定ガイドライン - SAP One Support Launchpad （ログインが必要）"

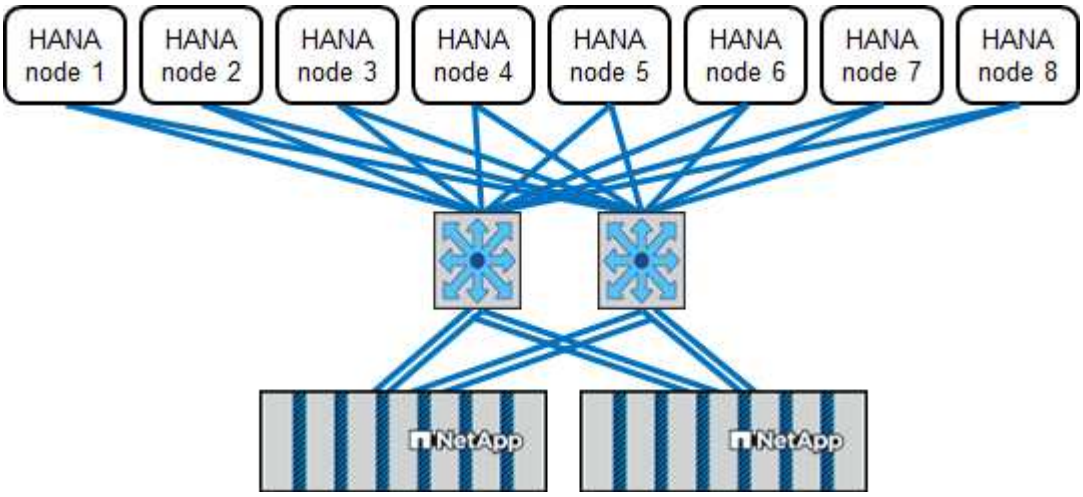
## アーキテクチャ

SAP HANA ホストは、冗長 10GbE 以上のネットワークインフラを使用して、ストレージコントローラに接続されます。SAP HANA ホストとストレージコントローラ間のデータ通信は、 NFS プロトコルに基づいています。スイッチまたはネットワークインターフェイスカード（ NIC ）の障害に備え、耐障害性に優れた SAP HANA ホスト / ストレージ接続を実現するには、冗長スイッチングインフラが必要です。

スイッチは、ポートチャネルを使用して個々のポートのパフォーマンスを集約し、ホストレベルでは単一の論理エンティティとして認識される場合があります。

AFF システム製品ファミリーのさまざまなモデルをストレージレイヤで混在させることができるため、拡張が必要になったり、パフォーマンスや容量のニーズが異なる場合があります。ストレージシステムに接続できる SAP HANA ホストの最大数は、 SAP HANA のパフォーマンス要件と、使用されているネットアップコントローラのモデルによって定義されます。必要なディスクシェルフの数は、 SAP HANA システムの容量とパフォーマンスの要件によってのみ決まります。

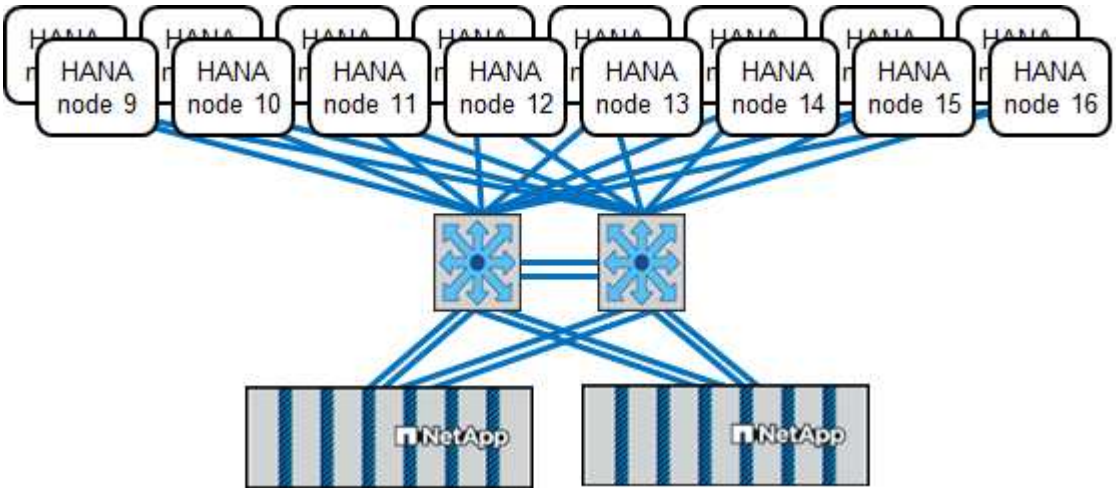
次の図は、 8 台の SAP HANA ホストをストレージハイアベイラビリティ（ HA ）ペアに接続した構成例を示しています。



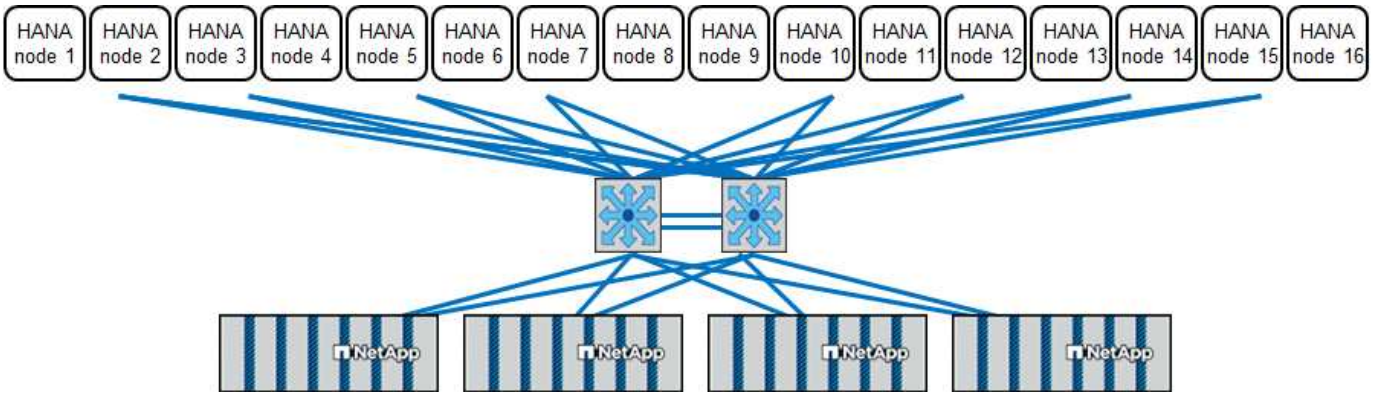

アーキテクチャは、次の 2 つの側面で拡張できます。

- 既存のストレージに SAP HANA ホストとストレージ容量を追加で接続することで、ストレージコントローラが現在の SAP HANA の主要パフォーマンス指標（ KPI ）を満たす十分なパフォーマンスを提供する場合。
- 追加の SAP HANA ホスト用にストレージ容量を追加したストレージシステムを追加する

次の図は、追加の SAP HANA ホストをストレージコントローラに接続した場合の構成例を示しています。この例では、 SAP HANA ホスト 16 台分の容量とパフォーマンスの要件を満たすために、さらにディスクシェルフが必要です。合計スループット要件に応じて、 10GbE 以上の接続をストレージコントローラに追加する必要があります。



次の図に示すように、導入した AFF システムとは関係なく、任意の認定済みストレージコントローラを追加して希望のノード密度に合わせて SAP HANA 環境を拡張することもできます。



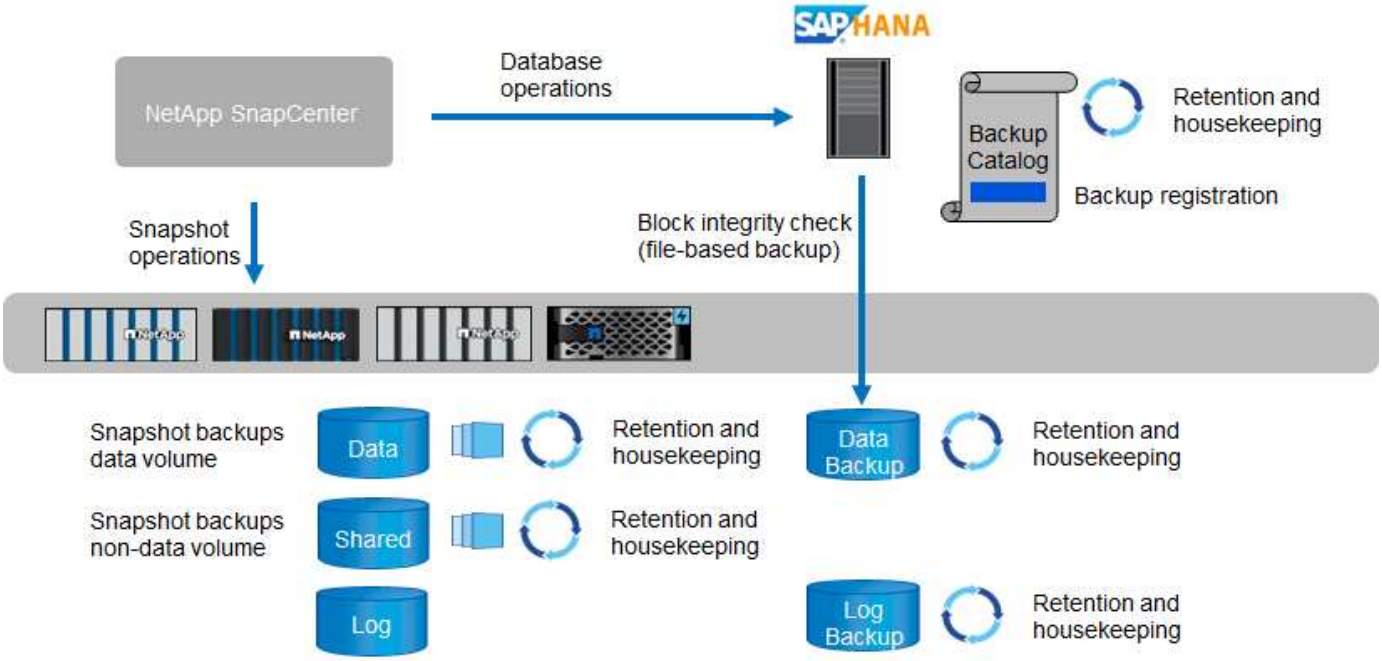

**SAP HANA** のバックアップ

すべてのネットアップストレージコントローラに搭載された ONTAP ソフトウェアは、動作中にパフォーマンスに影響を与えることなく SAP HANA データベースをバックアップするための組み込みメカニズムを提供します。ストレージベースの NetApp Snapshot バックアップは、 SAP HANA の単一コンテナ、および単一テナントまたは複数テナントを使用する SAP HANA マルチテナントデータベースコンテナ（ MDC ）システムで使用可能な、完全にサポートされた統合バックアップ解決策です。

ストレージベースの Snapshot バックアップは、 NetApp SnapCenter Plug-in for SAP HANA を使用して実装されます。これにより、 SAP HANA データベースに標準で搭載されているインターフェイスを使用して、整合性のあるストレージベースの Snapshot バックアップを作成できます。SnapCenter は、各 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。したがって、 SnapCenter で作成されたバックアップは、リストア処理とリカバリ処理用に直接選択できる SAP HANA Studio と Cockpit 内に表示されます。

NetApp SnapMirror テクノロジを使用すると、一方のストレージシステムで作成された Snapshot コピーを、SnapCenter で制御されるセカンダリバックアップストレージシステムにレプリケートできます。その後、プライマリストレージ上のバックアップセットごと、およびセカンダリストレージシステム上のバックアップセットごとに、異なるバックアップ保持ポリシーを定義できます。SnapCenter Plug-in for SAP HANA は、不要なバックアップカタログの削除を含め、 Snapshot コピーベースのデータバックアップとログバックアップの保持を自動的に管理します。また、 SnapCenter Plug-in for SAP HANA では、ファイルベースのバックアップを実行することで、 SAP HANA データベースのブロック整合性チェックを実行できます。

次の図に示すように、 NFS マウントを使用して、データベースログをセカンダリストレージに直接バックアップできます。




ストレージベースの Snapshot バックアップは、従来のファイルベースのバックアップに比べて大きなメリットをもたらします。たとえば、次のような利点があります。

- 高速バックアップ（数分）
- ストレージレイヤでのリストア時間（数分）が大幅に短縮され、バックアップの頻度が向上するため、Recovery Time Objective （ RTO ；目標復旧時間）が短縮されます
- バックアップとリカバリの処理中、 SAP HANA データベースのホスト、ネットワーク、またはストレージのパフォーマンスが低下することはありません
- ブロックの変更に基づいて、スペース効率と帯域幅効率に優れたセカンダリストレージへのレプリケーションを実行します

SAP HANAのバックアップとリカバリの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-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"。

### SAP HANA ディザスタリカバリ

SAP HANA ディザスタリカバリ（ DR ）は、 SAP HANA システムレプリケーションを使用してデータベースレイヤで実行するか、ストレージレプリケーションテクノロジを使用してストレージレイヤで実行できます。次のセクションでは、ストレージレプリケーションに基づくディザスタリカバリソリューションの概要について説明します。

SAP HANAディザスタリカバリ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-4646 ：『 SAP HANA Disaster Recovery with Storage Replication 』"。

#### SnapMirror に基づくストレージレプリケーション

次の図は、同期 SnapMirror レプリケーションを使用してローカル DR データセンターに 3 サイトのディザスタリカバリ解決策を作成し、非同期 SnapMirror を使用してリモート DR データセンターにデータをレプリケートする方法を示しています。

同期 SnapMirror を使用したデータレプリケーションでは、 RPO がゼロになります。プライマリデータセン

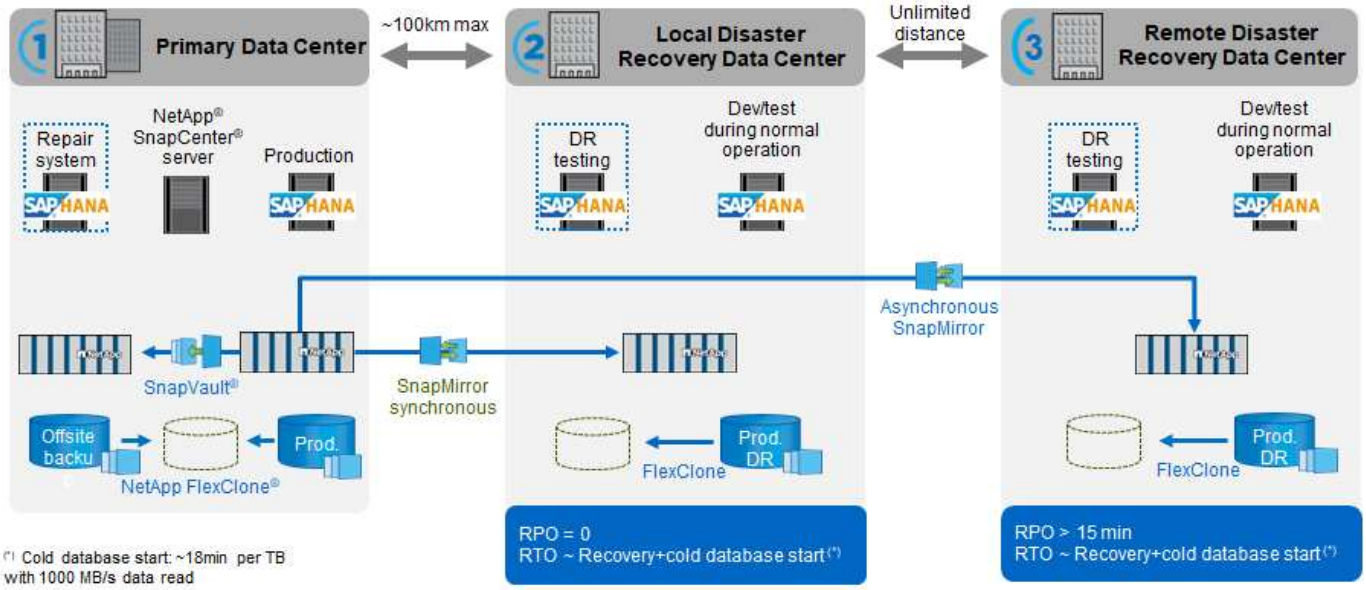
ターとローカル DR データセンター間の距離は約 100km です。

非同期 SnapMirror を使用して、プライマリとローカルの両方の DR サイトで障害が発生した場合のデータ保護を実行します。RPO は、レプリケーションの更新頻度と転送速度によって異なります。理論的には距離は無制限ですが、転送が必要なデータ量とデータセンター間の接続によって制限は異なります。通常の RPO の値は、 30 分から数時間です。

どちらのレプリケーション方法の RTO も、主に DR サイトで HANA データベースを起動してメモリにロードするのに必要な時間に左右されます。1000Mbps のスループットでデータが読み取られることを前提とし、1TB のデータをロードするには約 18 分かかります。

DR サイトのサーバは、通常運用時に開発 / テストシステムとして使用できます。災害が発生した場合は、開発 / テスト用システムをシャットダウンし、 DR 本番用サーバとして起動する必要があります。

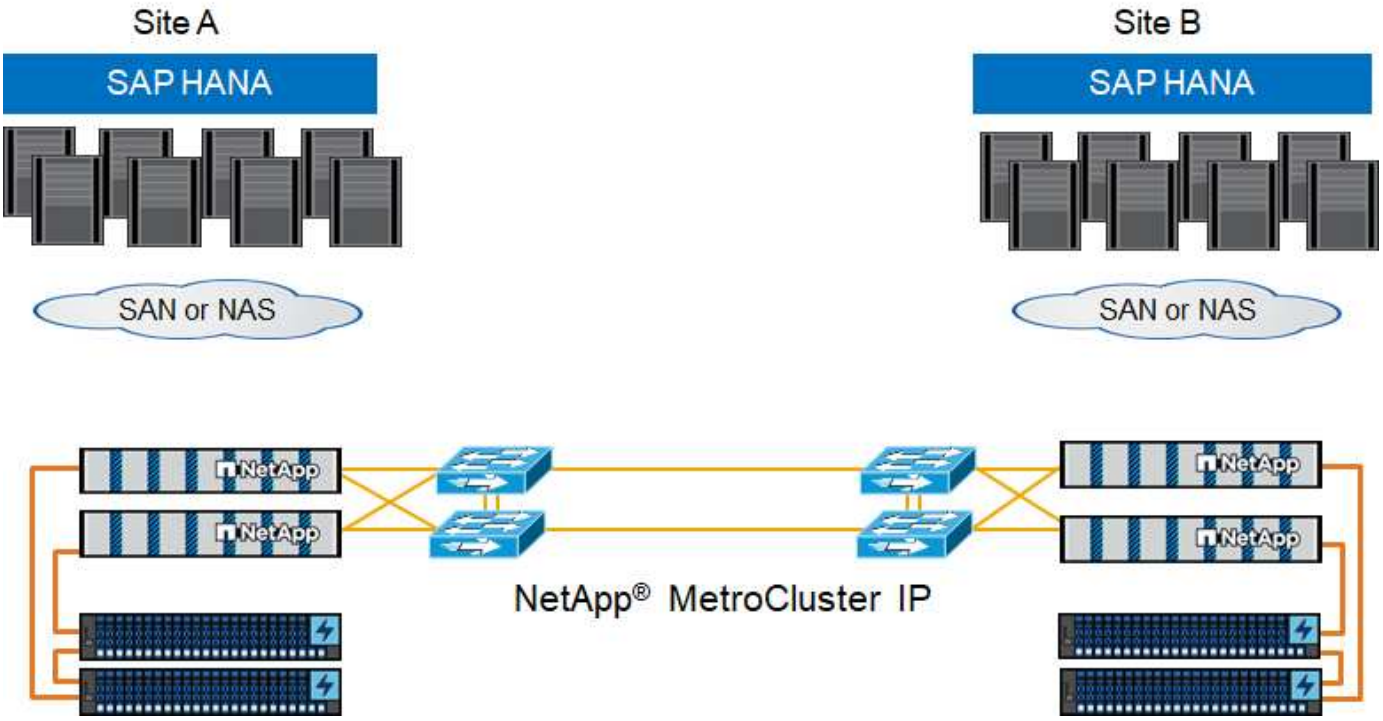
どちらのレプリケーション方法でも、 RPO と RTO に影響を与えることなく DR ワークフローテストを実行できます。FlexClone ボリュームはストレージ上に作成され、 DR テストサーバに接続されます。




同期レプリケーションで StrictSync モードが提供されます。何らかの理由でセカンダリストレージへの書き込みが完了しないと、アプリケーション I/O が失敗し、プライマリストレージシステムとセカンダリストレージシステムが同一になります。プライマリへのアプリケーション I/O は、 SnapMirror 関係のステータスが InSync に戻るまで再開されません。プライマリストレージで障害が発生した場合は、フェイルオーバー後にデータ損失なしでアプリケーション I/O をセカンダリストレージで再開できます。StrictSync モードでは、RPO は常にゼロです。

#### **MetroCluster** に基づくストレージレプリケーション

次の図は、解決策の概要を示しています。各サイトのストレージクラスタがローカルで高可用性を実現し、本番環境のワークロードに使用されます。各サイトのデータはもう一方のサイトに同期的にレプリケートされ、災害のフェイルオーバー時に使用できます。




## ストレージのサイジング

次のセクションでは、 SAP HANA 用のストレージシステムのサイジングに必要なパフォーマンスと容量に関する考慮事項の概要を説明します。

適切なサイズのストレージ環境を構築するために、ネットアップまたはネットアップパートナーの営業担当者にお問い合わせください。

### パフォーマンスに関する考慮事項

SAP では、ストレージ KPI の静的なセットが定義されています。これらの KPI は、データベースホストのメモリサイズや SAP HANA データベースを使用するアプリケーションに関係なく、すべての SAP HANA 本番環境に対して有効です。これらの KPI は、シングルホスト環境、マルチホスト環境、 Business Suite on HANA 環境、 Business Warehouse on HANA 環境、 S/4HANA 環境、および BW/4HANA 環境で有効です。したがって、現在のパフォーマンスサイジングアプローチは、ストレージシステムに接続されているアクティブな SAP HANA ホストの数にのみ依存します。

ストレージパフォーマンス KPI は、本番用 SAP HANA システムにのみ必須ですが、すべての HANA システムに実装できます。

SAP は、ストレージに接続されたアクティブな SAP HANA ホストのストレージシステムのパフォーマンスを検証するために使用する必要があるパフォーマンステストツールを提供します。

ネットアップは、特定のストレージモデルに接続できる SAP HANA ホストの最大数をテストし、事前に定義しました。本番環境ベースの SAP HANA システムに必要なストレージ KPI を SAP から実行できます。

ディスクシェルフで実行できる SAP HANA ホストの最大数と、 SAP HANA ホストごとに必要な SSD の最小数は、 SAP パフォーマンステストツールを実行して決定されています。このテストでは、ホストの実際のストレージ容量要件は考慮しません。また、必要な実際のストレージ構成を決定するために、容量要件を計算す

る必要があります。

#### SAS ディスクシェルフ

12Gb Serial-Attached SCSI （ SAS ）ディスクシェルフ（ DS224C ）では、次の固定ディスクシェルフ構成を使用してパフォーマンスのサイジングを行います。

- 12 本の SSD を備えたハーフ搭載のディスクシェルフです
- 24 本の SSD を搭載したフル搭載のディスクシェルフです

> どちらの構成もアドバンストディスクパーティショニング（ ADPv2 ）を使用します。ハーフ搭載のディスクシェルフは最大 9 台の SAP HANA ホストをサポートし、フル搭載のシェルフは 1 台のディスクシェルフで最大 14 台のホストをサポートします。SAP HANA ホストは、両方のストレージコントローラ間で均等に分散する必要があります。AFF A700s システムの同じ環境の内蔵ディスク。DS224C ディスクシェルフは、 SAP HANA ホストの数をサポートするため、 12Gb SAS を使用して接続する必要があります。

6Gb SAS ディスクシェルフ（ DS2246 ）は、最大 4 台の SAP HANA ホストをサポートします。SSD と SAP HANA ホストは、両方のストレージコントローラ間で均等に分散する必要があります。

次の表に、ディスクシェルフごとにサポートされる SAP HANA ホストの数を示します。

| | **24** 本の **SSD** をフル搭載した **6Gb SAS** シェルフ（ **DS2246** | **12Gb SAS** シェルフ（ **DS224C** ）には、 **12** 本の **SSD** と **ADPv2** が搭載されています | **12Gb SAS** シェルフ（ **DS224C** ）では、 **24** 本の **SSD** と **ADPv2** をフル搭載しています |
|---|---|---|---|
| ディスクシェルフあたりの SAP HANA ホストの最大数 | 4. | 9. | 14 |

> この計算は、使用しているストレージコントローラには依存しません。ディスクシェルフを追加しても、ストレージコントローラでサポートできる SAP HANA ホストの最大数は増加しません。

#### NS224 NVMe シェルフ

1つのNVMe SSD（データ）は、使用するNVMeディスクに応じて、最大2/5のSAP HANAホストをサポートします。SSDとSAP HANAホストは、両方のストレージコントローラ間で均等に分散する必要があります。AFFシステムの内蔵NVMeディスクについても同様です。

> ディスクシェルフを追加しても、ストレージコントローラでサポートできるSAP HANAホストの最大数は増えません。

混在ワークロード

SAP HANA とその他のアプリケーションワークロードを、同じストレージコントローラ上または同じストレージアグリゲート内で実行することはできません。ただし、ネットアップのベストプラクティスとして、 SAP HANA ワークロードを他のすべてのアプリケーションワークロードから分離することを推奨します。

SAP HANA ワークロードとその他のアプリケーションワークロードを、同じストレージコントローラまたは

同じアグリゲートに導入することもできます。その場合は、混在ワークロード環境内で SAP HANA に対して適切なパフォーマンスが確保されていることを確認する必要があります。また、 Quality of Service （ QoS ；サービス品質）パラメータを使用して、 SAP HANA アプリケーションに対する他のアプリケーションの影響を制御し、 SAP HANA アプリケーションのスループットを保証することも推奨します。

SAP パフォーマンステストツールを使用して、すでに他のワークロードに使用されている既存のストレージコントローラで追加の SAP HANA ホストを実行できるかどうかを確認する必要があります。SAP アプリケーションサーバは、 SAP HANA データベースと同じストレージコントローラやアグリゲートに安全に配置できます。

#### 容量に関する考慮事項

SAP HANA の容量要件の詳細な概要については、を参照してください "SAP ノート 1900823" ホワイトペーパー。

> 複数の SAP HANA システムで構成される SAP 環境全体の容量サイジングは、ネットアップの SAP HANA ストレージサイジングツールを使用して決定する必要があります。ストレージのサイジングプロセスを検証し、適切なサイズのストレージ環境を構築するには、ネットアップまたはネットアップパートナーの営業担当者にお問い合わせください。

### パフォーマンステストツールの設定

SAP HANA 1.0 SPS10 以降、 I/O 動作を調整し、使用中のファイルシステムとストレージシステムのデータベースを最適化するためのパラメータが導入されています。SAP のパフォーマンステストツールでストレージのパフォーマンスをテストする場合は、 SAP のパフォーマンステストツールにもこれらのパラメータを設定する必要があります。

ネットアップは、最適な値を定義するため、パフォーマンステストを実施しました。次の表に、 SAP パフォーマンステストツールの構成ファイルで設定する必要があるパラメータを示します。

| パラメータ | 価値 |
| --- | --- |
| max_parallel _io_requests と入力します | 128 |
| async _read_submit | オン |
| async ： write_submit_active | オン |
| async_write_submit_bblocks | すべて |

さまざまな SAP テストツールの設定の詳細については、を参照してください "SAP ノート 1943937" HWCCT （ SAP HANA 1.0 ）および "SAP ノート 2493172" HCMT/HCOT 用（ SAP HANA 2.0 ）。

次の例は、 HCMT/HCOT 実行プランに変数を設定する方法を示しています。

```
…{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
      },
```

```
      {
         "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
         "Name": "DataAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
```

```
per completion queue",
          "Name": "DataExtMaxParallelIoRequests",
          "Value": "128",
          "Request": "false"
       }, …
```

これらの変数はテスト構成に使用する必要があります。これは通常、 SAP が HCMT/HCOT ツールを使用して提供する事前定義された実行計画の場合です。次に、 4k ログの書き込みテストの例を示します。

```
…
       {
          "ID": "D664D001-933D-41DE-A904F304AEB67906",
          "Note": "File System Write Test",
          "ExecutionVariants": [
             {
                "ScaleOut": {
                   "Port": "${RemotePort}",
                   "Hosts": "${Hosts}",
                   "ConcurrentExecution": "${FSConcurrentExecution}"
                },
                "RepeatCount": "${TestRepeatCount}",
                "Description": "4K Block, Log Volume 5GB, Overwrite",
                "Hint": "Log",
                "InputVector": {
                   "BlockSize": 4096,
                   "DirectoryName": "${LogVolume}",
                   "FileOverwrite": true,
                   "FileSize": 5368709120,
                   "RandomAccess": false,
                   "RandomData": true,
                   "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                   "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                   "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                   "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                   "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                   "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                   "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                   "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                   "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
                }
             }, …
```

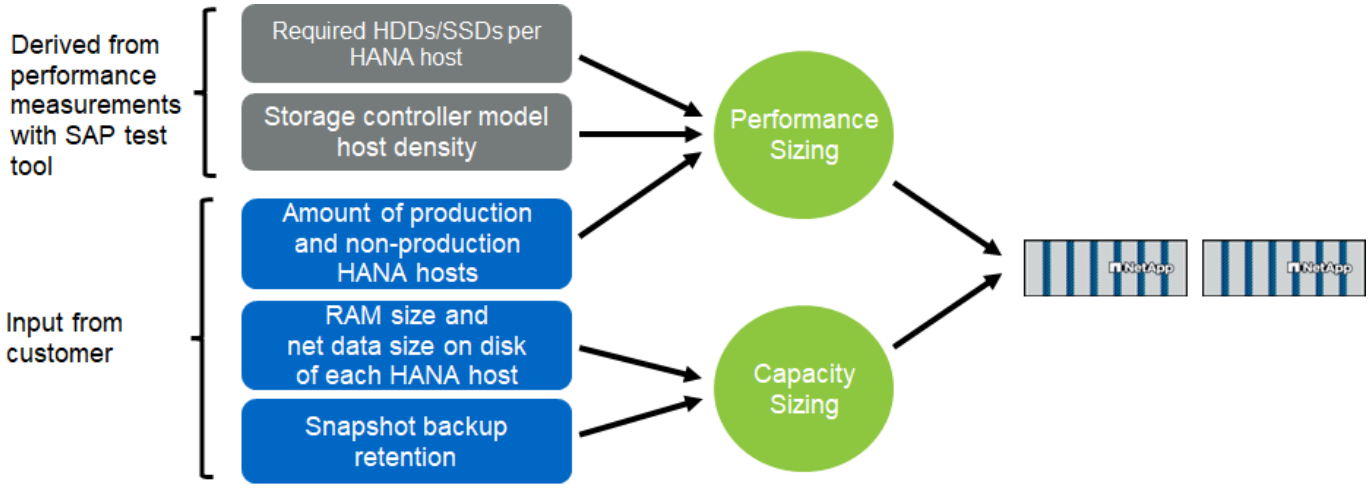
ストレージサイジングプロセスの概要

各ストレージモデルの HANA ホストあたりのディスク数と SAP HANA ホストの密度は、パフォーマンステストツールで決定されています。

サイジングプロセスでは、本番用および非本番用の SAP HANA ホストの数、各ホストの RAM サイズ、ストレージベースの Snapshot コピーのバックアップ保持期間などの詳細が必要です。SAP HANA ホストの数によって、必要なストレージコントローラとディスクの数が決まります。

RAM のサイズ、各 SAP HANA ホストでのディスク上の正味データサイズ、および Snapshot コピーのバックアップ保持期間は、容量サイジングの際に入力として使用されます。

次の図に、サイジングプロセスの概要を示します。




## インフラのセットアップと設定

ネットワークセットアップ

### このセクションでは、 SAP HANA ホスト専用のストレージネットワークセットアップについて説明します。

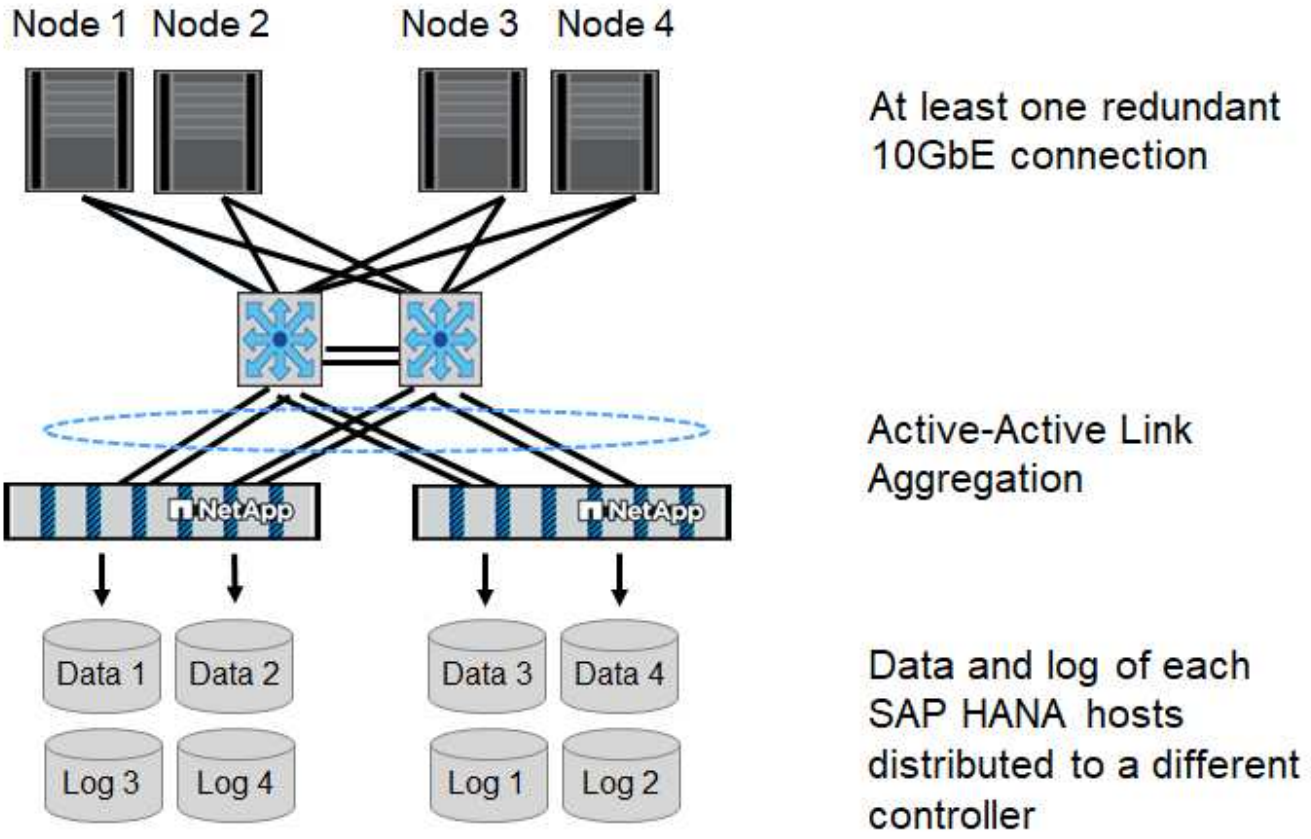
ネットワークを設定する際は、次のガイドラインに従ってください。

- SAP HANA ホストを 10GbE 以上のネットワークでストレージコントローラに接続するには、専用のストレージネットワークを使用する必要があります。
- ストレージコントローラと SAP HANA ホストには同じ接続速度を使用します。これができない場合は、ストレージコントローラと SAP HANA ホスト間のネットワークコンポーネントが異なる速度に対応できることを確認してください。たとえば、ストレージとホストの間で NFS レベルで速度のネゴシエーションを行うための十分なバッファスペースを確保する必要があります。ネットワークコンポーネントは通常スイッチですが、背面など、ブレードシャーシ内の他のコンポーネントも考慮する必要があります。
- ストレージネットワークスイッチおよびホストレイヤで、ストレージトラフィックに使用されるすべての物理ポートでフロー制御を無効にします。
- 各 SAP HANA ホストには、 10Gb 以上の帯域幅を持つ冗長ネットワーク接続が必要です。
- SAP HANA ホストとストレージコントローラ間のすべてのネットワークコンポーネントで、最大転送単位（ MTU ）サイズが 9 、 000 のジャンボフレームを有効にする必要があります。

- VMware のセットアップでは、実行中の各仮想マシンに、専用の VMXNET3 ネットワークアダプタを割り当てる必要があります。詳細については、「はじめに」に記載されている関連文書を参照してください。
- 相互の干渉を避けるため、ログとデータ領域には別々のネットワーク /IO パスを使用してください。

次の図は、 4 台の SAP HANA ホストを 10GbE ネットワークを使用してストレージコントローラ HA ペアに接続した場合の例を示しています。各SAP HANAホストには、冗長ファブリックへのアクティブ/アクティブ接続があります。

ストレージレイヤでは、4つのアクティブ接続が各SAP HANAホストに10Gbのスループットを提供するように構成されます。ストレージレイヤでは、MTUサイズが9、000のブロードキャストドメインが設定され、必要なすべての物理インターフェイスがこのブロードキャストドメインに追加されます。この方法では、これらの物理インターフェイスが同じフェイルオーバーグループに自動的に割り当てられます。これらの物理インターフェイスに割り当てられているすべての論理インターフェイス（ LIF ）が、このフェイルオーバーグループに追加されます。



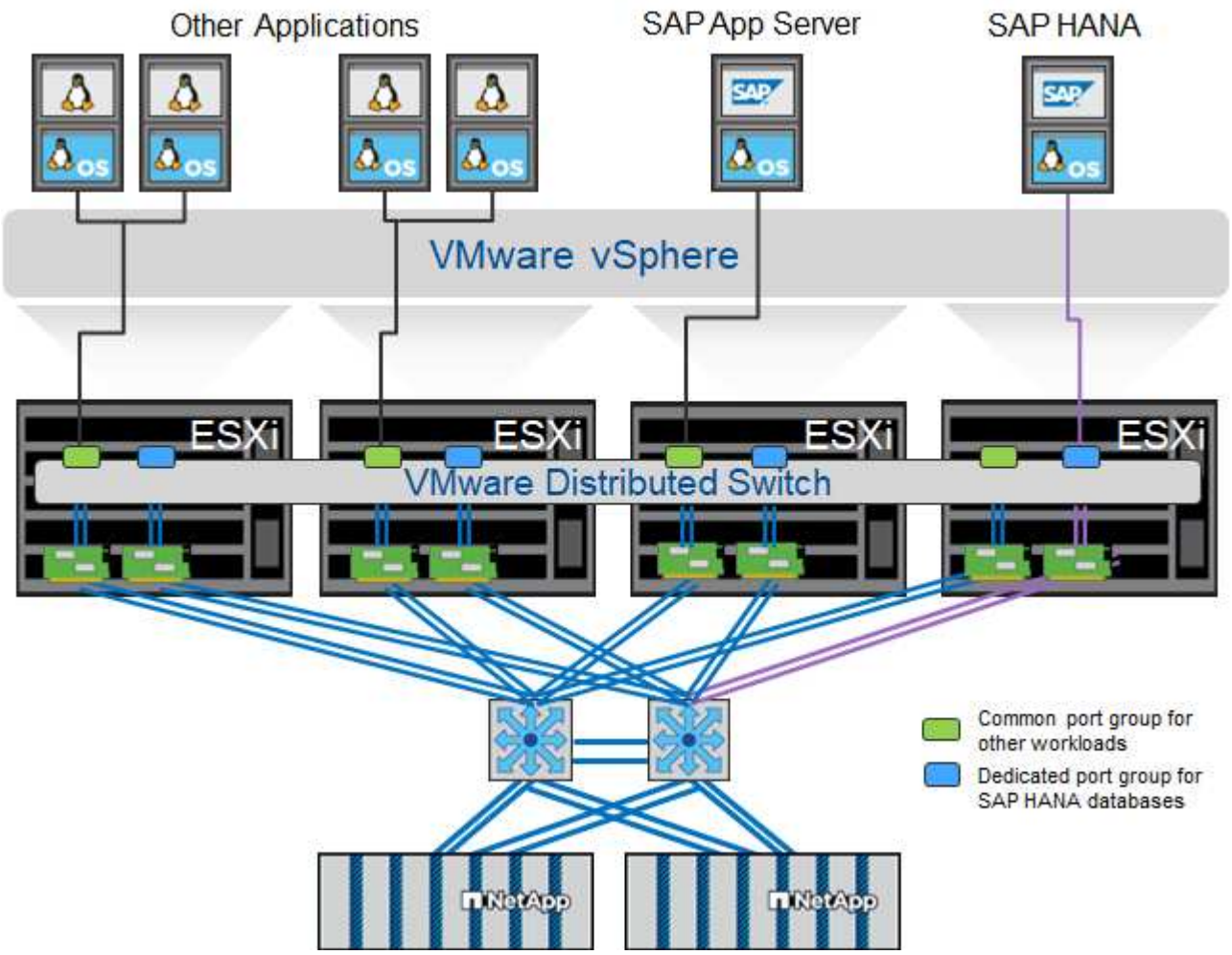

一般に、サーバ（ボンド）およびストレージシステムではHAインターフェイスグループ（Link Aggregation Control Protocol [LACP]やifgroupなど）を使用することを推奨します。HA インターフェイスグループを使用して、グループ内のすべてのインターフェイス間で負荷が均等に分散されていることを確認します。負荷分散は、ネットワークスイッチインフラの機能によって異なります。

SAP HANA ホストの数と使用されている接続速度に応じて、アクティブな物理ポートの数を変える必要があります。詳細については、を参照してください"LIF の設定"。

**VMware** 固有のネットワークセットアップ

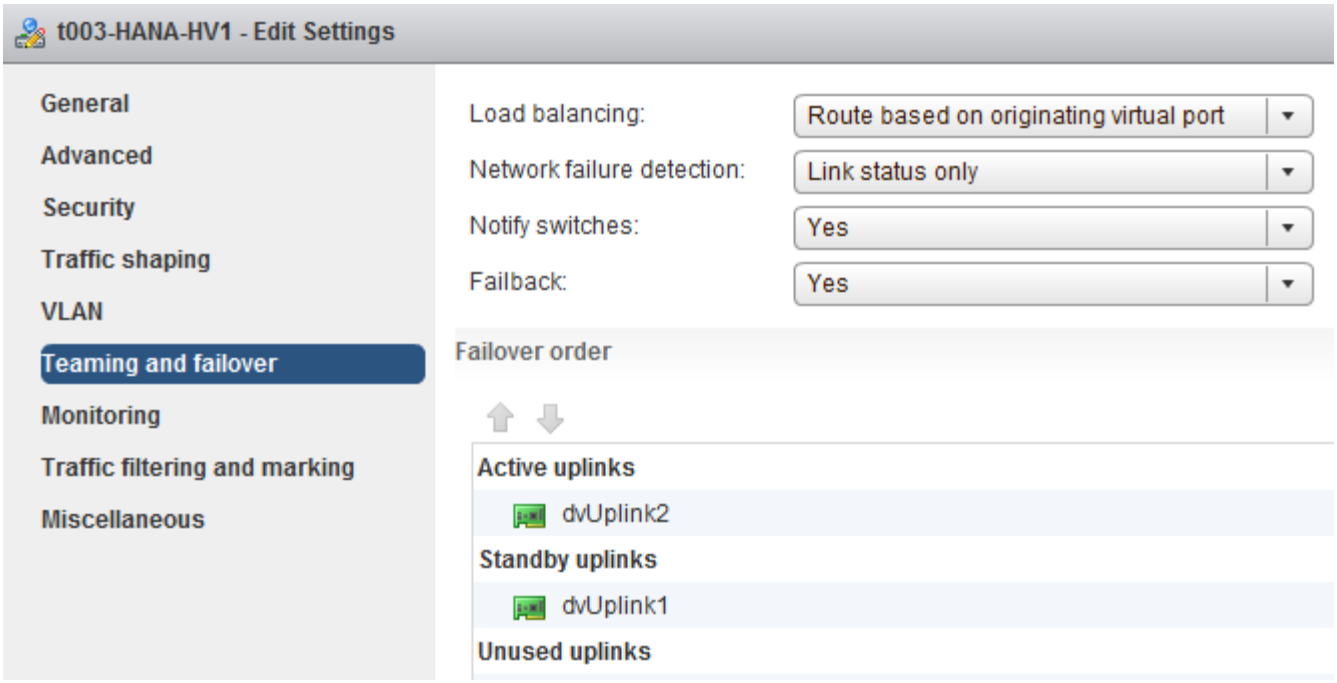
この解決策では、パフォーマンスを重視するデータベースのデータボリュームやログボリュームなど、 SAP

HANA インスタンスのすべてのデータが NFS 経由で提供されるため、適切なネットワーク設計と構成が不可欠です。専用のストレージネットワークは、 SAP HANA ノード間の通信トラフィックとユーザアクセストラフィックから NFS トラフィックを分離するために使用されます。各 SAP HANA ノードには、 10Gb 以上の帯域幅を持つ冗長専用ネットワーク接続が必要です。より高い帯域幅もサポートされています。このネットワークは、 VMware vSphere でホストされているゲストオペレーティングシステムまで、ストレージレイヤからネットワークスイッチングおよびコンピューティング経由でエンドツーエンドで拡張する必要があります。物理スイッチングインフラストラクチャに加えて、ハイパーバイザーレイヤでネットワークトラフィックのパフォーマンスと管理性を十分に確保するために、 VMware Distributed Switch （ vDS ）が使用されます。




前の図に示すように、各 SAP HANA ノードは、 VMware Distributed Switch 上の専用のポートグループを使用します。このポートグループを使用すると、 ESX ホストのサービス品質（ QoS ）の向上と物理 Network Interface Card （ NIC ；ネットワークインターフェイスカード）の専用割り当てが可能になります。NIC の障害時に HA 機能を維持したまま専用の物理 NIC を使用するには、専用の物理 NIC をアクティブアップリンクとして設定します。SAP HANA ポートグループのチーミングとフェイルオーバーの設定では、追加の NIC がスタンバイアップリンクとして設定されます。また、物理スイッチと仮想スイッチでジャンボフレーム（ MTU 9 、 000 ）をエンドツーエンドで有効にする必要があります。また、サーバ、スイッチ、およびストレージシステムのストレージトラフィックに使用されるすべてのイーサネットポートでフロー制御を無効にします。次の図に、このような構成の例を示します。

NFS トラフィックに使用されるインターフェイスでは、 LRO （ Large Receive Offload ）をオフにする必要があります。その他のネットワーク構成のガイドラインについては、それぞれの VMware ベストプラクティスガイドで SAP HANA を参照してください。




時刻の同期

ストレージコントローラと SAP HANA データベースホストの間で時刻を同期する必要があります。そのためには、すべてのストレージコントローラとすべての SAP HANA ホストに同じタイムサーバを設定します。

ストレージコントローラのセットアップ

ここでは、ネットアップストレージシステムの構成について説明します。プライマリのインストールとセットアップは、対応する ONTAP のセットアップガイドおよび設定ガイドに従って実行する必要があります。

ストレージ効率

SSD 構成の SAP HANA では、インライン重複排除、ボリューム間インライン重複排除、インライン圧縮、インラインコンパクションがサポートされています。

**NetApp FlexGroup**ボリューム

NetApp FlexGroup Volumeの使用はSAP HANAではサポートされていません。SAP HANAのアーキテクチャ上、FlexGroup Volumeを使用してもメリットはなく、パフォーマンスの問題が発生する可能性があります。

**NetApp**ボリュームとアグリゲートの暗号化

SAP HANAでは、NetApp Volume Encryption（NVE）とNetApp Aggregate Encryption（NAE）の使用がサポートされています。

**Quality of Service** の略

QoS を使用すると、特定の SAP HANA システムやその他のアプリケーションの共有使用コントローラにおけるストレージスループットを制限できます。1 つのユースケースとして、開発システムとテストシステムのス

ループットを制限し、混在環境で本番システムに影響を与えないようにすることが挙げられます。

サイジングプロセスでは、非本番システムのパフォーマンス要件を決定する必要があります。開発 / テスト用のシステムは、通常、 SAP で定義されている本番用システム KPI の 20~50% の範囲で、パフォーマンス値を低くしてサイジングすることができます。

ONTAP 9 以降では、ストレージボリュームレベルで QoS が設定され、スループット（ MBps ）と I/O 量（ IOPS ）に最大値が使用されます。

ストレージシステムのパフォーマンスに最大の影響があるのは、大きい書き込み I/O です。そのため、 QoS スループットの制限値として、データボリュームとログボリュームの対応する書き込み SAP HANA ストレージパフォーマンス KPI 値の割合を設定する必要があります。

#### NetApp FabricPool

SAP HANA システムのアクティブなプライマリファイルシステムには、 NetApp FabricPool テクノロジを使用しないでください。これには ' データとログ領域のファイル・システムと '/hana/shared-file システムが含まれますそのため、特に SAP HANA システムの起動時に、予測不可能なパフォーマンスが発生します。

「スナップショットのみ」の階層化ポリシーを使用することも、 NetApp SnapVault や SnapMirror デスティネーションなどのバックアップターゲットで FabricPool を一般的に使用することもできます。

> FabricPool を使用してプライマリストレージで Snapshot コピーを階層化するか、バックアップターゲットで FabricPool を使用すると、データベースまたはシステムクローンの作成や修復などのその他のタスクのリストアとリカバリに必要な時間が変わります。この点を考慮して、ライフサイクル全体の管理戦略を計画し、この機能を使用している間も SLA が満たされていることを確認してください。

FabricPool は、ログバックアップを別のストレージ階層に移動する場合に適しています。バックアップの移動は、 SAP HANA データベースのリカバリに要する時間に影響します。したがって、「 tiering-minimum-cooling-days 」オプションには、リカバリに必要なログバックアップをローカルの高速ストレージ階層に定期的に配置する値を設定する必要があります。

### ストレージ構成

以下に、必要なストレージ構成手順の概要を示します。各手順の詳細については、以降のセクションで説明します。このセクションでは、ストレージハードウェアがセットアップされており、 ONTAP ソフトウェアがすでにインストールされていることを前提としています。また、ストレージポート（ 10GbE 以上）とネットワークの間の接続がすでに確立されている必要があります。

1. 「」の説明に従って、正しいディスクシェルフ構成を確認します。[ディスクシェルフの接続]. 」
2. の説明に従って、必要なアグリゲートを作成および構成します。[アグリゲートの構成]. 」
3. の説明に従って、 Storage Virtual Machine （ SVM ）を作成します。SVM の設定. 」
4. の説明に従って LIF を作成します。LIF の設定. 」
5. およびSAP HANA マルチホストシステムのボリューム構成の説明に従って、アグリゲート内にボリュームを作成しますSAP HANA シングルホストシステムのボリューム構成。
6. の説明に従って、必要なボリュームオプションを設定します。[ボリュームのオプション]. 」
7. の説明に従って、 NFSv3 に必要なオプションを設定します。NFSv3 用の NFS 設定「 NFSv4 の場合は、」の説明に従ってまたはを参照してください。NFSv4 の NFS 設定. 」

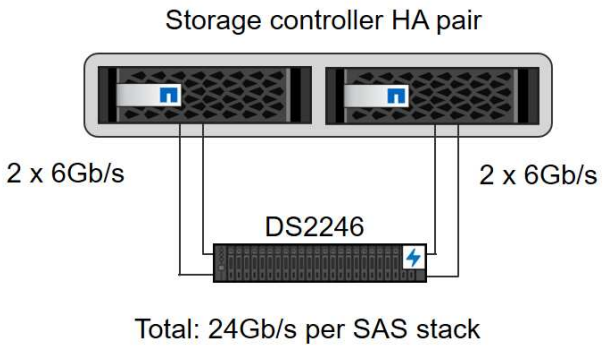
8. の説明に従って、ボリュームをネームスペースにマウントし、エクスポートポリシーを設定します。[ボリュームをネームスペースにマウントし、エクスポートポリシーを設定]. 」

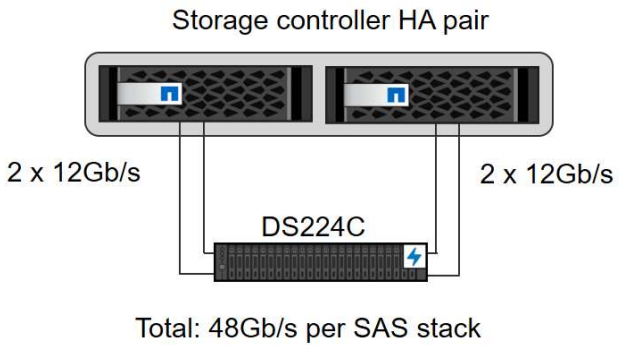
ディスクシェルフの接続

### SAS ディスクシェルフ

次の図に示すように、 1 つの SAS スタックに最大 1 台のディスクシェルフを接続して、 SAP HANA ホストに必要なパフォーマンスを実現できます。各シェルフ内のディスクは、 HA ペアの両方のコントローラに均等に分散する必要があります。ADPv2 は、 ONTAP 9 および DS224C ディスクシェルフで使用されます。

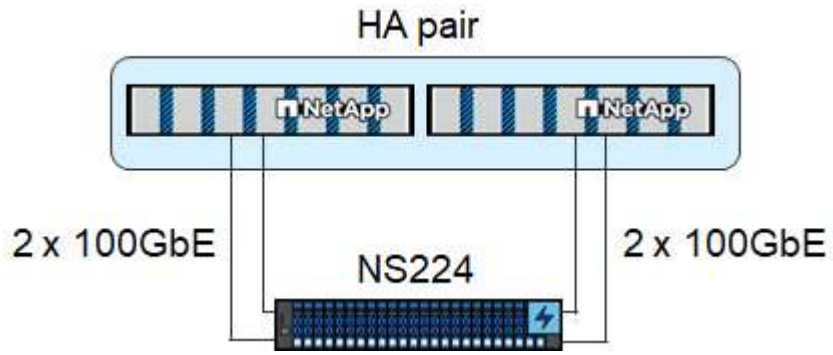
ディスクシェルフ DS224C では、クワッドパスの SAS ケーブルも使用できますが、必須ではありません。




### NVMe （ 100GbE ）ディスクシェルフ

次の図に示すように、NS224 NVMeディスクシェルフは、コントローラごとに2つの100GbEポートで接続されます。各シェルフ内のディスクは、HAペアの両方のコントローラに均等に分散する必要があります。ADPv2 は、アグリゲート構成の章で説明されているとおり、 NS224 ディスクシェルフにも使用されます。

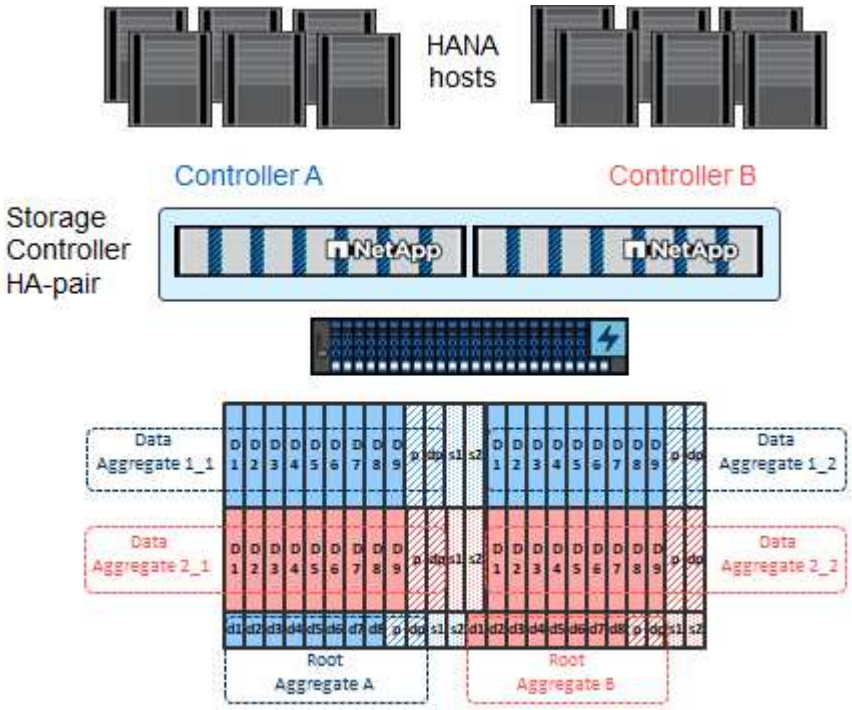



アグリゲートの構成

一般に、使用するディスクシェルフやドライブテクノロジ（ SAS SSD または NVMe SSD ）とは関係なく、コントローラごとに 2 つのアグリゲートを構成する必要があります。

次の図は、 ADPv2 を使用した、 12Gb の SAS シェルフで稼働する、 12 台の SAP HANA ホストの構成を示しています。6 台の SAP HANA ホストが各ストレージコントローラに接続されています。各ストレージコン

トローラに 2 つずつ、合計 4 つのアグリゲートが構成されています。各アグリゲートには、 9 つのデータパーティションと 2 つのパリティディスクパーティションを含む 11 本のディスクが構成されます。各コントローラで、 2 つのスペアパーティションを使用できます。




**SVM** の設定

SAP HANA データベースを使用する複数の SAP ランドスケープでは、単一の SVM を使用できます。SVM は、社内の複数のチームによって管理される場合に備え、必要に応じて各 SAP ランドスケープに割り当てることもできます。

新しい SVM の作成時に自動的に作成されて割り当てられた QoS プロファイルがある場合は、自動的に作成されたこのプロファイルを SVM から削除して、 SAP HANA に必要なパフォーマンスを有効にします。

```
vserver modify -vserver <svm-name> -qos-policy-group none
```

**LIF** の設定

SAP HANA 本番システムでは、 SAP HANA ホストからデータボリュームとログボリュームをマウントするときに別々の LIF を使用する必要があります。したがって、少なくとも 2 つの LIF が必要です。

異なる SAP HANA ホストのデータボリュームマウントとログボリュームマウントは、同じ LIF を使用するか、マウントごとに個別の LIF を使用することで、物理ストレージネットワークポートを共有できます。

物理インターフェイスごとのデータボリュームマウントとログボリュームマウントの最大数を次の表に示します。

| イーサネットポート速度 | **10GbE** | **25GbE** | **40GbE** | **100 Gee** |
| --- | --- | --- | --- | --- |
| 物理ポートあたりのログボリュームマウントまたはデータボリュームマウントの最大数 | 3 | 8 | 12. | 30 |

異なる SAP HANA ホスト間で 1 つの LIF を共有するには、データボリュームまたはログボリュームを別の LIF に再マウントすることが必要になる場合があります。この変更により、ボリュームが別のストレージコントローラに移動された場合のパフォーマンス低下を回避できます。

開発 / テスト用システムでは、物理ネットワークインターフェイス上で使用できるデータおよびボリュームのマウントや LIF を増やすことができます。

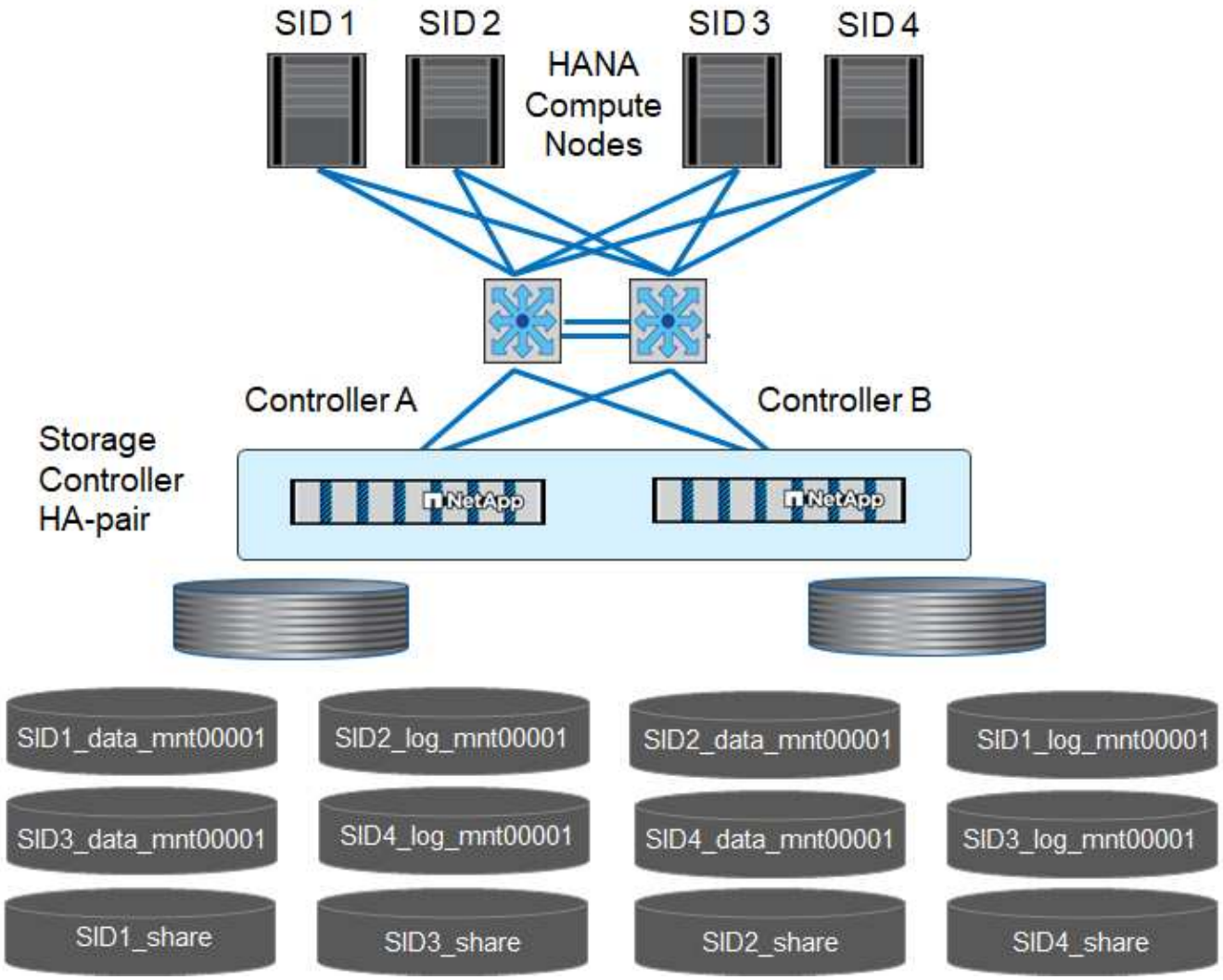
本番システム ' 開発システム ' およびテスト・システムでは '/hana/shared ファイル・システムは ' データ・ボリュームまたはログ・ボリュームと同じ LIF を使用できます

#### **SAP HANA** シングルホストシステムのボリューム構成

次の図は、 4 つのシングルホスト SAP HANA システムのボリューム構成を示しています。各 SAP HANA システムのデータボリュームとログボリュームは、異なるストレージコントローラに分散されます。たとえば、ボリューム「 ID1_data_mnt00001 」がコントローラ A で設定され、ボリューム「 ID1_log_mnt00001 」がコントローラ B で設定されているとします

HA ペアのうち、 1 台のストレージコントローラのみを SAP HANA システムに使用する場合は、データボリュームとログボリュームを同じストレージコントローラに保存することもできます。

データボリュームとログボリュームが同じコントローラに格納されている場合は、サーバからストレージへのアクセスに、 2 つの異なる LIF を使用して実行する必要があります。 1 つはデータボリュームにアクセスする LIF 、もう 1 つはログボリュームにアクセスする LIF です。




各 SAP HANA ホストには、データボリューム、ログボリューム、「 /hana/shared 」のボリュームが構成されています。次の表は、シングルホスト SAP HANA システムの構成例を示しています。

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **b** のアグリゲート **2** |
|---|---|---|---|---|
| システム SID1 のデータ、ログ、および共有ボリューム | データボリューム：SID1_data_mnt00001 | 共有ボリューム：SID1_shared | – | ログボリューム：SID1_log_mnt00001 |
| システム SID2 のデータボリューム、ログボリューム、および共有ボリューム | – | ログボリューム：SID2_log_mnt00001 | データボリューム：SID2_data_mnt00001 | 共有ボリューム：SID2_shared |
| システム SID3 のデータ、ログ、および共有ボリューム | 共有ボリューム：SID3_shared | データボリューム：SID3_data_mnt00001 | ログボリューム：SID3_log_mnt00001 | – |
| システム SID4 のデータボリューム、ログボリューム、および共有ボリューム | ログボリューム：SID4_log_mnt00001 | – | 共有ボリューム：SID4_shared | データボリューム：SID4_data_mnt00001 |

次の表に、シングルホストシステムのマウントポイント構成例を示します。「 idadm 」ユーザのホーム・ディレクトリを中央ストレージに配置するには、「 /usr/sap/SID 」ファイル・システムを「 S ID_SHARED 」ボリュームからマウントする必要があります。

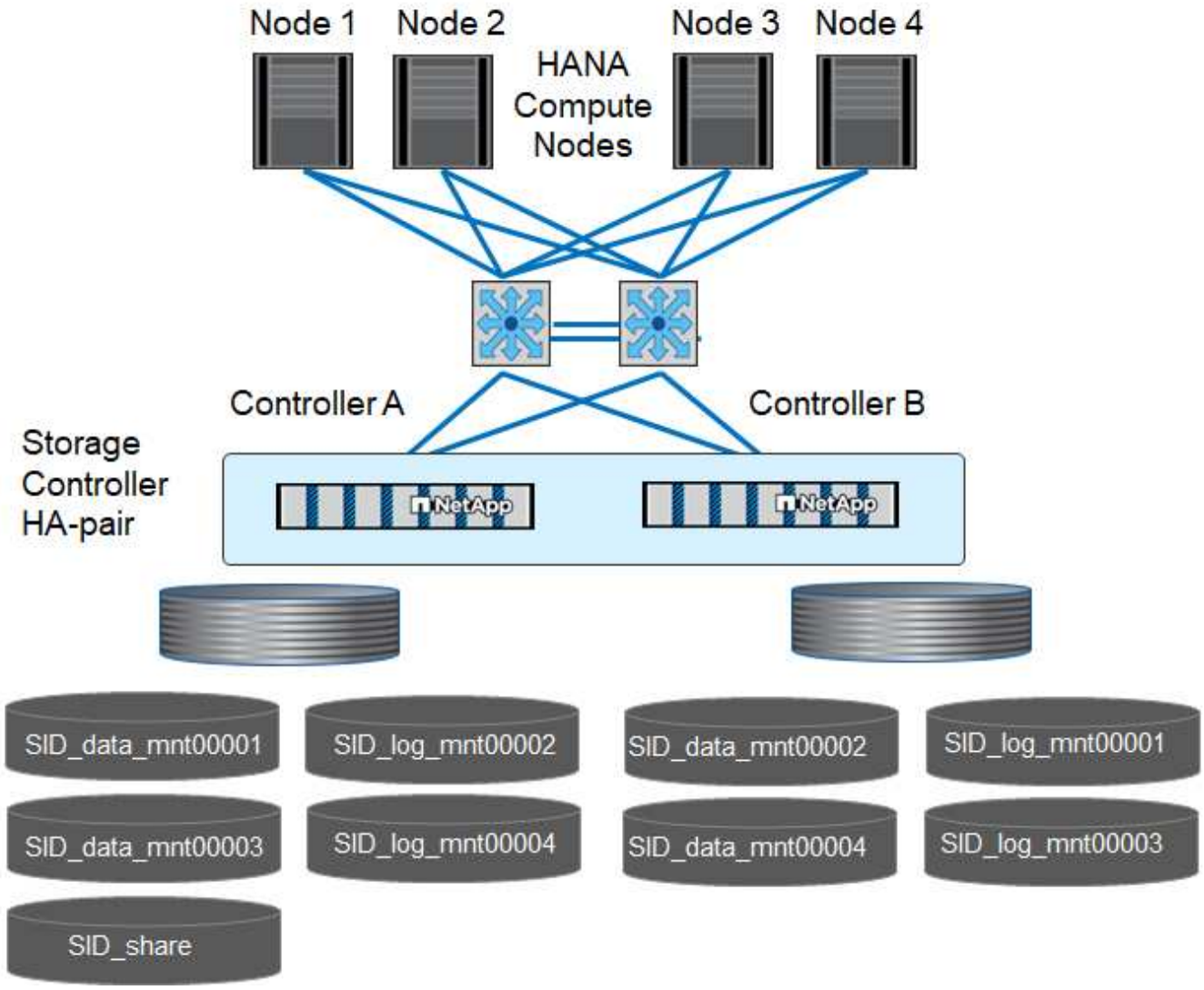
| ジャンクションパス | ディレクトリ | **HANA** ホストのマウントポイント |
|---|---|---|
| SID_data_mnt00001 | | /hana/data/SID/mnt00001 |
| SID_log_mnt00001 | | /hana/log/sid/mnt00001 |
| SID_shared | usr - SAP 共有 | /usr/sap/SID /hana/shareed/ |

**SAP HANA** マルチホストシステムのボリューム構成

次の図は、 4+1 の SAP HANA システムのボリューム構成を示しています。各 SAP HANA ホストのデータボリュームとログボリュームは、異なるストレージコントローラに分散されます。たとえば、ボリューム「 ID1_data1_mnt00001 」がコントローラ A に設定され、ボリューム「 ID1_log1_mnt00001 」がコントローラ B に設定されているとします

HA ペアのうち、 1 台のストレージコントローラのみを SAP HANA システムに使用する場合は、データボリュームとログボリュームを同じストレージコントローラに保存することもできます。

データボリュームとログボリュームが同じコントローラに格納されている場合は、サーバからストレージへのアクセスに、 2 つの異なる LIF を使用して実行する必要があります。 1 つはデータボリュームにアクセスする LIF で、もう 1 つはログボリュームにアクセスする LIF です。




各 SAP HANA ホストには、 1 個のデータボリュームと 1 個のログボリュームが作成されます。「 /hana/shared 」ボリュームは、 SAP HANA システムのすべてのホストで使用されます。次の表に、 4 つのアクティブホストを持つ、マルチホスト SAP HANA システムの構成例を示します。

| 目的 | アグリゲート **1** ：コントローラ **A** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| ノード 1 のデータボリュームとログボリューム | データボリューム： SID_data_mnt00001 | – | ログボリューム： SID_log_mnt00001 | – |
| ノード 2 のデータボリュームとログボリューム | ログボリューム： SID_log_mnt00002 | – | データボリューム： SID_data_mnt00002 | – |
| ノード 3 のデータボリュームとログボリューム | – | データボリューム： SID_data_mnt00003 | – | ログボリューム： SID_log_mnt00003 |
| ノード 4 のデータボリュームとログボリューム | – | ログボリューム： SID_log_mnt00004 | – | データボリューム： SID_data_mnt00004 |

| 目的 | アグリゲート **1** ：コントローラ **A** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| すべてのホストの共有ボリューム | 共有ボリューム：SID_shared | | | |

次の表に、アクティブな SAP HANA ホストが 4 台あるマルチホストシステムの構成とマウントポイントを示します。各ホストの 'idadm' ユーザのホーム・ディレクトリを中央ストレージに配置するために '/usr/sap/SID' ファイル・システムは 'S ID_SHARED' ボリュームからマウントされます

| ジャンクションパス | ディレクトリ | **SAP HANA** ホストのマウントポイント | 注 |
|---|---|---|---|
| SID_data_mnt00001 | – | /hana/data/SID/mnt00001 | すべてのホストにマウントされています |
| SID_log_mnt00001 | – | /hana/log/sid/mnt00001 | すべてのホストにマウントされています |
| SID_data_mnt00002 | – | /hana/data/sid/mnt00002 | すべてのホストにマウントされています |
| SID_log_mnt00002 | – | /hana/log/sid/mnt00002 | すべてのホストにマウントされています |
| SID_data_mnt00003 | – | /hana/data/sid/mnt00003 | すべてのホストにマウントされています |
| SID_log_mnt00003 | – | /hana/log/sid/mnt00003 | すべてのホストにマウントされています |
| SID_data_mnt00004 | – | /hana/data/sid/mnt00004 | すべてのホストにマウントされています |
| SID_log_mnt00004 | – | /hana/log/sid/mnt00004 | すべてのホストにマウントされています |
| SID_shared | 共有 | /hana/shared-SID を指定します | すべてのホストにマウントされています |
| SID_shared | usr-sap-host1 | /usr/sap/SID | ホスト 1 にマウントされています |
| SID_shared | usr-sap-host2 | /usr/sap/SID | ホスト 2 にマウントされています |
| SID_shared | usr-sap-host3 | /usr/sap/SID | ホスト 3 にマウント |
| SID_shared | usr-sap-host4 | /usr/sap/SID | ホスト 4 にマウント |
| SID_shared | usr-sap-host5 | /usr/sap/SID | ホスト 5 にマウント |

ボリュームのオプション

すべての SVM について、次の表に示すボリュームオプションを確認して設定する必要があります。一部のコマンドについては、 ONTAP で advanced 権限モードに切り替える必要があります。

| アクション | コマンドを実行します |
| --- | --- |
| Snapshot ディレクトリの可視化を無効にします | vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false |
| Snapshot コピーの自動作成を無効にする | vol modify – vserver <vserver-name> -volume <volname> -snapshot-policy none と指定します |
| SID_shared ボリュームを除くアクセス時間の更新を無効にします | advanced 権限レベルの vol modify -vserver <vserver-name> -volume <volname> -atime-update false set admin を設定します |

#### NFSv3 用の NFS 設定

次の表に示す NFS オプションは、すべてのストレージコントローラで検証および設定する必要があります。この表に示す一部のコマンドについては、 advanced 権限モードに切り替える必要があります。

| アクション | コマンドを実行します |
| --- | --- |
| NFSv3 を有効にします | nfs modify -vserver <vserver -name> v3.0 enabled |
| NFS TCPの最大転送サイズを1MBに設定する | advanced 権限レベルの nfs modify -vserver <vserver_name> -tcp-max-xfer-size 1048576 set admin を設定します |

ワークロードが異なる共有環境では、NFS TCPの最大転送サイズを262144に設定

#### NFSv4 の NFS 設定

次の表に示す NFS オプションは、すべての SVM で検証および設定する必要があります。

この表の一部のコマンドについては、 advanced 権限モードに切り替える必要があります。

| アクション | コマンドを実行します |
| --- | --- |
| NFSv4 を有効にします | nfs modify -vserver <vserver-name> -v4.1 enabled と入力します |
| NFS TCPの最大転送サイズを1MBに設定する | advanced 権限レベルの nfs modify -vserver <vserver_name> -tcp-max-xfer-size 1048576 set admin を設定します |
| NFSv4 のアクセス制御リスト（ ACL ）を無効にする | nfs modify -vserver <vserver_name>-v4.1-acl disabled |
| NFSv4 ドメイン ID を設定する | nfs modify -vserver <vserver_name>-v4-id-domain <domain-name> |
| NFSv4 の読み取り委譲を無効にする | nfs modify -vserver <vserver_name>-v4.1-read-delegation disabled |
| NFSv4 の書き込み委譲を無効にする | nfs modify -vserver <vserver_name>-v4.1-write-delegation disabled |
| NFSv4 数値 ID を無効にする | nfs modify -vserver <vserver_name>-v4-numeric-ids disabled |

| アクション | コマンドを実行します |
| --- | --- |
| NFSv4.xセッションスロットの数を変更する<br>任意。 | 詳細設定<br>nfs modify -vserver hana-v4.x -session-num-slots <value><br>管理者を設定 |

ワークロードが異なる共有環境では、NFS TCPの最大転送サイズを262144に設定

数値IDを無効にするにはユーザ管理が必要であることに注意してください。詳細については、を参照してください。"「 NFSv4 用の SAP HANA インストールの準備」"

(`/etc/idmapd.conf`セクションの説明に従って、NFSv4ドメインIDをすべてのLinuxサーバで同じ値に設定する必要があります。"「 NFSv4 用の SAP HANA インストールの準備」"

pNFSは有効にして使用できます。

ホストの自動フェイルオーバーを備えたSAP HANAマルチホストシステムを使用している場合は、 `nameserver.ini` 次の表を参照してください。
これらのセクション内では、デフォルトの再試行間隔（10秒）を維持してください。

| **nameserver.ini** 内のセクション | パラメータ | 価値 |
| --- | --- | --- |
| フェイルオーバー | normal_retries | 9. |
| distributed_watchdog | Deactivate_retries | 11. |
| distributed_watchdog | TAKEOVER_retries を指定します | 9. |

ボリュームをネームスペースにマウントし、エクスポートポリシーを設定

ボリュームを作成するときは、ボリュームをネームスペースにマウントする必要があります。このドキュメントでは、ジャンクションパス名がボリューム名と同じであると想定しています。デフォルトでは、ボリュームはデフォルトポリシーを使用してエクスポートされます。エクスポートポリシーは必要に応じて適用できます。

ホストのセットアップ

## このセクションで説明するホストのセットアップ手順は、すべて物理サーバ上の SAP HANA 環境と、 VMware vSphere 上で実行される SAP HANA 環境の両方で有効です。

#### **SUSE Linux Enterprise Server** の構成パラメータ

各 SAP HANA ホストでは、 SAP HANA によって生成されるワークロードに合わせて、追加のカーネルパラメータと構成パラメータを調整する必要があります。

### **SUSE Linux Enterprise Server 12** および **15**

SUSE Linux Enterprise Server 12 SP1 以降、カーネルパラメータは /etc/sysctl.d` ディレクトリの構成ファイルで設定する必要があります。たとえば、「 91-NetApp-/hana.conf 」という名前の構成ファイルを作成する必要があります。

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384  16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle=0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_max_slot_table_entries = 128
```

これらの値は、 SLES for SAP OS のバージョンに含まれている saptune を使用して設定できます。詳細については、を参照してください "SAP ノート 3024346" （ SAP ログインが必要です）。

```
```

**Red Hat Enterprise Linux 7.2** 以降の構成パラメータ

SAP HANA で生成されるワークロードに合わせて、各 SAP HANA ホストで追加のカーネルパラメータと構成パラメータを調整する必要があります。

Red Hat Enterprise Linux 7.2 以降では、 /etc/sysctl.d` ディレクトリにある構成ファイルでカーネルパラメータを設定する必要があります。たとえば、「 91-NetApp-/hana.conf 」という名前の構成ファイルを作成する必要があります。

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384  16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle = 0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_max_slot_table_entries = 128
```

Red Hat Enterprise Linuxバージョン8.6以降では、RHEL System Roles for SAP（Ansible）を使用して設定を適用することもできます。を参照してください "SAP ノート 3024346" （ SAP ログインが必要です）。

**/hana/shared** ボリュームにサブディレクトリを作成します

次の例は、 SID=NF2 の SAP HANA データベースを示しています。

必要なサブディレクトリを作成するには、次のいずれかの操作を行います。

- シングル・ホスト・システムの場合は '/hana/shared-volume をマウントし 'hared' サブディレクトリと usr-sap サブディレクトリを作成します

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap
sapcc-hana-tst-06:/mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

- マルチ・ホスト・システムの場合は '/hana/shared-volume をマウントし ' 各ホストの 'hared' サブディレクトリと 'usr-sap' サブディレクトリを作成します

  以下のコマンド例は、 2+1 のマルチホスト HANA システムを示しています。

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host1
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host2
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host3
sapcc-hana-tst-06:/mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

マウントポイントを作成する

次の例は、 SID=NF2 の SAP HANA データベースを示しています。

必要なマウントポイントディレクトリを作成するには、次のいずれかの操作を行います。

- シングルホストシステムの場合は、マウントポイントを作成し、データベースホストに権限を設定します。

```
sapcc-hana-tst-06:/ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/shared
sapcc-hana-tst-06:/ # mkdir -p /usr/sap/NF2

sapcc-hana-tst-06:/ # chmod –R 777 /hana/log/NF2
sapcc-hana-tst-06:/ # chmod –R 777 /hana/data/NF2
sapcc-hana-tst-06:/ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:/ # chmod -R 777 /usr/sap/NF2
```

- マルチホストシステムの場合は、マウントポイントを作成し、すべてのワーカーホストとスタンバイホストに権限を設定します。以下のコマンド例は、 2+1 のマルチホスト HANA システムを示しています。
  - 1 つ目のワーカーホスト：

```
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/shared
sapcc-hana-tst-06:~ # mkdir -p /usr/sap/NF2

sapcc-hana-tst-06:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:~ # chmod -R 777 /usr/sap/NF2
```

- 2 つ目のワーカーホスト：

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/shared
sapcc-hana-tst-07:~ # mkdir -p /usr/sap/NF2

sapcc-hana-tst-07:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-07:~ # chmod -R 777 /usr/sap/NF2
```

- スタンバイホスト：

```
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/shared
sapcc-hana-tst-08:~ # mkdir -p /usr/sap/NF2

sapcc-hana-tst-08:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-08:~ # chmod -R 777 /usr/sap/NF2
```

ファイルシステムをマウント

NFS のバージョンと ONTAP のリリースに応じて、異なるマウントオプションを使用する必要があります。次のファイルシステムをホストにマウントする必要があります。

- 「 /hana/data/sid/mnt0000* 」と入力します
- 「 /hana/log/sid/mnt0000* 」と入力します
- 「 /hana/shared 」
- /usr/sap/SID

次の表に、シングルホストデータベースとマルチホスト SAP HANA データベースの異なるファイルシステムに使用する必要がある NFS のバージョンを示します。

| ファイルシステム | **SAP HANA** シングルホスト | **SAP HANA** マルチホスト |
|---|---|---|
| /hana/data/sid/mnt0000* | NFSv3 または NFSv4 | NFSv4 |
| /hana/log/sid/mnt0000* | NFSv3 または NFSv4 | NFSv4 |
| /hana/shared にアクセスします | NFSv3 または NFSv4 | NFSv3 または NFSv4 |
| /usr/sap/SID | NFSv3 または NFSv4 | NFSv3 または NFSv4 |

次の表に、 NFS の各バージョンと ONTAP のリリースのマウントオプションを示します。共通パラメータは、 NFS と ONTAP のバージョンには依存しません。

SAP LaMa では、 /usr/sap/SID ディレクトリをローカルにする必要があります。したがって、 SAP LaMa を使用している場合は、 /usr/sap/SID の NFS ボリュームをマウントしないでください。

NFSv3 では、ソフトウェアまたはサーバに障害が発生した場合に NFS ロックのクリーンアップ処理が行われないようにするため、 NFS ロックをオフにする必要があります。

ONTAP 9 では、 NFS 転送サイズを最大 1MB に設定できます。具体的には、 40GbE 以上でのストレージシステムへの接続では、スループットの期待値を達成するために転送サイズを 1MB に設定する必要があります。

| 共通パラメータ | **NFSv3** | **NFSv4** | **ONTAP 9** での **NFS** 転送サイズ | **ONTAP 8** での **NFS** 転送サイズ |
|---|---|---|---|---|
| rw 、 bg 、 hard 、 timeo = 600 、 noatime | nfsvers = 3、nolock | nfsvers = 4.1、ロック | rsize=1048576 、 wsize=262144 | rsize=65536 、 wsize=65536 です |

NFSv3 の読み取りパフォーマンスを向上させるには、「 nConnect=n 」マウントオプションを使用することを推奨します。このオプションは、 SUSE Linux Enterprise Server 12 SP4 以降および RedHat Enterprise Linux （ RHEL ） 8.3 以降で使用できます。

パフォーマンステストによると、 `nconnect=4` データボリュームの読み取り結果が良好です。ログへの書き込みは、次のようなセッション数が少ないことでメリットが得られる場合があります。 `nconnect=2`。共有ボリュームには、「nConnect」オプションを使用することもできます。NFS サーバからの最初のマウント（ IP アドレス）では、使用されるセッションの量が定義されることに注意してください。同じIPアドレスにさらにマウントしても、nConnectに別の値が使用されていても、この値は変更されません。

ONTAP 9.8およびSUSE SLES15SP2以降、またはRed Hat RHEL 8.4以降では、ネットアップはNFSv4.1のnConnectオプションもサポートしています。追加情報については、 Linux ベンダーのマニュアルを参照してください。

nconnectをNFSv4.xで使用する場合は、次のルールに従ってNFSv4.xセッションスロットの数を調整する必要があります。セッションスロットの数は<nconnect value> x 64と等しくなります。ホストでこれを確認し `echo options nfs max_session_slots=<calculated value> > /etc/modprobe.d/nfsclient.conf`てから再起動します。サーバー側の値も調整する必要があります。で説明されているように、セッションスロットの数を設定します。"NFSv4 の NFS 設定"

次の例は、 SID=NF2 で、 NFSv3 を使用し、書き込みの場合は NFS 転送サイズが 1MB 、読み取りの場合は 256K の、シングルホスト SAP HANA データベースを示しています。/etc/fstab 構成ファイルを使用してシステムのブート中にファイル・システムをマウントするには ' 次の手順を実行します

1. 必要なファイル・システムを /etc/fstab 構成ファイルに追加します

```
sapcc-hana-tst-06:/ # cat /etc/fstab
<storage-vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data01>:/NF2_shared/usr-sap /usr/sap/NF2 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data01>:/NF2_shared/shared /hana/shared nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
```

2. Run `ount – a を実行して、すべてのホストのファイルシステムをマウントします。

次の例は、 SID=NF2 で、データファイルシステムとログファイルシステムに NFSv4.1 を使用し、「 /hana/shared 」ファイルシステムと「 /usr/sap/nf2 」ファイルシステムに NFSv3 を使用する、マルチホスト SAP HANA データベースを示しています。書き込みでは、読み取りの場合は 1MB 、書き込みの場合は 256K の NFS 転送サイズが使用されます。

1. 必要なファイル・システムを ' すべてのホスト上の /etc/fstab 構成ファイルに追加します

。 `/usr/sap/NF2` ファイルシステムはデータベースホストごとに異なります。次の例は、 `/NF2_shared/usr-sap-host1`。

```
stlrx300s8-5:/ # cat /etc/fstab
<storage-vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-data02>:/NF2_data_mnt00002 /hana/data/NF2/mnt00002 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-log02>:/NF2_log_mnt00002 /hana/log/NF2/mnt00002 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-data02>:/NF2_shared/usr-sap-host1 /usr/sap/NF2 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data02>:/NF2_shared/shared /hana/shared nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
```

2. Run `ount – a を実行して、すべてのホストのファイルシステムをマウントします。

**NFSv4** 用の **SAP HANA** インストールの準備

## NFS バージョン 4 以降では、ユーザ認証が必要です。この認証は、 Lightweight Directory Access Protocol （ LDAP ）サーバやローカルユーザアカウントなどの中央ユーザ管理ツールを使用して実行できます。次のセクションでは、ローカルユーザアカウントを設定する方法について説明します。

管理ユーザ <sid>adm,`<sid>crypt`SAP HANAソフトウェアのインストールを開始する前に、SAP HANAホストとストレージコントローラにと `sapsys`グループを手動で作成する必要があります。

**SAP HANA** ホスト

存在しない場合は、 SAP HANA ホストに「 sapsys 」グループを作成する必要があります。ストレージコントローラ上の既存のグループ ID と競合しない一意のグループ ID を選択する必要があります。

ユーザ `<sid>adm`と `<sid>crypt`がSAP HANAホストに作成されます。ストレージコントローラの既存のユーザIDと競合しない一意のIDを選択する必要があります。

マルチホストSAP HANAシステムの場合は、ユーザIDとグループIDがすべてのSAP HANAホストで同じである必要があります。グループとユーザは、および `/etc/passwd`の影響を受ける行をソースシステムから他のすべてのSAP HANAホストにコピーすることで、他のSAP HANAホストに作成され `/etc/group`ます。

マルチホスト SAP HANA システムの場合、ユーザ ID とグループ ID はすべての SAP HANA ホストで同じである必要があります。グループとユーザは、移行元システムから他のすべての SAP HANA ホストに「 /etc/group 」および「 /etc/passwd 」の該当する行をコピーすることによって、他の SAP HANA ホスト上に作成されます。

NFSv4 ドメインは、すべての Linux サーバと SVM で同じ値に設定する必要があります。Linux ホストの場合は ' ファイル /etc/idmapd.conf にドメイン・パラメータ「ドメイン・ドメイン = <domain_name>` 」を設定します

NFS idmapd サービスを有効にして開始します。

```
systemctl enable nfs-idmapd.service
systemctl start nfs-idmapd.service
```

最新の Linux カーネルでは、この手順は必要ありません。警告メッセージは無視してかまいません。

ストレージコントローラ

ユーザ ID とグループ ID は、 SAP HANA ホストとストレージコントローラで同じである必要があります。グループとユーザは、ストレージクラスタで次のコマンドを入力することで作成されます。

```
vserver services unix-group create -vserver <vserver> -name <group name>
-id <group id>
vserver services unix-user create -vserver <vserver> -user <user name> -id
<user-id> -primary-gid <group id>
```

また、 SVM の UNIX ユーザルートのグループ ID を 0 に設定します。

```
vserver services unix-user modify -vserver <vserver> -user root -primary
-gid 0
```

**SAP HANA** 向けの **I/O** スタック構成

## SAP HANA 1.0 SPS10 以降、 I/O 動作を調整し、使用中のファイルシステムとストレージシステムのデータベースを最適化するためのパラメータが導入されています。

ネットアップは、最適な値を定義するため、パフォーマンステストを実施しました。次の表に、パフォーマンステストから推定した最適な値を示します。

| パラメータ | 価値 |
| --- | --- |
| max_parallel _io_requests と入力します | 128 |
| async _read_submit | オン |
| async ： write_submit_active | オン |
| async_write_submit_bblocks | すべて |

バージョン SPS12 までの SAP HANA 1.0 では、これらのパラメータは、 SAP HANA データベースのインストール時に設定できます。これは、 SAP ノートで説明されています "2267798 ： Configuration of the SAP

HANA Database During Installation Using hdbparam 』で説明されています"。

また 'hdbparam フレームワークを使用して SAP HANA データベースのインストール後にパラメータを設定することもできます

```
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_read_submit=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

SAP HANA 2.0 以降 'hdbparam' は廃止され ' パラメータは global.ini` に移動されましたパラメータは、 SQL コマンドまたは SAP HANA Studio を使用して設定できます。詳細については、 SAP ノートを参照してください "2399079 ： HANA で hdbparam の除去 2"。パラメータは、次のように global.ini 内で設定することもできます。

```
nf2adm@stlrx300s8-6: /usr/sap/NF2/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

SAP HANA 2.0 SPS5 以降では、「 setParameter.py 」スクリプトを使用して正しいパラメータを設定できます。

```
nf2adm@sapcc-hana-tst-03:/usr/sap/NF2/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

**SAP HANA** データボリュームのサイズ

デフォルトでは、 SAP HANA サービスごとに使用されるデータボリュームは 1 つだけ

です。ファイルシステムの最大ファイルサイズ制限のため、データボリュームの最大サイズを制限することを推奨します。

これを自動的に行うには ' global.ini` の [persistence] セクションで次のパラメータを設定します

```
datavolume_striping = true
datavolume_striping_size_gb = 8000
```

これにより、 8 、 000GB の上限に達すると新しいデータボリュームが作成されます。 "SAP ノート 240005 の質問 15 を参照してください" 詳細については ' を参照してください

### SAP HANA ソフトウェアのインストール

このセクションでは、シングルホストシステムとマルチホストシステムに SAP HANA ソフトウェアをインストールするためのシステムの構成方法について説明します。

#### シングルホストシステムにインストールします

SAP HANA ソフトウェアのインストールでは、シングルホストシステムについて行う追加の準備作業はありません。

#### マルチホストシステムにをインストールします

マルチホストシステムに SAP HANA をインストールするには、次の手順を実行します。

1. SAPインストールツールを使用して `hdbclm`、いずれかのワーカーホストで次のコマンドを実行してインストールを開始します。オプションを使用し `addhosts`て（`sapcc-hana-tst-03`、2番目のワーカーとスタンバイホストを追加し(`sapcc-hana-tst-04`ます）。

```
apcc-hana-tst-02:/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_LCM_LINUX_X86_64 #
./hdblcm --action=install --addhosts=sapcc-hana-tst-03:role=worker,sapcc
-hana-tst-04:role=standby

SAP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
```

```
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1
(1.015.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
```

```
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip


SAP HANA Database version '2.00.073.00.1695288802' will be installed.

Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------
--------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version
2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
  9     | epmmds          | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
4.203.2321.0.0

Enter comma-separated list of the selected indices [3,4]: 2,3
```

2. 選択したすべてのコンポーネントが、すべてのワーカーホストとスタンバイホストにインストールされていることを確認します。

データボリュームのパーティションを追加しています

SAP HANA 2.0 SPS4 以降では、追加のデータボリュームパーティションを構成できます。これにより、 SAP HANA テナントデータベースのデータボリュームに複数のボリュームを構成し、単一ボリュームのサイズやパフォーマンスの制限を超えて拡張できます。

> データボリュームに 2 つ以上の個別のボリュームを使用すると、 SAP HANA シングルホストシステムと SAP HANA マルチホストシステムを使用できます。データボリュームのパーティションはいつでも追加できます。

追加のデータボリュームパーティションの有効化

追加のデータボリュームパーティションを有効にするには、 SYSTEMDB 構成で SAP HANA Studio または Cockpit を使用して、 global.ini` 内に次のエントリを追加します。

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

パラメータを global.ini` ファイルに手動で追加するには ' データベースを再起動する必要があります

シングルホスト **SAP HANA** システムのボリューム構成

複数のパーティションを持つシングルホスト SAP HANA システムのボリュームレイアウトは、 1 つのデータボリュームパーティションを含むシステムのレイアウトに似ていますが、追加のデータボリュームは、ログボリュームとして別のアグリゲートに格納され、残りのデータボリュームは他のデータボリュームに格納されます。次の表は、 2 つのデータボリュームパーティションを持つ SAP HANA シングルホストシステムの構成例を示しています。

| アグリゲート **1** ：コントローラ **A** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **b** のアグリゲート **2** |
|---|---|---|---|
| データボリューム： SID_data_mnt00001 | 共有ボリューム： SID_shared | データボリューム： SID_data2_mnt00001 | ログボリューム： SID_log_mnt00001 |

次の表に、 2 つのデータボリュームパーティションを持つシングルホストシステムのマウントポイント構成の例を示します。

| ジャンクションパス | ディレクトリ | **HANA** ホストのマウントポイント |
|---|---|---|
| SID_data_mnt00001 | – | /hana/data/SID/mnt00001 |
| SID_data2_mnt00001 | – | /hana/data2/SID/mnt00001 |
| SID_log_mnt00001 | – | /hana/log/sid/mnt00001 |
| SID_shared | usr - SAP 共有 | /usr/sap/SID/hana/shared に格納されています |

新しいデータボリュームを作成し、 NetApp ONTAP システムマネージャまたは ONTAP CLI を使用してネームスペースにマウントできます。

マルチホスト **SAP HANA** システムのボリューム構成

ボリュームのレイアウトは、 1 つのデータボリュームパーティションを含むマルチホスト SAP HANA システムのレイアウトに似ていますが、追加のデータボリュームはログボリュームとして別のアグリゲートに格納され、残りのデータボリュームはもう 1 つのデータボリュームに格納されます。次の表は、 2 つのデータボリュームパーティションを持つ SAP HANA マルチホストシステムの構成例を示しています。

| 目的 | アグリゲート **1** ：コントローラ **A** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| ノード 1 のデータボリュームとログボリューム | データボリューム：SID_data_mnt00001 | – | ログボリューム：SID_log_mnt00001 | data2 ボリューム：SID_data2_mnt00001 |
| ノード 2 のデータボリュームとログボリューム | ログボリューム：SID_log_mnt00002 | data2 ボリューム：SID_data2_mnt00002 | データボリューム：SID_data_mnt00002 | – |
| ノード 3 のデータボリュームとログボリューム | – | データボリューム：SID_data_mnt00003 | data2 ボリューム：SID_data2_mnt00003 | ログボリューム：SID_log_mnt00003 |
| ノード 4 のデータボリュームとログボリューム | data2 ボリューム：SID_data2_mnt00004 | ログボリューム：SID_log_mnt00004 | – | データボリューム：SID_data_mnt00004 |
| すべてのホストの共有ボリューム | 共有ボリューム：SID_shared | – | – | – |

次の表に、 2 つのデータボリュームパーティションを持つシングルホストシステムのマウントポイント構成の例を示します。

| ジャンクションパス | ディレクトリ | **SAP HANA** ホストのマウントポイント | 注 |
|---|---|---|---|
| SID_data_mnt00001 | – | /hana/data/SID/mnt00001 | すべてのホストにマウントされています |
| SID_data2_mnt00001 | – | /hana/data2/SID/mnt00001 | すべてのホストにマウントされています |
| SID_log_mnt00001 | – | /hana/log/sid/mnt00001 | すべてのホストにマウントされています |
| SID_data_mnt00002 | – | /hana/data/sid/mnt00002 | すべてのホストにマウントされています |
| SID_data2_mnt00002 | – | /hana/data2/SID/mnt00002 | すべてのホストにマウントされています |
| SID_log_mnt00002 | – | /hana/log/sid/mnt00002 | すべてのホストにマウントされています |
| SID_data_mnt00003 | – | /hana/data/sid/mnt00003 | すべてのホストにマウントされています |
| SID_data2_mnt00003 | | /hana/data2/SID/mnt00003 | すべてのホストにマウントされています |
| SID_log_mnt00003 | | /hana/log/sid/mnt00003 | すべてのホストにマウントされています |
| SID_data_mnt00004 | | /hana/data/sid/mnt00004 | すべてのホストにマウントされています |

| ジャンクションパス | ディレクトリ | **SAP HANA** ホストのマウントポイント | 注 |
|---|---|---|---|
| SID_data2_mnt00004 | – | /hana/data2/SID/mnt00004 | すべてのホストにマウントされています |
| SID_log_mnt00004 | – | /hana/log/sid/mnt00004 | すべてのホストにマウントされています |
| SID_shared | 共有 | /hana/shared-SID を指定します | すべてのホストにマウントされています |
| SID_shared | usr-sap-host1 | /usr/sap/SID | ホスト 1 にマウントされています |
| SID_shared | usr-sap-host2 | /usr/sap/SID | ホスト 2 にマウントされています |
| SID_shared | usr-sap-host3 | /usr/sap/SID | ホスト 3 にマウント |
| SID_shared | usr-sap-host4 | /usr/sap/SID | ホスト 4 にマウント |
| SID_shared | usr-sap-host5 | /usr/sap/SID | ホスト 5 にマウント |

新しいデータボリュームを作成し、 ONTAP System Manager または ONTAP CLI を使用してネームスペースにマウントできます。

ホストの設定

セクションで説明したタスクに加えて"ホストのセットアップ、"、新しい追加データボリュームの追加のマウントポイントおよび `fstab`エントリを作成し、新しいボリュームをマウントする必要があります。

1. 追加のマウントポイントを作成します。
   - シングルホストシステムの場合は、マウントポイントを作成し、データベースホストに権限を設定します。

     ```
     sapcc-hana-tst-06:/ # mkdir -p /hana/data2/SID/mnt00001
     sapcc-hana-tst-06:/ # chmod –R 777 /hana/data2/SID
     ```

   - マルチホストシステムの場合は、マウントポイントを作成し、すべてのワーカーホストとスタンバイホストに権限を設定します。

     以下のコマンド例は、 2+1 のマルチホスト HANA システムを示しています。

     - 1 つ目のワーカーホスト：

       ```
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-06:~ # chmod -R 777 /hana/data2/SID
       ```

     - 2 つ目のワーカーホスト：

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
```

- スタンバイホスト：

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
```

2. すべてのホスト上の /etc/fstab 構成ファイルに追加のファイル・システムを追加します

   NFSv4.1 を使用するシングルホストシステムの場合は、次の例を参照してください。

```
<storage-vif-data02>:/SID_data2_mnt00001 /hana/data2/SID/mnt00001 nfs
rw, vers=4
minorversion=1,hard,timeo=600,rsize=1048576,wsize=262144,bg,noatime,lock
0 0
```

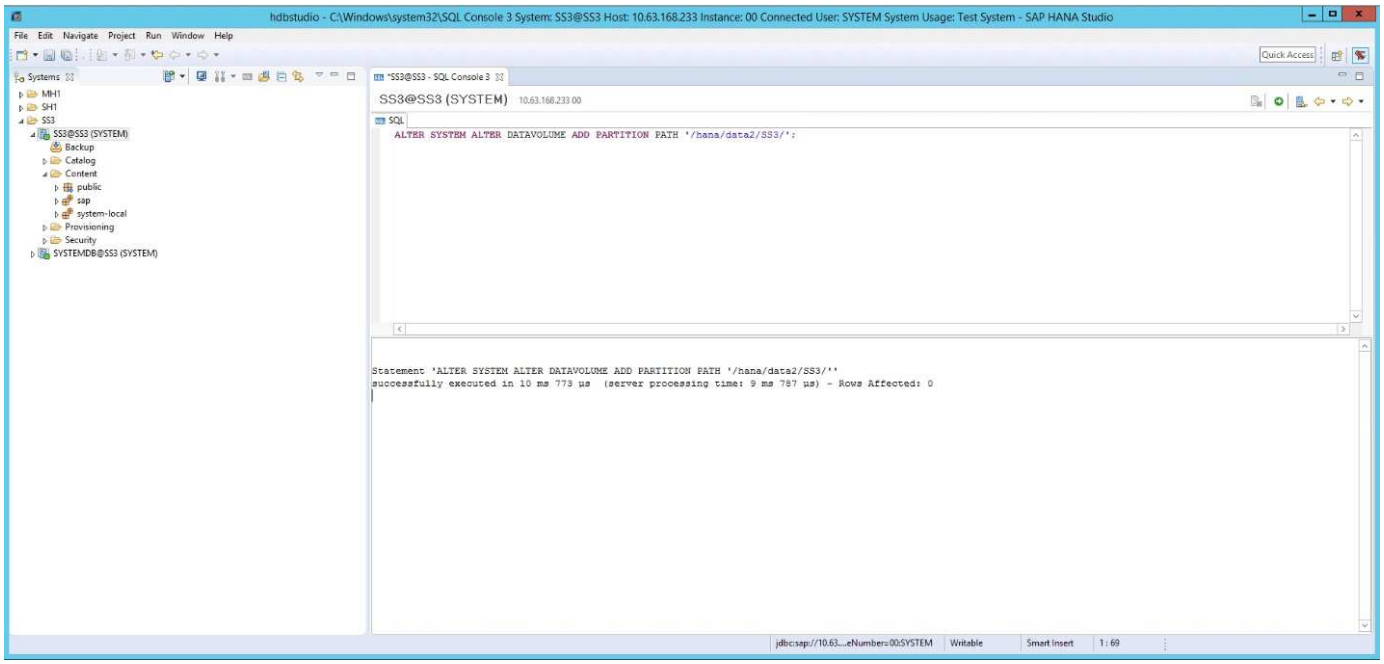
   各データボリュームを接続するために異なるストレージ仮想インターフェイスを使用して、ボリュームごとに異なる TCP セッションを使用するか、使用している OS で利用可能な場合は nConnect マウントオプションを使用します。

3. 「 mount – a 」コマンドを実行して、ファイルシステムをマウントします。

データボリュームパーティションを追加しています

テナントデータベースに対して次の SQL ステートメントを実行し、テナントデータベースにデータボリュームパーティションを追加します。追加のボリュームへのパスを使用します。

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```




## 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。

- "SAP HANA ソフトウェアソリューション"
- "TR-4646 ：『 SAP HANA Disaster Recovery with Storage Replication 』"
- "TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"
- "TR-4667：『Automating SAP System Copies Using the SnapCenter SAP HANA Plug-in』"
- ネットアップドキュメントセンター

  "https://www.netapp.com/support-and-training/documentation/"

- SAP HANA 向け SAP 認定エンタープライズストレージハードウェア

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"

- SAP HANA のストレージ要件

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"

- 『 SAP HANA Tailored Data Center Integration Frequently Asked Questions 』

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"

- SAP HANA on VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"

- 『SAP HANA on VMware vSphere Best Practices Guide』

"https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

## 履歴を更新します

この解決策の初版以降には、次の技術的な変更が加えられています。

| 日付 | 概要を更新します |
|---|---|
| 2015年10月 | 初版 |
| 2016年3月 | 容量のサイジングを更新し '/hana/shared のマウント・オプションを更新し 'sysctl パラメータを更新 |
| 2017年2月 | 新しいネットアップストレージシステムとディスクシェルフ 40GbE に対応した ONTAP 9 の新機能新しい OS リリース（ SUSE Linux Enterprise Server 12 SP1 および Red Hat Enterprise Linux 7.2 ）新しい SAP HANA リリース |
| 2017年7月 | マイナーアップデート |
| 2018年9月 | 新しいネットアップストレージシステムは 100GbE をサポート新しい OS リリース（ SUSE Linux Enterprise Server 12 SP3 および Red Hat Enterprise Linux 7.4 ）では、 SAP HANA 2.0 SPS3 のマイナーな変更が追加されています |
| 2019年10月 | 新しいネットアップストレージシステムと NVMe シェルフ新しい OS リリース（ SUSE Linux Enterprise Server 12 SP4 、 SUSE Linux Enterprise Server 15 、および Red Hat Enterprise Linux 7.6 ） MAX Data ボリュームサイズが変更になりました |
| 2019年12月 | 新しいネットアップストレージシステム新しい OS リリース SUSE Linux Enterprise Server 15 SP1 |
| 2020年3月 | NFSv3 での nConnect のサポート新しい OS リリースは Red Hat Enterprise Linux 8 です |
| 2020年5月 | SAP HANA 2.0 SPS4 で複数のデータボリュームパーティションがサポートされます |
| 2020 年 6 月 | 追加情報オプションの機能に関するマイナーアップデート |
| 2020年12月 | ONTAP 9.8 以降で NFSv4.1 の nconnect がサポートされるようになりました。新しいバージョンの SAP HANA がリリースされました |
| 2021年2月 | ネットアップストレージシステムが新しく追加されると、ホストネットワークの設定が変更されます。軽微な変更が |
| 2021年4月 | VMware vSphere 固有の情報を追加しました |
| 2022年9月 | 新しいOS -リリース |
| 2023年8月 | 新しいストレージシステム（AFF Cシリーズ） |
| 2023年12月 | ホストセットアップの更新：nconnectの設定が改訂され、NFSv4.1セッションに関する情報が追加されました。 |
| 2024年5月 | 新しいストレージシステム（AFF Aシリーズ） |
| 2024年9月 | マイナーアップデート |
| 2024年11月 | 新しいストレージシステム |

| 日付 | 概要を更新します |
| --- | --- |
| 2025年7月 | マイナーアップデート |

# 『 SAP HANA on NetApp ASA Systems with FCP Configuration Guide 』

## 『 SAP HANA on NetApp ASA Systems with Fibre Channel Protocol 』を参照してください

NetApp ASA 製品ファミリーは、 TDI プロジェクトの SAP HANA との使用が認定されています。このガイドでは、このプラットフォーム上の SAP HANA に関するベスト プラクティスについて説明します。

Marco Schoen 、ネットアップ

### はじめに

NetApp ASA AシリーズおよびASA Cシリーズ製品ファミリーは、Tailored Data Center Integration（TDI；テーラードデータセンター統合）プロジェクトでSAP HANAとの使用が認定されています。このガイドでは、次の認定モデルのベスト プラクティスについて説明します。

- ASA A20、ASA A30、ASA A50、ASA A70、ASA A90、ASA A1K
- ASA C30

SAP HANA 向けのネットアップ認定ストレージソリューションの一覧については、を参照してください "認定およびサポートされている SAP HANA ハードウェアディレクトリ"。

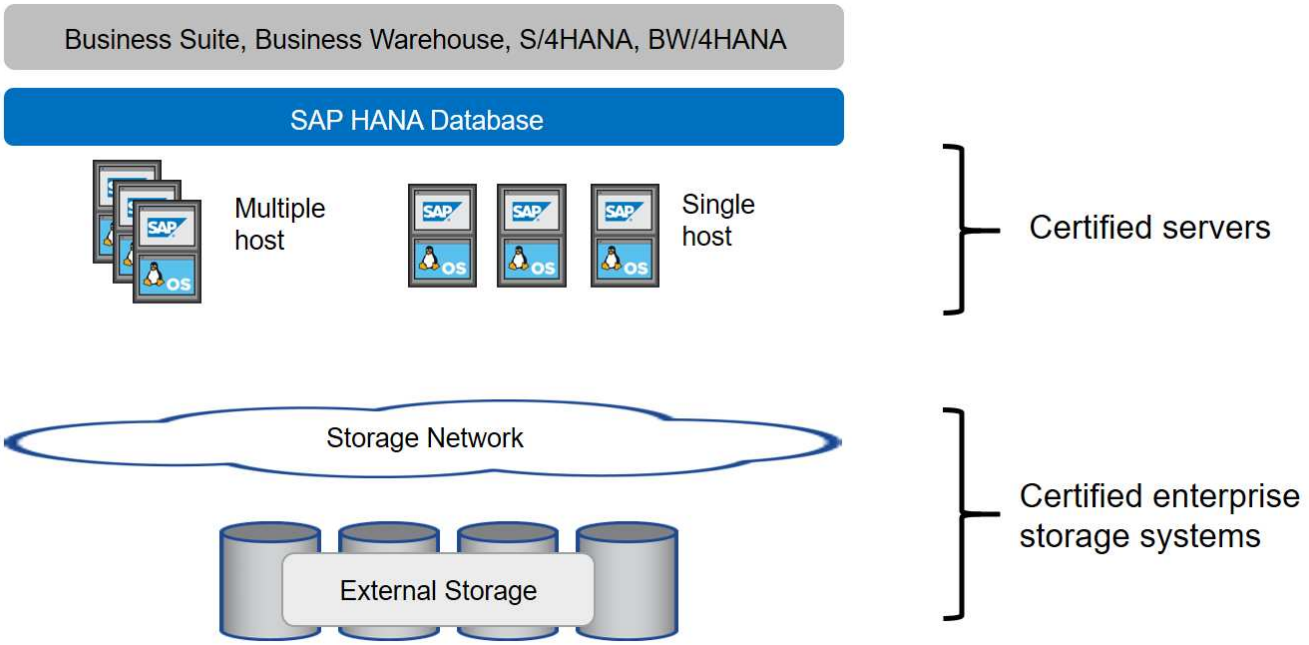
本ドキュメントでは、 Fibre Channel Protocol （ FCP ；ファイバチャネルプロトコル）を使用した ASA 構成について説明します。

> このホワイトペーパーで説明している構成は、 SAP HANA に必要な SAP HANA KPI と、 SAP HANA に最適なパフォーマンスを達成するために必要です。ここに記載されていない設定または機能を変更すると、原因のパフォーマンスが低下したり、予期しない動作が発生したりする可能性があります。変更は、ネットアップのサポートから助言された場合にのみ実施

SAP HANA マルチホスト環境では、 SAP HANA ホストのフェイルオーバー時にフェンシングを提供するために、標準の SAP HANA ストレージコネクタが使用されます。オペレーティングシステムの構成ガイドラインと、 HANA 固有の Linux カーネルの依存関係については、必ず該当する SAP ノートを参照してください。詳細については、を参照してください "SAP Note 2235581 – SAP HANA Supported Operating Systems 』"。

### SAP HANA テーラードデータセンター統合

NetApp ASA ストレージ システムは、FC (SAN) プロトコルを使用する SAP HANA TDI プログラムで認定されています。SAP Business Suite on HANA、S/4HANA、BW/4HANA、SAP Business Warehouse on HANA など、現在のどの SAP HANA シナリオにも、単一ホスト構成または複数ホスト構成で導入できます。SAP HANA との使用が認定されているサーバは、ネットアップ認定のストレージソリューションと組み合わせることができます。次の図に、アーキテクチャの概要を示します。




生産性の高いSAP HANAシステムを実現するための前提条件と推奨事項の詳細については、次のリソースを参照してください。

- "『 SAP HANA Tailored Data Center Integration Frequently Asked Questions 』"

## VMware vSphere を使用した SAP HANA

ストレージを仮想マシン（ VM ）に接続する方法はいくつかあります。Raw デバイス マッピング (RDM) 、FCP データストア、または FCP を使用した VVOL データストアがサポートされています。どちらのデータストアオプションも、本番環境で使用するためにデータストアに格納する SAP HANA データボリュームまたはログボリュームは 1 つだけです。

SAP HANA での vSphere の使用の詳細については、次のリンクを参照してください。

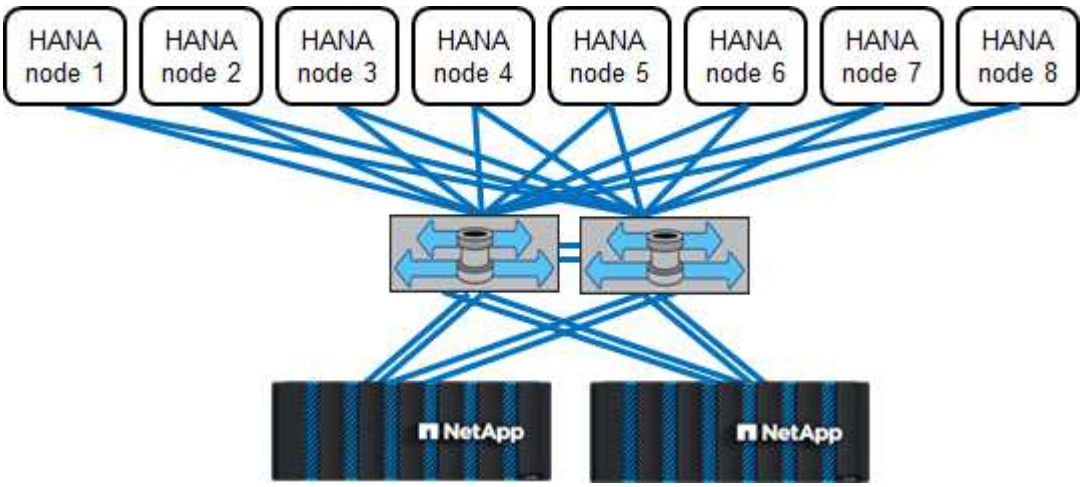
- "SAP HANA on VMware vSphere - 仮想化 - コミュニティ Wiki"
- "『SAP HANA on VMware vSphere Best Practices Guide』"
- "2161991 - VMware vSphere 設定ガイドライン - SAP One Support Launchpad （ログインが必要）"

### アーキテクチャ

SAP HANA ホストは、冗長 FCP インフラとマルチパスソフトウェアを使用してストレージコントローラに接続されます。スイッチまたはホストバスアダプタ（ HBA ）で障害が発生した場合に、耐障害性に優れた SAP HANA ホスト / ストレージ接続を実現するには、冗長 FCP スイッチインフラが必要です。すべての HANA ホストがストレージコントローラ上の必要な LUN にアクセスできるように、スイッチで適切なゾーニングを設定する必要があります。

ASA システム製品ファミリーのさまざまなモデルをストレージレイヤで混在させることができるため、拡張が必要になったり、パフォーマンスや容量のニーズが異なる場合があります。ストレージシステムに接続できる SAP HANA ホストの最大数は、 SAP HANA のパフォーマンス要件と、使用されているネットアップコントローラのモデルによって定義されます。必要なディスクシェルフの数は、 SAP HANA システムの容量とパフォーマンスの要件によってのみ決まります。

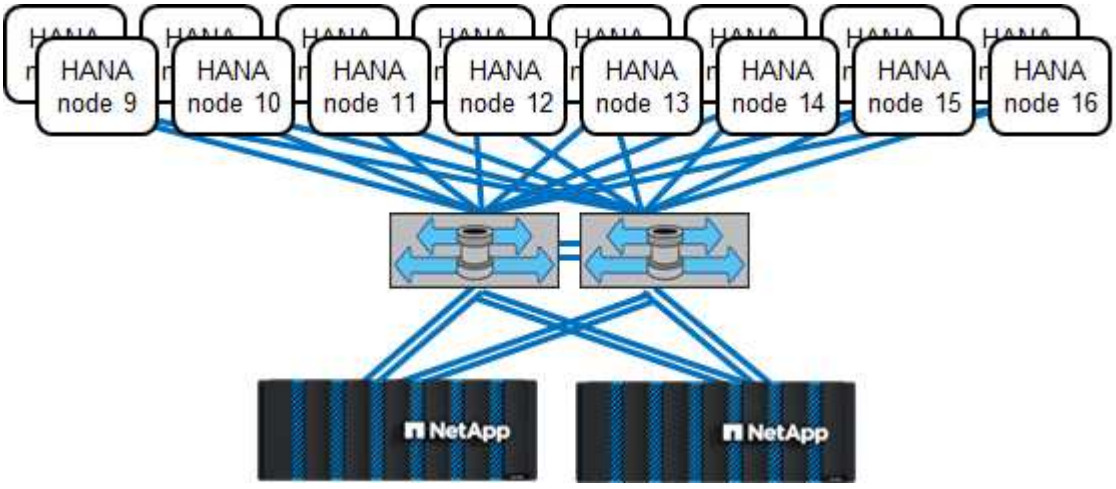
次の図は、 8 台の SAP HANA ホストをストレージ HA ペアに接続した構成例を示しています。



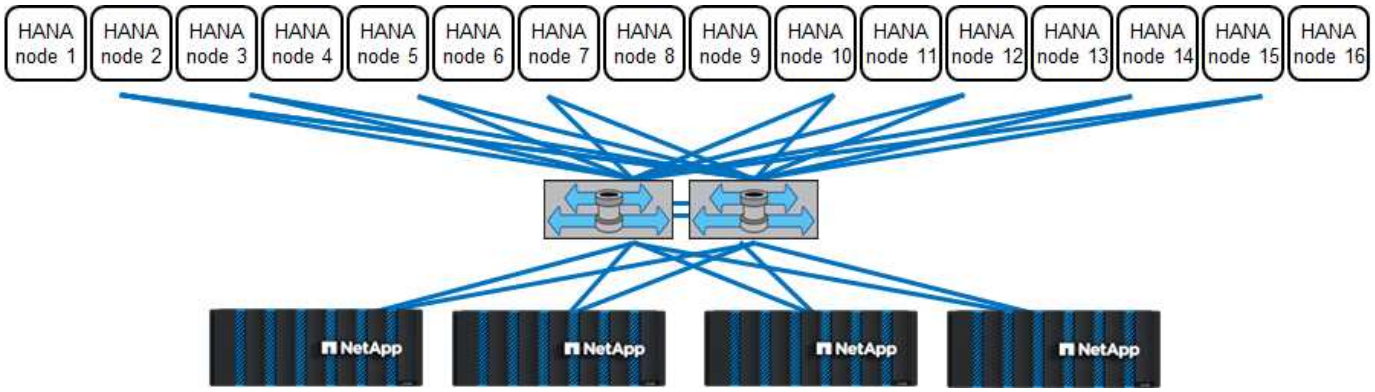

このアーキテクチャは、次の 2 つの側面で拡張できます。

- 既存のストレージに SAP HANA ホストとストレージ容量を追加で接続することで、ストレージコントローラが現在の SAP HANA KPI を満たす十分なパフォーマンスを提供する場合
- 追加の SAP HANA ホスト用にストレージ容量を追加したストレージシステムを追加する

次の図は、追加の SAP HANA ホストをストレージコントローラに接続した場合の構成例を示しています。この例では、 16 台の SAP HANA ホストの容量とパフォーマンスの要件を満たすために、さらにディスクシェルフが必要です。合計スループット要件に応じて、ストレージコントローラへの FC 接続を追加する必要があります。




次の図に示すように、導入した ASA システムとは関係なく、認定済みのストレージコントローラを追加することで、 SAP HANA 環境を拡張して希望するノード密度に合わせることもできます。

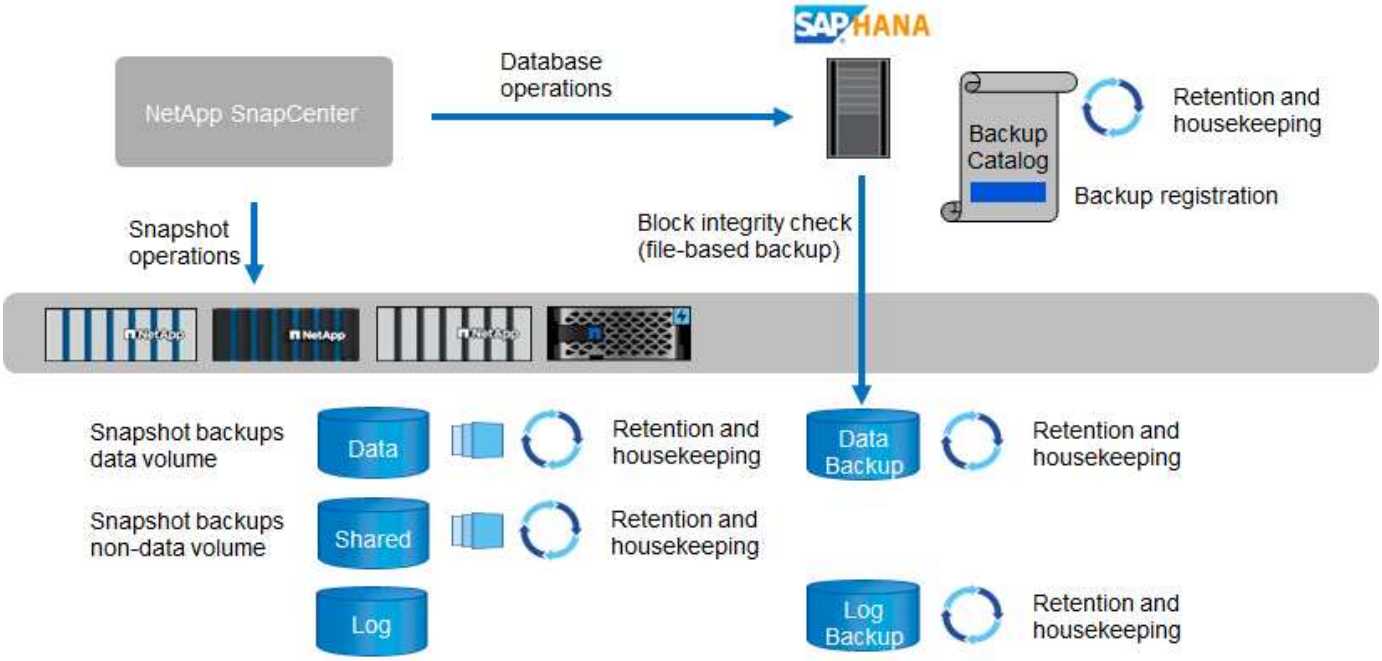



**SAP HANA** のバックアップ

すべてのネットアップストレージコントローラに搭載された ONTAP ソフトウェアは、動作中にパフォーマンスに影響を与えることなく SAP HANA データベースをバックアップするための組み込みメカニズムを提供します。ストレージベースの NetApp Snapshot バックアップは、 SAP HANA の単一コンテナ、および単一のテナントや複数のテナントを使用する SAP HANA MDC システムで使用可能な、完全にサポートされた統合バックアップ解決策です。

ストレージベースの Snapshot バックアップは、 NetApp SnapCenter Plug-in for SAP HANA を使用して実装されます。これにより、 SAP HANA データベースに標準で搭載されているインターフェイスを使用して、整合性のあるストレージベースの Snapshot バックアップを作成できます。SnapCenter は、各 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。そのため、 SnapCenter で作成されたバックアップは、リストア処理とリカバリ処理用に直接選択できる SAP HANA Studio または Cockpit 内に表示できます。

NetApp SnapMirror テクノロジを使用すると、 1 つのストレージシステムで作成された Snapshot コピーを、 SnapCenter で制御されるセカンダリバックアップストレージシステムにレプリケートできます。その後、プライマリストレージ上のバックアップセットごと、およびセカンダリストレージシステム上のバックアップセットごとに、異なるバックアップ保持ポリシーを定義できます。SnapCenter Plug-in for SAP HANA は、不要なバックアップカタログの削除を含め、 Snapshot コピーベースのデータバックアップとログバックアップの保持を自動的に管理します。また、 SnapCenter Plug-in for SAP HANA では、ファイルベースのバックアップを実行することで、 SAP HANA データベースのブロック整合性チェックを実行できます。




ストレージベースの Snapshot バックアップは、従来のファイルベースのバックアップに比べて大きなメリットをもたらします。これには次のような利点がありますが、これらに限定されるわけではありません。

- 高速バックアップ（数分）
- ストレージレイヤでのリストア時間（数分）が大幅に短縮され、バックアップの頻度も高まり、 RTO が短縮されます
- バックアップとリカバリの処理中、 SAP HANA データベースのホスト、ネットワーク、またはストレージのパフォーマンスが低下することはありません
- ブロックの変更に基づいて、スペース効率と帯域幅効率に優れたセカンダリストレージへのレプリケーションを実行します

SAP HANAのバックアップとリカバリのソリューションの詳細については、を参照してください "SnapCenter、SnapMirror Active Sync、VMware Metro Storage ClusterによるSAP HANAのデータ保護と高可用性"。

このドキュメントの作成時点では、VMDK をストレージとして使用する VMware ベースの VM のみが SnapCenter for ASA でサポートされています。

### SAP HANA ディザスタリカバリ

SAP HANA ディザスタリカバリは、 SAP HANA システムレプリケーションを使用してデータベースレイヤで実行するか、ストレージレプリケーションテクノロジを使用してストレージレイヤで実行できます。次のセクションでは、ストレージレプリケーションに基づくディザスタリカバリソリューションの概要について説明します。

SAP HANAディザスタリカバリ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-4646 ： 『 SAP HANA Disaster Recovery with Storage Replication 』"。

#### SnapMirror に基づくストレージレプリケーション

次の図は、ローカルDRデータセンターへの同期SnapMirror Active Syncと、リモートDRデータセンターへの

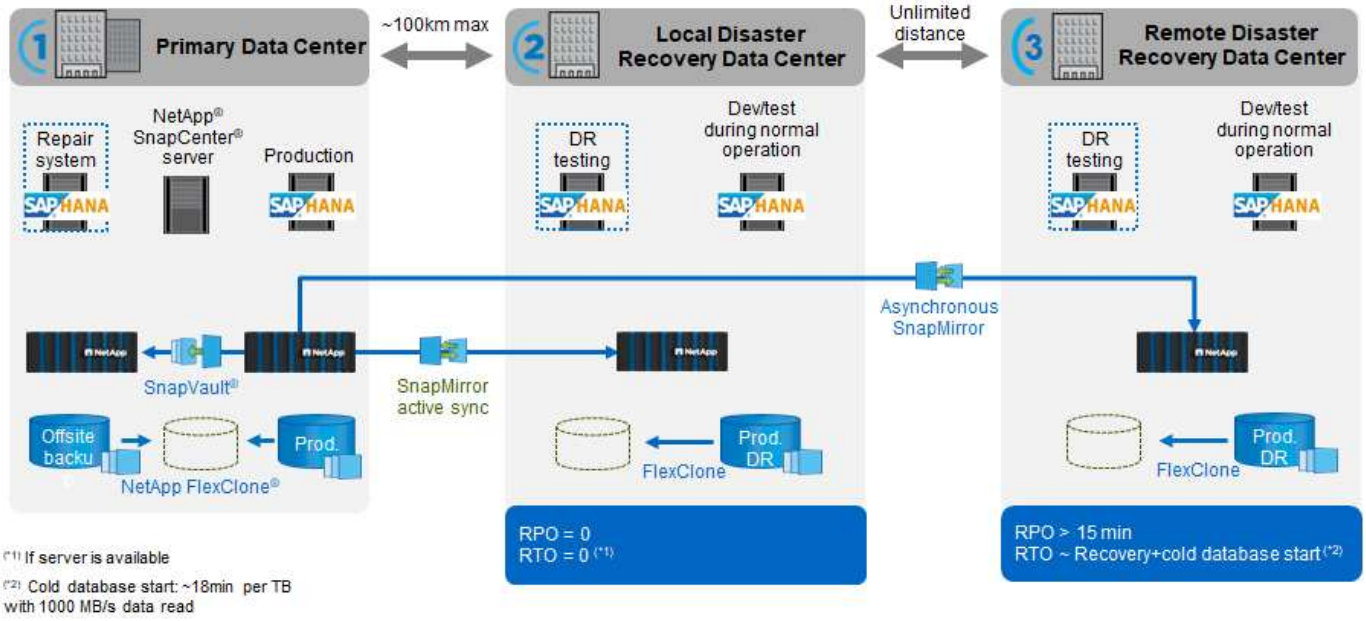
データ複製に非同期SnapMirrorを使用する3サイトのディザスタリカバリソリューションを示しています。SnapMirrorActive Syncにより、サイト全体の障害発生時でもビジネスサービスは継続して稼働し、セカンダリコピー（RPO=0、RTO=0）を使用してアプリケーションを透過的にフェイルオーバーできます。SnapMirrorActive Syncでは、フェイルオーバーを開始するために手動による介入やカスタムスクリプトは必要ありません。ONTAP 9.15.1以降では、SnapMirrorアクティブ同期で対称アクティブ/アクティブ機能がサポートされます。対称アクティブ/アクティブ：双方向同期レプリケーションにより、保護されたLUNの両方のコピーからの読み取りおよび書き込みI/O処理を有効にし、両方のLUNコピーがローカルでI/O処理を処理できるようにします。

詳細は以下をご覧ください。 "ONTAPでのSnapMirrorアクティブ同期の概要" ..

非同期 SnapMirror レプリケーションの RTO は、主に DR サイトで HANA データベースを起動し、データをメモリにロードするのに必要な時間によって決まります。1000Mbps のスループットでデータが読み取られることを前提とし、 1TB のデータをロードするには約 18 分かかります。

DR サイトのサーバは、通常運用時に開発 / テストシステムとして使用できます。災害が発生した場合は、開発 / テスト用システムをシャットダウンし、 DR 本番用サーバとして起動する必要があります。

どちらのレプリケーション方法でも、 RPO と RTO に影響を与えることなく DR ワークフローテストを実行できます。FlexClone ボリュームはストレージ上に作成され、 DR テストサーバに接続されます。




## ストレージのサイジング

次のセクションでは、 SAP HANA 用のストレージシステムのサイジングに必要なパフォーマンスと容量に関する考慮事項の概要を説明します。

ストレージのサイジングプロセスをサポートし、適切なサイズのストレージ環境を構築するには、ネットアップまたはネットアップパートナーの営業担当者にお問い合わせください。

### パフォーマンスに関する考慮事項

SAP では、ストレージの主要パフォーマンス指標（ KPI ）の静的なセットが定義されています。これらの KPI は、データベースホストのメモリサイズや SAP HANA データベースを使用するアプリケーションに関係

なく、すべての SAP HANA 本番環境に対して有効です。これらの KPI は、シングルホスト環境、マルチホスト環境、 Business Suite on HANA 環境、 Business Warehouse on HANA 環境、 S/4HANA 環境、および BW/4HANA 環境で有効です。したがって、現在のパフォーマンスサイジングアプローチは、ストレージシステムに接続されているアクティブな SAP HANA ホストの数にのみ依存します。

ストレージパフォーマンス KPI は、本番用 SAP HANA システムにのみ必須ですが、すべての HANA システムに実装できます。

SAP はパフォーマンステストツールを提供します。このツールは、ストレージに接続されたアクティブな SAP HANA ホストのストレージシステムパフォーマンスを検証するために使用する必要があります。

ネットアップは、特定のストレージモデルに接続できる SAP HANA ホストの最大数をテストして事前に定義しました。さらに、本番環境ベースの SAP HANA システムに必要なストレージ KPI を実現しています。

ディスクシェルフで実行できる SAP HANA ホストの最大数と、 SAP HANA ホストごとに必要な SSD の最小数は、 SAP パフォーマンステストツールを実行して決定されています。このテストでは、ホストの実際のストレージ容量要件は考慮しません。また、必要な実際のストレージ構成を決定するために、容量要件を計算する必要があります。

#### NS224 NVMe シェルフ

1つのNVMe SSD（データ）は、使用する特定のNVMeディスクに応じて、最大2/5のSAP HANAホストをサポートします。

ディスクシェルフを追加しても、ストレージコントローラでサポートできる SAP HANA ホストの最大数は増加しません。

混在ワークロード

SAP HANA とその他のアプリケーションワークロードを、同じストレージコントローラ上または同じストレージアグリゲート内で実行することはできません。ただし、ネットアップのベストプラクティスとして、 SAP HANA ワークロードを他のすべてのアプリケーションワークロードから分離することを推奨します。

SAP HANA ワークロードとその他のアプリケーションワークロードを、同じストレージコントローラまたは同じアグリゲートに導入することもできます。その場合は、混在ワークロード環境内で SAP HANA に対して適切なパフォーマンスが確保されていることを確認する必要があります。また、 Quality of Service （ QoS ；サービス品質）パラメータを使用して、 SAP HANA アプリケーションに対する他のアプリケーションの影響を制御し、 SAP HANA アプリケーションのスループットを保証することも推奨します。

SAP HCMT テストツールを使用して、他のワークロードにすでに使用されている既存のストレージコントローラで、追加の SAP HANA ホストを実行できるかどうかを確認する必要があります。SAP アプリケーションサーバは、 SAP HANA データベースと同じストレージコントローラやアグリゲートに安全に配置できます。

容量に関する考慮事項

SAP HANA の容量要件の詳細な概要については、を参照してください "SAP ノート 1900823" ホワイトペーパー。

複数の SAP HANA システムで構成される SAP 環境全体の容量サイジングは、ネットアップの SAP HANA ストレージサイジングツールを使用して決定する必要があります。ストレージのサイジングプロセスを検証し、適切なサイズのストレージ環境を構築するには、ネットアップまたはネットアップパートナーの営業担当者にお問い合わせください。

パフォーマンステストツールの設定

SAP HANA 1.0 SPS10 以降、 I/O 動作を調整し、使用中のファイルシステムとストレージシステムのデータベースを最適化するためのパラメータが導入されています。SAP のテストツールでストレージのパフォーマンスをテストするときは、 SAP のパフォーマンステストツールにもこれらのパラメータを設定する必要があります。

ネットアップは、最適な値を定義するため、パフォーマンステストを実施しました。次の表に、 SAP テストツールの構成ファイルで設定する必要があるパラメータを示します。

| パラメータ | 価値 |
| --- | --- |
| max_parallel _io_requests と入力します | 128 |
| async _read_submit | オン |
| async ： write_submit_active | オン |
| async_write_submit_bblocks | すべて |

SAP テストツールの設定の詳細については、を参照してください "SAP ノート 1943937" HWCCT （ SAP HANA 1.0 ）および "SAP ノート 2493172" HCMT/HCOT 用（ SAP HANA 2.0 ）。

次の例は、 HCMT/HCOT 実行プランに変数を設定する方法を示しています。

```
…
{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "DataAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
          "Name": "LogAsyncWriteSubmitActive",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
```

```
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

これらの変数はテスト構成に使用する必要があります。これは通常、 SAP が HCMT/HCOT ツールを使用して提供する事前定義された実行計画の場合です。次に、 4k ログの書き込みテストの例を示します。

```
…
       {
          "ID": "D664D001-933D-41DE-A904F304AEB67906",
          "Note": "File System Write Test",
          "ExecutionVariants": [
             {
                "ScaleOut": {
                   "Port": "${RemotePort}",
                   "Hosts": "${Hosts}",
                   "ConcurrentExecution": "${FSConcurrentExecution}"
                },
                "RepeatCount": "${TestRepeatCount}",
                "Description": "4K Block, Log Volume 5GB, Overwrite",
                "Hint": "Log",
                "InputVector": {
                   "BlockSize": 4096,
                   "DirectoryName": "${LogVolume}",
                   "FileOverwrite": true,
                   "FileSize": 5368709120,
                   "RandomAccess": false,
                   "RandomData": true,
                   "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                   "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                   "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                   "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                   "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                   "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                   "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                   "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                   "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
                }
             },
…
```

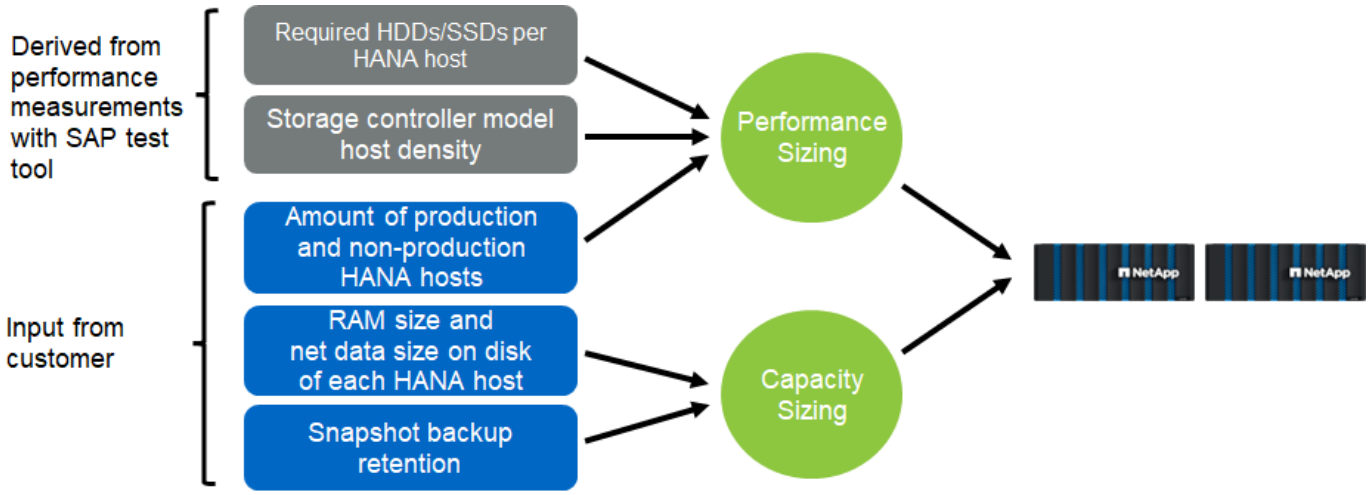
ストレージサイジングプロセスの概要

各ストレージモデルの HANA ホストあたりのディスク数と SAP HANA ホストの密度は、 SAP HANA テストツールを使用して決定されています。

サイジングプロセスでは、本番用および非本番用の SAP HANA ホストの数、各ホストの RAM サイズ、ストレージベースの Snapshot コピーのバックアップ保持期間などの詳細が必要です。SAP HANA ホストの数によって、必要なストレージコントローラとディスクの数が決まります。

RAM のサイズ、各 SAP HANA ホストでのディスク上の正味データサイズ、および Snapshot コピーのバックアップ保持期間は、容量サイジングの際に入力として使用されます。

次の図に、サイジングプロセスの概要を示します。




## インフラのセットアップと設定

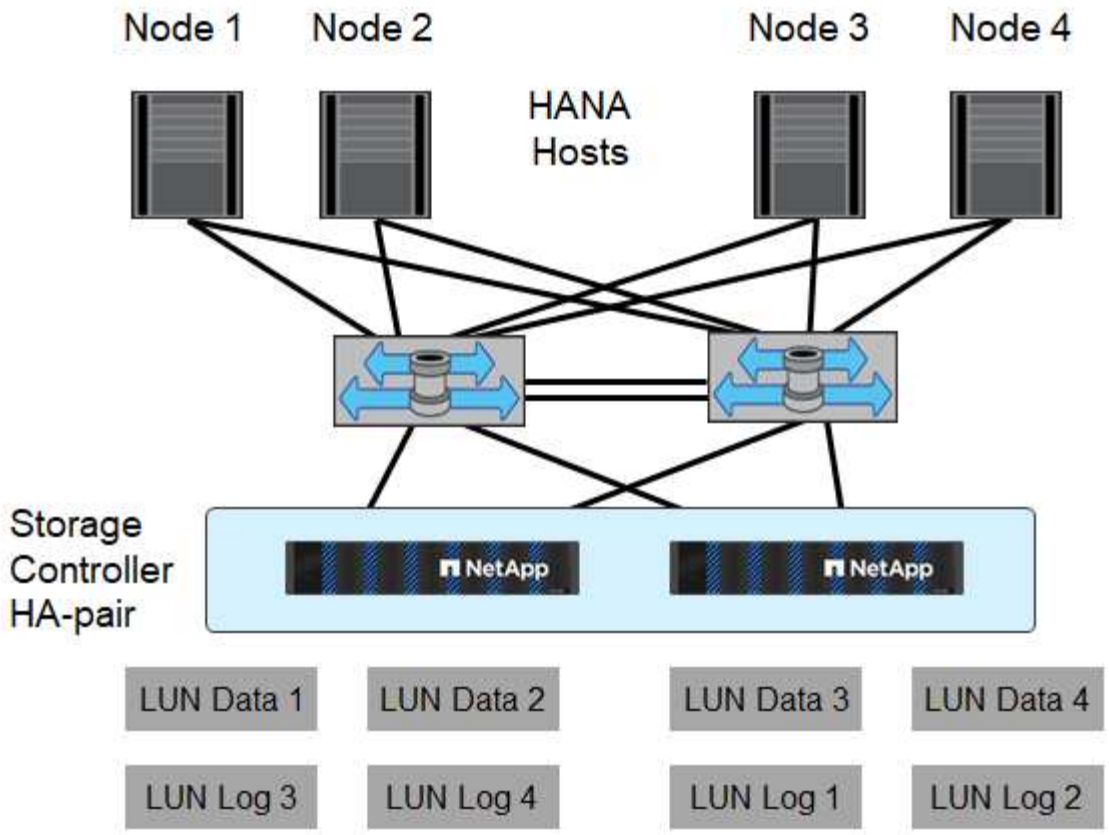
以降のセクションでは、 SAP HANA インフラのセットアップと構成のガイドラインについて説明し、 SAP HANA システムのセットアップに必要なすべての手順について説明します。ここでは、次の設定例を使用します。

- SID=FC5のHANAシステム
  - SAP HANA シングルおよびマルチホスト

### SAN ファブリックのセットアップ

各 SAP HANA サーバには、最低 8Gbps の帯域幅の冗長 FCP SAN 接続が必要です。ストレージコントローラに接続された各 SAP HANA ホストでは、少なくとも 8Gbps の帯域幅をストレージコントローラで設定する必要があります。

次の図は、 4 台の SAP HANA ホストを 2 台のストレージコントローラに接続した場合の例を示しています。各 SAP HANA ホストには、冗長ファブリックに接続された 2 つの FCP ポートがあります。ストレージレイヤでは、各 SAP HANA ホストに必要なスループットを提供するために、 4 つの FCP ポートが構成されます。




スイッチレイヤのゾーニングに加えて、ストレージシステム上の各 LUN を、この LUN に接続するホストにマッピングする必要があります。スイッチ上のゾーニングはシンプルにします。つまり、すべてのホスト HBA がすべてのコントローラ HBA を認識できるゾーンセットを 1 つ定義します。

時刻の同期

ストレージコントローラと SAP HANA データベースホストの間で時刻を同期する必要があります。そのためには、すべてのストレージコントローラとすべての SAP HANA ホストに同じタイムサーバを設定します。

ストレージコントローラのセットアップ

ここでは、ネットアップストレージシステムの構成について説明します。プライマリのインストールとセットアップは、対応する Data ONTAP のセットアップガイドおよび設定ガイドに従って実行する必要があります。

ストレージ効率

SSD 構成の SAP HANA では、インライン重複排除、ボリューム間インライン重複排除、インライン圧縮、インラインコンパクションがサポートされています。

**Quality of Service** の略

QoSを使用すると、共有コントローラ上の特定のSAP HANAシステムまたはSAP以外のアプリケーションのストレージスループットを制限できます。

本番環境と開発/テスト

1つのユースケースは、開発システムとテストシステムのスループットを制限して、混在環境で本番システムに影響を与えないようにすることです。サイジングプロセスでは、非本番システムのパフォーマンス要件を決定する必要があります。開発 / テスト用のシステムは、通常、 SAP で定義されている本番用システム KPI の 20~50% の範囲で、パフォーマンス値を低くしてサイジングすることができます。ストレージシステムのパフォーマンスに最も大きな影響を与えるのは、大きな書き込みI/Oです。そのため、QoSスループットの上限を、データボリュームとログボリュームの対応する書き込みSAP HANAストレージパフォーマンスKPI値の割合に設定する必要があります。

共有環境

もう1つのユースケースは、負荷の高い書き込みワークロードのスループットを制限することです。特に、レイテンシの影響を受けやすい他の書き込みワークロードにこれらのワークロードが影響しないようにするためです。このような環境では、非共有のスループットの上限QoSグループポリシーを各Storage Virtual Machine（SVM）内の各LUNに適用して、個 々 のストレージオブジェクトの最大スループットを指定した値に制限することを推奨します。これにより、1つのワークロードが他のワークロードに悪影響を及ぼす可能性が低くなります。

そのためには、SVMごとにONTAPクラスタのCLIを使用してグループポリシーを作成する必要があります。

```
qos policy-group create -policy-group <policy-name> -vserver <vserver
name> -max-throughput 1000MB/s -is-shared false
```

SVM内の各LUNに適用されます。次の例では、SVM内の既存のすべてのLUNにポリシーグループを適用します。

```
lun modify -vserver <vserver name>  -path * -qos-policy-group  <policy-
name>
```

この作業はSVMごとに行う必要があります。QoSポリシンググループの名前は、SVMごとに異なる名前にする必要があります。新しいLUNの場合は、ポリシーを直接適用できます。

```
lun create -vserver <vserver_name> -path  /vol/<volume_name>/<lun_name>
-size <size> -ostype <e.g. linux>  -qos-policy-group <policy-name>
```

特定のLUNの最大スループットとして1000MB/秒を使用することを推奨します。アプリケーションがより多くのスループットを必要とする場合は、LUNストライピングを備えた複数のLUNを使用して、必要な帯域幅を提供する必要があります。このガイドでは、セクションで、Linux LVMをベースとしたSAP HANAの例を紹介します"ホスト セットアップ"。

> この制限は読み取りにも適用されます。そのため、SAP HANAデータベースの起動時間やバックアップに必要なSLAを満たす十分な数のLUNを使用します。

ストレージを設定する

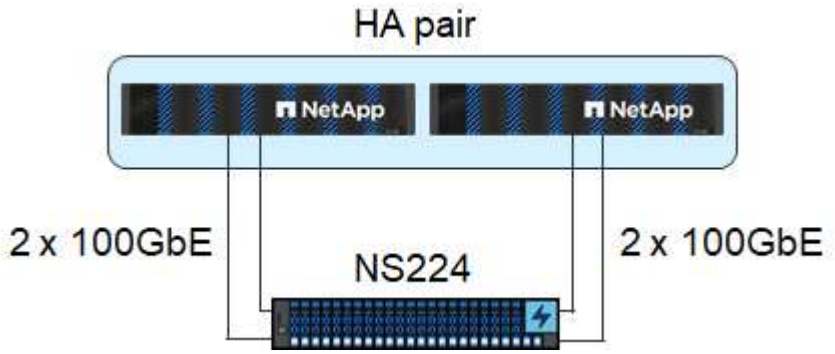
以下に、必要なストレージ構成手順の概要を示します。各手順の詳細については、以降のセクションで説明し

ます。このセクションでは、ストレージハードウェアがセットアップされており、 ONTAP ソフトウェアがすでにインストールされていることを前提としています。また、ストレージ FCP ポートと SAN ファブリックの接続がすでに確立されている必要があります。

1. の説明に従って、正しいディスク・シェルフ構成を確認しますNVMeベースのディスクシェルフ。
2. セクション xref:./bp/saphana-asa-fc-storage-controller-setup.html#initiator-groups の説明に従って、HANA サーバーのワールドワイド名 (WWN) を持つイニシエーター グループ (igroup) を作成します。 [イニシエータグループ] 。
3. LUNを作成し、それをセクションで説明されているサーバーにマッピングします。 "SAP HANA 単一ホストシステムの LUN 構成"そして"SAP HANA マルチホストシステムの LUN 構成"

**NVMe**ベースのディスクシェルフ

次の図に示すように、NS224 NVMeディスクシェルフは、コントローラごとに2つの100GbEポートで接続されます。ディスクは HA ペアの両方のコントローラに自動的に配布されます。




イニシエータグループ

igroup は、サーバごとに、または LUN へのアクセスを必要とするサーバのグループに対して設定できます。igroup の構成には、サーバの World Wide Port Name （ WWPN ）が必要です。

「 anlun 」ツールを使用して次のコマンドを実行し、各 SAP HANA ホストの WWPN を取得します。

```
sapcc-hana-tst:~ # sanlun fcp show adapter
/sbin/udevadm
/sbin/udevadm

host0 ..... WWPN:2100000e1e163700
host1 ..... WWPN:2100000e1e163701
```

この `sanlun`ツールはNetApp Host Utilitiesに含まれており、各SAP HANAホストにインストールする必要があります。詳細については、セクションを参照してください。"ホストのセットアップ："

シングルホスト

# このセクションでは、SAP HANAシングルホストシステムに固有のNetAppストレージシステムの構成について説明します。

### LUN の作成とイニシエーター グループへの LUN のマッピング

NetApp ONTAP System Manager を使用してストレージ ボリュームと LUN を作成し、それらをサーバーの igroup とONTAP CLI にマップできます。

### CLI を使用して LUN を作成し、LUN をイニシエータ グループにマッピングする

このセクションでは、LVM と LVM ボリューム グループごとに 2 つの LUN を使用する SID FC5 の SAP HANA 単一ホスト システムに対して、ONTAP 9 のコマンド ラインを使用した構成例を示します。

1. すべての LUN を作成します。

```
lun create -path  FC5_data_mnt00001_1 -size 1t -ostype linux  -class
regular
lun create -path FC5_data_mnt00001_2 -size 1t -ostype linux  -class
regular
lun create -path FC5_log_mnt00001_1 -size 260g -ostype linux  -class
regular
lun create -path FC5_log_mnt00001_2 -size 260g -ostype linux  -class
regular
lun create -path FC5_shared -size 260g -ostype linux  -class regular
```

2. システム FC5 に属するすべてのサーバのイニシエータグループを作成します。

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb -vserver svm1
```

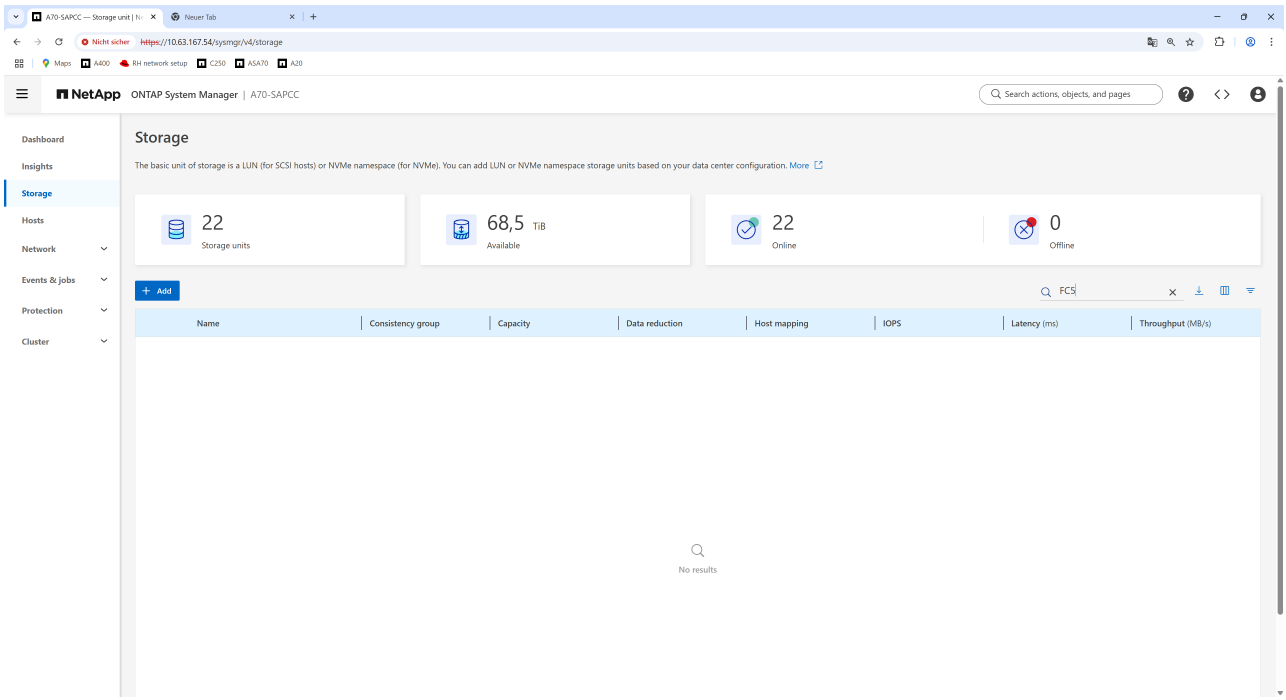
3. 作成したイニシエータグループにすべての LUN をマッピングします。

```
lun map -path FC5_data_mnt00001_1 -igroup HANA-FC5
lun map -path FC5_data_mnt00001_2 -igroup HANA-FC5
lun map -path FC5_log_mnt00001_1 -igroup HANA-FC5
lun map -path FC5_log_mnt00001_2 -igroup HANA-FC5
lun map -path FC5_shared -igroup HANA-FC5
```

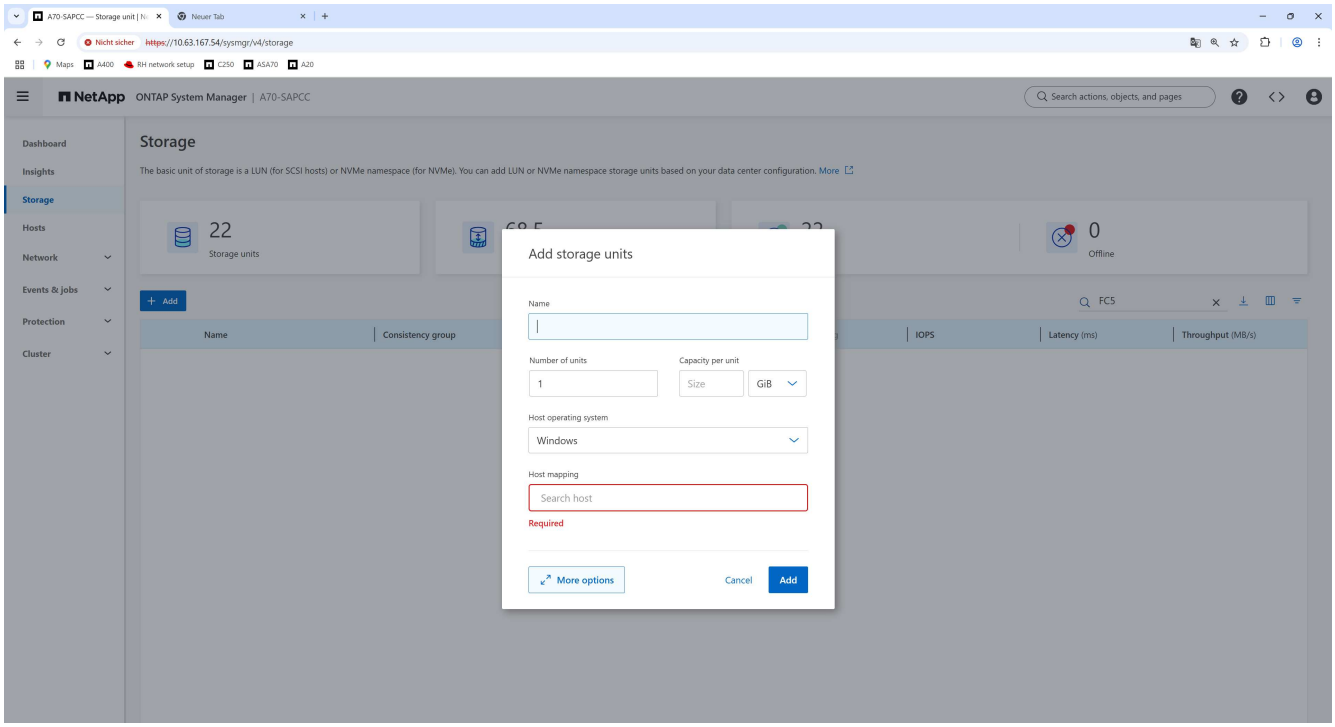
### GUIを使用してLUNを作成し、LUNをイニシエータグループにマッピングする

このセクションでは、 `ONTAP System Manager` LVM を使用し、LVM ボリューム グループごとに 2 つの LUN を持つ SID FC5 の SAP HANA 単一ホスト システムの場合:

1. ログオン `ONTAP System Manager`ONTAPクラスタを選択し、 `Storage`左のメニューから。
   a. プレス `Add`




2. 選ぶ `More options`




3. 必要な情報を入力してください:
   a. データLUNの名前、例：`FC5_data_mnt00001`
   b. LVMと組み合わせるLUNの数、例：2

c. 各LUNのサイズ（例：1000 GB）

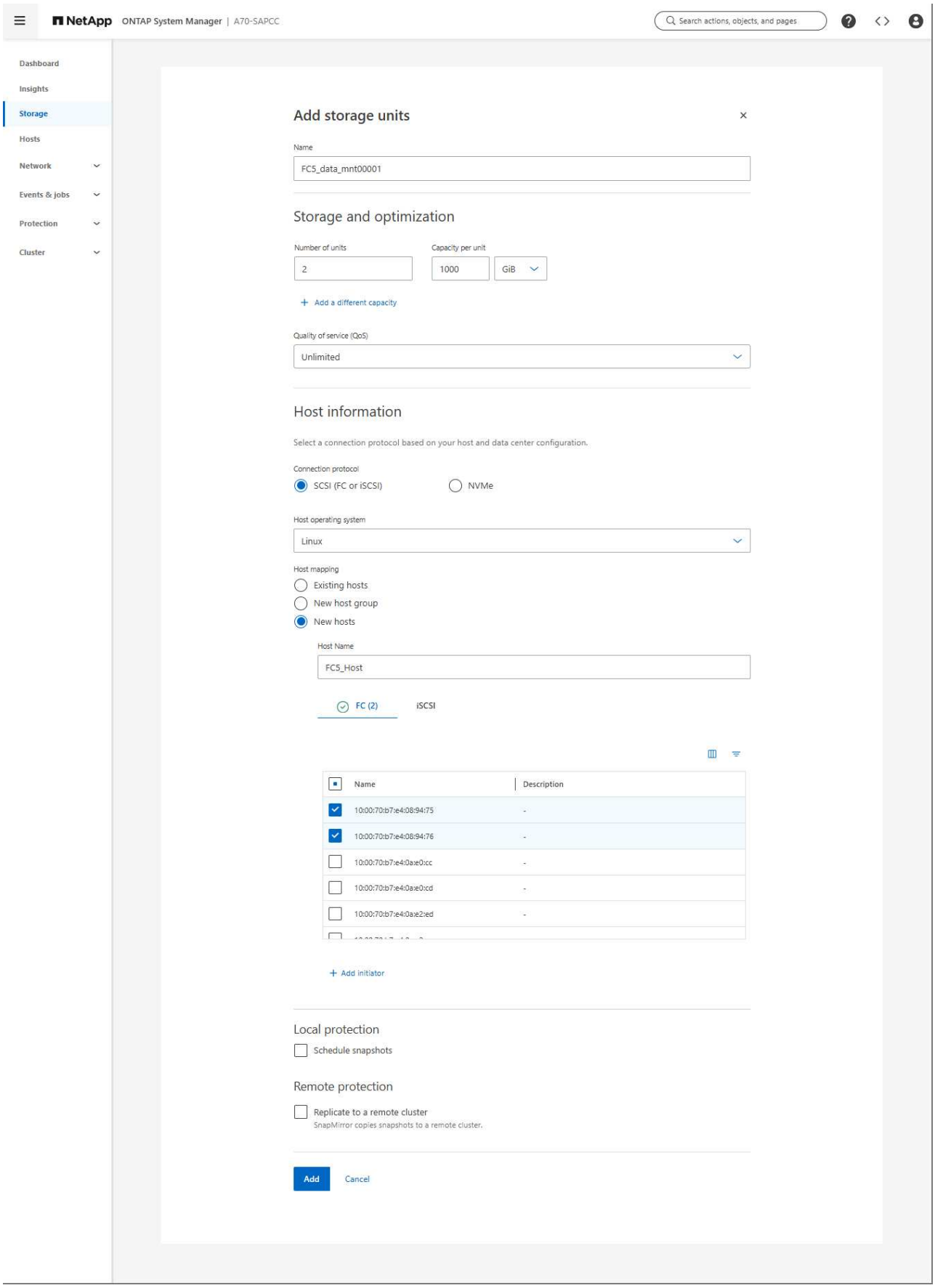
d. 選ぶ `SCSI (FC or iSCSI)`

e. 選ぶ `Linux`として `Host Operating system`

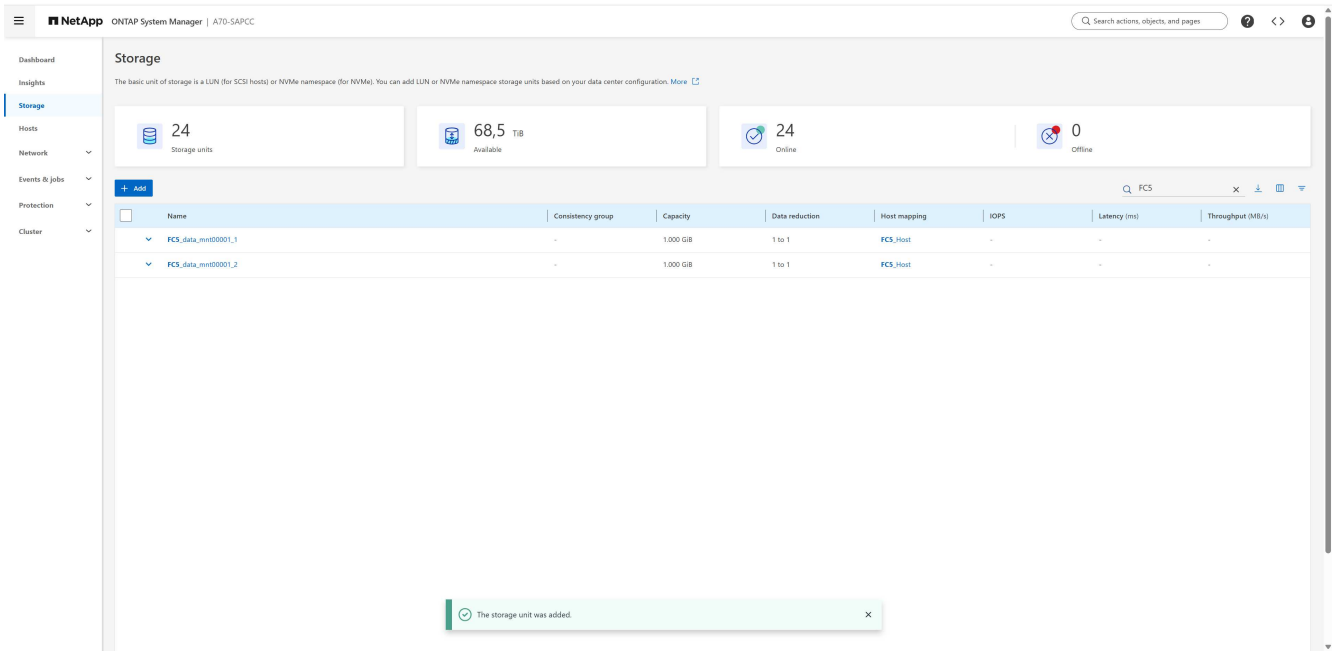
f. 選ぶ `New host`のために `Host mapping`オプションで名前を指定します。例: `FC5_host`希望するイニシエーターを選択または追加します

g. 保つ `Schedule snapshots`チェックなし

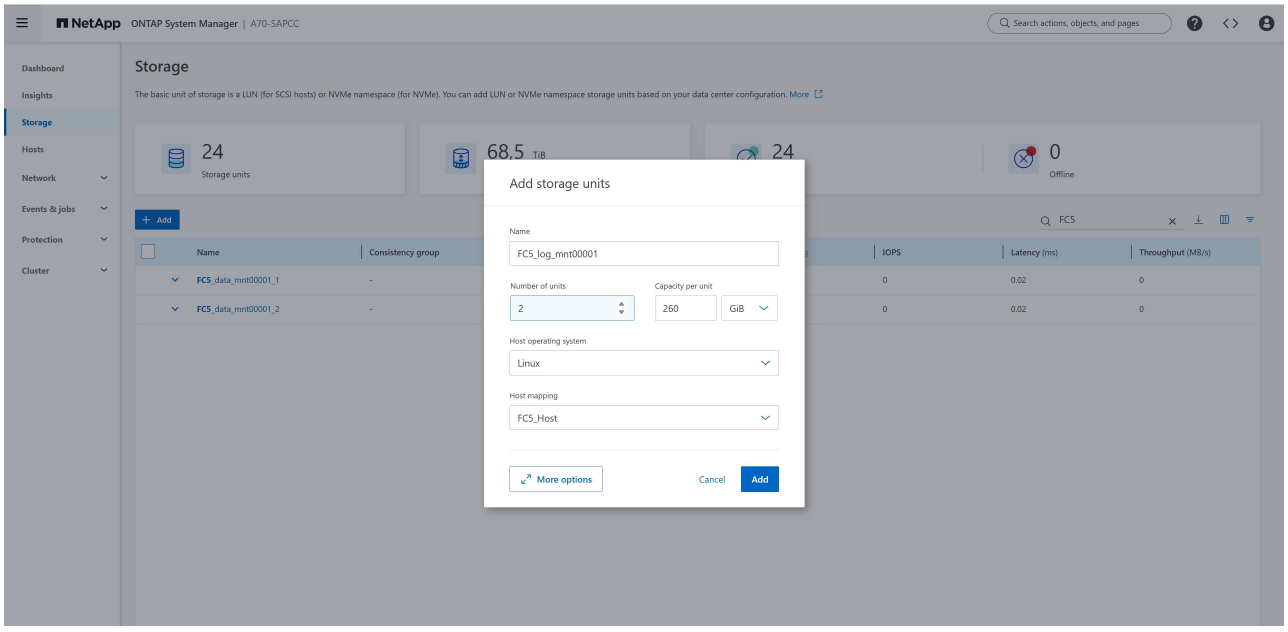
h. プレス `Add`



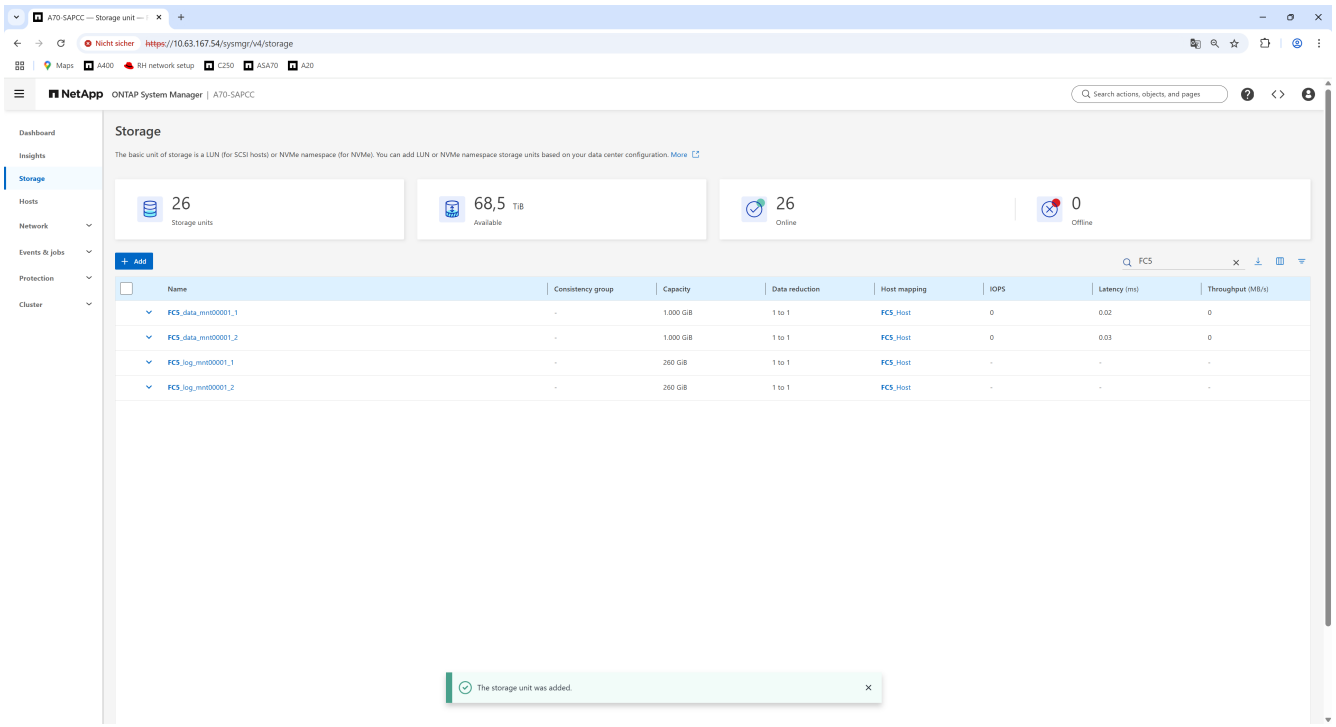

4. データLUNの作成に成功したら、ログLUNを作成します。 `Add`



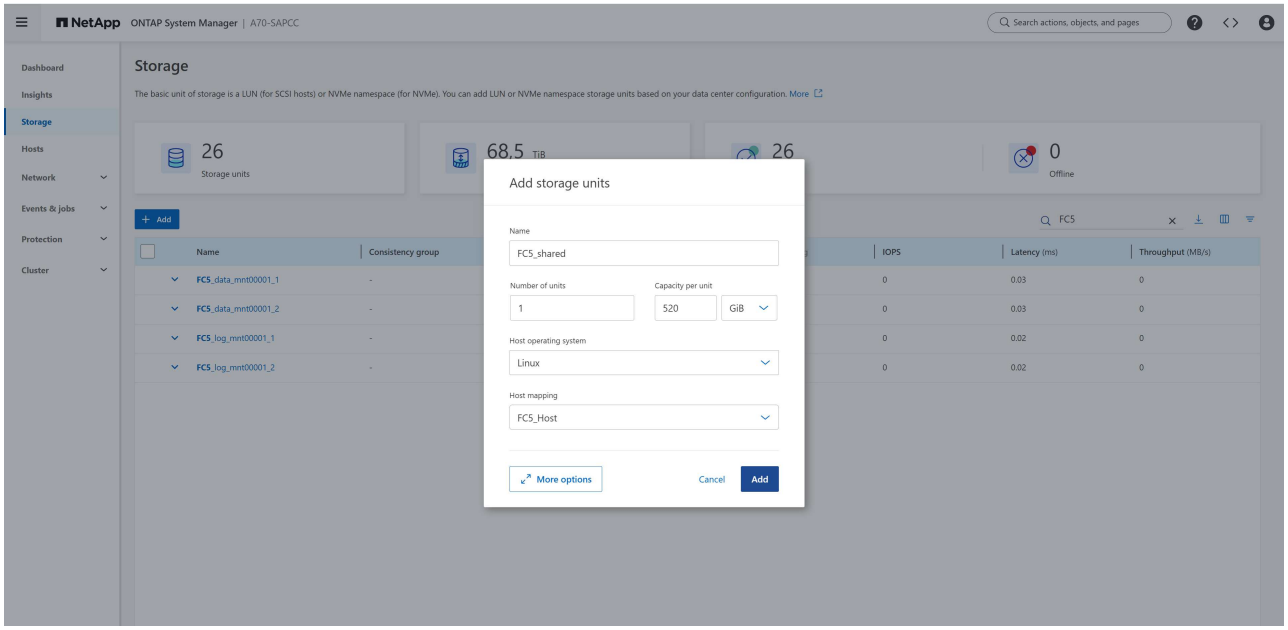

5. 必要な情報を入力してください:
   a. ログLUNの名前、例： `FC5_log_mnt00001`
   b. LVMと組み合わせるLUNの数、例：2
   c. 各LUNのサイズ（例：260 GB）
   d. 選ぶ `Linux`として `Host Operating system`
   e. 以前に作成したマッピングを選択する `FC5_host`のために `Host mapping`オプション
   f. プレス `Add`



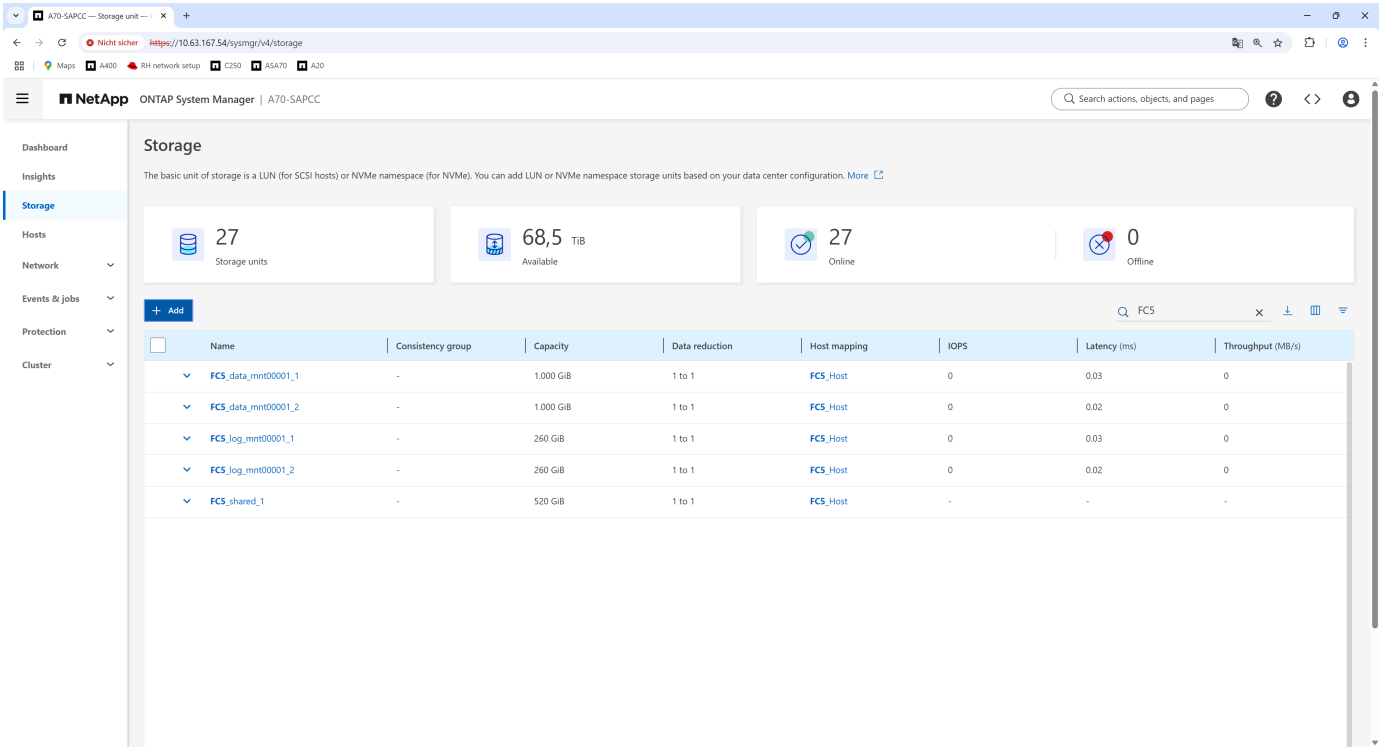

6. ログLUNの作成に成功したら、を押して共有LUNを作成します。 `Add`




7. 必要な情報を入力してください:
   a. 共有LUNの名前、例：.`FC5_shared`
   b. LUNの数、例：1
   c. LUNのサイズ（例：520 GB）
   d. 選ぶ `Linux`として `Host Operating system`
   e. 以前に作成したマッピングを選択する `FC5_host`のために `Host mapping`オプション
   f. プレス `Add`




SAP HANA 単一ホスト システムに必要なすべての LUN が作成されました。




複数のホスト

複数のホスト

このセクションでは、SAP HANAマルチホストシステムに固有のNetAppストレージシステムの構成について説明します。

### LUN の作成とイニシエーター グループへの LUN のマッピング

NetApp ONTAP System Manager を使用してストレージ ボリュームと LUN を作成し、それらをサーバーの igroup とONTAP CLI にマップできます。

### CLI を使用して LUN を作成し、LUN をイニシエータ グループにマッピングする

このセクションでは、コマンドラインを使用した ONTAP 9 と、 SID FC5 を使用した 2+1 の SAP HANA マルチホストシステムで、 LVM ボリュームグループごとに 2 つの LUN を使用した構成例を示します。

1. すべての LUN を作成します。

```
lun create -path FC5_data_mnt00001_1 -size 1t -ostype linux  -class
regular
lun create -path FC5_data_mnt00001_2 -size 1t -ostype linux  -class
regular
lun create -path FC5_data_mnt00002_1 -size 1t -ostype linux  -class
regular
lun create -path FC5_data_mnt00002_2 -size 1t -ostype linux  -class
regular
lun create -path FC5_log_mnt00001_1 -size 260g -ostype linux  -class
regular
lun create -path FC5_log_mnt00001_2 -size 260g -ostype linux  -class
regular
lun create -path FC5_log_mnt00002_1 -size 260g -ostype linux  -class
regular
lun create -path FC5_log_mnt00002_2 -size 260g -ostype linux  -class
regular
```

2. システム FC5 に属するすべてのサーバのイニシエータグループを作成します。

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator
10000090fadcc5fa,10000090fadcc5fb,10000090fadcc5c1,10000090fadcc5c2,1000
0090fadcc5c3,10000090fadcc5c4 -vserver svm1
```

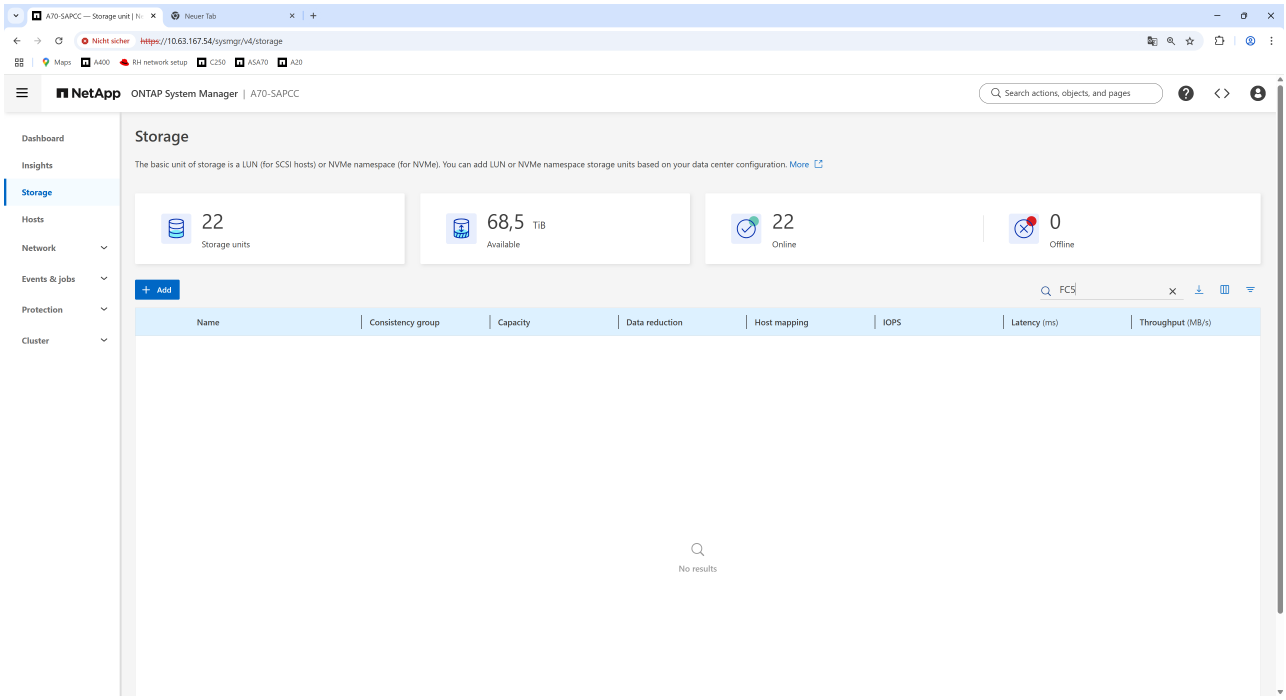
3. 作成したイニシエータグループにすべての LUN をマッピングします。

```
lun map -path FC5_data_mnt00001_1 -igroup HANA-FC5
lun map -path FC5_data_mnt00001_2 -igroup HANA-FC5
lun map -path FC5_data_mnt00002_1 -igroup HANA-FC5
lun map -path FC5_data_mnt00002_2 -igroup HANA-FC5
lun map -path FC5_log_mnt00001_1 -igroup HANA-FC5
lun map -path FC5_log_mnt00001_2 -igroup HANA-FC5
lun map -path FC5_log_mnt00002_1 -igroup HANA-FC5
lun map -path FC5_log_mnt00002_2 -igroup HANA-FC5
```

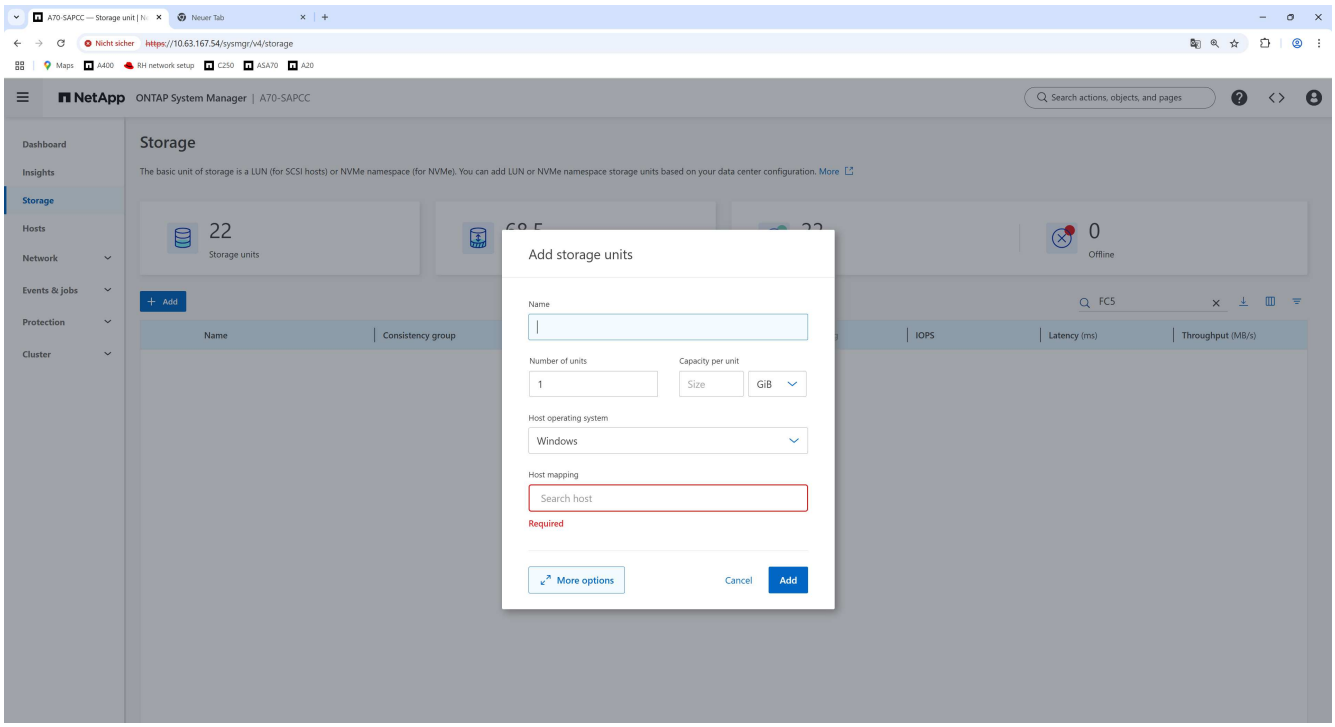
**GUI**を使用して**LUN**を作成し、**LUN**をイニシエータグループにマッピングする

このセクションでは、 `ONTAP System Manager` LVM を使用し、LVM ボリューム グループごとに 2 つの LUN を持つ SID FC5 の 2+1 SAP HANA マルチホスト システムの場合:

1. ログオン `ONTAP System Manager`ONTAPクラスタを選択し、 `Storage`左のメニューから。
   a. プレス `Add`




2. 選ぶ `More options`

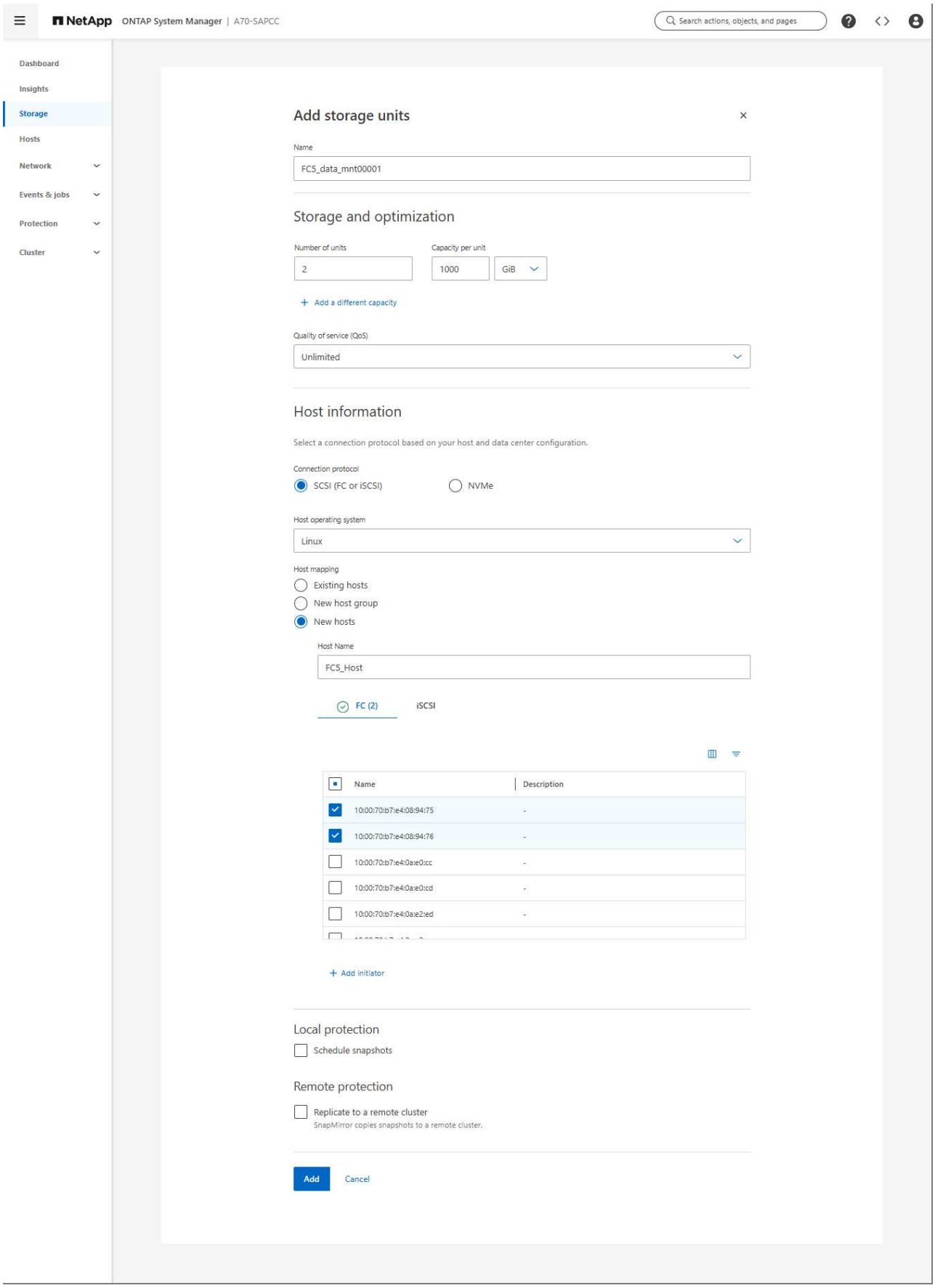



3. 必要な情報を入力してください:
   a. データLUNの名前、例：`.FC5_data_mnt00001`
   b. LVMと組み合わせるLUNの数、例：2
   c. 各LUNのサイズ（例：1000 GB）
   d. 選ぶ `SCSI (FC or iSCSI)`
   e. 選ぶ `Linux`として `Host Operating system`

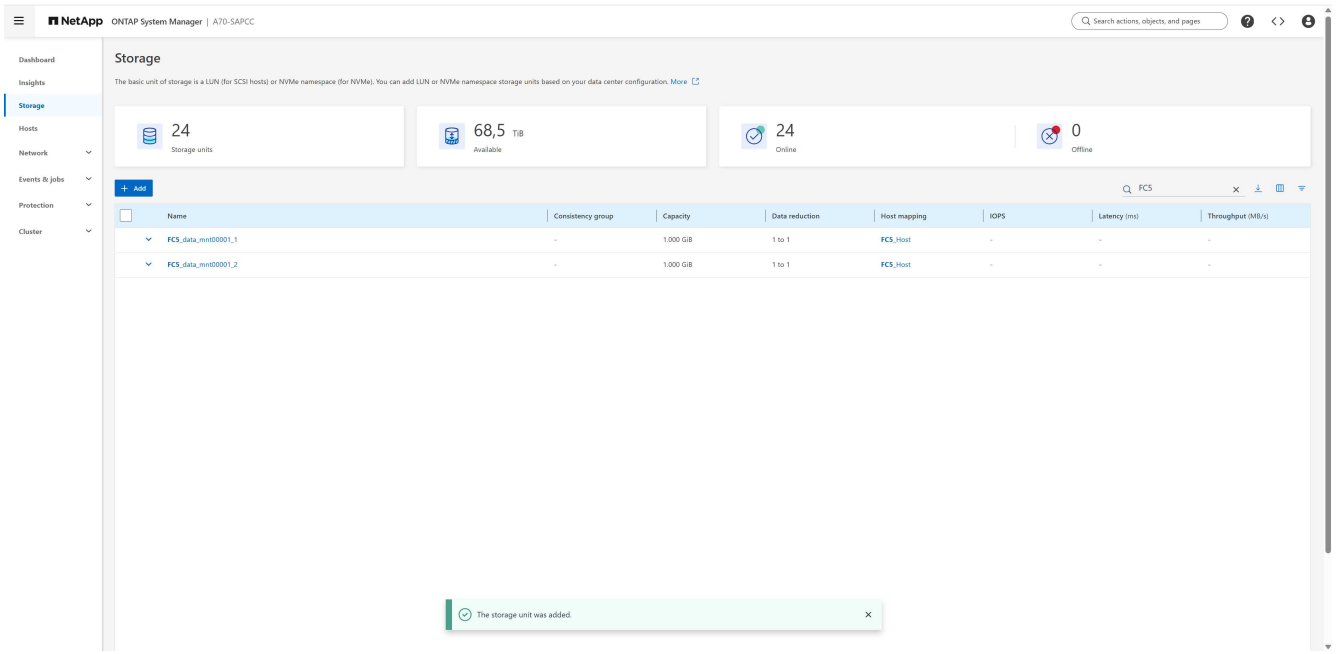
f. 選ぶ `New host`のために `Host mapping`オプションで名前を指定します。例: `FC5_host`希望するイニシエーターを選択または追加します

g. 保つ `Schedule snapshots`チェックなし

h. プレス `Add`




4. 次のワーカーホストのデータLUNを作成するには、 `Add`




5. 必要な情報を入力してください:

   a. 追加のデータLUNの名前、例： `FC5_data_mnt00002`

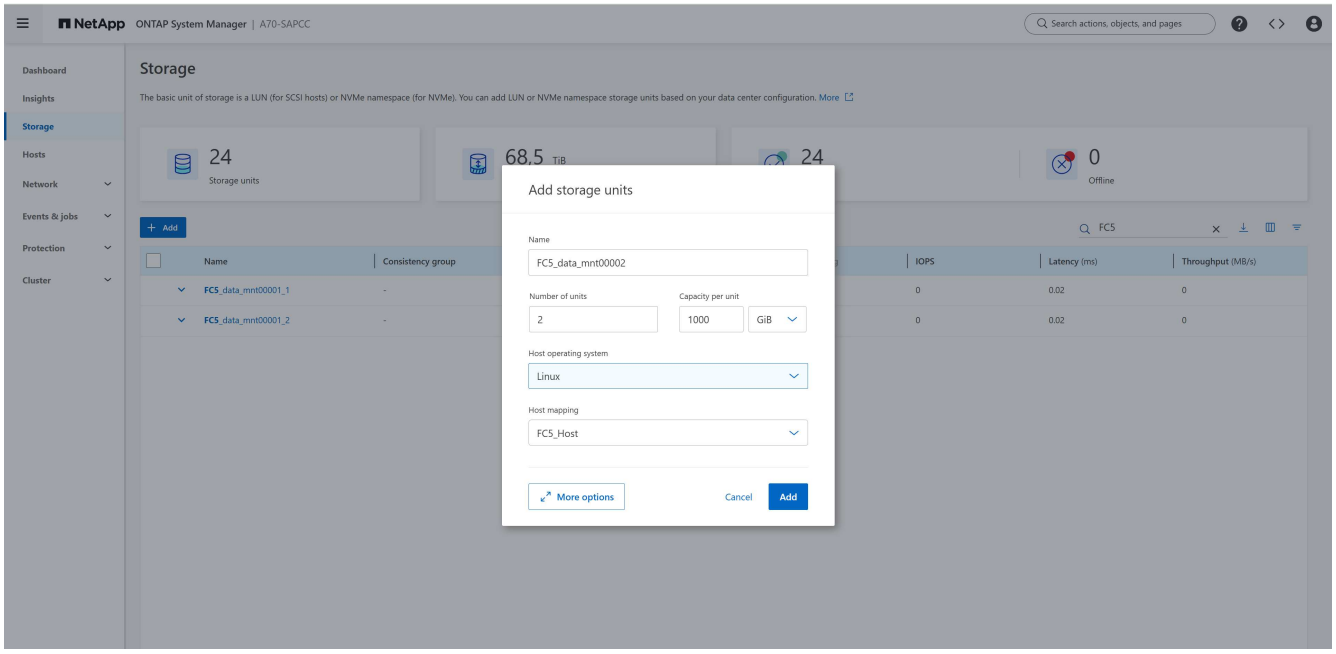
   b. LVMと組み合わせるLUNの数、例：2

   c. 各LUNのサイズ（例：1000 GB）

   d. 選ぶ `Linux`として `Host Operating system`

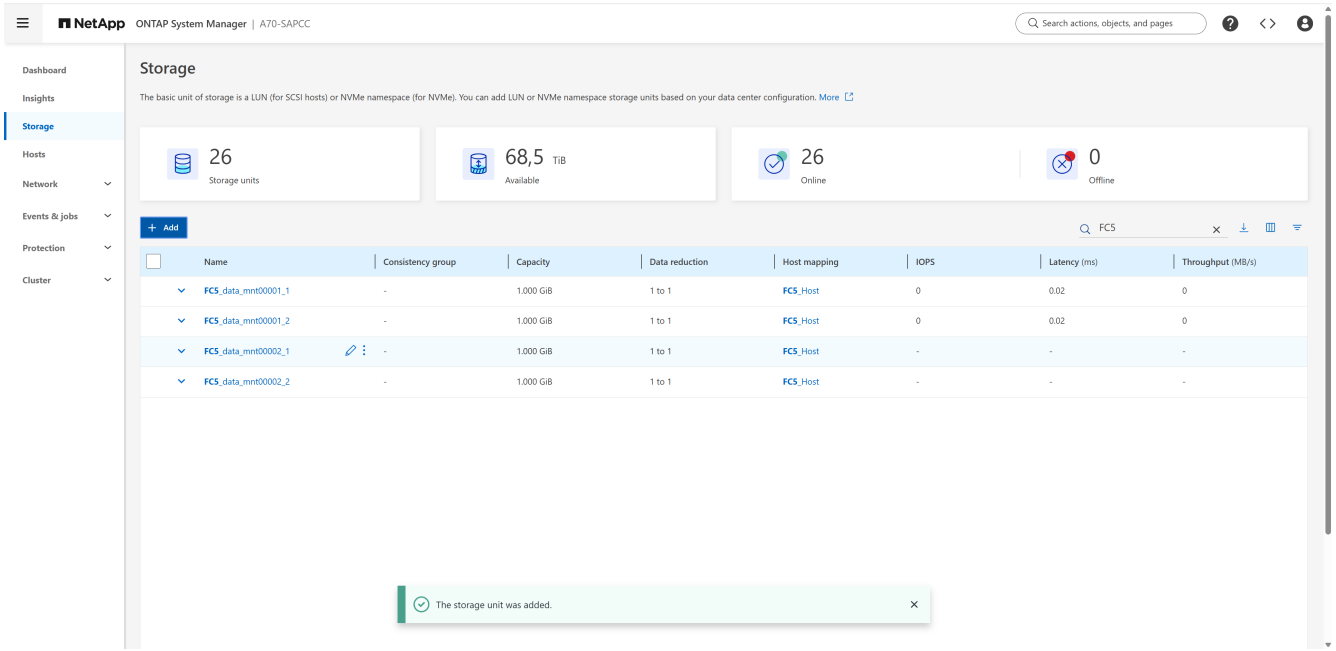
   e. 以前に作成したマッピングを選択する `FC5_host`のために `Host mapping`オプション

   f. プレス `Add`

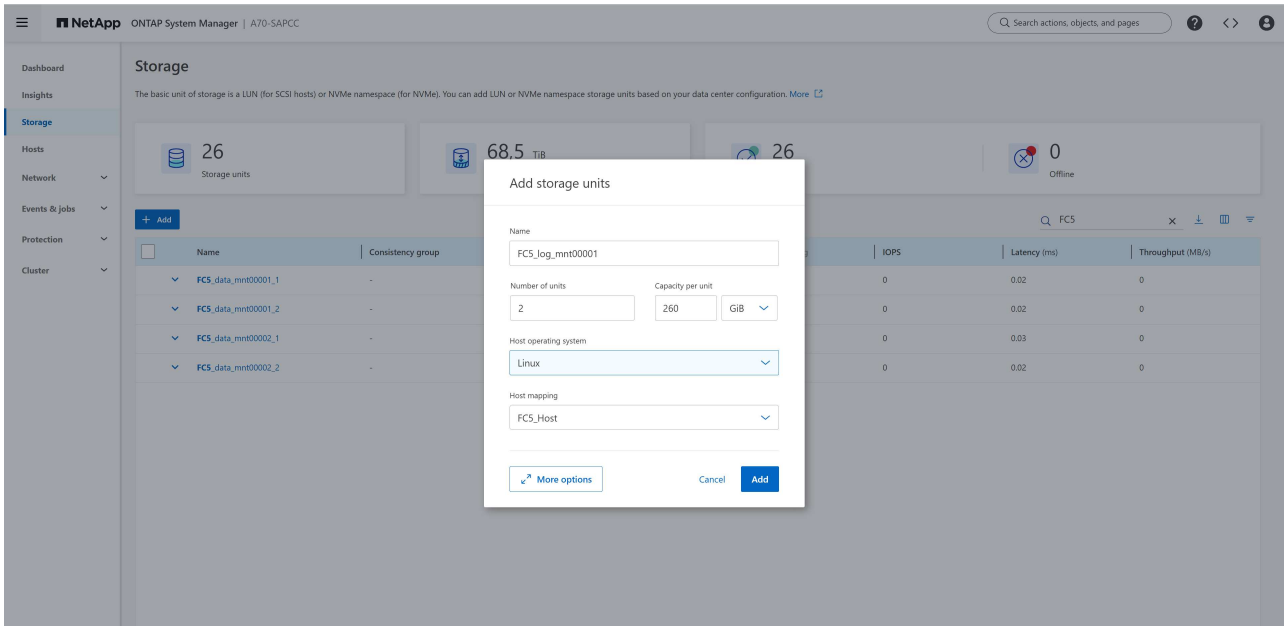



6. 追加のワーカーホストごとに手順4と5を繰り返します。

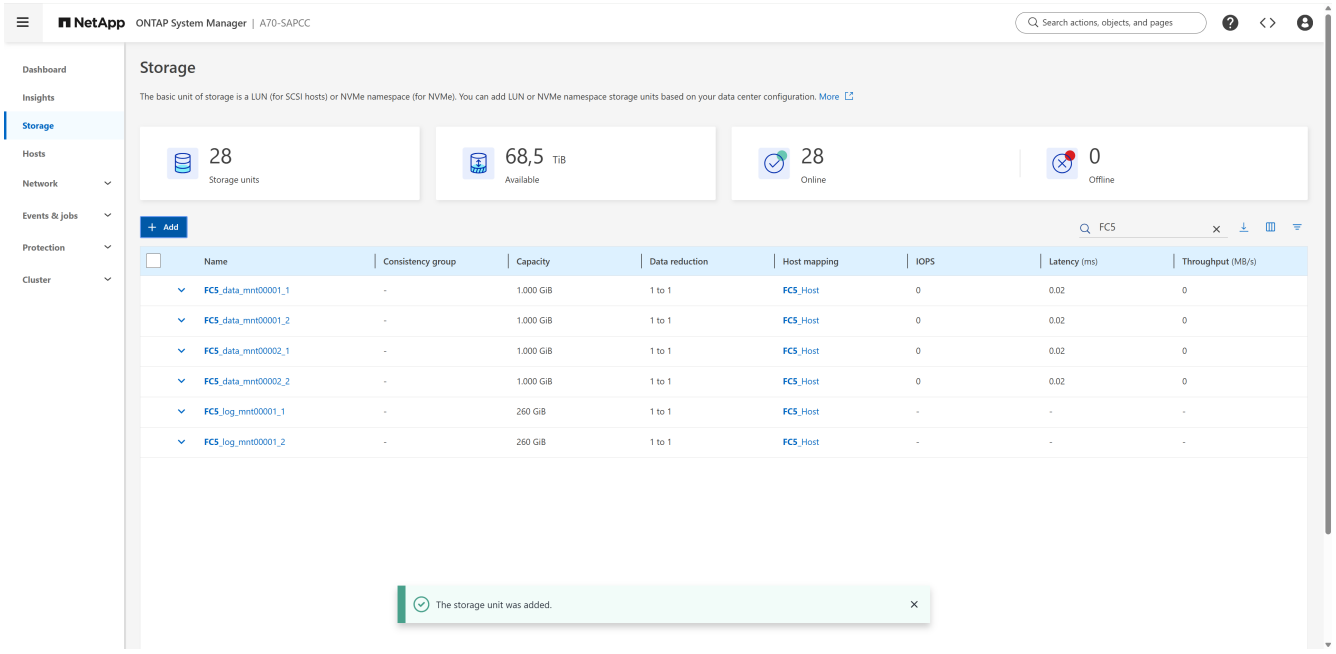
7. データLUNの作成に成功したら、ログLUNを作成します。 `Add`



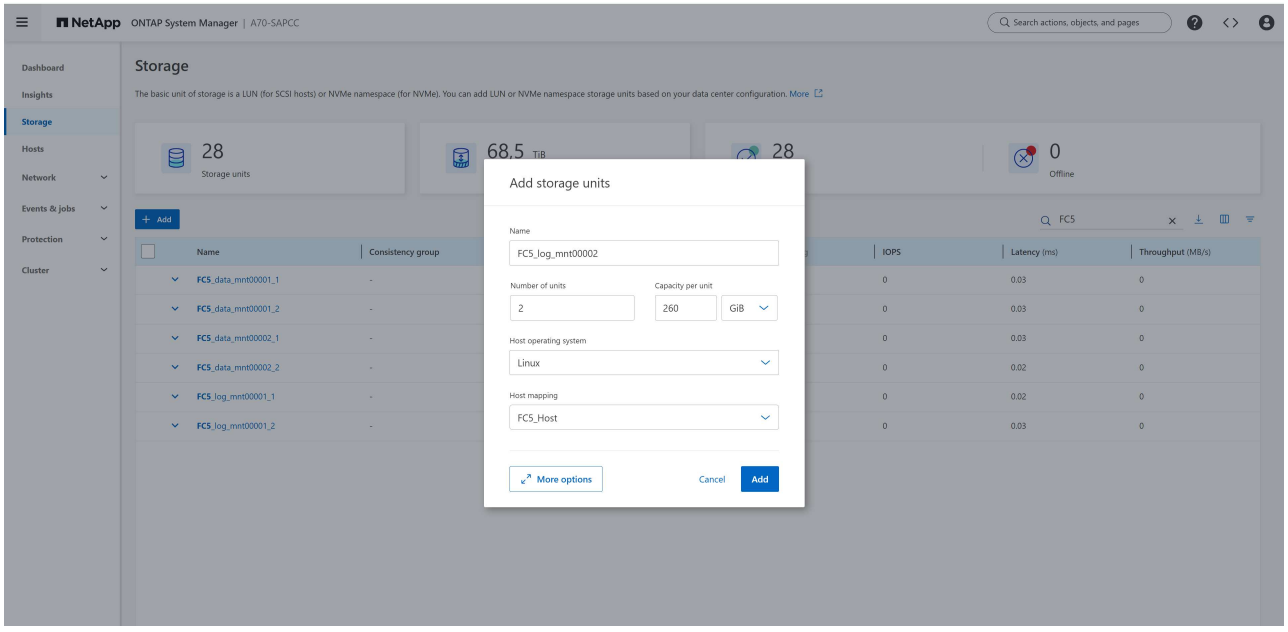

8. 必要な情報を入力してください:
   a. LVMと組み合わせるログLUNの名前、例： `FC5_log_mnt00001`
   b. LVMと組み合わせるLUNの数、例：2
   c. 各LUNのサイズ（例：260 GB）
   d. 選ぶ `Linux`として `Host Operating system`
   e. 以前に作成したマッピングを選択する `FC5_host`のために `Host mapping`オプション
   f. プレス `Add`




9. 次のワーカーホストのログLUNを作成するには、 `Add`

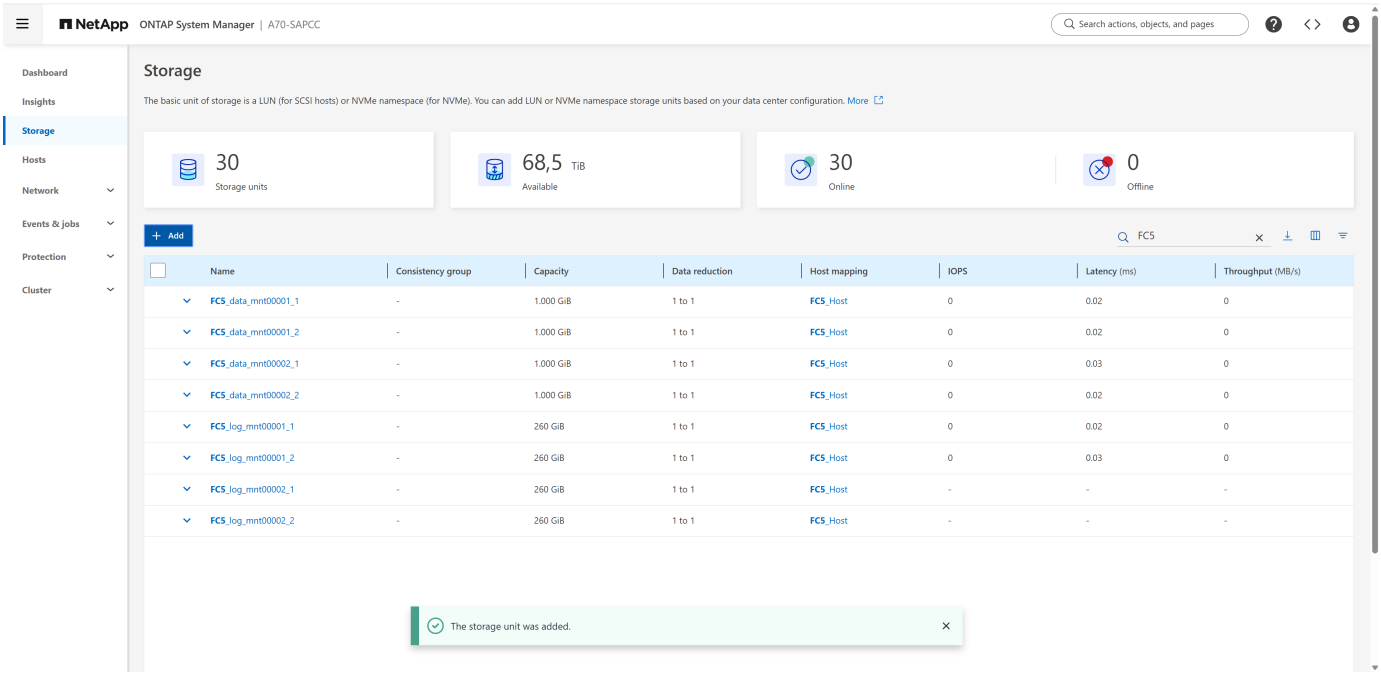



10. 必要な情報を入力してください:
    a. 追加のログLUNの名前、例： `FC5_log_mnt00002`
    b. LVMと組み合わせるLUNの数、例：2
    c. 各LUNのサイズ（例：260 GB）
    d. 選ぶ `Linux`として `Host Operating system`
    e. 以前に作成したマッピングを選択する `FC5_host`のために `Host mapping`オプション
    f. プレス `Add`




11. 追加のワーカーホストごとに手順9と10を繰り返します。

SAP HANA マルチホスト システムに必要なすべての LUN が作成されました。




## SAP HANA Storage Connector API

ストレージコネクタは、フェイルオーバー機能を備えたマルチホスト環境でのみ必要です。マルチホスト構成では、 SAP HANA に高可用性機能が提供されるため、 SAP HANA データベースホストはスタンバイホストにフェイルオーバーできます。

この場合、障害が発生したホストの LUN には、スタンバイホストからアクセスして使用されます。ストレージコネクタは、一度に 1 つのデータベースホストだけがストレージパーティションにアクティブにアクセスできるようにするために使用されます。

ネットアップストレージを使用した SAP HANA マルチホスト構成では、 SAP が提供する標準のストレージコネクタが使用されます。『 SAP HANA Fibre Channel Storage Connector Admin Guide 』は、への添付ファイルとして提供されています "SAP ノート 1900823"。

### ホストのセットアップ

ホストをセットアップする前に、 NetApp SAN Host Utilities をからダウンロードしておく必要があります "ネットアップサポート" HANA サーバにインストールします。ホスト・ユーティリティのマニュアルには、使用する FCP HBA に応じてインストールする必要がある追加ソフトウェアの情報が記載されています。

また、使用している Linux バージョンに固有のマルチパス構成に関する情報も記載されています。このドキュメントでは、 SLES 12 SP1 以降および RHEL 7 で必要な設定手順について説明します。2 以降。を参照してください "『 Linux Host Utilities 7.1 Installation and Setup Guide 』"。

### マルチパスを設定します

SAP HANA マルチホスト構成のすべてのワーカーホストとスタンバイホストで、手順 1~6 を実行する必要があります。

マルチパスを設定するには、次の手順を実行します。

1. 各サーバで Linux の「 re scan-scsi-bus.sh -a' 」コマンドを実行して、新しい LUN を検出します。
2. 実行 `sanlun lun show`コマンドを実行し、必要なLUNがすべて表示されていることを確認します。次の例は、 `sanlun lun show` 2つのデータLUNと2つのログLUNを持つ2+1マルチホストHANAシステムのコマンド出力。出力には、LUNと対応するデバイスファイル（LUNなど）が表示されます。 `FC5_data_mnt00001`デバイスファイル `/dev/sdag`各 LUN には、ホストからストレージ コントローラへの FC パスが 8 つあります。

```
sapcc-hana-tst:~ # sanlun lun show
controller(7mode/E-Series)/                                    device
host                  lun
vserver(cDOT/FlashRay)        lun-pathname                     filename
adapter    protocol   size    product
------------------------------------------------------------------------------
---------------------------------------
svm1                          FC5_log_mnt00002_2               /dev/sdbb
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002_1               /dev/sdba
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001_2               /dev/sdaz
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001_1               /dev/sday
host21     FCP        500g    cDOT
svm1                          FC5_data_mnt00002_2              /dev/sdax
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002_1              /dev/sdaw
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001_2              /dev/sdav
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001_1              /dev/sdau
host21     FCP        1t      cDOT
svm1                          FC5_log_mnt00002_2               /dev/sdat
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002_1               /dev/sdas
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001_2               /dev/sdar
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001_1               /dev/sdaq
host21     FCP        500g    cDOT
svm1                          FC5_data_mnt00002_2              /dev/sdap
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002_1              /dev/sdao
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001_2              /dev/sdan
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001_1              /dev/sdam
host21     FCP        1t      cDOT
```

```
svm1                            FC5_log_mnt00002_2              /dev/sdal
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00002_1              /dev/sdak
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001_2              /dev/sdaj
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001_1              /dev/sdai
host20     FCP         500g     cDOT
svm1                            FC5_data_mnt00002_2             /dev/sdah
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00002_1             /dev/sdag
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001_2             /dev/sdaf
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001_1             /dev/sdae
host20     FCP         1t       cDOT
svm1                            FC5_log_mnt00002_2              /dev/sdad
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00002_1              /dev/sdac
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001_2              /dev/sdab
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001_1              /dev/sdaa
host20     FCP         500g     cDOT
svm1                            FC5_data_mnt00002_2             /dev/sdz
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00002_1             /dev/sdy
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001_2             /dev/sdx
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001_1             /dev/sdw
host20     FCP         1t       cDOT
```

3. 実行 `multipath -r`そして `multipath -ll`デバイス ファイル名のワールドワイド識別子 (WWID) を取得するコマンド。

この例では、8 つの LUN があります。

```
sapcc-hana-tst:~ # multipath -r
sapcc-hana-tst:~ # multipath -ll
3600a098038314e63492b59326b4b786d dm-7 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
```

```
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
3600a098038314e63492b59326b4b786e dm-9 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
3600a098038314e63492b59326b4b786f dm-11 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
3600a098038314e63492b59326b4b7870 dm-13 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
3600a098038314e63532459326d495a64 dm-6 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
3600a098038314e63532459326d495a65 dm-8 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
3600a098038314e63532459326d495a66 dm-10 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
```

```
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
3600a098038314e63532459326d495a67 dm-12 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

4. /etc/multipath.conf ファイルを編集し 'WWID とエイリアス名を追加します



出力例は '2+1 マルチホスト・システムの 4 つの LUN のエイリアス名を含む /etc/multipath.conf ファイルの内容を示しています使用可能な multipath.conf ファイルがない場合、「 multipath-T 」 /etc/multipath.conf を実行して作成できます。

```
sapcc-hana-tst:/ # cat /etc/multipath.conf
multipaths {
                multipath {
                wwid    3600a098038314e63492b59326b4b786d
                alias   svm1-FC5_data_mnt00001_2
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786e
                alias   svm1-FC5_data_mnt00002_2
        }
        multipath {
                wwid    3600a098038314e63532459326d495a64
                alias   svm1-FC5_data_mnt00001_1
        }
        multipath {
                wwid    3600a098038314e63532459326d495a65
                alias   svm1-FC5_data_mnt00002_1
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786f
                alias   svm1-FC5_log_mnt00001_2
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b7870
                alias   svm1-FC5_log_mnt00002_2
        }
        multipath {
                wwid    3600a098038314e63532459326d495a66
                alias   svm1-FC5_log_mnt00001_1
        }
        multipath {
                wwid    3600a098038314e63532459326d495a67
                alias   svm1-FC5_log_mnt00002_1
        }


}
```

5. 「 multipath -r 」コマンドを実行して、デバイスマップをリロードします。
6. すべての LUN 、エイリアス名、およびアクティブパスとスタンバイパスを一覧表示するには、「マルチパス -ll 」コマンドを実行して構成を確認します。

次の出力例は、 2 つのデータ LUN と 2 つのログ LUN を持つ 2+1 マルチホスト HANA システムの出力を示しています。

```
sapcc-hana-tst:~ # multipath -ll
svm1-FC5_data_mnt00001_2 (3600a098038314e63492b59326b4b786d) dm-7
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
svm1-FC5_data_mnt00002_2 (3600a098038314e63492b59326b4b786e) dm-9
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
svm1-FC5_data_mnt00001_1 (3600a098038314e63532459326d495a64) dm-6
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
svm1-FC5_data_mnt00002_1 (3600a098038314e63532459326d495a65) dm-8
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
svm1-FC5_log_mnt00001_2 (3600a098038314e63492b59326b4b786f) dm-11
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
```

```
svm1-FC5_log_mnt00002_2 (3600a098038314e63492b59326b4b7870) dm-13
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
svm1-FC5_log_mnt00001_1 (3600a098038314e63532459326d495a66) dm-10
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
svm1-FC5_log_mnt00002_1 (3600a098038314e63532459326d495a67) dm-12
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

単一ホスト設定

単一ホスト設定

# この章では、SAP HANA 単一ホストのセットアップについて説明します。

### SAP HANA 単一ホストシステムの LUN 構成

Linux LVM は、パフォーマンスを向上し、LUN サイズの制限に対処するために使用されています。次の表に示すように、 SAP HANA ホストで、ボリュームグループと論理ボリュームを作成してマウントする必要があります。

| 論理ボリューム / LUN | SAP HANA<br>ホストのマウントポイント | 注 |
|---|---|---|
| lv ： FC5_data_mnt00001 -vol | /hana/data FC5/mnt00001 のように指定します | /etc/fstab エントリを使用してマウントされます |
| lv ： FC5_log_mnt00001 -vol | /hana/log/FC5/mnt00001 | /etc/fstab エントリを使用してマウントされます |

| 論理ボリューム / **LUN** | **SAP HANA**<br>ホストのマウントポイント | 注 |
| --- | --- | --- |
| LUN：FC5_shared | /hana/shareed/FC5 | /etc/fstab エントリを使用してマウントされます |

説明した構成では、 `/usr/sap/FC5`ユーザFC5admのデフォルトのホームディレクトリが格納されているディレクトリは、ローカルディスク上にあります。ディスクベースのレプリケーションによる災害復旧設定では、NetAppは、 `/usr/sap/FC5`すべてのファイルシステムが中央ストレージ上に存在するようにディレクトリを作成します。

**LVM** ボリュームグループと論理ボリュームを作成

1. すべての LUN を物理ボリュームとして初期化します。

```
pvcreate /dev/mapper/svm1-FC5_data_mnt00001_1
pvcreate /dev/mapper/svm1-FC5_data_mnt00001_2
pvcreate /dev/mapper/svm1-FC5_log_mnt00001_1
pvcreate /dev/mapper/svm1-FC5_log_mnt00001_2
```

2. 各データパーティションとログパーティションのボリュームグループを作成します。

```
vgcreate FC5_data_mnt00001 /dev/mapper/svm1-FC5_data_mnt00001_1
/dev/mapper/svm1-FC5_data_mnt00001_2
vgcreate FC5_log_mnt00001 /dev/mapper/svm1-FC5_log_mnt00001_1
/dev/mapper/svm1-FC5_log_mnt00001_2
```

3. データパーティションとログパーティションごとに論理ボリュームを作成します。ボリュームグループごとに使用されている LUN の数（この例では 2 つ）と同じストライプサイズを使用し、データの場合は 256K 、ログの場合は 64k を使用します。SAP では、ボリュームグループごとに 1 つの論理ボリュームのみがサポートされます。

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. その他すべてのホストで、物理ボリューム、ボリュームグループ、およびボリュームグループをスキャンします。

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

これらのコマンドでボリュームが見つからない場合は、再起動する必要があります。

論理ボリュームをマウントするには、論理ボリュームをアクティブ化する必要があります。ボリュームをアクティブ化するには、次のコマンドを実行します。

```
vgchange -a y
```

ファイルシステムの作成

すべてのデータおよびログ論理ボリュームと hana 共有 LUN に XFS ファイル システムを作成します。

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs /dev/mapper/svm1-FC5_shared
```

複数ホストのコマンド例には、 2+1 のマルチホスト HANA システムが示されています。

マウントポイントを作成する

必要なマウント ポイント ディレクトリを作成し、データベース ホストの権限を設定します。

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod –R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod –R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

ファイルシステムをマウント

システム起動中にファイルシステムをマウントするには、 `/etc/fstab`設定ファイルに必要なファイルシステムを追加し、 `/etc/fstab`設定ファイル:

```
# cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/FC5_log_mnt00001-vol /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/FC5_data_mnt00001-vol /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
```

データ LUN とログ LUN の XFS ファイルシステムは 'relatim' および inode64' マウントオプションを使用してマウントする必要があります

ファイルシステムをマウントするには、 `mount –a`ホストでコマンドを実行します。

# 複数ホストの設定

この章では、2+1 SAP HANA マルチホストシステムのセットアップを例として説明します。

## SAP HANA マルチホストシステムの LUN 構成

Linux LVM は、パフォーマンスを向上し、LUN サイズの制限に対処するために使用されています。

次の表に示すように、 SAP HANA ホストで、ボリュームグループと論理ボリュームを作成してマウントする必要があります。

| 論理ボリューム（LV） | SAP HANA<br>ホストのマウントポイント | 注 |
|---|---|---|
| lv ： FC5_data_mnt00001 -vol | /hana/data FC5/mnt00001 のように指定します | ストレージコネクタを使用してマウント |
| lv ： FC5_log_mnt00001 -vol | /hana/log/FC5/mnt00001 | ストレージコネクタを使用してマウント |
| lv ： FC5_data_mnt00002 -vol | /hana/data FC5/mnt00002 のように指定します | ストレージコネクタを使用してマウント |
| lv ： FC5_log_mnt00002 -vol | /hana/log/FC5/mnt00002 | ストレージコネクタを使用してマウント |
| 外部NFS共有: FC5_shared | /hana/shared にアクセスします | NFS と /etc/fstab のエントリを使用して、すべてのホストにマウントされます |

SAP HANAマルチホストシステムでは、 `/hana/shared`システムのすべてのホストに接続されたファイルシステム。通常、これはNFSサーバーによって提供されるNFS共有です。NetAppFASやAFFシステムなどの高可用性NFSサーバーの使用をお勧めします。また、Linuxホストに内蔵されているNFSサーバーを使用することもできます。

説明した構成では、 `/usr/sap/FC5`ユーザーFC5admのデフォルトのホームディレクトリが格納されているディレクトリは、各HANAホストのローカルディスク上にあります。ディスクベースのレプリケーションによる災害復旧設定では、NetAppは4つの追加LUNを使用することを推奨しています。 `/usr/sap/FC5`各ホストにファイルシステムを配置して、各データベース ホストのすべてのファイルシステムが中央ストレージ上に存在するようにします。

## LVM ボリュームグループと論理ボリュームを作成

1. すべての LUN を物理ボリュームとして初期化します。

```
pvcreate /dev/mapper/svm1-FC5_data_mnt00001_1
pvcreate /dev/mapper/svm1-FC5_data_mnt00001_2
pvcreate /dev/mapper/svm1-FC5_data_mnt00002_1
pvcreate /dev/mapper/svm1-FC5_data_mnt00002_2
pvcreate /dev/mapper/svm1-FC5_log_mnt00001_1
pvcreate /dev/mapper/svm1-FC5_log_mnt00001_2
pvcreate /dev/mapper/svm1-FC5_log_mnt00002_1
pvcreate /dev/mapper/svm1-FC5_log_mnt00002_2
```

2. 各データパーティションとログパーティションのボリュームグループを作成します。

```
vgcreate FC5_data_mnt00001 /dev/mapper/svm1-FC5_data_mnt00001_1
/dev/mapper/svm1-FC5_data_mnt00001_2
vgcreate FC5_data_mnt00002 /dev/mapper/svm1-FC5_data_mnt00002_1
/dev/mapper/svm1-FC5_data_mnt00002_2
vgcreate FC5_log_mnt00001 /dev/mapper/svm1-FC5_log_mnt00001_1
/dev/mapper/svm1-FC5_log_mnt00001_2
vgcreate FC5_log_mnt00002 /dev/mapper/svm1-FC5_log_mnt00002_1
/dev/mapper/svm1-FC5_log_mnt00002_2
```

3. データパーティションとログパーティションごとに論理ボリュームを作成します。ボリュームグループごとに使用されている LUN の数（この例では 2 つ）と同じストライプサイズを使用し、データの場合は 256K 、ログの場合は 64k を使用します。SAP では、ボリュームグループごとに 1 つの論理ボリュームのみがサポートされます。

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. その他すべてのホストで、物理ボリューム、ボリュームグループ、およびボリュームグループをスキャンします。

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

これらのコマンドでボリュームが見つからない場合は、再起動する必要があります。

論理ボリュームをマウントするには、論理ボリュームをアクティブ化する必要があります。ボリュームをアクティブ化するには、次のコマンドを実行します。

```
vgchange -a y
```

ファイルシステムの作成

すべてのデータおよびログ論理ボリュームに XFS ファイル システムを作成します。

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_data_mnt00002-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs FC5_log_mnt00002-vol
```

マウントポイントを作成する

必要なマウント ポイント ディレクトリを作成し、すべてのワーカー ホストとスタンバイ ホストの権限を設定します。

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod -R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod -R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

ファイルシステムをマウント

マウントするには `/hana/shared`システム起動時にファイルシステムを使用する `/etc/fstab`設定ファイルに、`/hana/shared`ファイルシステムに `/etc/fstab`各ホストの構成ファイル。

```
sapcc-hana-tst:/ # cat /etc/fstab
<storage-ip>:/hana_shared /hana/shared nfs rw,vers=3,hard,timeo=600,
intr,noatime,nolock 0 0
```

すべてのデータファイルシステムとログファイルシステムは、 SAP HANA ストレージコネクタを使用してマウントされます。

ファイルシステムをマウントするには、各ホストで「 mount – a 」コマンドを実行します。

**SAP HANA** の **I/O** スタック構成

#### SAP HANA の I/O スタック構成

SAP HANA 1.0 SPS10 以降、 I/O 動作を調整し、使用中のファイルシステムとストレージシステムのデータベースを最適化するためのパラメータが導入されています。

ネットアップは、最適な値を定義するため、パフォーマンステストを実施しました。次の表に、パフォーマンステストから推定した最適な値を示します。

| パラメータ | 価値 |
| --- | --- |
| max_parallel _io_requests と入力します | 128 |
| async _read_submit | オン |
| async ： write_submit_active | オン |
| async_write_submit_bblocks | すべて |

S12 までの SAP HANA 1.0 では、 SAP ノートに記載されているように、 SAP HANA データベースのインストール時にこれらのパラメータを設定できます "2267798 – Configuration of the SAP HANA Database During Installation Using hdbparam 』で説明されています"。

また、パラメータは、 SAP HANA データベースのインストール後に「 hdbparam 」フレームワークを使用して設定することもできます。

```
FC5adm@sapcc-hana-tst:/usr/sap/FC5/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
FC5adm@sapcc-hana-tst:/usr/sap/FC5/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
FC5adm@sapcc-hana-tst:/usr/sap/FC5/HDB00> hdbparam --paramset
fileio.async_read_submit=on
FC5adm@sapcc-hana-tst:/usr/sap/FC5/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

SAP HANA 2.0 以降 'hdbparam' は廃止され ' パラメータは global.ini` ファイルに移動されますパラメータは、 SQL コマンドまたは SAP HANA Studio を使用して設定できます。詳細については、 SAP ノートを参照してください "2399079 ： HANA で hdbparam の除去 2"。パラメータは 'global.ini` ファイル内で設定することもできます

```
FC5adm@sapcc-hana-tst: /usr/sap/FC5/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

SAP HANA 2.0 SPS5 以降では、「 setParameter.py 」スクリプトを使用して正しいパラメータを設定します。

```
fc5adm@sapcc-hana-tst-03:/usr/sap/FC5/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

**SAP HANA** ソフトウェアのインストール

## このセクションでは、シングルホストシステムとマルチホストシステムに SAP HANA をインストールするために必要な準備について説明します。

### シングルホストシステムへのインストール

SAP HANA ソフトウェアのインストールでは、シングルホストシステムについて行う追加の準備作業はありません。

### マルチホストシステムへのインストール

インストールを開始する前に 'global.ini` ファイルを作成して 'SAP ストレージ・コネクタの使用を有効にしますSAP ストレージコネクタは、インストールプロセス中にワーカーホストで必要なファイルシステムをマウントします。global.ini` ファイルは '/hana/shared ファイル・システムなど ' すべてのホストからアクセス可能なファイル・システムで使用できる必要があります

マルチホストシステムに SAP HANA ソフトウェアをインストールする前に、次の手順を実行する必要があります。

1. データ LUN およびログ LUN の次のマウント・オプションを global.ini` ファイルに追加します
   - 「データとログファイルシステム」の「 relatime 」と「 inode64 」です
2. データパーティションとログパーティションの WWID を追加します。WWID は '/etc/multipath.conf' ファイルに設定されているエイリアス名と一致している必要があります

   次の例は、 SID が FC5 の 2+1 マルチホストセットアップを示しています。

```
sapcc-hana-tst-03:/hana/shared # cat global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/FC5
basepath_logvolumes = /hana/log/FC5
[storage]
ha_provider = hdb_ha.fcClientLVM
partition_*_*__prtype = 5
partition_*_data__mountOptions = -o relatime,inode64
partition_*_log__mountOptions = -o relatime,inode64
partition_1_data__lvmname = FC5_data_mnt00001-vol
partition_1_log__lvmname = FC5_log_mnt00001-vol
partition_2_data__lvmname = FC5_data_mnt00002-vol
partition_2_log__lvmname = FC5_log_mnt00002-vol
sapcc-hana-tst-03:/hana/shared #
```

SAP hdblcm インストール ツールを使用して、ワーカー ホストの 1 つで次のコマンドを実行してインストールを開始します。オプションを使用し `addhosts`て、2番目のワーカー（sapc-hana-tst-06）とスタンバイホスト（sapc-hana-tst-07）を追加します。

+

準備したファイルが格納されているディレクトリ `global.ini`は( --storage_cfg=/hana/shared`、CLIオプションに含まれてい `storage_cfg`ます）。

+

使用する OS のバージョンによっては、 SAP HANA データベースをインストールする前に Python 2.7 をインストールする必要があります。

+

```
./hdblcm --action=install --addhosts=sapcc-hana-tst
-06:role=worker:storage_partition=2,sapcc-hana-tst-07:role=standby
--storage_cfg=/hana/shared/

AP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
```

```
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1 (1.015.0)
in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
```

```
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip


SAP HANA Database version '2.00.073.00.1695288802' will be installed.

Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------------
------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version 2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
  9     | epmmds          | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
4.203.2321.0.0

Enter comma-separated list of the selected indices [3,4]: 2,3
```

1. 選択したすべてのコンポーネントが、すべてのワーカーホストとスタンバイホストにインストールされていることを確認します。

## 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。

- "SAP HANA ソフトウェアソリューション"
- "TR-4646 ：『 SAP HANA Disaster Recovery with Storage Replication 』"
- "SnapCenter、SnapMirror Active Sync、VMware Metro Storage ClusterによるSAP HANAのデータ保護と高可用性"

- "TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"
- "TR-4667：『Automating SAP HANA System Copy and Clone Operations with SnapCenter 』"
- ネットアップドキュメントセンター

  "https://www.netapp.com/support-and-training/documentation/"

- SAP HANA 向け SAP 認定エンタープライズストレージハードウェア

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"

- SAP HANA のストレージ要件

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"

- 『 SAP HANA Tailored Data Center Integration Frequently Asked Questions 』

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"

- SAP HANA on VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"

- 『SAP HANA on VMware vSphere Best Practices Guide』

  "https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

## 履歴を更新します

この解決策の初版以降には、次の技術的な変更が加えられています。

| 日付 | 概要を更新します |
| --- | --- |
| 2025年7月 | 初期バージョン |

# 『 SAP HANA on NetApp FAS Systems with NFS Configuration Guide 』

## 『SAP HANA on NetApp FAS systems with NFS Configuration Guide』

NetApp FAS 製品ファミリーは、 TDI プロジェクトの SAP HANA との使用が認定されています。このガイドでは、NFS を使用したこのプラットフォーム上の SAP HANA のベスト プラクティスについて説明します。

Marco Schoen 、ネットアップ

この認定は現在、次のモデルでのみ有効です。

- FAS2750、FAS2820、FAS8300、FAS50、FAS8700、FAS70、FAS9500、FAS90 SAP HANA向けのNetApp認定ストレージソリューションの一覧については、を参照してください "認定およびサポートさ

れている SAP HANA ハードウェアディレクトリ"。

本ドキュメントでは、 NFS バージョン 3 （ NFSv3 ）プロトコルまたは NFS バージョン 4 （ NFSv4.1 ）プロトコルの ONTAP 設定要件について説明します。

NFSバージョン3または4.1のみがサポートされます。NFSバージョン1、2、4.0、4.2はサポートされていません。

このホワイトペーパーで説明している構成は、 SAP HANA に必要な SAP HANA KPI と、 SAP HANA に最適なパフォーマンスを達成するために必要です。ここに記載されていない設定または機能を変更すると、原因のパフォーマンスが低下したり、予期しない動作が発生したりする可能性があります。変更は、ネットアップのサポートから指示された場合にのみ実施

FCP を使用する NetApp FAS システム、および NFS または FC を使用する AFF システムの構成ガイドは、次のリンクから入手できます。

- "FCP を使用した NetApp FAS システムでの SAP HANA"
- "NFS を使用した NetApp AFF システムでの SAP HANA"
- "FCP 搭載の NetApp AFF システム上の SAP HANA"
- "FCP 搭載の NetApp ASA システム上の SAP HANA"

次の表に、 SAP HANA データベースの構成に応じた、 NFS バージョン、 NFS ロック、および必要な分離実装についてサポートされる組み合わせを示します。

SAP HANA シングルホストシステム、またはホストの自動フェイルオーバーを使用しない複数のホストでは、 NFSv3 と NFSv4 がサポートされます。

ホストの自動フェイルオーバーを有効にした SAP HANA マルチホストシステムでは、サーバ固有の STONITH （ SAP HANA HA/DR プロバイダ）実装の代わりに NFSv4 ロックを使用した場合に、ネットアップは NFSv4 のみをサポートします。

| **SAP HANA** のサポート | **NFS** バージョン | **NFS** ロック | **SAP HANA** の **HA/DR** プロバイダ |
|---|---|---|---|
| SAP HANA シングルホスト、ホストの自動フェイルオーバーを使用しない複数のホスト | NFSv3 | オフ | 該当なし |
| | NFSv4 | オン | 該当なし |
| ホストの自動フェイルオーバーを使用する SAP HANA マルチホスト | NFSv3 | オフ | サーバ固有の STONITH の実装は必須です |
| | NFSv4 | オン | 必要ありません |

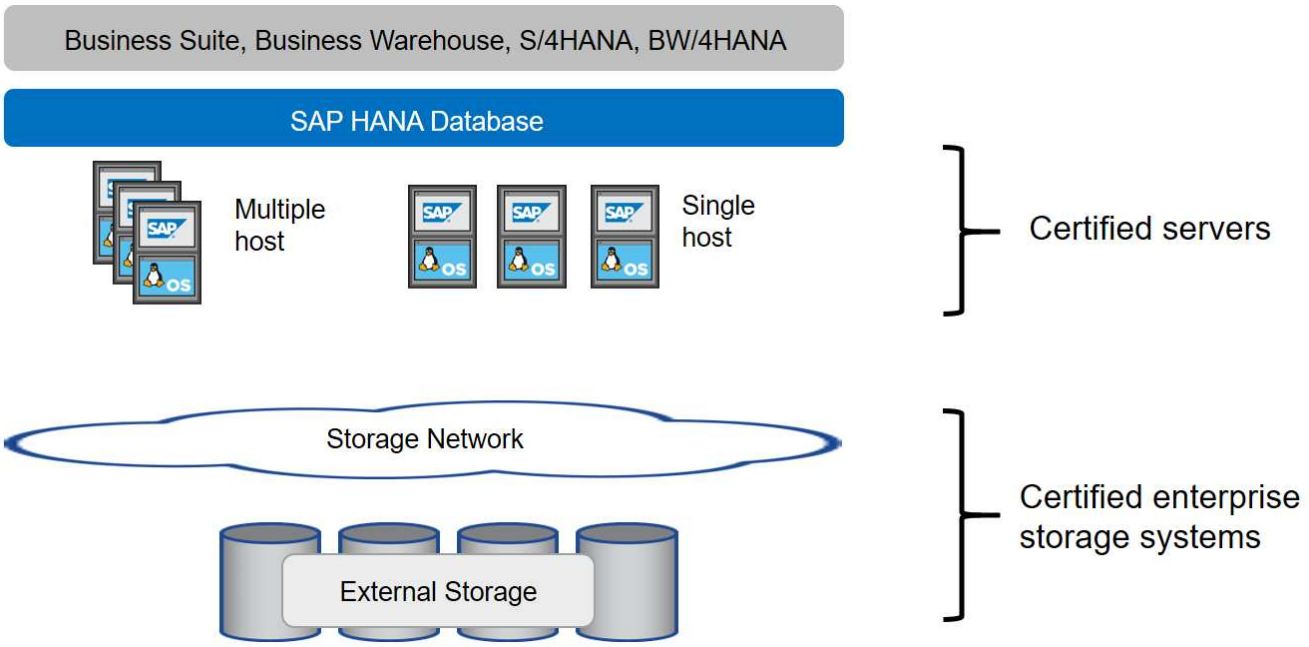
サーバ固有の STONITH 実装については、このガイドでは説明していません。そのような実装については、サーバのベンダーにお問い合わせください。

このドキュメントでは、物理サーバ上および VMware vSphere を使用する仮想サーバ上で実行される SAP HANA の構成に関する推奨事項について説明します。

オペレーティングシステムの構成ガイドラインと、 HANA 固有の Linux カーネルの依存関係については、必ず該当する SAP ノートを参照してください。詳細については、を参照してください "SAP ノート 2235581 ：『 SAP HANA Supported Operating Systems 』"。

**SAP HANA** テーラードデータセンター統合

NetApp FAS ストレージコントローラは、 NFS （ NAS ）プロトコルと FC （ SAN ）プロトコルの両方を使用した SAP HANA TDI プログラムで認定されています。これらは、シングルホスト構成とマルチホスト構成のどちらでも、 SAP Business Suite on HANA 、 S/4HANA 、 BW/4HANA 、 SAP Business Warehouse on HANA など、最新の SAP HANA シナリオに導入できます。SAP HANA との使用が認定されているサーバは、ネットアップ認定のストレージソリューションと組み合わせることができます。アーキテクチャの概要については、次の図を参照してください。




本番用SAP HANAシステムの前提条件と推奨事項の詳細については、次のSAPリソースを参照してください。

- "『 SAP HANA Tailored Data Center Integration Frequently Asked Questions 』"

**VMware vSphere** を使用した **SAP HANA**

ストレージを仮想マシン（ VM ）に接続する方法はいくつかあります。推奨される方法は、ストレージボリュームと NFS をゲストオペレーティングシステムから直接接続することです。このオプションを使用しても、ホストやストレージの構成が物理ホストや VM で同じになることはありません。

NFS データストアまたは NFS を使用する VVol データストアもサポートされます。どちらの場合も、本番環境で使用するデータストアに格納する必要があるのは、 1 つの SAP HANA データボリュームまたはログボリュームだけです。

このドキュメントでは、ゲスト OS から NFS への直接マウントを使用する場合の推奨セットアップについて説明します。

SAP HANA での vSphere の使用の詳細については、次のリンクを参照してください。

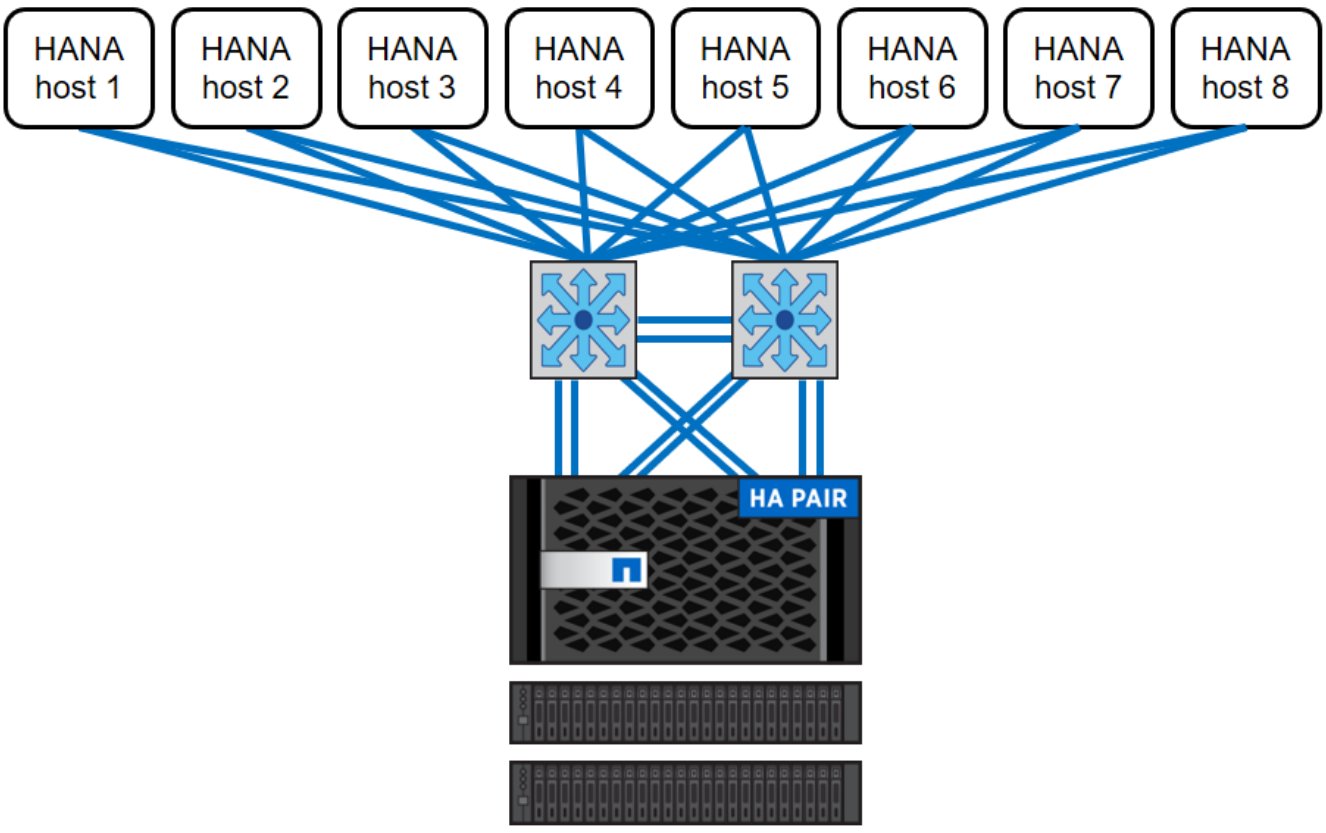
- "SAP HANA on VMware vSphere - 仮想化 - コミュニティ Wiki"
- "『SAP HANA on VMware vSphere Best Practices Guide』"
- "2161991 - VMware vSphere 設定ガイドライン - SAP One Support Launchpad （ログインが必要）"

## アーキテクチャ

SAP HANA ホストは、冗長 10GbE 以上のネットワークインフラを使用して、ストレージコントローラに接続されます。SAP HANA ホストとストレージコントローラ間のデータ通信は、 NFS プロトコルに基づいています。

スイッチまたはネットワークインターフェイスカード（ NIC ）に障害が発生した場合に、耐障害性に優れた SAP HANA ホスト / ストレージ接続を実現するために、冗長スイッチングインフラを推奨します。スイッチは、ポートチャネルを使用して個々のポートのパフォーマンスを集約し、ホストレベルでは単一の論理エンティティとして認識される場合があります。

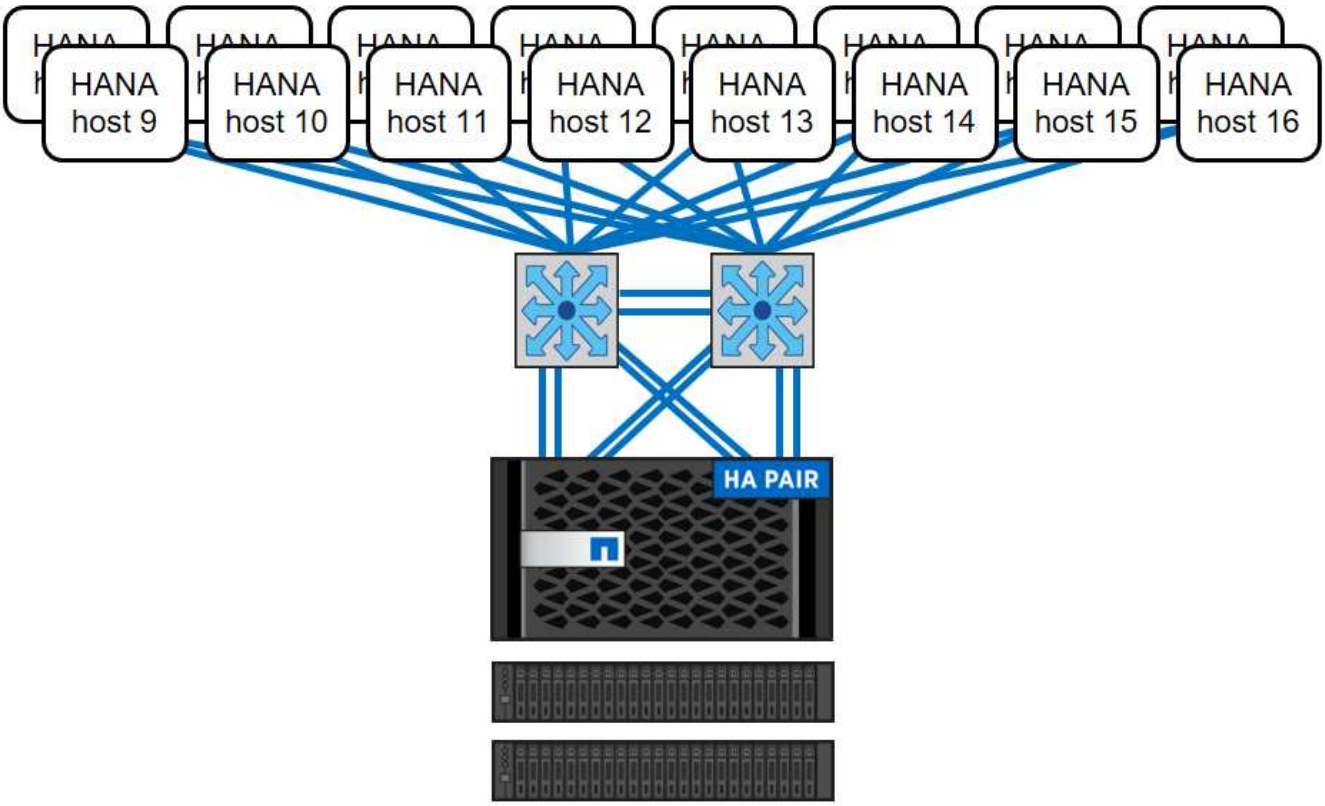
FAS システム製品ファミリーのさまざまなモデルをストレージレイヤで混在させることができるため、拡張が必要になったり、パフォーマンスや容量のニーズが異なる場合があります。ストレージシステムに接続できる SAP HANA ホストの最大数は、 SAP HANA のパフォーマンス要件と、使用されているネットアップコントローラのモデルによって定義されます。必要なディスクシェルフの数は、 SAP HANA システムの容量とパフォーマンスの要件によってのみ決まります。次の図は、 8 台の SAP HANA ホストをストレージハイアベイラビリティ（ HA ）ペアに接続した構成例を示しています。



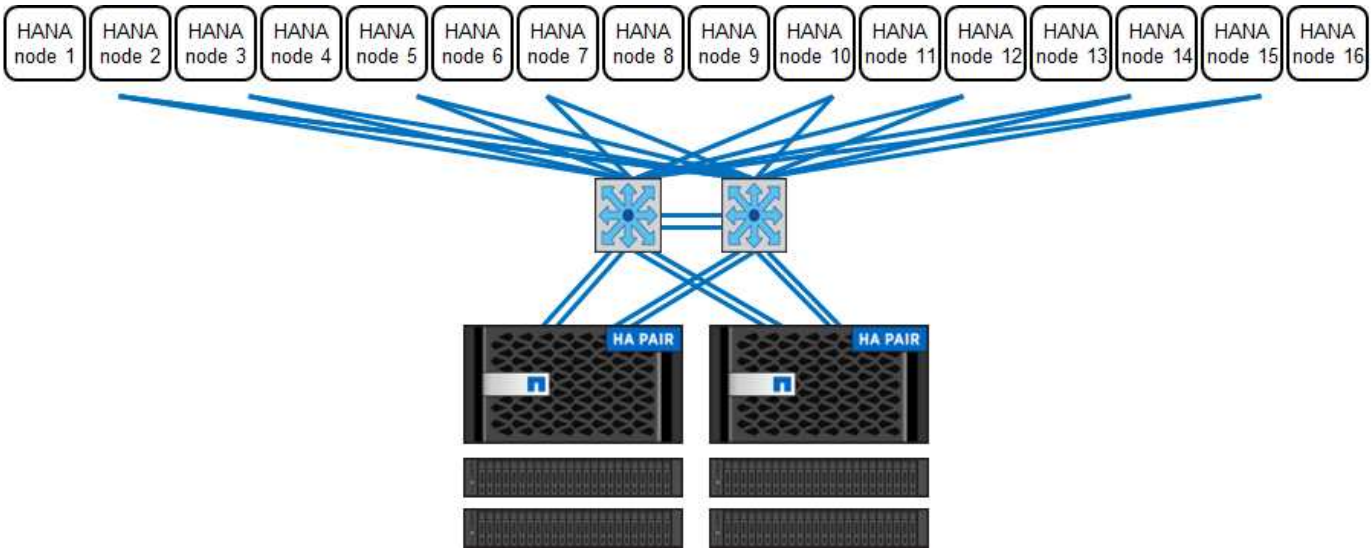

アーキテクチャは、次の 2 つの側面で拡張できます。

- 既存のストレージに SAP HANA ホストやストレージ容量を追加で接続することで、ストレージコントローラが現在の SAP 主要パフォーマンス指標（ KPI ）を満たす十分なパフォーマンスを提供する場合
- 追加の SAP HANA ホスト用にストレージ容量を追加したストレージシステムを追加する

次の図は、追加の SAP HANA ホストをストレージコントローラに接続した場合の構成例を示しています。この例では、 SAP HANA ホスト 16 台分の容量とパフォーマンスの両方の要件を満たすために、さらにディスクシェルフが必要です。合計スループット要件に応じて、ストレージコントローラへの 10GbE （以上）接続を追加する必要があります。




導入した FAS システムとは関係なく、任意の認定済みストレージコントローラを追加して、希望するノード密度に合わせて SAP HANA 環境を拡張することもできます（次の図を参照）。



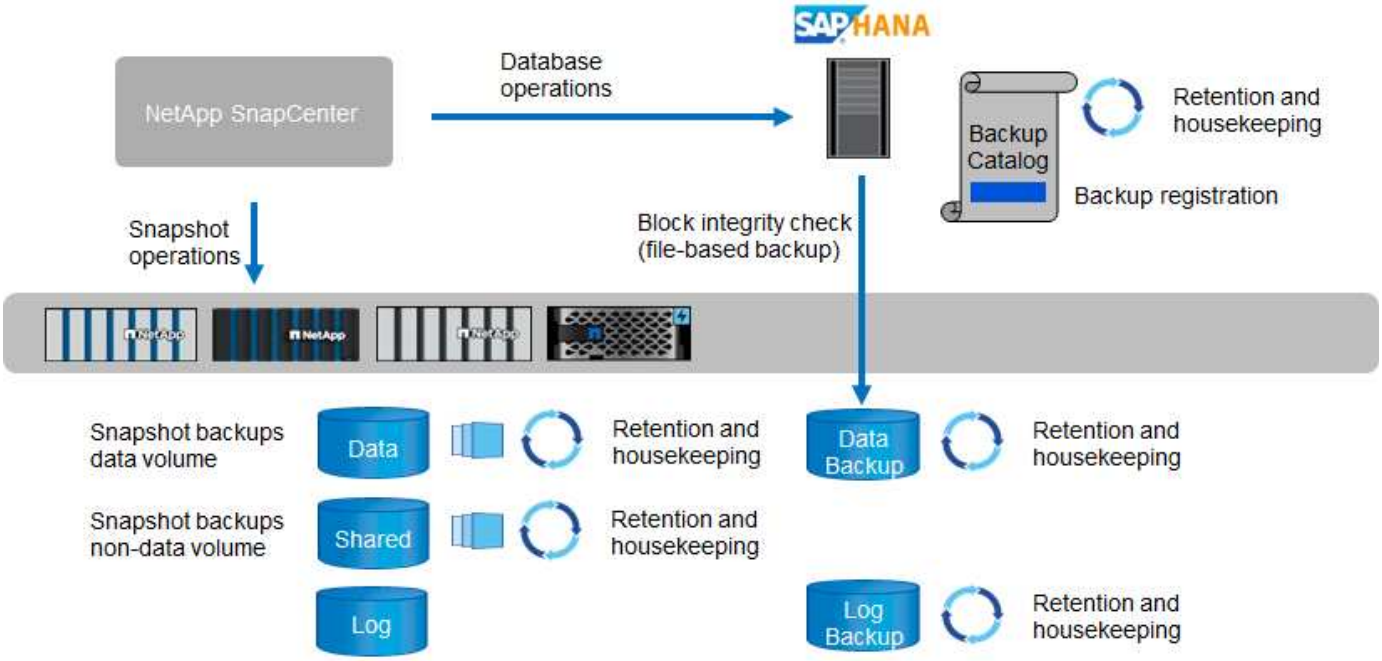

**SAP HANA** のバックアップ

すべてのネットアップストレージコントローラに搭載された ONTAP ソフトウェアは、動作中にパフォーマンスに影響を与えることなく SAP HANA データベースをバックアップするための組み込みメカニズムを提供します。ストレージベースの NetApp Snapshot バックアップは、 SAP HANA の単一コンテナ、および単一テナントまたは複数テナントを使用する SAP HANA マルチテナントデータベースコンテナ（ MDC ）システムで使用可能な、完全にサポートされた統合バックアップ解決策です。

ストレージベースの Snapshot バックアップは、 NetApp SnapCenter Plug-in for SAP HANA を使用して実装されます。これにより、 SAP HANA データベースに標準で搭載されているインターフェイスを使用して、整合性のあるストレージベースの Snapshot バックアップを作成できます。SnapCenter は、各 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。したがって、 SnapCenter で作成されたバックアップは、リストア処理とリカバリ処理用に直接選択できる SAP HANA Studio と Cockpit 内に表示されます。

NetApp SnapMirror テクノロジを使用すると、一方のストレージシステムで作成された Snapshot コピーを、SnapCenter で制御されるセカンダリバックアップストレージシステムにレプリケートできます。その後、プライマリストレージ上のバックアップセットごと、およびセカンダリストレージシステム上のバックアップセットごとに、異なるバックアップ保持ポリシーを定義できます。SnapCenter Plug-in for SAP HANA は、不要なバックアップカタログの削除を含め、 Snapshot コピーベースのデータバックアップとログバックアップの保持を自動的に管理します。また、 SnapCenter Plug-in for SAP HANA では、ファイルベースのバックアップを実行することで、 SAP HANA データベースのブロック整合性チェックを実行できます。

次の図に示すように、 NFS マウントを使用して、データベースログをセカンダリストレージに直接バックアップできます。




ストレージベースの Snapshot バックアップは、従来のファイルベースのバックアップに比べて大きなメリットをもたらします。たとえば、次のような利点があります。

- 高速バックアップ（数分）
- ストレージレイヤでのリストア時間（数分）が大幅に短縮され、バックアップの頻度が向上するため、Recovery Time Objective （ RTO ；目標復旧時間）が短縮されます
- バックアップとリカバリの処理中、 SAP HANA データベースのホスト、ネットワーク、またはストレージのパフォーマンスが低下することはありません
- ブロックの変更に基づいて、スペース効率と帯域幅効率に優れたセカンダリストレージへのレプリケーションを実行します

SnapCenterを使用したSAP HANAバックアップ/リカバリ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-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"。

### SAP HANA ディザスタリカバリ

SAP HANA ディザスタリカバリは、 SAP HANA システムレプリケーションを使用してデータベースレイヤで実行するか、ストレージレプリケーションテクノロジを使用してストレージレイヤで実行できます。次のセクションでは、ストレージレプリケーションに基づくディザスタリカバリソリューションの概要について説明します。

SAP HANAディザスタリカバリ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-4646 ：『 SAP HANA Disaster Recovery with Storage Replication 』"。

#### SnapMirror に基づくストレージレプリケーション

次の図に、同期 SnapMirror レプリケーションを使用してローカルのディザスタリカバリデータセンターにデータをレプリケートする 3 サイトのディザスタリカバリ解決策と、非同期 SnapMirror を使用してリモートのディザスタリカバリデータセンターにデータをレプリケートする様子を示します。

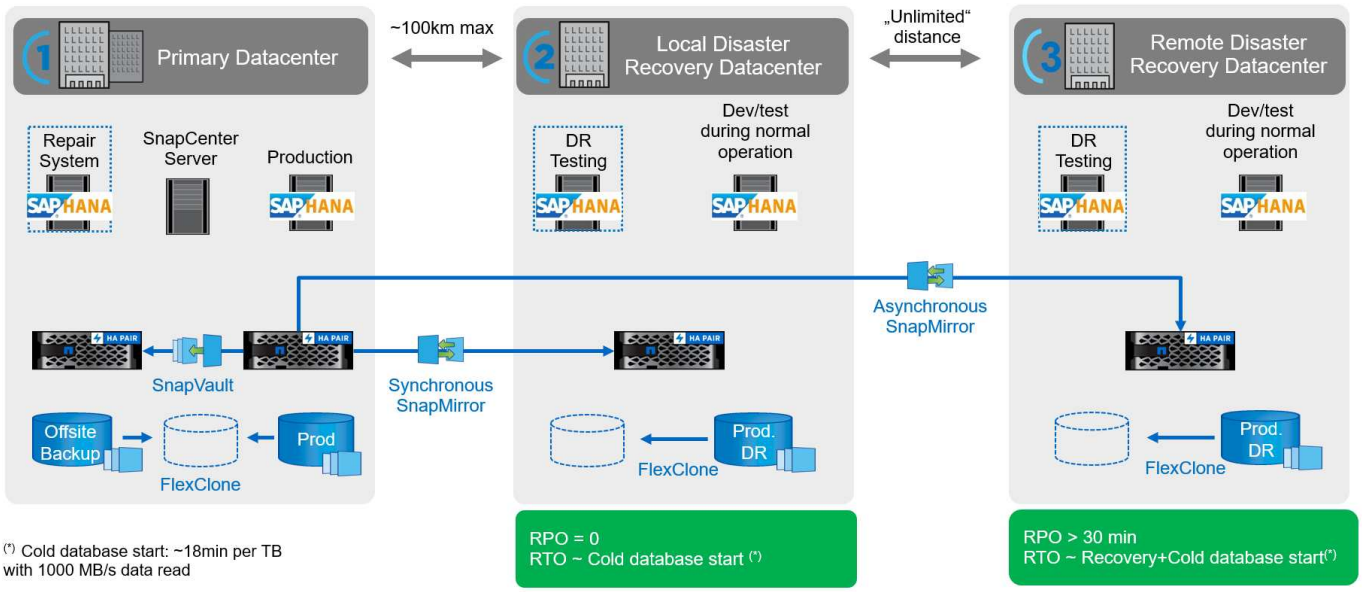
同期 SnapMirror を使用したデータレプリケーションでは、 RPO がゼロになります。プライマリとローカルのディザスタリカバリデータセンター間の距離は約 100km です。

プライマリとローカルの両方のディザスタリカバリサイトで障害が発生した場合の保護は、非同期 SnapMirror を使用して、第 3 のリモートディザスタリカバリデータセンターにデータをレプリケートすることで実現されます。RPO は、レプリケーションの更新頻度と転送速度によって異なります。理論的には距離は無制限ですが、転送が必要なデータ量とデータセンター間の接続によって制限は異なります。通常の RPO の値は、 30 分から数時間です。

どちらのレプリケーション方法の RTO も、主に、 HANA データベースをディザスタリカバリサイトで開始してデータをメモリにロードするのに必要な時間に左右されます。1000Mbps のスループットでデータが読み取られることを前提とし、 1TB のデータをロードするには約 18 分かかります。

通常の運用中は、ディザスタリカバリサイトのサーバを開発 / テストシステムとして使用できます。災害が発生した場合は、開発 / テストシステムをシャットダウンし、ディザスタリカバリ本番用サーバとして起動する必要があります。

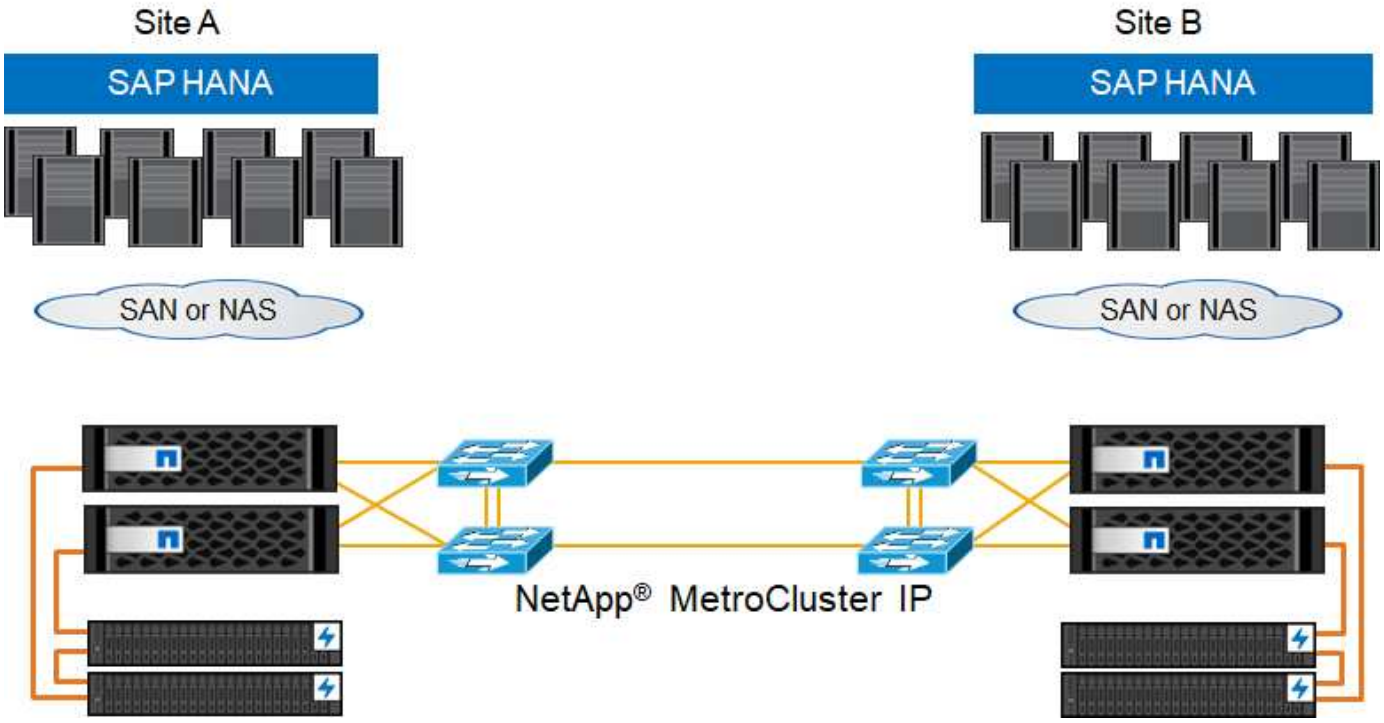
どちらのレプリケーション方法でも、 RPO と RTO に影響を与えることなくディザスタリカバリのワークフローテストを実行できます。FlexClone ボリュームはストレージ上に作成され、ディザスタリカバリテスト用サーバに接続されます。




同期レプリケーションで StrictSync モードが提供されます。何らかの理由でセカンダリストレージへの書き込みが完了しないと、アプリケーション I/O が失敗し、プライマリストレージシステムとセカンダリストレージシステムが同一になります。プライマリへのアプリケーション I/O は、 SnapMirror 関係のステータスが InSync に戻るまで再開されません。プライマリストレージで障害が発生した場合は、フェイルオーバー後にセカンダリストレージでアプリケーション I/O を再開できます。データ損失は発生しません。StrictSync モードでは、 RPO は常にゼロです。

#### MetroCluster に基づくストレージレプリケーション

次の図は、解決策の概要を示しています。各サイトのストレージクラスタがローカルで高可用性を実現し、本番環境のワークロードに使用されます。各サイトのデータはもう一方のサイトに同期的にレプリケートされ、災害のフェイルオーバーが発生した場合に使用できます。




## ストレージのサイジング

次のセクションでは、 SAP HANA 用のストレージシステムのサイジングに必要なパフォーマンスと容量に関する考慮事項の概要を説明します。

適切なサイズのストレージ環境を構築するために、ネットアップまたはネットアップパートナーの営業担当者にお問い合わせください。

### パフォーマンスに関する考慮事項

SAP では、データベースホストのメモリサイズや SAP HANA データベースを使用するアプリケーションに関係なく、すべての本番用 SAP HANA 環境に有効な静的なストレージ KPI のセットが定義されています。これらの KPI は、シングルホスト環境、マルチホスト環境、 Business Suite on HANA 環境、 Business Warehouse on HANA 環境、 S/4HANA 環境、および BW/4HANA 環境で有効です。したがって、現在のパフォーマンスサイジングアプローチは、ストレージシステムに接続されているアクティブな SAP HANA ホストの数にのみ依存します。

ストレージパフォーマンス KPI は、本番用 SAP HANA システムにのみ必須ですが、すべての HANA システムに実装できます。

SAP は、ストレージシステムのパフォーマンスを検証するためのパフォーマンステストツールを提供し、ストレージに接続されたアクティブな SAP HANA ホストに対応します。

ネットアップは、特定のストレージモデルに接続できる SAP HANA ホストの最大数をテストして事前に定義しました。さらに、本番環境ベースの SAP HANA システムに必要なストレージ KPI を実現しています。

認定 FAS 製品ファミリーのストレージコントローラは、他のディスクタイプやディスクバックエンドソリューションと組み合わせて SAP HANA にも使用できます。ただし、ネットアップがサポートし、 SAP HANA TDI パフォーマンス KPI を達成する必要があります。たとえば、 NetApp Storage Encryption （ NSE ）や NetApp FlexArray テクノロジなどです。

本ドキュメントでは、 SAS HDD およびソリッドステートドライブ（ SSD ）のディスクサイジングについて説明します。

#### HDD

SAP のストレージパフォーマンス KPI を実現するには、 SAP HANA ノードごとに 10 本以上のデータディスク（ 10k rpm SAS ）が必要です。

この計算は、ストレージコントローラ、ディスクシェルフ、およびデータベースの容量要件に左右されません。ディスクシェルフを追加しても、ストレージコントローラでサポートできる SAP HANA ホストの最大数は増加しません。

ソリッドステートドライブ

SSD の場合は、データディスクの数は、ストレージコントローラから SSD シェルフへの SAS 接続スループットによって決まります。

単一のディスクシェルフで実行できる SAP HANA ホストの最大数と、 SAP HANA ホストごとに必要な SSD の最小数は、 SAP パフォーマンステストツールを実行して決定されています。このテストでは、ホストの実際のストレージ容量要件は考慮しません。また、実際に必要なストレージ構成を判断するために必要な容量も計算する必要があります。

- SSD を 24 本搭載した 12Gb SAS ディスクシェルフ（ DS224C ）は、ディスクシェルフが 12Gb に接続される場合、最大 14 台の SAP HANA ホストをサポートします。
- SSD を 24 本搭載した 6Gb SAS ディスクシェルフ（ DS2246 ）は、最大 4 台の SAP HANA ホストをサポートします。

SSD と SAP HANA ホストは、両方のストレージコントローラ間で均等に分散する必要があります。

次の表に、ディスクシェルフごとにサポートされる SAP HANA ホストの数を示します。

| | **24** 本の **SSD** をフル搭載した **6Gb SAS** シェルフ（ **DS2246** | **12Gb SAS** シェルフ（ **DS224C** ）には **24** 本の **SSD** がフル搭載されています |
|---|---|---|
| ディスクシェルフあたりの SAP HANA ホストの最大数 | 4. | 14 |

この計算は、使用しているストレージコントローラには依存しません。ディスクシェルフを追加しても、ストレージコントローラでサポートできる SAP HANA ホストの最大数は増加しません。

混在ワークロード

SAP HANA とその他のアプリケーションワークロードを、同じストレージコントローラ上または同じストレージアグリゲート内で実行することはできません。ただし、ネットアップのベストプラクティスとして、

SAP HANA ワークロードを他のすべてのアプリケーションワークロードから分離することを推奨します。

SAP HANA ワークロードとその他のアプリケーションワークロードを、同じストレージコントローラまたは同じアグリゲートに導入することもできます。その場合は、混在ワークロード環境内で SAP HANA に対して適切なパフォーマンスが確保されていることを確認する必要があります。また、 Quality of Service （ QoS ；サービス品質）パラメータを使用して、他のアプリケーションの影響を制御し、 SAP HANA アプリケーションのスループットを保証することも推奨します。

SAP パフォーマンステストツールを使用して、すでに他のワークロードに使用されている既存のストレージコントローラで追加の SAP HANA ホストを実行できるかどうかを確認する必要があります。SAP アプリケーションサーバは、 SAP HANA データベースと同じストレージコントローラやアグリゲートに安全に配置できます。

### 容量に関する考慮事項

SAP HANA の容量要件の詳細な概要については、を参照してください "SAP ノート 1900823" ホワイトペーパーを添付。

> 複数の SAP HANA システムで構成される SAP 環境全体の容量サイジングは、ネットアップの SAP HANA ストレージサイジングツールを使用して決定する必要があります。ストレージのサイジングプロセスを検証し、適切なサイズのストレージ環境を構築するには、ネットアップまたはネットアップパートナーの営業担当者にお問い合わせください。

### パフォーマンステストツールの設定

SAP HANA 1.0 SPS10 以降、 I/O 動作を調整し、使用中のファイルシステムとストレージシステムのデータベースを最適化するためのパラメータが導入されています。これらのパラメータは、 SAP パフォーマンステストツールでストレージのパフォーマンスをテストするときにも設定する必要があります。

ネットアップは、最適な値を定義するため、パフォーマンステストを実施しました。次の表に、 SAP パフォーマンステストツールの構成ファイルで設定する必要があるパラメータを示します。

| パラメータ | 価値 |
| --- | --- |
| max_parallel _io_requests と入力します | 128 |
| async _read_submit | オン |
| async ： write_submit_active | オン |
| async_write_submit_bblocks | すべて |

SAP テストツールの設定の詳細については、を参照してください "SAP ノート 1943937" HWCCT （ SAP HANA 1.0 ）および "SAP ノート 2493172" HCMT/HCOT 用（ SAP HANA 2.0 ）。

次の例は、 HCMT/HCOT 実行プランに変数を設定する方法を示しています。

```
…{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
```

```
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
         "Name": "DataAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
```

```
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

これらの変数はテスト構成に使用する必要があります。これは通常、 SAP が HCMT/HCOT ツールを使用して提供する事前定義された実行計画の場合です。次に、 4k ログの書き込みテストの例を示します。

```
…
       {
          "ID": "D664D001-933D-41DE-A904F304AEB67906",
          "Note": "File System Write Test",
          "ExecutionVariants": [
             {
                "ScaleOut": {
                   "Port": "${RemotePort}",
                   "Hosts": "${Hosts}",
                   "ConcurrentExecution": "${FSConcurrentExecution}"
                },
                "RepeatCount": "${TestRepeatCount}",
                "Description": "4K Block, Log Volume 5GB, Overwrite",
                "Hint": "Log",
                "InputVector": {
                   "BlockSize": 4096,
                   "DirectoryName": "${LogVolume}",
                   "FileOverwrite": true,
                   "FileSize": 5368709120,
                   "RandomAccess": false,
                   "RandomData": true,
                   "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                   "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                   "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                   "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                   "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                   "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                   "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                   "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                   "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
                }
             }, …
```

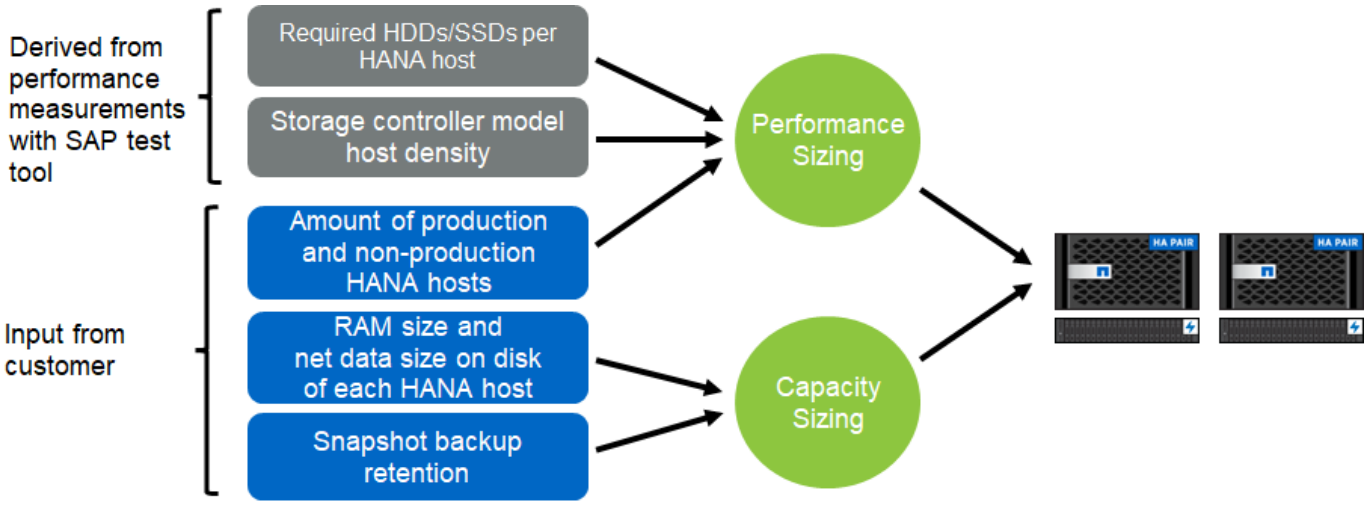
ストレージサイジングプロセスの概要

各ストレージモデルの HANA ホストあたりのディスク数と SAP HANA ホストの密度は、 SAP パフォーマンステストツールで決定されています。

サイジングプロセスでは、本番用および非本番用の SAP HANA ホストの数、各ホストの RAM サイズ、ストレージベースの Snapshot コピーのバックアップ保持期間などの詳細が必要です。SAP HANA ホストの数によって、必要なストレージコントローラとディスクの数が決まります。

RAM のサイズ、各 SAP HANA ホストでのディスク上の正味データサイズ、および Snapshot コピーのバックアップ保持期間は、容量サイジングの際に入力として使用されます。

次の図に、サイジングプロセスの概要を示します。




## インフラのセットアップと設定

ネットワークセットアップ

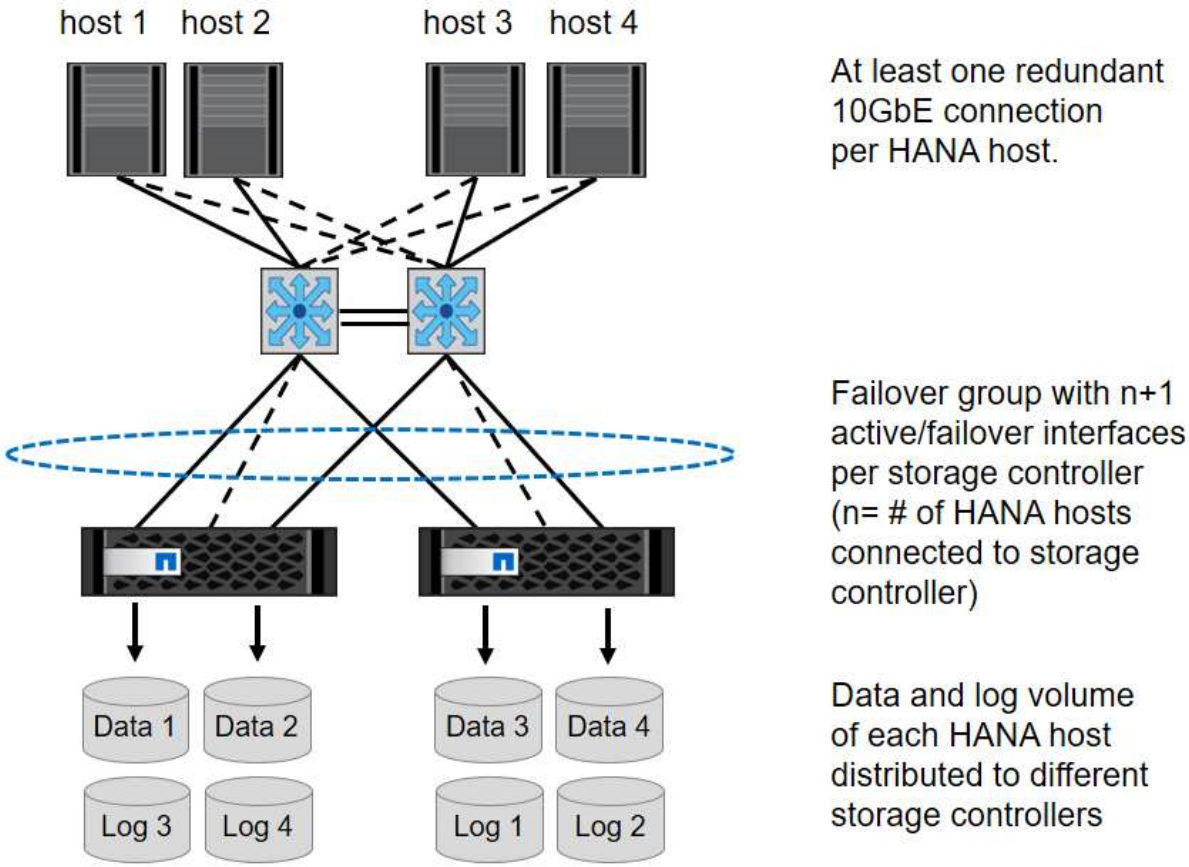
## ネットワークを設定する際は、次のガイドラインに従ってください。

- SAP HANA ホストを 10GbE 以上のネットワークでストレージコントローラに接続するには、専用のストレージネットワークを使用する必要があります。
- ストレージコントローラと SAP HANA ホストには同じ接続速度を使用します。これができない場合は、ストレージコントローラと SAP HANA ホスト間のネットワークコンポーネントが異なる速度に対応できることを確認してください。たとえば、ストレージとホストの間で NFS レベルで速度のネゴシエーションを行うための十分なバッファスペースを確保する必要があります。ネットワークコンポーネントは通常スイッチですが、背面など、ブレードシャーシ内の他のコンポーネントも考慮する必要があります。
- ストレージネットワークスイッチおよびホストレイヤで、ストレージトラフィックに使用されるすべての物理ポートでフロー制御を無効にします。
- 各 SAP HANA ホストには、 10Gb 以上の帯域幅を持つ冗長ネットワーク接続が必要です。
- SAP HANA ホストとストレージコントローラ間のすべてのネットワークコンポーネントで、最大転送単位（ MTU ）サイズが 9 、 000 のジャンボフレームを有効にする必要があります。
- VMwareのセットアップでは、実行中の各仮想マシンに専用のVMXNET3ネットワークアダプタを割り当てる必要があります。詳細な要件については、に記載されている関連文書を確認してください"はじめに"。
- 相互の干渉を避けるため、ログとデータ領域には別々のネットワーク /IO パスを使用してください。

次の図は、 4 台の SAP HANA ホストを 10GbE ネットワークを使用してストレージコントローラ HA ペアに接続した場合の例を示しています。各 SAP HANA ホストには、冗長ファブリックへのアクティブ / パッシブ接続があります。

ストレージレイヤでは、各 SAP HANA ホストに 10Gb のスループットを提供する、 4 つのアクティブ接続が構成されます。また、各ストレージコントローラにスペアインターフェイスが 1 つ設定されます。

ストレージレイヤでは、 MTU サイズが 9 、 000 のブロードキャストドメインが設定され、必要なすべての物理インターフェイスがこのブロードキャストドメインに追加されます。このアプローチでは、これらの物理インターフェイスが自動的に同じフェイルオーバーグループに割り当てられます。これらの物理インターフェイスに割り当てられているすべての論理インターフェイス（ LIF ）が、このフェイルオーバーグループに追加されます。



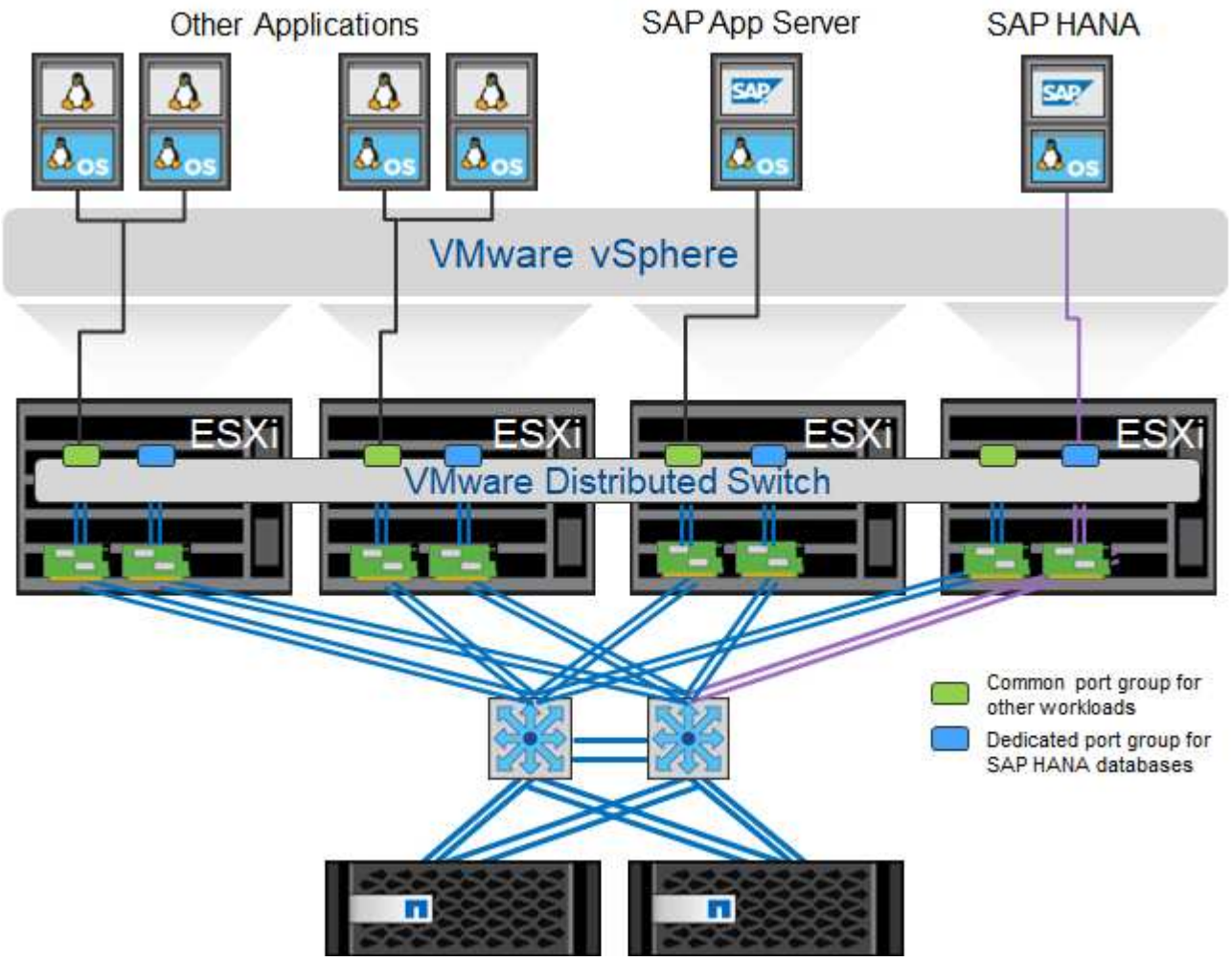

一般に、サーバ（ボンド）とストレージシステム（ Link Aggregation Control Protocol （ LACP ）、 ifgroups など）で HA インターフェイスグループを使用することもできます。HA インターフェイスグループを使用して、グループ内のすべてのインターフェイス間で負荷が均等に分散されていることを確認します。負荷分散は、ネットワークスイッチインフラの機能によって異なります。

SAP HANA ホストの数と使用されている接続速度に応じて、アクティブな物理ポートの数を変える必要があります。

**VMware** 固有のネットワークセットアップ

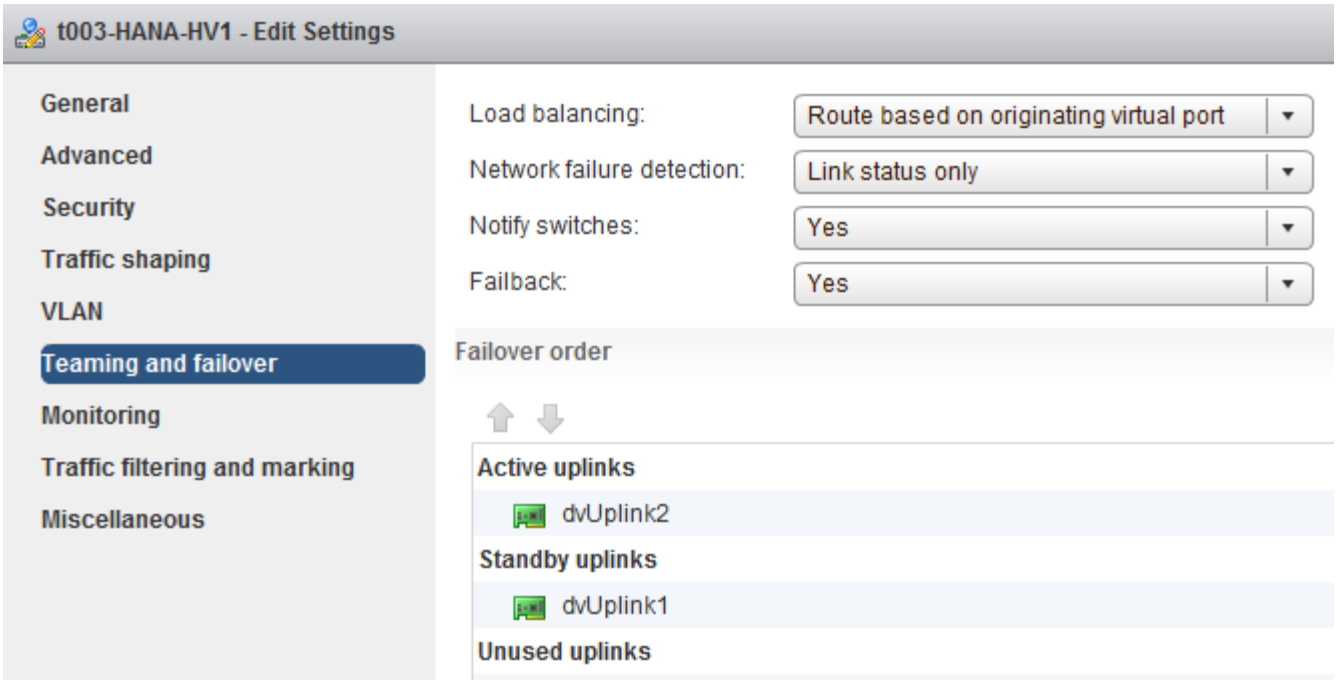
この解決策では、パフォーマンス重視のデータボリュームやデータベースのログボリュームなど、 SAP HANA インスタンスのデータはすべて NFS 経由で提供されるため、適切なネットワーク設計と構成が不可欠です。専用のストレージネットワークは、 SAP HANA ノード間の通信トラフィックとユーザアクセストラフィックから NFS トラフィックを分離するために使用されます。各 SAP HANA ノードには、 10Gb 以上の帯域幅を持つ冗長専用ネットワーク接続が必要です。より高い帯域幅もサポートされています。このネットワークは、 VMware vSphere でホストされているゲストオペレーティングシステムまで、ストレージレイヤからネットワークスイッチングおよびコンピューティング経由でエンドツーエンドで拡張する必要があります。物理スイッチングインフラストラクチャに加えて、ハイパーバイザーレイヤでネットワークトラフィックのパフォーマンスと管理性を十分に確保するために、 VMware Distributed Switch （ vDS ）が使用されます。

次の図に、ネットワークの概要を示します。




各 SAP HANA ノードは、 VMware Distributed Switch 上で専用のポートグループを使用します。このポートグループを使用すると、 ESX ホストのサービス品質（ QoS ）の向上と物理 Network Interface Card （ NIC ；ネットワークインターフェイスカード）の専用割り当てが可能になります。NIC の障害が発生した場合に HA 機能を維持しながら専用の物理 NIC を使用するには、専用の物理 NIC をアクティブアップリンクとして構成します。SAP HANA ポートグループのチーミングとフェイルオーバーの設定では、追加の NIC がスタンバイアップリンクとして設定されます。また、物理スイッチと仮想スイッチでジャンボフレーム（ MTU 9 、000 ）をエンドツーエンドで有効にする必要があります。また、サーバ、スイッチ、およびストレージシステムのストレージトラフィックに使用されるすべてのイーサネットポートでフロー制御を無効にします。次の図に、このような構成の例を示します。

NFS トラフィックに使用されるインターフェイスでは、 LRO （ Large Receive Offload ）をオフにする必要があります。その他のネットワーク構成のガイドラインについては、それぞれの VMware ベストプラクティスガイドで SAP HANA を参照してください。




時刻の同期

ストレージコントローラと SAP HANA データベースホストの間で時刻を同期する必要があります。そのためには、すべてのストレージコントローラとすべての SAP HANA ホストに同じタイムサーバを設定します。

ストレージコントローラのセットアップ

ここでは、ネットアップストレージシステムの構成について説明します。プライマリのインストールとセットアップは、対応する ONTAP のセットアップガイドおよび設定ガイドに従って実行する必要があります。

ストレージ効率

SSD 構成の SAP HANA では、インライン重複排除、ボリューム間インライン重複排除、インライン圧縮、インラインコンパクションがサポートされています。

HDD ベースの構成で Storage Efficiency 機能を有効にすることはできません。

**NetApp FlexGroup**ボリューム

NetApp FlexGroup Volumeの使用はSAP HANAではサポートされていません。SAP HANAのアーキテクチャ上、FlexGroup Volumeを使用してもメリットはなく、パフォーマンスの問題が発生する可能性があります。

**NetApp**ボリュームとアグリゲートの暗号化

SAP HANAでは、NetApp Volume Encryption（NVE）とNetApp Aggregate Encryption（NAE）の使用がサポートされています。

サービス品質

QoS を使用すると、特定の SAP HANA システムやその他のアプリケーションの共有使用コントローラにおけるストレージスループットを制限できます。1 つのユースケースとして、開発システムとテストシステムのスループットを制限し、混在環境で本番システムに影響を与えないようにすることが挙げられます。

サイジングプロセスでは、非本番システムのパフォーマンス要件を決定する必要があります。開発 / テスト用のシステムは、通常、 SAP で定義されている本番用システム KPI の 20~50% の範囲で、パフォーマンス値を低くしてサイジングすることができます。

ONTAP 9 以降では、ストレージボリュームレベルで QoS が設定され、スループット（ MBps ）と I/O 量（ IOPS ）に最大値が使用されます。

ストレージシステムのパフォーマンスに最大の影響があるのは、大きい書き込み I/O です。そのため、 QoS スループットの制限値として、データボリュームとログボリュームの対応する書き込み SAP HANA ストレージパフォーマンス KPI 値の割合を設定する必要があります。

#### NetApp FabricPool

SAP HANA システムのアクティブなプライマリファイルシステムには、 NetApp FabricPool テクノロジを使用しないでください。これには ' データとログ領域のファイル・システムと '/hana/shared-file システムが含まれますそのため、特に SAP HANA システムの起動時に、予測不可能なパフォーマンスが発生します。

「 snapshot-only 」階層化ポリシーを使用することも、 SnapVault または SnapMirror デスティネーションなどのバックアップターゲットで一般的に FabricPool を使用することもできます。

> FabricPool を使用してプライマリストレージで Snapshot コピーを階層化するか、バックアップターゲットで FabricPool を使用すると、データベースまたはシステムクローンの作成や修復などのその他のタスクのリストアとリカバリに必要な時間が変わります。この点を考慮して、ライフサイクル全体の管理戦略を計画し、この機能を使用している間も SLA が満たされていることを確認してください。

FabricPool は、ログバックアップを別のストレージ階層に移動する場合に適しています。バックアップの移動は、 SAP HANA データベースのリカバリに要する時間に影響します。したがって、「 tiering-minimum-cooling-days 」オプションには、リカバリに必要なログバックアップをローカルの高速ストレージ階層に定期的に配置する値を設定する必要があります。

ストレージ構成

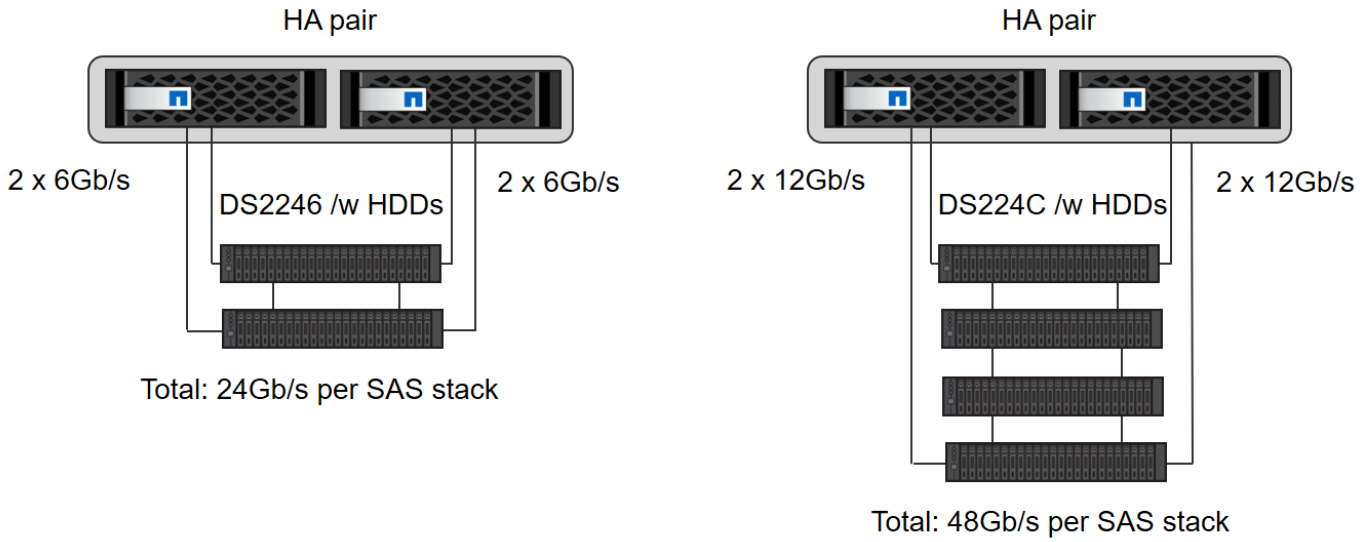
以下に、必要なストレージ構成手順の概要を示します。各手順の詳細については、以降のセクションで説明します。このセクションでは、ストレージハードウェアがセットアップされており、 ONTAP ソフトウェアがすでにインストールされていることを前提としています。また、ストレージポート（ 10GbE 以上）とネットワークの間の接続がすでに確立されている必要があります。

1. の説明に従って、正しいSASスタック構成を確認します。"ディスクシェルフの接続"
2. の説明に従って、必要なアグリゲートを作成して設定します。"アグリゲートの構成："
3. の説明に従ってStorage Virtual Machine（SVM）を作成します。"Storage Virtual Machine の設定。"
4. の説明に従ってLIFを作成します。"論理インターフェイスの構成"
5. およびの説明に従って、アグリゲート内にボリュームを作成します。"SAP HANA シングルホストシステムのボリューム構成""SAP HANA マルチホストシステムのボリューム構成。"

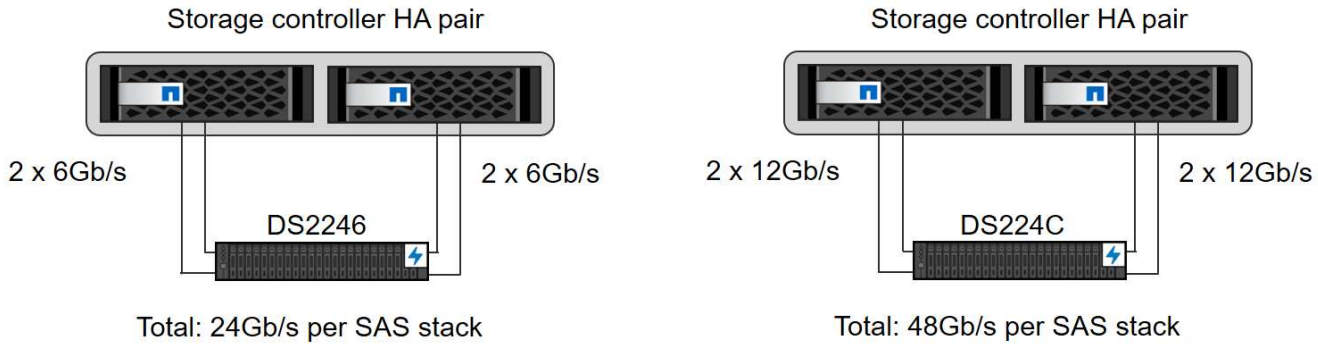
6. の説明に従って、必要なボリュームオプションを設定します。"ボリュームのオプション"
7. の説明に従ってNFSv3に必要なオプションを設定するか、の説明に従ってNFSv4に必要なオプションを設定し"NFSv3 用の NFS 設定"ます。"NFSv4 の NFS 設定"
8. の説明に従って、ボリュームをネームスペースにマウントし、エクスポートポリシーを設定します。"ボリュームをネームスペースにマウントし、エクスポートポリシーを設定"

ディスクシェルフの接続

HDD を使用すると、次の図に示すように、 1 つの SAS スタックに最大 2 台の DS2246 ディスクシェルフまたは 4 台の DS224C ディスクシェルフを接続することで、 SAP HANA ホストに必要なパフォーマンスを実現できます。各シェルフ内のディスクは、 HA ペアの両方のコントローラに均等に分散する必要があります。

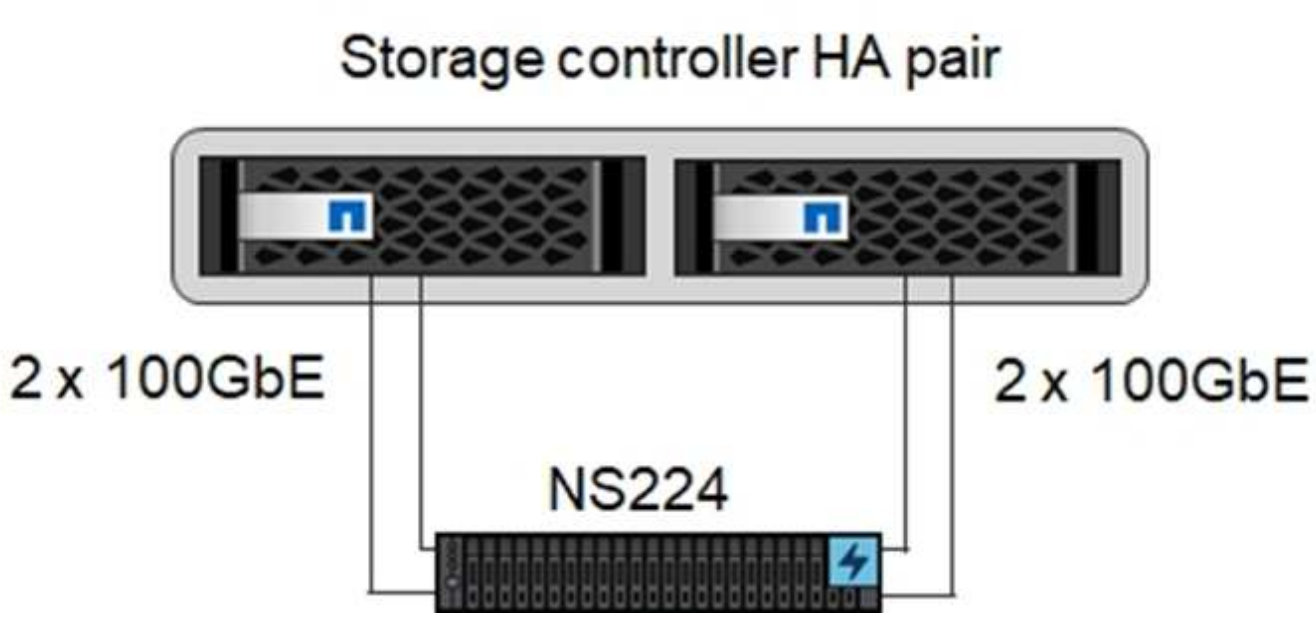



SSD を使用する場合は、次の図に示すように、 1 つの SAS スタックに最大 1 台のディスクシェルフを接続して、 SAP HANA ホストに必要なパフォーマンスを実現できます。各シェルフ内のディスクは、 HA ペアの両方のコントローラに均等に分散する必要があります。ディスクシェルフ DS224C では、クワッドパスの SAS ケーブルも使用できますが、必須ではありません。




**NVMe （ 100GbE ）ディスクシェルフ**

次の図に示すように、NS224 NVMeディスクシェルフは、コントローラごとに2つの100GbEポートで接続されます。各シェルフ内のディスクは、HAペアの両方のコントローラに均等に分散する必要があります。

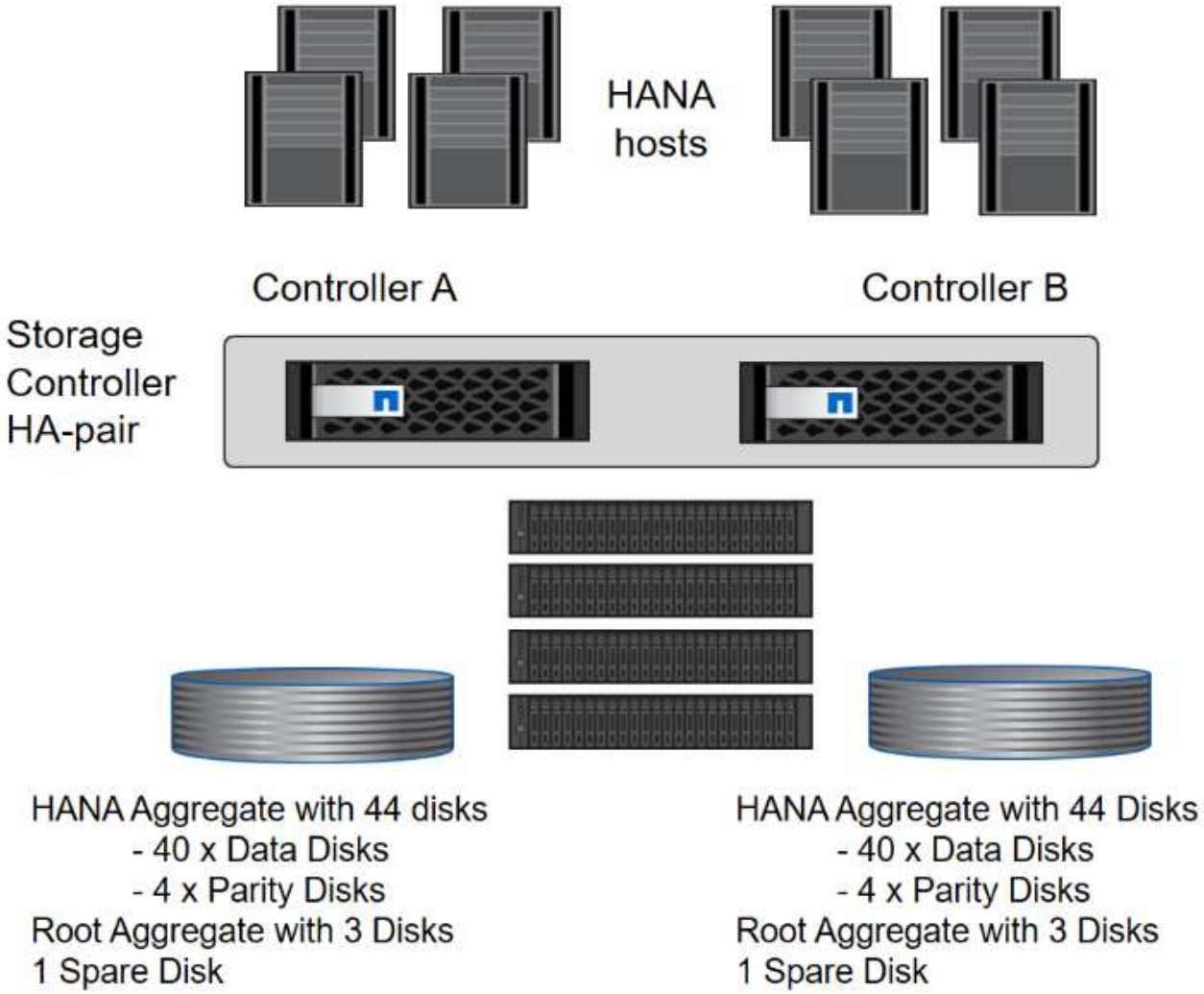



アグリゲートの構成

一般に、使用するディスクシェルフやドライブテクノロジ（ SSD または HDD ）に関係なく、コントローラごとに 2 つのアグリゲートを設定する必要があります。FAS2000 シリーズ・システムには、 1 つのデータ・アグリゲートで十分です。

**HDD** を使用したアグリゲート構成

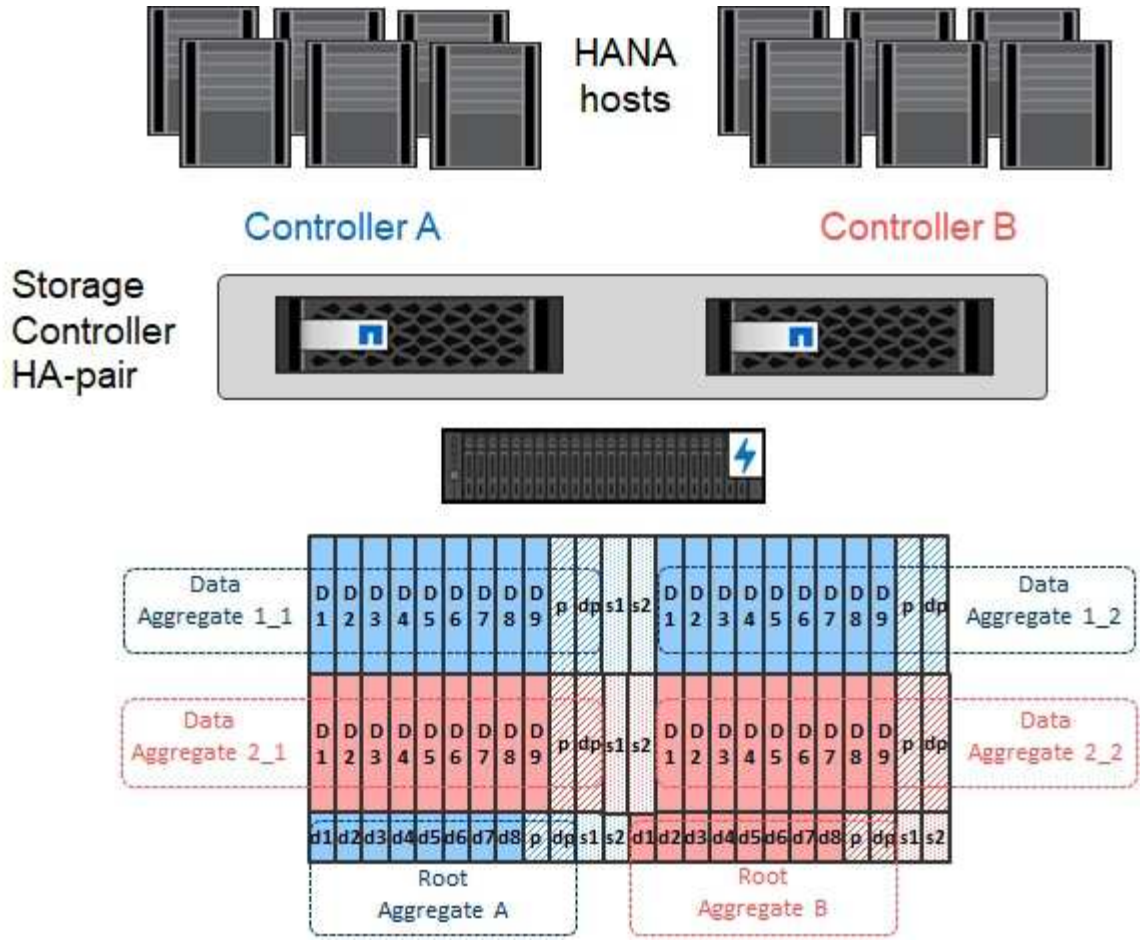
次の図は、 8 台の SAP HANA ホストの構成を示しています。4 台の SAP HANA ホストが各ストレージコントローラに接続されています。各ストレージコントローラに 1 つずつ、合計 2 つのアグリゲートが構成されています。各アグリゲートには、 4 × 10 = 40 のデータディスク（ HDD ）が構成されます。




**SDD** 専用システムで構成を集約する

一般に、使用するディスクシェルフやディスクテクノロジ（ SSD または HDD ）に関係なく、コントローラごとに 2 つのアグリゲートを構成する必要があります。FAS2000 シリーズ・システムには、 1 つのデータ・アグリゲートで十分です。

次の図は、 ADPv2 を使用した、 12Gb の SAS シェルフで稼働する、 12 台の SAP HANA ホストの構成を示しています。6 台の SAP HANA ホストが各ストレージコントローラに接続されています。各ストレージコントローラに 2 つずつ、合計 4 つのアグリゲートが構成されています。各アグリゲートには、 9 つのデータパーティションと 2 つのパリティディスクパーティションを含む 11 本のディスクが構成されます。各コントローラで、 2 つのスペアパーティションを使用できます。




**Storage Virtual Machine** の設定

SAP HANA データベースを使用する複数の SAP ランドスケープでは、単一の SVM を使用できます。SVM は、社内の複数のチームによって管理される場合に備え、必要に応じて各 SAP ランドスケープに割り当てることもできます。

QoS プロファイルが自動的に作成されて新しい SVM の作成時に割り当てられた場合は、自動的に作成されたプロファイルを SVM から削除して、 SAP HANA に必要なパフォーマンスを提供します。

```
vserver modify -vserver <svm-name> -qos-policy-group none
```

論理インターフェイスの構成

SAP HANA 本番システムでは、 SAP HANA ホストからデータボリュームとログボリュームをマウントするために別々の LIF を使用する必要があります。したがって、少なくとも 2 つの LIF が必要です。

異なる SAP HANA ホストのデータボリュームマウントとログボリュームマウントは、同じ LIF を使用するか、マウントごとに個別の LIF を使用することで、物理ストレージネットワークポートを共有できます。

物理インターフェイスごとのデータボリュームマウントとログボリュームマウントの最大数を次の表に示します。

| イーサネットポート速度 | **10GbE** | **25GbE** | **40GbE** | **100 Gee** |
| --- | --- | --- | --- | --- |
| 物理ポートあたりのログボリュームマウントまたはデータボリュームマウントの最大数 | 3 | 8 | 12. | 30 |

異なる SAP HANA ホスト間で 1 つの LIF を共有するには、データボリュームまたはログボリュームを別の LIF に再マウントすることが必要になる場合があります。この変更により、ボリュームが別のストレージコントローラに移動された場合のパフォーマンス低下を回避できます。

開発 / テスト用システムでは、物理ネットワークインターフェイス上で使用できるデータおよびボリュームのマウントや LIF を増やすことができます。

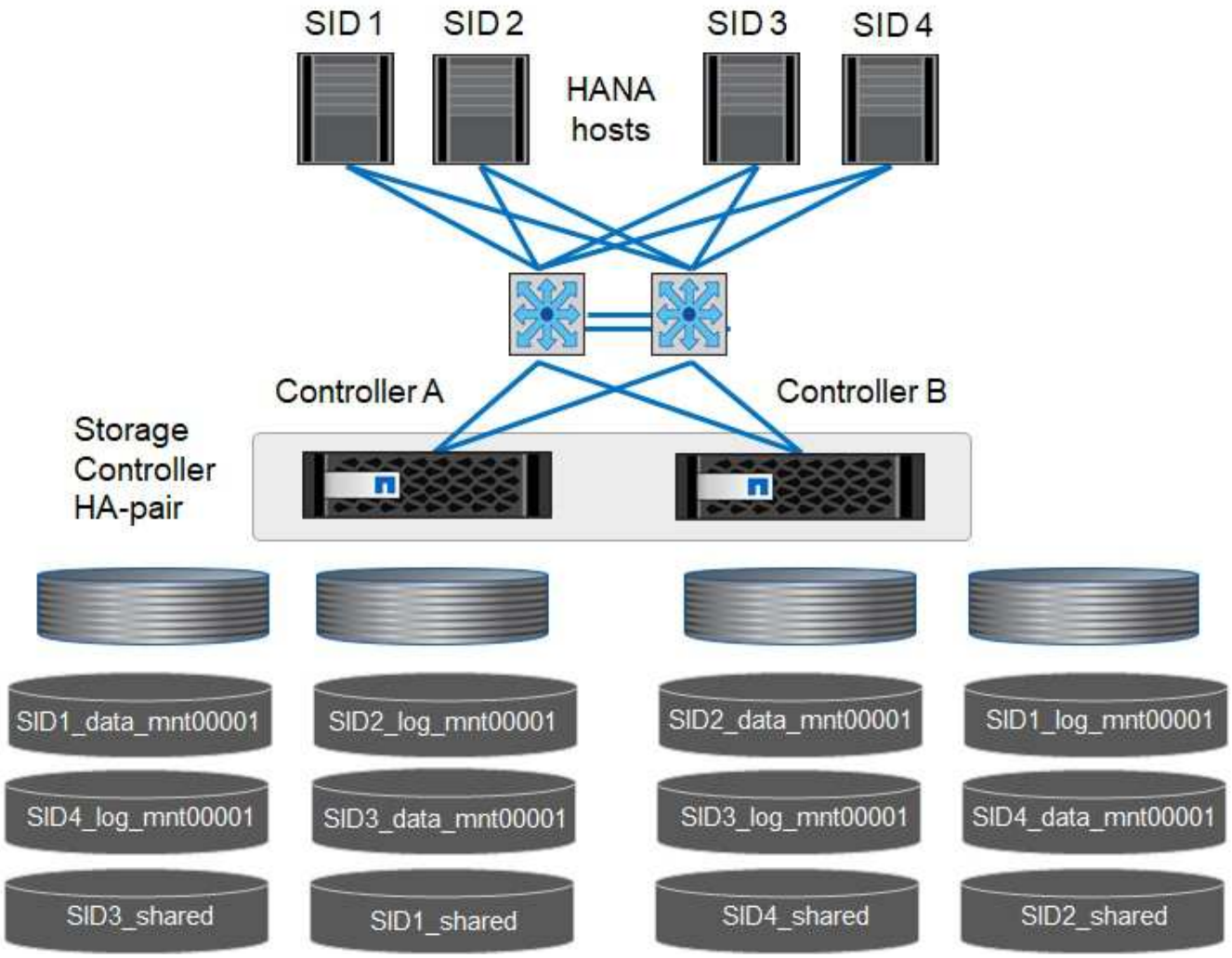
本番システム ' 開発システム ' およびテスト・システムでは '/hana/shared ファイル・システムは ' データ・ボリュームまたはログ・ボリュームと同じ LIF を使用できます

#### **SAP HANA** シングルホストシステムのボリューム構成

次の図は、 4 つのシングルホスト SAP HANA システムのボリューム構成を示しています。各 SAP HANA システムのデータボリュームとログボリュームは、異なるストレージコントローラに分散されます。たとえば、ボリューム「 ID1_data_mnt00001 」がコントローラ A で設定され、ボリューム「 ID1_log_mnt00001 」がコントローラ B で設定されているとします

HA ペアのうち、 1 台のストレージコントローラのみを SAP HANA システムに使用する場合は、データボリュームとログボリュームを同じストレージコントローラに保存することもできます。

データボリュームとログボリュームが同じコントローラに格納されている場合は、サーバからストレージへのアクセスに、 2 つの異なる LIF を使用して実行する必要があります。 1 つはデータボリュームにアクセスする LIF で、もう 1 つはログボリュームにアクセスする LIF です。




各 SAP HANA DB ホストには、データボリューム、ログボリューム、「 /hana/shared 」のボリュームが構成されています。次の表は、シングルホスト SAP HANA システムの構成例を示しています。

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **b** のアグリゲート **2** |
|---|---|---|---|---|
| システム SID1 のデータ、ログ、および共有ボリューム | データボリューム：SID1_data_mnt00001 | 共有ボリューム：SID1_shared | – | ログボリューム：SID1_log_mnt00001 |
| システム SID2 のデータボリューム、ログボリューム、および共有ボリューム | – | ログボリューム：SID2_log_mnt00001 | データボリューム：SID2_data_mnt00001 | 共有ボリューム：SID2_shared |
| システム SID3 のデータ、ログ、および共有ボリューム | 共有ボリューム：SID3_shared | データボリューム：SID3_data_mnt00001 | ログボリューム：SID3_log_mnt00001 | – |
| システム SID4 のデータボリューム、ログボリューム、および共有ボリューム | ログボリューム：SID4_log_mnt00001 | – | 共有ボリューム：SID4_shared | データボリューム：SID4_data_mnt00001 |

次の表に、シングルホストシステムのマウントポイント構成例を示します。「 idadm 」ユーザのホーム・ディレクトリを中央ストレージに配置するには、「 /usr/sap/SID 」ファイル・システムを「 S ID_SHARED 」ボリュームからマウントする必要があります。

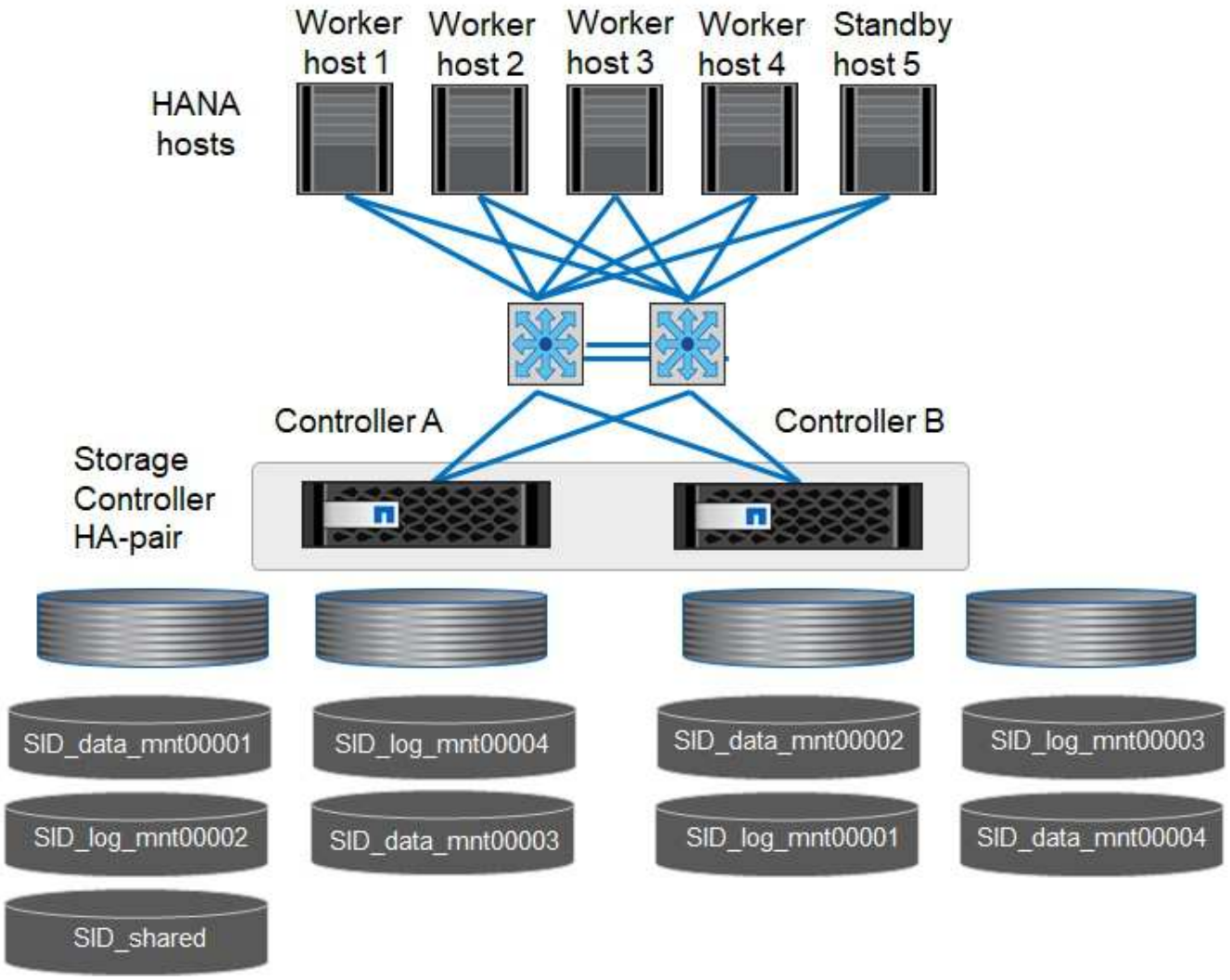
| ジャンクションパス | ディレクトリ | **HANA** ホストのマウントポイント |
|---|---|---|
| SID_data_mnt00001 | – | /hana/data/SID/mnt00001 |
| SID_log_mnt00001 | – | /hana/log/sid/mnt00001 |
| SID_shared | usr - SAP 共有 | /usr/sap/SID/hana/shared に格納されています |

**SAP HANA** マルチホストシステムのボリューム構成

次の図は、 4+1 の SAP HANA システムのボリューム構成を示しています。各 SAP HANA ホストのデータボリュームとログボリュームは、異なるストレージコントローラに分散されます。たとえば、ボリューム「 ID1_data1_mnt00001 」がコントローラ A に設定され、ボリューム「 ID1_log1_mnt00001 」がコントローラ B に設定されているとします

HA ペアのうち、 1 台のストレージコントローラのみを SAP HANA システムに使用する場合は、データボリュームとログボリュームを同じストレージコントローラに保存することもできます。

データボリュームとログボリュームが同じコントローラに格納されている場合は、サーバからストレージへのアクセスに、 2 つの異なる LIF を使用して実行する必要があります。 1 つはデータボリュームにアクセスするため、もう 1 つはログボリュームにアクセスするためです。




各 SAP HANA ホストには、 1 個のデータボリュームと 1 個のログボリュームが作成されます。「 /hana/shared 」ボリュームは、 SAP HANA システムのすべてのホストで使用されます。次の表に、 4 つのアクティブホストを持つ、マルチホスト SAP HANA システムの構成例を示します。

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| ノード 1 のデータボリュームとログボリューム | データボリューム： SID_data_mnt00001 | – | ログボリューム： SID_log_mnt00001 | – |
| ノード 2 のデータボリュームとログボリューム | ログボリューム： SID_log_mnt00002 | – | データボリューム： SID_data_mnt00002 | – |
| ノード 3 のデータボリュームとログボリューム | – | データボリューム： SID_data_mnt00003 | – | ログボリューム： SID_log_mnt00003 |
| ノード 4 のデータボリュームとログボリューム | – | ログボリューム： SID_log_mnt00004 | – | データボリューム： SID_data_mnt00004 |

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| すべてのホストの共有ボリューム | 共有ボリューム：SID_shared | – | – | – |

次の表に、アクティブな SAP HANA ホストが 4 台あるマルチホストシステムの構成とマウントポイントを示します。各ホストの 'idadm' ユーザのホーム・ディレクトリを中央ストレージに配置するために '/usr/sap/SID' ファイル・システムは 'S ID_SHARED' ボリュームからマウントされます

| ジャンクションパス | ディレクトリ | **SAP HANA** ホストのマウントポイント | 注 |
|---|---|---|---|
| SID_data_mnt00001 | – | /hana/data/SID/mnt00001 | すべてのホストにマウントされています |
| SID_log_mnt00001 | – | /hana/log/sid/mnt00001 | すべてのホストにマウントされています |
| SID_data_mnt00002 | – | /hana/data/sid/mnt00002 | すべてのホストにマウントされています |
| SID_log_mnt00002 | – | /hana/log/sid/mnt00002 | すべてのホストにマウントされています |
| SID_data_mnt00003 | – | /hana/data/sid/mnt00003 | すべてのホストにマウントされています |
| SID_log_mnt00003 | – | /hana/log/sid/mnt00003 | すべてのホストにマウントされています |
| SID_data_mnt00004 | – | /hana/data/sid/mnt00004 | すべてのホストにマウントされています |
| SID_log_mnt00004 | – | /hana/log/sid/mnt00004 | すべてのホストにマウントされています |
| SID_shared | 共有 | /hana/shareed/ | すべてのホストにマウントされています |
| SID_shared | usr-sap-host1 | /usr/sap/SID | ホスト 1 にマウントされています |
| SID_shared | usr-sap-host2 | /usr/sap/SID | ホスト 2 にマウントされています |
| SID_shared | usr-sap-host3 | /usr/sap/SID | ホスト 3 にマウント |
| SID_shared | usr-sap-host4 | /usr/sap/SID | ホスト 4 にマウント |
| SID_shared | usr-sap-host5 | /usr/sap/SID | ホスト 5 にマウント |

ボリュームのオプション

すべての SVM について、次の表に示すボリュームオプションを確認して設定する必要があります。一部のコマンドについては、 ONTAP で advanced 権限モードに切り替える必要があります。

| アクション | コマンドを実行します |
| --- | --- |
| Snapshot ディレクトリの可視化を無効にします | vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false |
| Snapshot コピーの自動作成を無効にする | vol modify – vserver <vserver-name> -volume <volname> -snapshot-policy none と指定します |
| SID_shared ボリュームを除くアクセス時間の更新を無効にします | advanced 権限レベルの vol modify -vserver <vserver-name> -volume <volname> -atime-update false set admin を設定します |

#### NFSv3 用の NFS 設定

次の表に示す NFS オプションは、すべてのストレージコントローラで検証および設定する必要があります。

ここに示す一部のコマンドについては、 ONTAP で advanced 権限モードに切り替える必要があります。

| アクション | コマンドを実行します |
| --- | --- |
| NFSv3 を有効にします | nfs modify -vserver <vserver -name> v3.0 enabled |
| NFS TCPの最大転送サイズを1MBに設定する | advanced 権限レベルの nfs modify -vserver <vserver_name> -tcp-max-xfer-size 1048576 set admin を設定します |

ワークロードが異なる共有環境では、NFS TCPの最大転送サイズを262144に設定

#### NFSv4 の NFS 設定

次の表に示す NFS オプションは、すべての SVM で検証および設定する必要があります。

一部のコマンドについては、 ONTAP で advanced 権限モードに切り替える必要があります。

| アクション | コマンドを実行します |
| --- | --- |
| NFSv4 を有効にします | nfs modify -vserver <vserver-name> -v4.1 enabled と入力します |
| NFS TCPの最大転送サイズを1MBに設定する | advanced 権限レベルの nfs modify -vserver <vserver_name> -tcp-max-xfer-size 1048576 set admin を設定します |
| NFSv4 のアクセス制御リスト（ ACL ）を無効にする | nfs modify -vserver <vserver_name>-v4.1-acl disabled |
| NFSv4 ドメイン ID を設定する | nfs modify -vserver <vserver_name>-v4-id-domain <domain-name> |
| NFSv4 の読み取り委譲を無効にする | nfs modify -vserver <vserver_name>-v4.1-read-delegation disabled |
| NFSv4 の書き込み委譲を無効にする | nfs modify -vserver <vserver_name>-v4.1-write-delegation disabled |
| NFSv4 数値 ID を無効にする | nfs modify -vserver <vserver_name>-v4-numeric-ids disabled |

| アクション | コマンドを実行します |
| --- | --- |
| NFSv4.xセッションスロットの数の変更（オプション） | 詳細設定<br>nfs modify -vserver hana-v4.x -session-num-slots <value><br>管理者を設定 |

ワークロードが異なる共有環境では、NFS TCPの最大転送サイズを262144に設定

ID番号を無効にするには、ユーザー管理が必要であることに注意してください（を参照）。"NFSv4 用の SAP HANA インストールの準備"

NFSv4ドメインIDは、すべてのLinuxサーバ（）およびSVMで同じ値に設定する必要があります`/etc/idmapd.conf`（を参照）。"NFSv4 用の SAP HANA インストールの準備"

pNFSは有効にして使用できます。

ホストの自動フェイルオーバーを備えたSAP HANAマルチホストシステムを使用している場合は、`nameserver.ini` 次の表を参照してください。これらのセクションでは、デフォルトの再試行間隔を 10 秒に設定します。

| **nameserver.ini** 内のセクション | パラメータ | 価値 |
| --- | --- | --- |
| フェイルオーバー | normal_retries | 9. |
| distributed_watchdog | Deactivate_retries | 11. |
| distributed_watchdog | TAKEOVER_retries を指定します | 9. |

ボリュームをネームスペースにマウントし、エクスポートポリシーを設定

ボリュームを作成するときは、ボリュームをネームスペースにマウントする必要があります。このドキュメントでは、ジャンクションパス名がボリューム名と同じであると想定しています。デフォルトでは、ボリュームはデフォルトポリシーを使用してエクスポートされます。エクスポートポリシーは必要に応じて適用できます。

ホストのセットアップ

## このセクションで説明するすべての手順は、物理サーバ上の SAP HANA 環境と、VMware vSphere 上で実行される SAP HANA 環境の両方で有効です。

#### SUSE Linux Enterprise Server の構成パラメータ

各 SAP HANA ホストでは、 SAP HANA によって生成されるワークロードに合わせて、追加のカーネルパラメータと構成パラメータを調整する必要があります。

### SUSE Linux Enterprise Server 12 および 15

SUSE Linux Enterprise Server （ SLES ） 12 SP1 以降、カーネルパラメータは /etc/sysctl.d`d ディレクトリ内の構成ファイルで設定する必要があります。たとえば '91-NetApp-/hana.conf という名前の構成ファイルを作成する必要があります

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384 16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle = 0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_max_slot_table_entries = 128
```

SAP OS バージョン用の SLES に含まれている Saptune を使用してこれらの値を設定できます。を参照してください "SAP ノート 3024346" （ SAP ログインが必要です）。

**Red Hat Enterprise Linux 7.2** 以降の構成パラメータ

SAP HANA で生成されるワークロードに合わせて、各 SAP HANA ホストで追加のカーネルパラメータと構成パラメータを調整する必要があります。

Red Hat Enterprise Linux 7.2 以降では、 /etc/sysctl.d` ディレクトリにある構成ファイルでカーネルパラメータを設定する必要があります。たとえば '91-NetApp-/hana.conf という名前の構成ファイルを作成する必要があります

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384  16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle = 0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_max_slot_table_entries = 128
```

Red Hat Enterprise Linuxバージョン8.6以降では、RHEL System Roles for SAP（Ansible）を使用してこれらの設定を適用することもできます。を参照してください "SAP ノート 3024346" （ SAP ログインが必要です）。

**/hana/shared** ボリュームにサブディレクトリを作成します

以下の例は、 SID=NF2 の SAP HANA データベースを示しています。

必要なサブディレクトリを作成するには、次のいずれかの操作を行います。

- シングル・ホスト・システムの場合は '/hana/shared-volume をマウントし 'hared' サブディレクトリと usr-sap サブディレクトリを作成します

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap
sapcc-hana-tst-06:mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

- マルチ・ホスト・システムの場合は '/hana/shared-volume をマウントし ' 各ホストの 'hared' サブディレクトリと 'usr-sap' サブディレクトリを作成します

  以下のコマンド例は、 2+1 のマルチホスト HANA システムを示しています。

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host1
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host2
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host3
sapcc-hana-tst-06:/mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

マウントポイントを作成する

以下の例は、 SID=NF2 の SAP HANA データベースを示しています。

必要なマウントポイントディレクトリを作成するには、次のいずれかの操作を行います。

- シングルホストシステムの場合は、マウントポイントを作成し、データベースホストに権限を設定します。

```
sapcc-hana-tst-06:/ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/shared
sapcc-hana-tst-06:/ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-06:/ # chmod –R 777 /hana/log/NF2
sapcc-hana-tst-06:/ # chmod –R 777 /hana/data/NF2
sapcc-hana-tst-06:/ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:/ # chmod -R 777 /usr/sap/NF2
```

- マルチホストシステムの場合は、マウントポイントを作成し、すべてのワーカーホストとスタンバイホストに権限を設定します。

  以下のコマンド例は、 2+1 のマルチホスト HANA システムを示しています。

  - 1 つ目のワーカーホスト：

```
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/shared
sapcc-hana-tst-06:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:~ # chmod -R 777 /usr/sap/NF2
```

- 2 つ目のワーカーホスト：

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/shared
sapcc-hana-tst-07:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-07:~ # chmod -R 777 /usr/sap/NF2
```

- スタンバイホスト：

```
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/shared
sapcc-hana-tst-08:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-08:~ # chmod -R 777 /usr/sap/NF2
```

ファイルシステムをマウント

NFSのバージョンとONTAP のリリースに応じて、異なるマウントオプションが使用されます。次のファイルシステムをホストにマウントする必要があります。

- 「 /hana/data/sid/mnt0000* 」と入力します
- 「 /hana/log/sid/mnt0000* 」と入力します
- 「 /hana/shared 」
- /usr/sap/SID

次の表に、シングルホスト SAP HANA データベースとマルチホスト SAP HANA データベースのファイルシステムごとに使用する必要がある NFS のバージョンを示します。

| ファイルシステム | **SAP HANA** シングルホスト | **SAP HANA** マルチホスト |
|---|---|---|
| /hana/data/sid/mnt0000* | NFSv3 または NFSv4 | NFSv4 |
| /hana/log/sid/mnt0000* | NFSv3 または NFSv4 | NFSv4 |
| /hana/shared にアクセスします | NFSv3 または NFSv4 | NFSv3 または NFSv4 |
| /usr/sap/SID | NFSv3 または NFSv4 | NFSv3 または NFSv4 |

次の表に、 NFS の各バージョンと ONTAP のリリースのマウントオプションを示します。共通パラメータは、 NFS と ONTAP のバージョンには依存しません。

SAP LaMa では、 /usr/sap/SID ディレクトリをローカルにする必要があります。したがって、 SAP LaMa を使用している場合は、 /usr/sap/SID の NFS ボリュームをマウントしないでください。

NFSv3 では、ソフトウェアまたはサーバに障害が発生した場合に NFS ロックのクリーンアップ処理が行われないようにするため、 NFS ロックをオフにする必要があります。

ONTAP 9 では、 NFS 転送サイズを最大 1MB に設定できます。具体的には、 40GbE 以上でのストレージシステムへの接続では、スループットの期待値を達成するために転送サイズを 1MB に設定する必要があります。

| 共通パラメータ | **NFSv3** | **NFSv4** | **ONTAP 9** での **NFS** 転送サイズ | **ONTAP 8** での **NFS** 転送サイズ |
|---|---|---|---|---|
| rw 、 bg 、 hard 、 timeo = 600 、 noatime 、 | nfsvers = 3、 nolock、 | nfsvers = 4.1、ロック | rsize=1048576 、 wsize=262144 、 | rsize=65536 、 wsize=65536 、 |

NFSv3 の読み取りパフォーマンスを向上させるには、「 nConnect=n 」マウントオプションを使用することを推奨します。このオプションは、 SUSE Linux Enterprise Server 12 SP4 以降および RedHat Enterprise Linux （ RHEL ） 8.3 以降で使用できます。

パフォーマンステストによると、 `nconnect=4` 特にデータボリュームに対して良好な読み取り結果が得られます。ログへの書き込みは、次のようなセッション数が少ないことでメリットが得られる場合があります。 `nconnect=2`。「nConnect」オプションを使用すると、共有ボリュームにもメリットがあります。NFS サーバからの最初のマウント（ IP アドレス）では、使用されるセッションの量が定義されることに注意してください。同じIPアドレスにさらにマウントしても、nConnectに別の値が使用されていても、この値は変更されません。

ONTAP 9.8およびSUSE SLES15SP2以降、またはRed Hat RHEL 8.4以降では、ネットアップはNFSv4.1のnConnectオプションもサポートしています。

nconnectをNFSv4.xで使用する場合は、次のルールに従ってNFSv4.xセッションスロットの数を調整する必要があります。セッションスロットの数は<nconnect value> x 64と等しくなります。ホストでこれを確認し
`echo options nfs max_session_slots=<calculated value> > /etc/modprobe.d/nfsclient.conf`てから再起動します。サーバー側の値も調整する必要があります。で説明されているように、セッションスロットの数を設定します。"NFSv4 の NFS 設定"

/etc/fstab 構成ファイルを使用してシステムのブート中にファイル・システムをマウントするには ' 次の手順を実行します

次の例は、 SID=NF2 で、 NFSv3 を使用し、書き込みの場合は NFS 転送サイズが 1MB 、読み取りの場合は 256K の、シングルホスト SAP HANA データベースを示しています。

1. 必要なファイル・システムを /etc/fstab 構成ファイルに追加します

```
sapcc-hana-tst-06:/ # cat /etc/fstab
<storage-vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data01>:/NF2_shared/usr-sap /usr/sap/NF2 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data01>:/NF2_shared/shared /hana/shared nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
```

2. Run `ount – a を実行して、すべてのホストのファイルシステムをマウントします。

次の例は、 SID=NF2 で、データファイルシステムとログファイルシステムに NFSv4.1 を使用し、「 /hana/shared 」ファイルシステムと「 /usr/sap/nf2 」ファイルシステムに NFSv3 を使用する、マルチホスト SAP HANA データベースを示しています。書き込みでは、読み取りの場合は 1MB 、書き込みの場合は 256K の NFS 転送サイズが使用されます。

1. 必要なファイル・システムを ' すべてのホスト上の /etc/fstab 構成ファイルに追加します



。 `/usr/sap/NF2` ファイルシステムはデータベースホストごとに異なります。次の例は、 `/NF2_shared/usr-sap-host1`。

```
sapcc-hana-tst-06:/ # cat /etc/fstab
<storage-vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-data02>:/NF2_data_mnt00002 /hana/data/NF2/mnt00002 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-log02>:/NF2_log_mnt00002 /hana/log/NF2/mnt00002 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-data02>:/NF2_shared/usr-sap-host1 /usr/sap/NF2 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data02>:/NF2_shared/shared /hana/shared nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
```

2. Run `ount – a を実行して、すべてのホストのファイルシステムをマウントします。

**NFSv4** 用の **SAP HANA** インストールの準備

NFS バージョン 4 以降では、ユーザ認証が必要です。この認証は、 Lightweight Directory Access Protocol （ LDAP ）サーバやローカルユーザアカウントなどの中央ユーザ管理ツールを使用して実行できます。次のセクションでは、ローカルユーザアカウントを設定する方法について説明します。

管理ユーザ <sid>adm,`<sid>crypt`SAP HANAソフトウェアのインストールを開始する前に、SAP HANAホストとストレージコントローラにと `sapsys`グループを手動で作成する必要があります。

**SAP HANA** ホスト

存在しない場合は、 SAP HANA ホストに「 sapsys 」グループを作成する必要があります。ストレージコントローラ上の既存のグループ ID と競合しない一意のグループ ID を選択する必要があります。

ユーザ `<sid>adm`と `<sid>crypt`がSAP HANAホストに作成されます。ストレージコントローラの既存のユーザIDと競合しない一意のIDを選択する必要があります。

マルチホストSAP HANAシステムの場合は、ユーザIDとグループIDがすべてのSAP HANAホストで同じである必要があります。グループとユーザは、および `/etc/passwd`の影響を受ける行をソースシステムから他のすべてのSAP HANAホストにコピーすることで、他のSAP HANAホストに作成され `/etc/group`ます。

NFSv4 ドメインは、すべての Linux サーバ（ /etc/idmapd.conf ）と SVM で同じ値に設定する必要があります。Linux ホストの /etc/idmapd.conf ファイル内の domain パラメータ「 Domain=<domain-name> 」を設定します。

NFS IDMAPD サービスを有効にして開始します。

```
systemctl enable nfs-idmapd.service
systemctl start nfs-idmapd.service
```

最新の Linux カーネルでは、この手順は必要ありません。警告メッセージは無視してかまいません。

ストレージコントローラ

ユーザIDとグループIDは、SAP HANAホストとストレージコントローラで同じである必要があります。グループとユーザは、ストレージクラスタで次のコマンドを入力することで作成されます。

```
vserver services unix-group create -vserver <vserver> -name <group name>
-id <group id>
vserver services unix-user create -vserver <vserver> -user <user name> -id
<user-id> -primary-gid <group id>
```

また、 SVM の UNIX ユーザルートのグループ ID を 0 に設定します。

```
vserver services unix-user modify -vserver <vserver> -user root -primary
-gid 0
```

**SAP HANA** 向けの **I/O** スタック構成

## SAP HANA 1.0 SPS10 以降、 I/O 動作を調整し、使用中のファイルシステムとストレージシステムのデータベースを最適化するためのパラメータが導入されています。

ネットアップは、最適な値を定義するため、パフォーマンステストを実施しました。次の表に、パフォーマンステストから推定した最適な値を示します。

| パラメータ | 価値 |
| --- | --- |
| max_parallel _io_requests と入力します | 128 |
| async _read_submit | オン |
| async ： write_submit_active | オン |
| async_write_submit_bblocks | すべて |

バージョン SPS12 までの SAP HANA 1.0 では、これらのパラメータは、 SAP HANA データベースのインストール時に設定できます。これは、 SAP ノートで説明されています "2267798 ： Configuration of the SAP HANA Database During Installation Using hdbparam 』で説明されています"。

また、パラメータは、 SAP HANA データベースのインストール後に「 hdbparam 」フレームワークを使用して設定することもできます。

```
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_read_submit=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

SAP HANA 2.0 以降 'hdbparam' は廃止され ' パラメータは global.ini` に移動されましたパラメータは、 SQL コマンドまたは SAP HANA Studio を使用して設定できます。詳細については、 SAP ノートを参照してください "2399079 ： HANA で hdbparam の除去 2"。次のテキストに示すように、 global.ini 内でパラメータを設定することもできます。

```
nf2adm@stlrx300s8-6: /usr/sap/NF2/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

SAP HANA 2.0 SPS5 以降、「 setParameter.py 」スクリプトを使用して、正しいパラメータを設定できます。

```
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

**SAP HANA** データボリュームのサイズ

デフォルトでは、 SAP HANA サービスごとに使用されるデータボリュームは 1 つだけです。ファイルシステムの最大ファイルサイズの制限のため、データボリュームの最大サイズを制限することを推奨します。

これを自動的に行うには ' global.ini` の [persistence] セクションで次のパラメータを設定します

```
datavolume_striping = true
datavolume_striping_size_gb = 8000
```

これにより、 8 、 000GB の上限に達すると、新しいデータボリュームが作成されます。 "SAP ノート 240005 の質問 15 を参照してください" 詳細については ' を参照してください

**SAP HANA** ソフトウェアのインストール

## SAP HANA のソフトウェアインストールの要件は次のとおりです。

シングルホストシステムにインストールします

SAP HANA ソフトウェアのインストールでは、シングルホストシステムについて行う追加の準備作業はありません。

マルチホストシステムにをインストールします

マルチホストシステムに SAP HANA をインストールするには、次の手順を実行します。

1. SAPインストールツールを使用して `hdbclm`、いずれかのワーカーホストで次のコマンドを実行してインストールを開始します。オプションを使用し `addhosts`て(`sapcc-hana-tst-03`、2番目のワーカーとスタンバイホストを追加し(`sapcc-hana-tst-04`ます）。

```
apcc-hana-tst-02:/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_LCM_LINUX_X86_64 #
./hdblcm --action=install --addhosts=sapcc-hana-tst-03:role=worker,sapcc
-hana-tst-04:role=standby

SAP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
```

```
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1
(1.015.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip


SAP HANA Database version '2.00.073.00.1695288802' will be installed.
```

```
Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------
-------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version
2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
  9     | epmmds          | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
4.203.2321.0.0

Enter comma-separated list of the selected indices [3,4]: 2,3
```

2. 選択したすべてのコンポーネントが、すべてのワーカーホストとスタンバイホストにインストールされていることを確認します。

データボリュームのパーティションを追加しています

SAP HANA 2.0 SPS4 以降では、追加のデータボリュームパーティションを設定できます。これにより、 SAP HANA テナントデータベースのデータボリュームに 2 つ以上のボリュームを構成することができます。単一ボリュームのサイズやパフォーマンスの制限を超えて拡張することもできます。

> データボリュームに 2 つ以上の個別のボリュームを使用すると、 SAP HANA のシングルホストシステムとマルチホストシステムを使用できます。データボリュームのパーティションはいつでも追加できますが、追加するには SAP HANA データベースの再起動が必要になる場合があります。

追加のデータボリュームパーティションの有効化

1. 追加のデータボリュームパーティションを有効にするには、 SYSTEMDB 構成の SAP HANA Studio または Cockpit を使用して、 global.ini` 内に次のエントリを追加します。

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

パラメータを global.ini` ファイルに手動で追加するには ' データベースを再起動する必要があります

#### シングルホスト **SAP HANA** システムのボリューム構成

複数のパーティションを持つシングルホスト SAP HANA システムのボリュームレイアウトは、 1 つのデータボリュームパーティションを含むシステムのレイアウトに似ていますが、追加のデータボリュームは、ログボリュームとその他のデータボリュームとして別のアグリゲートに格納されます。次の表は、 2 つのデータボリュームパーティションを持つ SAP HANA シングルホストシステムの構成例を示しています。

| コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **b** のアグリゲート **2** |
|---|---|---|---|
| データボリューム： SID_data_mnt00001 | 共有ボリューム： SID_shared | データボリューム： SID_data2_mnt00001 | ログボリューム： SID_log_mnt00001 |

次の表に、 2 つのデータボリュームパーティションを持つシングルホストシステムのマウントポイント構成の例を示します。

| ジャンクションパス | ディレクトリ | **HANA** ホストのマウントポイント |
|---|---|---|
| SID_data_mnt00001 | – | /hana/data/SID/mnt00001 |
| SID_data2_mnt00001 | – | /hana/data2/SID/mnt00001 |
| SID_log_mnt00001 | – | /hana/log/sid/mnt00001 |
| SID_shared | usr - SAP 共有 | /usr/sap/SID/hana/shared に格納されています |

新しいデータボリュームを作成し、 ONTAP System Manager または ONTAP クラスタのコマンドラインインターフェイスを使用してネームスペースにマウントします。

#### マルチホスト **SAP HANA** システムのボリューム構成

複数のパーティションを持つマルチホスト SAP HANA システムのボリュームレイアウトは、 1 つのデータボリュームパーティションを含むシステムのレイアウトに似ていますが、追加のデータボリュームは、ログボリュームとその他のデータボリュームとして別のアグリゲートに格納されます。次の表は、 2 つのデータボリュームパーティションを持つ SAP HANA マルチホストシステムの構成例を示しています。

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| ノード 1 のデータボリュームとログボリューム | データボリューム： SID_data_mnt00001 | – | ログボリューム： SID_log_mnt00001 | data2 ボリューム： SID_data2_mnt00001 |

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| ノード 2 のデータボリュームとログボリューム | ログボリューム：SID_log_mnt00002 | data2 ボリューム：SID_data2_mnt00002 | データボリューム：SID_data_mnt00002 | – |
| ノード 3 のデータボリュームとログボリューム | – | データボリューム：SID_data_mnt00003 | data2 ボリューム：SID_data2_mnt00003 | ログボリューム：SID_log_mnt00003 |
| ノード 4 のデータボリュームとログボリューム | data2 ボリューム：SID_data2_mnt00004 | ログボリューム：SID_log_mnt00004 | – | データボリューム：SID_data_mnt00004 |
| すべてのホストの共有ボリューム | 共有ボリューム：SID_shared | – | – | – |

次の表に、 2 つのデータボリュームパーティションを持つシングルホストシステムのマウントポイント構成の例を示します。

| ジャンクションパス | ディレクトリ | **SAP HANA** ホストのマウントポイント | 注 |
|---|---|---|---|
| SID_data_mnt00001 | – | /hana/data/SID/mnt00001 | すべてのホストにマウントされています |
| SID_data2_mnt00001 | – | /hana/data2/SID/mnt00001 | すべてのホストにマウントされています |
| SID_log_mnt00001 | – | /hana/log/sid/mnt00001 | すべてのホストにマウントされています |
| SID_data_mnt00002 | – | /hana/data/sid/mnt00002 | すべてのホストにマウントされています |
| SID_data2_mnt00002 | – | /hana/data2/SID/mnt00002 | すべてのホストにマウントされています |
| SID_log_mnt00002 | – | /hana/log/sid/mnt00002 | すべてのホストにマウントされています |
| SID_data_mnt00003 | – | /hana/data/sid/mnt00003 | すべてのホストにマウントされています |
| SID_data2_mnt00003 | – | /hana/data2/SID/mnt00003 | すべてのホストにマウントされています |
| SID_log_mnt00003 | – | /hana/log/sid/mnt00003 | すべてのホストにマウントされています |
| SID_data_mnt00004 | – | /hana/data/sid/mnt00004 | すべてのホストにマウントされています |
| SID_data2_mnt00004 | – | /hana/data2/SID/mnt00004 | すべてのホストにマウントされています |
| SID_log_mnt00004 | – | /hana/log/sid/mnt00004 | すべてのホストにマウントされています |

| ジャンクションパス | ディレクトリ | **SAP HANA** ホストのマウントポイント | 注 |
|---|---|---|---|
| SID_shared | 共有 | /hana/shared-SID を指定します | すべてのホストにマウントされています |
| SID_shared | usr-sap-host1 | /usr/sap/SID | ホスト 1 にマウントされています |
| SID_shared | usr-sap-host2 | /usr/sap/SID | ホスト 2 にマウントされています |
| SID_shared | usr-sap-host3 | /usr/sap/SID | ホスト 3 にマウント |
| SID_shared | usr-sap-host4 | /usr/sap/SID | ホスト 4 にマウント |
| SID_shared | usr-sap-host5 | /usr/sap/SID | ホスト 5 にマウント |

新しいデータボリュームを作成し、 ONTAP System Manager または ONTAP クラスタのコマンドラインインターフェイスを使用してネームスペースにマウントします。

ホストの設定

セクションで説明するタスクに加えて、"「ホストのセットアップ」"新しい追加データボリューム用の追加のマウントポイントとfstabエントリを作成し、新しいボリュームをマウントする必要があります。

1. 追加のマウントポイントを作成します。
   - シングルホストシステムの場合は、マウントポイントを作成し、データベースホストに権限を設定します。

```
sapcc-hana-tst-06:/ # mkdir -p /hana/data2/SID/mnt00001
sapcc-hana-tst-06:/ # chmod –R 777 /hana/data2/SID
```

   - マルチホストシステムの場合は、マウントポイントを作成し、すべてのワーカーホストとスタンバイホストに権限を設定します。以下のコマンド例は、 2+1 のマルチホスト HANA システムを示しています。
     - 1 つ目のワーカーホスト：

```
sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00002
sapcc-hana-tst-06:~ # chmod -R 777 /hana/data2/SID
```

     - 2 つ目のワーカーホスト：

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
```

- スタンバイホスト：

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
```

2. すべてのホスト上の /etc/fstab 構成ファイルに追加のファイル・システムを追加しますNFSv4.1 を使用するシングルホストシステムの例を次に示します。

```
<storage-vif-data02>:/SID_data2_mnt00001 /hana/data2/SID/mnt00001 nfs
rw,vers=4,
minorversion=1,hard,timeo=600,rsize=1048576,wsize=262144,bg,noatime,lock
0 0
```

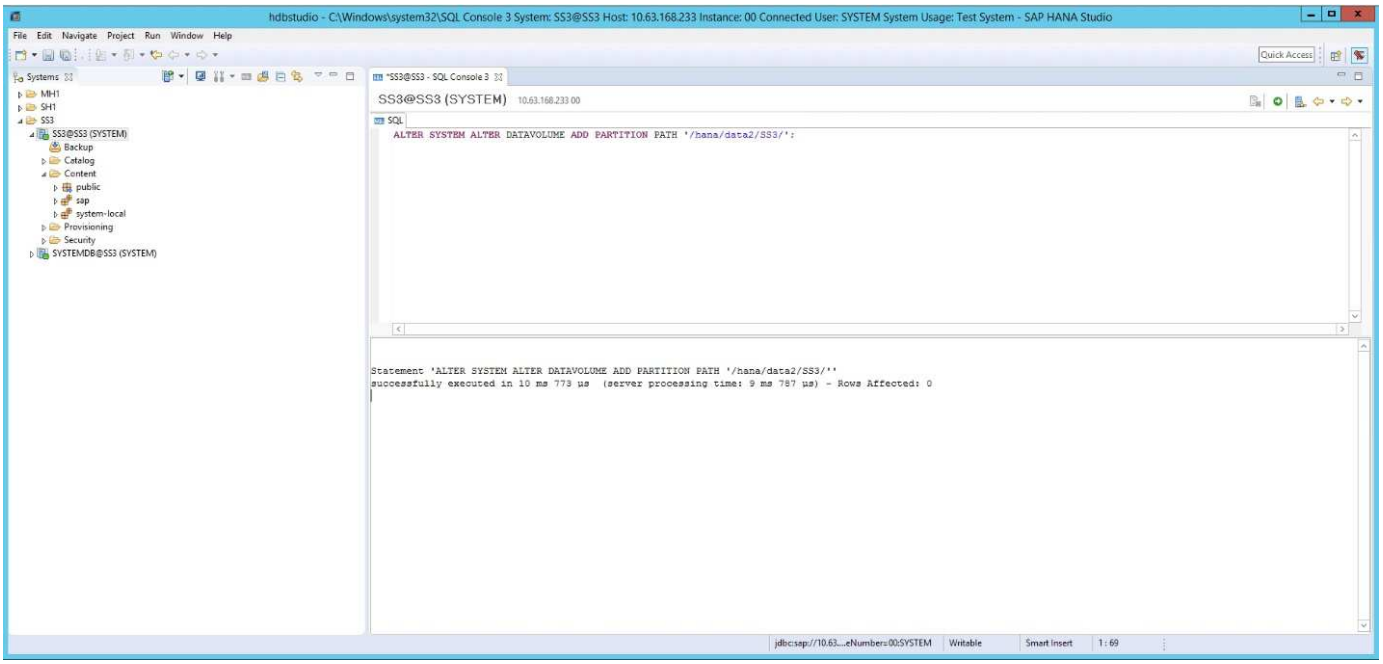
ボリュームごとに異なる TCP セッションを使用するために、各データボリュームへの接続には異なる SVM 仮想インターフェイスを使用します。nConnect マウントオプションが OS で使用可能な場合は、そのオプションを使用することもできます。

3. ファイルシステムをマウントするには、「 mount – a 」コマンドを実行します。

データボリュームパーティションを追加しています

テナントデータベースに対して次の SQL ステートメントを実行し、テナントデータベースにデータボリュームパーティションを追加します。追加のボリュームへのパスを使用：

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```



## 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。

- "SAP HANA ソフトウェアソリューション"
- "TR-4646 ：『 SAP HANA Disaster Recovery with Storage Replication 』"
- "TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"
- "TR-4667：『Automating SAP System Copies Using the SnapCenter SAP HANA Plug-in』"
- ネットアップドキュメントセンター

  "https://www.netapp.com/support-and-training/documentation/"

- SAP HANA 向け SAP 認定エンタープライズストレージハードウェア

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"

- SAP HANA のストレージ要件

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"

- 『 SAP HANA Tailored Data Center Integration Frequently Asked Questions 』

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"

- SAP HANA on VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"

- 『SAP HANA on VMware vSphere Best Practices Guide』

  "https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

## 履歴を更新します

この解決策の初版以降には、次の技術的な変更が加えられています。

| 日付 | 概要を更新します |
| --- | --- |
| 2014年4月 | 初版 |
| 2014年8月 | ディスクサイジングの選択を更新し、 SSD 構成を追加しました Red Hat Enterprise Linux OS 構成を追加 SAP HANA ストレージコネクタ情報を追加しました VMware 構成に関する情報を追加しました |
| 2014年11月 | ストレージのサイジングに関するセクションを更新しました |
| 2015年1月 | ストレージコネクタの API セクションが更新され、アグリゲートとボリュームの構成が更新されました |

| 日付 | 概要を更新します |
| --- | --- |
| 2015年3月 | SAP HANA SPS9 向けの新しい StorageGRID の実装に関するセクション、コンピューティングノードのセットアップと HANA のインストールのセクションを追加しました |
| 2015年10月 | clustered ONTAP では、 SAP HANA および HWVAL > SPS10 の I/O パラメータを追加し、 sysctl パラメータを更新しました |
| 2016年3月 | 容量のサイジングを更新し、 /hana/shared のマウントオプションを更新した sysctl パラメータを更新 |
| 2017年2月 | 新しいネットアップストレージシステムとディスクシェルフ 40GbE に対応した ONTAP 9 の新機能新しい OS リリース（ SUSE Linux Enterprise Server12 SP1 と Red Hat Enterprise Linux 7.2 ）新しい SAP HANA リリース |
| 2017年7月 | マイナーアップデート |
| 2018年9月 | 新しいネットアップストレージシステム新しい OS リリース（ SUSE Linux Enterprise Server 12 SP3 および Red Hat Enterprise Linux 7.4 ）では、 SAP HANA 2.0 SPS3 のマイナーな変更が追加されています |
| 2019 年 9 月 | 新しい OS リリース（ SUSE Linux Enterprise Server 12 SP4 、 SUSE Linux Enterprise Server 15 、および Red Hat Enterprise Linux 7.6 ）では、 MAX Data ボリュームサイズが若干変更されています |
| 2019年12月 | 新しいネットアップストレージシステム新しい OS リリース SUSE Linux Enterprise Server 15 SP1 |
| 2020年3月 | NFSv3 で nConnect がサポートされるようになりました。新しい OS リリースである Red Hat Enterprise Linux 8 がサポートされます |
| 2020年5月 | SAP HANA 2.0 SPS4 以降に複数のデータパーティション機能が導入されています |
| 2020 年 6 月 | 追加情報オプションの機能に関するマイナーアップデート |
| 2020年12月 | ONTAP 9.8 以降で NConnect for NFSv4.1 がサポートされるようになりました。新しいオペレーティングシステムがリリースされました |
| 2021年2月 | ホストのネットワーク設定の変更やその他の軽微な変更 |
| 2021年4月 | VMware vSphere 固有の情報を追加しました |
| 2022年9月 | 新しいOS -リリース |
| 2023年12月 | ホストセットアップの更新：nconnectの設定が改訂され、NFSv4.1セッションに関する情報が追加されました。 |
| 2024年9月 | 新しいストレージシステムとマイナーアップデート |
| 2025年2月 | 新しいストレージシステム |
| 2025年7月 | マイナーアップデート |

# 『 SAP HANA on FAS Systems with FCP Configuration Guide 』を参照してください

# 『SAP HANA on NetApp FAS Systems with Fibre Channel Protocol』構成ガイド

NetApp FAS 製品ファミリは、TDI プロジェクトで SAP HANA と併用することが認定されています。このガイドでは、FCP のこのプラットフォームでの SAP HANA のベストプラクティスについて説明します。

Marco Schoen 、ネットアップ

認定は、次のモデルで有効です。

- FAS2750、FAS2820、FAS8300、FAS50、FAS8700、 FAS70、FAS9500、FAS90

SAP HANA 向けのネットアップ認定ストレージソリューションの一覧については、を参照してください "認定およびサポートされている SAP HANA ハードウェアディレクトリ"。

本ドキュメントでは、 Fibre Channel Protocol （ FCP ；ファイバチャネルプロトコル）を使用した FAS 構成について説明します。

> このホワイトペーパーで説明している構成は、 SAP HANA に必要な SAP HANA KPI と、 SAP HANA に最適なパフォーマンスを達成するために必要です。ここに記載されていない設定を変更したり、機能を使用したりすると、パフォーマンスが低下したり、予期しない動作が発生したりする可能性があります。変更を実施するのは、ネットアップのサポートから助言さ

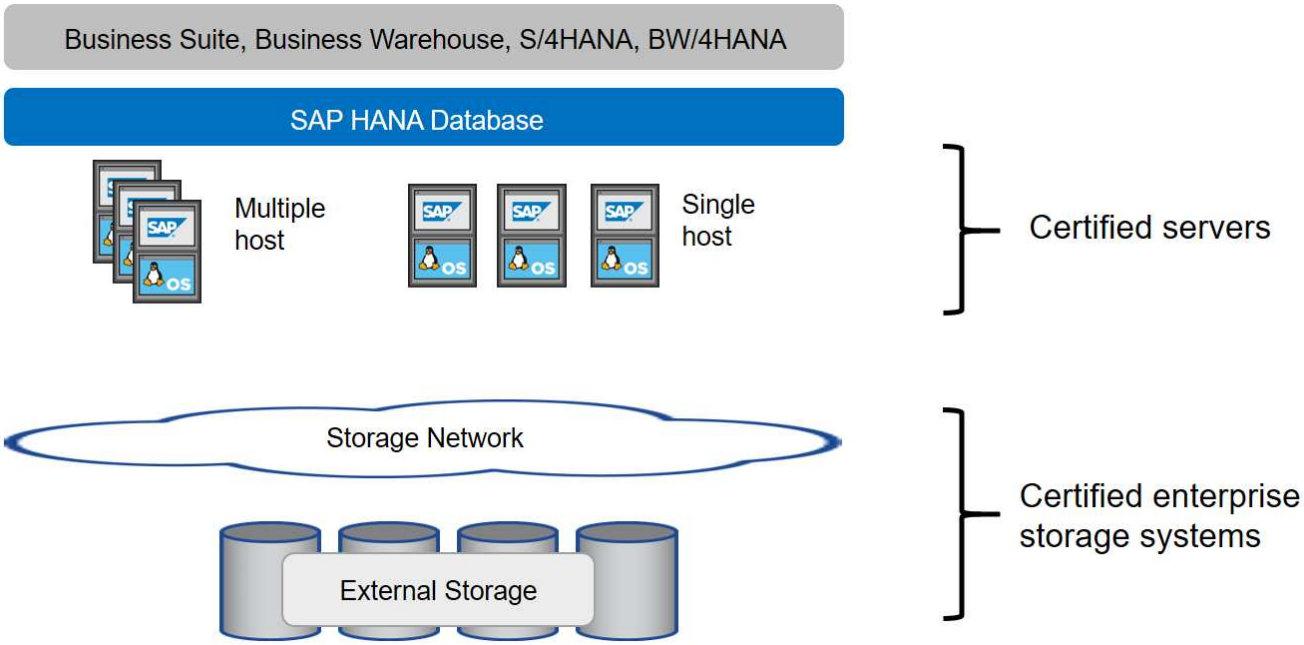
NFS システムと NetApp AFF システムを使用する FAS システムの構成ガイドは、次のリンクから入手できます。

- "FCP 搭載の NetApp AFF システム上の SAP HANA"
- "FCP 搭載の NetApp ASA システム上の SAP HANA"
- "NFS を使用した NetApp FAS システムでの SAP HANA"
- "NFS を使用した NetApp AFF システムでの SAP HANA"

SAP HANA マルチホスト環境では、 SAP HANA ホストのフェイルオーバー時にフェンシングを提供するために、標準の SAP HANA ストレージコネクタが使用されます。オペレーティングシステムの構成ガイドラインと、 HANA 固有の Linux カーネルの依存関係については、該当する SAP ノートを参照してください。詳細については、を参照してください "SAP Note 2235581 – SAP HANA Supported Operating Systems 』"。

### SAP HANA テーラードデータセンター統合

NetApp FAS ストレージコントローラは、 NFS （ NAS ）プロトコルとファイバチャネル（ SAN ）プロトコルを使用した、 SAP HANA の TDI プログラムで認定されています。これらは、シングルホスト構成またはマルチホスト構成の SAP Business Suite on HANA 、 S/4HANA 、 BW/4HANA 、 SAP Business Warehouse on HANA など、任意の SAP HANA シナリオに導入できます。SAP HANA での使用が認定されているサーバは、認定ストレージの解決策と組み合わせることができます。アーキテクチャの概要については、次の図を参照してください。




生産性の高いSAP HANAシステムを実現するための前提条件と推奨事項の詳細については、次のリソースを参照してください。

- "『 SAP HANA Tailored Data Center Integration Frequently Asked Questions 』"

**VMware vSphere** を使用した **SAP HANA**

ストレージを仮想マシン（ VM ）に接続する方法はいくつかあります。推奨される方法は、ストレージボリュームと NFS をゲストオペレーティングシステムから直接接続することです。このオプションについては、を"NFS を使用した NetApp AFF システムでの SAP HANA"参照してください。

raw デバイスマッピング（ RDM ）、 FCP データストア、または FCP を使用する VVol データストアもサポートされます。どちらのデータストアオプションも、本番環境で使用するためにデータストアに格納する SAP HANA データボリュームまたはログボリュームは 1 つだけです。

SAP HANA での vSphere の使用の詳細については、次のリンクを参照してください。

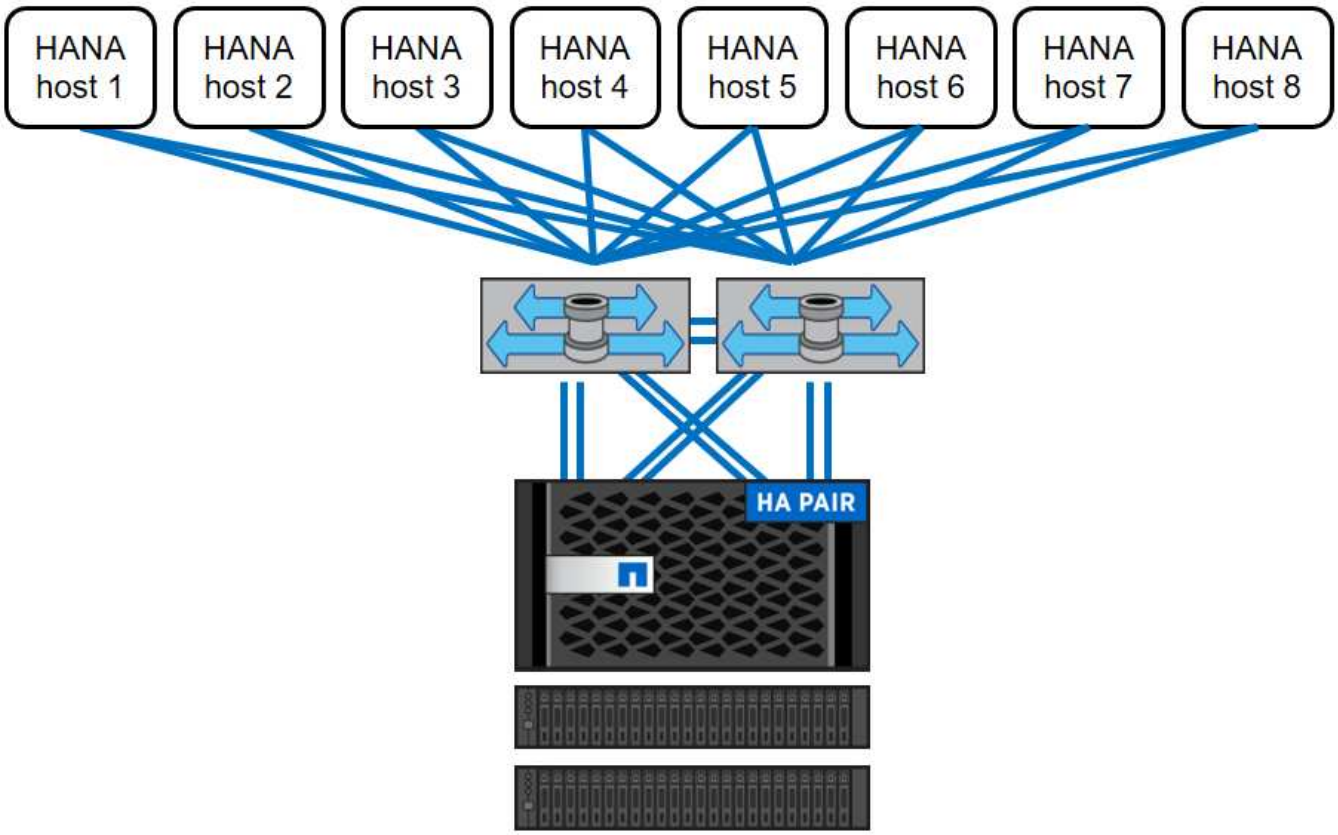
- "SAP HANA on VMware vSphere - 仮想化 - コミュニティ Wiki"
- "『SAP HANA on VMware vSphere Best Practices Guide』"
- "2161991 - VMware vSphere 設定ガイドライン - SAP One Support Launchpad （ログインが必要）"

## アーキテクチャ

SAP HANA ホストは、冗長 FCP インフラとマルチパスソフトウェアを使用してストレージコントローラに接続されます。スイッチまたはホストバスアダプタ（ HBA ）で障害が発生した場合に、耐障害性に優れた SAP HANA ホスト / ストレージ接続を実現するには、冗長 FCP スイッチインフラが必要です。すべての HANA ホストがストレージコントローラ上の必要な LUN にアクセスできるように、スイッチで適切なゾーニングを設定する必要があります。

ストレージレイヤでは、 FAS 製品ファミリーのさまざまなモデルを使用できます。ストレージに接続される SAP HANA ホストの最大数は、 SAP HANA のパフォーマンス要件によって定義されます。必要なディスクシェルフの数は、 SAP HANA システムの容量とパフォーマンスの要件によって決まります。

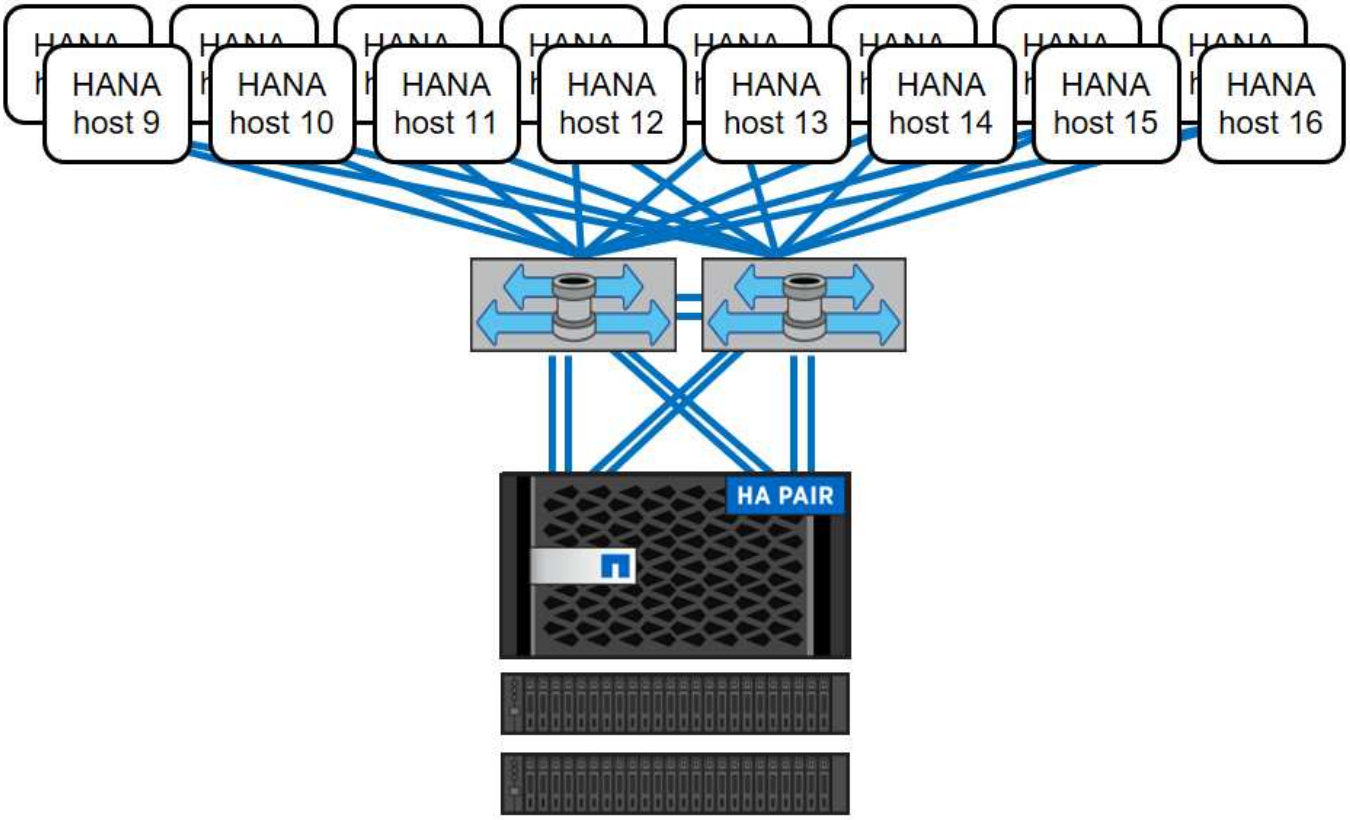
次の図は、 8 台の SAP HANA ホストをストレージ HA ペアに接続した構成例を示しています。



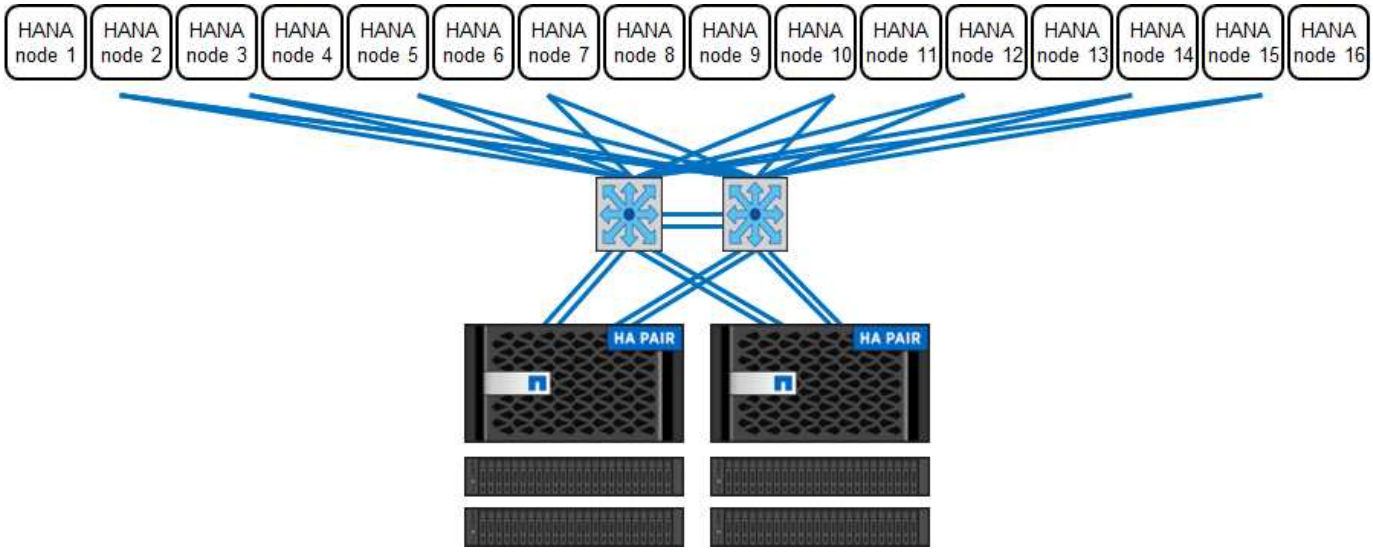

このアーキテクチャは、次の 2 つの側面で拡張できます。

- ストレージコントローラが新しい負荷の下で十分なパフォーマンスを提供し、主要なパフォーマンス指標（ KPI ）を満たすことができると仮定して、 SAP HANA ホストとディスク容量をストレージに追加で接続する。
- 追加の SAP HANA ホスト用にストレージシステムとディスク容量を追加する

次の図は、追加の SAP HANA ホストをストレージコントローラに接続した場合の構成例を示しています。この例では、 16 台の SAP HANA ホストの容量とパフォーマンスの要件を満たすために、さらにディスクシェルフが必要です。合計スループット要件に応じて、ストレージコントローラへの FC 接続を追加する必要があります。




導入した FAS システムストレージモデルに関係なく、次の図に示すように、ストレージコントローラを追加することで SAP HANA 環境を拡張することもできます。




**SAP HANA** のバックアップ

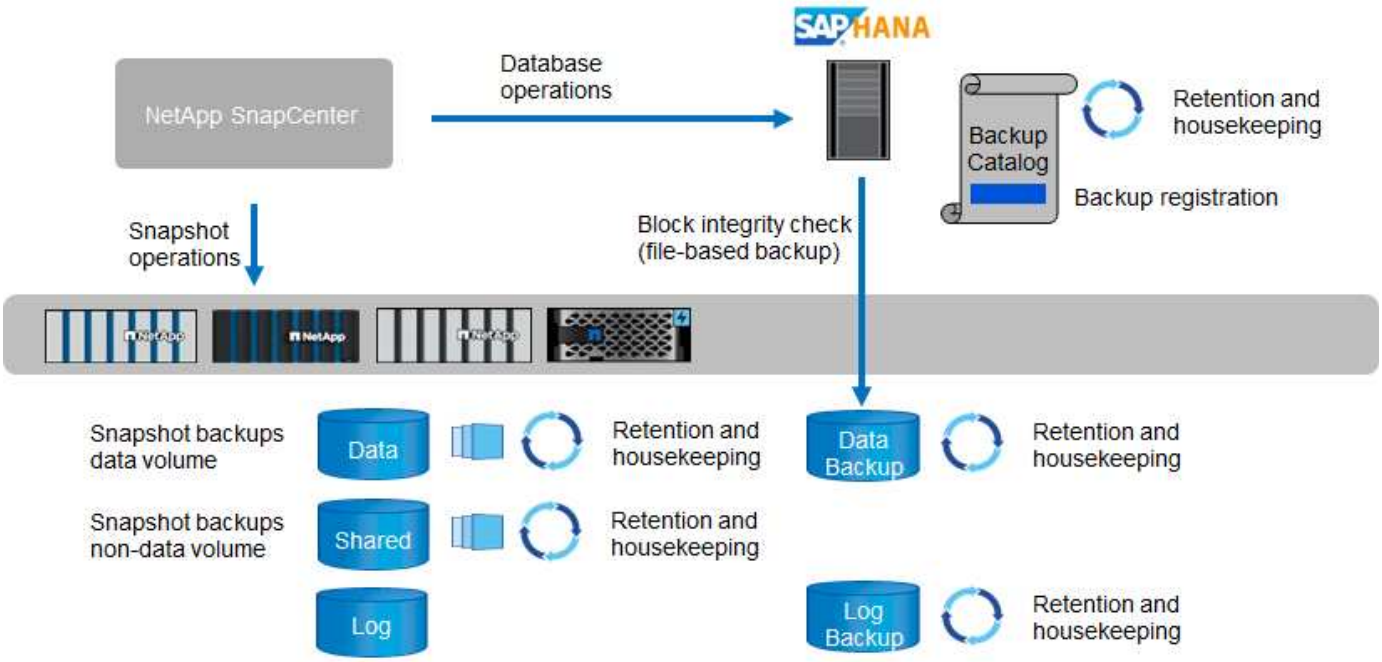
NetApp ONTAP ソフトウェアには、 SAP HANA データベースをバックアップするための組み込みメカニズムが用意されています。ストレージベースの Snapshot バックアップは、 SAP HANA のシングルコンテナシステムや SAP HANA MDC のシングルテナントシステムで使用可能な、完全にサポートされた統合バックアップ解決策です。

ストレージベースの Snapshot バックアップは、 NetApp SnapCenter Plug-in for SAP HANA を使用して実装

されます。このプラグインは、 SAP HANA データベースのインターフェイスを使用して、一貫したストレージベースの Snapshot バックアップを実現します。SnapCenter を使用すると、 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、 SAP HANA Studio 内で参照したり、リストアやリカバリ処理用に選択できるようになります。

NetApp SnapVault ソフトウェアを使用すると、プライマリストレージに作成された Snapshot コピーを、SnapCenter で制御されるセカンダリバックアップストレージにレプリケートできます。プライマリストレージ上のバックアップとセカンダリストレージ上のバックアップには、異なるバックアップ保持ポリシーを定義できます。SnapCenter Plug-in for SAP HANA Database は、 Snapshot コピーベースのデータバックアップとログバックアップの保持について、不要なバックアップカタログの削除も含めて管理します。SnapCenter Plug-in for SAP HANA Database は、ファイルベースのバックアップを実行することで、 SAP HANA データベースのブロック整合性チェックの実行も可能にします。

次の図に示すように、 NFS マウントを使用して、データベースログをセカンダリストレージに直接バックアップできます。




ストレージベースの Snapshot バックアップは、ファイルベースのバックアップに比べて大きなメリットをもたらします。たとえば、次のような利点があります。

- 高速バックアップ（数分）
- ストレージレイヤでの高速リストア（数分）
- バックアップ中、 SAP HANA データベースホスト、ネットワーク、またはストレージのパフォーマンスが影響を受けることはありません
- ブロックの変更に基づいて、スペース効率と帯域幅効率に優れたセカンダリストレージへのレプリケーションを実行します

SnapCenterを使用したSAP HANAバックアップ/リカバリ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-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"。

## SAP HANA ディザスタリカバリ

SAP HANA ディザスタリカバリは、 SAP システムレプリケーションを使用してデータベースレイヤで実行するか、ストレージレプリケーションテクノロジを使用してストレージレイヤで実行できます。次のセクションでは、ストレージレプリケーションに基づくディザスタリカバリソリューションの概要について説明します。

SnapCenterを使用したSAP HANAディザスタリカバリ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-4646 ：『 SAP HANA Disaster Recovery with Storage Replication 』"。

### SnapMirror に基づくストレージレプリケーション

次の図は、同期 SnapMirror レプリケーションを使用してローカル DR データセンターにデータをレプリケートし、非同期 SnapMirror を使用してリモート DR データセンターにデータをレプリケートする、 3 サイトのディザスタリカバリ解決策を示しています。

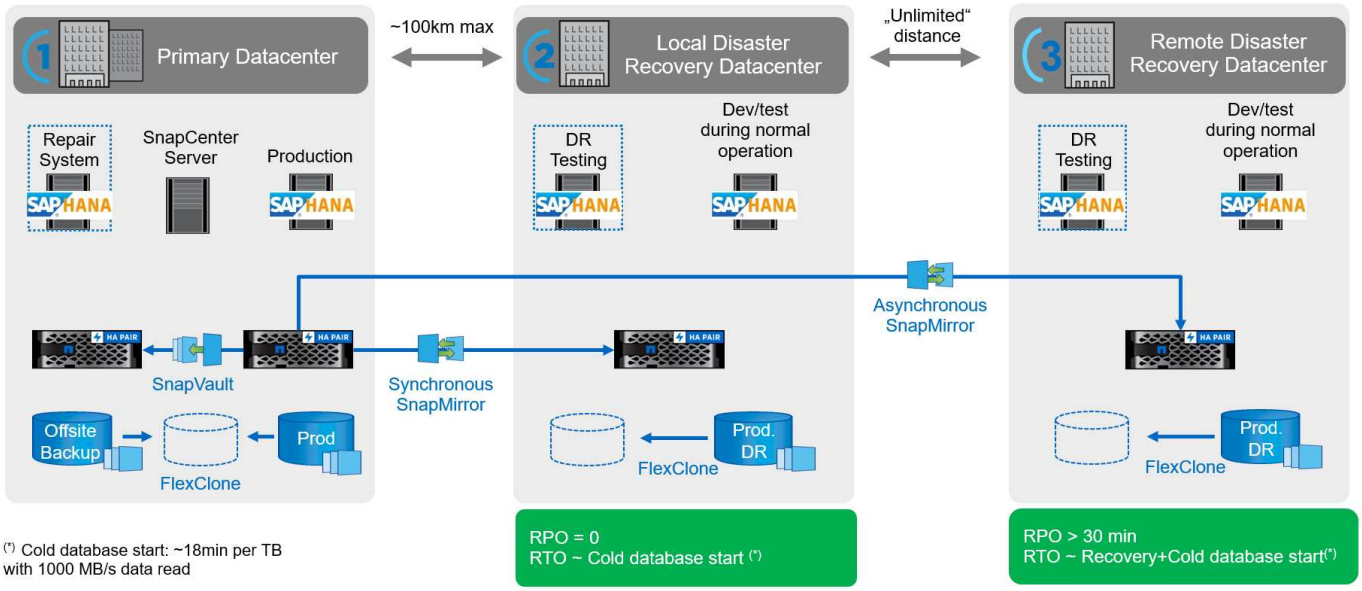
同期 SnapMirror を使用したデータレプリケーションでは、 RPO がゼロになります。プライマリデータセンターとローカル DR データセンター間の距離は約 100km です。

非同期 SnapMirror を使用して、プライマリとローカルの両方の DR サイトで障害が発生した場合のデータ保護を実行します。RPO は、レプリケーションの更新頻度と転送速度によって異なります。理論的には距離は無制限ですが、転送が必要なデータ量とデータセンター間の接続によって制限は異なります。通常の RPO の値は、 30 分から数時間です。

どちらのレプリケーション方法の RTO も、主に DR サイトで HANA データベースを起動してメモリにロードするのに必要な時間に左右されます。1000Mbps のスループットでデータが読み取られることを前提とし、1TB のデータをロードするには約 18 分かかります。

DR サイトのサーバは、通常運用時に開発 / テストシステムとして使用できます。災害が発生した場合は、開発 / テスト用システムをシャットダウンし、 DR 本番用サーバとして起動する必要があります。

どちらのレプリケーション方法でも、 RPO と RTO に影響を与えることなく DR ワークフローテストを実行できます。FlexClone ボリュームはストレージ上に作成され、 DR テストサーバに接続されます。

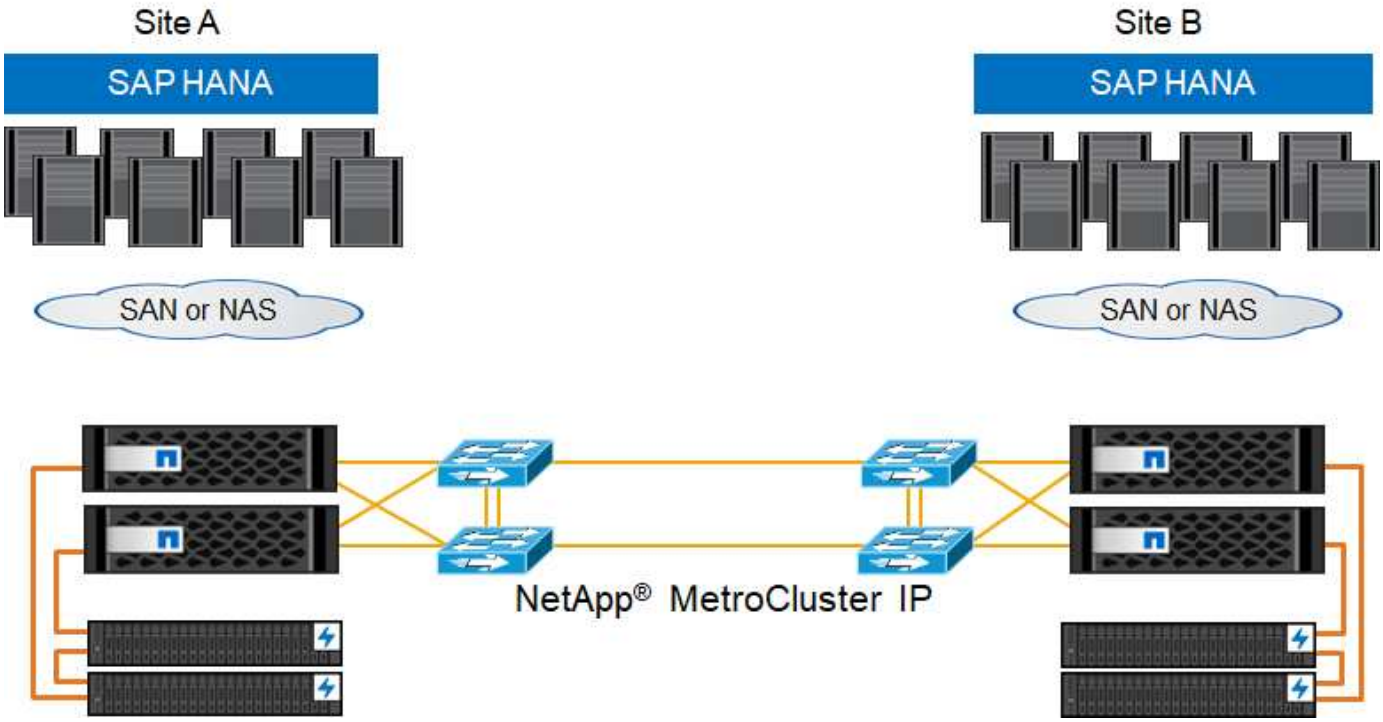



同期レプリケーションで StrictSync モードが提供されます。何らかの理由でセカンダリストレージへの書き込みが完了しないと、アプリケーション I/O が失敗し、プライマリストレージシステムとセカンダリストレージ

システムが同一になります。プライマリへのアプリケーション I/O は、 SnapMirror 関係のステータスが InSync に戻るまで再開されません。プライマリストレージで障害が発生した場合は、フェイルオーバー後にデータ損失なしでアプリケーション I/O をセカンダリストレージで再開できます。StrictSync モードでは、RPO は常にゼロです。

#### NetApp MetroCluster に基づくストレージレプリケーション

次の図は、解決策の概要を示しています。各サイトのストレージクラスタは、ローカルで高可用性を実現し、本番環境のワークロードに使用されます。各サイトのデータはもう一方のサイトに同期的にレプリケートされ、災害のフェイルオーバー時に使用できます。




## ストレージのサイジング

次のセクションでは、 SAP HANA 用のストレージシステムのサイジングに関するパフォーマンスと容量に関する考慮事項の概要を説明します。

ストレージのサイジングプロセスをサポートし、適切なサイズのストレージ環境を構築するには、ネットアップまたはネットアップパートナーの営業担当者にお問い合わせください。

### パフォーマンスに関する考慮事項

SAP では、ストレージ KPI の静的なセットが定義されています。これらの KPI は、データベースホストのメモリサイズや SAP HANA データベースを使用するアプリケーションに関係なく、すべての SAP HANA 本番環境に対して有効です。これらの KPI は、シングルホスト環境、マルチホスト環境、 Business Suite on HANA 環境、 Business Warehouse on HANA 環境、 S/4HANA 環境、および BW/4HANA 環境で有効です。したがって、現在のパフォーマンスサイジングアプローチは、ストレージシステムに接続されているアクティブな SAP HANA ホストの数にのみ依存します。

ストレージパフォーマンス KPI は、本番用 SAP HANA システムにのみ必要です。

SAP はパフォーマンステストツールを提供します。このツールは、ストレージに接続されたアクティブな SAP HANA ホストのストレージパフォーマンスを検証するために使用する必要があります。

ネットアップは、特定のストレージモデルに接続できる SAP HANA ホストの最大数をテストして事前に定義しました。さらに、本番環境ベースの SAP HANA システムに必要なストレージ KPI を実現しています。

> 認定 FAS 製品ファミリーのストレージコントローラは、ネットアップがサポートし、 SAP HANA TDI パフォーマンス KPI を達成していれば、他のディスクタイプやディスクバックエンドソリューションと SAP HANA の両方に使用することもできます。たとえば、 NetApp Storage Encryption （ NSE ）や NetApp FlexArray テクノロジなどです。

本ドキュメントでは、 SAS ハードディスクドライブおよびソリッドステートドライブのディスクサイジングについて説明します。

### ハードディスクドライブ

SAP のストレージパフォーマンス KPI を実現するには、 SAP HANA ノードごとに 10 本以上のデータディスク（ 10k rpm SAS ）が必要です。

> この計算は、使用するストレージコントローラとディスクシェルフには依存しません。

### ソリッドステートドライブ

ソリッドステートドライブ（ SSD ）の場合、データディスクの数は、ストレージコントローラから SSD シェルフへの SAS 接続スループットによって決まります。

ディスクシェルフで実行できる SAP HANA ホストの最大数と、 SAP HANA ホストごとに必要な SSD の最小数は、 SAP パフォーマンステストツールを実行して決定されています。

- SSD を 24 本搭載した 12Gb SAS ディスクシェルフ（ DS224C ）は、ディスクシェルフが 12Gb に接続される場合、最大 14 台の SAP HANA ホストをサポートします。
- SSD を 24 本搭載した 6Gb SAS ディスクシェルフ（ DS2246 ）は、最大 4 台の SAP HANA ホストをサポートします。

SSD と SAP HANA ホストは、両方のストレージコントローラ間で均等に分散する必要があります。

次の表に、ディスクシェルフごとにサポートされる SAP HANA ホストの数を示します。

| | **24** 本の **SSD** をフル搭載した **6Gb SAS** シェルフ（ **DS2246** | **12Gb SAS** シェルフ（ **DS224C** ）には **24** 本の **SSD** がフル搭載されています |
|---|---|---|
| ディスクシェルフあたりの SAP HANA ホストの最大数 | 4. | 14 |

> この計算は、使用しているストレージコントローラには依存しません。ディスクシェルフを追加しても、ストレージコントローラでサポートできる SAP HANA ホストの最大数は増加しません。

**NS224 NVMe** シェルフ

1本のNVMe SSD（データ）は、最大2台のSAP HANAホストをサポートします。SSDとSAP HANAホストは、両方のストレージコントローラ間で均等に分散する必要があります。

### 混在ワークロード

SAP HANA とその他のアプリケーションワークロードを、同じストレージコントローラ上または同じストレージアグリゲート内で実行することはできません。ただし、ネットアップのベストプラクティスとして、SAP HANA ワークロードを他のすべてのアプリケーションワークロードから分離することを推奨します。

SAP HANA ワークロードとその他のアプリケーションワークロードを、同じストレージコントローラまたは同じアグリゲートに導入することもできます。その場合は、混在ワークロード環境内の SAP HANA に対して十分なパフォーマンスが常に確保されていることを確認する必要があります。また、 Quality of Service （ QoS ；サービス品質）パラメータを使用して、 SAP HANA アプリケーションに対する他のアプリケーションの影響を制御することも推奨します。

SAP HCMT テストツールを使用して、他のワークロードにすでに使用されているストレージコントローラで追加の SAP HANA ホストを実行できるかどうかを確認する必要があります。ただし、 SAP アプリケーションサーバは、 SAP HANA データベースと同じストレージコントローラおよびアグリゲートに安全に配置できます。

### 容量に関する考慮事項

SAP HANA の容量要件の詳細な概要については、を参照してください "SAP ノート 1900823" ホワイトペーパー。

> 複数の SAP HANA システムで構成される SAP 環境全体の容量サイジングは、ネットアップの SAP HANA ストレージサイジングツールを使用して決定する必要があります。ストレージのサイジングプロセスを検証し、適切なサイズのストレージ環境を構築するには、ネットアップまたはネットアップパートナーの営業担当者にお問い合わせください。

### パフォーマンステストツールの設定

SAP HANA 1.0 SPS10 以降、 I/O 動作を調整し、使用中のファイルシステムとストレージシステムのデータベースを最適化するためのパラメータが導入されています。SAP のテストツールを使用してストレージパフォーマンスをテストする場合は、 SAP のパフォーマンステストツール（ fsperf ）にもこれらのパラメータを設定する必要があります。

ネットアップは、最適な値を定義するためにパフォーマンステストを実施しました。次の表に、 SAP テストツールの構成ファイルで設定する必要があるパラメータを示します。

| パラメータ | 価値 |
| --- | --- |
| max_parallel _io_requests と入力します | 128 |
| async _read_submit | オン |
| async ： write_submit_active | オン |
| async_write_submit_bblocks | すべて |

SAP テストツールの設定の詳細については、を参照してください "SAP ノート 1943937" HWCCT （ SAP HANA 1.0 ）および "SAP ノート 2493172" HCMT/HCOT 用（ SAP HANA 2.0 ）。

次の例は、 HCMT/HCOT 実行プランに変数を設定する方法を示しています。

```
…{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "DataAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
          "Name": "LogAsyncWriteSubmitActive",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
          "Name": "DataAsyncWriteSubmitActive",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
          "Name": "LogAsyncWriteSubmitBlocks",
          "Value": "all",
          "Request": "false"
       },
       {
          "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
          "Name": "DataAsyncWriteSubmitBlocks",
          "Value": "all",
          "Request": "false"
       },
```

```
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

これらの変数はテスト構成に使用する必要があります。これは通常、 SAP が HCMT/HCOT ツールを使用して提供する事前定義された実行計画の場合です。次に、 4k ログの書き込みテストの例を示します。

```
…
       {
          "ID": "D664D001-933D-41DE-A904F304AEB67906",
          "Note": "File System Write Test",
          "ExecutionVariants": [
             {
                "ScaleOut": {
                   "Port": "${RemotePort}",
                   "Hosts": "${Hosts}",
                   "ConcurrentExecution": "${FSConcurrentExecution}"
                },
                "RepeatCount": "${TestRepeatCount}",
                "Description": "4K Block, Log Volume 5GB, Overwrite",
                "Hint": "Log",
                "InputVector": {
                   "BlockSize": 4096,
                   "DirectoryName": "${LogVolume}",
                   "FileOverwrite": true,
                   "FileSize": 5368709120,
                   "RandomAccess": false,
                   "RandomData": true,
                   "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                   "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                   "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                   "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                   "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                   "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                   "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                   "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                   "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
                }
             }, …
```

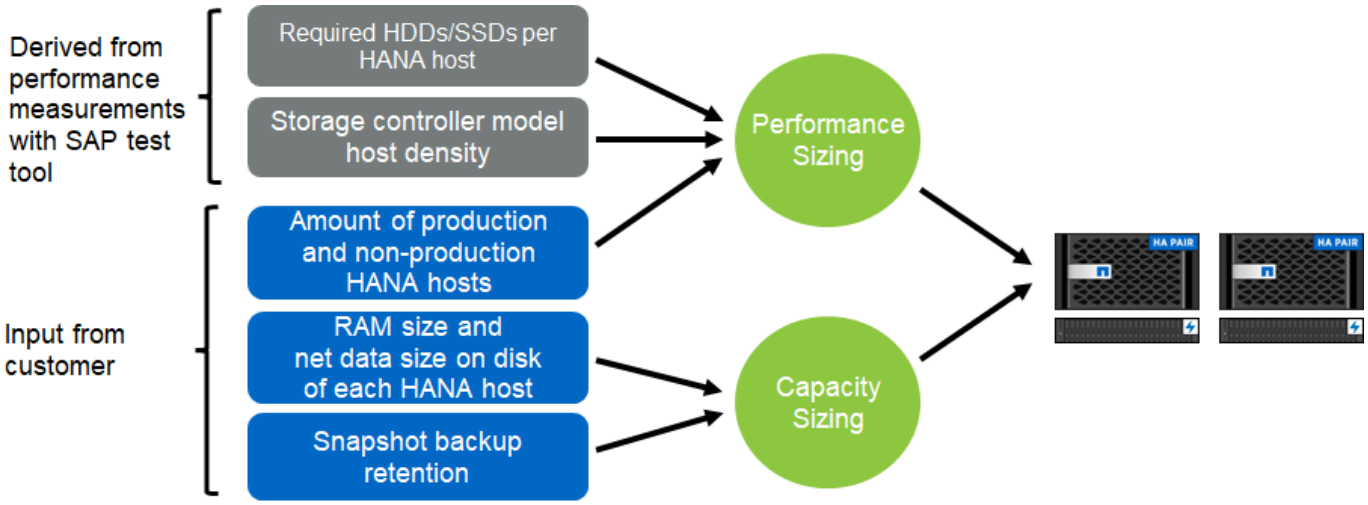
ストレージサイジングプロセスの概要

各ストレージモデルの HANA ホストあたりのディスク数と SAP HANA ホストの密度は、 SAP HANA テストツールで決定されています。

サイジングプロセスでは、本番用および非本番用の SAP HANA ホストの数、各ホストの RAM サイズ、ストレージベースの Snapshot コピーのバックアップ保持期間などの詳細が必要です。SAP HANA ホストの数によって、必要なストレージコントローラとディスクの数が決まります。

RAM のサイズ、各 SAP HANA ホストのディスク上の正味データサイズ、および Snapshot コピーのバックアップ保持期間は、容量サイジングの際に入力として使用されます。

次の図に、サイジングプロセスの概要を示します。




## インフラのセットアップと設定

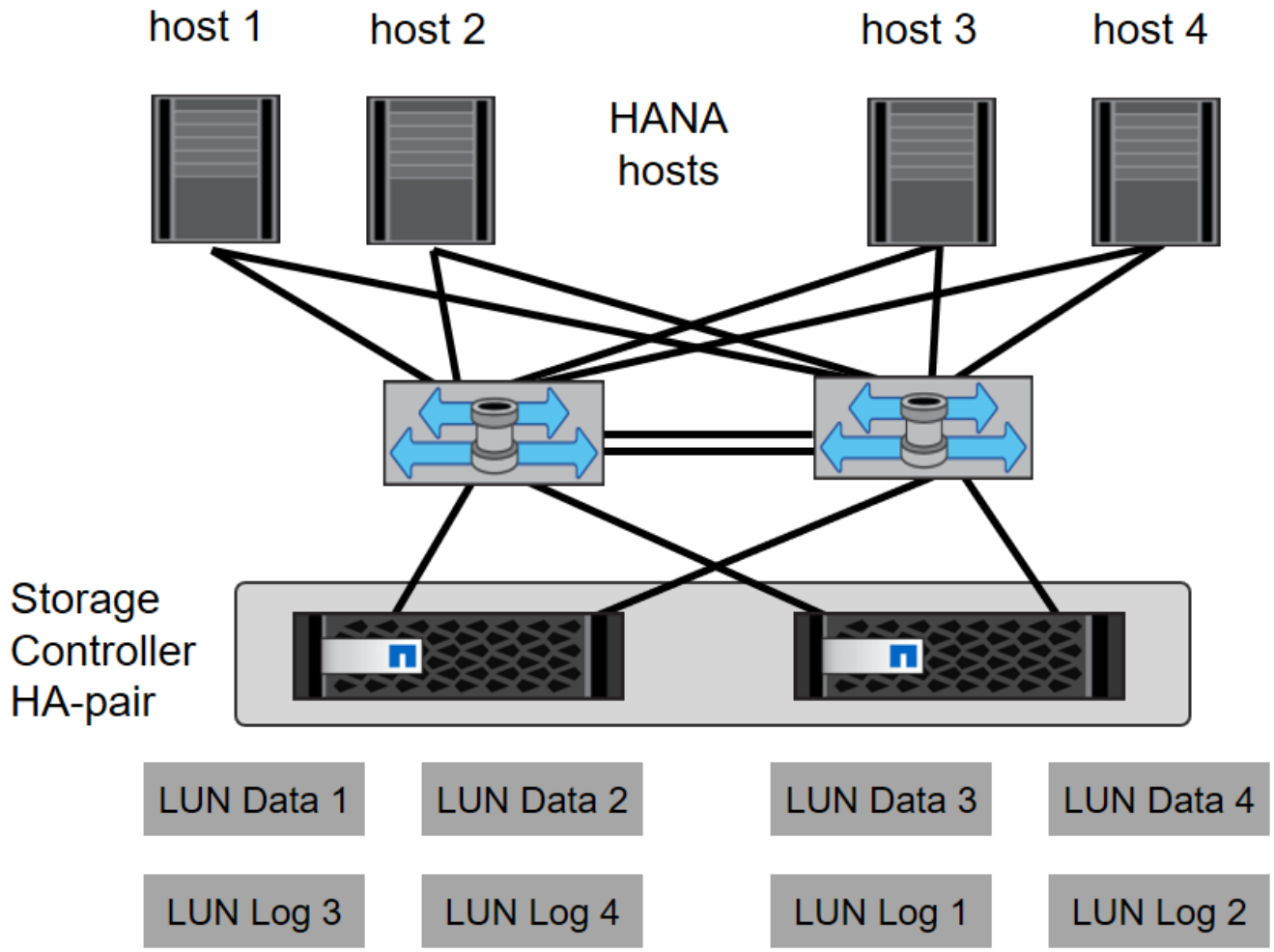
以降のセクションでは、 SAP HANA インフラのセットアップと構成のガイドラインについて説明し、 SAP HANA システムのセットアップに必要なすべての手順について説明します。ここでは、次の設定例を使用します。

- SID=FC5のHANAシステム
  - Linux 論理ボリューム マネージャー (LVM) を使用した SAP HANA の単一ホストと複数ホスト
  - SAP HANA マルチパーティションを使用する SAP HANA シングルホスト

### SAN ファブリックのセットアップ

各 SAP HANA サーバには、最低 8Gbps の帯域幅の冗長 FCP SAN 接続が必要です。ストレージコントローラに接続された各 SAP HANA ホストでは、 8Gbps 以上の帯域幅をストレージコントローラで設定する必要があります。

次の図は、 4 台の SAP HANA ホストを 2 台のストレージコントローラに接続した場合の例を示しています。各 SAP HANA ホストには、冗長ファブリックに接続された 2 つの FCP ポートがあります。ストレージレイヤでは、各 SAP HANA ホストに必要なスループットを提供するために、 4 つの FCP ポートが構成されます。




スイッチレイヤのゾーニングに加えて、ストレージシステム上の各 LUN を、この LUN に接続するホストにマッピングする必要があります。スイッチ上のゾーニングはシンプルにします。つまり、すべてのホスト HBA がすべてのコントローラ HBA を認識できるゾーンセットを 1 つ定義します。

### 時刻の同期

ストレージコントローラと SAP HANA データベースホストの間で時刻を同期する必要があります。すべてのストレージコントローラとすべての SAP HANA ホストに、同じタイムサーバを設定する必要があります。

### ストレージコントローラのセットアップ

ここでは、ネットアップストレージシステムの構成について説明します。プライマリのインストールとセットアップは、対応する ONTAP のセットアップガイドおよび設定ガイドに従って実行する必要があります。

### ストレージ効率

SSD 構成の SAP HANA では、インライン重複排除、ボリューム間インライン重複排除、インライン圧縮、インラインコンパクションがサポートされています。

HDD 構成で Storage Efficiency 機能を有効にすることはできません。

#### NetApp FlexGroupボリューム

NetApp FlexGroup Volumeの使用はSAP HANAではサポートされていません。SAP HANAのアーキテクチャ上、FlexGroup Volumeを使用してもメリットはなく、パフォーマンスの問題が発生する可能性があります。

#### NetAppボリュームとアグリゲートの暗号化

SAP HANAでは、NetApp Volume Encryption（NVE）とNetApp Aggregate Encryption（NAE）の使用がサポートされています。

#### Quality of Service の略

QoSを使用すると、共有コントローラ上の特定のSAP HANAシステムまたはSAP以外のアプリケーションのストレージスループットを制限できます。

本番環境と開発/テスト

1つのユースケースは、開発システムとテストシステムのスループットを制限して、混在環境で本番システムに影響を与えないようにすることです。サイジングプロセスでは、非本番システムのパフォーマンス要件を決定する必要があります。開発 / テスト用のシステムは、通常、 SAP で定義されている本番用システム KPI の 20~50% の範囲で、パフォーマンス値を低くしてサイジングすることができます。ストレージシステムのパフォーマンスに最も大きな影響を与えるのは、大きな書き込みI/Oです。そのため、QoSスループットの上限を、データボリュームとログボリュームの対応する書き込みSAP HANAストレージパフォーマンスKPI値の割合に設定する必要があります。

共有環境

もう1つのユースケースは、負荷の高い書き込みワークロードのスループットを制限することです。特に、レイテンシの影響を受けやすい他の書き込みワークロードにこれらのワークロードが影響しないようにするためです。このような環境では、非共有のスループットの上限QoSグループポリシーを各Storage Virtual Machine（SVM）内の各LUNに適用して、個 々 のストレージオブジェクトの最大スループットを指定した値に制限することを推奨します。これにより、1つのワークロードが他のワークロードに悪影響を及ぼす可能性が低くなります。

そのためには、SVMごとにONTAPクラスタのCLIを使用してグループポリシーを作成する必要があります。

```
qos policy-group create -policy-group <policy-name> -vserver <vserver
name> -max-throughput 1000MB/s -is-shared false
```

SVM内の各LUNに適用されます。次の例では、SVM内の既存のすべてのLUNにポリシーグループを適用します。

```
lun modify -vserver <vserver name>  -path * -qos-policy-group  <policy-
name>
```

この作業はSVMごとに行う必要があります。QoSポリシンググループの名前は、SVMごとに異なる名前にする必要があります。新しいLUNの場合は、ポリシーを直接適用できます。

```
lun create -vserver <vserver_name> -path  /vol/<volume_name>/<lun_name>
-size <size> -ostype <e.g. linux>  -qos-policy-group <policy-name>
```

特定のLUNの最大スループットとして1000MB/秒を使用することを推奨します。アプリケーションがより多くのスループットを必要とする場合は、LUNストライピングを備えた複数のLUNを使用して、必要な帯域幅を提供する必要があります。このガイドでは、セクションで、Linux LVMをベースとしたSAP HANAの例を紹介します"ホスト セットアップ"。

> この制限は読み取りにも適用されます。そのため、SAP HANAデータベースの起動時間やバックアップに必要なSLAを満たす十分な数のLUNを使用します。

#### NetApp FabricPool

SAP HANA システムのアクティブなプライマリファイルシステムには、 NetApp FabricPool テクノロジを使用しないでください。これには ' データとログ領域のファイル・システムと '/hana/shared-file システムが含まれますそのため、特に SAP HANA システムの起動時に、予測不可能なパフォーマンスが発生します。

「 snapshot-only 」階層化ポリシーを使用することも、一般的に SnapVault または SnapMirror デスティネーションなどのバックアップターゲットで FabricPool を使用することもできます。

> FabricPool を使用してプライマリストレージで Snapshot コピーを階層化するか、バックアップターゲットで FabricPool を使用すると、データベースまたはシステムクローンの作成や修復などのその他のタスクのリストアとリカバリに必要な時間が変わります。この点を考慮して、全体的なライフサイクル管理戦略を計画し、この機能を使用している間も SLA が満たされていることを確認してください。

FabricPool は、ログバックアップを別のストレージ階層に移動する場合に適しています。バックアップの移動は、 SAP HANA データベースのリカバリに要する時間に影響します。したがって、「 tiering-minimum-cooling-days 」オプションには、リカバリに必要なログバックアップをローカルの高速ストレージ階層に定期的に配置する値を設定する必要があります。

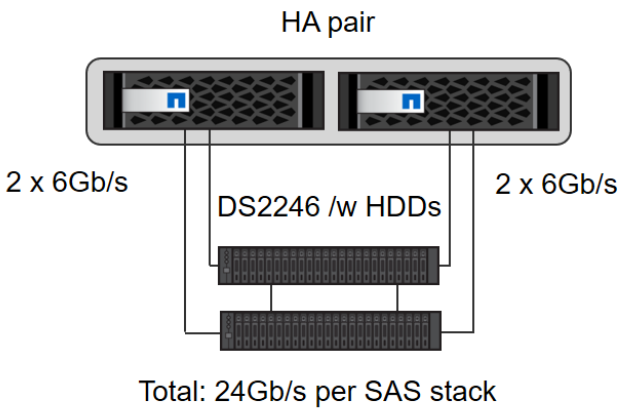
### ストレージを設定する

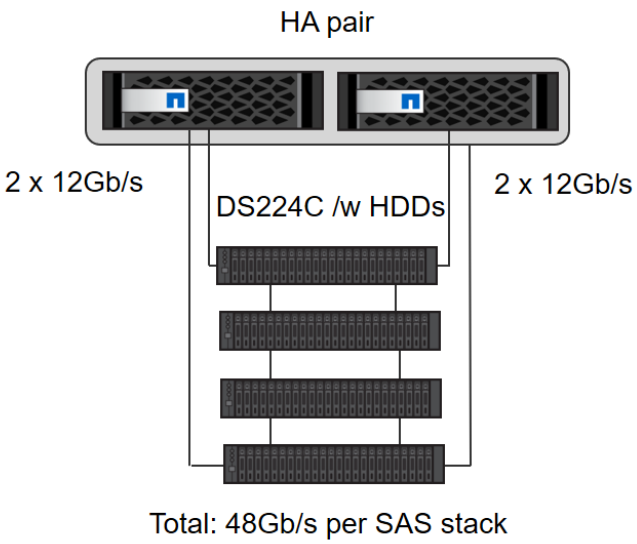
以下に、必要なストレージ構成手順の概要を示します。各手順の詳細については、以降のセクションで説明します。これらの手順を開始する前に、ストレージハードウェアのセットアップ、 ONTAP ソフトウェアのインストール、およびストレージ FCP ポートと SAN ファブリックの接続を完了してください。

1. の説明に従って、正しいディスク・シェルフ構成を確認します[ディスクシェルフの接続]。
2. の説明に従って、必要なアグリゲートを作成して設定します[アグリゲートの構成]。
3. の説明に従って、Storage Virtual Machine（SVM）を作成しますStorage Virtual Machine の設定。
4. の説明に従って、論理インターフェイス（LIF）を作成します[論理インターフェイスの構成]。
5. 「link：hana-fas-fc-storage-controller-setup.html# initiator-groups」の説明に従って、HANAサーバのWorld Wide Name（WWN；ワールドワイド名）を含むイニシエータグループ（igroup）[イニシエータグループ]を作成します。
6. セクションの説明に従って、アグリゲート内にボリュームとLUNを作成して構成します。 "単一ホスト設定"単一のホストまたはセクション内"複数ホストのセットアップ"複数のホストの場合

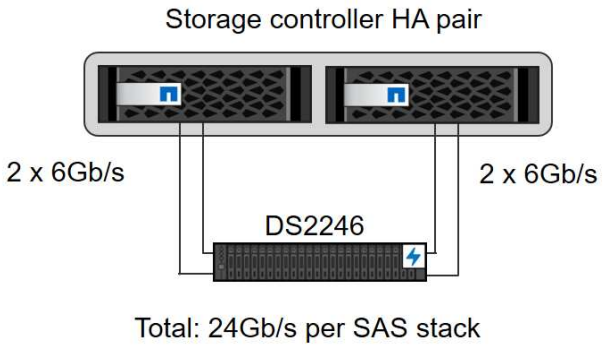
HDD を使用すると、次の図に示すように、 1 つの SAS スタックに最大 2 台の DS2246 ディスクシェルフま

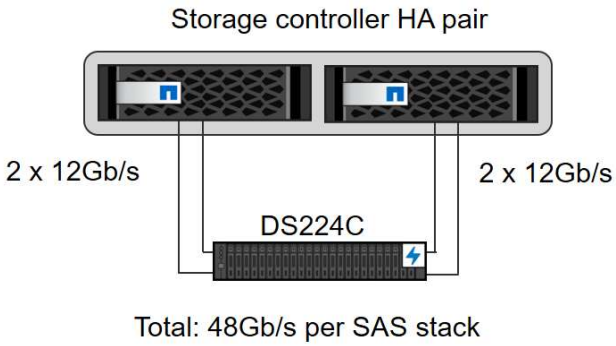
たは 4 台の DS224C ディスクシェルフを接続することで、 SAP HANA ホストに必要なパフォーマンスを実現できます。各シェルフ内のディスクは、 HA ペアの両方のコントローラに均等に分散する必要があります。



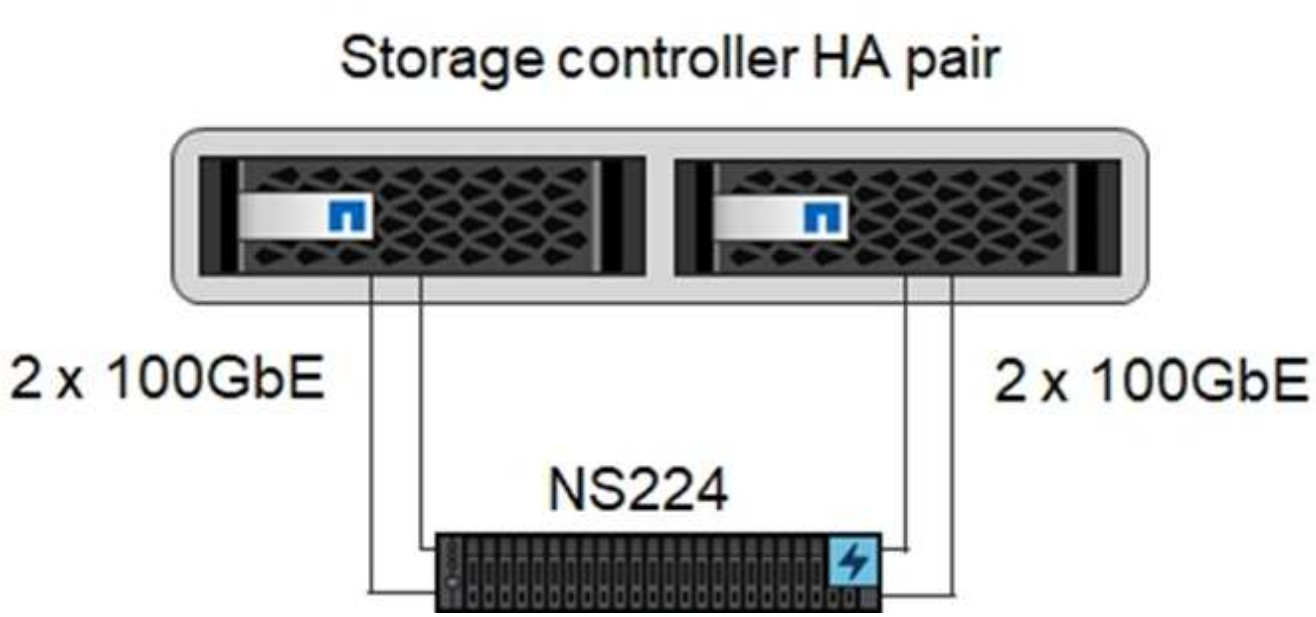

SSD を使用する場合は、次の図に示すように、 1 つの SAS スタックに最大 1 台のディスクシェルフを接続して、 SAP HANA ホストに必要なパフォーマンスを実現できます。各シェルフ内のディスクは、 HA ペアの両方のコントローラに均等に分散する必要があります。ディスクシェルフ DS224C では、クワッドパスの SAS ケーブルも使用できますが、必須ではありません。




**NVMe**ディスクシェルフ

次の図に示すように、NS224 NVMeディスクシェルフは、コントローラごとに2つの100GbEポートで接続されます。各シェルフ内のディスクは、HAペアの両方のコントローラに均等に分散する必要があります。

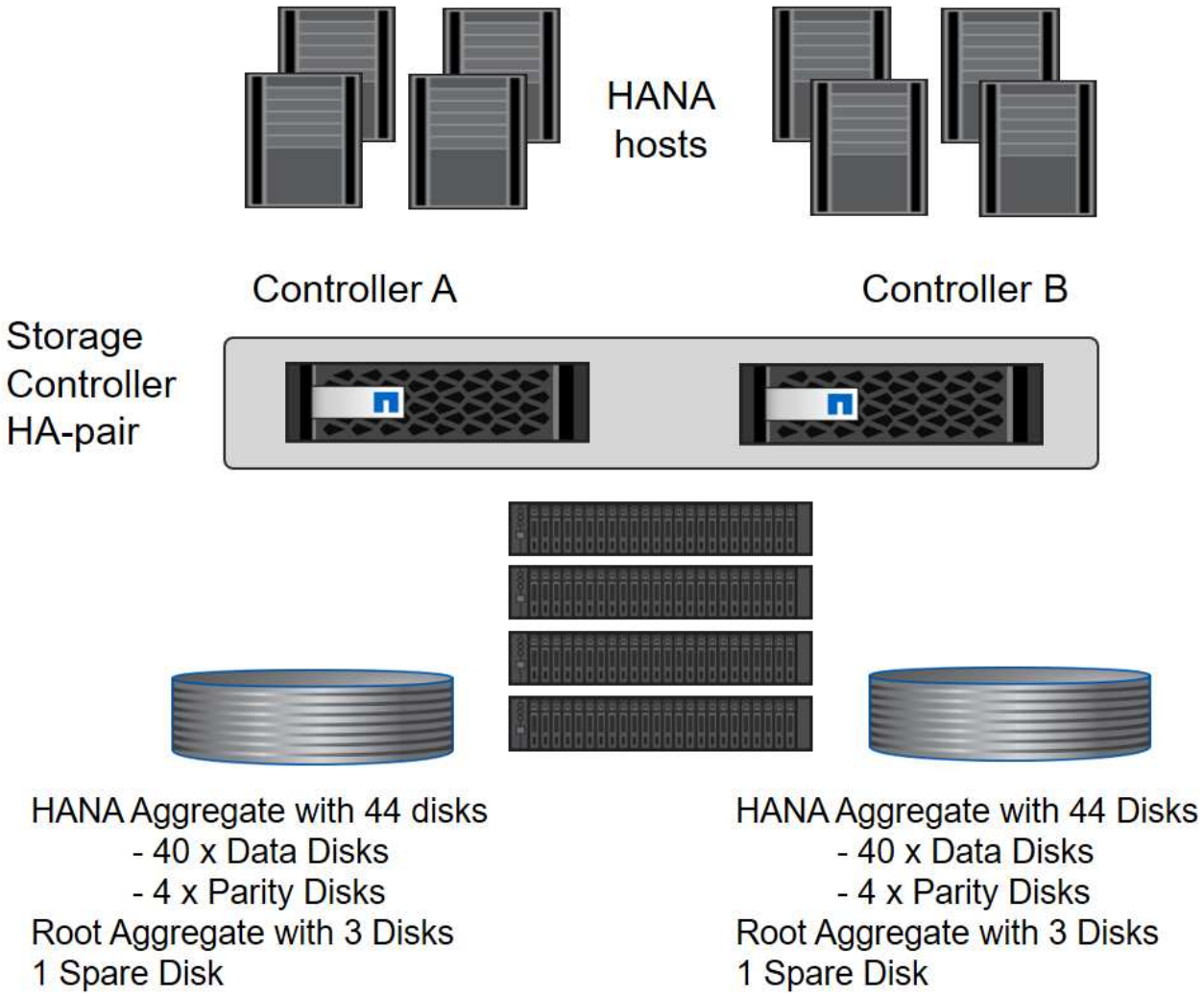



アグリゲートの構成

一般に、使用するディスクシェルフやディスクテクノロジ（ SSD または HDD ）に関係なく、コントローラごとに 2 つのアグリゲートを設定する必要があります。この手順は、使用可能なすべてのコントローラリソースを使用できるようにするために必要です。FAS 2000 シリーズシステムの場合、 1 つのデータアグリゲートで十分です。

**HDD** を使用したアグリゲート構成

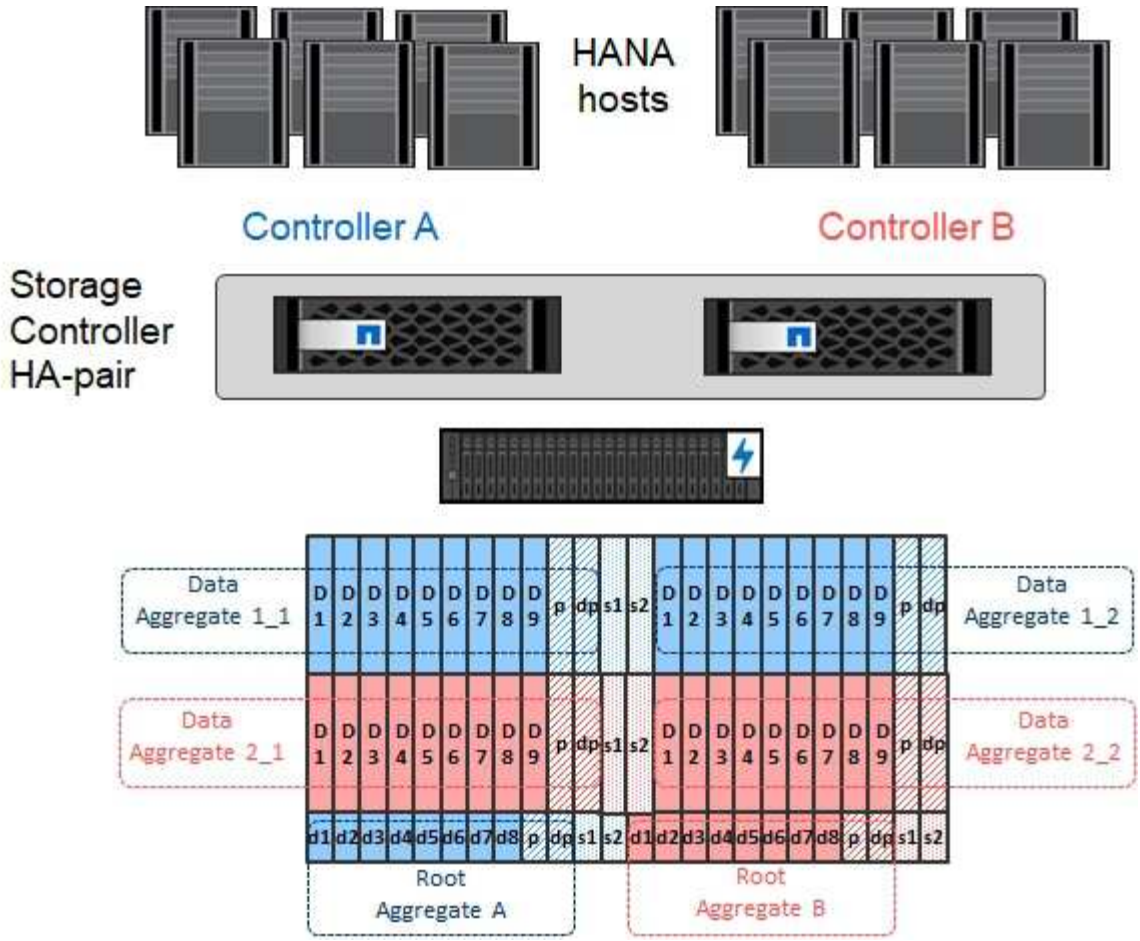
次の図は、 8 台の SAP HANA ホストの構成を示しています。4 台の SAP HANA ホストが各ストレージコントローラに接続されています。各ストレージコントローラに 1 つずつ、合計 2 つのアグリゲートが構成されています。各アグリゲートには、 4 × 10 = 40 のデータディスク（ HDD ）が構成されます。




**SDD** 専用システムで構成を集約する

一般に、使用するディスクシェルフやディスクテクノロジ（ SSD または HDD ）とは別に、各コントローラに 2 つのアグリゲートを構成する必要があります。

次の図は、 ADPv2 を使用した、 12Gb の SAS シェルフで稼働する、 12 台の SAP HANA ホストの構成を示しています。6 台の SAP HANA ホストが各ストレージコントローラに接続されています。各ストレージコントローラに 2 つずつ、合計 4 つのアグリゲートが構成されています。各アグリゲートには、 9 つのデータパーティションと 2 つのパリティディスクパーティションを含む 11 本のディスクが構成されます。各コントローラで、 2 つのスペアパーティションを使用できます。

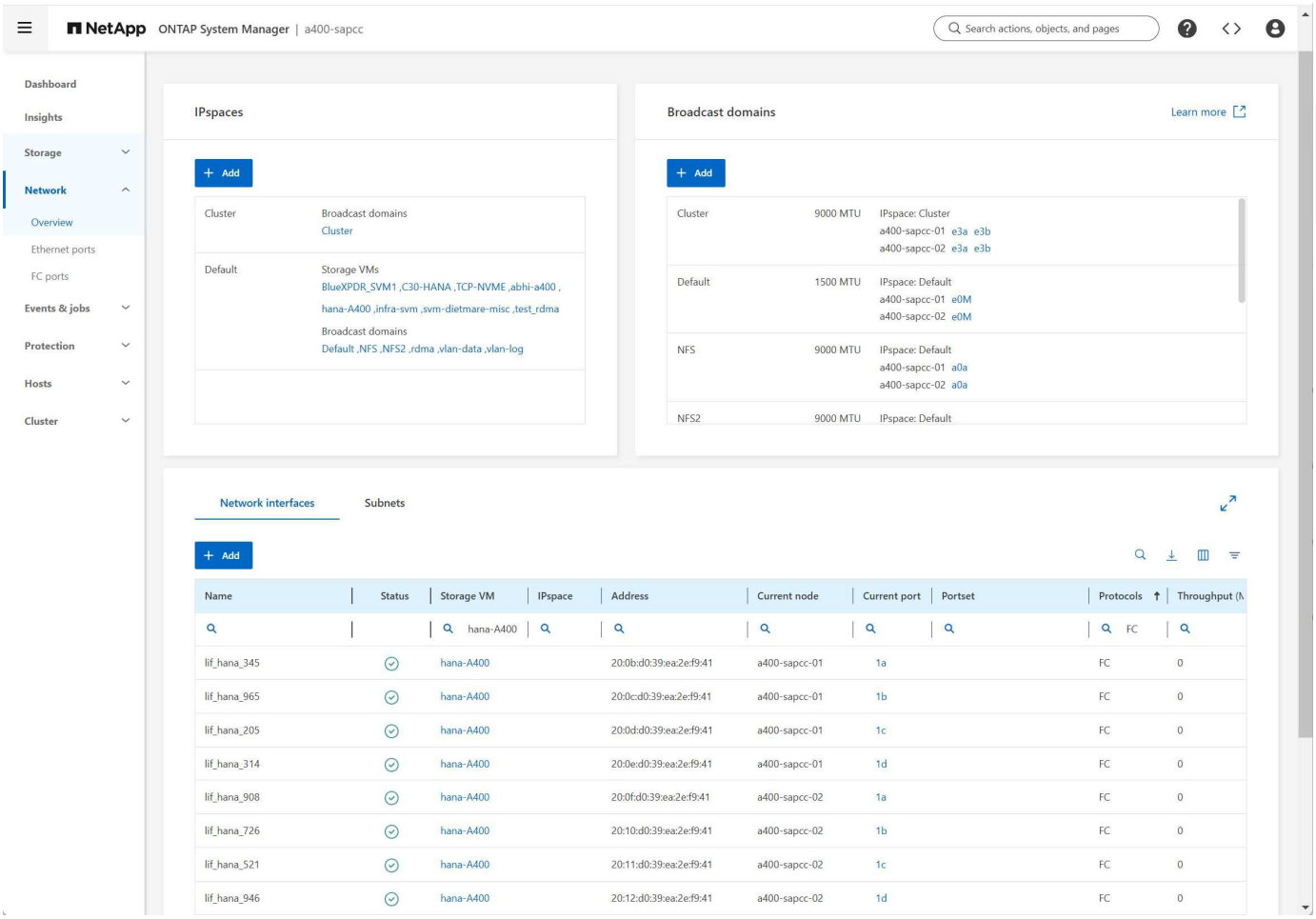



**Storage Virtual Machine** の設定

SAP HANA データベースを使用する複数ホストの SAP 環境では、単一の SVM を使用できます。SVM は、社内の複数のチームによって管理される場合に備え、必要に応じて各 SAP ランドスケープに割り当てることもできます。このドキュメントのスクリーンショットとコマンド出力には、「 HANA 」という名前の SVM が使用されています。

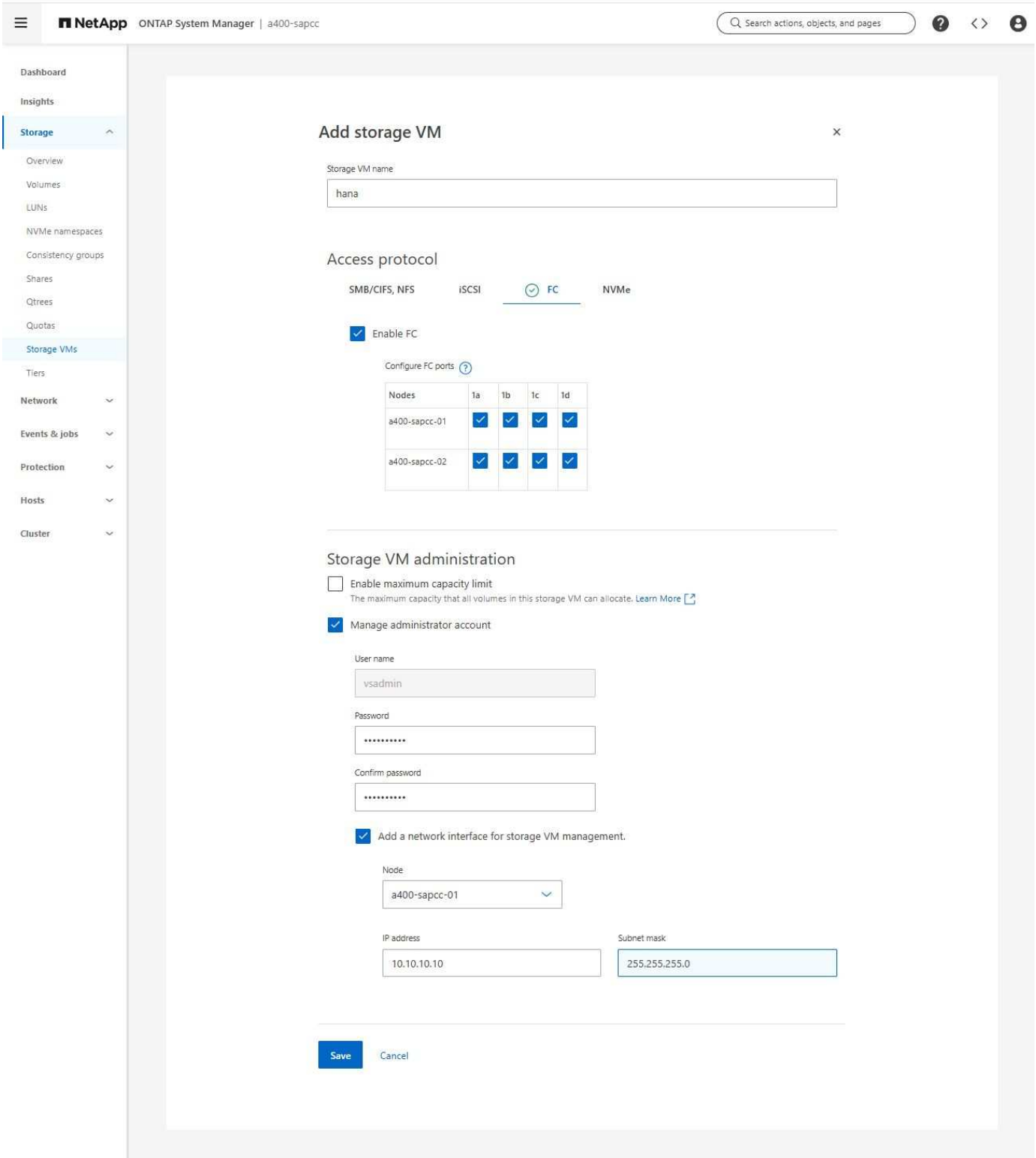
論理インターフェイスの構成

ストレージクラスタ構成内に、 1 つのネットワークインターフェイス（ LIF ）を作成して専用の FCP ポートに割り当てる必要があります。たとえば、パフォーマンス上の理由から 4 つの FCP ポートが必要な場合は、 4 つの LIF を作成する必要があります。次の図は、SVMに設定された8つのLIFのスクリーンショットを示しています。




ONTAP 9 の System Manager で SVM を作成する際には、必要なすべての物理 FCP ポートを選択し、物理ポートごとに 1 つの LIF を自動的に作成できます。

次の図は、ONTAP System Managerを使用したSVMとLIFの作成を示しています。




イニシエータグループ

igroup は、サーバごとに、または LUN へのアクセスを必要とするサーバのグループに対して設定できます。igroup の構成には、サーバの World Wide Port Name （ WWPN ）が必要です。

「 anlun 」ツールを使用して次のコマンドを実行し、各 SAP HANA ホストの WWPN を取得します。

```
stlrx300s8-6:~ # sanlun fcp show adapter
/sbin/udevadm
/sbin/udevadm

host0 ..... WWPN:2100000e1e163700
host1 ..... WWPN:2100000e1e163701
```

この `sanlun`ツールはNetApp Host Utilitiesに含まれており、各SAP HANAホストにインストールする必要があります。詳細については、セクションを参照してください。"ホストのセットアップ："

igroupは、ONTAPクラスタのCLIを使用して作成できます。

```
lun igroup create -igroup <igroup name> -protocol fcp -ostype linux
-initiator <list of initiators> -vserver <SVM name>
```

シングルホスト

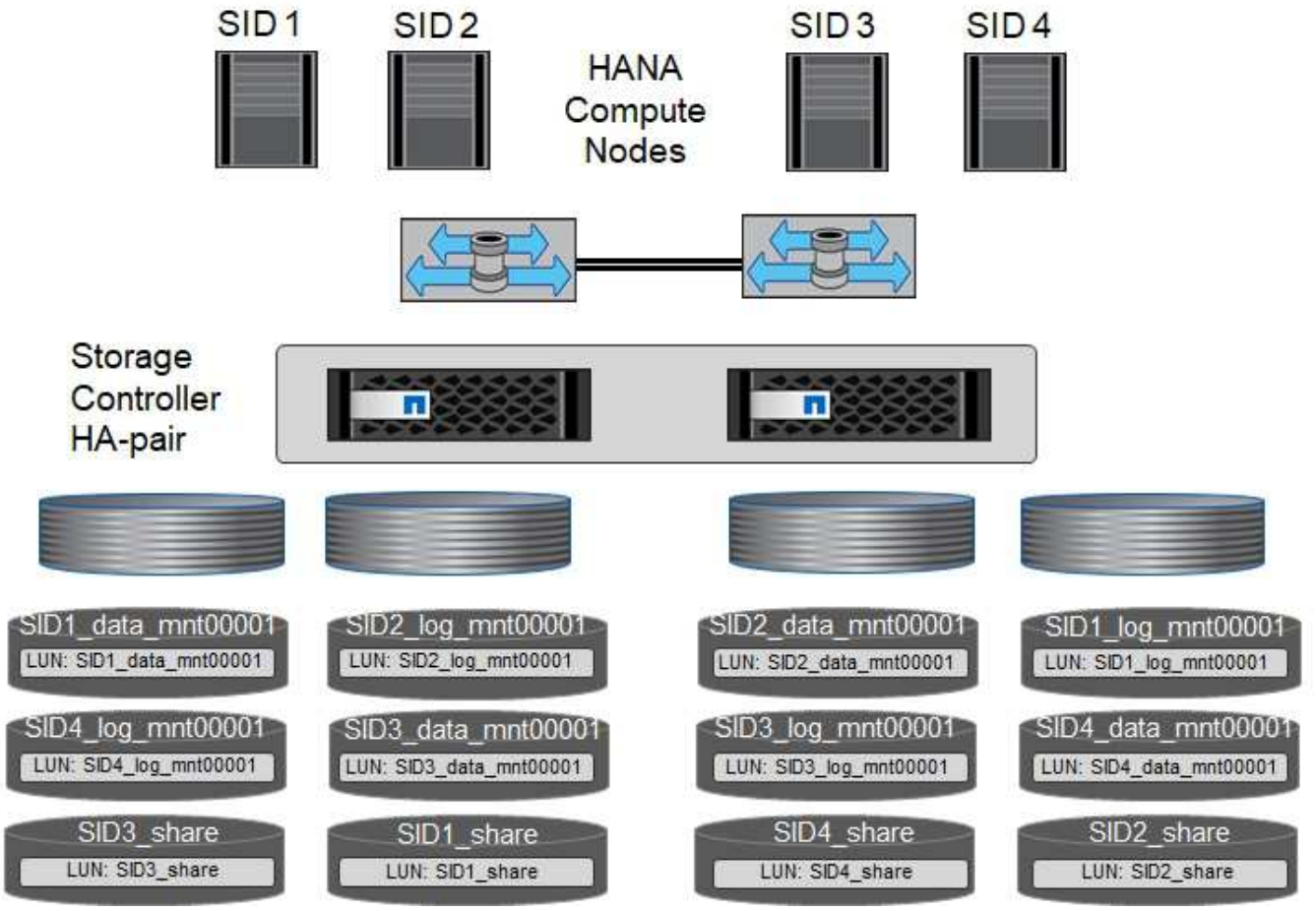
シングルホスト

## このセクションでは、SAP HANAシングルホストシステムに固有のNetAppストレージシステムの構成について説明します。

### SAP HANA シングルホストシステムのボリュームと LUN の構成

次の図は、 4 つのシングルホスト SAP HANA システムのボリューム構成を示しています。各SAP HANAシステムのデータボリュームとログボリュームは、異なるストレージコントローラに分散されます。たとえば、ボリュームは `SID1_data_mnt00001`コントローラAで構成され、ボリュームはコントローラBで構成され `SID1_log_mnt00001`ます。各ボリューム内には単一のLUNが構成されます。

ハイアベイラビリティ（ HA ）ペアのうち、 1 台のストレージコントローラのみを SAP HANA システムに使用する場合は、データボリュームとログボリュームを同じストレージコントローラに保存することもできます。




各 SAP HANA ホストには、データボリューム、ログボリューム、「 /hana/shared 」のボリュームが構成されています。次の表は、 4 台の SAP HANA シングルホストシステムを使用した構成例を示しています。

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| システム SID1 のデータ、ログ、および共有ボリューム | データボリューム：SID1_data_mnt00001 | 共有ボリューム：SID1_shared | – | ログボリューム：SID1_log_mnt00001 |
| システム SID2 のデータボリューム、ログボリューム、および共有ボリューム | – | ログボリューム：SID2_log_mnt00001 | データボリューム：SID2_data_mnt00001 | 共有ボリューム：SID2_shared |
| システム SID3 のデータ、ログ、および共有ボリューム | 共有ボリューム：SID3_shared | データボリューム：SID3_data_mnt00001 | ログボリューム：SID3_log_mnt00001 | – |
| システム SID4 のデータボリューム、ログボリューム、および共有ボリューム | ログボリューム：SID4_log_mnt00001 | – | 共有ボリューム：SID4_shared | データボリューム：SID4_data_mnt00001 |

次の表に、シングルホストシステムのマウントポイント構成の例を示します。

| LUN | HANA ホストのマウントポイント | 注 |
| --- | --- | --- |
| SID1_data_mnt00001 | /hana/data SID1/mnt00001 のように指定します | /etc/fstab エントリを使用してマウントされます |
| SID1_log_mnt00001 | /hana/log/s1/mnt00001 | /etc/fstab エントリを使用してマウントされます |
| SID1_shared | /hana/shareed/SID1 | /etc/fstab エントリを使用してマウントされます |

ここで説明する構成では ' ユーザ SID1adm のデフォルトのホーム・ディレクトリが格納されている /usr/sap/SID1 ディレクトリがローカル・ディスク上にありますディスク・ベースのレプリケーションを使用した災害復旧セットアップでは、すべてのファイル・システムが中央ストレージ上にあるように、 /usr/sap/SID1 ディレクトリの「 ID1_shared 」ボリューム内に追加の LUN を作成することを推奨します。

**Linux LVM** を使用した **SAP HANA** シングルホストシステムのボリュームと **LUN** の構成

Linux LVM を使用すると、パフォーマンスを向上させ、 LUN サイズの制限に対処できます。LVM ボリュームグループの各 LUN は、別のアグリゲートおよび別のコントローラに格納する必要があります。次の表に、ボリュームグループごとに 2 つの LUN を使用する例を示します。

SAP HANA KPIを満たすために複数のLUNでLVMを使用する必要はありませんが、推奨されます。

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
| --- | --- | --- | --- | --- |
| LVM ベースのシステムのデータ、ログ、および共有ボリューム | データボリューム：SID1_data_mnt00001 | 共有ボリューム：SID1_shared log2 ボリューム：SID1_log2_mnt00001 | data2 ボリューム：SID1_data2_mnt00001 | ログボリューム：SID1_log_mnt00001 |

ここで説明する構成では ' ユーザ SID1adm のデフォルトのホーム・ディレクトリが格納されている /usr/sap/SID1 ディレクトリがローカル・ディスク上にありますディスク・ベースのレプリケーションを使用した災害復旧セットアップでは、すべてのファイル・システムが中央ストレージ上にあるように、 /usr/sap/SID1 ディレクトリの「 ID1_shared 」ボリューム内に追加の LUN を作成することを推奨します。

ボリュームのオプション

次の表にリストされているボリューム オプションは、SAP HANA に使用されるすべてのボリュームで検証および設定する必要があります。

| アクション | **ONTAP 9** |
| --- | --- |
| Snapshot コピーの自動作成を無効にする | vol modify – vserver <vserver-name> -volume <volname> -snapshot-policy none と指定します |
| Snapshot ディレクトリの可視化を無効にします | vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false |

**LUN** 、ボリュームを作成し、 **LUN** をイニシエータグループにマッピングします

NetApp ONTAP System Managerを使用してストレージボリュームとLUNを作成し、それらをサーバとONTAP CLIのigroupにマッピングすることができます。このマニュアルでは、CLIの使用方法について説明します。

**CLI** を使用して **LUN** 、ボリュームを作成し、 **igroup** に **LUN** をマッピングします

このセクションでは、LVM と LVM ボリューム グループごとに 2 つの LUN を使用する SID FC5 の SAP HANA 単一ホスト システムに対して、ONTAP 9 のコマンド ラインを使用した構成例を示します。

1. 必要なボリュームをすべて作成します。

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. すべての LUN を作成します。

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. FC5 のシステム ホストに属するすべてのポートのイニシエーター グループを作成します。

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb -vserver hana
```

4. 作成したイニシエータグループにすべての LUN をマッピングします。

```
lun map -path /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
```



複数のホスト

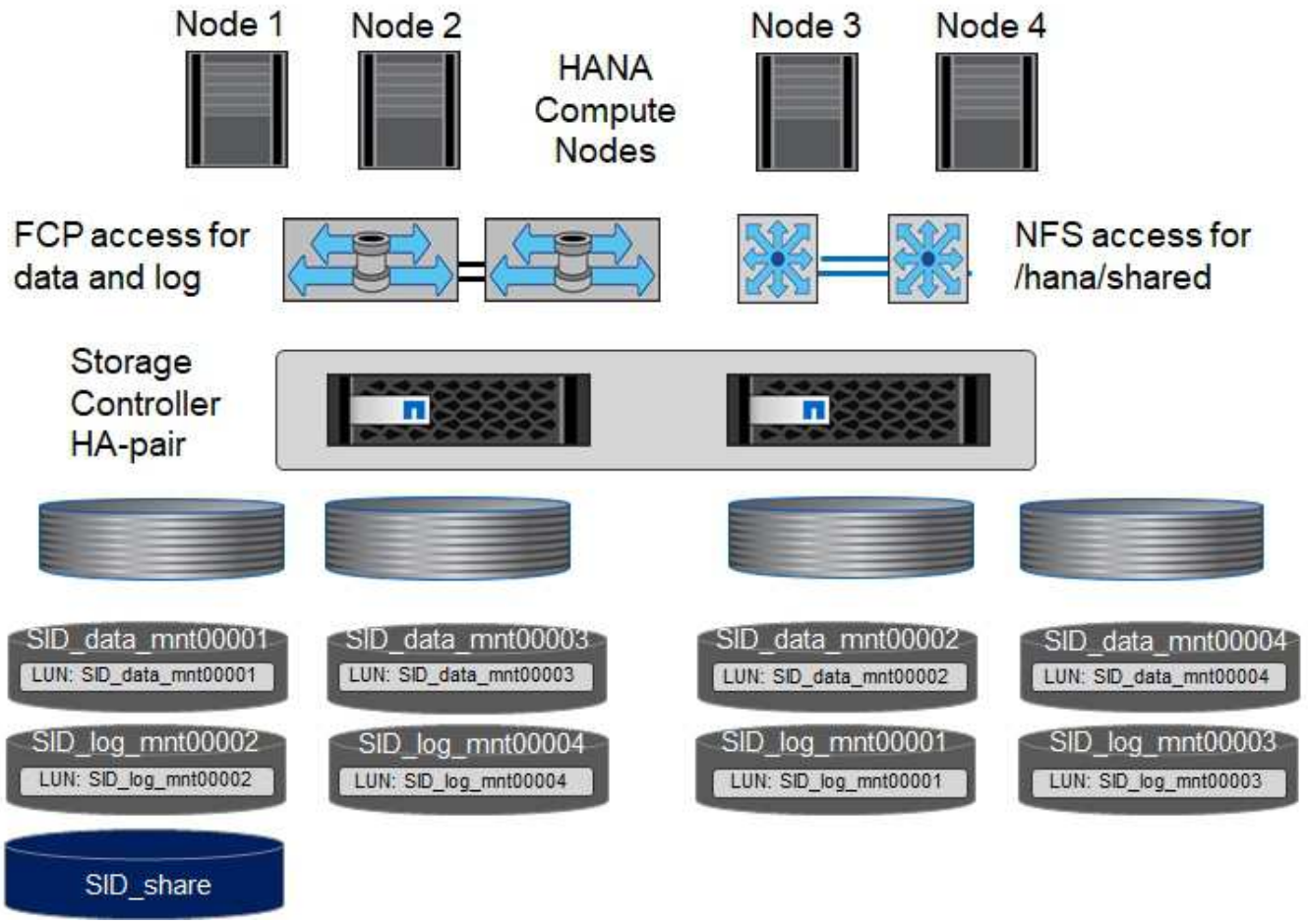
## このセクションでは、SAP HANAマルチホストシステムに固有のNetAppストレージシステムの構成について説明します。

### **SAP HANA** マルチホストシステムのボリュームと **LUN** の構成

次の図は、 4+1 のマルチホスト SAP HANA システムのボリューム構成を示しています。各 SAP HANA ホストのデータボリュームとログボリュームは、異なるストレージコントローラに分散されます。たとえば、ボリューム「 `S ID_data_mnt00001 」はコントローラ A に設定され、ボリューム「 S ID_LOG_mnt00001 」はコントローラ B に設定されています各ボリュームに 1 つの LUN を設定します。

「 /hana/shared 」ボリュームは、すべての HANA ホストからアクセスできる必要があり、 NFS を使用してエクスポートされます。「 /hana/shared 」ファイルシステムには特定のパフォーマンス KPI がありませんが、 10Gb のイーサネット接続を使用することを推奨します。

HA ペアのうち、 1 台のストレージコントローラのみを SAP HANA システムに使用する場合は、データボリュームとログボリュームを同じストレージコントローラに保存することもできます。




各 SAP HANA ホストには、 1 個のデータボリュームと 1 個のログボリュームが作成されます。「 /hana/shared 」ボリュームは、 SAP HANA システムのすべてのホストで使用されます。次の図は、 4+1 のマルチホスト SAP HANA システムの構成例を示しています。

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| ノード 1 のデータボリュームとログボリューム | データボリューム： SID_data_mnt00001 | – | ログボリューム： SID_log_mnt00001 | – |
| ノード 2 のデータボリュームとログボリューム | ログボリューム： SID_log_mnt00002 | – | データボリューム： SID_data_mnt00002 | – |
| ノード 3 のデータボリュームとログボリューム | – | データボリューム： SID_data_mnt00003 | – | ログボリューム： SID_log_mnt00003 |
| ノード 4 のデータボリュームとログボリューム | – | ログボリューム： SID_log_mnt00004 | – | データボリューム： SID_data_mnt00004 |
| すべてのホストの共有ボリューム | 共有ボリューム： SID_shared | – | – | – |

次の表に、アクティブな SAP HANA ホストが 4 台あるマルチホストシステムの構成とマウントポイントを示

します。

| **LUN** またはボリューム | **SAP HANA** ホストのマウントポイント | 注 |
|---|---|---|
| LUN ： SID_data_mnt00001 | /hana/data/SID/mnt00001 | ストレージコネクタを使用してマウント |
| LUN ： SID_log_mnt00001 | /hana/log/sid/mnt00001 | ストレージコネクタを使用してマウント |
| LUN ： SID_data_mnt00002 | /hana/data/sid/mnt00002 | ストレージコネクタを使用してマウント |
| LUN ： SID_log_mnt00002 | /hana/log/sid/mnt00002 | ストレージコネクタを使用してマウント |
| LUN ： SID_data_mnt00003 | /hana/data/sid/mnt00003 | ストレージコネクタを使用してマウント |
| LUN ： SID_log_mnt00003 | /hana/log/sid/mnt00003 | ストレージコネクタを使用してマウント |
| LUN ： SID_data_mnt00004 | /hana/data/sid/mnt00004 | ストレージコネクタを使用してマウント |
| LUN ： SID_log_mnt00004 | /hana/log/sid/mnt00004 | ストレージコネクタを使用してマウント |
| ボリューム： SID_shared | /hana/shared-SID を指定します | NFS と /etc/fstab のエントリを使用して、すべてのホストにマウントされます |

上記の構成では、 `/usr/sap/SID`ユーザSIDadmのデフォルトのホームディレクトリが格納されているディレクトリが、各HANAホストのローカルディスクに配置されます。ディスクベースのレプリケーションを使用するディザスタリカバリの設定では、NetAppでは、各データベースホストのすべてのファイルシステムが中央ストレージに配置されるように、ファイルシステム用のボリュームに `/usr/sap/SID`さらに4つのサブディレクトリを作成することを推奨してい `SID_shared`ます。

**Linux LVM** を使用した **SAP HANA** マルチホストシステムのボリュームと **LUN** の構成

Linux LVM を使用すると、パフォーマンスを向上させ、 LUN サイズの制限に対処できます。LVM ボリュームグループの各 LUN は、別のアグリゲートおよび別のコントローラに格納する必要があります。次の表に、 2+1 の SAP HANA マルチホストシステムのボリュームグループあたり 2 つの LUN の例を示します。

SAP HANA KPI を満たすために LVM を使用して複数の LUN を組み合わせる必要はありませんが、推奨されます。

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| ノード 1 のデータボリュームとログボリューム | データボリューム： SID_data_mnt00001 | ログ 2 ボリューム： SID_log2_mnt00001 | ログボリューム： SID_log_mnt00001 | data2 ボリューム： SID_data2_mnt00001 |

| 目的 | コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|---|
| ノード 2 のデータボリュームとログボリューム | ログ 2 ボリューム：SID_log2_mnt00002 | データボリューム：SID_data_mnt00002 | data2 ボリューム：SID_data2_mnt00002 | ログボリューム：SID_log_mnt00002 |
| すべてのホストの共有ボリューム | 共有ボリューム：SID_shared | – | – | – |

ボリュームのオプション

次の表にリストされているボリューム オプションは、SAP HANA に使用されるすべてのボリュームで検証および設定する必要があります。

| アクション | **ONTAP 9** |
|---|---|
| Snapshot コピーの自動作成を無効にする | vol modify – vserver <vserver-name> -volume <volname> -snapshot-policy none と指定します |
| Snapshot ディレクトリの可視化を無効にします | vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false |

**LUN** 、ボリュームを作成し、 **LUN** をイニシエータグループにマッピングします

NetApp ONTAP System Managerを使用してストレージボリュームとLUNを作成し、それらをサーバとONTAP CLIのigroupにマッピングすることができます。このマニュアルでは、CLIの使用方法について説明します。

**CLI** を使用して **LUN** 、ボリュームを作成し、 **igroup** に **LUN** をマッピングします

このセクションでは、コマンドラインを使用した構成例を示します。 ONTAP 9 は、 LVM を使用した 2+1 の SAP HANA マルチホストシステムで、 LVM ボリュームグループごとに 2 つの LUN を使用した SID FC5 です。

1. 必要なボリュームをすべて作成します。

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00002  -aggregate aggr2_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data_mnt00002  -aggregate aggr2_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00002  -aggregate aggr2_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_data2_mnt00002  -aggregate aggr2_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. すべての LUN を作成します。

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data_mnt00002/FC5_data_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00002/FC5_log_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. システム FC5 に属するすべてのサーバの igroup を作成します。

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb,
10000090fadcc5c1,10000090fadcc5c2,  10000090fadcc5c3,10000090fadcc5c4
-vserver hana
```

4. 作成した igroup にすべての LUN をマッピングします。

```
lun map -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_data_mnt00002/FC5_data_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log_mnt00002/FC5_log_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002  -igroup HANA-FC5
```

#### SAP HANA Storage Connector API

ストレージコネクタは、フェイルオーバー機能を備えたマルチホスト環境でのみ必要です。マルチホスト構成では、 SAP HANA に高可用性機能が提供されるため、 SAP HANA データベースホストはスタンバイホストにフェイルオーバーできます。この場合、障害が発生したホストの LUN には、スタンバイホストからアクセスして使用されます。ストレージコネクタは、一度に 1 つのデータベースホストだけがストレージパーティションにアクティブにアクセスできるようにするために使用されます。

ネットアップストレージを使用した SAP HANA マルチホスト構成では、 SAP が提供する標準のストレージコネクタが使用されます。『 SAP HANA FC Storage Connector Admin Guide 』は、への添付ファイルとして提供されています "SAP ノート 1900823"。

ホストのセットアップ

ホストをセットアップする前に、 NetApp SAN Host Utilities をからダウンロードしておく必要があります "ネットアップサポート" HANA サーバにインストールします。Host Utility のマニュアルには、使用する FCP HBA に応じてインストールする必要がある追加ソフトウェアに関する情報が記載されています。

また、使用している Linux バージョンに固有のマルチパス構成に関する情報も記載されています。このドキュメントでは、 SLES 15 および Red Hat Enterprise Linux 7.6 以降で必要な設定手順について説明します。を参照してください "『 Linux Host Utilities 7.1 Installation and Setup Guide 』"。

マルチパスを設定します

> SAP HANA マルチホスト構成のすべてのワーカーホストとスタンバイホストで、手順 1~6 を実行する必要があります。

マルチパスを設定するには、次の手順を実行します。

1. 各サーバで Linux の「 re scan-scsi-bus.sh -a' 」コマンドを実行して、新しい LUN を検出します。
2. 「 lun lun lun show 」コマンドを実行し、必要なすべての LUN が表示されることを確認します。次に、 2 つのデータ LUN と 2 つのログ LUN を持つ 2+1 マルチホスト HANA システムの「 lun lun show 」コマン

ドの出力例を示します。出力には、 LUN および LUN 「 S 3data_mnt00001 」やデバイスファイル「 /dev/sdag 」などの対応するデバイスファイルが表示されます。各 LUN には、ホストからストレージコントローラへの FC パスが 8 つあります。

```
sapcc-hana-tst:~ # sanlun lun show
controller(7mode/E-Series)/                                    device
host                  lun
vserver(cDOT/FlashRay)        lun-pathname                     filename
adapter    protocol   size    product
------------------------------------------------------------------------
---------------------------------------
svm1                          FC5_log2_mnt00002                /dev/sdbb
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdba
host21     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001                /dev/sdaz
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001                 /dev/sday
host21     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002               /dev/sdax
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002                /dev/sdaw
host21     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001               /dev/sdav
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001                /dev/sdau
host21     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002                /dev/sdat
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdas
host21     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001                /dev/sdar
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001                 /dev/sdaq
host21     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002               /dev/sdap
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002                /dev/sdao
host21     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001               /dev/sdan
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001                /dev/sdam
host21     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002                /dev/sdal
host20     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdak
```

```
host20     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001              /dev/sdaj
host20     FCP        500g    cDOT
svm1                          FC5_log_mnt00001               /dev/sdai
host20     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002             /dev/sdah
host20     FCP        1t      cDOT
svm1                          FC5_data_mnt00002              /dev/sdag
host20     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001             /dev/sdaf
host20     FCP        1t      cDOT
svm1                          FC5_data_mnt00001              /dev/sdae
host20     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002              /dev/sdad
host20     FCP        500g    cDOT
svm1                          FC5_log_mnt00002               /dev/sdac
host20     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001              /dev/sdab
host20     FCP        500g    cDOT
svm1                          FC5_log_mnt00001               /dev/sdaa
host20     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002             /dev/sdz
host20     FCP        1t      cDOT
svm1                          FC5_data_mnt00002              /dev/sdy
host20     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001             /dev/sdx
host20     FCP        1t      cDOT
svm1                          FC5_data_mnt00001              /dev/sdw
host20     FCP        1t      cDOT
```

3. 実行 `multipath -r`そして `multipath -ll`デバイス ファイル名のワールドワイド識別子 (WWID) を取得するコマンド。

この例では、8 つの LUN があります。

```
sapcc-hana-tst:~ # multipath -r
sapcc-hana-tst:~ # multipath -ll
3600a098038314e63492b59326b4b786d dm-7 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
```

```
3600a098038314e63492b59326b4b786e dm-9 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
3600a098038314e63492b59326b4b786f dm-11 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
3600a098038314e63492b59326b4b7870 dm-13 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
3600a098038314e63532459326d495a64 dm-6 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
3600a098038314e63532459326d495a65 dm-8 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
3600a098038314e63532459326d495a66 dm-10 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
```

```
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
3600a098038314e63532459326d495a67 dm-12 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

4. /etc/multipath.conf ファイルを編集し 'WWID とエイリアス名を追加します



出力例は '2+1 マルチホスト・システムの 4 つの LUN のエイリアス名を含む /etc/multipath.conf ファイルの内容を示しています使用可能な multipath.conf ファイルがない場合、「 multipath-T 」 /etc/multipath.conf を実行して作成できます。

```
sapcc-hana-tst:/ # cat /etc/multipath.conf
multipaths {
                multipath {
                wwid    3600a098038314e63492b59326b4b786d
                alias   svm1-FC5_data2_mnt00001
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786e
                alias   svm1-FC5_data2_mnt00002
        }
        multipath {
                wwid    3600a098038314e63532459326d495a64
                alias   svm1-FC5_data_mnt00001
        }
        multipath {
                wwid    3600a098038314e63532459326d495a65
                alias   svm1-FC5_data_mnt00002
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786f
                alias   svm1-FC5_log2_mnt00001
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b7870
                alias   svm1-FC5_log2_mnt00002
        }
        multipath {
                wwid    3600a098038314e63532459326d495a66
                alias   svm1-FC5_log_mnt00001
        }
        multipath {
                wwid    3600a098038314e63532459326d495a67
                alias   svm1-FC5_log_mnt00002
        }


}
```

5. 「 multipath -r 」コマンドを実行して、デバイスマップをリロードします。
6. すべての LUN 、エイリアス名、およびアクティブパスとスタンバイパスを一覧表示するには、「マルチパス -ll 」コマンドを実行して構成を確認します。

次の出力例は、 2 つのデータ LUN と 2 つのログ LUN を持つ 2+1 マルチホスト HANA システムの出力を示しています。

```
sapcc-hana-tst:~ # multipath -ll
hsvm1-FC5_data2_mnt00001 (3600a098038314e63492b59326b4b786d) dm-7
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
svm1-FC5_data2_mnt00002 (3600a098038314e63492b59326b4b786e) dm-9
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
svm1-FC5_data_mnt00001 (3600a098038314e63532459326d495a64) dm-6
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
svm1-FC5_data_mnt00002 (3600a098038314e63532459326d495a65) dm-8
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
svm1-FC5_log2_mnt00001 (3600a098038314e63492b59326b4b786f) dm-11
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
```

```
svm1-FC5_log2_mnt00002 (3600a098038314e63492b59326b4b7870) dm-13
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
svm1-FC5_log_mnt00001 (3600a098038314e63532459326d495a66) dm-10
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
svm1-FC5_log_mnt00002 (3600a098038314e63532459326d495a67) dm-12
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

単一ホスト設定

単一ホスト設定

# この章では、Linux LVM を使用した SAP HANA 単一ホストのセットアップについて説明します。

### SAP HANA 単一ホストシステムの LUN 構成

次の表に示すように、 SAP HANA ホストで、ボリュームグループと論理ボリュームを作成してマウントする必要があります。

| 論理ボリューム / LUN | SAP HANA<br>ホストのマウントポイント | 注 |
|---|---|---|
| lv ： FC5_data_mnt0000 -vol | /hana/data/FC51/mnt00001 | /etc/fstab エントリを使用してマウントされます |
| lv ： FC5_log_mnt00001 -vol | /hana/log/FC5/mnt00001 | /etc/fstab エントリを使用してマウントされます |

| 論理ボリューム / **LUN** | **SAP HANA**<br>ホストのマウントポイント | 注 |
| --- | --- | --- |
| LUN：FC5_shared | /hana/shareed/FC5 | /etc/fstab エントリを使用してマウントされます |

説明した構成では、 `/usr/sap/FC5`ユーザー FC5adm のデフォルトのホーム ディレクトリが格納されているディレクトリは、ローカル ディスク上にあります。ディスクベースのレプリケーションによる災害復旧設定では、 NetAppは、 `FC5_shared`のボリューム `/usr/sap/FC5`すべてのファイルシステムが中央ストレージ上に存在するようにディレクトリを作成します。

**LVM** ボリュームグループと論理ボリュームを作成

1. すべての LUN を物理ボリュームとして初期化します。

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001
```

2. 各データパーティションとログパーティションのボリュームグループを作成します。

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
```

3. データパーティションとログパーティションごとに論理ボリュームを作成します。ボリュームグループごとに使用されている LUN の数（この例では 2 つ）と同じストライプサイズを使用し、データの場合は 256K 、ログの場合は 64k を使用します。SAP では、ボリュームグループごとに 1 つの論理ボリュームのみがサポートされます。

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. その他すべてのホストで、物理ボリューム、ボリュームグループ、およびボリュームグループをスキャンします。

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

これらのコマンドでボリュームが見つからない場合は、再起動する必要があります。

論理ボリュームをマウントするには、論理ボリュームをアクティブ化する必要があります。ボリュームをアクティブ化するには、次のコマンドを実行します。

```
vgchange -a y
```

ファイルシステムの作成

すべてのデータおよびログ論理ボリュームと hana 共有 LUN に XFS ファイル システムを作成します。

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs /dev/mapper/svm1-FC5_shared
```

マウントポイントを作成する

必要なマウント ポイント ディレクトリを作成し、データベース ホストの権限を設定します。

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod –R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod –R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

ファイルシステムをマウント

システム起動中にファイルシステムをマウントするには、 `/etc/fstab`設定ファイルに必要なファイルシステムを追加し、 `/etc/fstab`設定ファイル:

```
# cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/FC5_log_mnt00001-vol /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/FC5_data_mnt00001-vol /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
```



データ LUN とログ LUN の XFS ファイルシステムは 'relatim' および inode64' マウントオプションを使用してマウントする必要があります

ファイルシステムをマウントするには、 `mount –a`ホストでコマンドを実行します。

# 複数ホストの設定

この章では、2+1 SAP HANA マルチホストシステムのセットアップを例として説明します。

## SAP HANA マルチホストシステムの LUN 構成

次の表に示すように、 SAP HANA ホストで、ボリュームグループと論理ボリュームを作成してマウントする必要があります。

| 論理ボリューム（ **LV** ）またはボリューム | **SAP HANA** ホストのマウントポイント | 注 |
|---|---|---|
| lv ： FC5_data_mnt00001 -vol | /hana/data FC5/mnt00001 のように指定します | ストレージコネクタを使用してマウント |
| lv ： FC5_log_mnt00001 -vol | /hana/log/FC5/mnt00001 | ストレージコネクタを使用してマウント |
| lv ： FC5_data_mnt00002 -vol | /hana/data FC5/mnt00002 のように指定します | ストレージコネクタを使用してマウント |
| lv ： FC5_log_mnt00002 -vol | /hana/log/FC5/mnt00002 | ストレージコネクタを使用してマウント |
| ボリューム: FC5_shared | /hana/shared にアクセスします | NFS と /etc/fstab のエントリを使用して、すべてのホストにマウントされます |

説明した構成では、 `/usr/sap/FC5`ユーザー FC5adm のデフォルトのホーム ディレクトリが格納されているディレクトリは、各 HANA ホストのローカル ディスク上にあります。ディスクベースのレプリケーションによる災害復旧設定では、 NetAppは、以下の4つの追加サブディレクトリを作成することを推奨しています。 `FC5_shared`のボリューム `/usr/sap/FC5`ファイル システムを作成して、各データベース ホストのすべてのファイル システムを中央ストレージ上に配置します。

## LVM ボリュームグループと論理ボリュームを作成

1. すべての LUN を物理ボリュームとして初期化します。

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001
pvcreate /dev/mapper/hana-FC5_data_mnt00002
pvcreate /dev/mapper/hana-FC5_data2_mnt00002
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001
pvcreate /dev/mapper/hana-FC5_log_mnt00002
pvcreate /dev/mapper/hana-FC5_log2_mnt00002
```

2. 各データパーティションとログパーティションのボリュームグループを作成します。

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_data_mnt00002 /dev/mapper/hana-FC5_data_mnt00002
/dev/mapper/hana-FC5_data2_mnt00002
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
vgcreate FC5_log_mnt00002 /dev/mapper/hana-FC5_log_mnt00002
/dev/mapper/hana-FC5_log2_mnt00002
```

3. データパーティションとログパーティションごとに論理ボリュームを作成します。ボリュームグループごとに使用されている LUN の数（この例では 2 つ）と同じストライプサイズを使用し、データの場合は 256K 、ログの場合は 64k を使用します。SAP では、ボリュームグループごとに 1 つの論理ボリュームのみがサポートされます。

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. その他すべてのホストで、物理ボリューム、ボリュームグループ、およびボリュームグループをスキャンします。

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

これらのコマンドでボリュームが見つからない場合は、再起動する必要があります。

論理ボリュームをマウントするには、論理ボリュームをアクティブ化する必要があります。ボリュームをアクティブ化するには、次のコマンドを実行します。

```
vgchange -a y
```

ファイルシステムの作成

すべてのデータおよびログ論理ボリュームに XFS ファイル システムを作成します。

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_data_mnt00002-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs FC5_log_mnt00002-vol
```

マウントポイントを作成する

必要なマウント ポイント ディレクトリを作成し、すべてのワーカー ホストとスタンバイ ホストの権限を設定します。

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod -R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod -R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

ファイルシステムをマウント

マウントするには `/hana/shared`システム起動時にファイルシステムを使用する `/etc/fstab`設定ファイルに、`/hana/shared`ファイルシステムに `/etc/fstab`各ホストの構成ファイル。

```
sapcc-hana-tst:/ # cat /etc/fstab
<storage-ip>:/hana_shared /hana/shared nfs rw,vers=3,hard,timeo=600,
intr,noatime,nolock 0 0
```

すべてのデータファイルシステムとログファイルシステムは、 SAP HANA ストレージコネクタを使用してマウントされます。

ファイルシステムをマウントするには、各ホストで「 mount – a 」コマンドを実行します。

**SAP HANA** 向けの **I/O** スタック構成

## SAP HANA 1.0 SPS10 以降、 I/O 動作を調整し、使用中のファイルシステムとストレージシステムのデータベースを最適化するためのパラメータが導入されています。

ネットアップは、最適な値を定義するため、パフォーマンステストを実施しました。次の表に、パフォーマンステストから推定した最適な値を示します。

| パラメータ | 価値 |
| --- | --- |
| max_parallel _io_requests と入力します | 128 |

| パラメータ | 価値 |
| --- | --- |
| async _read_submit | オン |
| async ： write_submit_active | オン |
| async_write_submit_bblocks | すべて |

S12 までの SAP HANA 1.0 では、 SAP ノートに記載されているように、 SAP HANA データベースのインストール時にこれらのパラメータを設定できます "2267798 – Configuration of the SAP HANA Database During Installation Using hdbparam 』で説明されています"。

また、パラメータは、 SAP HANA データベースのインストール後に「 hdbparam 」フレームワークを使用して設定することもできます。

```
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_read_submit=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

SAP HANA 2.0 以降 'hdbparam' は廃止され ' パラメータは global.ini` ファイルに移動されましたパラメータは、 SQL コマンドまたは SAP HANA Studio を使用して設定できます。詳細については、 SAP ノートを参照してください "2399079 - Elimination of hdbparam in HANA 2 』を参照してください"。パラメータは 'global.ini` ファイル内で設定することもできます

```
SS3adm@stlrx300s8-6:/usr/sap/SS3/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

SAP HANA 2.0 SPS5 以降では、「 etParameter.py 」のスクリプトを使用して上記のパラメータを設定できます。

```
fc5adm@sapcc-hana-tst-03:/usr/sap/FC5/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

**SAP HANA** ソフトウェアのインストール

## 以下は、 SAP HANA ソフトウェアのインストール要件です。

シングルホストシステムにインストールします

SAP HANA ソフトウェアのインストールでは、シングルホストシステムについて行う追加の準備作業はありません。

マルチホストシステムにをインストールします

以下のインストール手順は、 SAP HANA 1.0 SPS12 以降に基づいています。

インストールを開始する前に 'global.ini` ファイルを作成して 'SAP ストレージ・コネクタの使用を有効にしますSAP ストレージコネクタは、インストールプロセス中にワーカーホストで必要なファイルシステムをマウントします。global.ini` ファイルは '/hana/shared-SID' ファイル・システムなど ' すべてのホストからアクセス可能なファイル・システムで使用できる必要があります

マルチホストシステムに SAP HANA ソフトウェアをインストールする前に、次の手順を実行する必要があります。

1. データ LUN およびログ LUN の次のマウント・オプションを global.ini` ファイルに追加します
   - 「データとログファイルシステム」の「 relatime 」と「 inode64 」です
2. データパーティションとログパーティションの WWID を追加します。WWID は '/etc/multipath.conf' ファイルに設定されているエイリアス名と一致している必要があります

   次の出力は、システム ID （ SID ）が SS3 の 2+1 マルチホストセットアップの例を示しています。

```
stlrx300s8-6:~ # cat /hana/shared/global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/SS3
basepath_logvolumes = /hana/log/SS3
[storage]
ha_provider = hdb_ha.fcClient
partition_*_*__prtype = 5
partition_*_data__mountoptions = -o relatime,inode64
partition_*_log__mountoptions = -o relatime,inode64,nobarrier
partition_1_data__wwid = hana-SS3_data_mnt00001
partition_1_log__wwid = hana-SS3_log_mnt00001
partition_2_data__wwid = hana-SS3_data_mnt00002
partition_2_log__wwid = hana-SS3_log_mnt00002
[system_information]
usage = custom
[trace]
ha_fcclient = info
stlrx300s8-6:~ #
```

LVM を使用した場合は、必要な設定が異なります。次の例は、 SID が FC5 の 2+1 マルチホストセットアップを示しています。

```
sapcc-hana-tst-03:/hana/shared # cat global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/FC5
basepath_logvolumes = /hana/log/FC5
[storage]
ha_provider = hdb_ha.fcClientLVM
partition_*_*__prtype = 5
partition_*_data__mountOptions = -o relatime,inode64
partition_*_log__mountOptions = -o relatime,inode64
partition_1_data__lvmname = FC5_data_mnt00001-vol
partition_1_log__lvmname = FC5_log_mnt00001-vol
partition_2_data__lvmname = FC5_data_mnt00002-vol
partition_2_log__lvmname = FC5_log_mnt00002-vol
sapcc-hana-tst-03:/hana/shared #
```

SAPインストールツールを使用して `hdblcm`、いずれかのワーカーホストで次のコマンドを実行してインストールを開始します。オプションを使用し `addhosts`て、2番目のワーカー（`sapc-hana-tst-06`）とスタンバイホスト（`sapc-hana-tst-07`）を追加します。準備したファイルが格納されているディレ

クトリ `global.ini`は(--storage_cfg=/hana/shared`、CLIオプションに含まれてい`storage_cfg`ます）。使用する OS のバージョンによっては、 SAP HANA データベースをインストールする前に Phyton 2.7 をインストールする必要があります。

```
/hdblcm --action=install --addhosts=sapcc-hana-tst
-06:role=worker:storage_partition=2,sapcc-hana-tst-07:role=standby
--storage_cfg=/hana/shared/

AP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1 (1.015.0)
in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
```

```
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip


SAP HANA Database version '2.00.073.00.1695288802' will be installed.

Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------
------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version 2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
  9     | epmmds          | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
```

```
4.203.2321.0.0

Enter comma-separated list of the selected indices [3,4]: 2,3
```

```
Verify that the installation tool installed all selected components at all
worker and standby hosts.
```

**SAP HANA** シングルホストシステムのデータボリュームパーティションを追加します

SAP HANA 2.0 SPS4 以降では、追加のデータボリュームパーティションを構成できます。この機能を使用すると、 SAP HANA テナントデータベースのデータボリュームに複数の LUN を設定し、単一 LUN のサイズやパフォーマンスの制限を超えて拡張することができます。

SAP HANA KPI を達成するために複数のパーティションを使用する必要はありません。単一の LUN にパーティションが 1 つあると、必要な KPI が満たされます。

データボリュームに複数の個別の LUN を使用することは、 SAP HANA シングルホストシステムでのみ可能です。SAP HANA マルチホストシステムに必要な SAP ストレージコネクタは、データボリュームに対して 1 つのデバイスのみをサポートします。

データボリュームのパーティションはいつでも追加できますが、 SAP HANA データベースの再起動が必要になる場合があります。

追加のデータボリュームパーティションの有効化

追加のデータボリュームパーティションを有効にするには、次の手順を実行します。

1. global.ini` ファイルに次のエントリを追加します

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

2. データベースを再起動して機能を有効にしてください。SAP HANA Studio でパラメータを global.ini` ファイルに追加する際に Systemdb 設定を使用すると、データベースが再起動されなくなります。

ボリュームと **LUN** の構成

ボリュームと LUN のレイアウトは、 1 つのデータボリュームパーティションを持つ単一のホストのレイアウトと似ていますが、追加のデータボリュームと LUN が、ログボリュームとして別のアグリゲートに格納され、他のデータボリュームも同様です。次の表は、 2 つのデータボリュームパーティションを持つ SAP HANA シングルホストシステムの構成例を示しています。

| コントローラ **A** のアグリゲート **1** | コントローラ **A** のアグリゲート **2** | コントローラ **B** のアグリゲート **1** | コントローラ **B** のアグリゲート **2** |
|---|---|---|---|
| データボリューム： SID_data_mnt00001 | 共有ボリューム： SID_shared | データボリューム： SID_data2_mnt00001 | ログボリューム： SID_log_mnt00001 |

次の表は、 2 つのデータボリュームパーティションを含むシングルホストシステムのマウントポイント構成の例を示しています。

| **LUN** | **HANA** ホストのマウントポイント | 注 |
|---|---|---|
| SID_data_mnt00001 | /hana/data/SID/mnt00001 | /etc/fstab エントリを使用してマウントされます |
| SID_data2_mnt00001 | /hana/data2/SID/mnt00001 | /etc/fstab エントリを使用してマウントされます |
| SID_log_mnt00001 | /hana/log/sid/mnt00001 | /etc/fstab エントリを使用してマウントされます |
| SID_shared | /hana/shared-SID を指定します | /etc/fstab エントリを使用してマウントされます |

ONTAP システムマネージャまたは ONTAP CLI を使用して、新しいデータ LUN を作成します。

ホストの設定

ホストを設定するには、次の手順を実行します。

1. セクション 0 の説明に従って、追加の LUN のマルチパスを設定します。
2. HANA システムに属する追加の LUN ごとに XFS ファイルシステムを作成します。

```
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana-FC5_data2_mnt00001
```

3. 追加のファイル・システム /s を '/etc/fstab 構成ファイルに追加します

> データ LUN の XFS ファイル・システムは 'relatim' および inode64' マウント・オプションを使用してマウントする必要がありますログ LUN の XFS ファイルシステムは 'relatim’inode64’nobarrier マウント・オプションを使用してマウントする必要があります

```
stlrx300s8-6:/ # cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/hana-FC5_log_mnt00001 /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/hana-FC5_data_mnt00001 /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/hana-FC5_data2_mnt00001 /hana/data2/FC5/mnt00001 xfs
relatime,inode64 0 0
```

4. マウントポイントを作成し、データベースホストに権限を設定します。

```
stlrx300s8-6:/ # mkdir -p /hana/data2/FC5/mnt00001
stlrx300s8-6:/ # chmod -R 777 /hana/data2/FC5
```

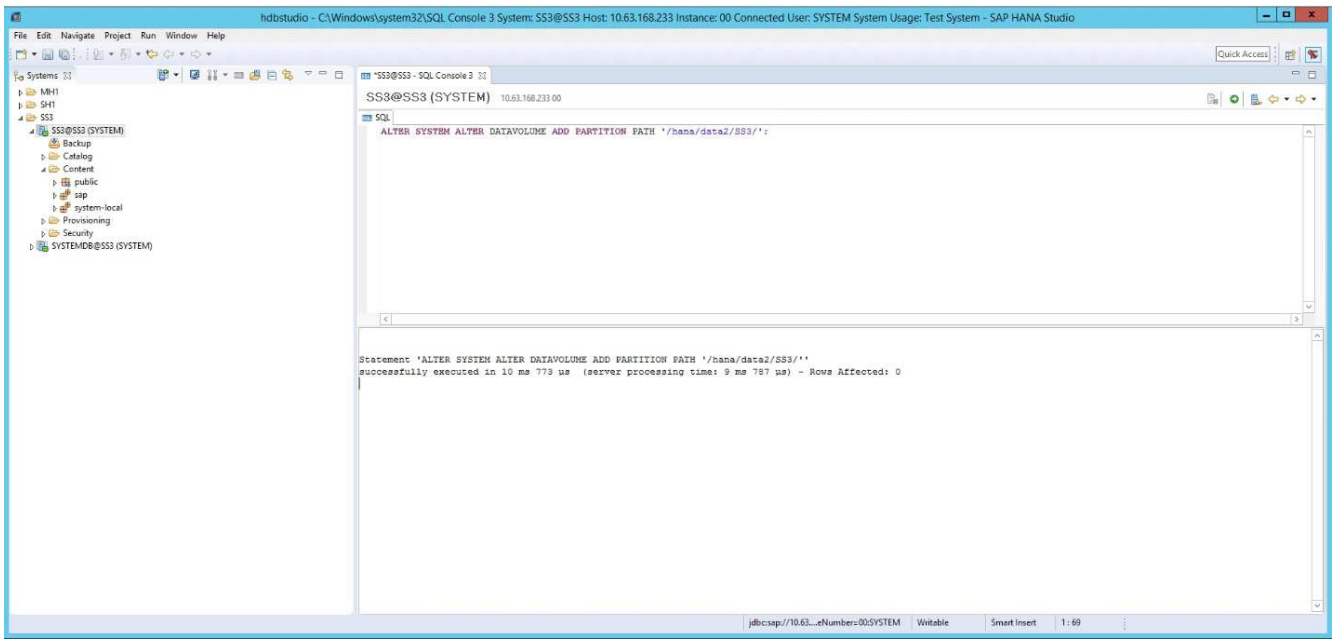
5. ファイルシステムをマウントするには、「 mount – a 」コマンドを実行します。

データボリュームパーティションを追加しています

データボリュームパーティションをテナントデータベースに追加するには、次の手順を実行します。

1. テナントデータベースに対して次の SQL ステートメントを実行します。追加する LUN のパスはそれぞれ異なります。

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```




## 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。

- "SAP HANA ソフトウェアソリューション"
- "TR-4646 ： 『 SAP HANA Disaster Recovery with Storage Replication 』"
- "TR-4614 ： 『 SAP HANA Backup and Recovery with SnapCenter 』"
- "TR-4667 ： 『Automating SAP System Copies Using the SnapCenter SAP HANA Plug-in』"
- ネットアップドキュメントセンター

"https://www.netapp.com/support-and-training/documentation/"

- SAP HANA 向け SAP 認定エンタープライズストレージハードウェア

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"

- SAP HANA のストレージ要件

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"

- 『 SAP HANA Tailored Data Center Integration Frequently Asked Questions 』

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"

- SAP HANA on VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"

- 『SAP HANA on VMware vSphere Best Practices Guide』

  "https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

## 履歴を更新します

この解決策の初版以降には、次の技術的な変更が加えられています。

| 日付 | 概要を更新します |
|---|---|
| 2015年2月 | 初版 |
| 2015年10月 | SAP HANA および HWVAL SPS 10 以降の I/O パラメータが含まれています |
| 2016年2月 | 容量のサイジングを更新しました |
| 2017年2月 | ネットアップの新しいストレージシステムとディスクシェルフ ONTAP 9 の新機能 SLES12 SP1 および Red Hat Enterprise Linux 7.2 新しい SAP HANA リリース |
| 2017年7月 | マイナーアップデート |
| 2018年9月 | 新しいネットアップストレージシステム新しい OS リリース（ SLES12 SP3 および Red Hat Enterprise Linux 7.4 ）では、 SAP HANA 2.0 SPS3 のマイナーアップデートが追加されています |
| 2019 年 9 月 | 新しい OS リリースマイナーアップデート |
| 2020年4月 | SAP HANA 2.0 SPS4 以降に複数のデータパーティション機能が導入されています |
| 2020 年 6 月 | 追加情報オプションの機能に関するマイナーアップデート |
| 2021年2月 | 新しいネットアップストレージシステムをサポートする Linux LVM （ SLES15SP2 、 RHEL 8 ） |
| 2021年4月 | VMware vSphere 固有の情報を追加しました |
| 2022年9月 | 新しいOS -リリース |

| 日付 | 概要を更新します |
| --- | --- |
| 2024年9月 | 新しいストレージシステム |
| 2025年2月 | 新しいストレージシステム |
| 2025年7月 | マイナーアップデート |

# バックアップ、リストア、ディザスタリカバリ

## 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。

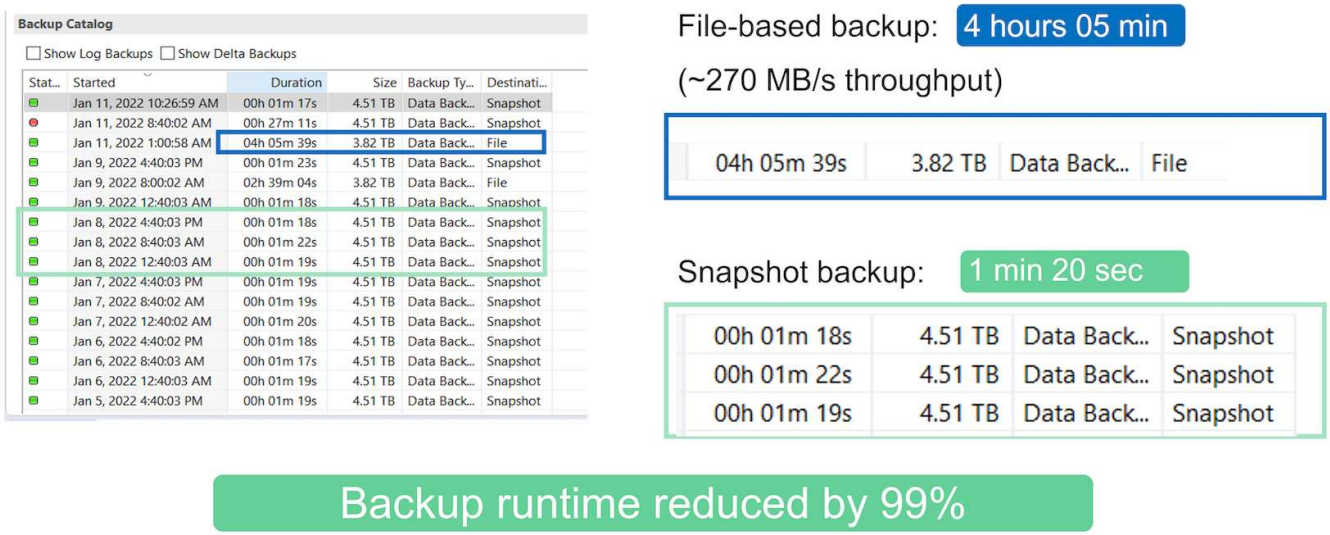
セカンダリストレージへのバックアップは、プライマリストレージに作成された Snapshot コピーがベースとなります。そのため、プライマリストレージシステムから直接データが読み取られ、 SAP データベースサーバに負荷は生成されません。プライマリストレージは、セカンダリストレージと直接通信し、NetApp SnapVault 機能を使用してバックアップデータをデスティネーションにレプリケートします。

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。




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、4 TB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。

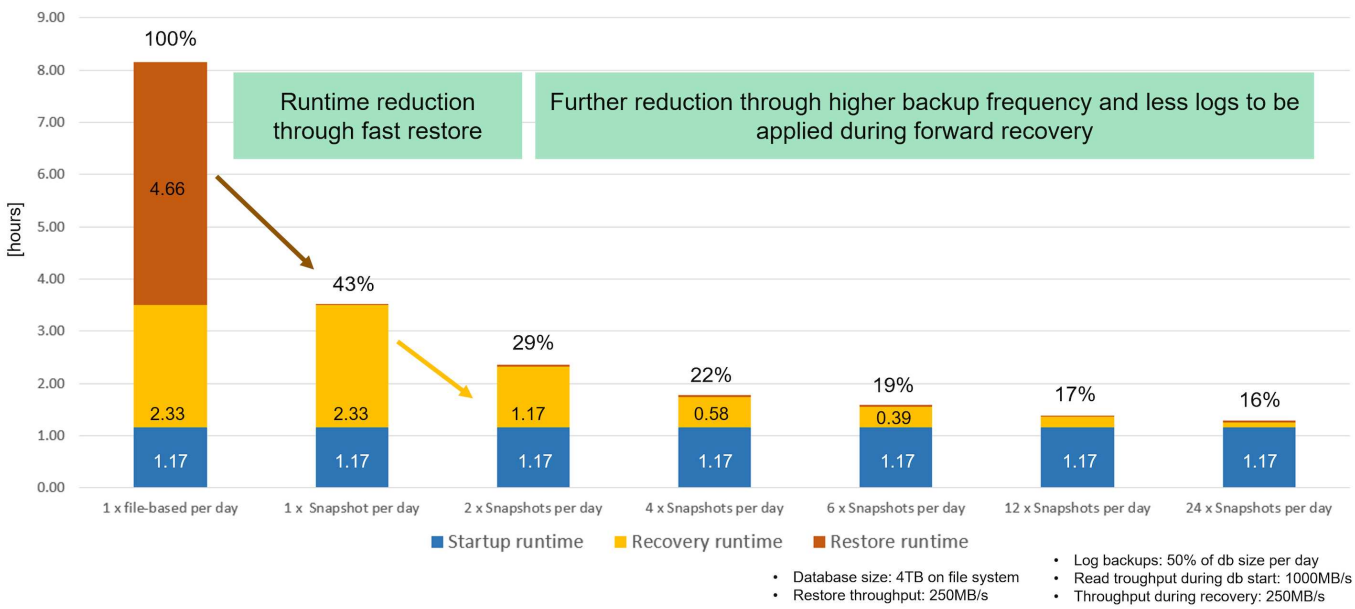
ファイルベースのデータバックアップでは、通常、バックアップスケジュールは 1 日に 1 回となります。バックアップによって本番環境のパフォーマンスが低下するため、通常はバックアップ頻度を高くすることはできません。したがって、最悪の場合は、フォワードリカバリ時に 1 日中に書き込まれたすべてのログを適用する必要があります。

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。




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。

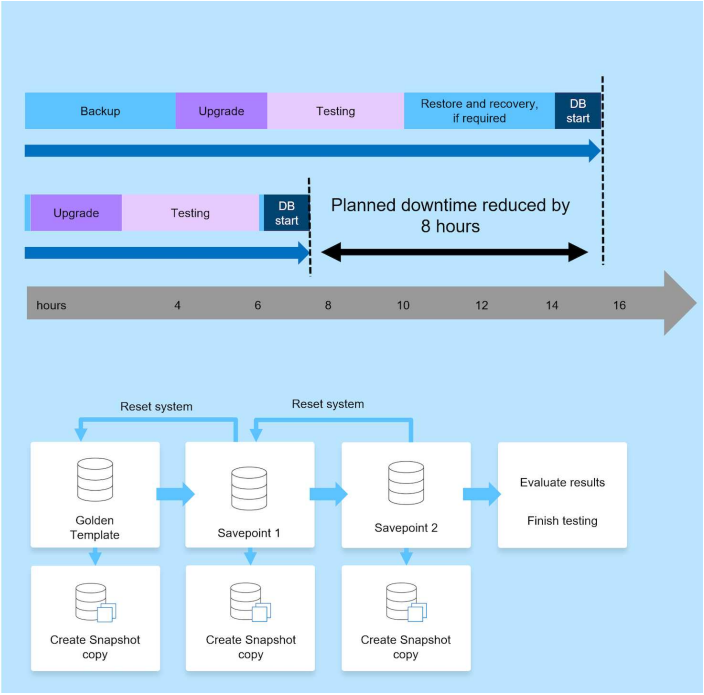
SAP HANAシステムのアップグレードは、たとえば、アップグレード前のオンデマンドバックアップと、アップグレードが失敗した場合のリストア処理が計画的停止全体に大きく影響する例です。4TBのデータベースの例を使用すると、Snapshotベースのバックアップおよびリストア処理を使用して、計画的なダウンタイムを8時間短縮できます。

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

- Acclerate 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。

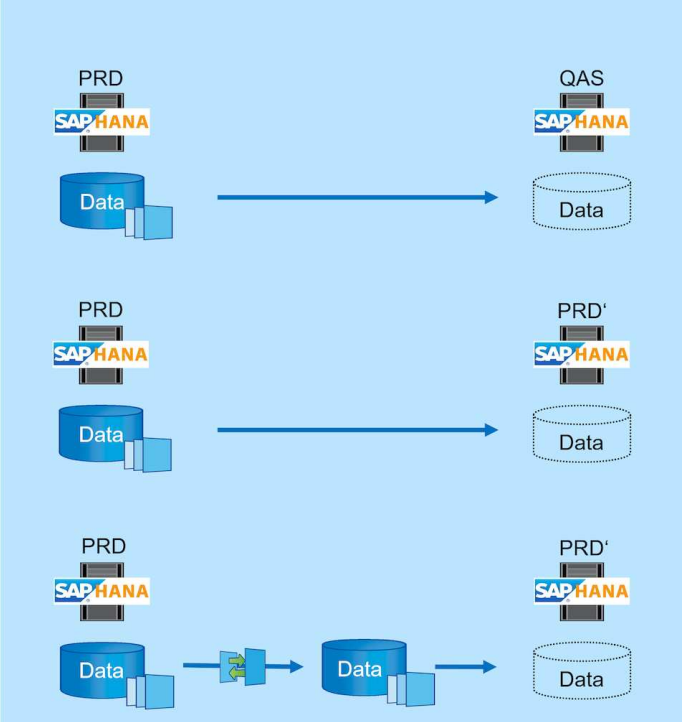
最も一般的なユースケースはSAPシステムの更新です。本番用システムのデータをテストシステムまたはQAシステムにコピーする必要があります。FSX for ONTAP クローニング機能を利用すると、本番用システムの任意のSnapshotコピーから、わずか数秒でテストシステム用のボリュームをプロビジョニングできます。その後、新しいボリュームをテストシステムに接続し、HANAデータベースをリカバリする必要があります。

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、本番用システムの古い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



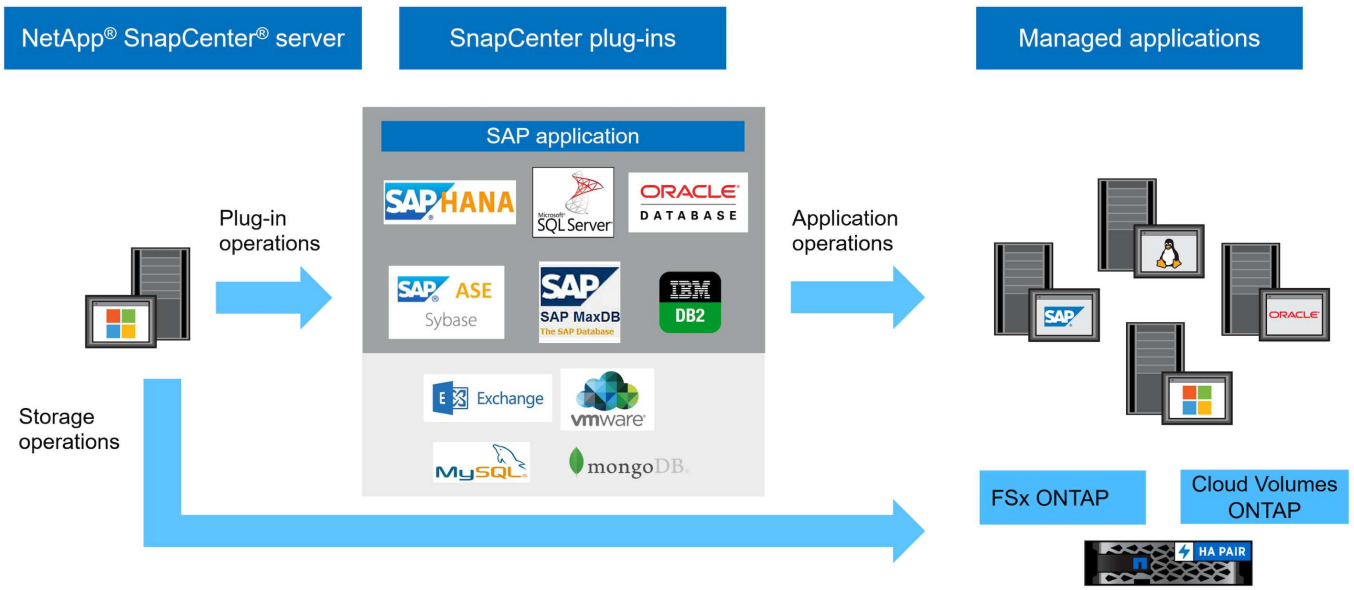

# SnapCenter アーキテクチャ

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、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。

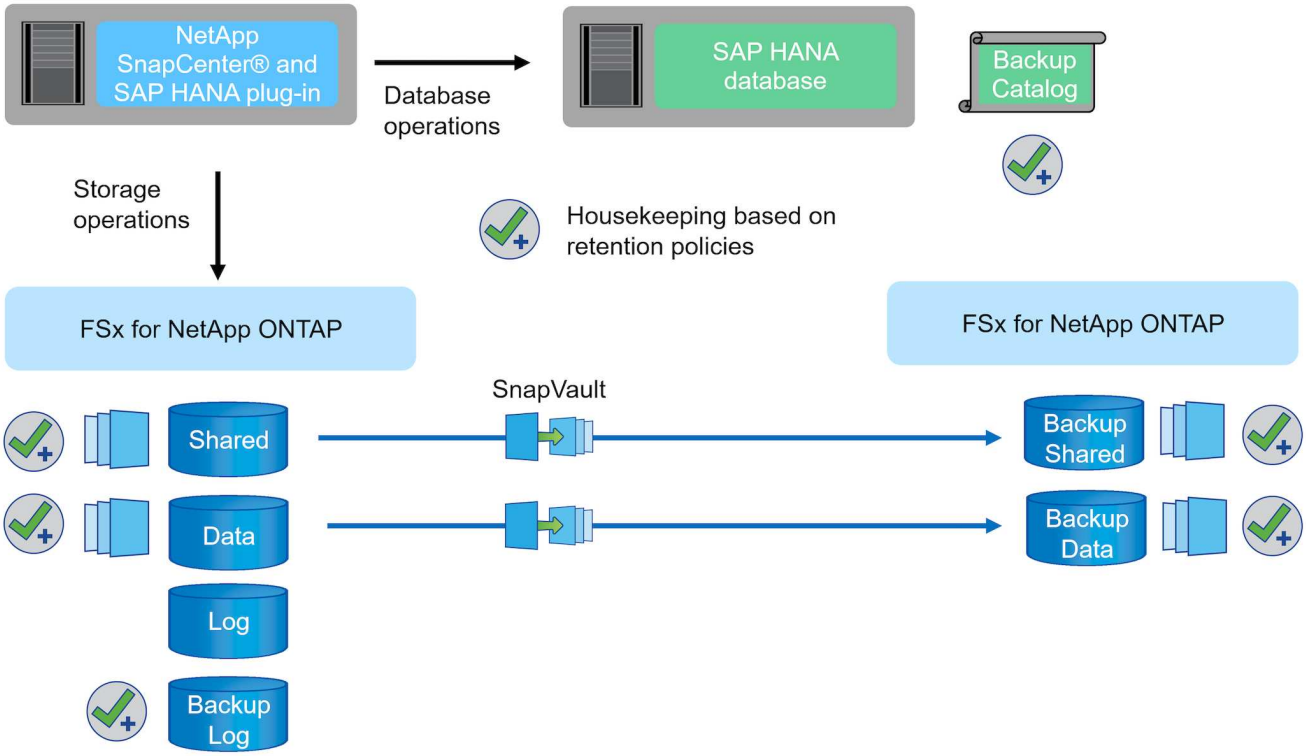
SnapCenter では、SAP HANA関連のすべてのリソースを完全にバックアップするために、ストレージベース

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。

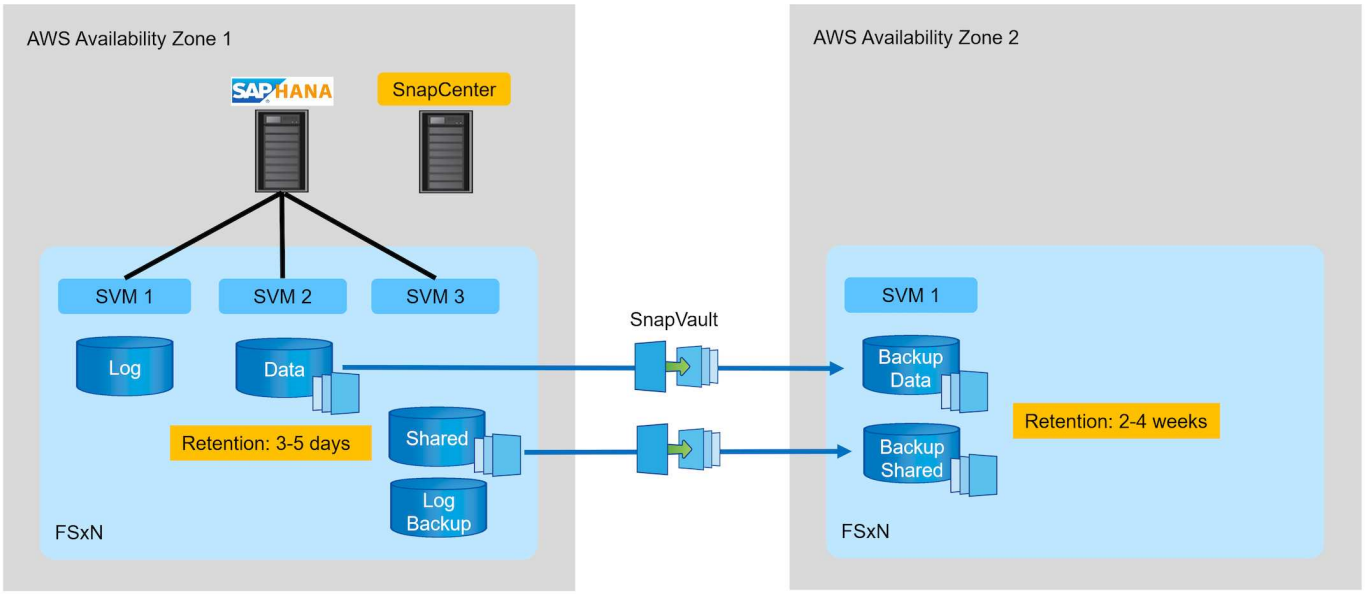
本ドキュメントの内容

このドキュメントでは、ONTAP 用FSXでシングルテナントを使用するSAP HANA MDCシングル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使用できます。また、場合によっては、複数ホストシステムの場合など、特定のSAP HANAシステムに必要な構成オプションもあります。その他の設定オプションの詳細については、を参照してください"SnapCenter の概念とベストプラクティス（netapp.com）"。

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）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**LocalSnap**です | ポリシー**LocalSnapAndSnapVault** | 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：

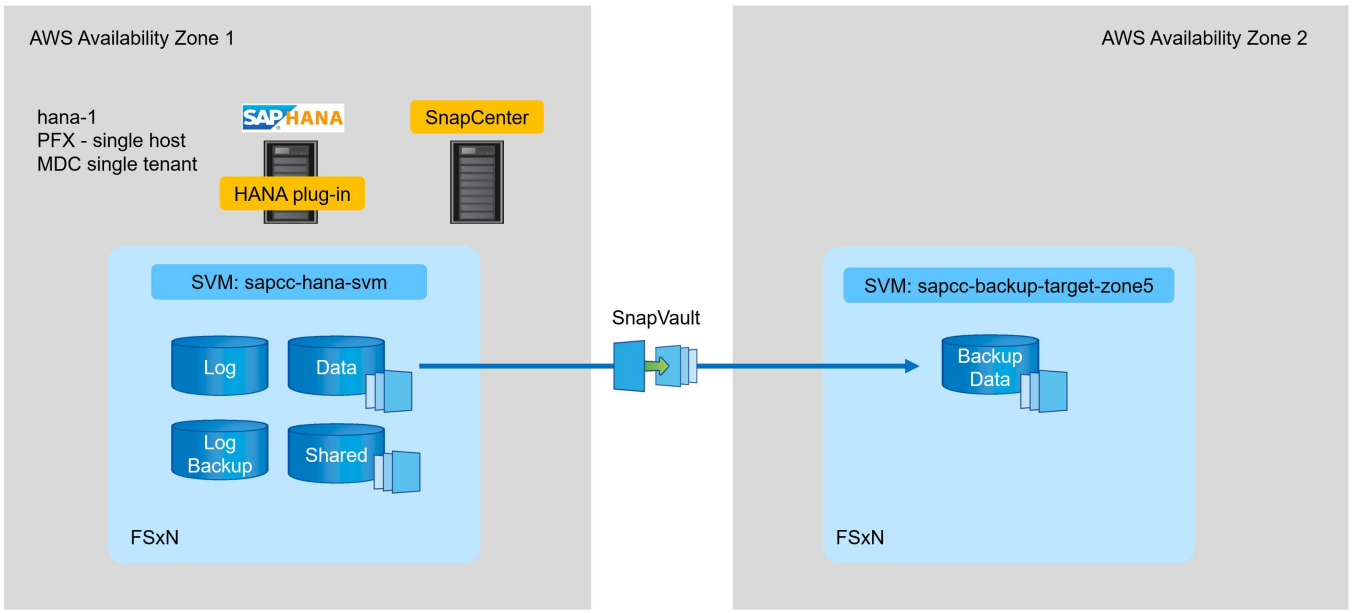
- シングルテナントのシングルホストMDCシステム
- HANA 2.0 SPS 6リビジョン60
- SLES for SAP 15SP3』を参照してください

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。

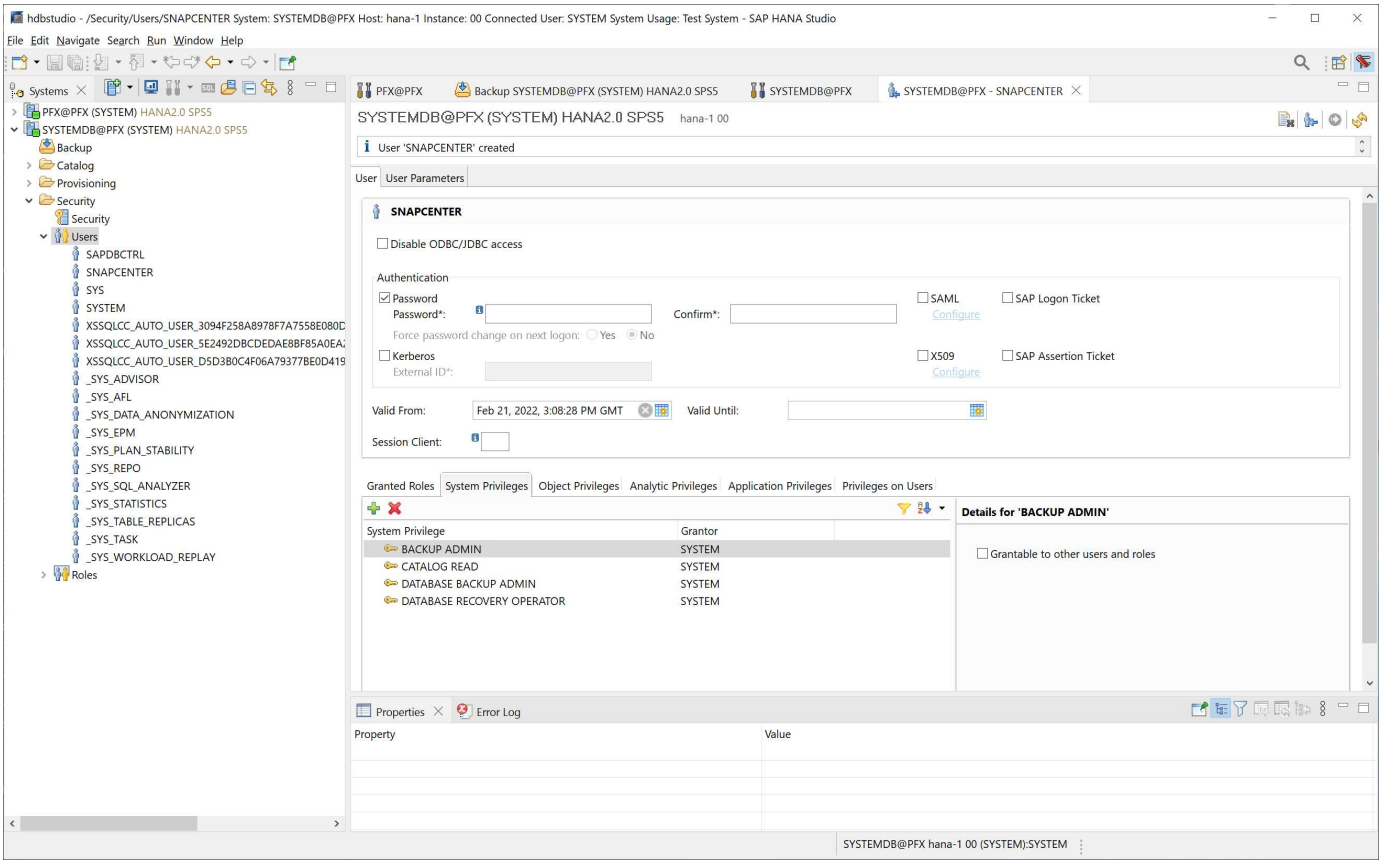
### SAP HANA のバックアップユーザと hdbuserstore の設定を指定します

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.
```

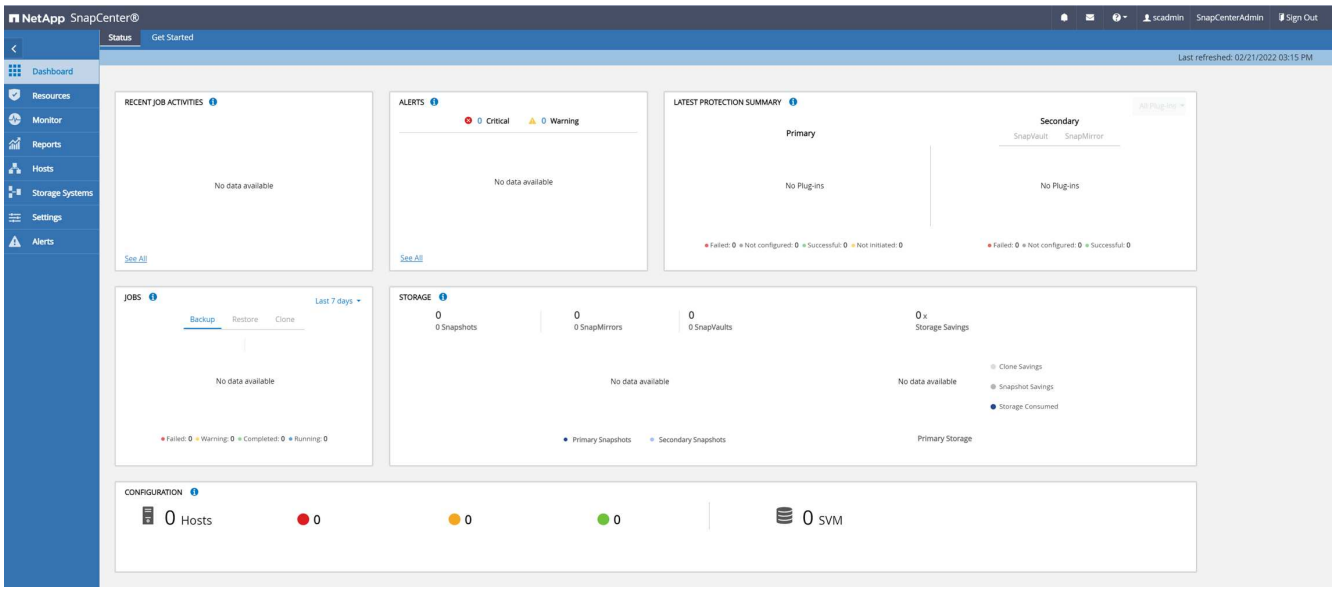
キーを使用するHANAシステムデータベースへのアクセスは、「hdbsql」コマンドで確認できます。

```
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=>
```

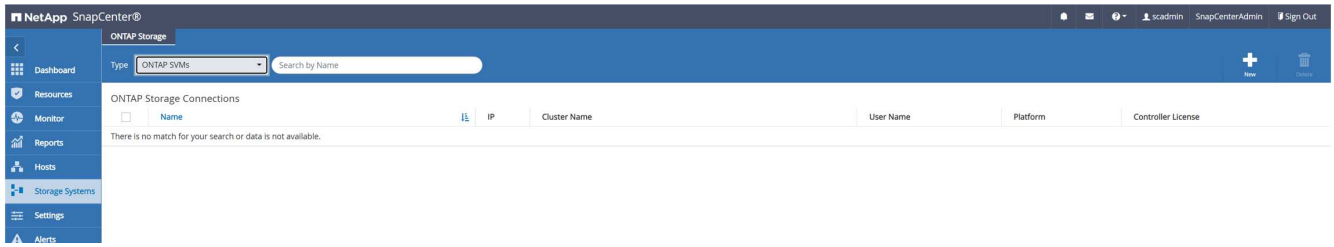
ストレージを設定する

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。

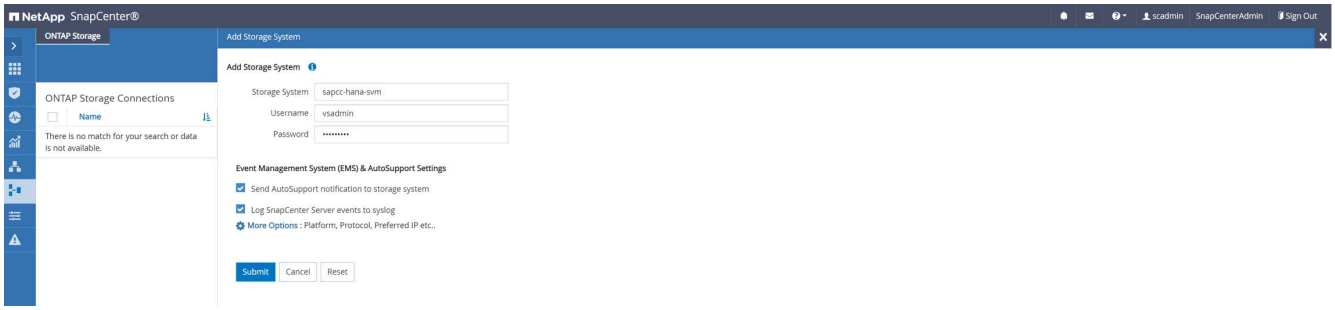



ストレージシステムのタイプとして、ONTAP SVMまたはONTAP クラスタを選択できます。次の例では、SVM管理を選択しています。

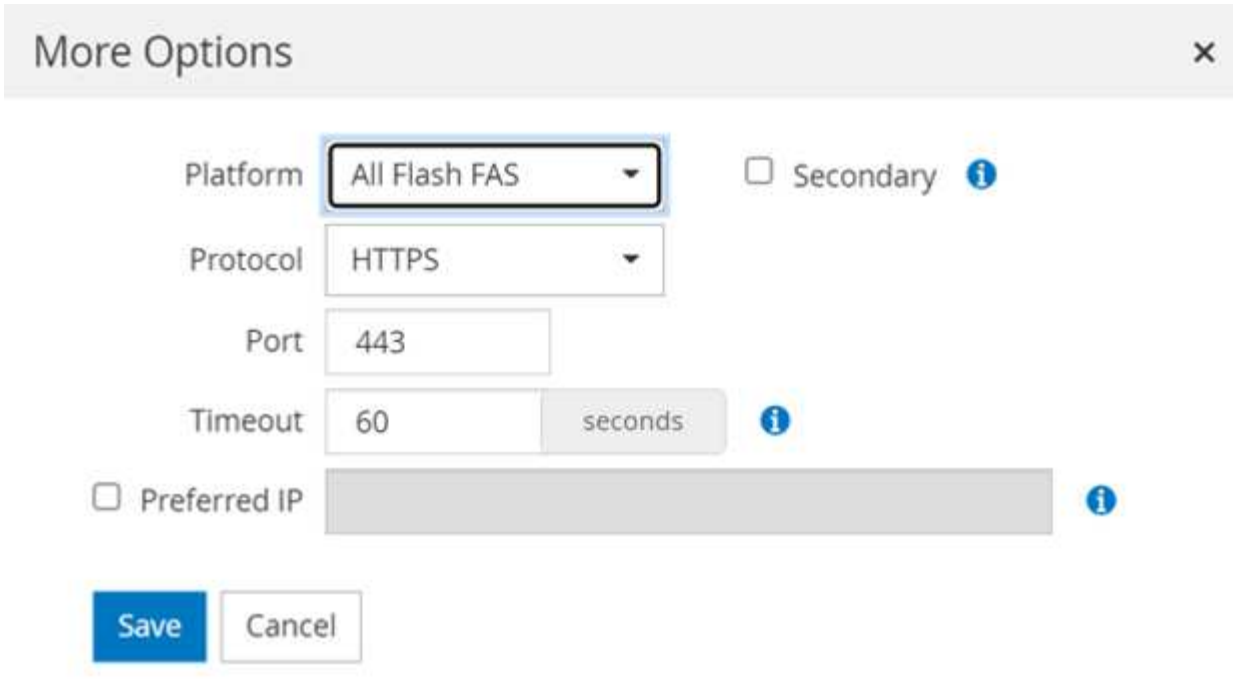



2. ストレージシステムを追加し、必要なホスト名とクレデンシャルを入力するには、Newをクリックします。

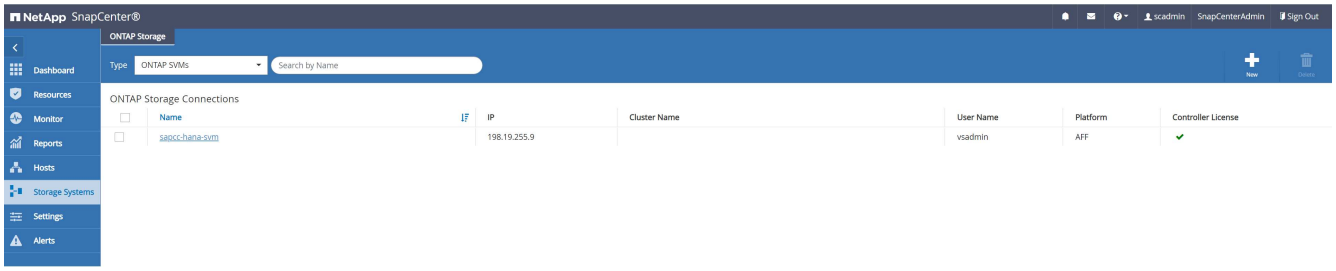
次の図に示すように、SVMユーザをvsadminユーザにする必要はありません。通常、ユーザは SVM 上で設定し、バックアップとリストアの処理を実行するために必要な権限を割り当てます。必要な権限については、を参照してください "SnapCenter インストールガイド" 「 Minimum ONTAP Privileges Required 」の項を参照してください。




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。



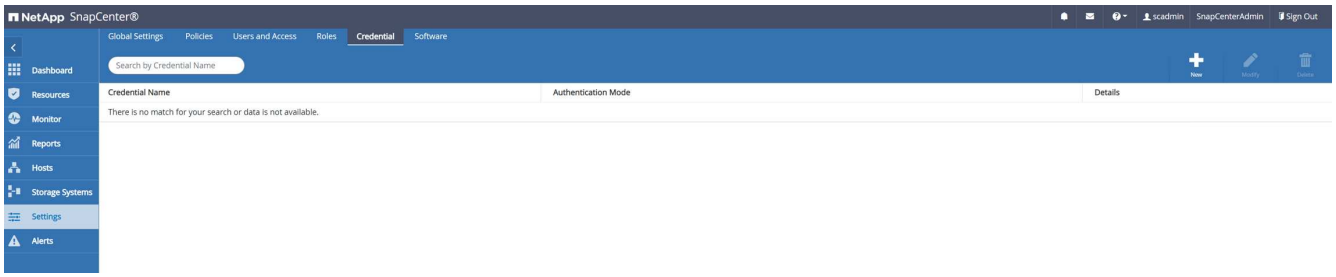

SVM「sapcc-sana-svm」がSnapCenter で設定されました。



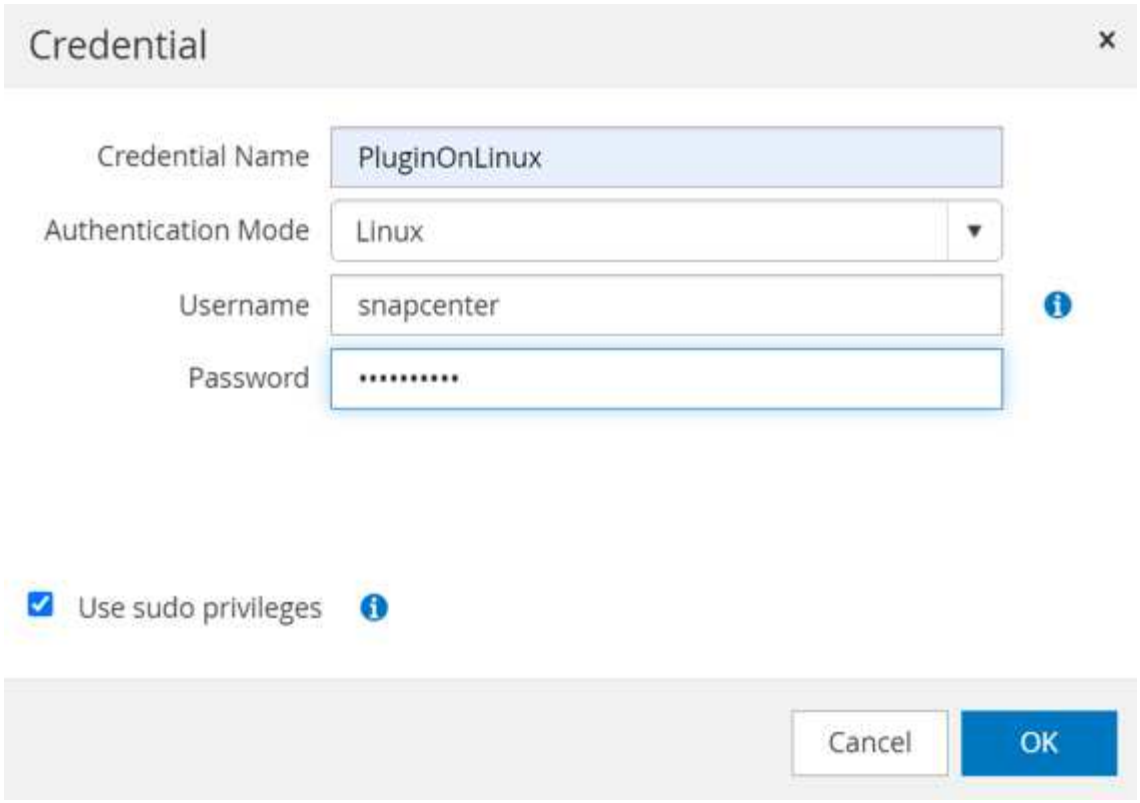

プラグイン導入用のクレデンシャルを作成します

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




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 prvileeを有効にする必要があります。




```
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。

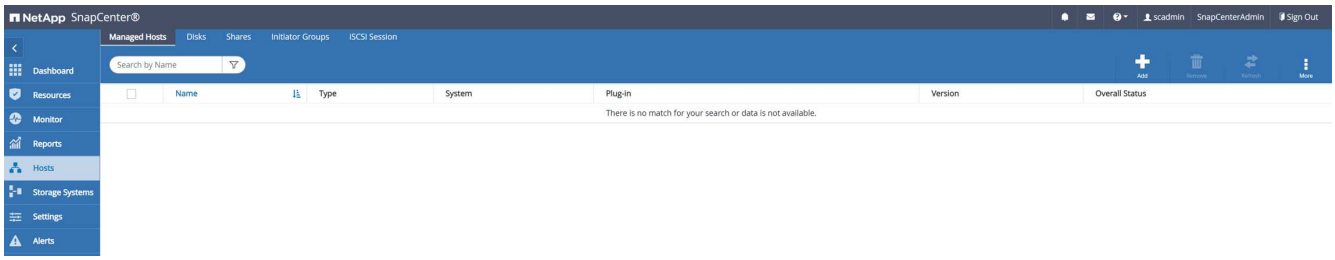
SAP HANA プラグインには、 Java 64 ビットバージョン 1.8 が必要です。ホストをSnapCenter に追加する前に、ホストにJavaをインストールする必要があります。

```
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 #
```

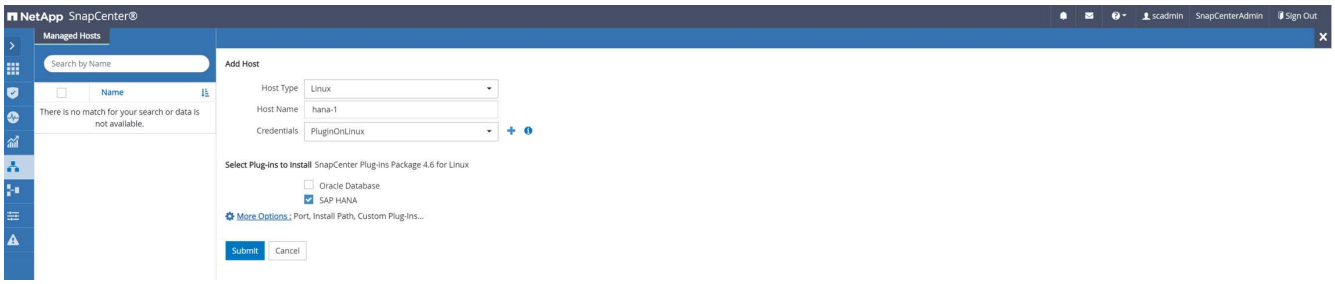
OpenJDKまたはOracle JavaはSnapCenter でサポートされています。

SAP HANAホストを追加するには、次の手順を実行します。

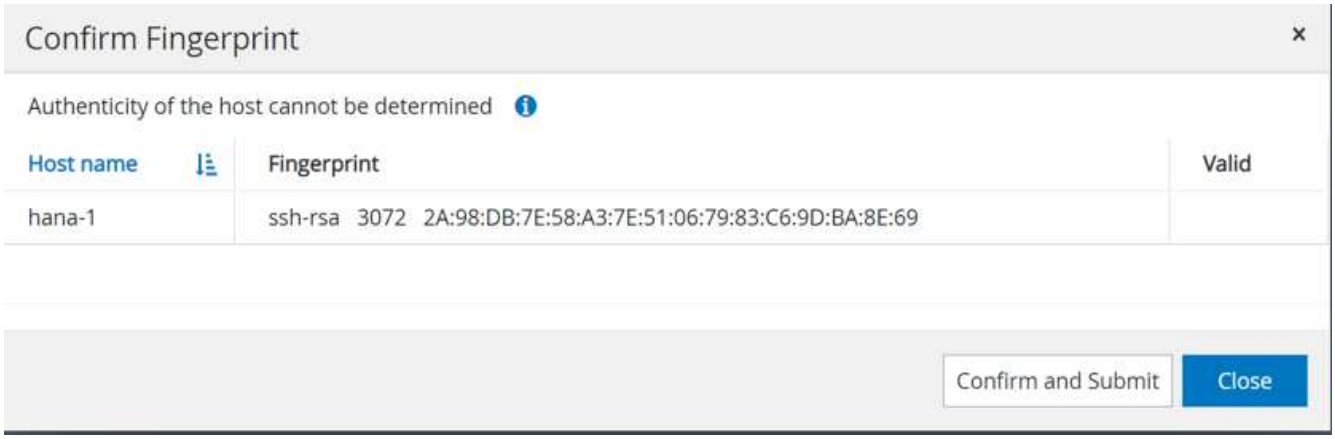
1. ホストタブで、追加をクリックします。




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。

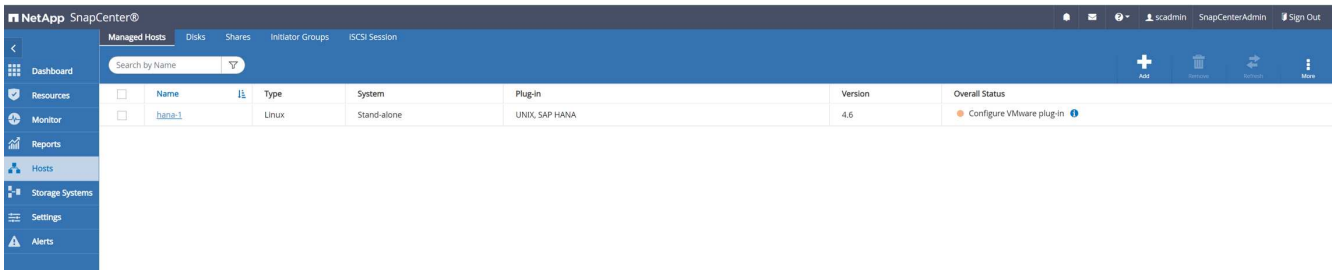



3. フィンガープリントを確認します。



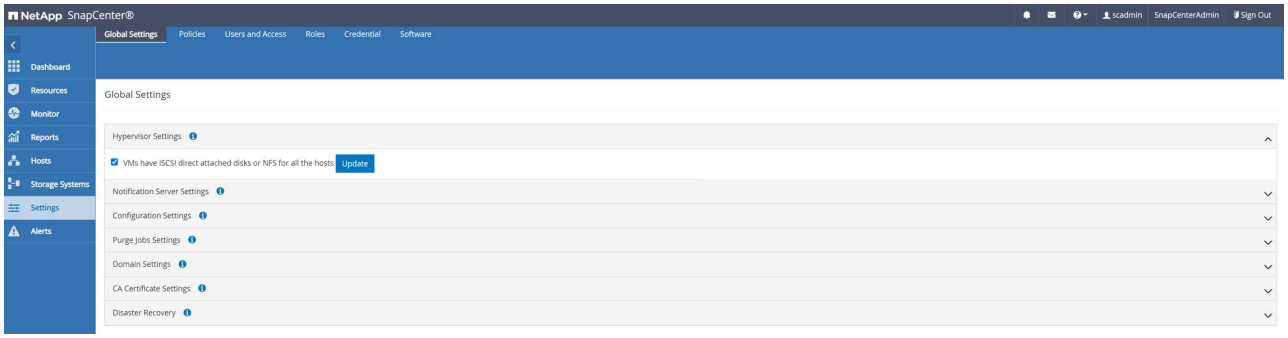

HANAとLinuxプラグインのインストールが自動的に開始されます。インストールが完了すると、ホストのステータス列にConfigure VMware Plug-inと表示されます。SnapCenter は、 SAP HANA プラグインが仮想環境にインストールされているかどうかを検出します。これは、VMware環境か、パブリッククラウドプロバイダの環境です。この場合、SnapCenter はハイパーバイザーを設定するように警告を表示します。

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。

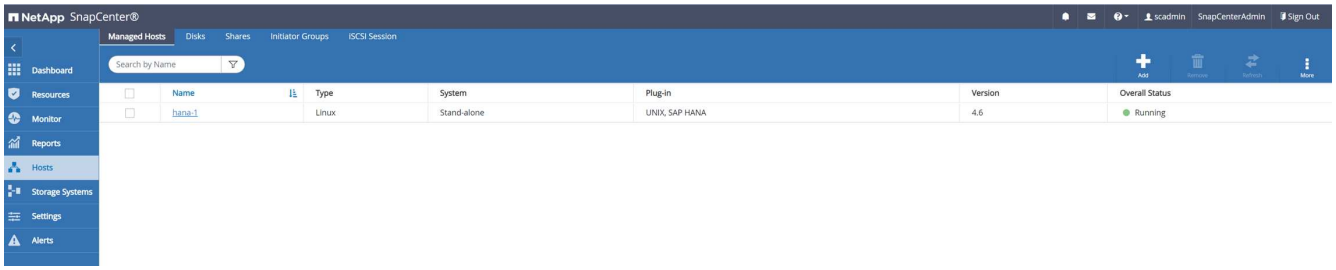



a. [ 設定 ] タブで、 [ グローバル設定 ] を選択します。

b. 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。

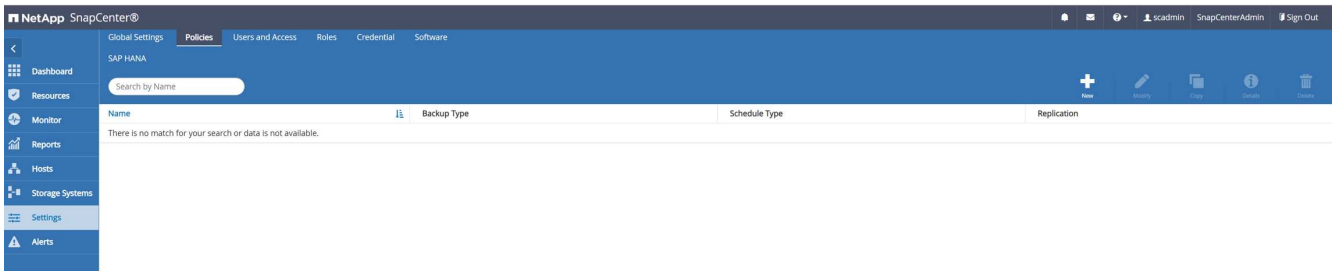
- レプリケーションを行わずに1時間ごとのバックアップを行うためのポリシー：LocalSnap
- ファイル・ベースのバックアップを使用した週次ブロック整合性チェックのポリシー：BlockIntegrityCheck

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。

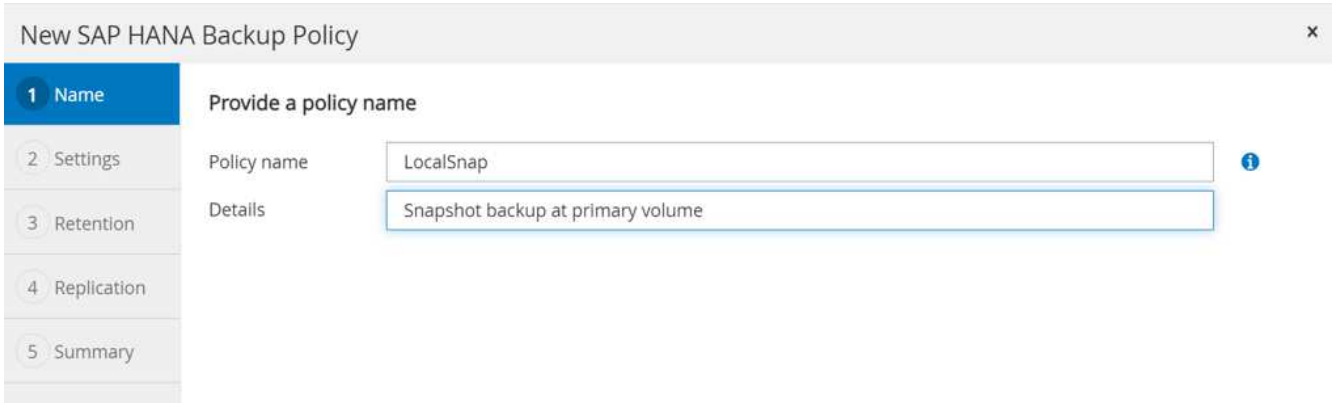
**Snapshot**バックアップのポリシー

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。

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

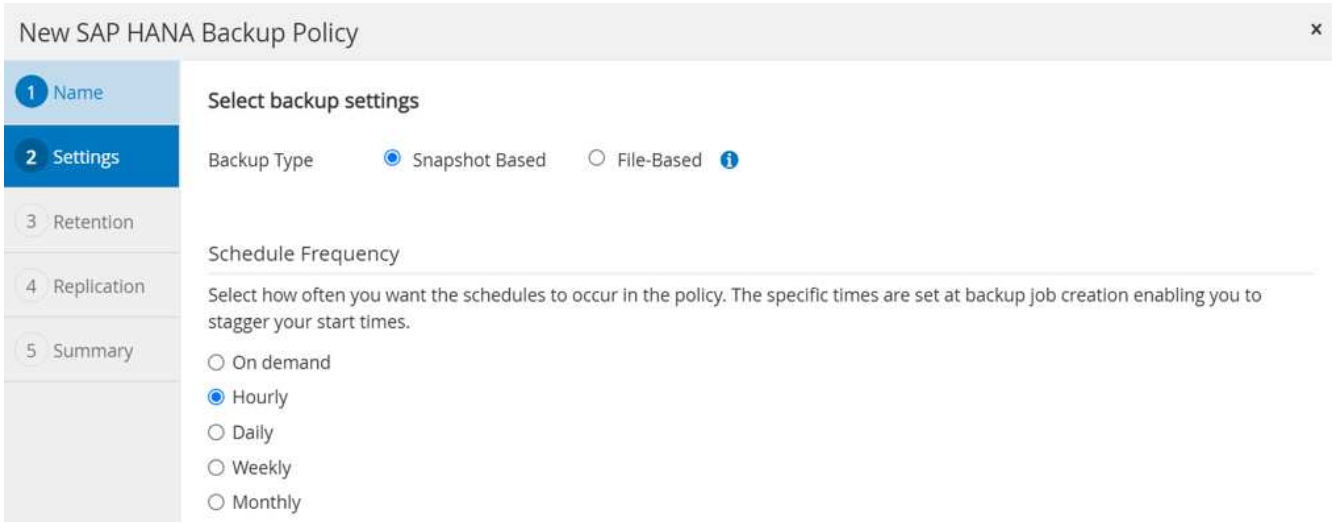



2. ポリシー名と概要を入力します。次へをクリックします。

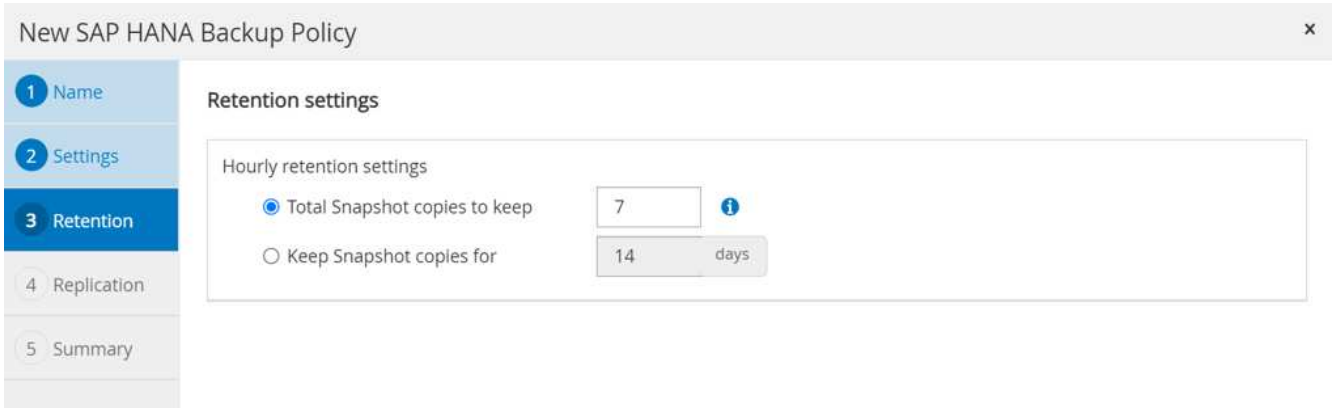



3. バックアップタイプとして「 Snapshot Based 」を選択し、スケジュール頻度を選択するには「 Hourly 」を選択します。

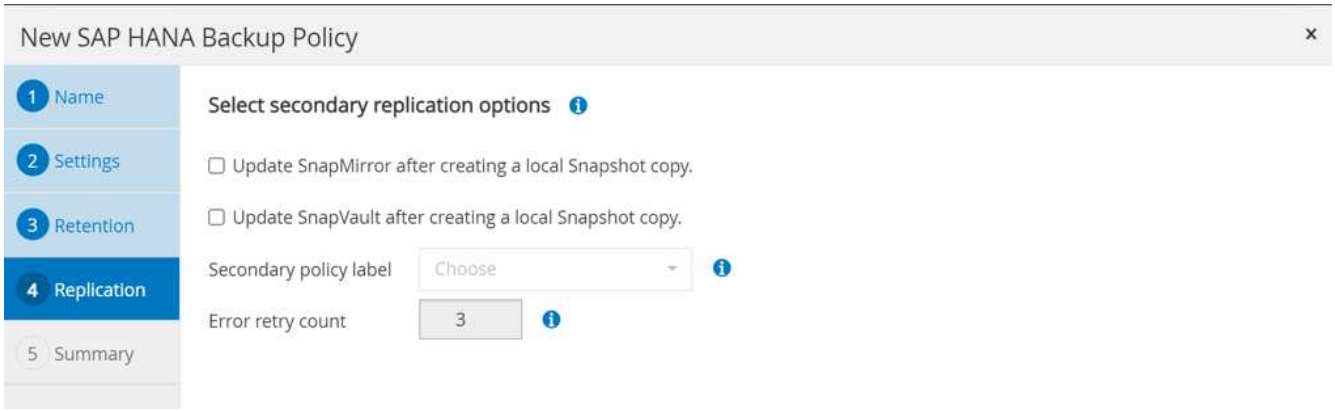
   スケジュール自体は、あとでHANAのリソース保護構成で設定します。

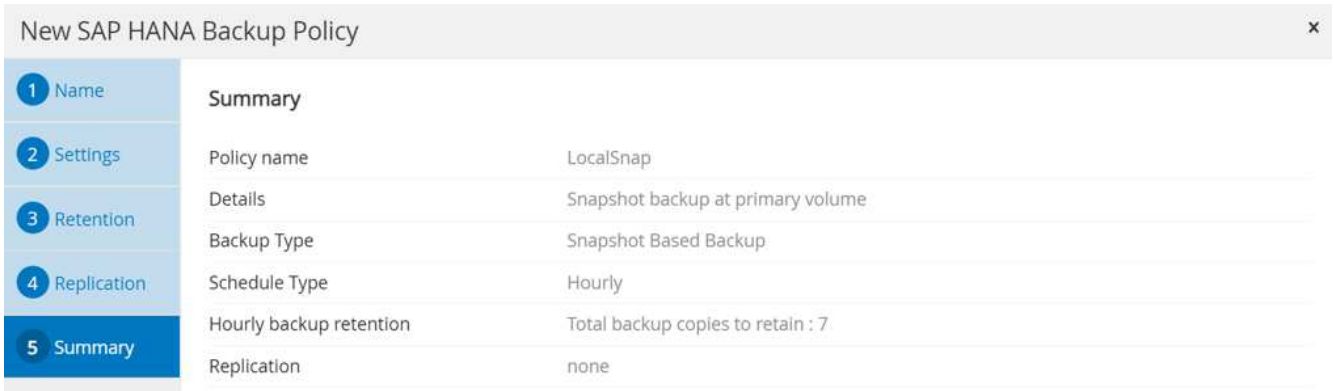



4. オンデマンドバックアップの保持を設定します。

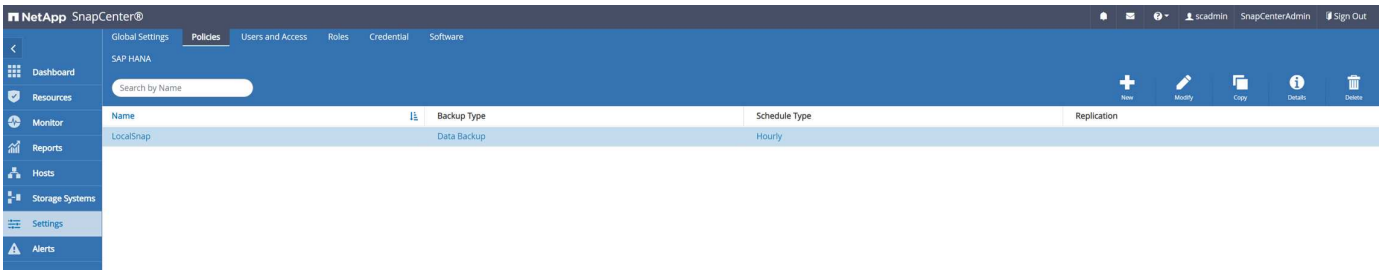



5. レプリケーションオプションを設定します。この場合、 SnapVault または SnapMirror の更新は選択されていません。



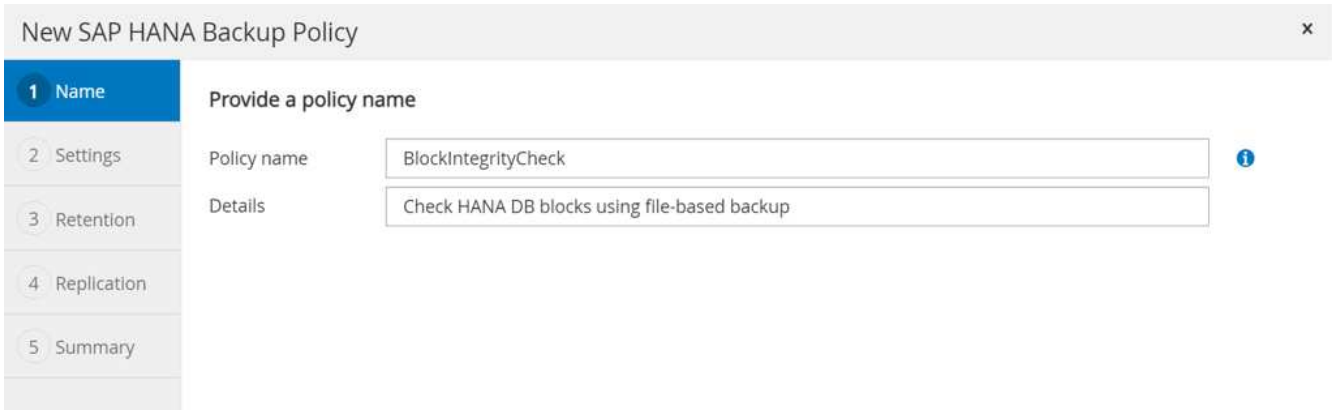




これで新しいポリシーが設定されました。

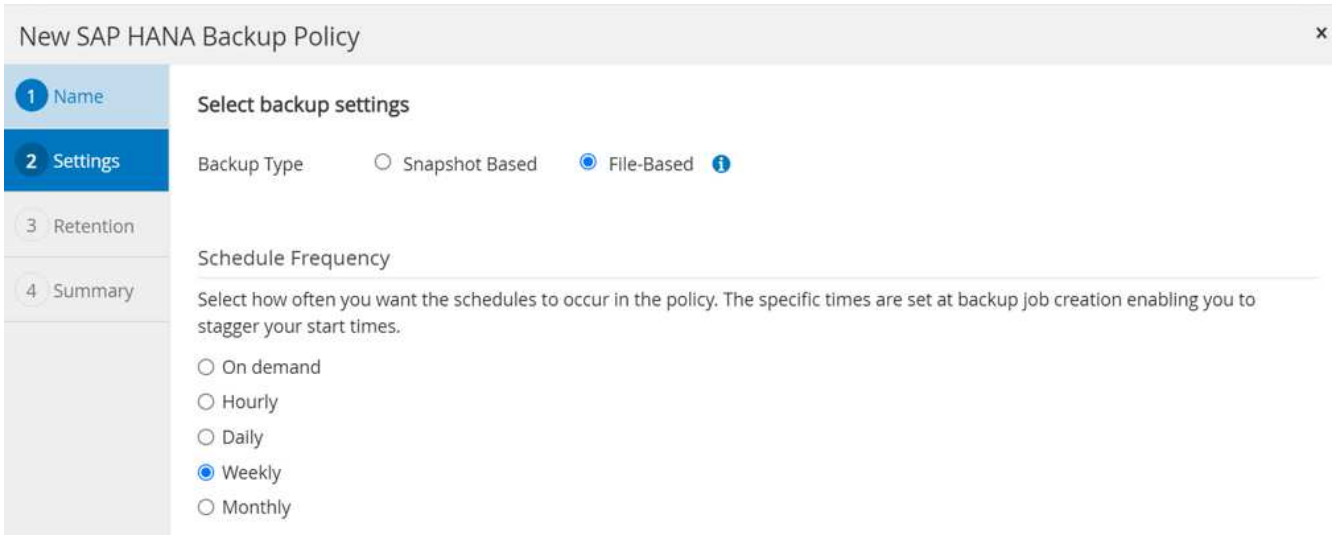


ブロック整合性チェックポリシーを設定する手順は、次のとおりです。

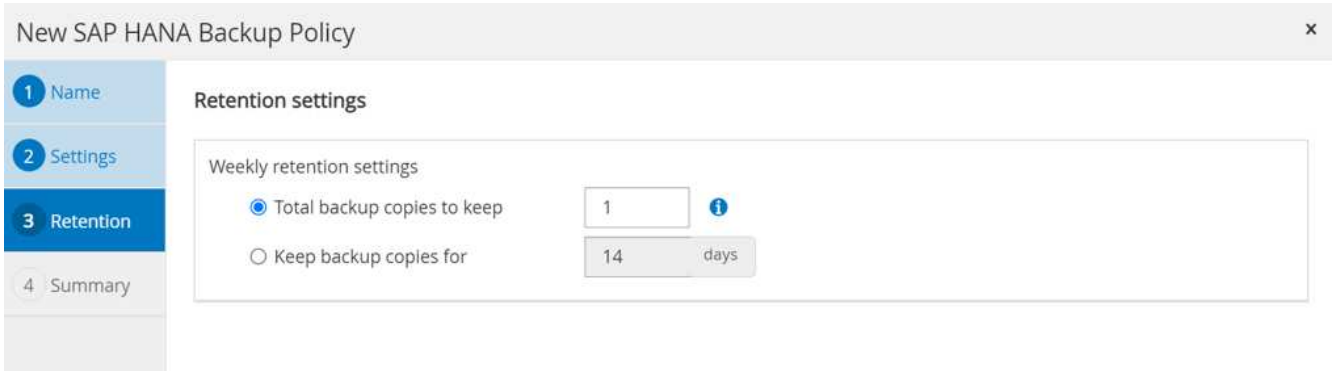
1. [ 設定 ] 、 [ ポリシー ] の順に移動し、 [ 新規 ] をクリックします
2. ポリシー名と概要を入力します。次へをクリックします。



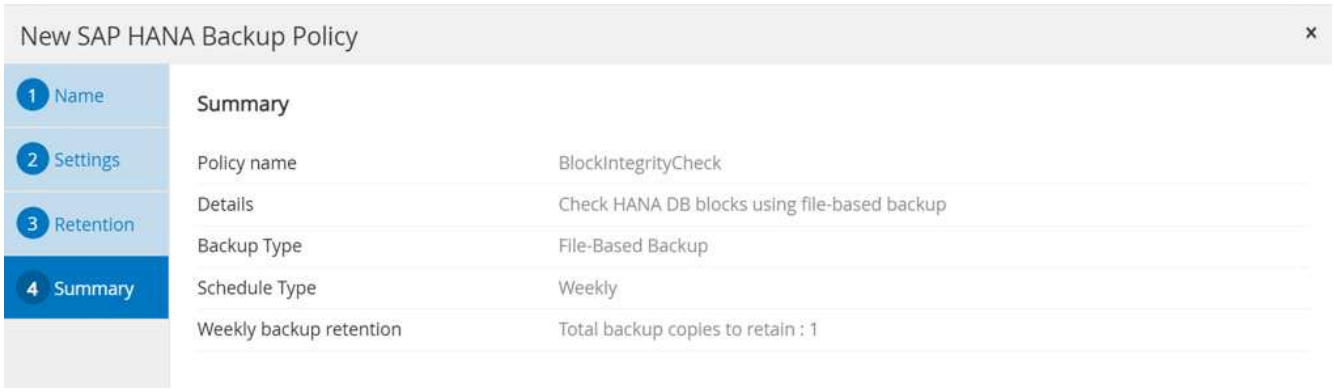

3. バックアップタイプを「ファイルベース」に、スケジュール頻度を「毎週」に設定します。スケジュール自体は、あとでHANAのリソース保護構成で設定します。

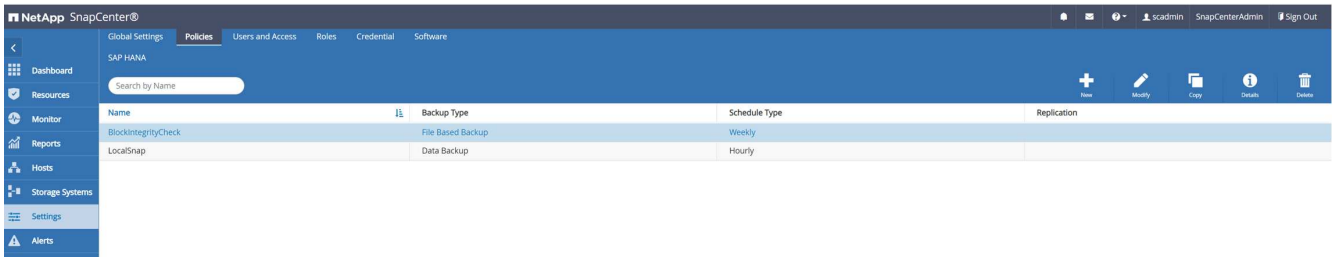



4. オンデマンドバックアップの保持を設定します。



5. [ 概要 ] ページで、 [ 完了 ] をクリックします。



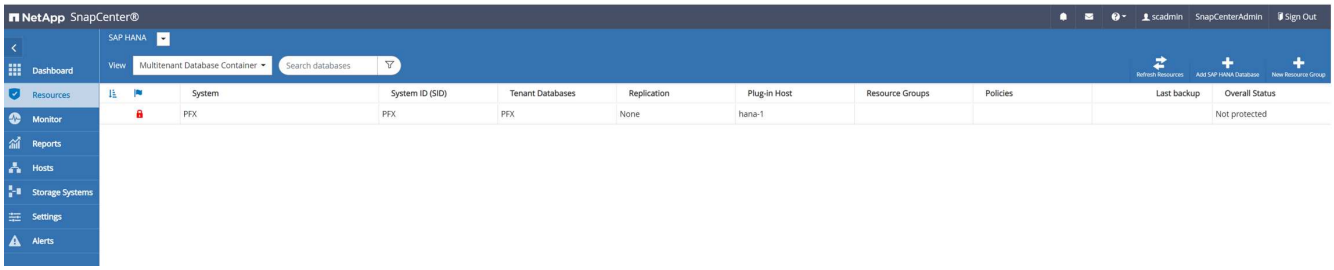




## HANAリソースを構成して保護

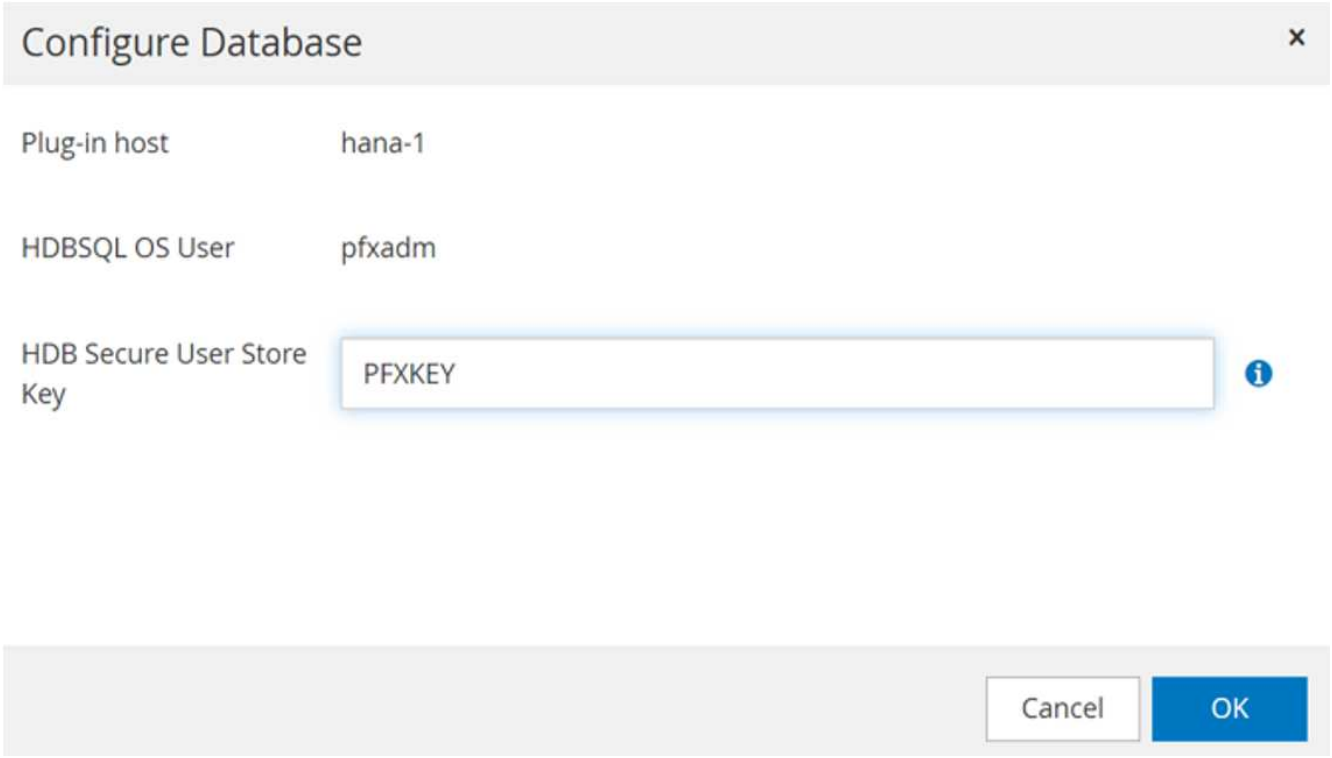
プラグインのインストール後、 HANA リソースの自動検出プロセスが自動的に開始されます。[ リソース ] 画面で、新しいリソースが作成されます。このリソースは、赤い南京錠のアイコンでロックされていることが示されます。新しいHANAリソースを設定して保護するには、次の手順を実行します。

1. を選択し、リソースをクリックして設定を続行します。

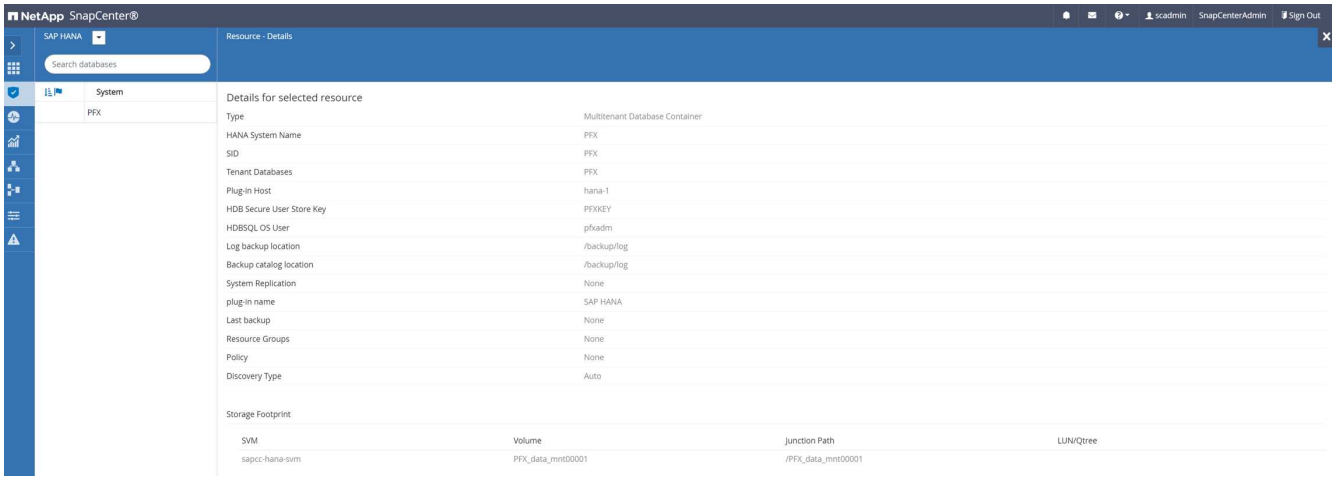
   [リソースの更新]をクリックして、[リソース]画面で自動検出プロセスを手動で開始することもできます。



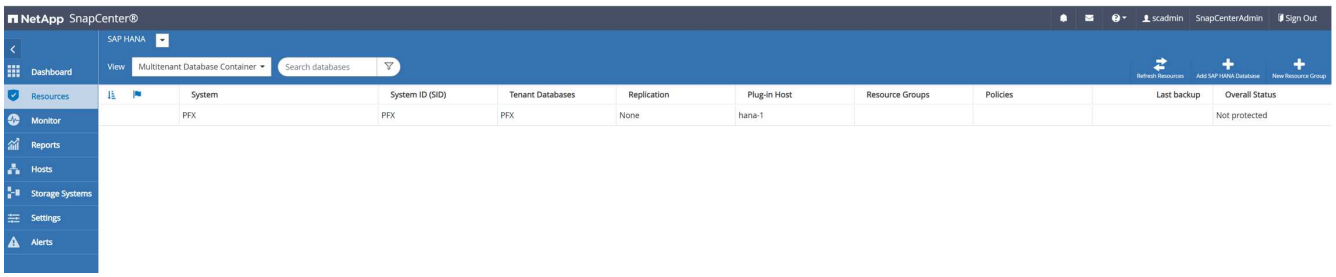

2. HANA データベースのユーザストアキーを指定します。




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。

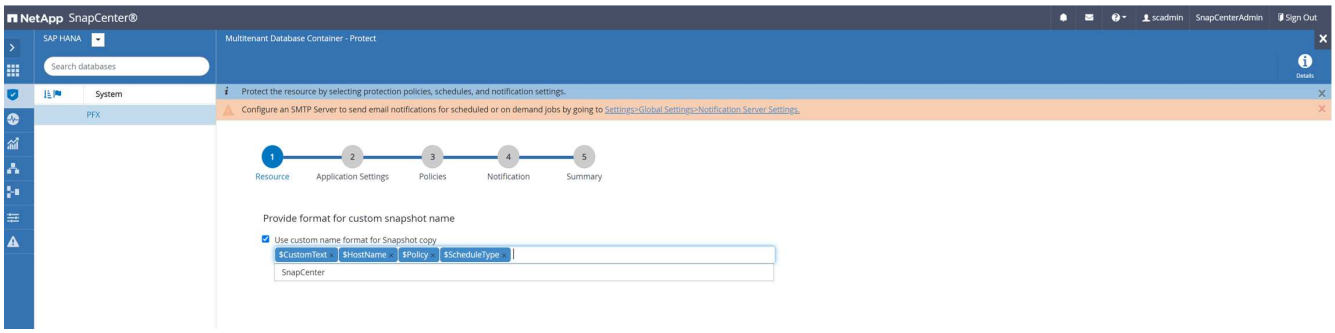



3. [リソース]タブで、リソースをダブルクリックしてリソース保護を構成します。

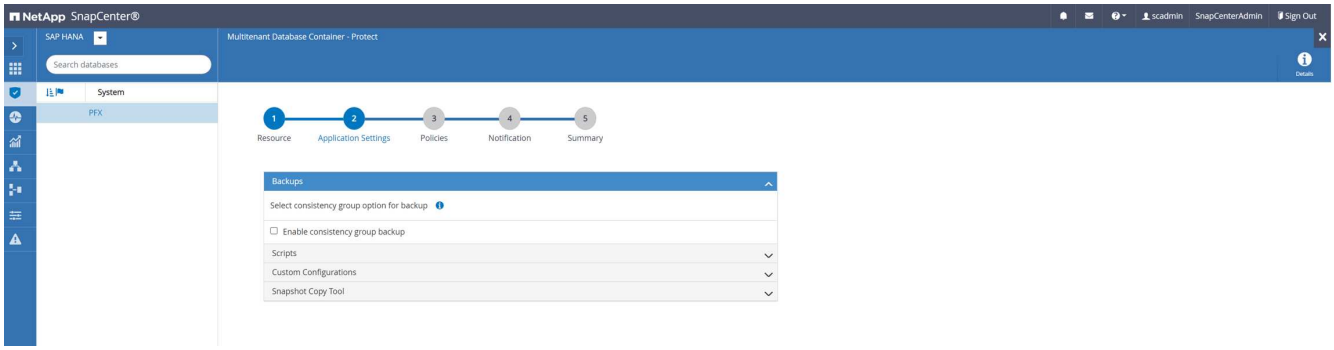



4. Snapshot コピーにカスタムの名前形式を設定します。

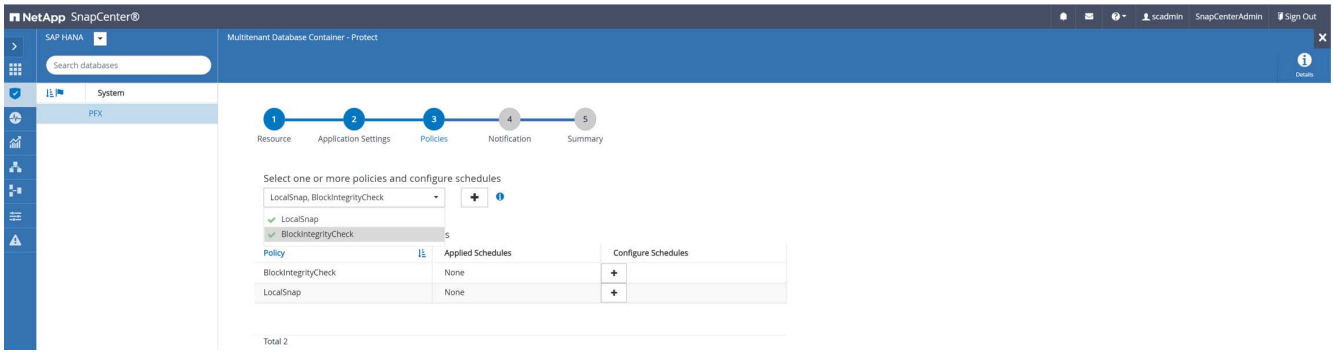
カスタムの Snapshot コピー名を使用して、どのバックアップがどのポリシーおよびスケジュールタイプで作成されたかを簡単に識別することを推奨します。Snapshot コピー名にスケジュールタイプを追加することで、スケジュールバックアップとオンデマンドバックアップを区別できます。オンデマンドバックアップの「スケジュール名」文字列は空ですが、スケジュールバックアップには「毎時」、「毎日」、または「毎週」という文字列が含まれます。




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。

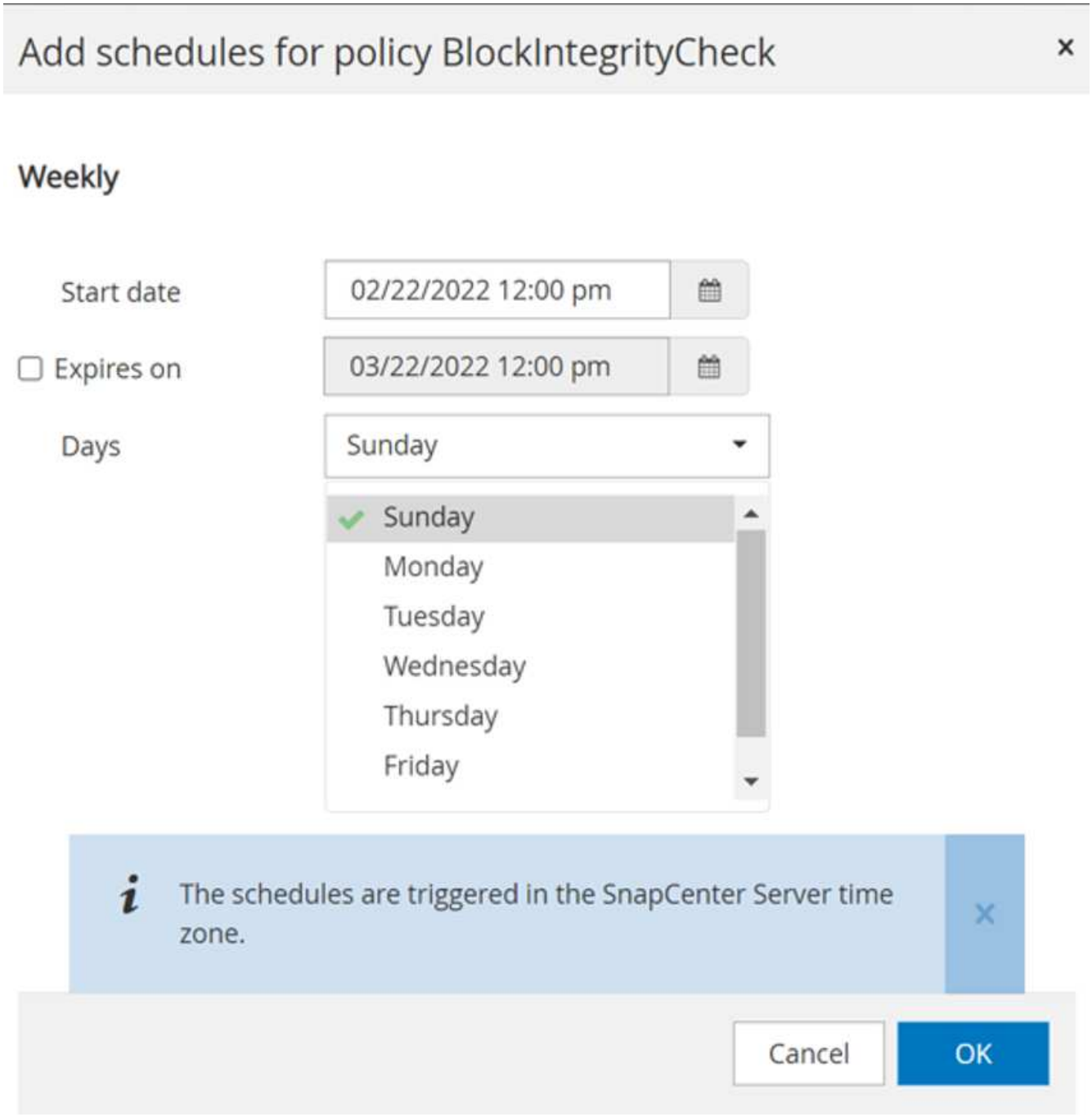



6. リソースに追加するポリシーを選択してください。



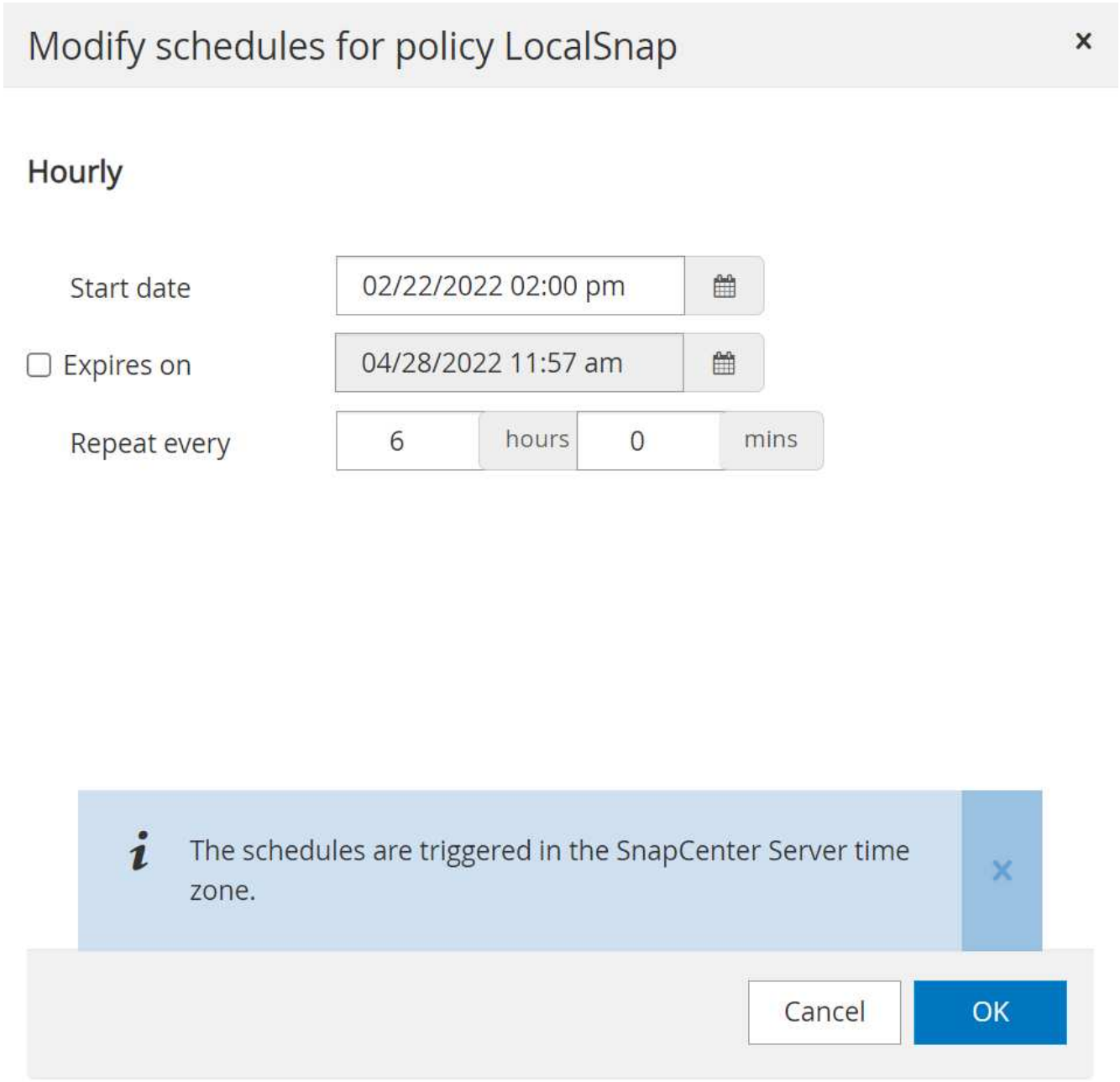

7. ブロック整合性チェックポリシーのスケジュールを定義します。

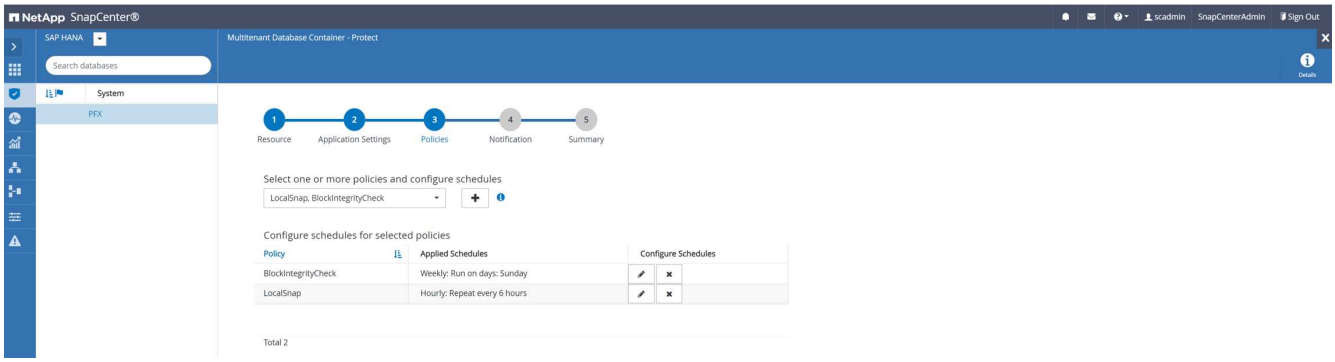
   この例では、週に1回に設定されています。



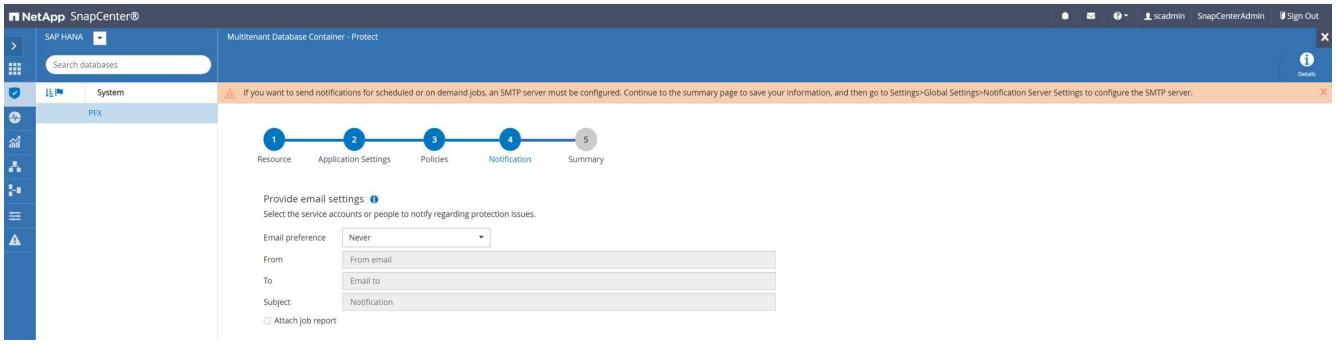

8. ローカルSnapshotポリシーのスケジュールを定義します。

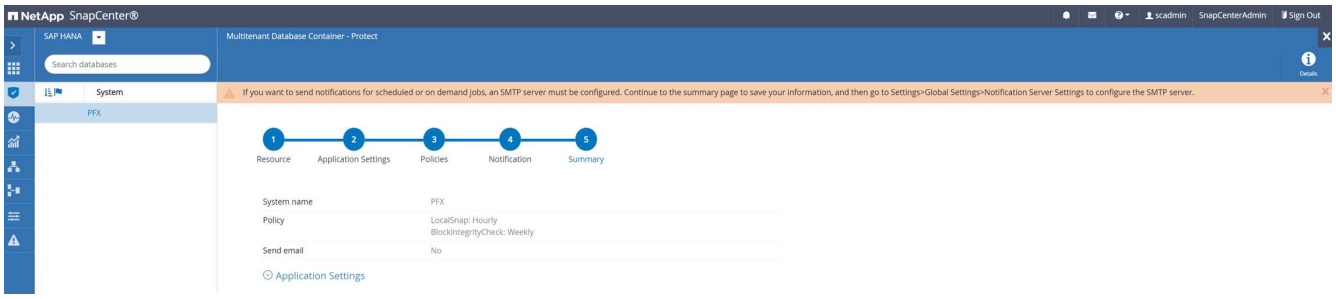
   この例では、6時間ごとに設定されています。



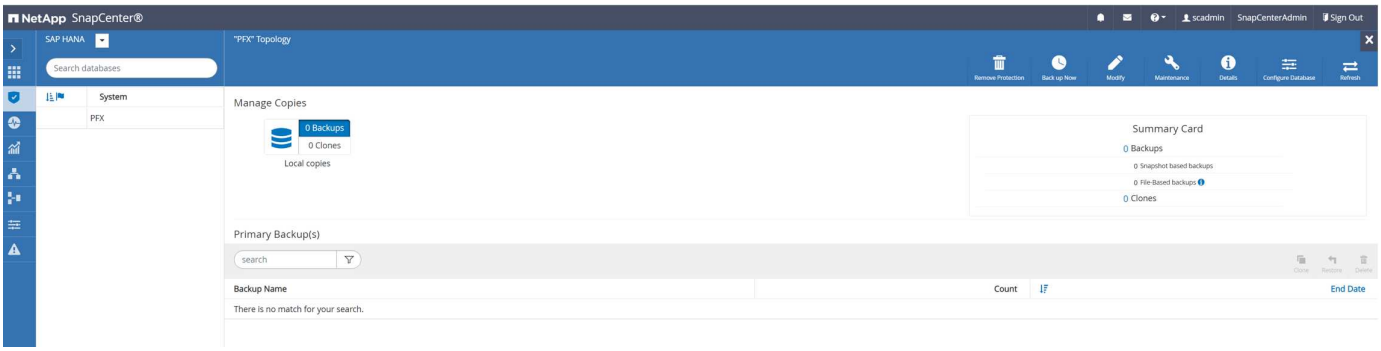




9. E メール通知に関する情報を指定します。




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。

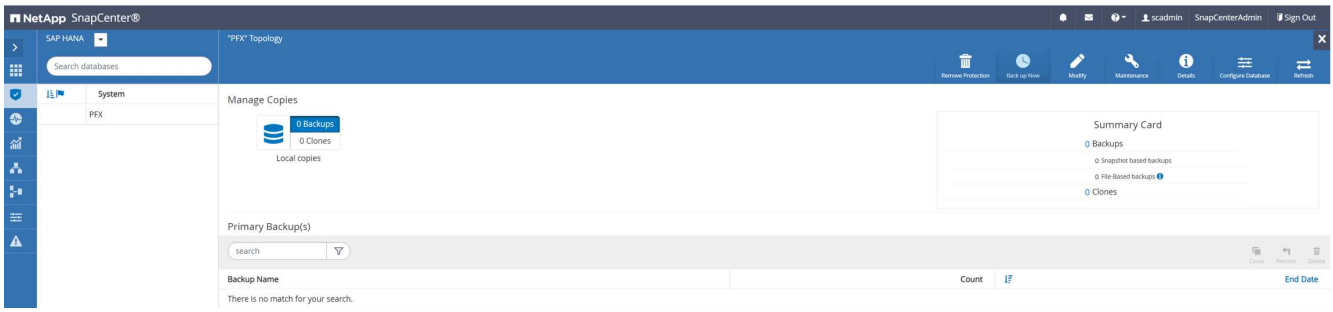
### オンデマンドの**Snapshot**バックアップを作成します

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。

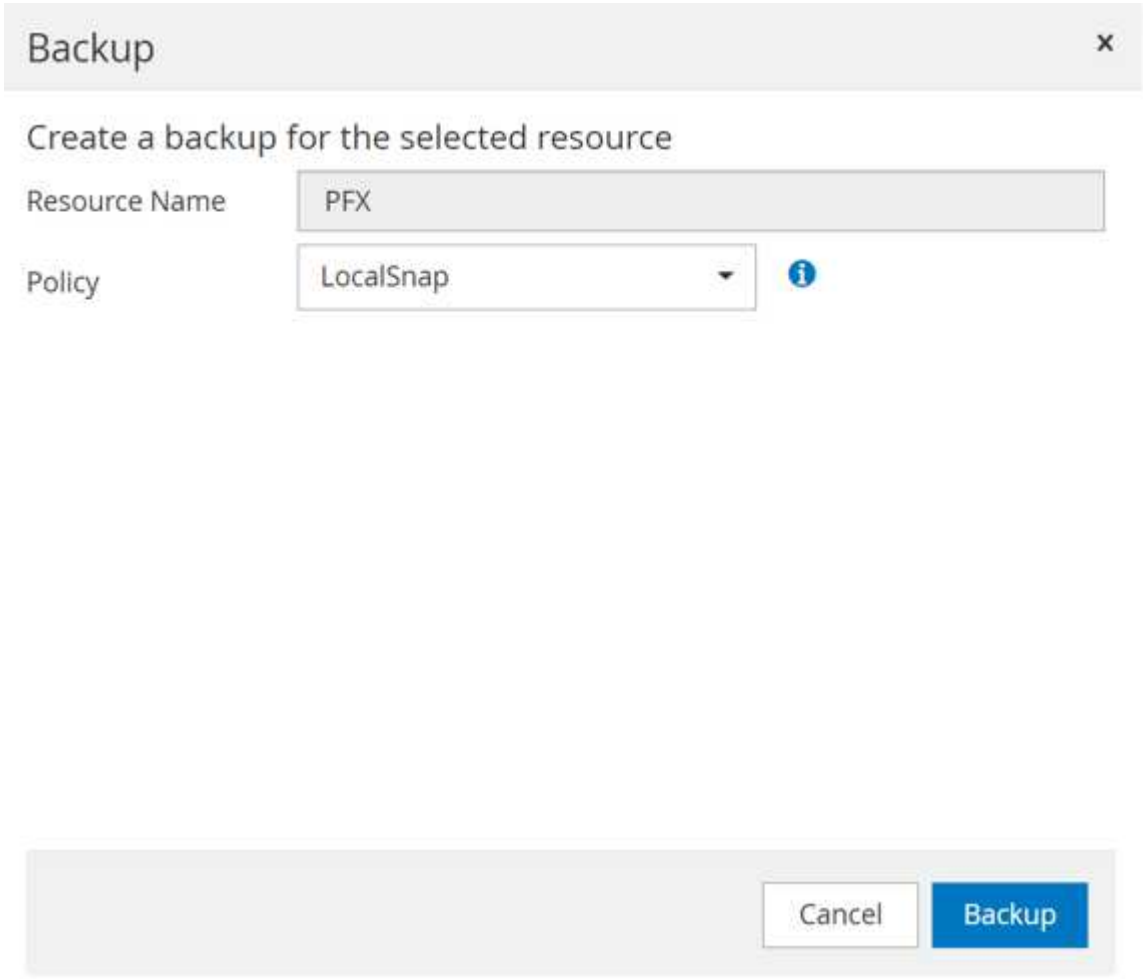
1. リソースビューで、リソースを選択し、行をダブルクリックしてトポロジビューに切り替えます。

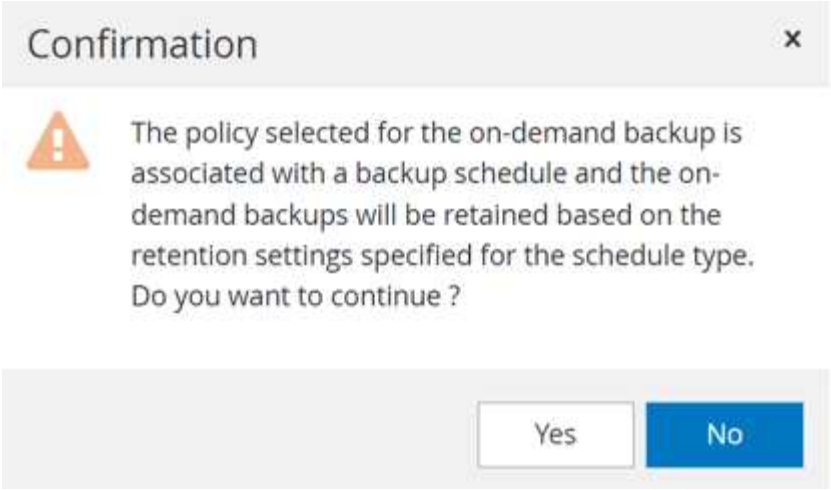
   リソーストポロジビューには、SnapCenter を使用して作成された、使用可能なすべてのバックアップの概要が表示されます。上部には、プライマリストレージのバックアップ（ローカルコピー）と、オフサイトのバックアップストレージ（バックアップコピー）のバックアップトポロジが表示されます。

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。



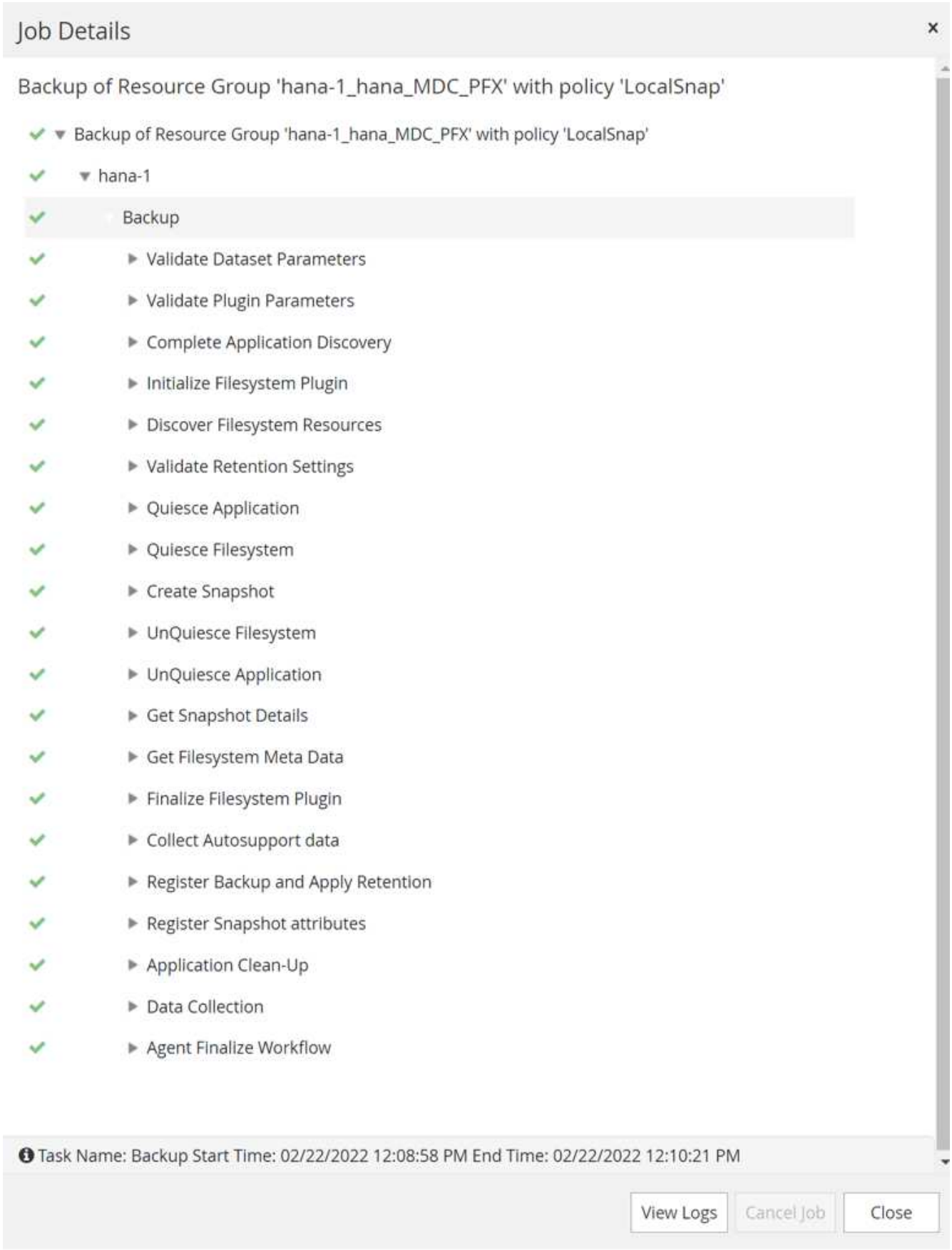

3. ドロップダウン・リストから'バックアップ・ポリシーLocalSnapを選択し'[Backup]をクリックして'オンデマンド・バックアップを開始します





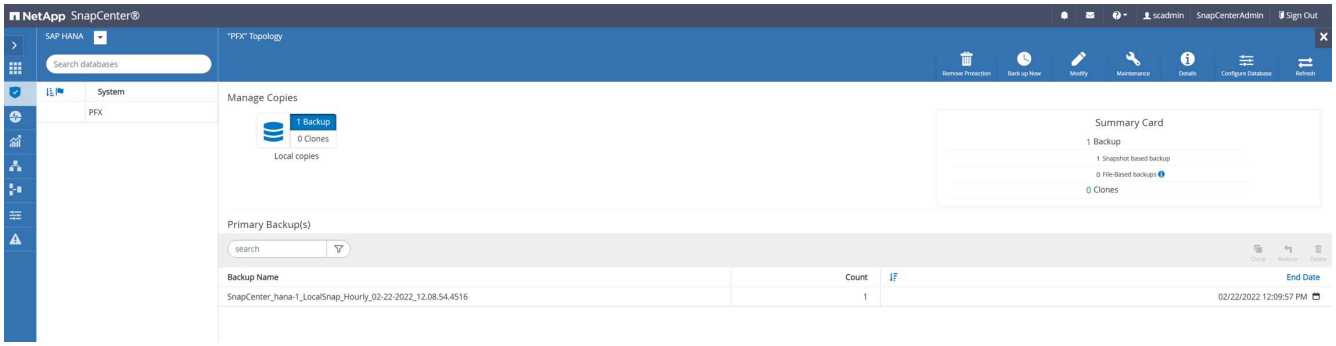

前の5つのジョブのログは、Topologyビューの下部にあるActivity領域に表示されます。

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

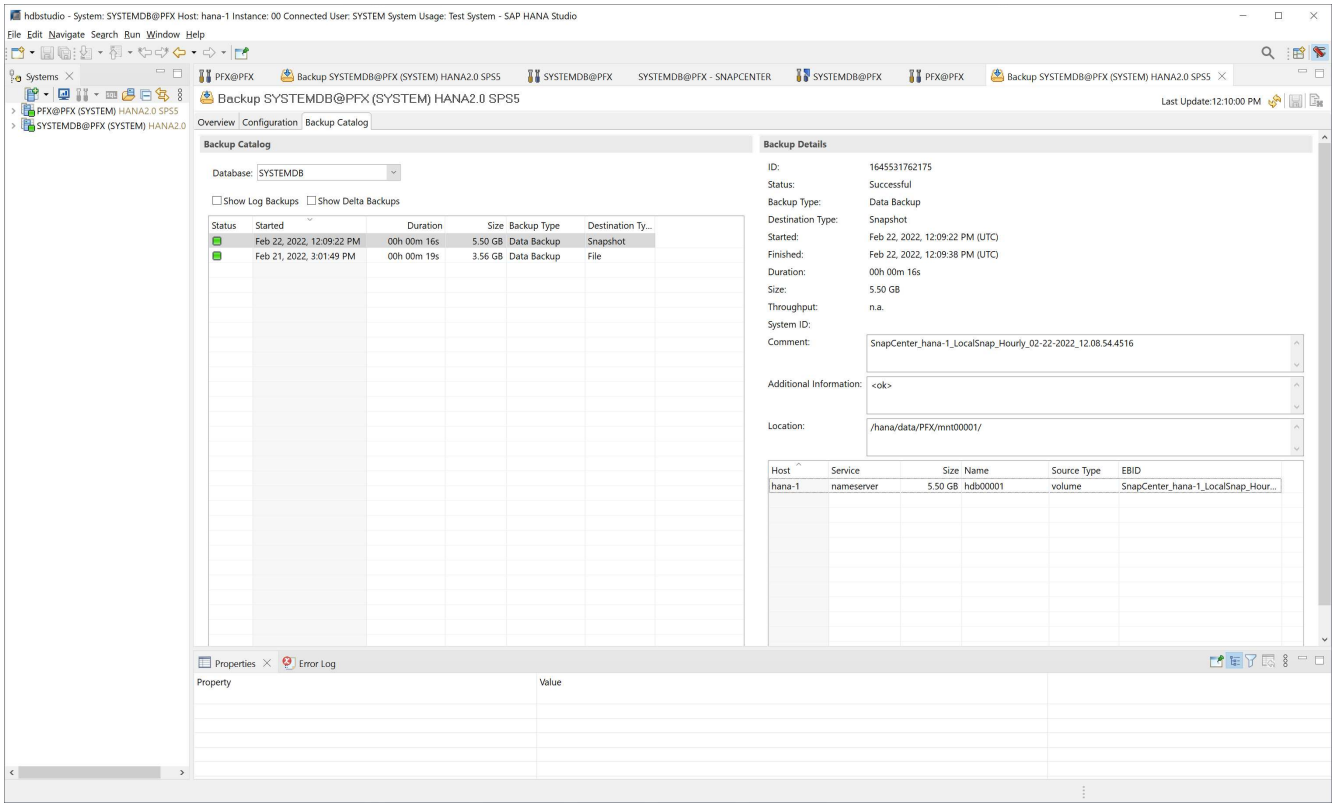


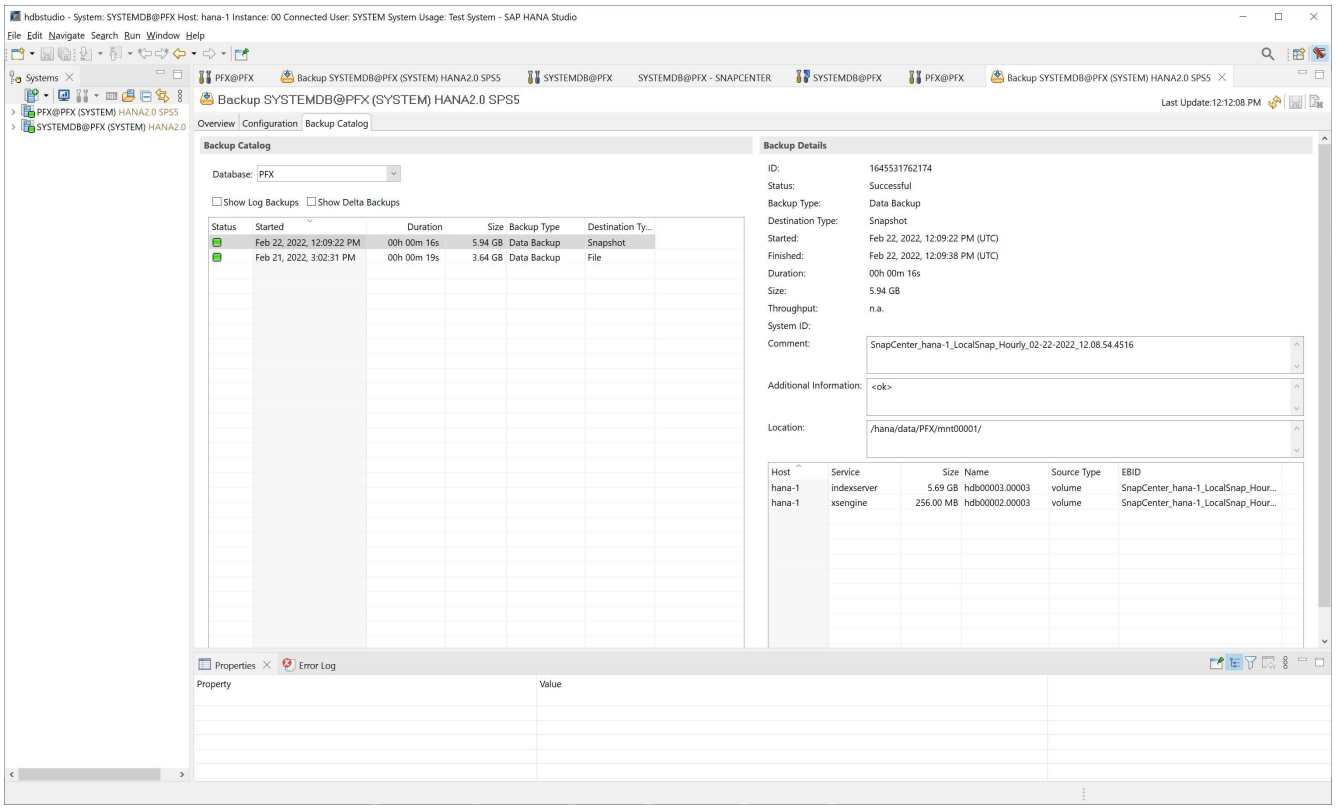

バックアップが完了すると、トポロジビューに新しいエントリが表示されます。バックアップ名は、セクションで定義したSnapshot名と同じ命名規則に従います。"「HANAリソースを構成して保護する」"

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。



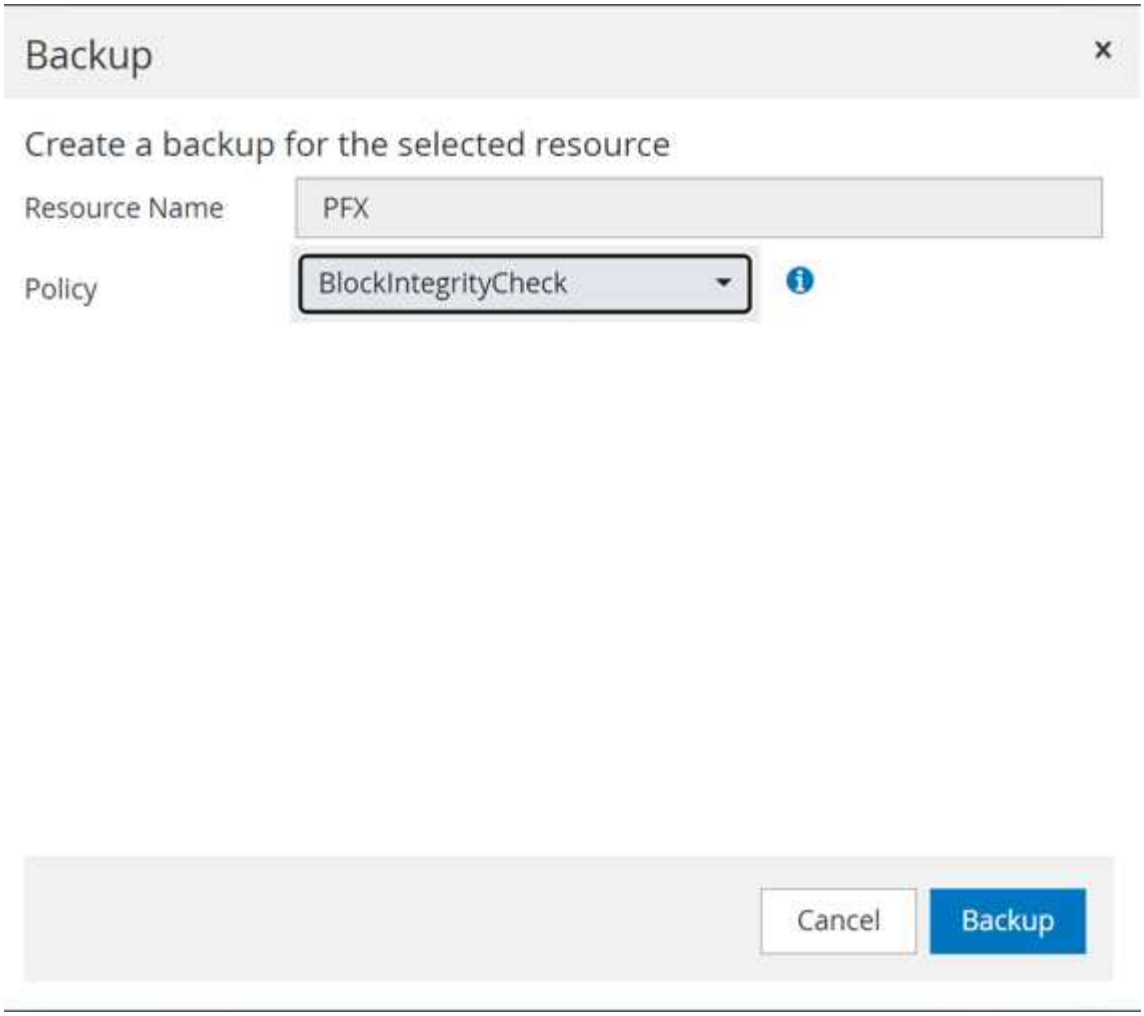


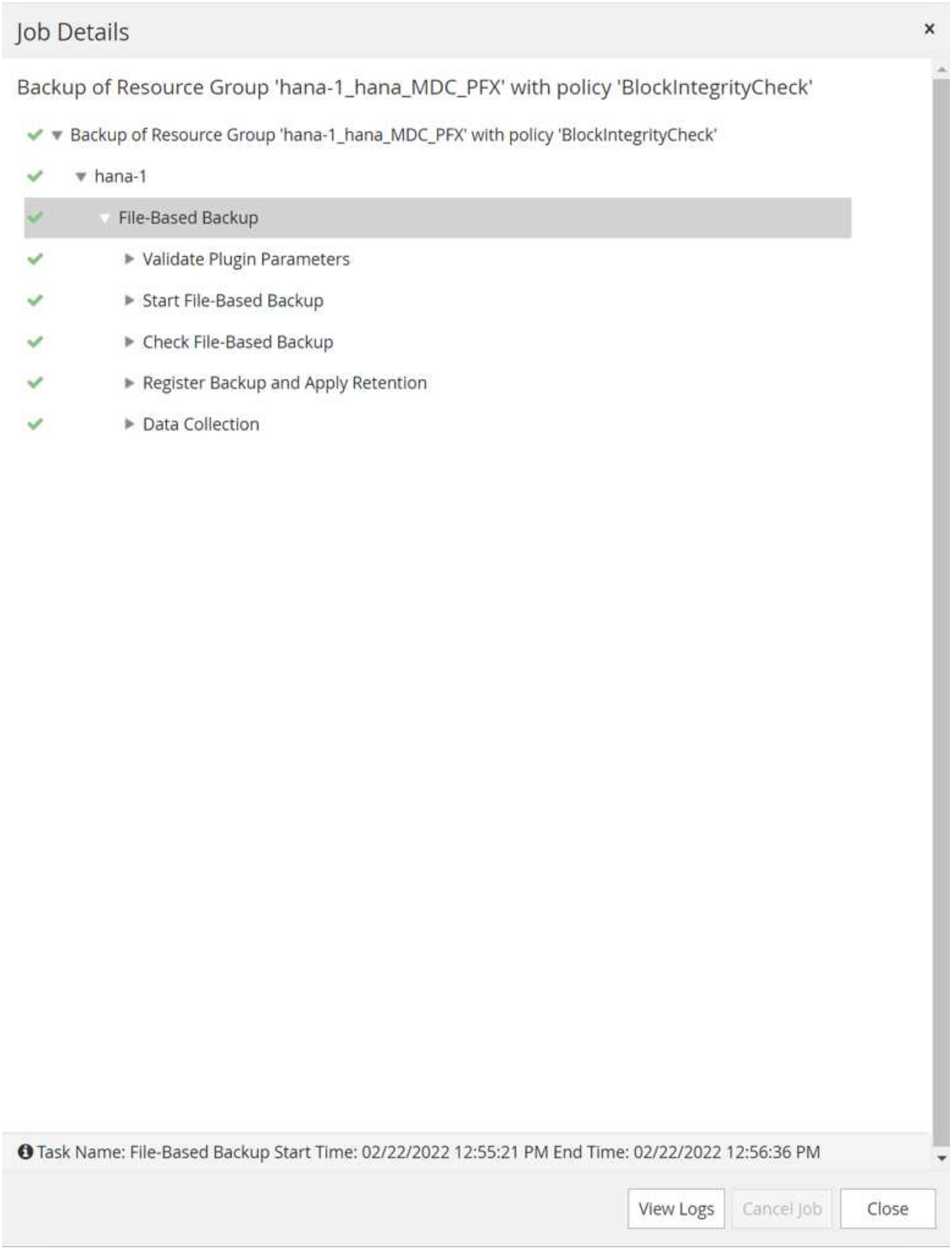

ONTAP ファイルシステムのFSXでは、SVMのコンソールに接続してSnapshotバックアップを表示できます。

```
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

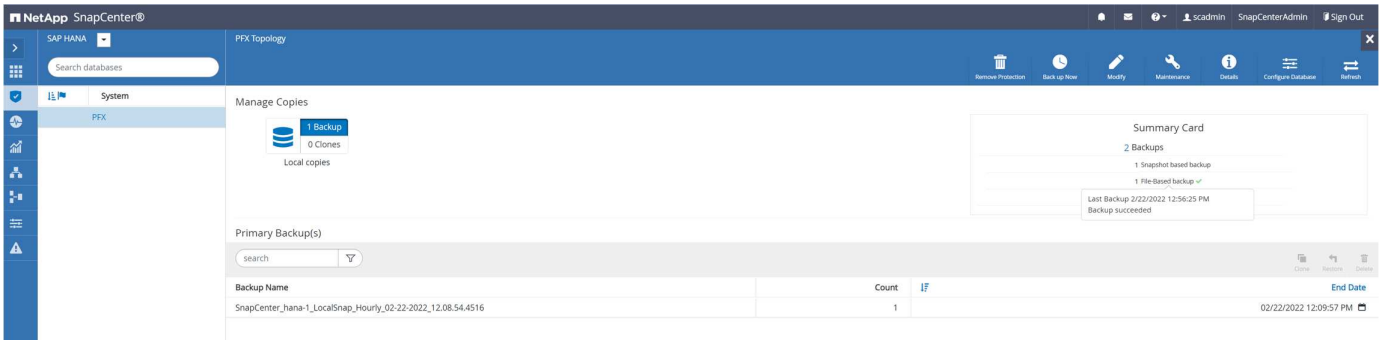
ポリシーBlockIntegrityCheckを選択すると、Snapshotバックアップジョブと同様にオンデマンドでブロック整合性チェック処理が実行されます。このポリシーを使用してバックアップをスケジュールすると、SnapCenter によってシステムデータベースとテナントデータベース用の標準の SAP HANA ファイルバックアップが作成されます。


Backup
Create a backup for the selected resource
Resource Name
PFX
Policy
BlockIntegrityCheck
Cancel
Backup

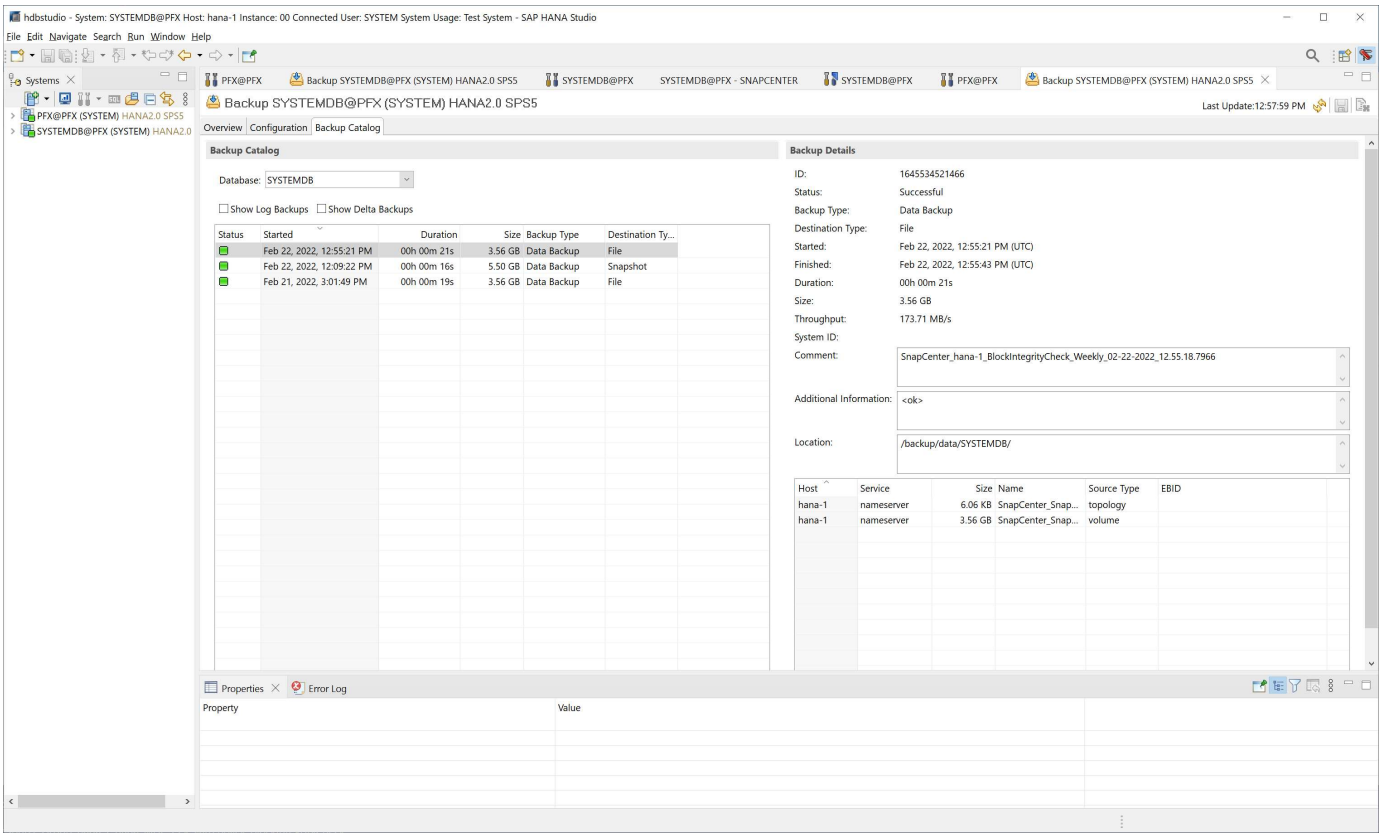


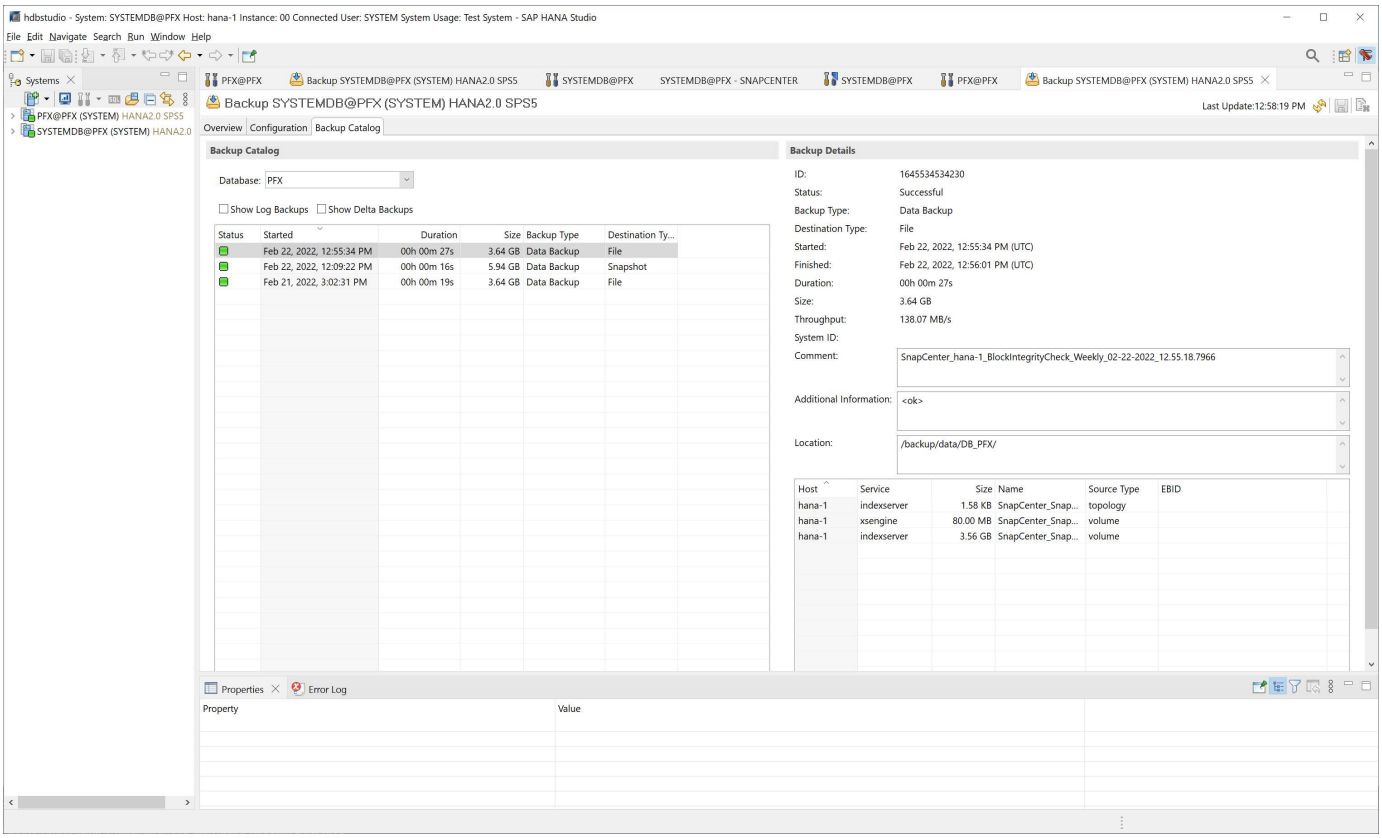

SnapCenter では、 Snapshot コピーベースのバックアップと同じ方法でブロック整合性チェックが表示され

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。






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

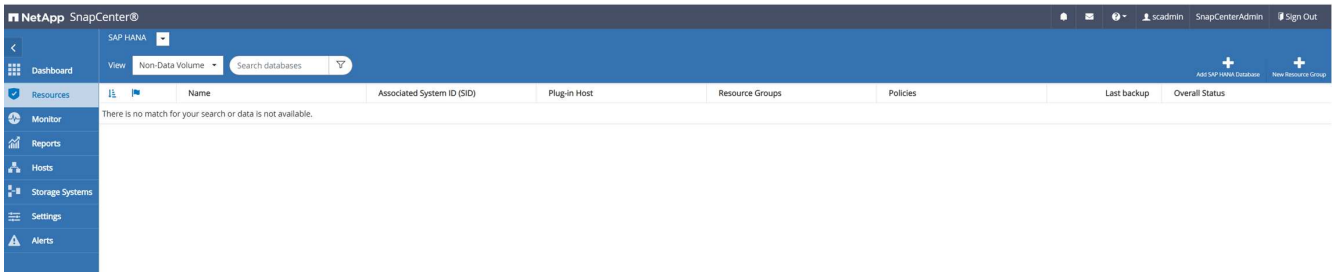
プを補うために、データボリューム以外のボリュームに対する追加のバックアップ戦略を開発することを推奨します。固有の要件に応じて、非データボリュームのバックアップはスケジュールの頻度と保持の設定が異なる場合があります。また、非データファイルを変更する頻度も考慮する必要があります。たとえば、 HANA ボリューム「 /hana/shared 」には、実行可能ファイルと SAP HANA トレースファイルが格納されています。実行ファイルが変更されるのは SAP HANA データベースがアップグレードされた場合だけですが、 SAP HANA の問題を分析するためには、 SAP HANA のトレースファイ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

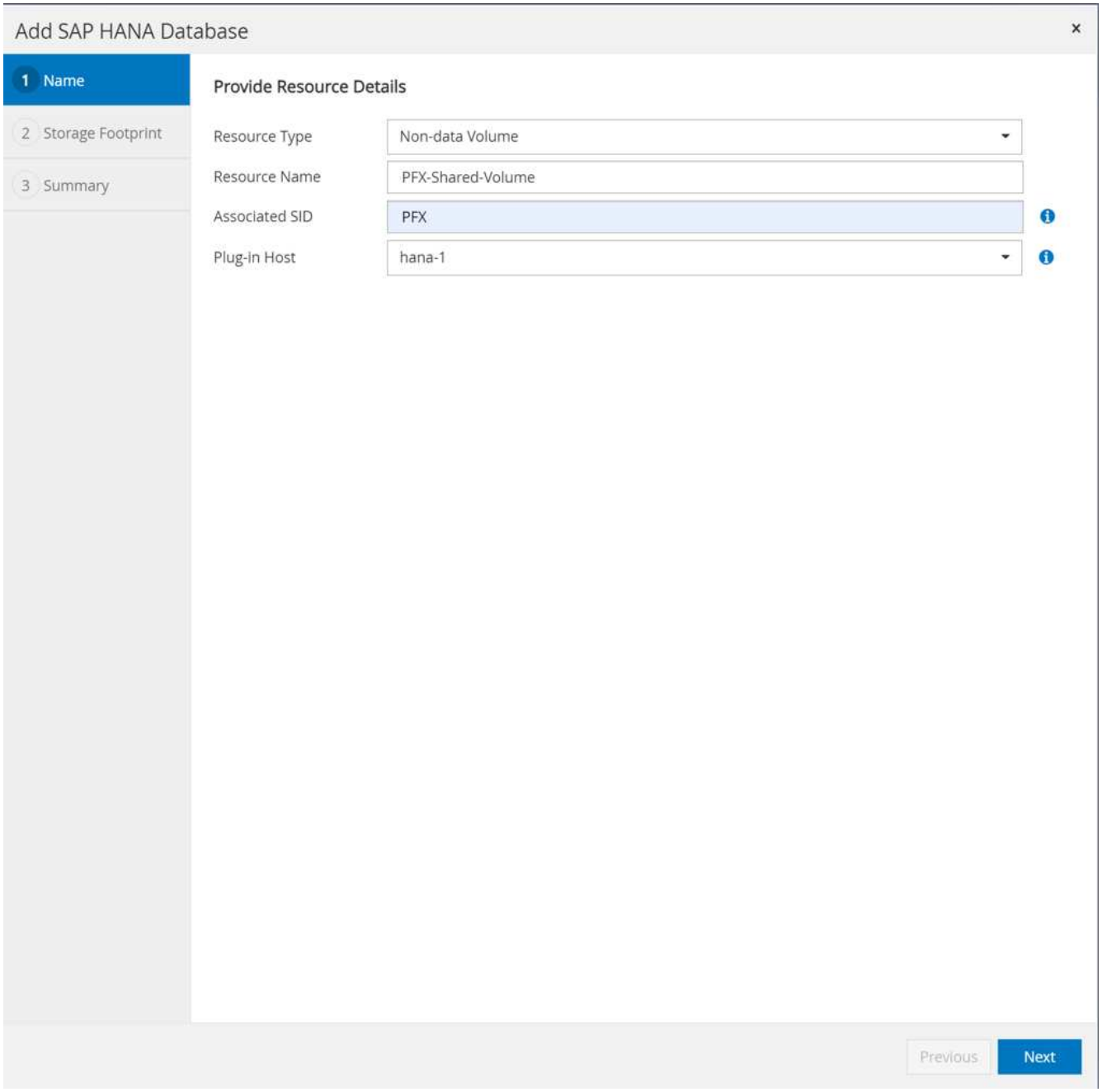
### データボリューム以外のリソースを設定

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。

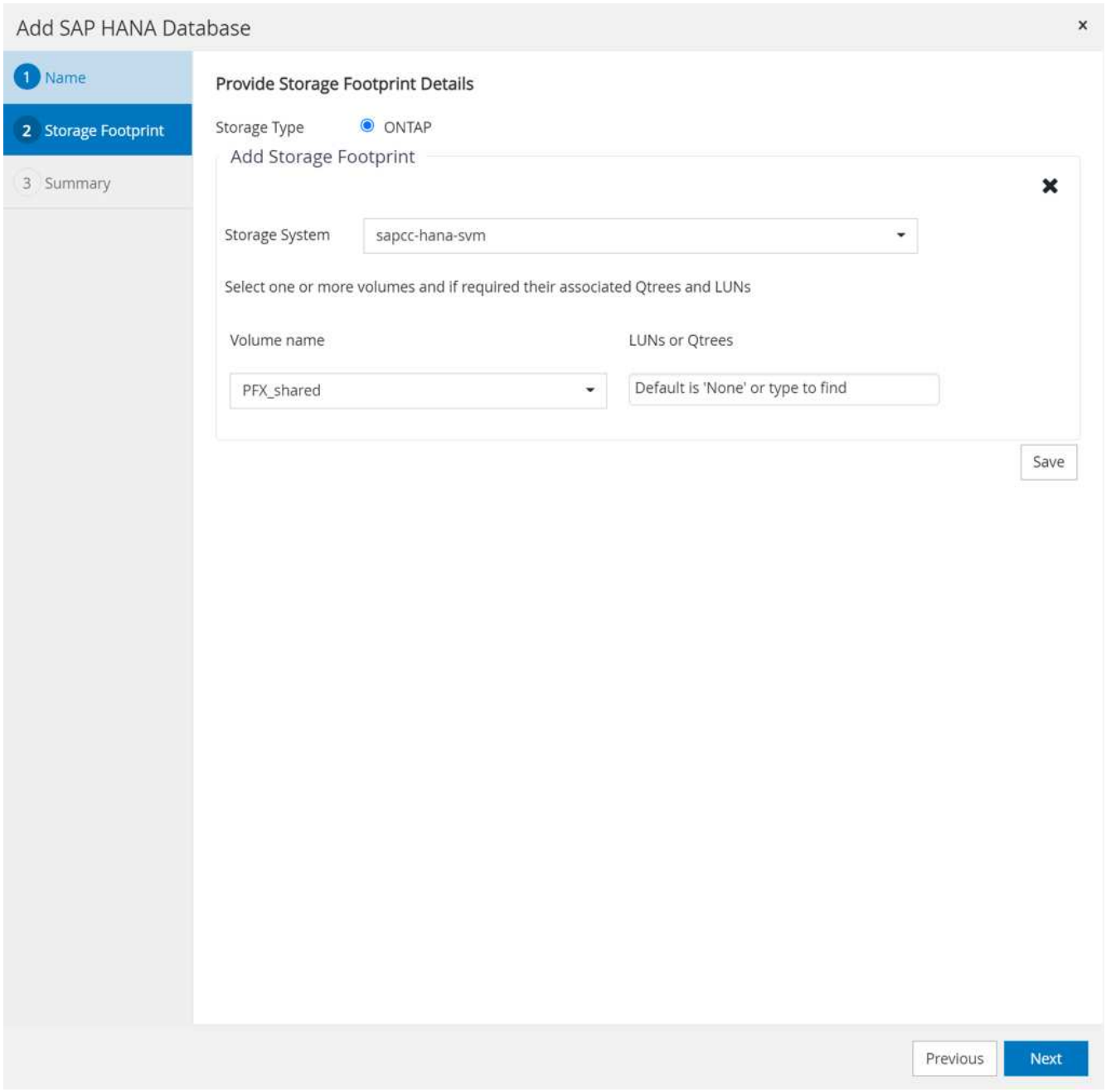
1. [リソース]タブで、[データボリュームではない]を選択し、[ SAP HANAデータベースの追加]をクリックします。



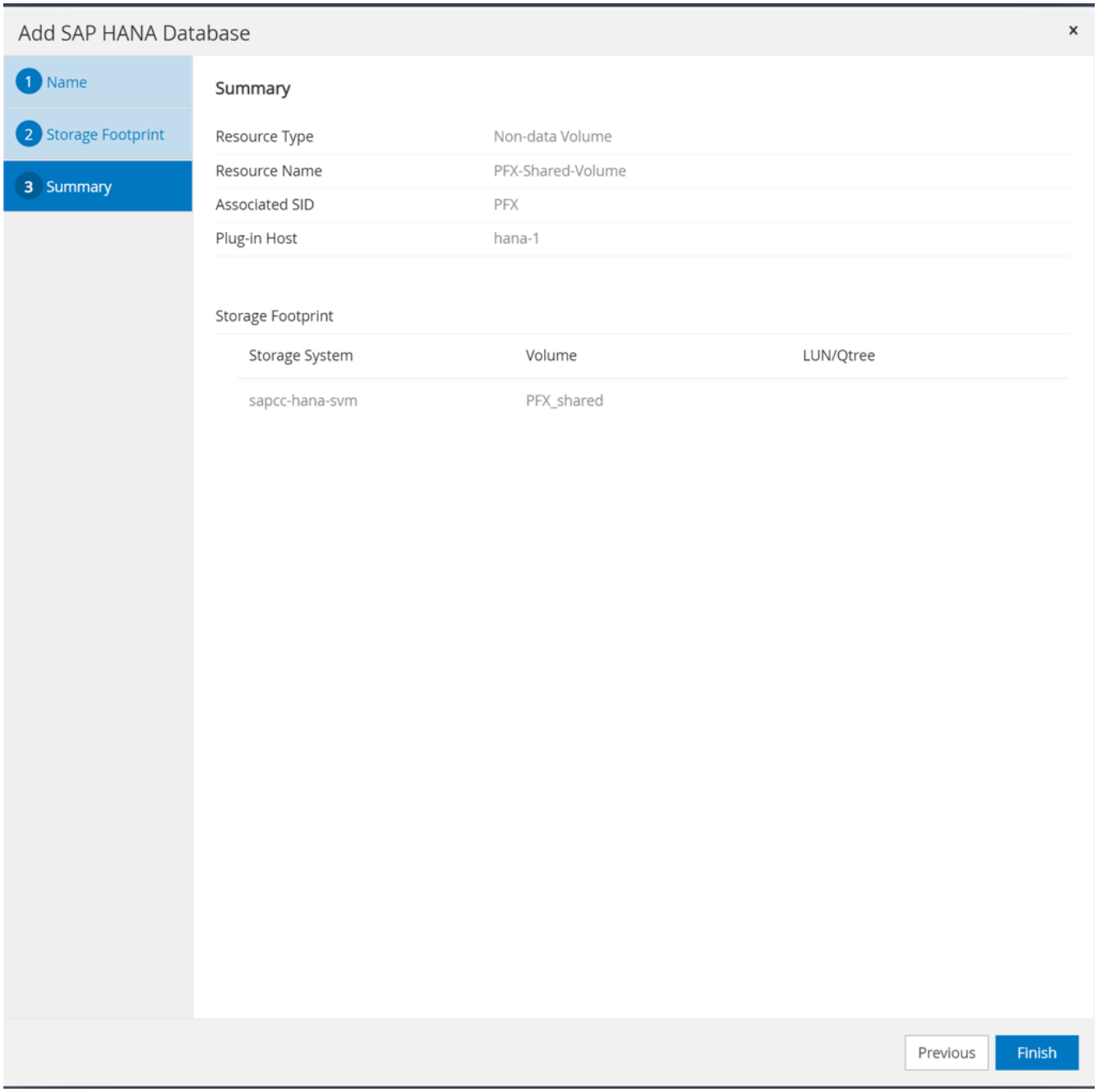

2. SAP HANAデータベースの追加ダイアログのステップ1で、リソースタイプリストから非データボリュームを選択します。リソースの名前、およびリソースに使用する関連SIDとSAP HANAプラグインホストを指定し、[次へ]をクリックします。



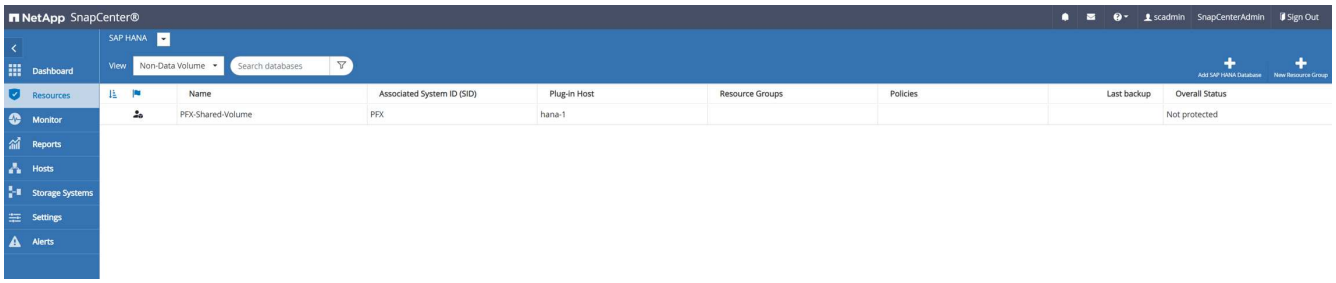

3. SVM とストレージボリュームをストレージ容量として追加し、次へをクリックします。




4. 設定を保存するには、概要手順で[完了]をクリックします。




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。

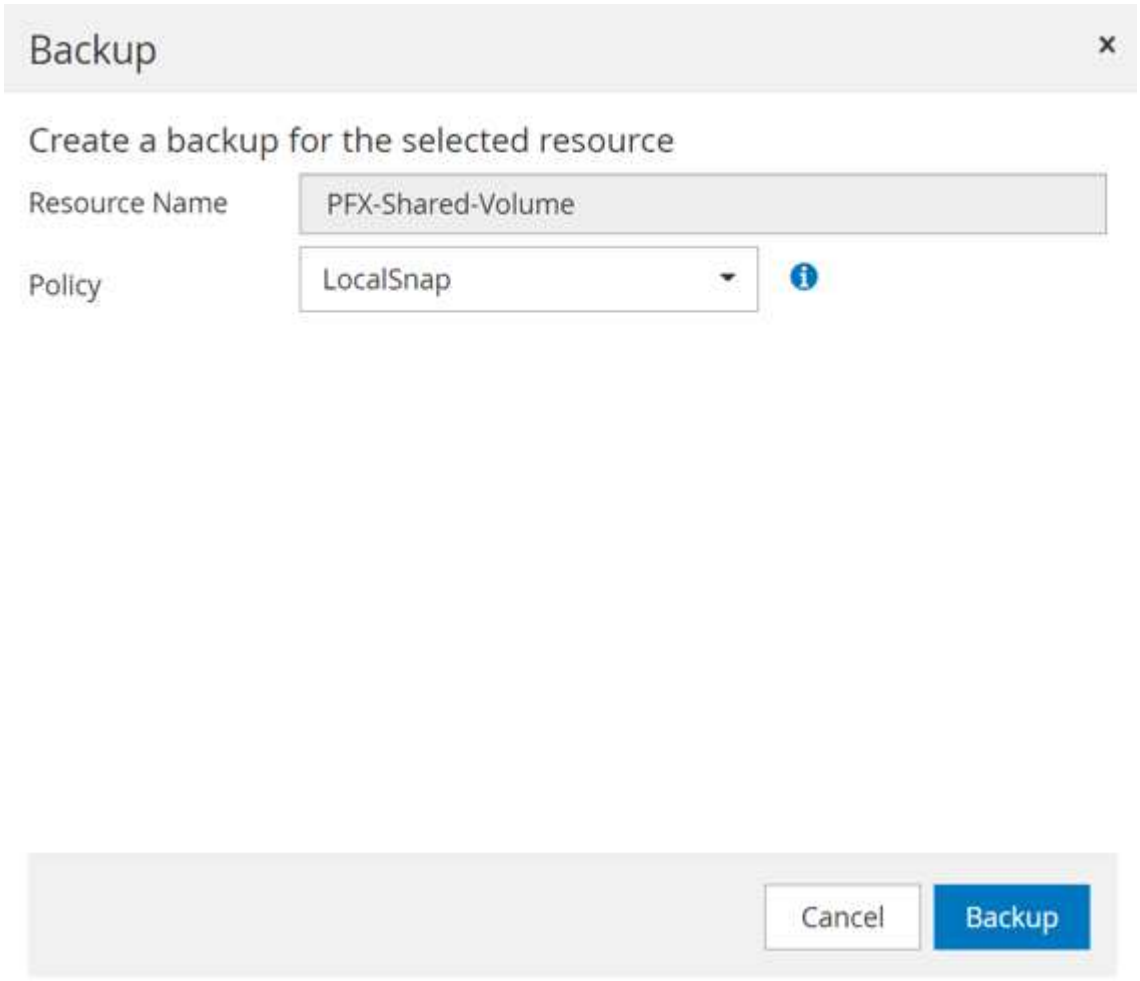



リソースの保護は、HANAデータベースのリソースで前述した方法と同じ方法で行われます。

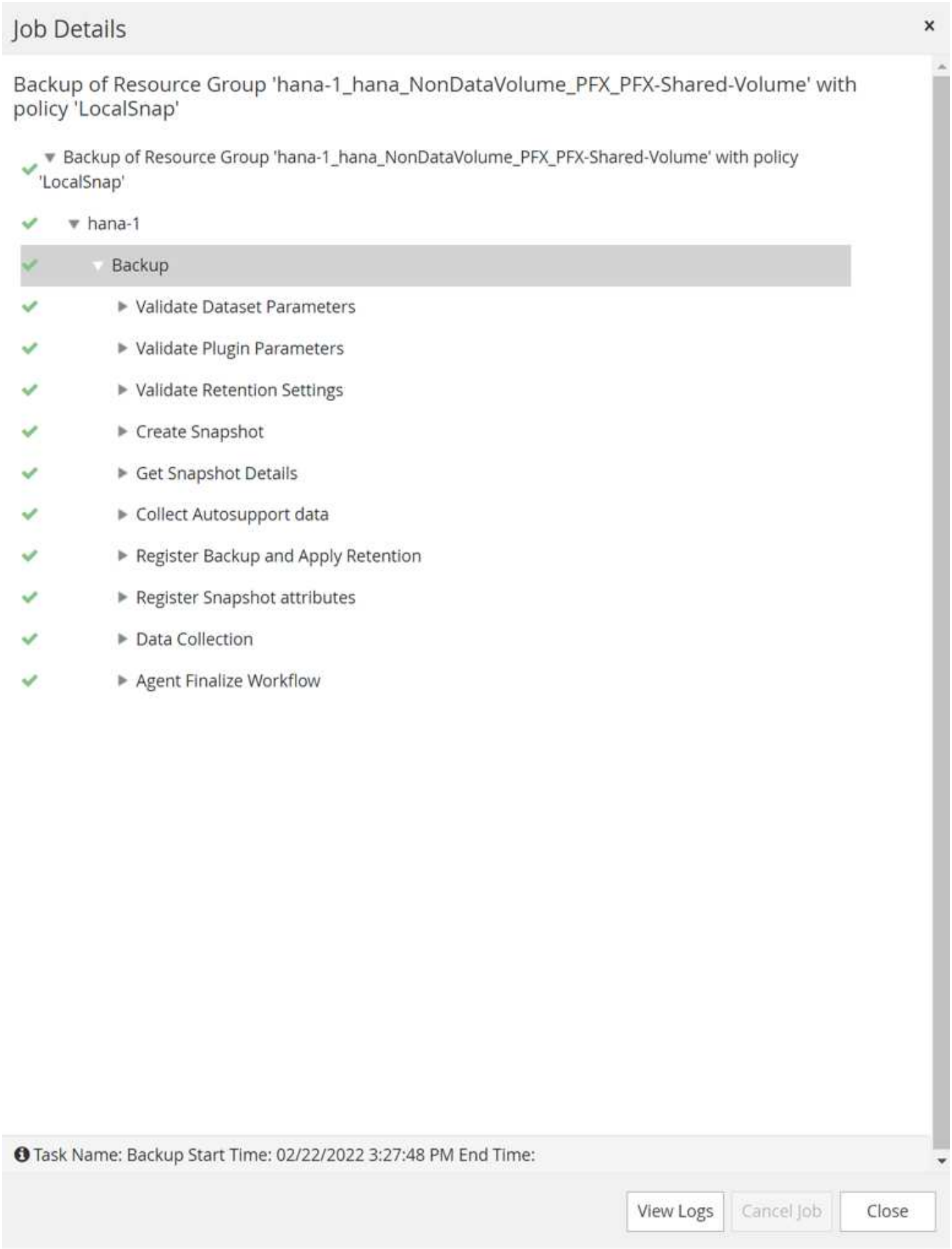
5. [今すぐバックアップ]をクリックして、バックアップを実行できるようになりました。



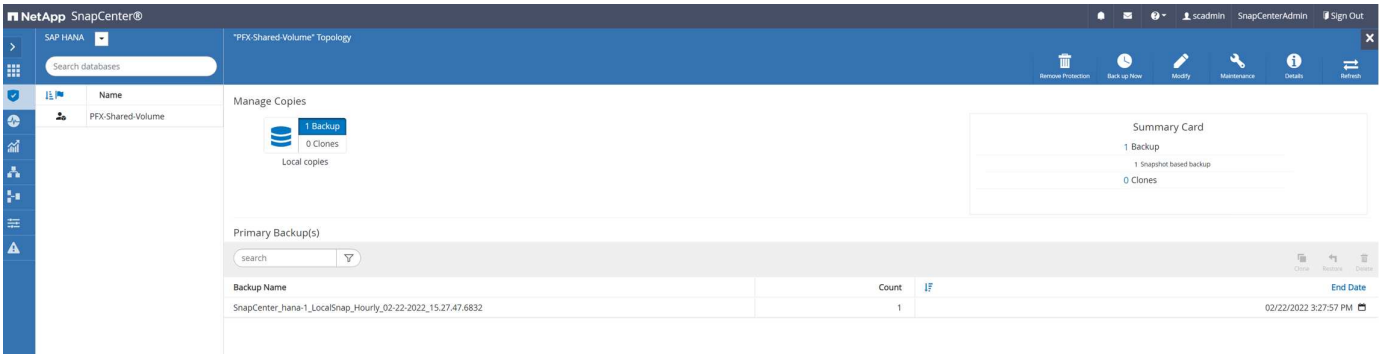

6. ポリシーを選択し、バックアップ処理を開始します。




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。




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。




# 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。

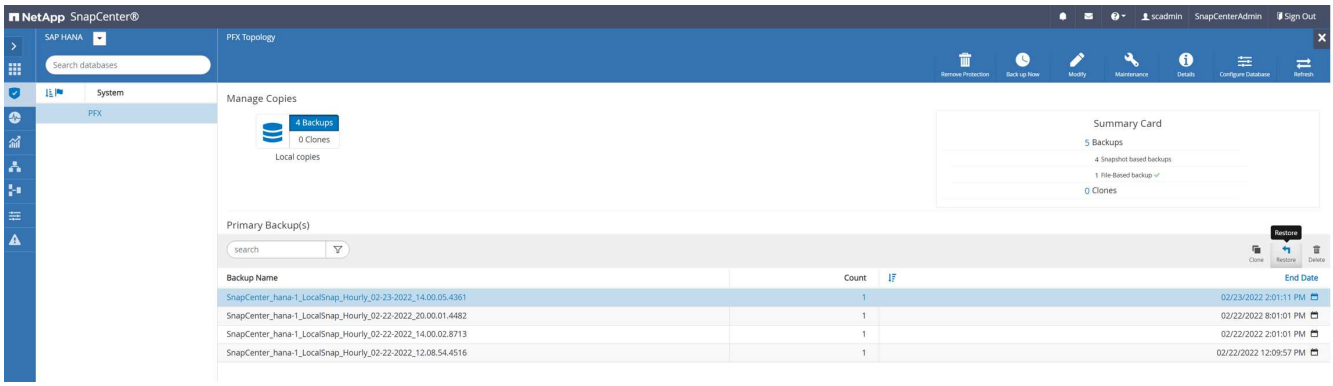
次に、 SnapCenter は次の処理を実行します。

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。

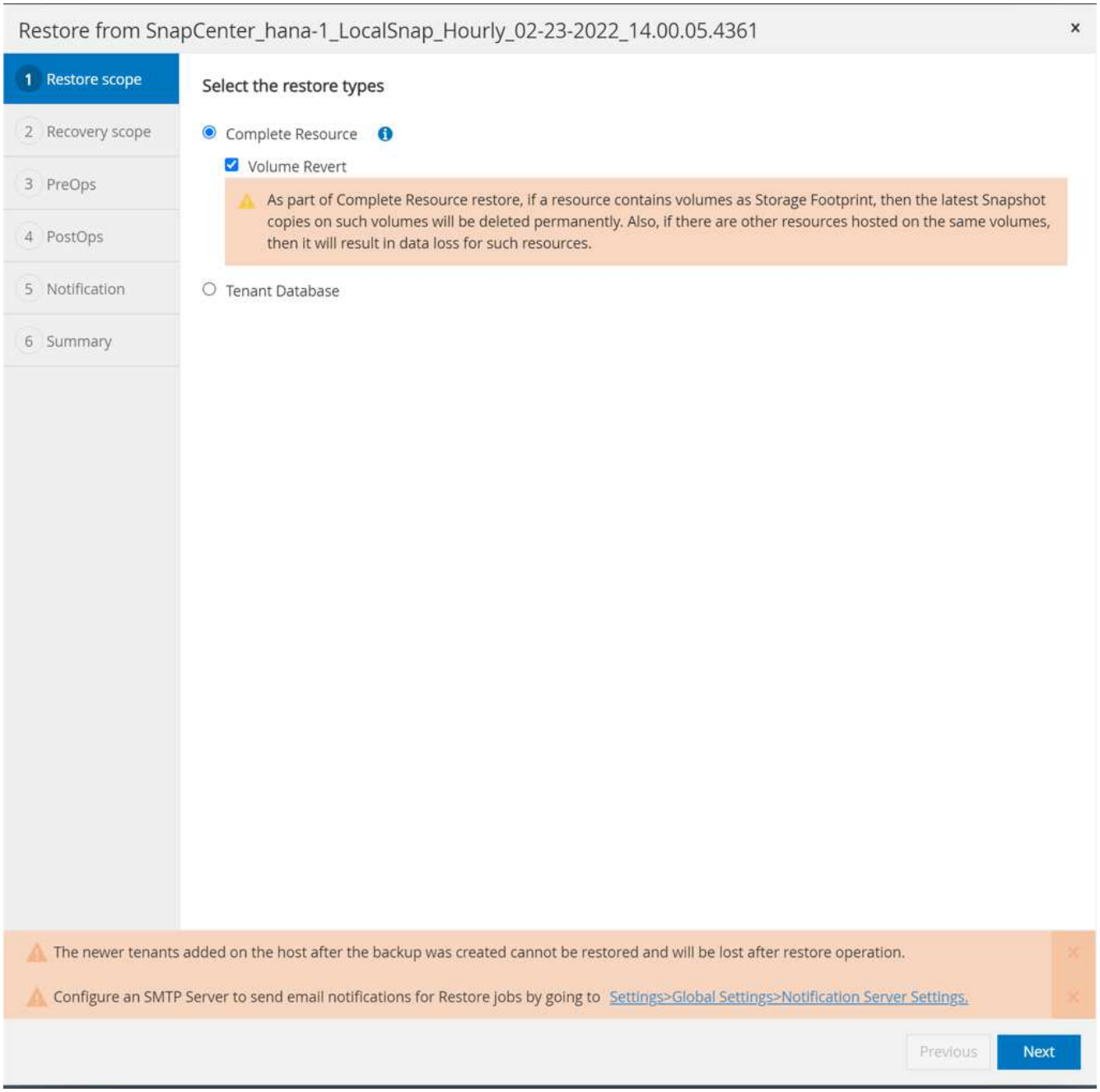
手動でリストアを実行するには、次の手順を実行します。

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。



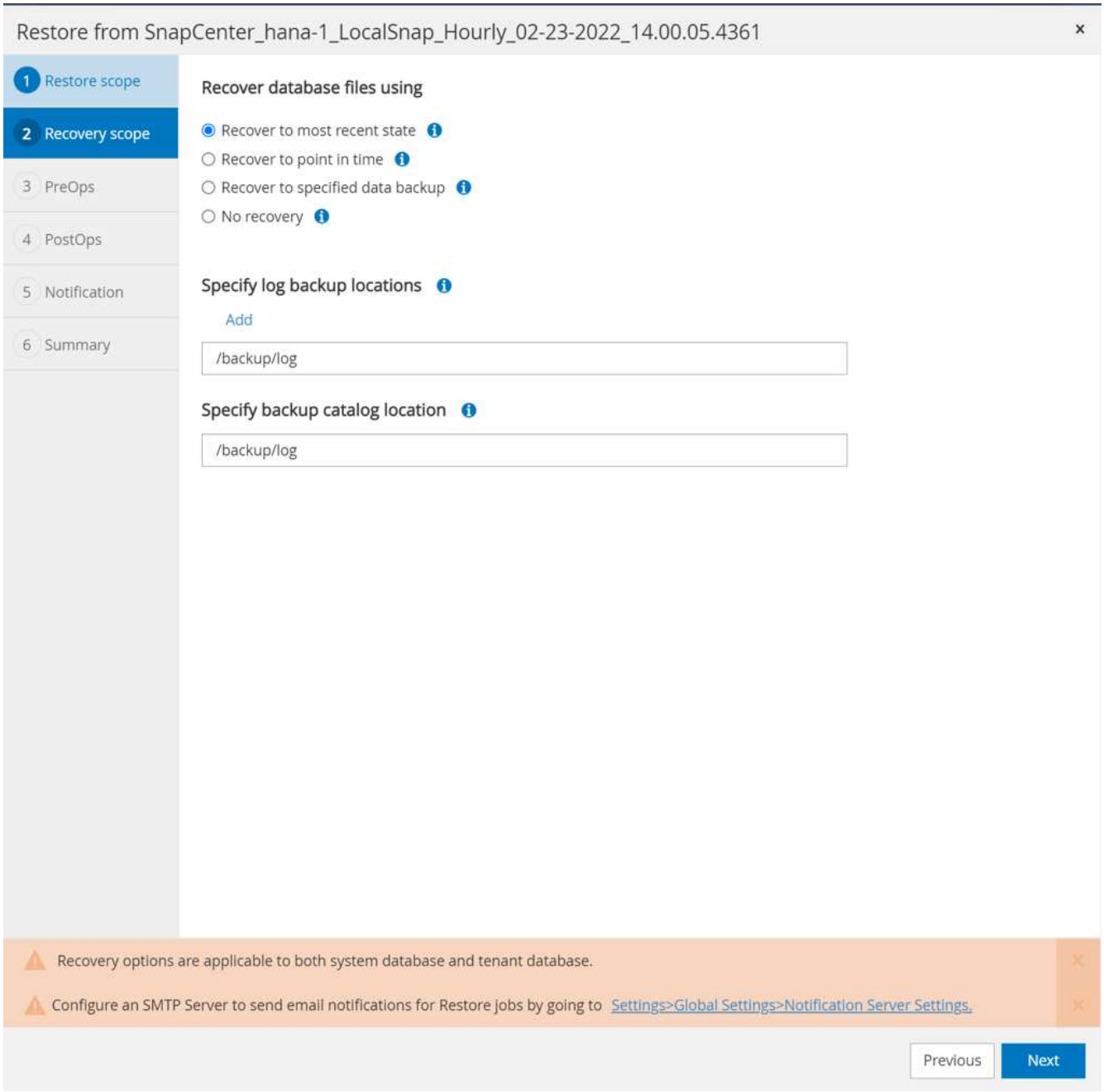

2. リストアの範囲とタイプを選択します。

   HANA MDCのシングルテナントシステムの標準的なシナリオは、ボリュームをリバートしてリソース全体を使用する場合です。複数のテナントを使用するHANA MDCシステムでは、単一のテナントのみをリストアできます。単一テナントのリストアの詳細については、を参照してください"リストアとリカバリ（netapp.com）"。

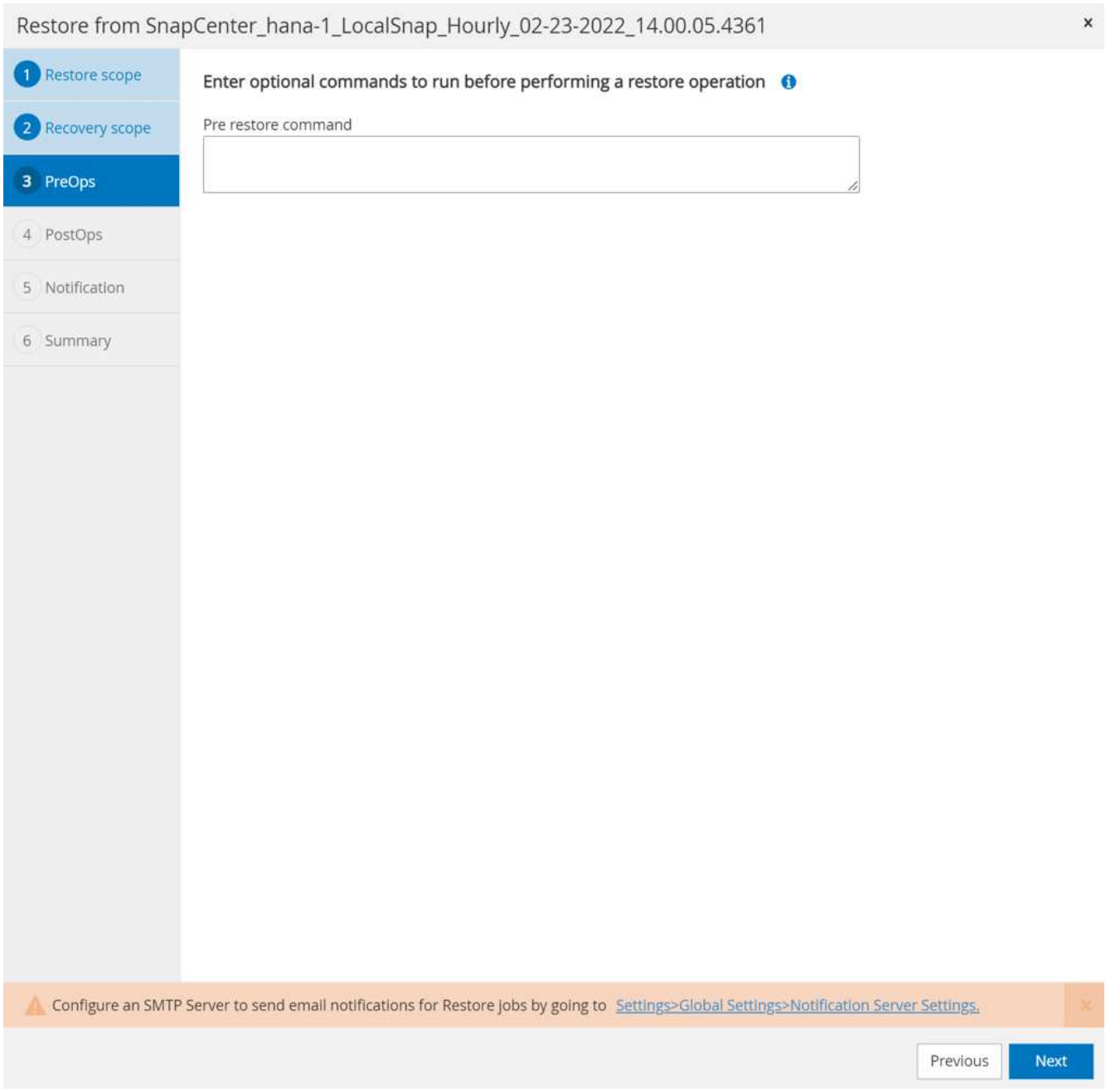



3. Recovery Scope を選択し、ログバックアップとカタログバックアップの場所を指定します。

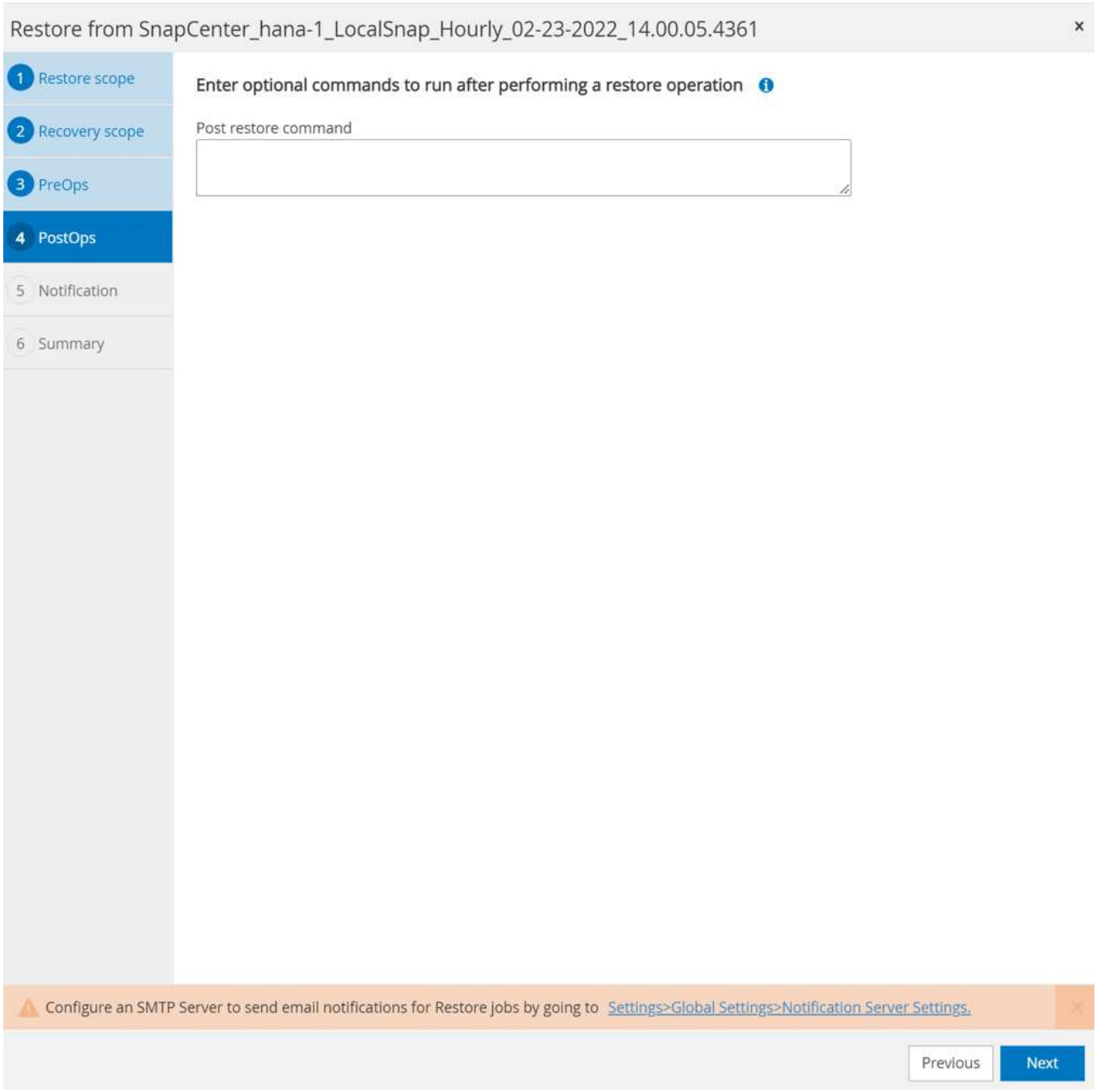
   SnapCenter では、 HANA の global.ini ファイルのデフォルトパスまたは変更されたパスを使用して、ログとカタログのバックアップの場所が事前に入力されます。



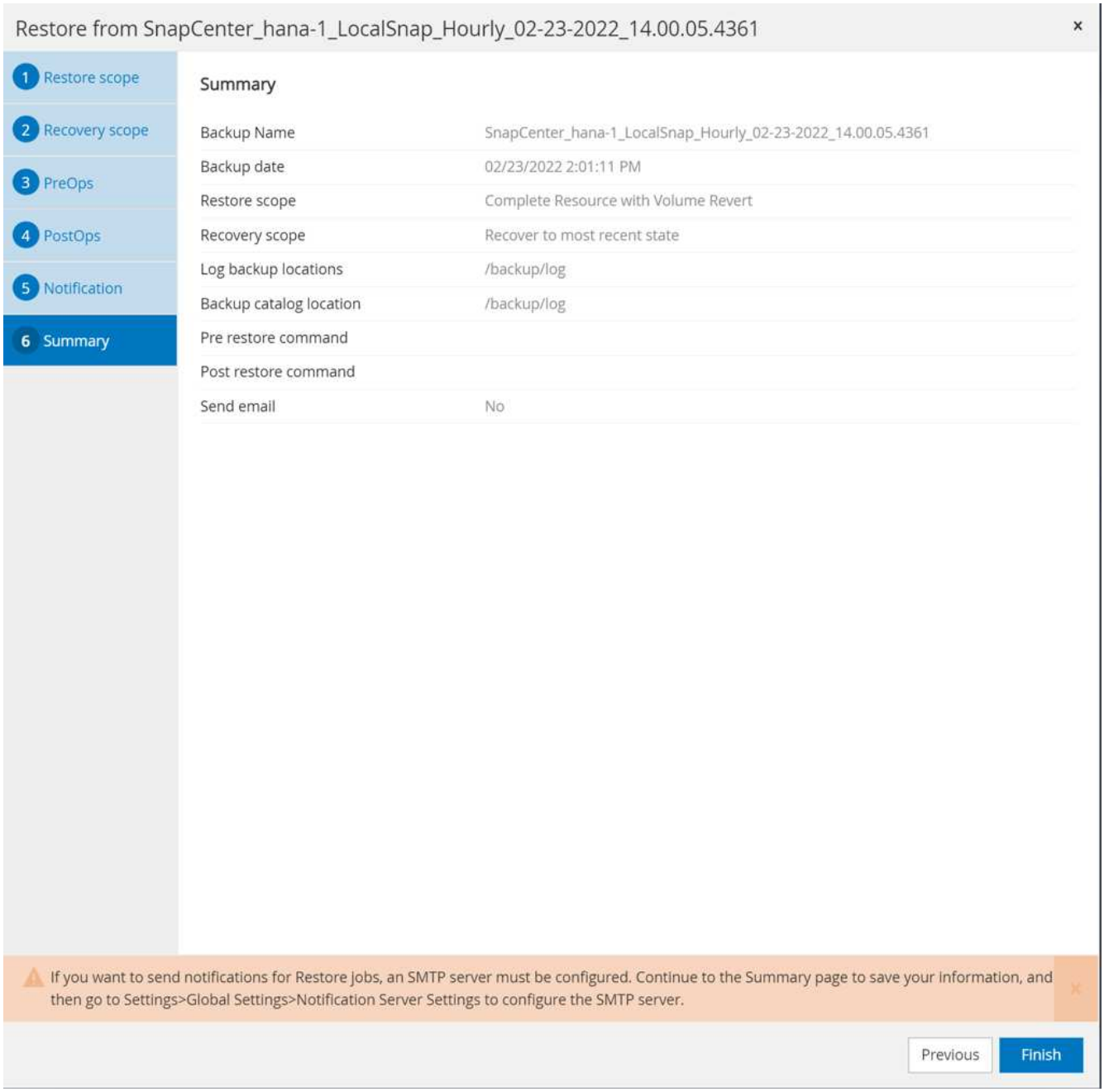

4. オプションのリストア前のコマンドを入力します。



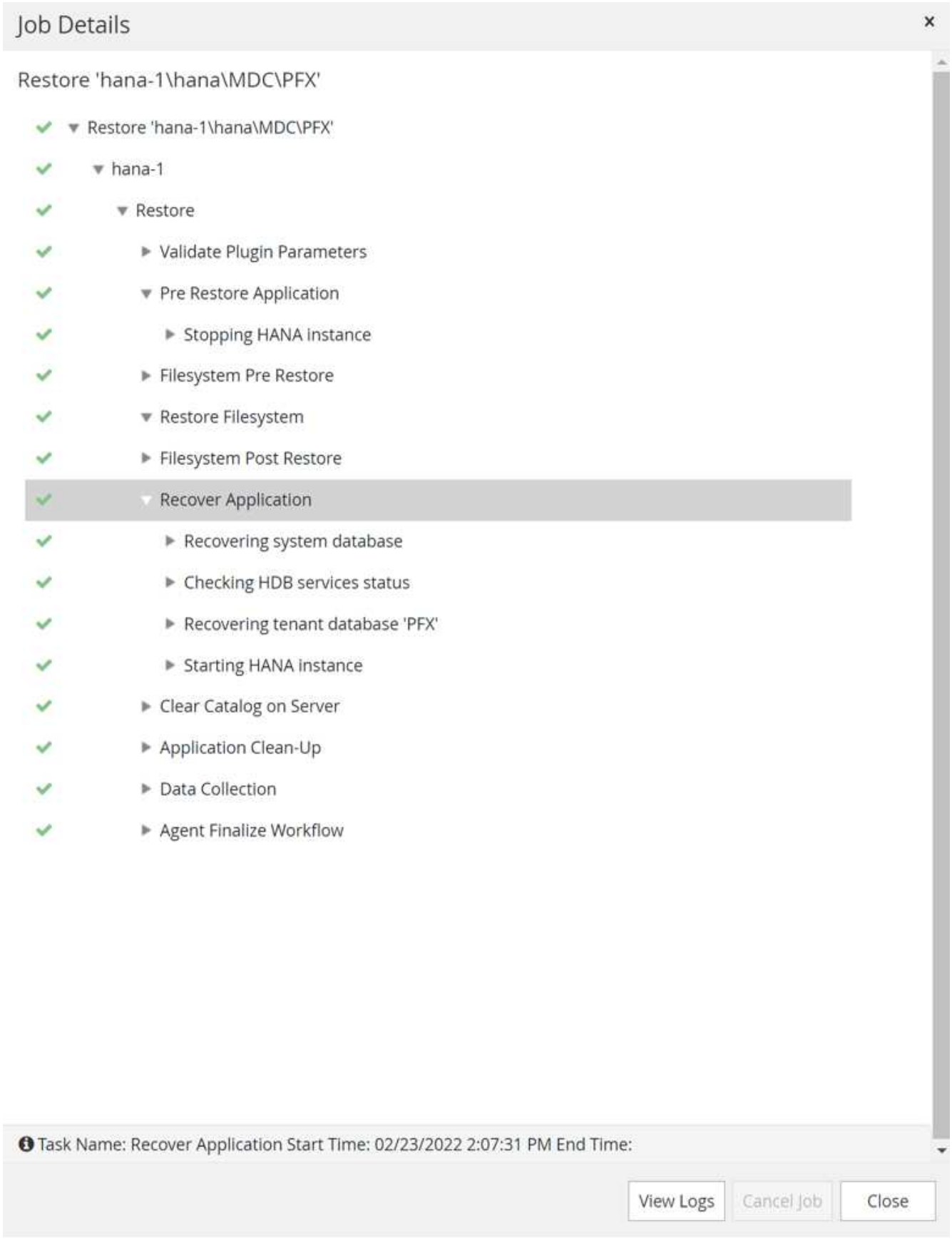

5. オプションのリストア後のコマンドを入力します。




6. 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




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。

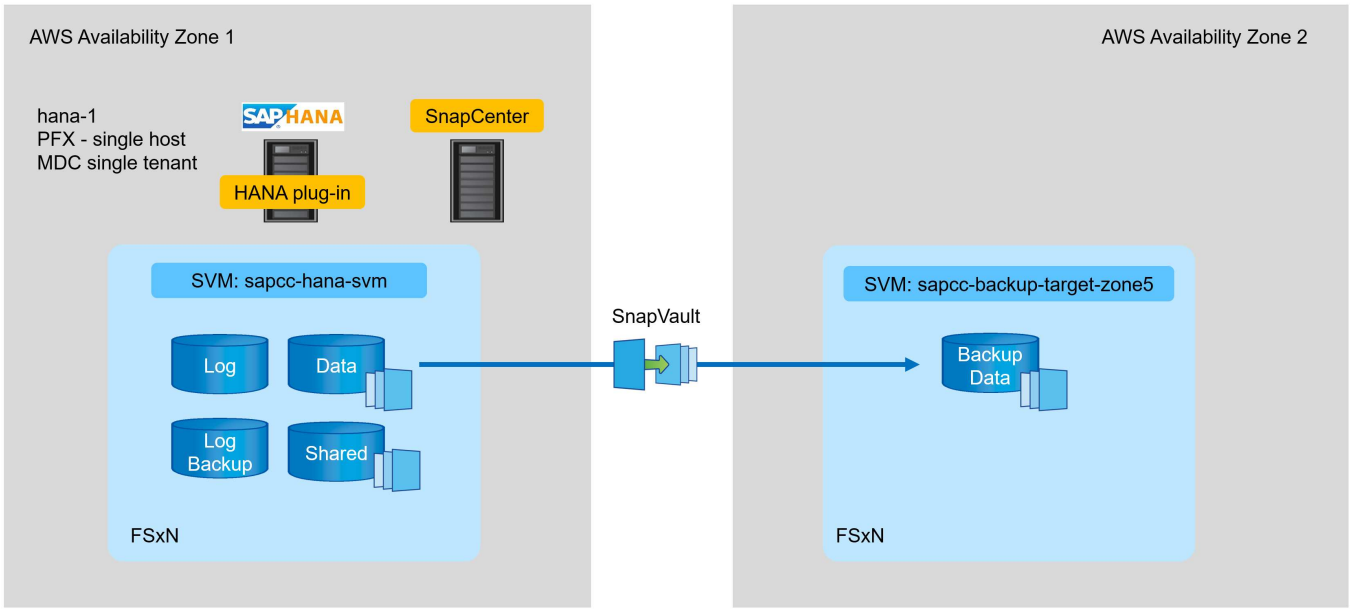

Job Details
Restore 'hana-1\hana\MDC\PFX'
Restore 'hana-1\hana\MDC\PFX'
hana-1
Restore
Validate Plugin Parameters
Pre Restore Application
Stopping HANA instance
Filesystem Pre Restore
Restore Filesystem
Filesystem Post Restore
Recover Application
Recovering system database
Checking HDB services status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

- 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
            Logical    Status     Network            Current       Current
Is
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
-addrs 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-addrs」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
-addrs  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
```

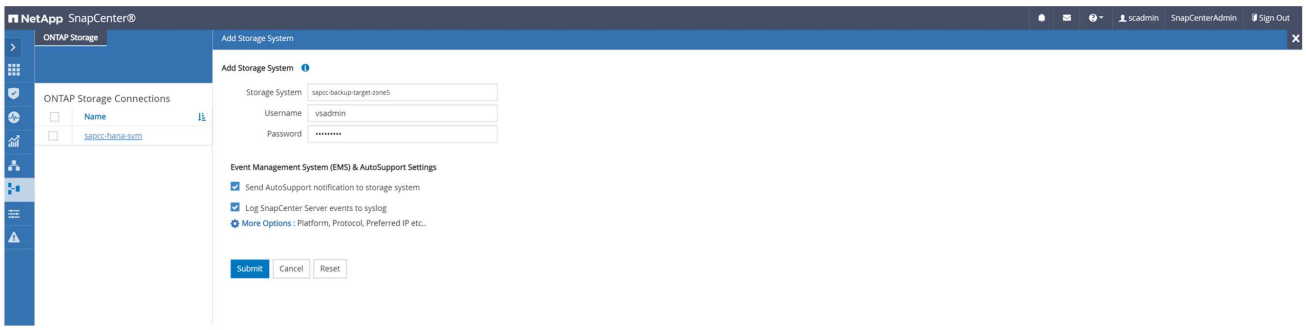
```
FsxId05f7f00af49dc7a3e::> snapmirror show

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    -
```

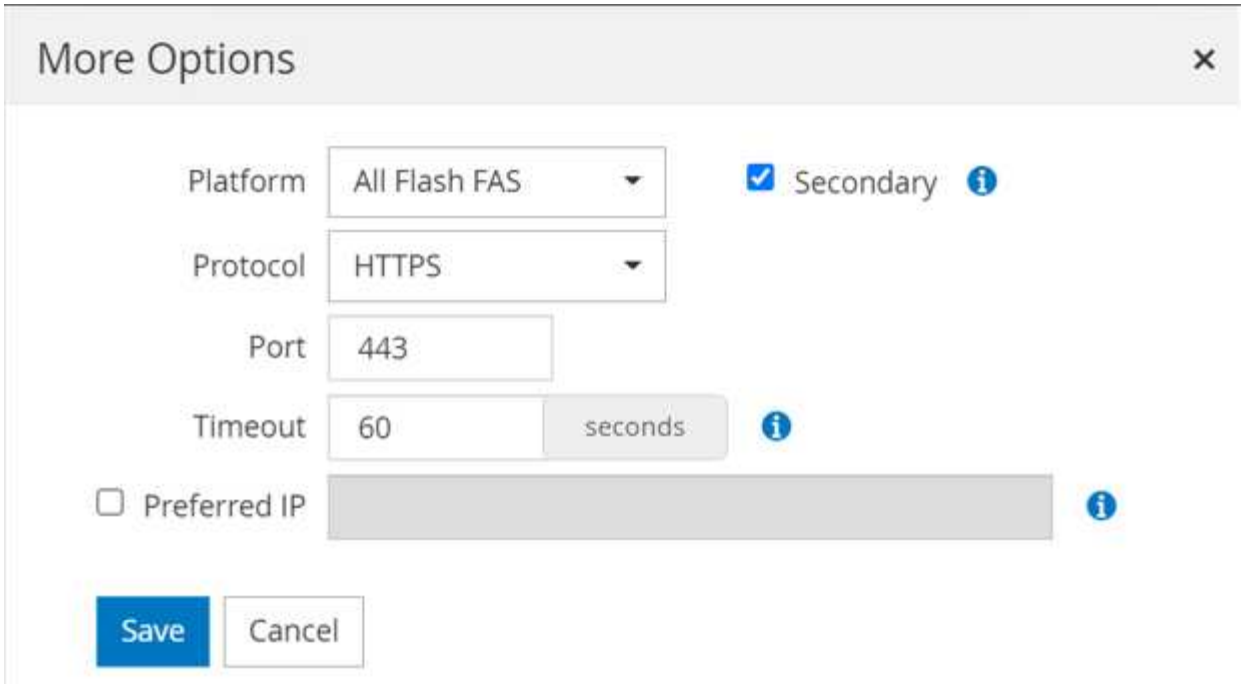
**SnapCenter** にバックアップ**SVM**を追加

## 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。

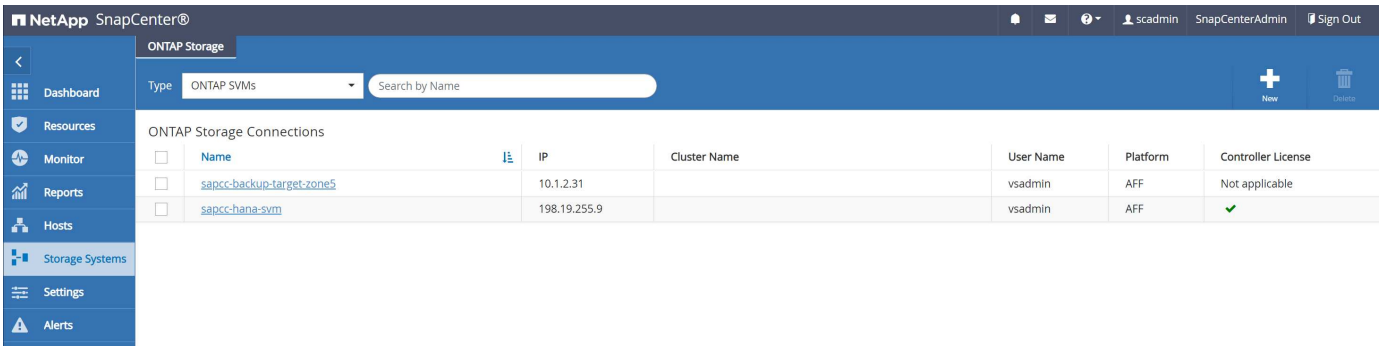
1. SnapVault ターゲットボリュームが配置されているSVMをSnapCenter に設定します。




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。



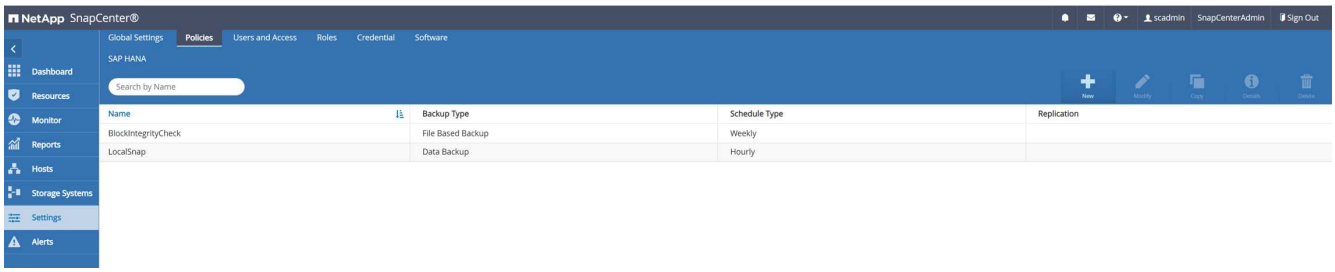

これで、SVMをSnapCenter で使用できるようになります。



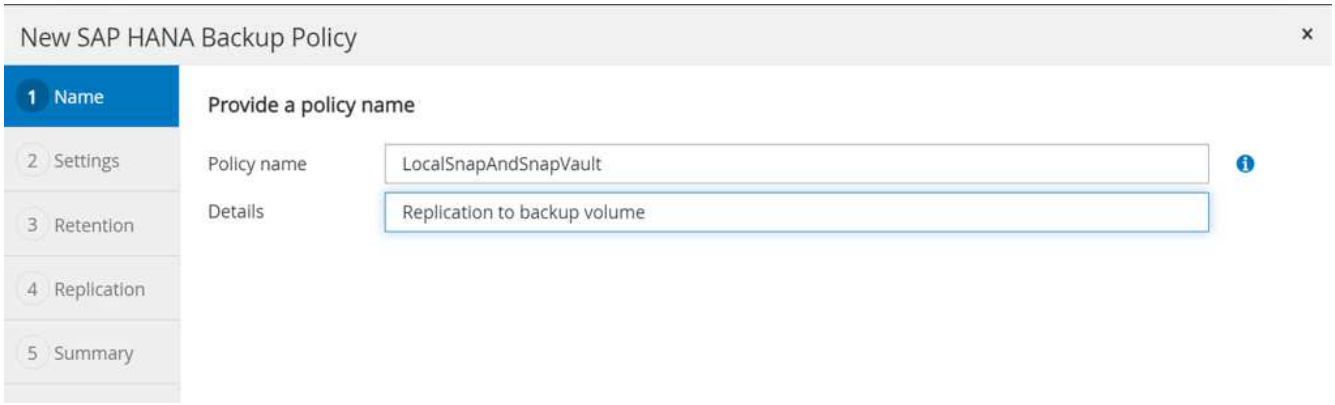

バックアップレプリケーション用の新しい**SnapCenter** ポリシーを作成します

## 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。

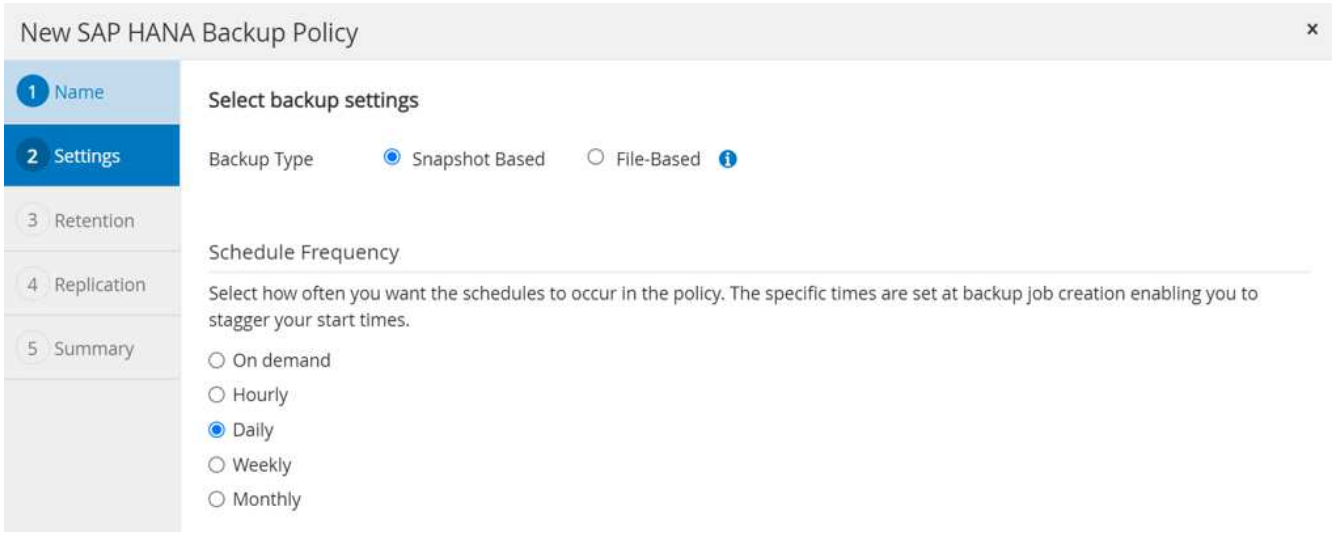
1. ポリシーの名前を指定します。



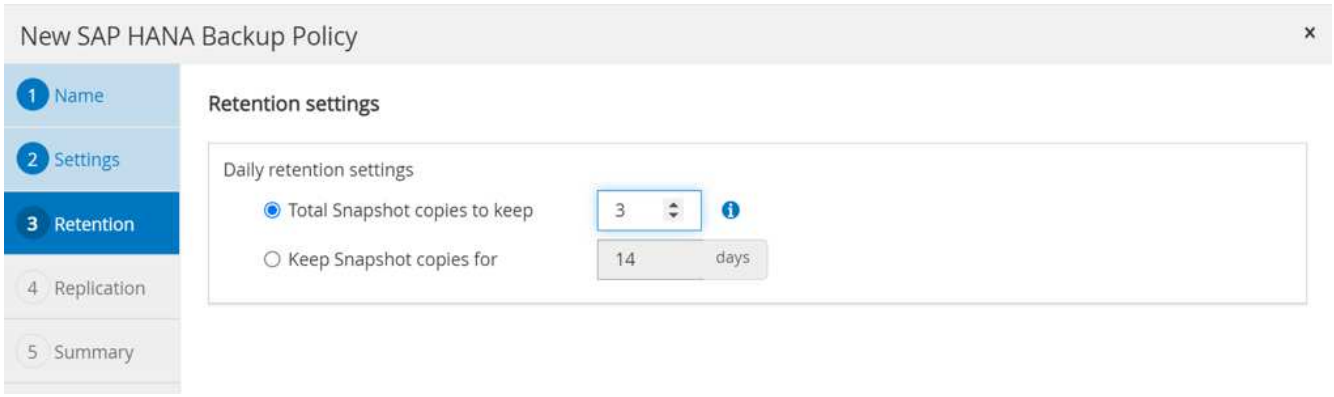

2. Snapshotバックアップとスケジュール頻度を選択します。通常、Dailyはバックアップのレプリケーションに使用されます。




3. Snapshotバックアップの保持期間を選択します。

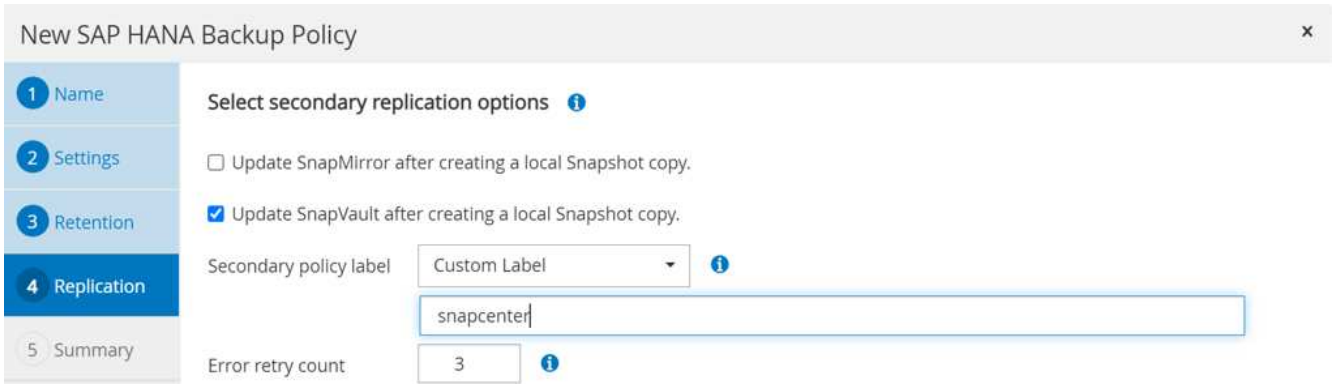


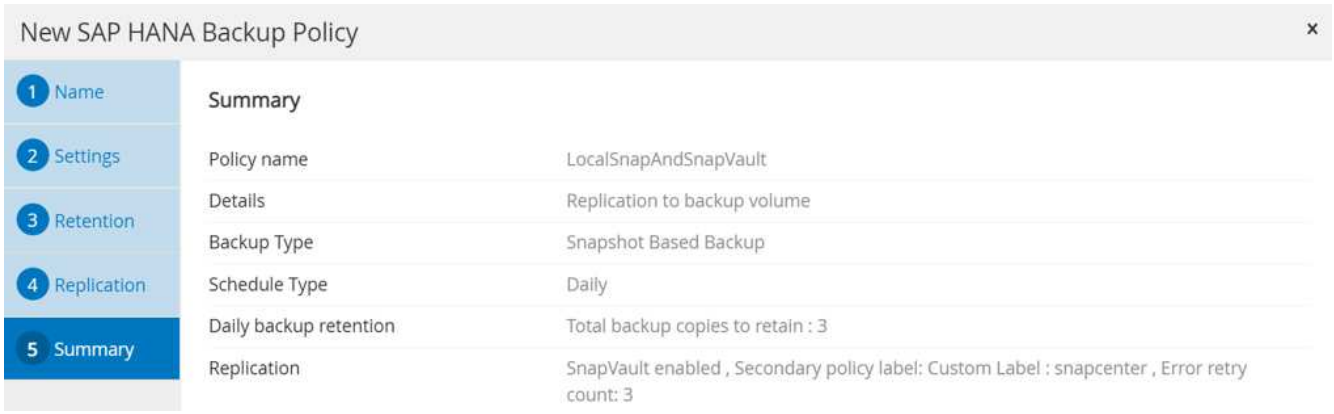

これは、プライマリストレージで作成された日単位のSnapshotバックアップの保持です。SnapVault ターゲットでのセカンダリバックアップの保持設定は、ONTAP レベルでadd ruleコマンドを使用してすでに設定されています。「ONTAP ファイルシステムのFSXでのレプリケーション関係の構成」（xref）を参照してください。



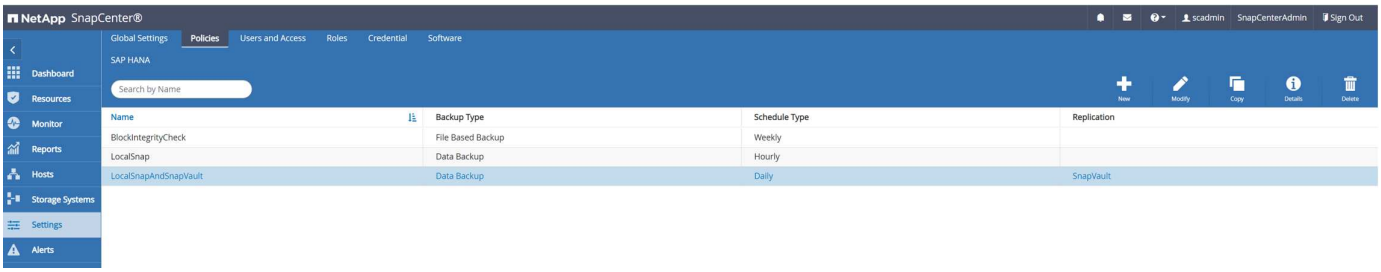

4. Update SnapVault フィールドを選択し、カスタムラベルを指定します。

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。



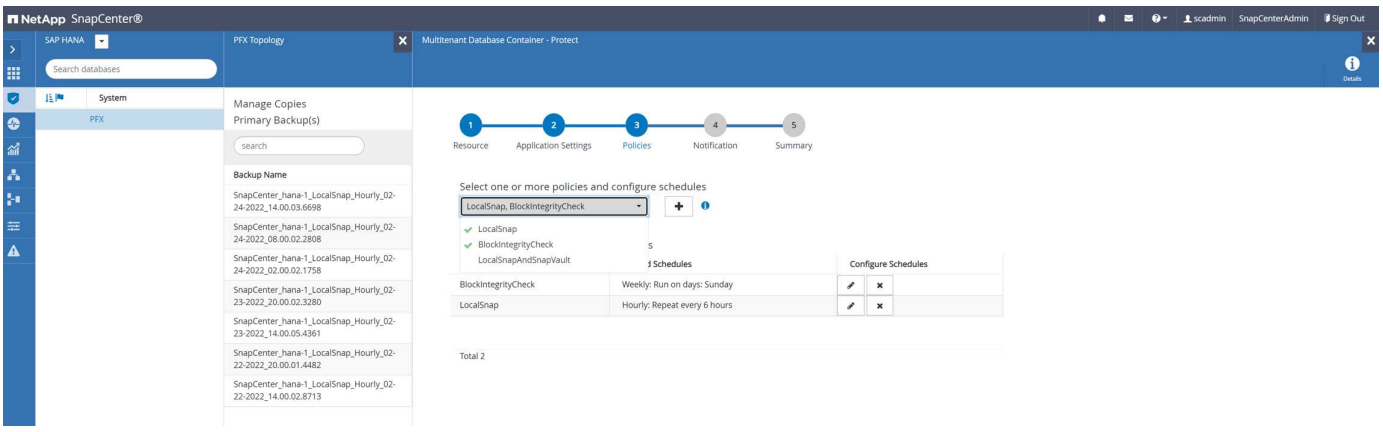




これで新しいSnapCenter ポリシーが設定されました。

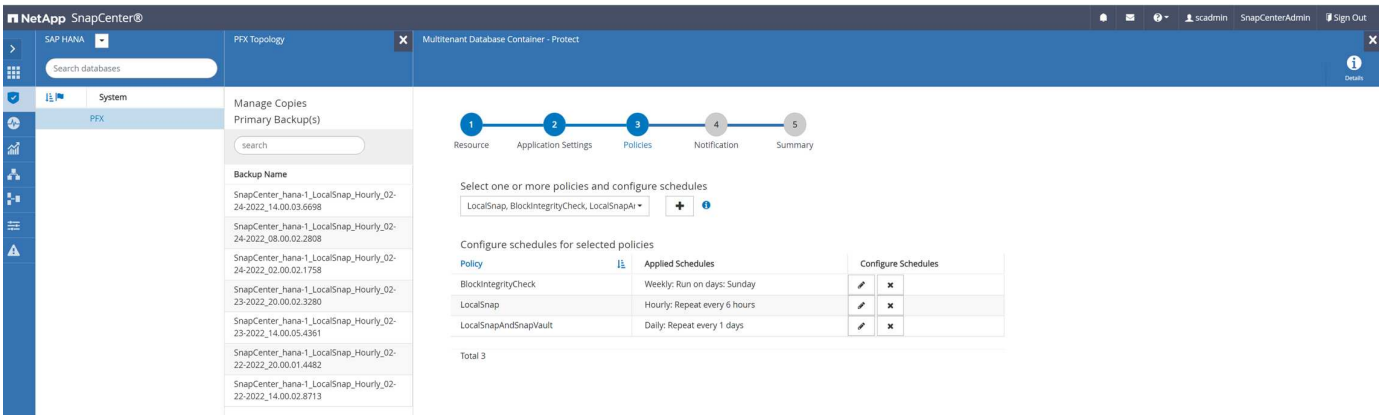



リソースの保護にポリシーを追加します

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。



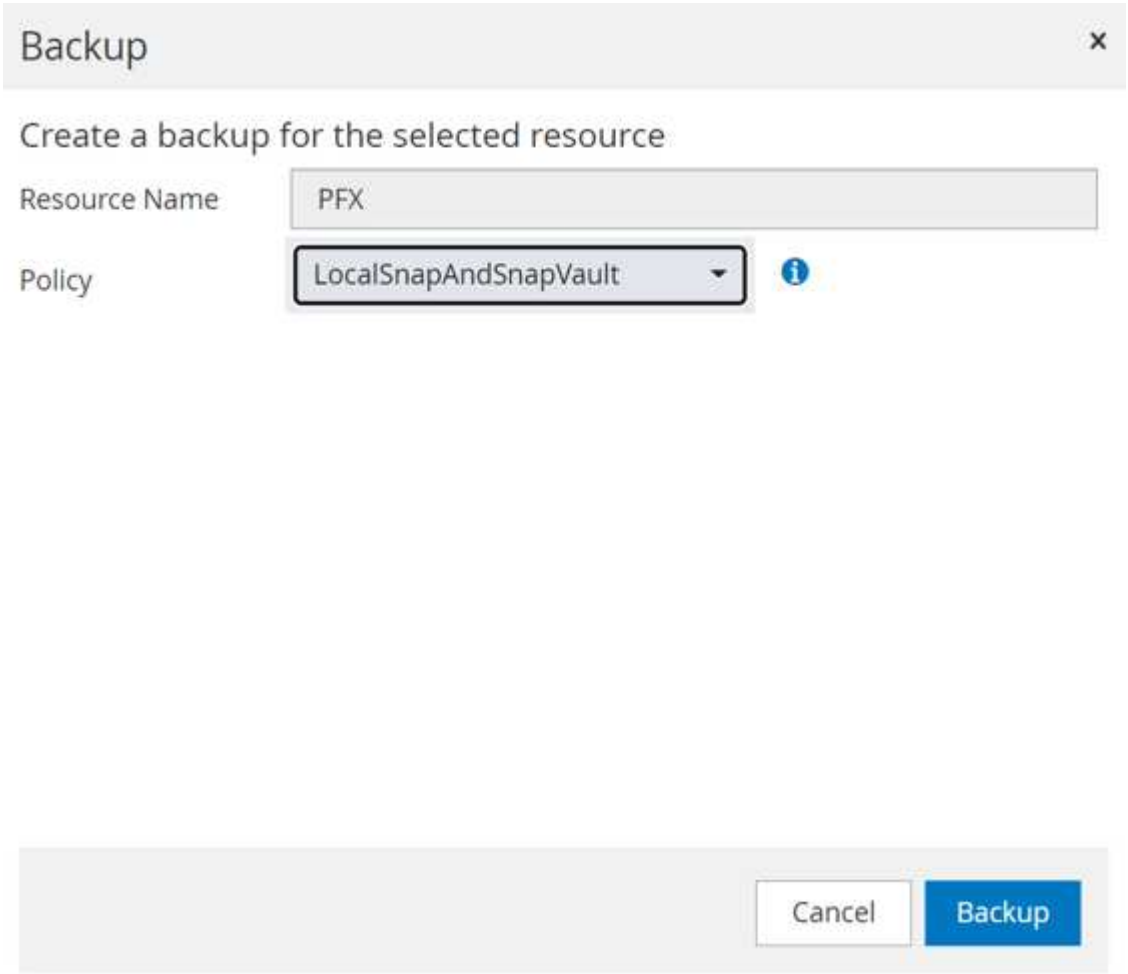
セットアップでは、日次スケジュールを定義します。




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

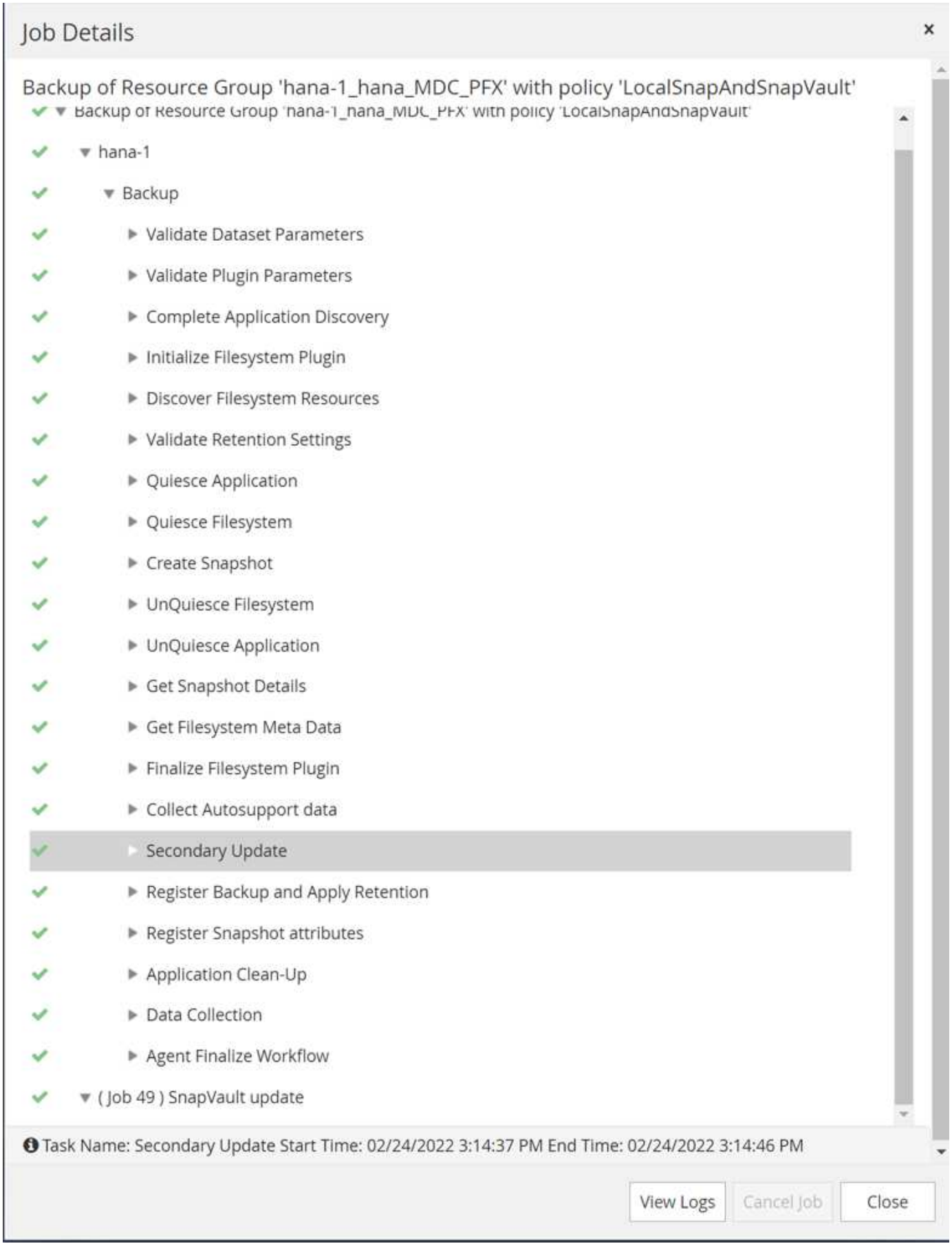
## バックアップは、ローカルSnapshotコピーと同じ方法で作成します。

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。

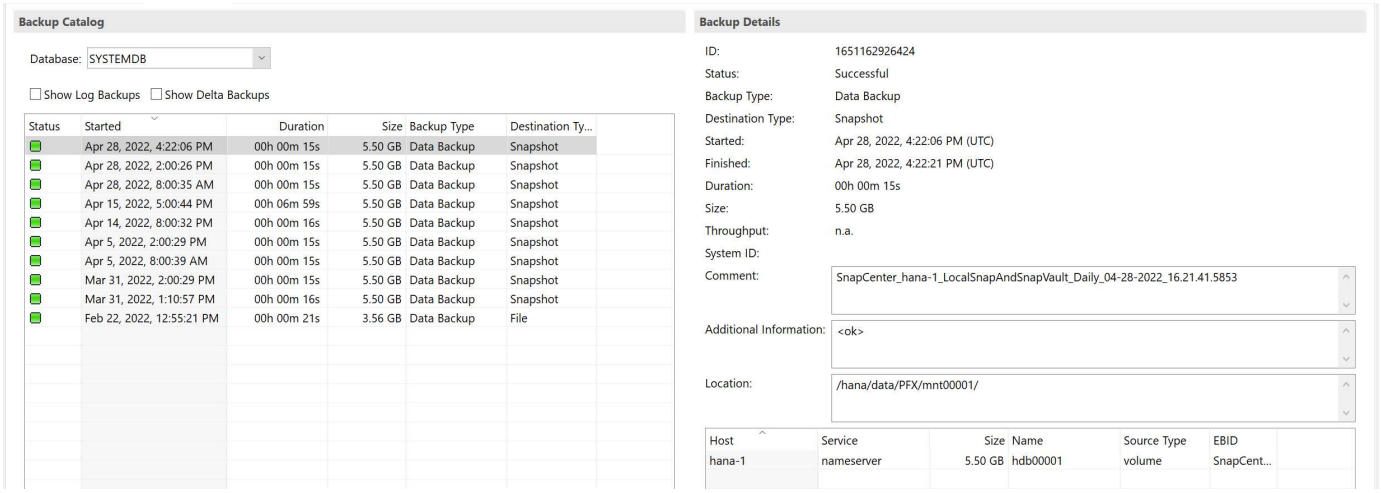
```
FsxId00fa9e3c784b6abbb::> snapshot show -vserver sapcc-hana-svm -volume
PFX_data_mnt00001 -fields snapmirror-label
vserver        volume            snapshot
snapmirror-label
-------------- -----------------
---------------------------------------------------------------
----------------
sapcc-hana-svm 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.
```

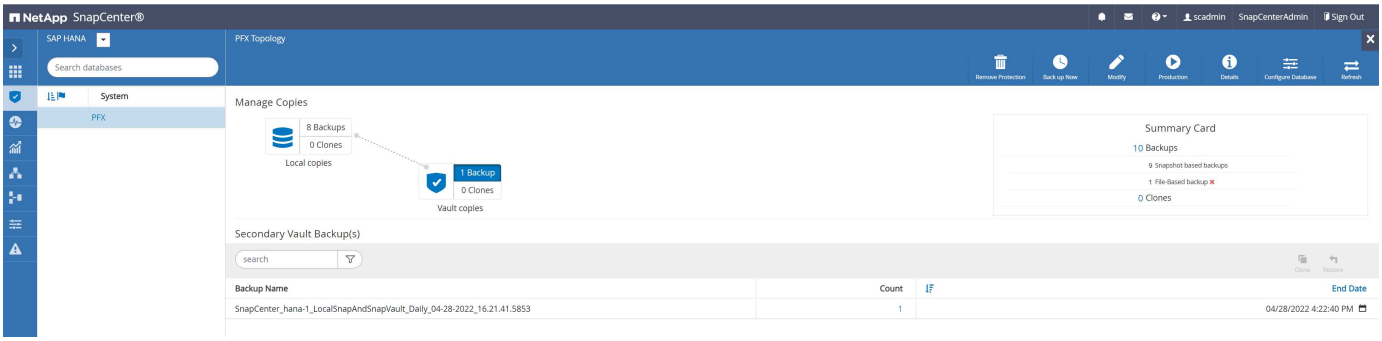
ターゲットボリュームに、同じ名前のSnapshotコピーが作成されます。

```
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。



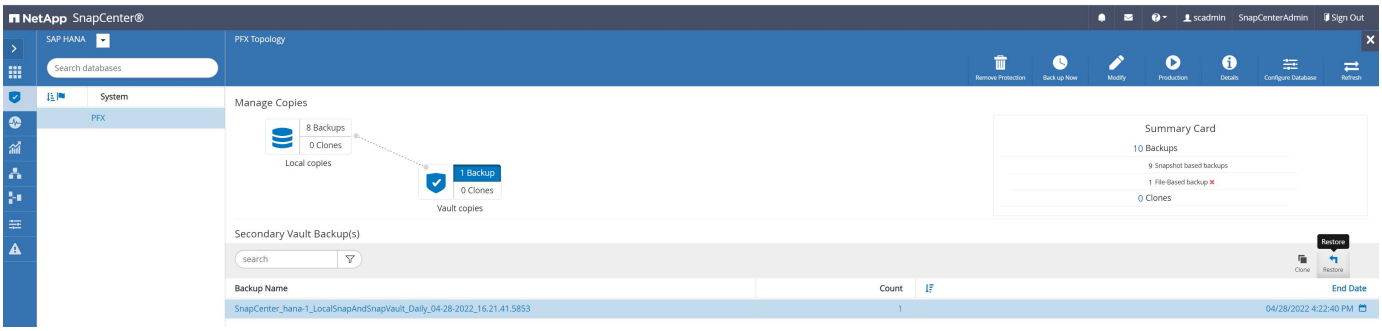

SnapCenter では、トポロジビューのバックアップコピーをクリックして、レプリケートされたバックアップのリストを表示できます。



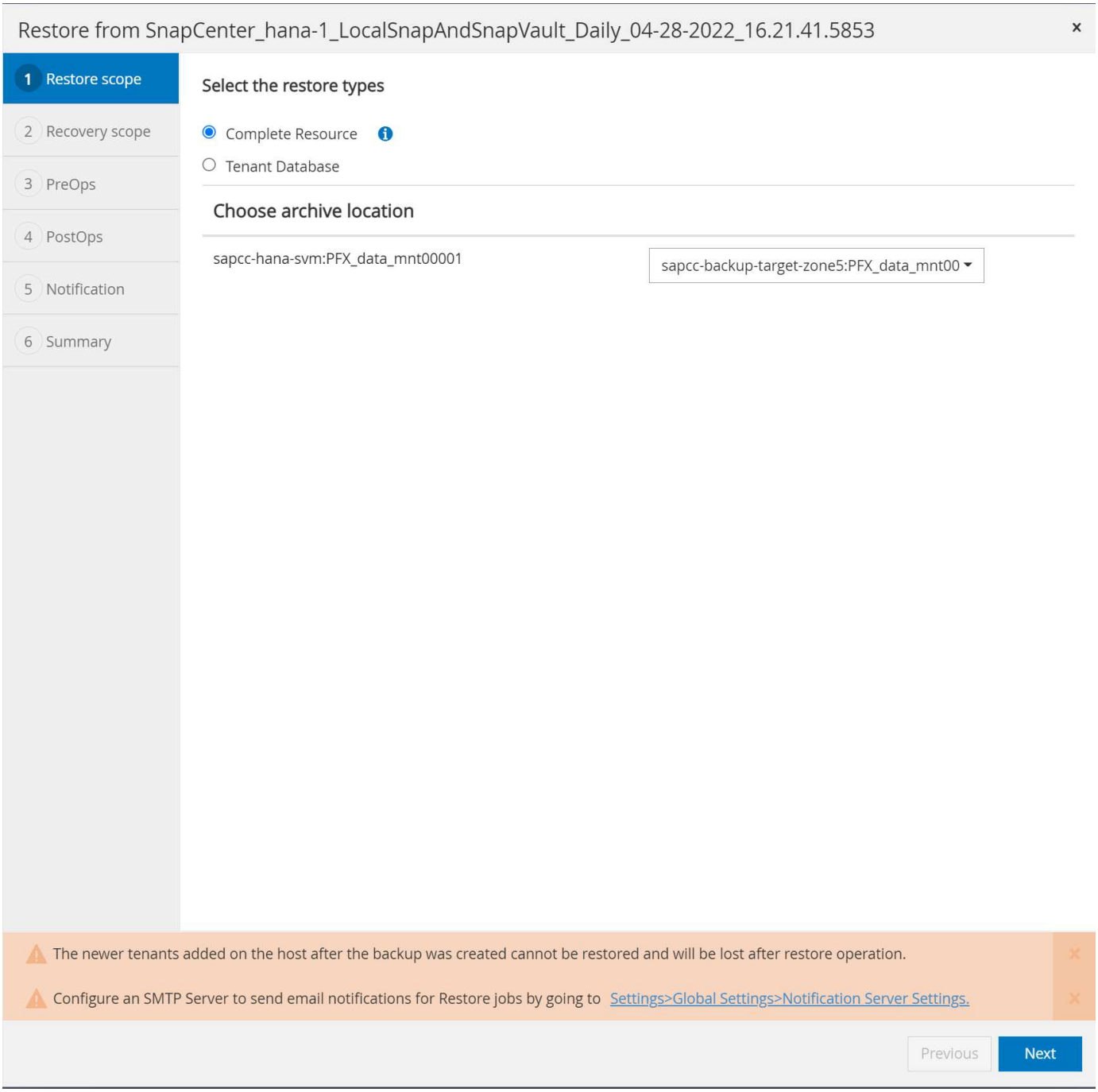

セカンダリストレージからリストアおよびリカバリする

## 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。




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"

- 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 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 |

# 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 』

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。

作成者：Nils Bauer、NetApp

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。

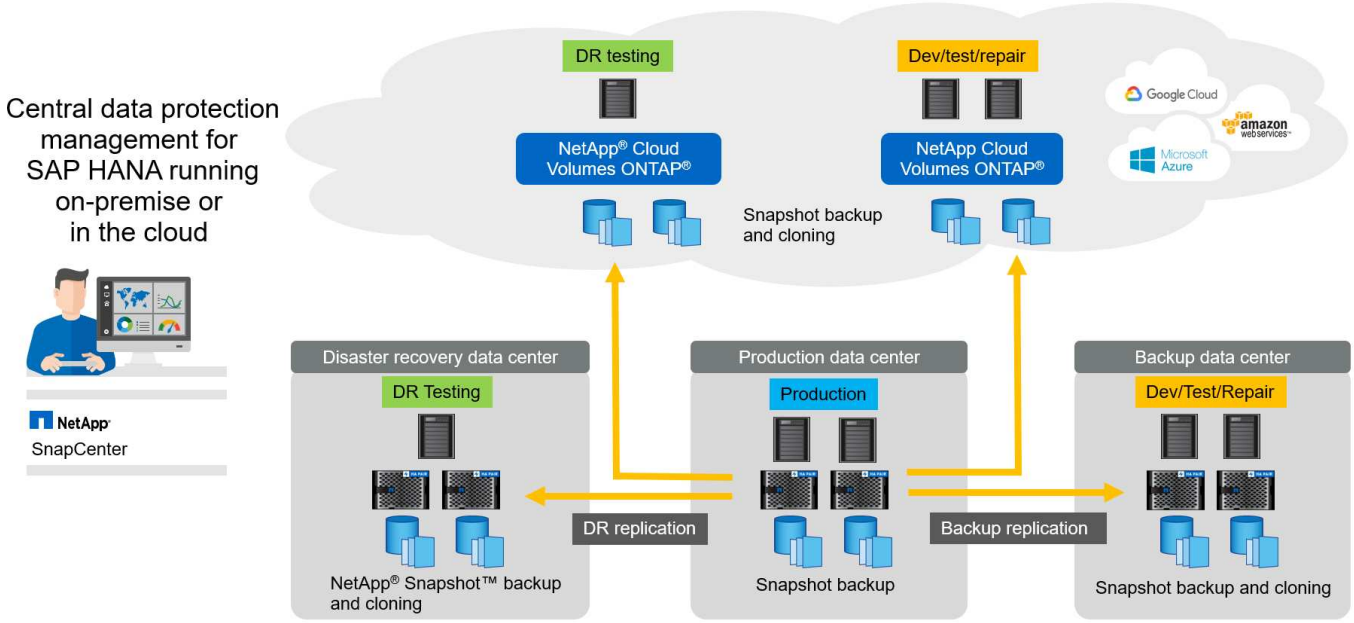
Snapshot コピーは、リストア処理とリカバリ処理にも大きなメリットがあります。NetApp SnapRestore データリカバリソフトウェアを使用すると、データベース全体または利用可能な Snapshot コピーに基づいて、データベースの一部を任意の時点にリストアできます。このようなリストアプロセスは、データベースのサイズに関係なく数分で完了します。オンラインの Snapshot バックアップは 1 日に数回作成されるため、従来のバックアップ方式に比べて、リカバリプロセスに要する時間が大幅に短縮されます。24 時間以内ではなく数時間前の Snapshot コピーを使用してリストアできるため、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。

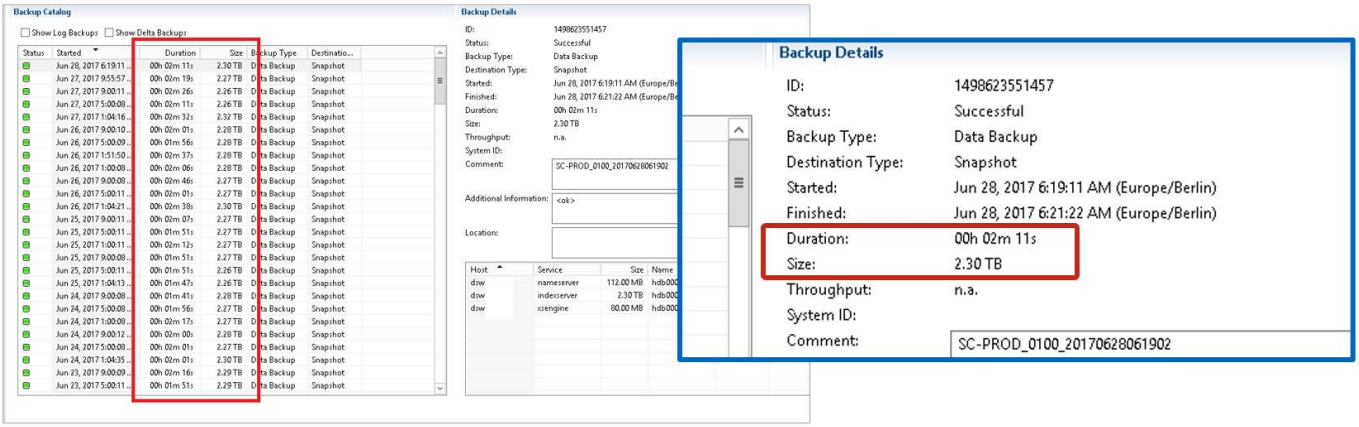
解決策 は、ハイブリッドクラウド運用モデルにシームレスに拡張することもできます。ディザスタリカバリやオフサイトのバックアップを目的としたデータレプリケーションは、オンプレミスの NetApp ONTAP システムから、クラウドで実行されている Cloud Volumes ONTAP インスタンスに実施できます。SnapCenter は、 SAP HANA システムをオンプレミスで実行する場合でも、クラウドで実行する場合でも、データ保護とデータレプリケーションを一元的に管理するツールとして使用できます。次の図に、バックアップ解決策 の概要を示します。




**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

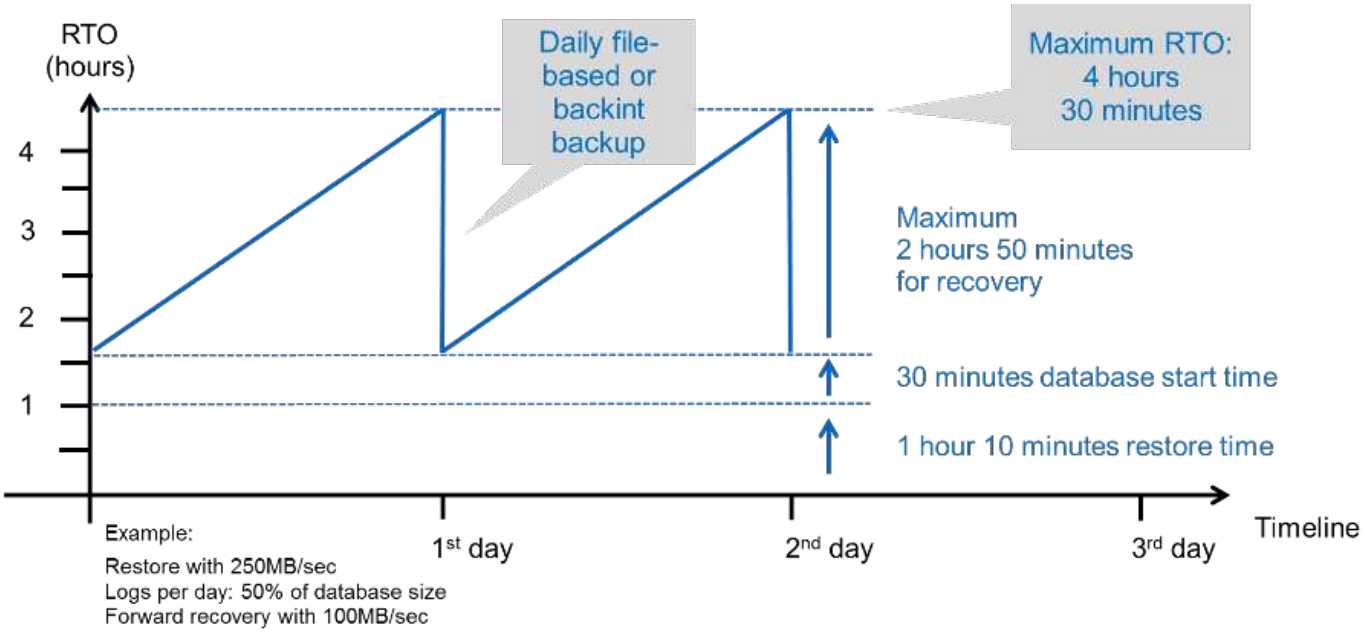
リカバリ時間は、リストア後に適用する必要があるログの数によって異なります。この数は、データバックアップを実行する頻度によって決まります。

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。

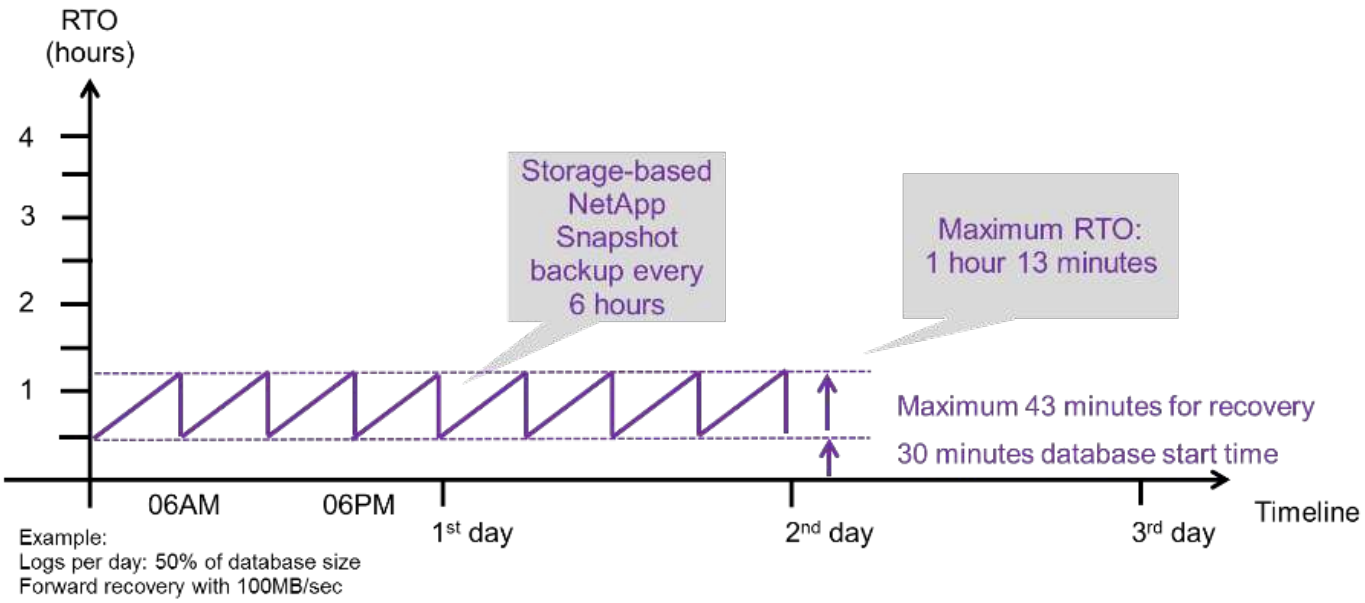
ストレージ Snapshot コピーのデータバックアップは、通常、 SAP HANA データベースのパフォーマンスに影響しないため、頻繁にスケジュールされます。たとえば、 Snapshot コピーのバックアップを 6 時間ごとに実行するようにスケジュールした場合、最大でファイルベースのバックアップのリカバリ時間の 4 分の 1 （ 6 時間 /24 時間 = ¼ ）というリカバリ時間がかかります。

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。

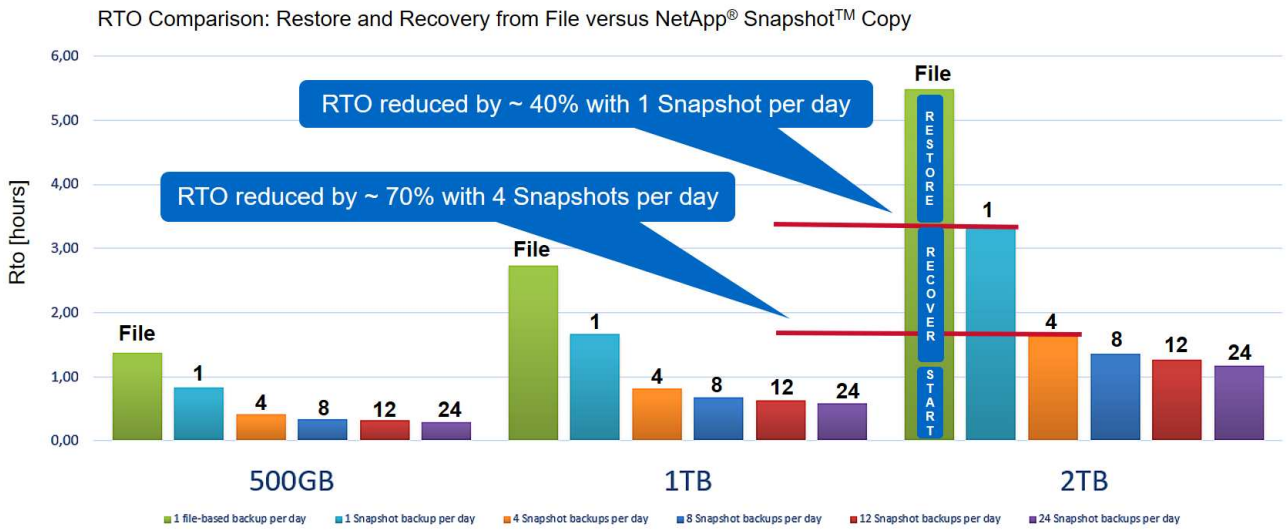



次の図に、 Snapshot バックアップの使用時の 1TB データベースの RTO の例を示します。ストレージベースの Snapshot バックアップでは、データベースのサイズに関係なく数秒でリストアが完了するため、 RTO はデータベースの開始時間と転送リカバリ時間にのみ左右されます。また、リストアとリカバリの実行タイミングによってもフォワードリカバリの時間が長くなりますが、バックアップの頻度が高い（この例では 6 時間ごと）ため、最大で 43 分までリカバリ時間が短縮されます。この例では、最大 RTO は 1 時間 13 分です。




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。

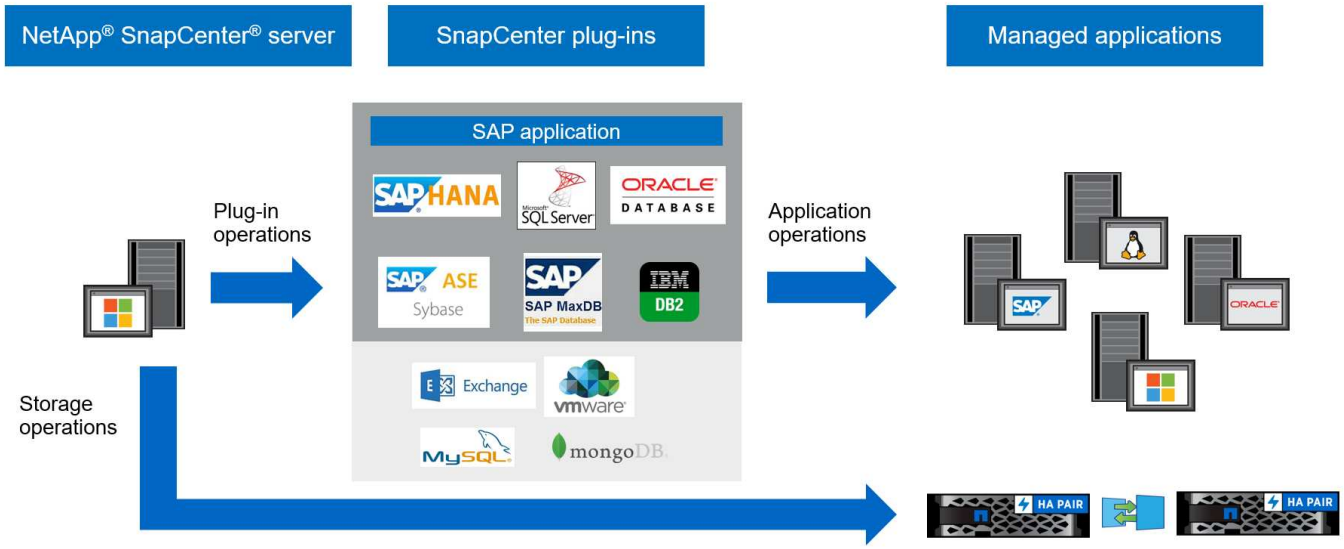
SnapCenter は、ネットアップのデータファブリック内のすべてのエンドポイントのデータを管理します。SnapCenter を使用して、オンプレミス環境間、オンプレミス環境とクラウド間、およびプライベートクラウド、ハイブリッドクラウド、パブリッククラウド間でデータをレプリケートできます。

### 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。

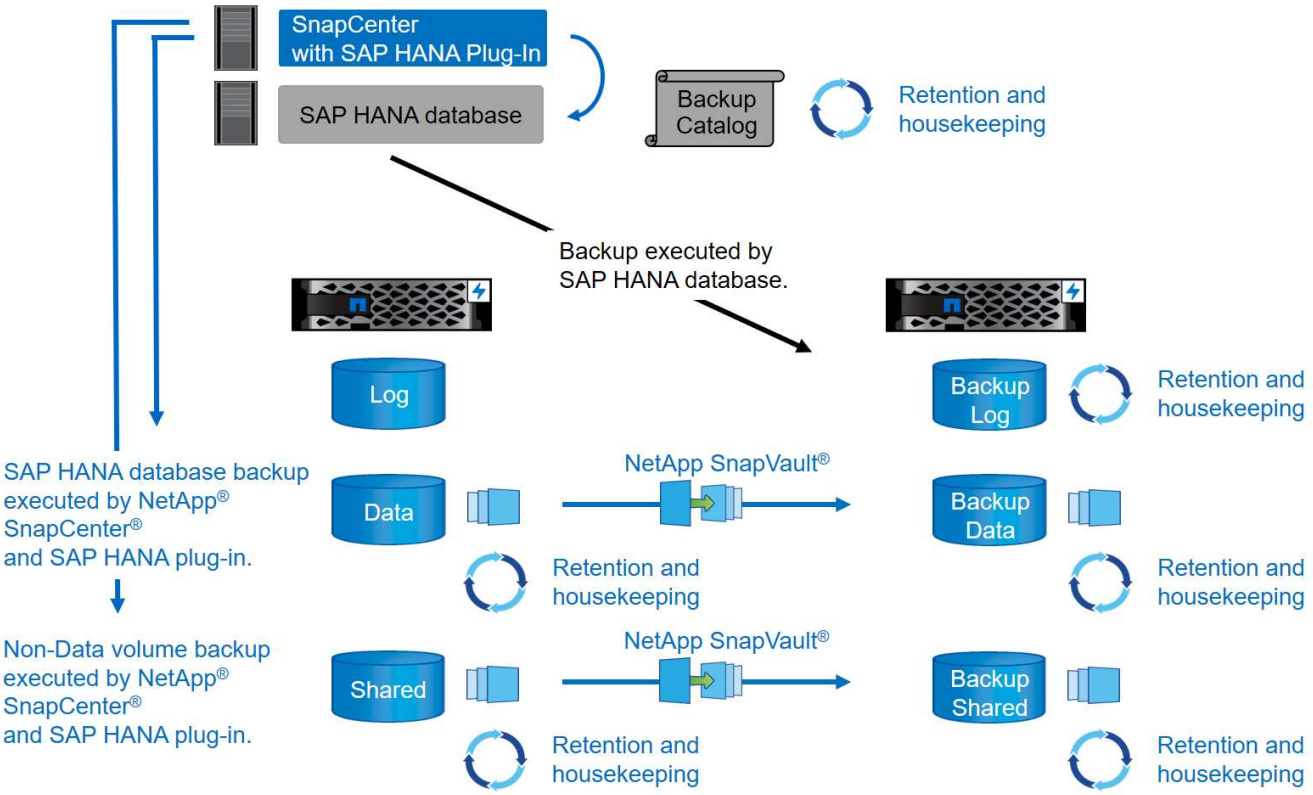
SAP HANA データベースは、ログバックアップを自動的に実行します。目標復旧時点に応じて、ログ・バックアップの保存場所に関するいくつかのオプションがあります。

- 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

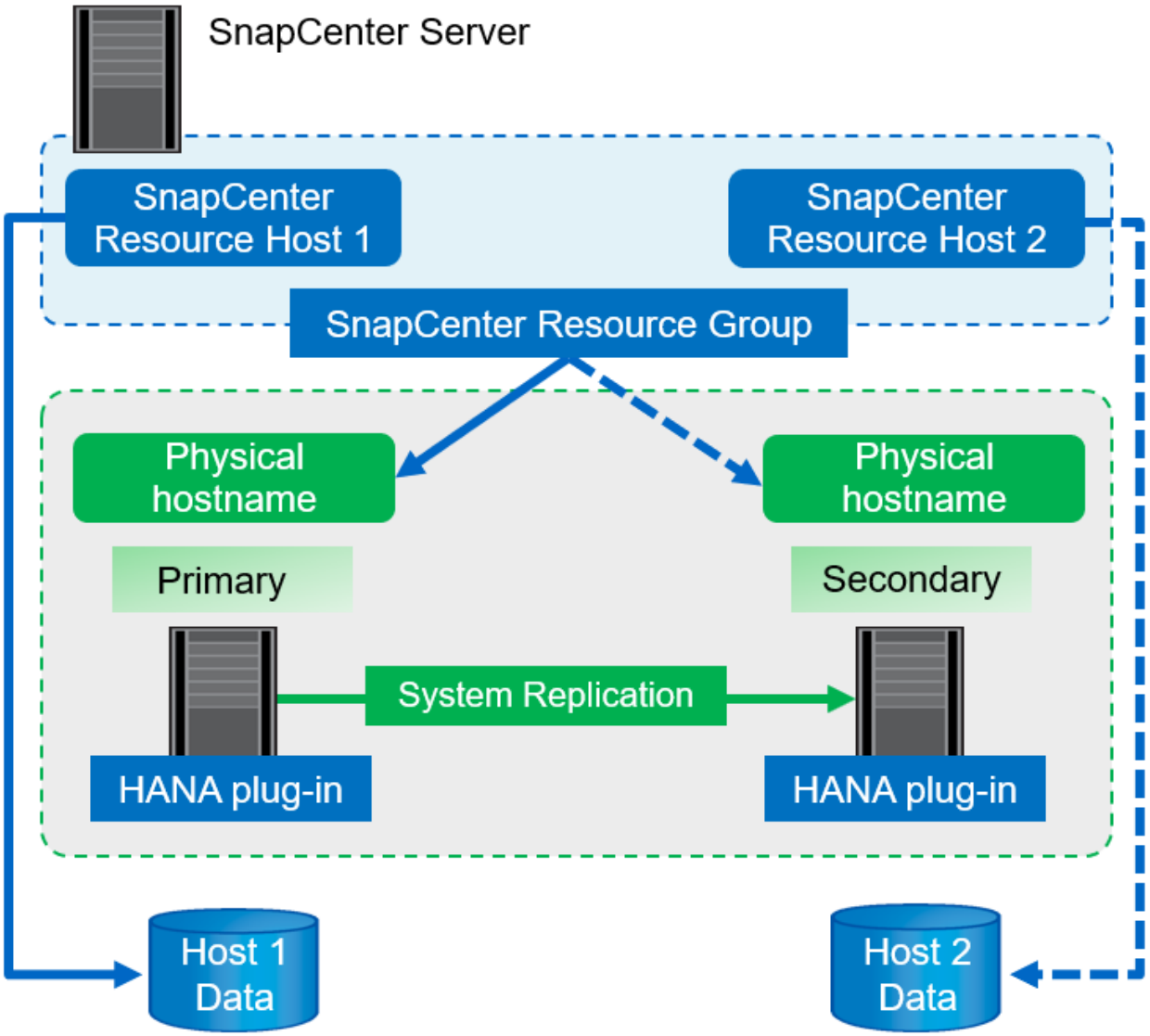
SnapCenter は、 NFS または FC 接続のネットアップストレージシステム（ AFF および FAS ）を使用した SAP HANA シングルホスト構成とマルチホスト構成、および NFS を使用した AWS 、 Azure 、 Google Cloud Platform 、 AWS FSX ONTAP で Cloud Volumes ONTAP を実行している SAP HANA システムをサポートしています。

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でのHANAシステムレプリケーションに対応したHANAシステムの構成と運用の詳細については、を参照 "TR-4719 『 SAP HANA System Replication 、 Backup and Recovery with SnapCenter 』"してください。




# 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。

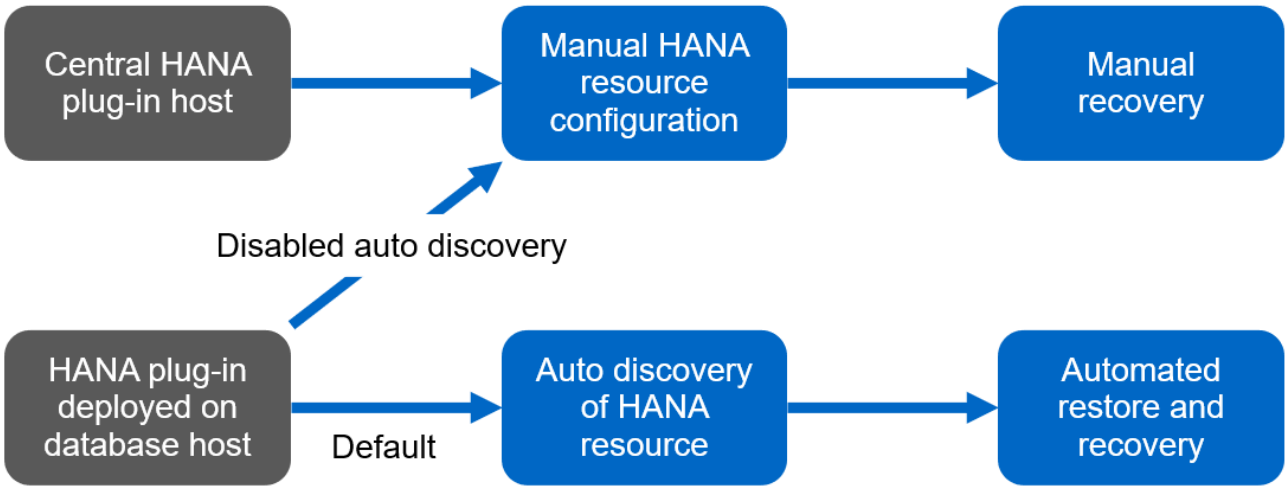
- * リソースを手動で構成。 * HANA のリソースとストレージの設置面積に関する情報は、手動で提供する必要があります。
- * HANA リソースの自動検出。 * 自動検出により、 SnapCenter での HANA データベースの設定が簡易化され、リストアとリカバリが自動化されます。

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<br>• 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<br>• HANA システムレプリケーション | • NFS のベアメタル<br>• 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<br>• 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。

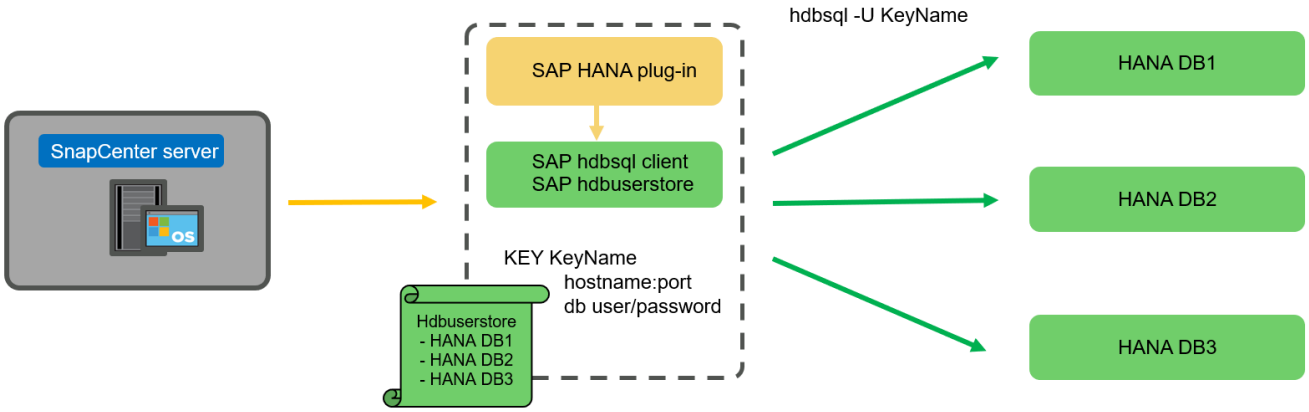
| **HANA** プラグインのインストール場所： | **HANA** のアーキテクチャ | **HANA** システム構成 | インフラ |
| --- | --- | --- | --- |
| 中央プラグインホスト（ SnapCenter サーバまたは個別の Linux ホスト） | 単一または複数のホスト | • HANA の単一コンテナ<br>• シングルテナントまたはマルチテナントの HANA MDC<br>• HANA システムレプリケーション | • NFS のベアメタル<br>• Linux LVM の有無に関係なく、 XFS と FC を使用するベアメタル<br>• VMware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

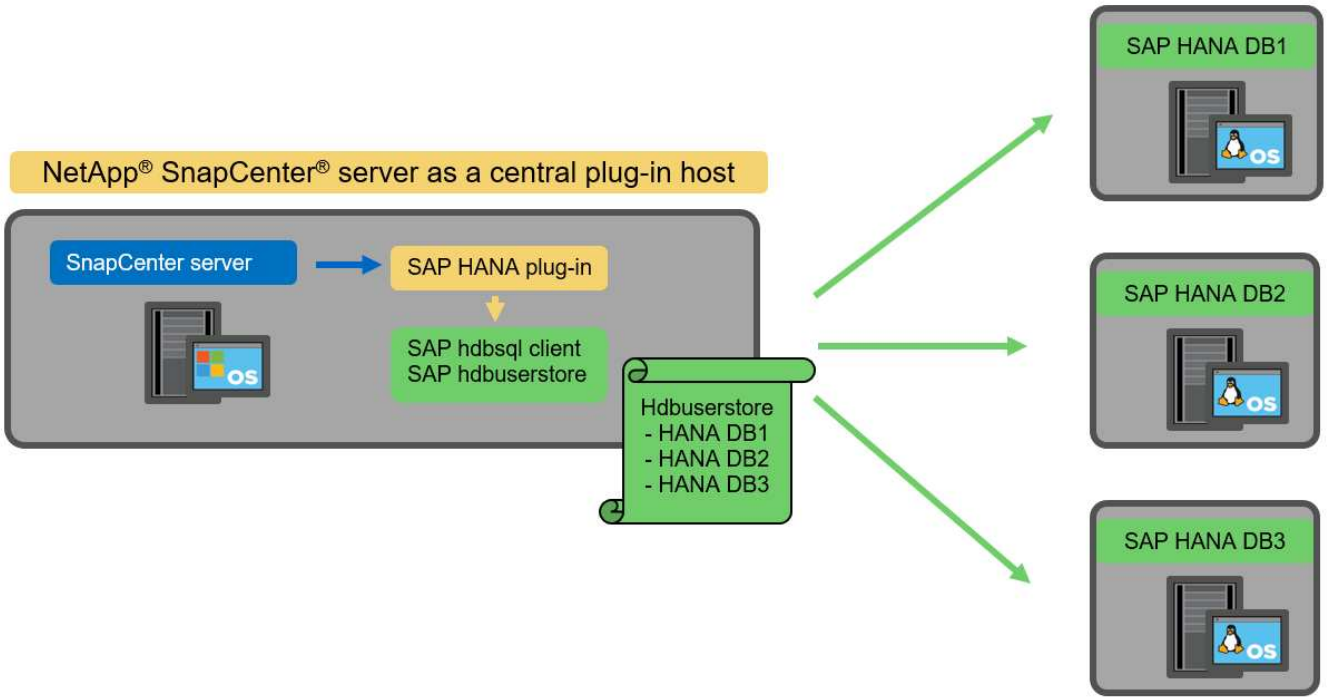
#### SnapCenter サーバの高可用性

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。

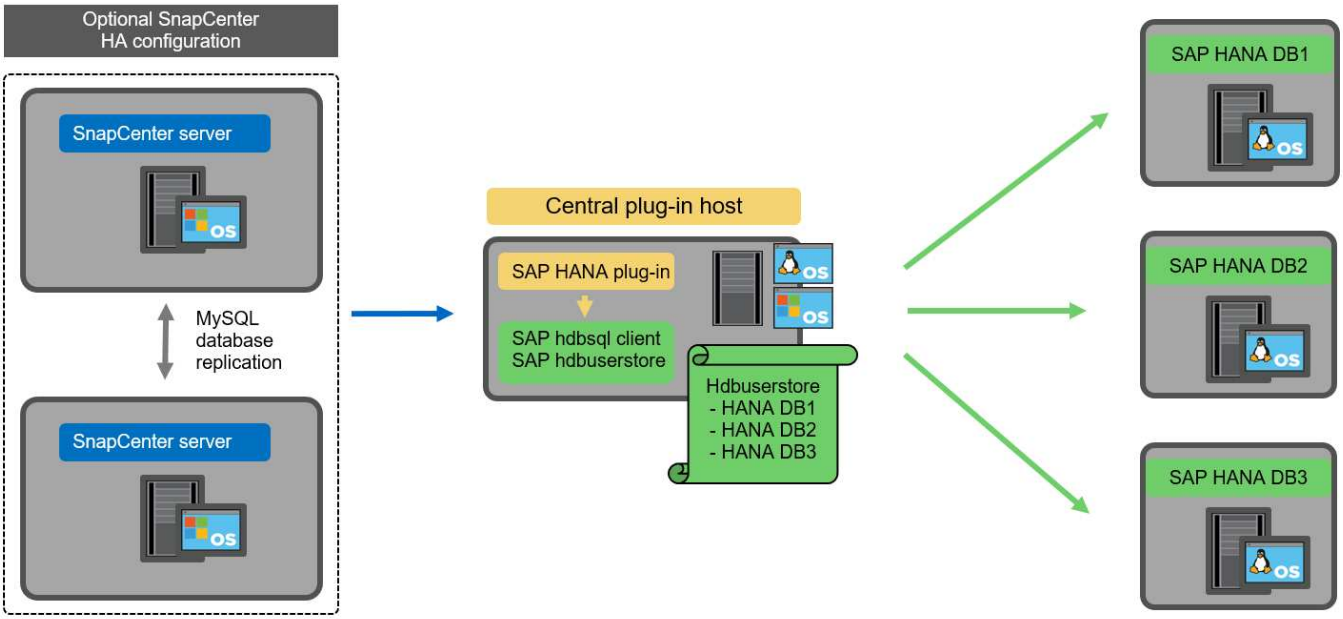
一方、自動検出のワークフロー自動化の強化、リストアとリカバリの自動化、 SAP システムの更新処理を行う際には、データベースホストに SnapCenter コンポーネントをインストールする必要があります。中央の HANA プラグインホストを使用している場合、これらの機能は使用できません。

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。

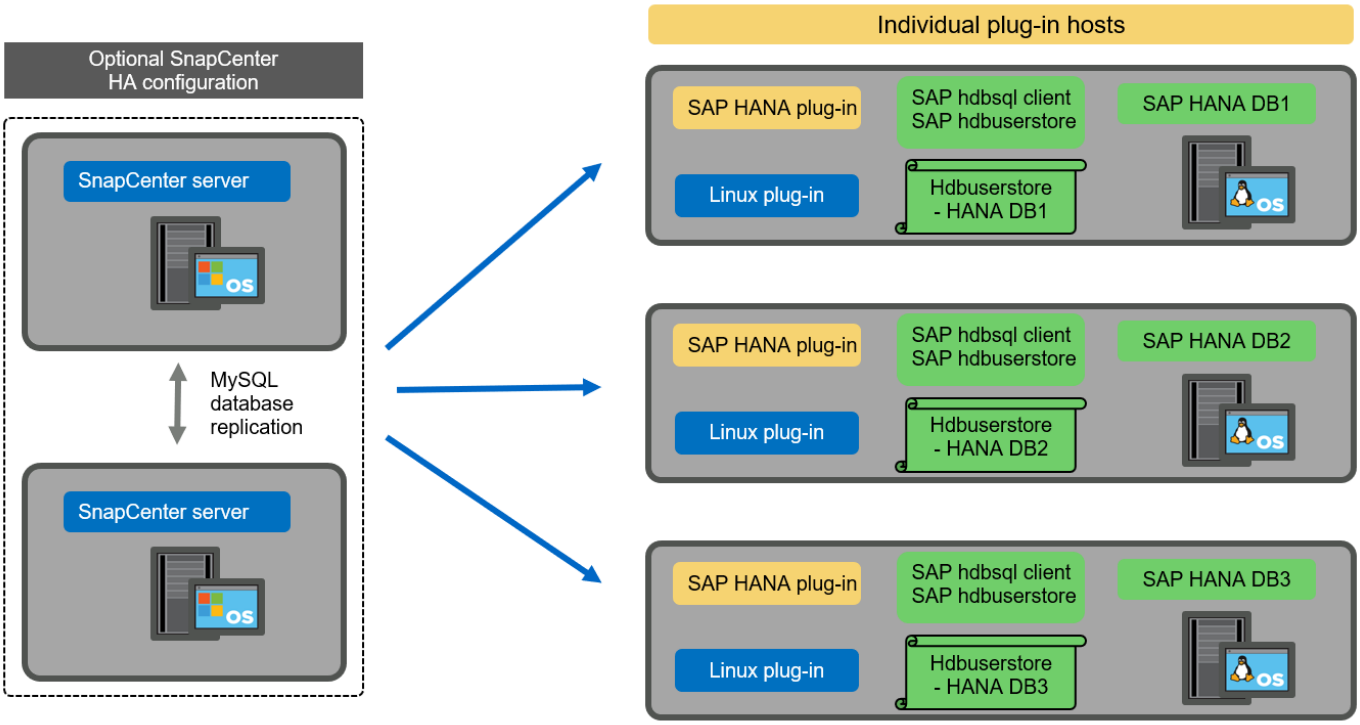



前のセクションで説明した機能の可用性に関する同様の制限は、別の中央プラグインホストにも適用されます。

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。



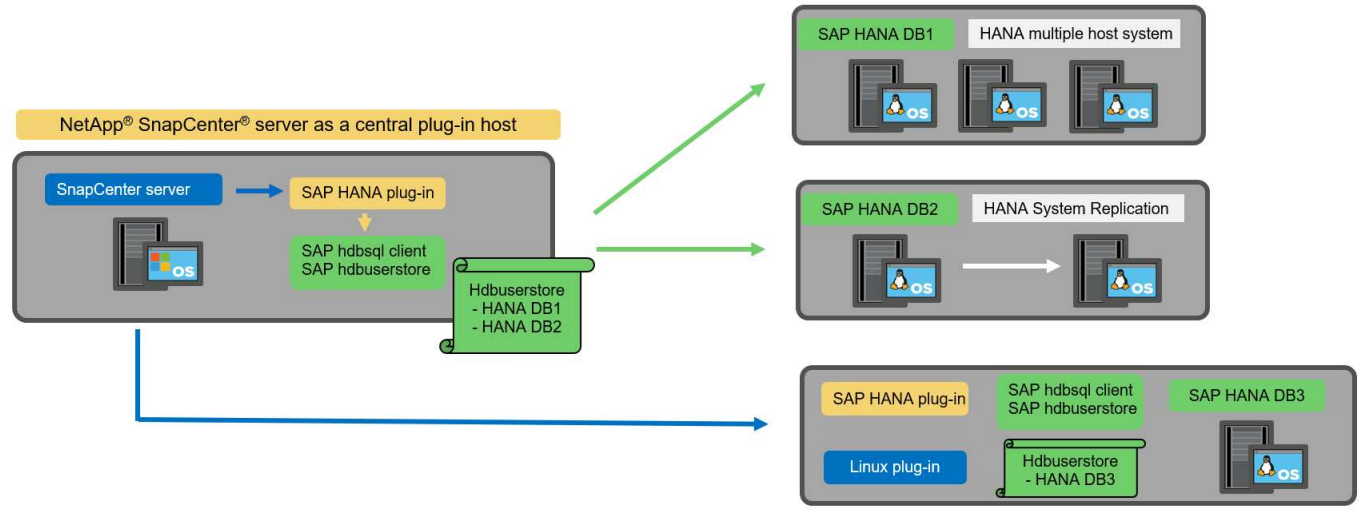
HANA プラグインを各 HANA データベースホストにインストールすると、自動検出やリストアとリカバリの自動化などのすべての機能を使用できるようになります。また、 SnapCenter サーバは HA 構成でセットアップできます。

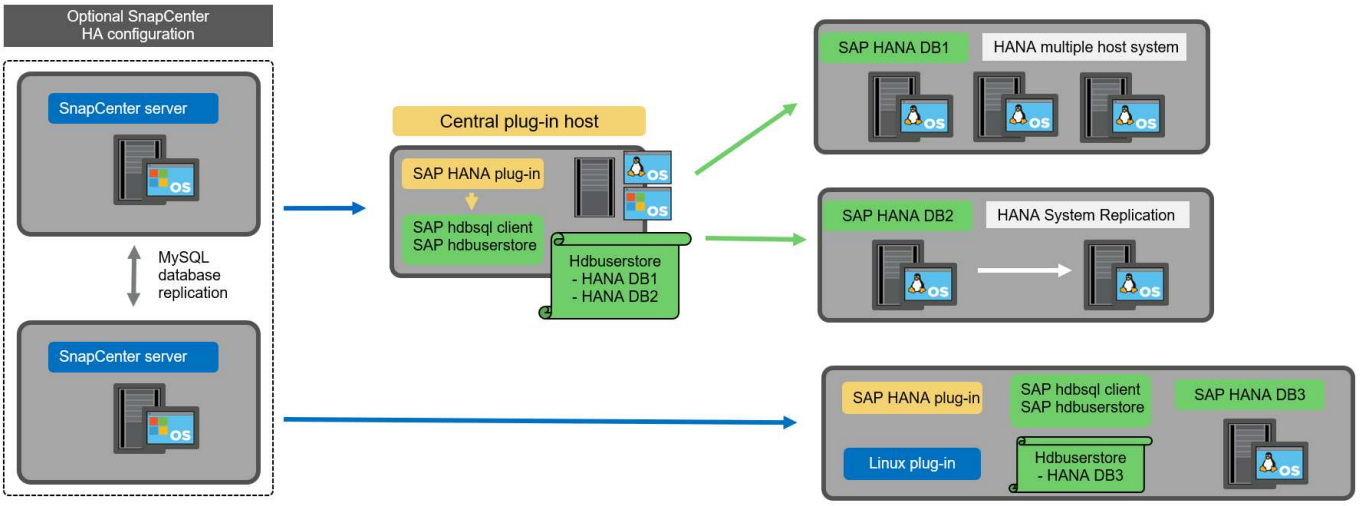
#### HANA 混在プラグイン環境をサポート

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。

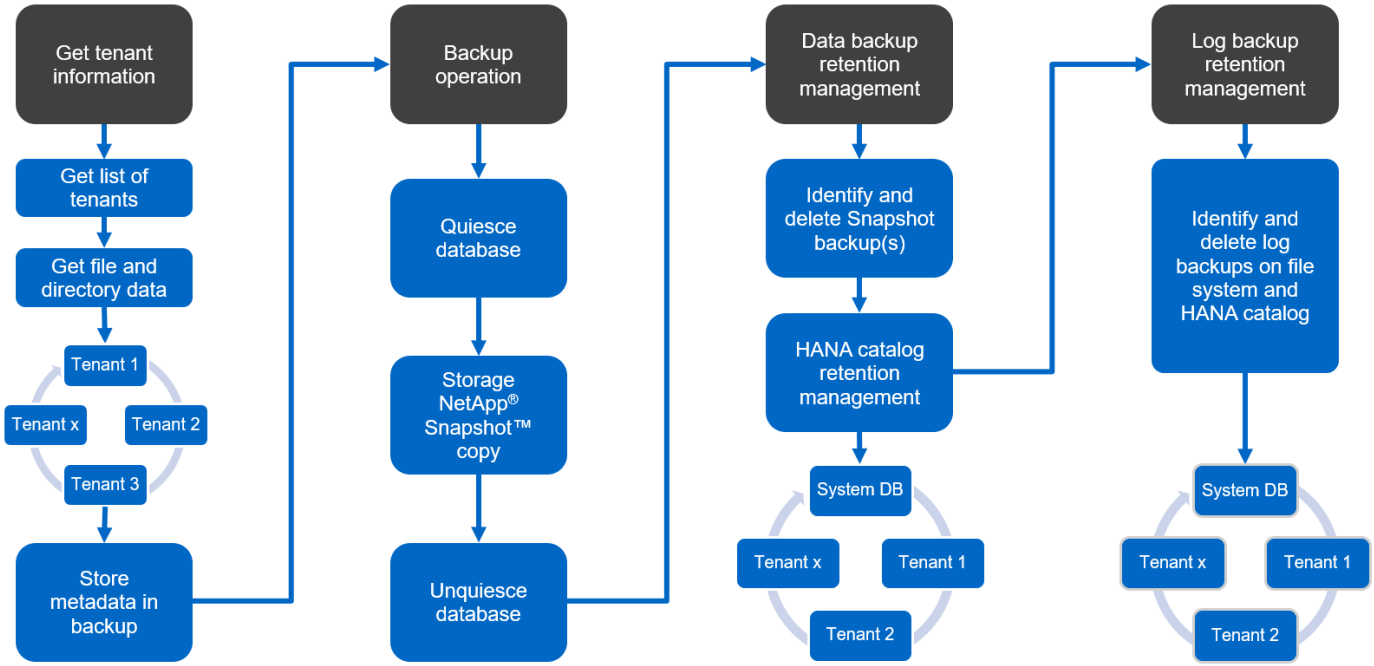
したがって、バックアップ処理を実行するたびに、テナント情報を取得する必要があります。これには、テナ

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。

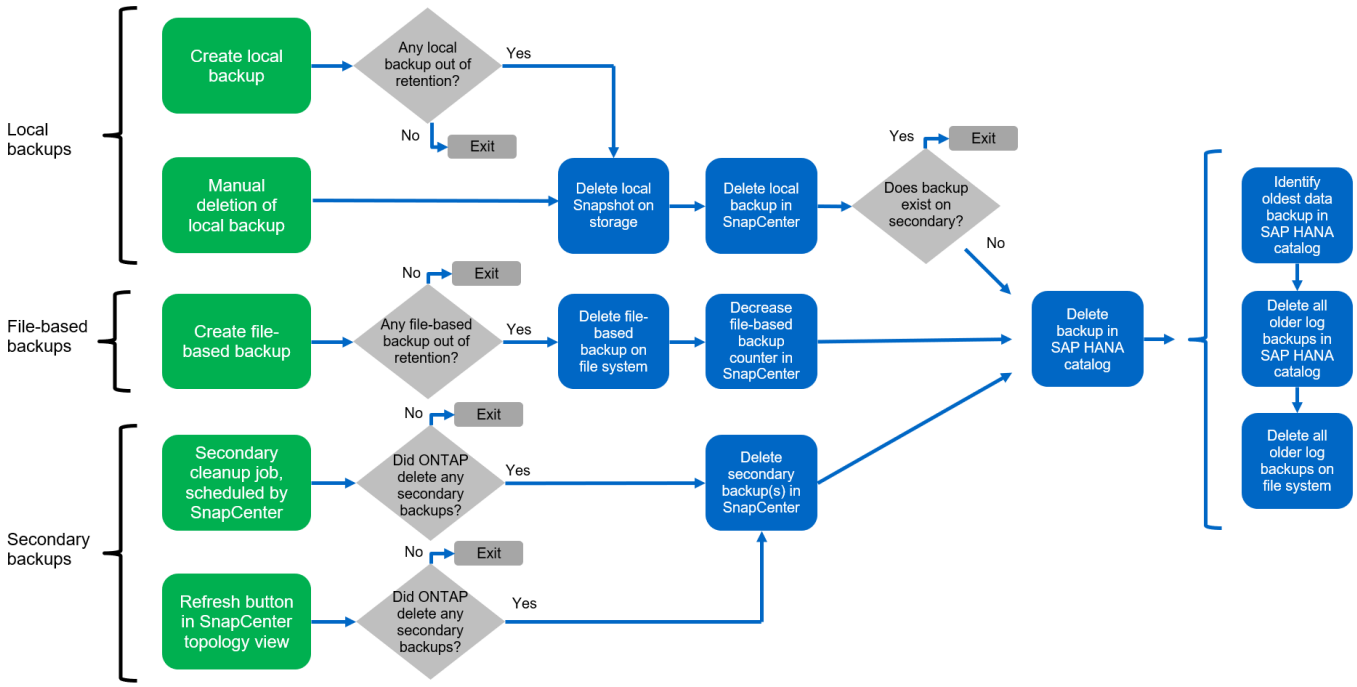
   この手順は、ログバックアップの不要ファイルの削除が無効になっていない場合にのみ実行します。

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調整する方法、または手動更新をトリガーする方法の詳細については、のセクション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、セクション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 ：

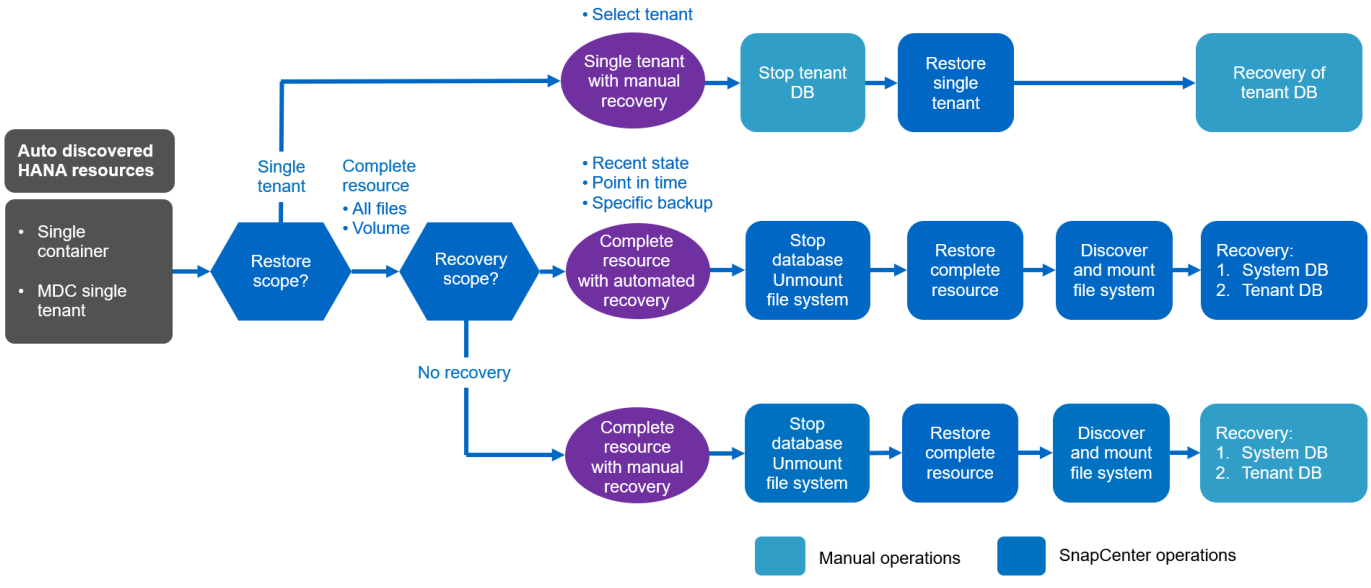
- プライマリストレージ。ファイルベースの SnapRestore 処理は、テナントデータベースのすべてのファイルに対して実行されます。
- オフサイトのバックアップストレージ： SnapVault リストア処理は、テナントデータベースのすべてのファイルに対して実行されます。

- 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。



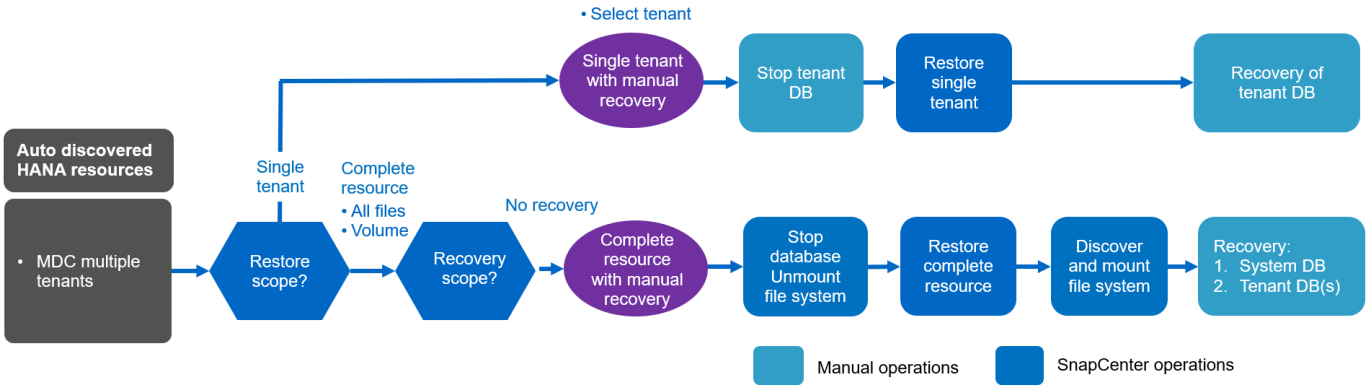

自動検出された **HANA MDC** のマルチテナントシステムのリストアとリカバリ

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

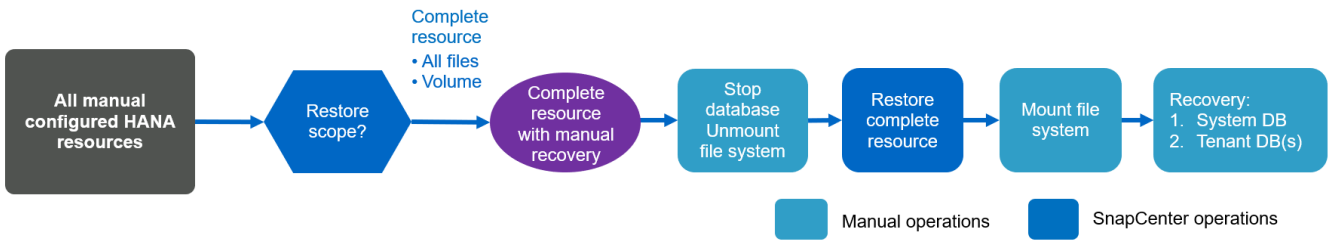
ワークフローは、前のセクションで説明したものと同じです。




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<br>• デフォルト（すべてのファイル）<br>• 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）<br>• 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<br>• デフォルト（すべてのファイル）<br>• 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）<br>• 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<br>• デフォルト（すべてのファイル）<br>• 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）<br>• 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）<br>• ファイルレベル（すべてのファイル）<br>• 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.*

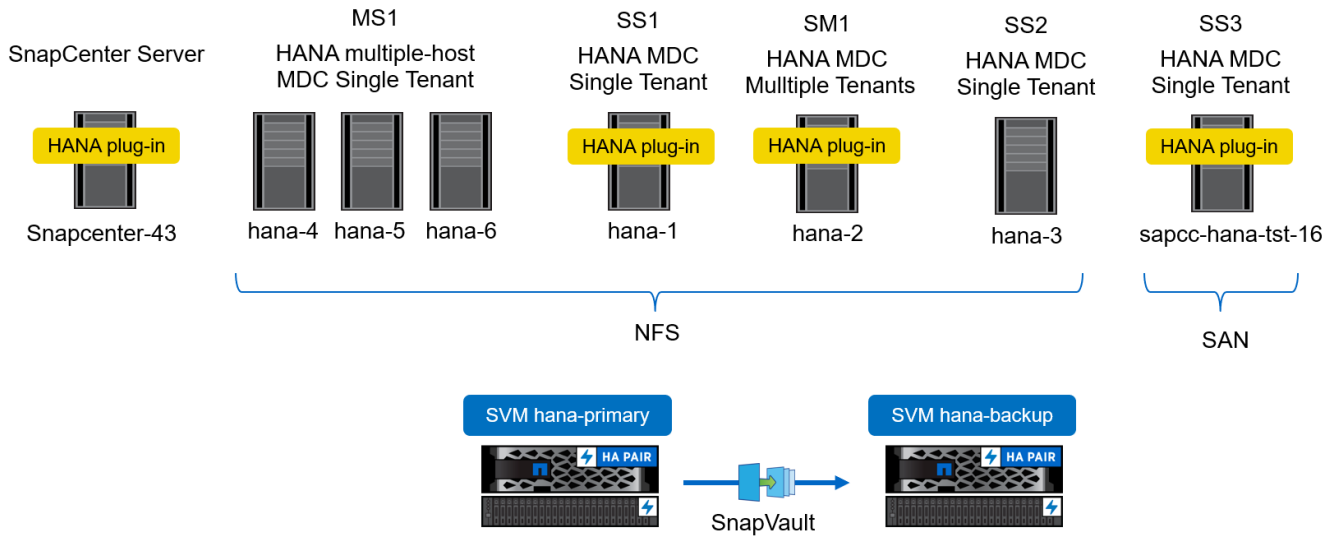
- SAP HANA シングルホスト MDC のシングルテナントシステム
- HANA プラグインが HANA データベースホストにインストールされている状態で自動検出されます
- ストレージプロトコルとして NFS を使用します

- * 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。

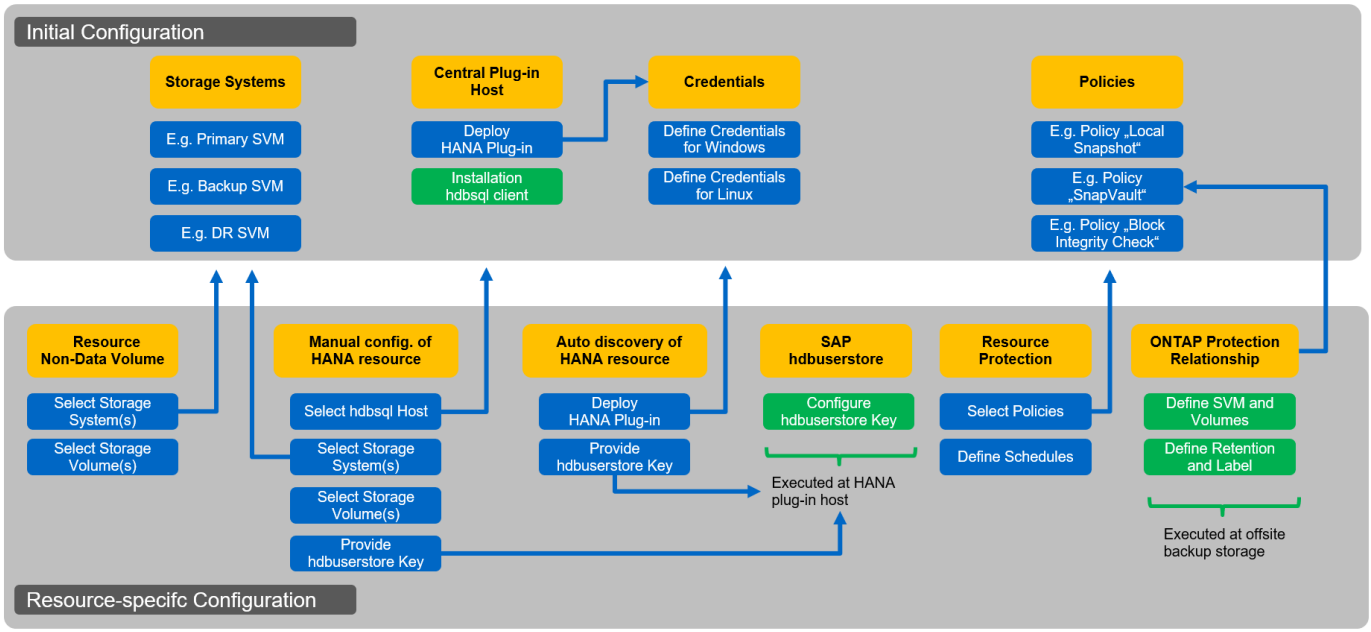


## SnapCenter 構成

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

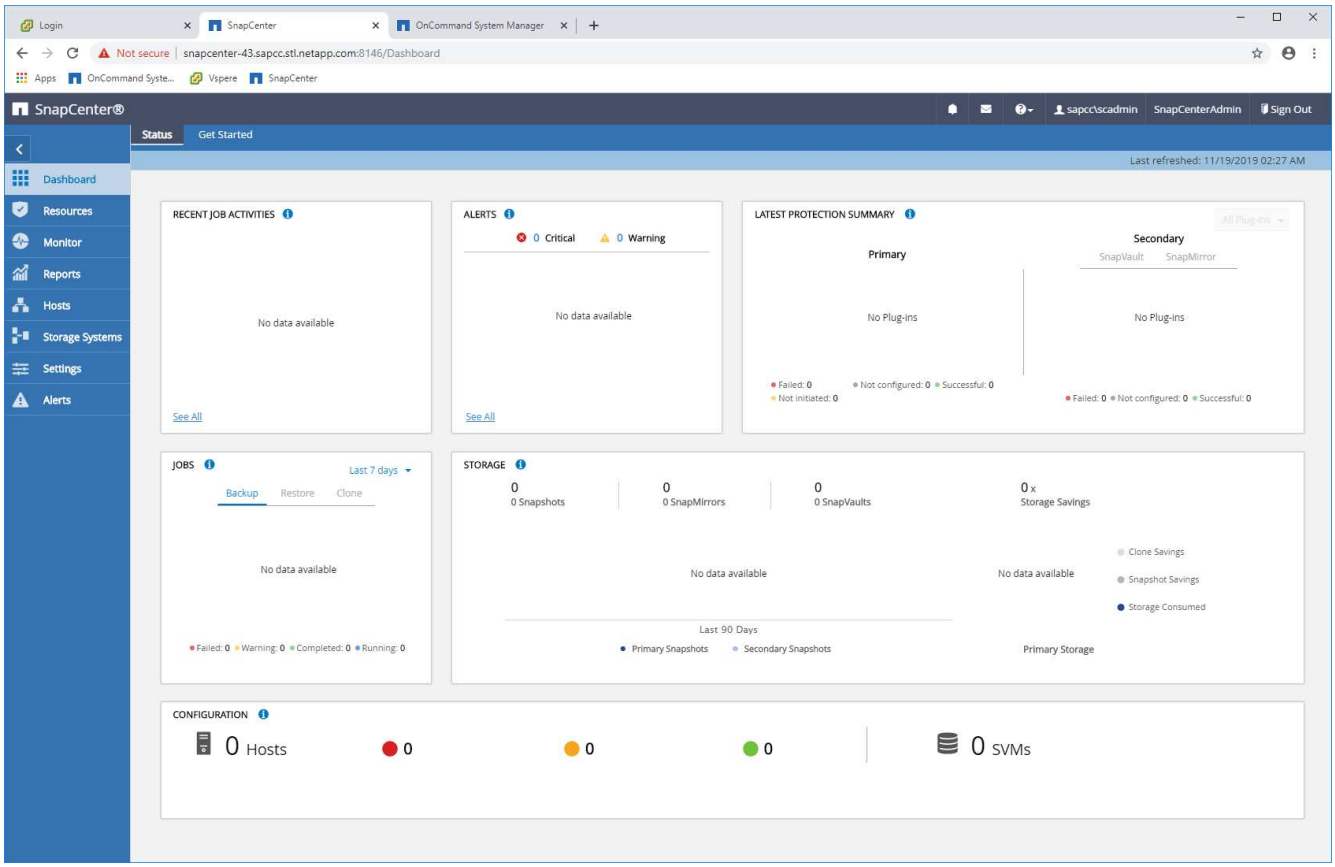
初期設定には、次の手順が含まれます。

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。

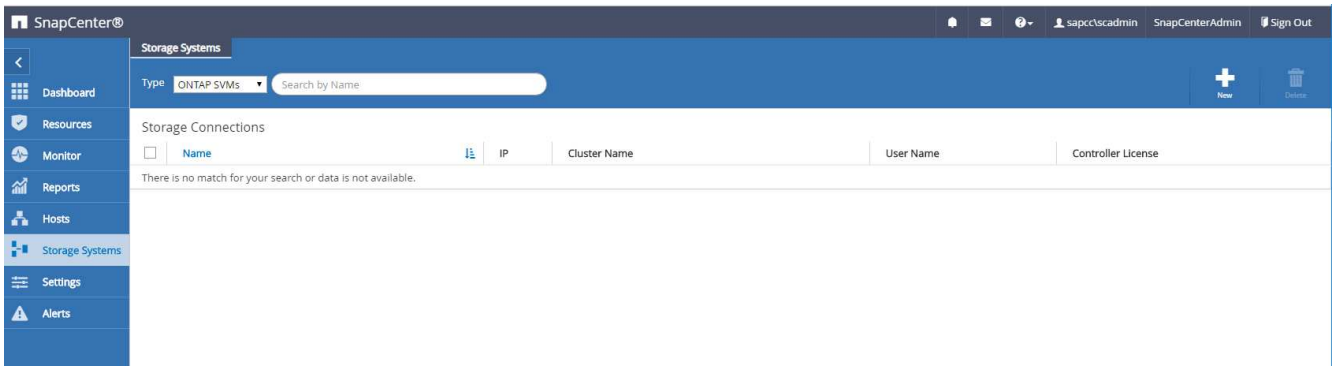
ストレージシステムの構成：

1. SnapCenter サーバ GUI にログインします。



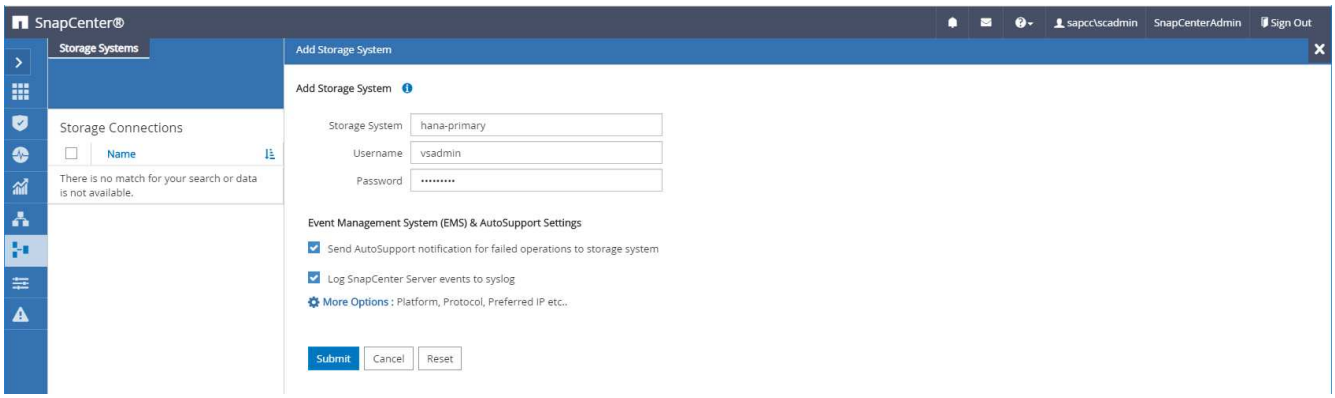

2. [ ストレージシステム ] を選択します。

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。

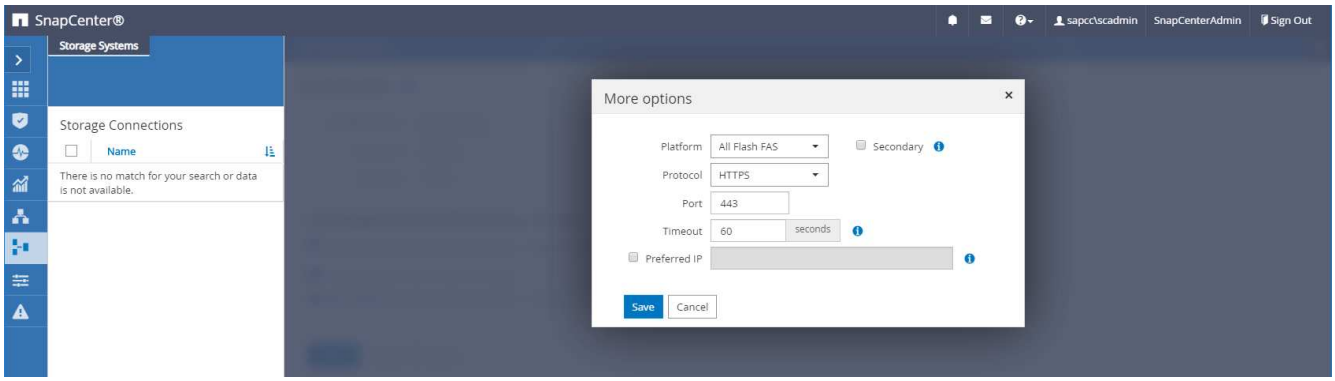
スクリーンショットに示されているように、 SVM ユーザを vsadmin ユーザにする必要はありません。通常、ユーザは SVM 上で設定し、バックアップとリストアの処理を実行するために必要な権限を割り当てます。必要な権限の詳細については、を参照してください "SnapCenter インストールガイド" 「 Minimum ONTAP Privileges Required 」の項を参照してください。



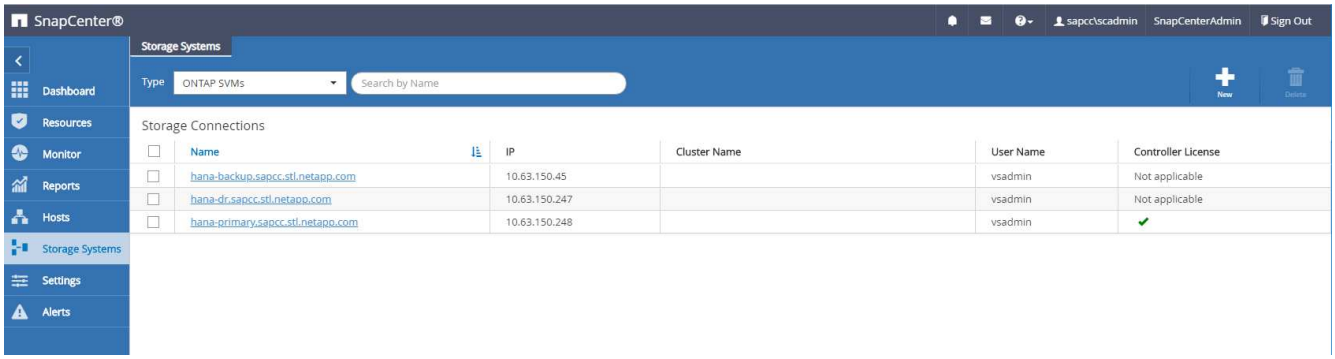

4. [ その他のオプション ] をクリックして、ストレージプラットフォームを構成します。

   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。

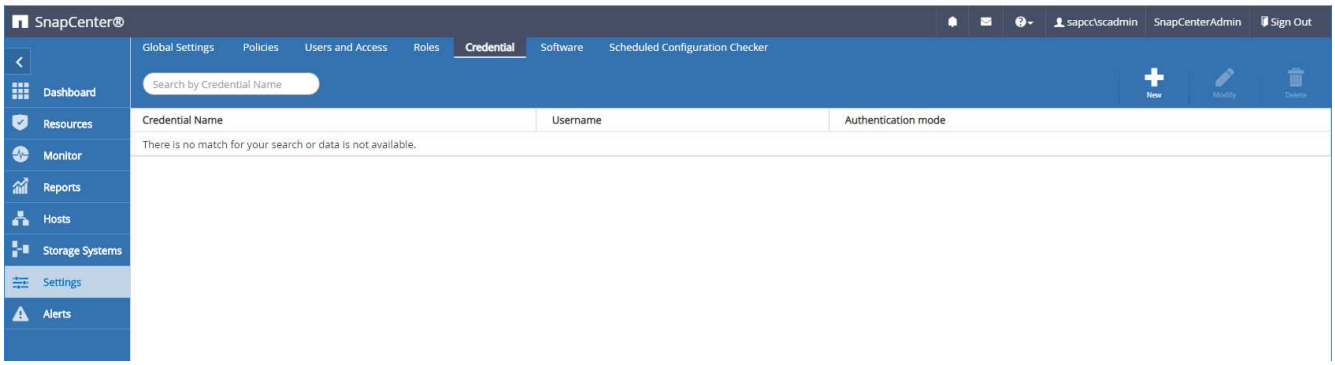



5. 必要に応じてストレージシステムを追加この例では、追加のオフサイトバックアップストレージとディザスタリカバリ用ストレージが追加されています。

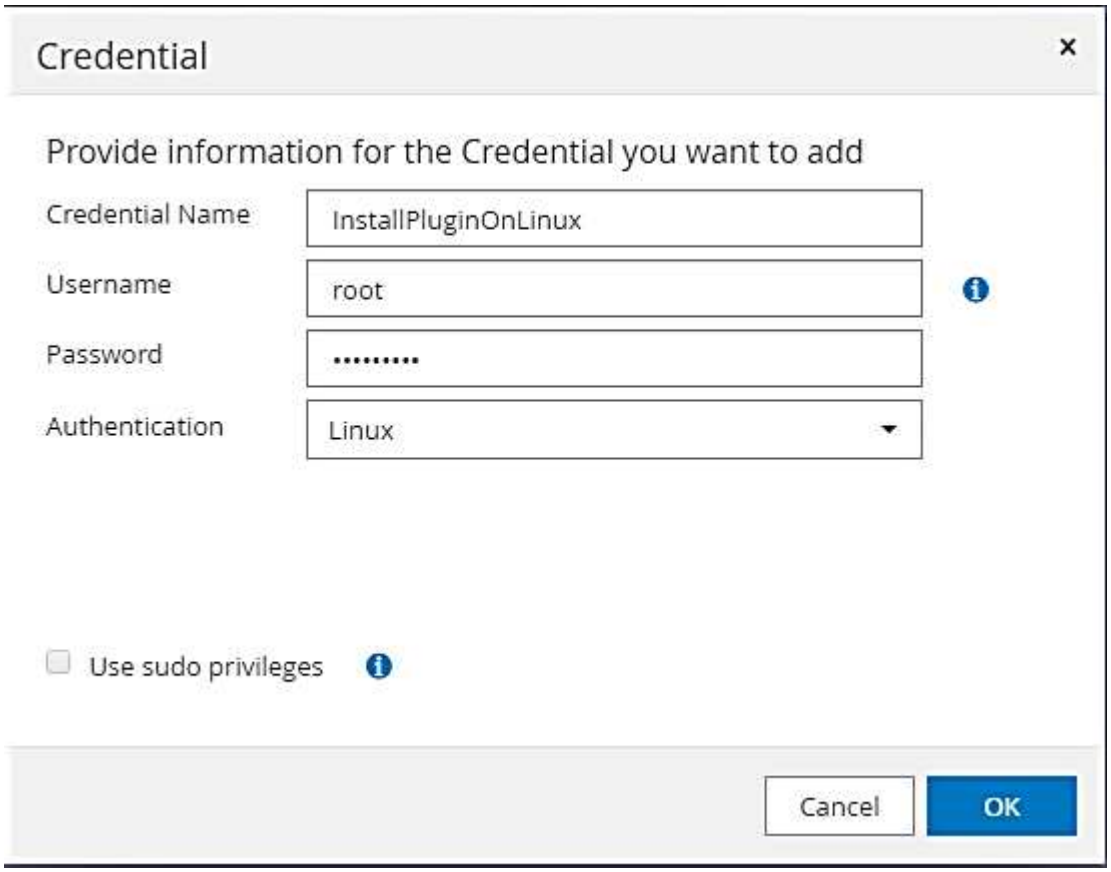



クレデンシャルの設定

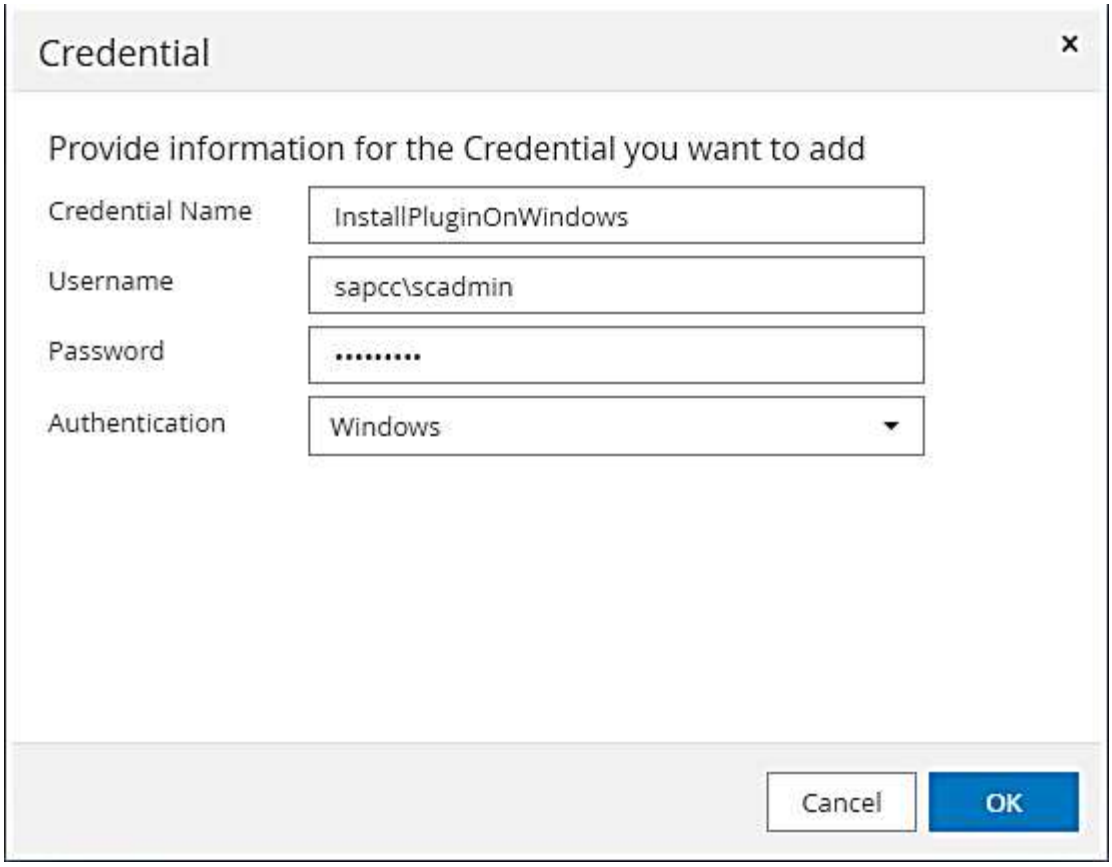
1. [ 設定 ] に移動し、 [ 資格情報 ] を選択して、 [ 新規 ] をクリックします



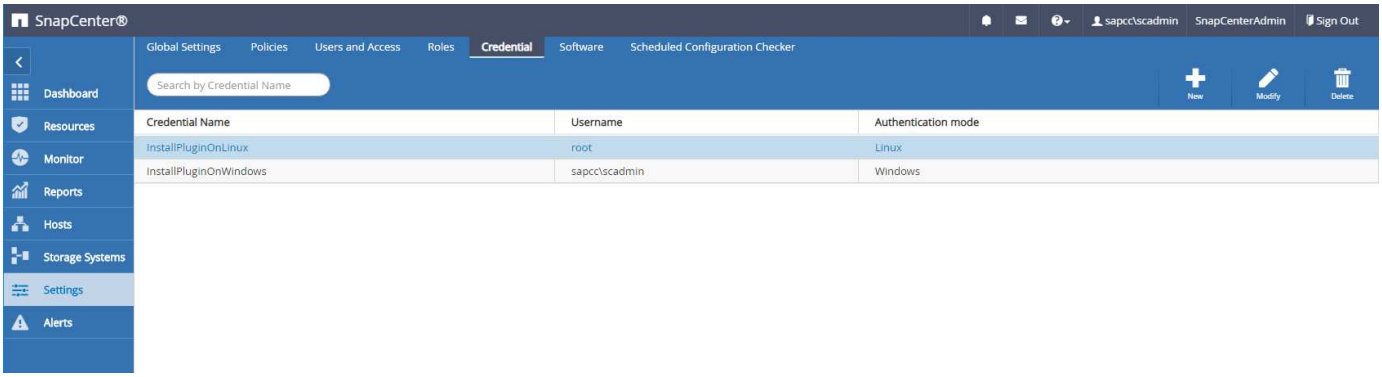

2. Linux システムへのプラグインのインストールに使用するユーザのクレデンシャルを入力します。




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。

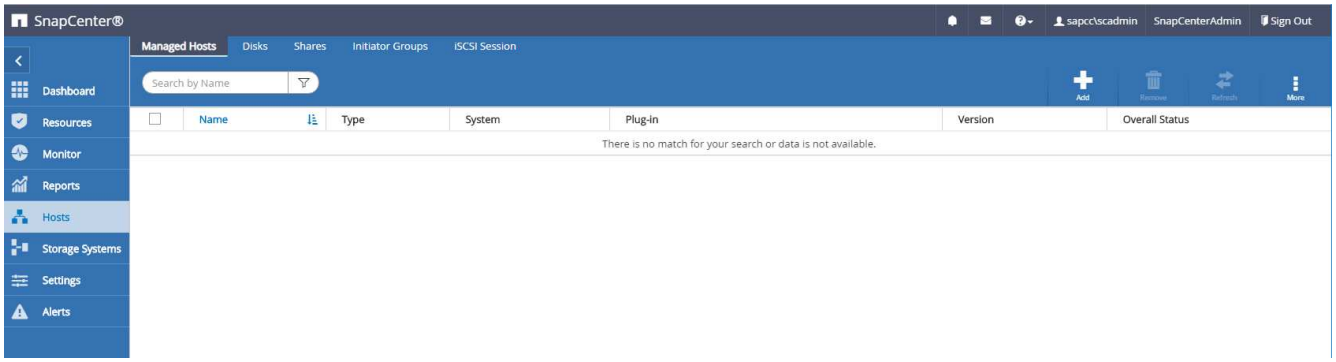



中央のプラグインホストへの **SAP HANA** プラグインのインストール

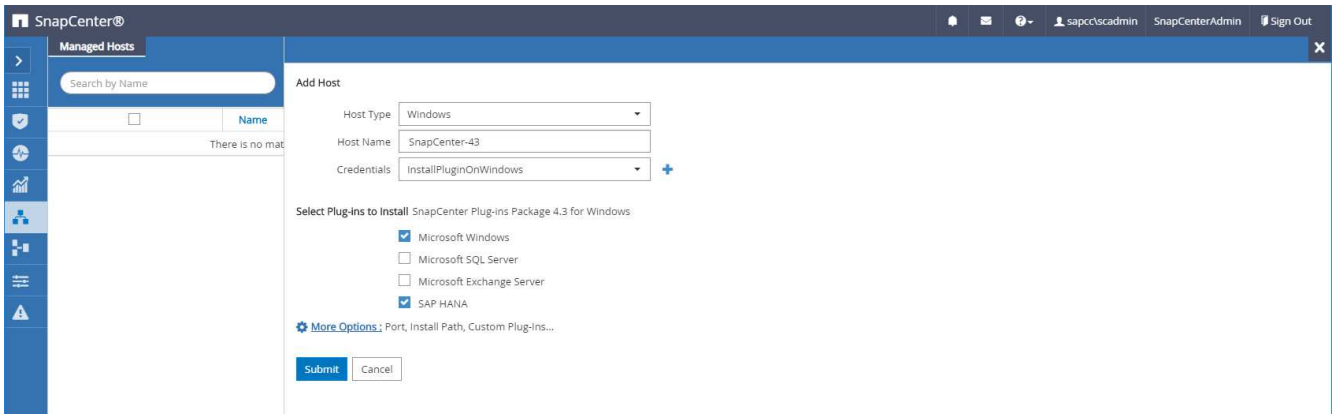
ラボのセットアップでは、 SnapCenter サーバは中央の HANA プラグインホストとしても使用されます。SnapCenter サーバを実行する Windows ホストがホストとして追加され、 SAP HANA プラグインが Windows ホストにインストールされます。

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。

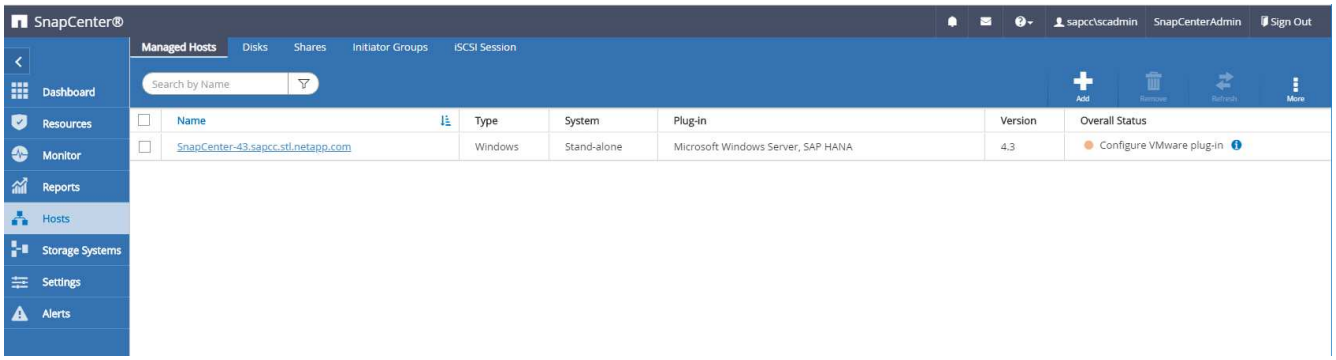
1. Hosts に移動し、 Add をクリックします。




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

セクションで説明したように、"「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。

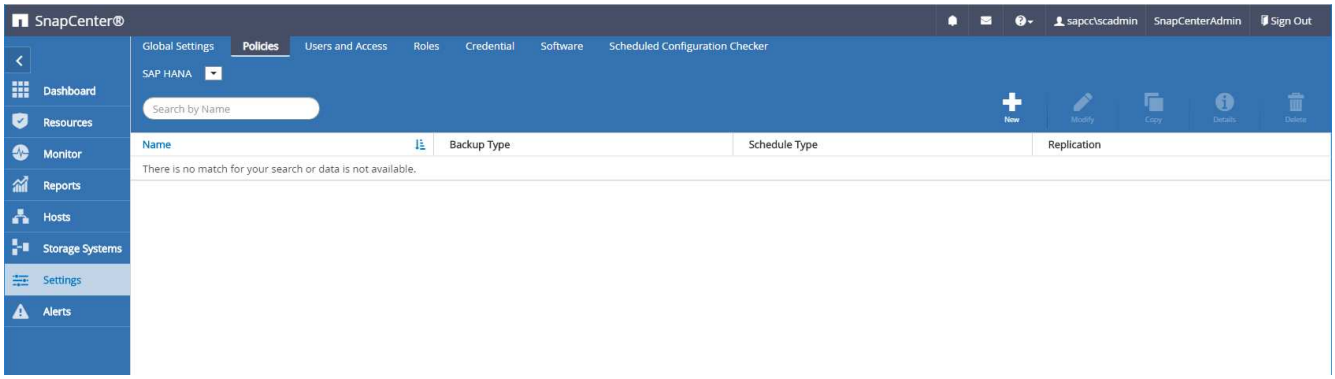
一般的な最小構成は、次のポリシーで構成されます。

- 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

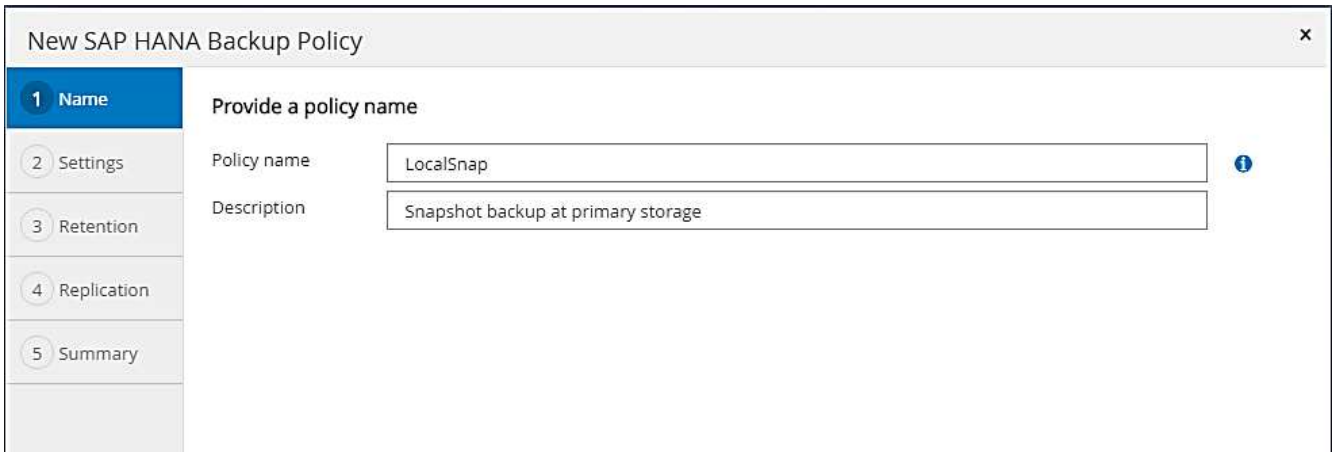
以降のセクションでは、これら 3 つのポリシーの設定について説明します。

#### 1 時間ごとの **Snapshot** バックアップのポリシー

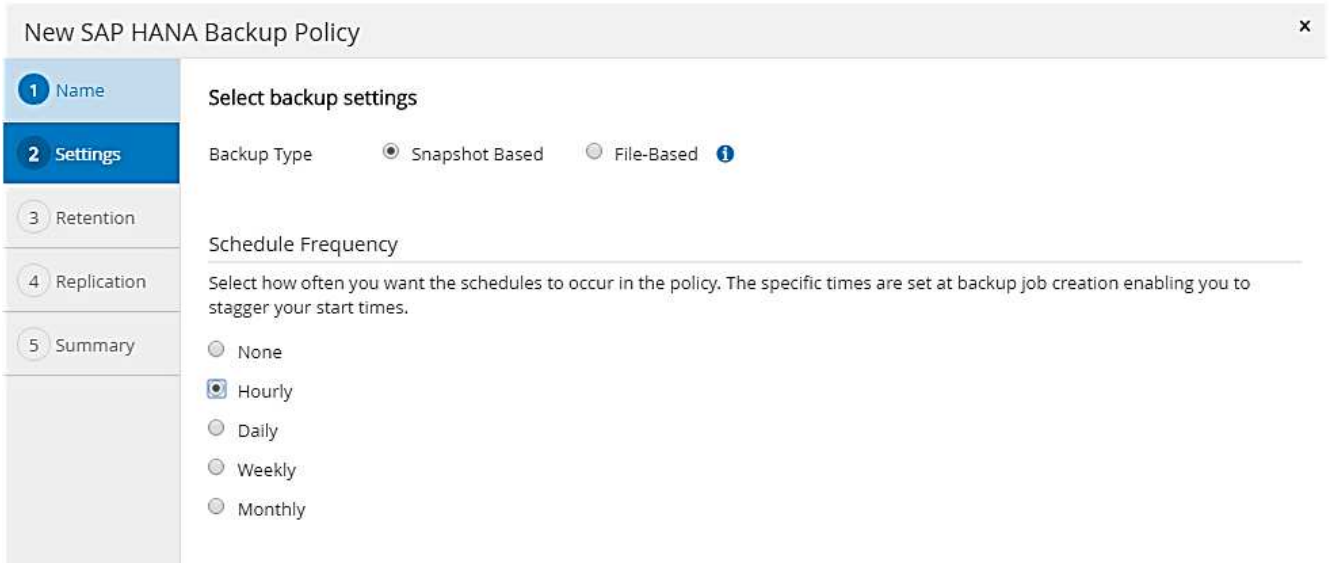
1. [ 設定 ] 、 [ ポリシー ] の順に移動し、 [ 新規 ] をクリックします



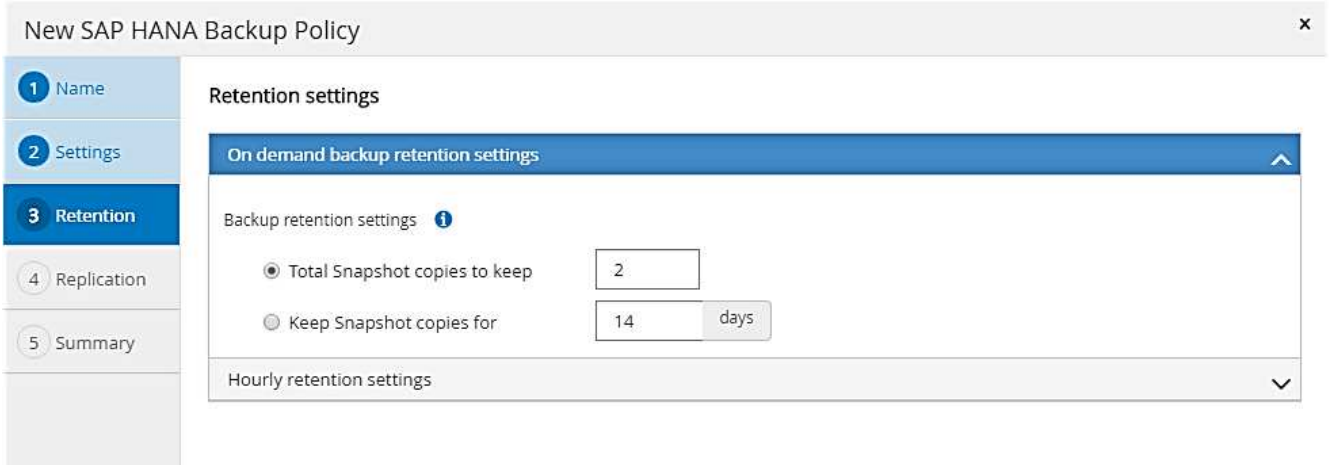

2. ポリシー名と概要を入力します。次へをクリックします。



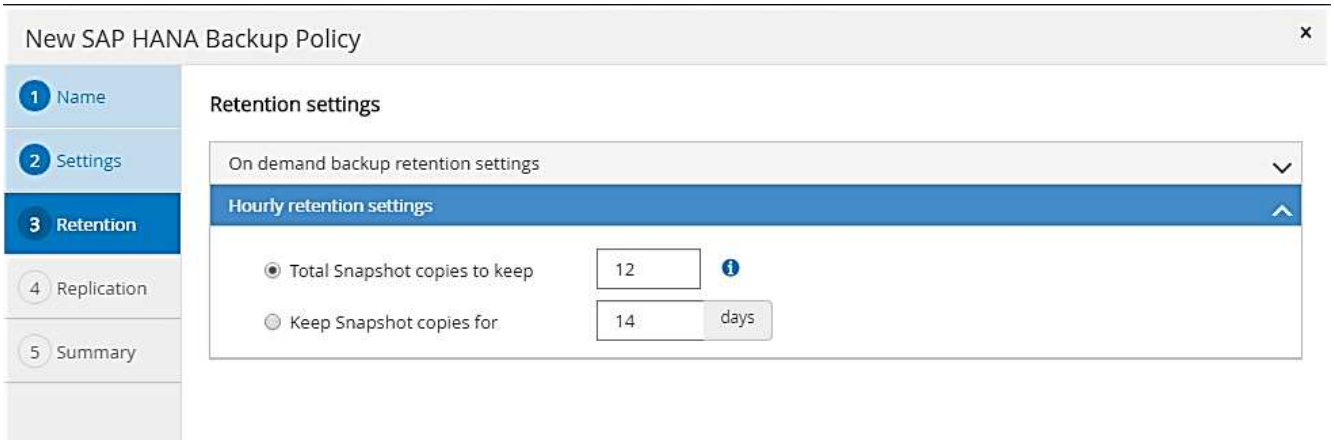

3. バックアップタイプとして「 Snapshot Based 」を選択し、スケジュール頻度を選択するには「 Hourly 」を選択します。



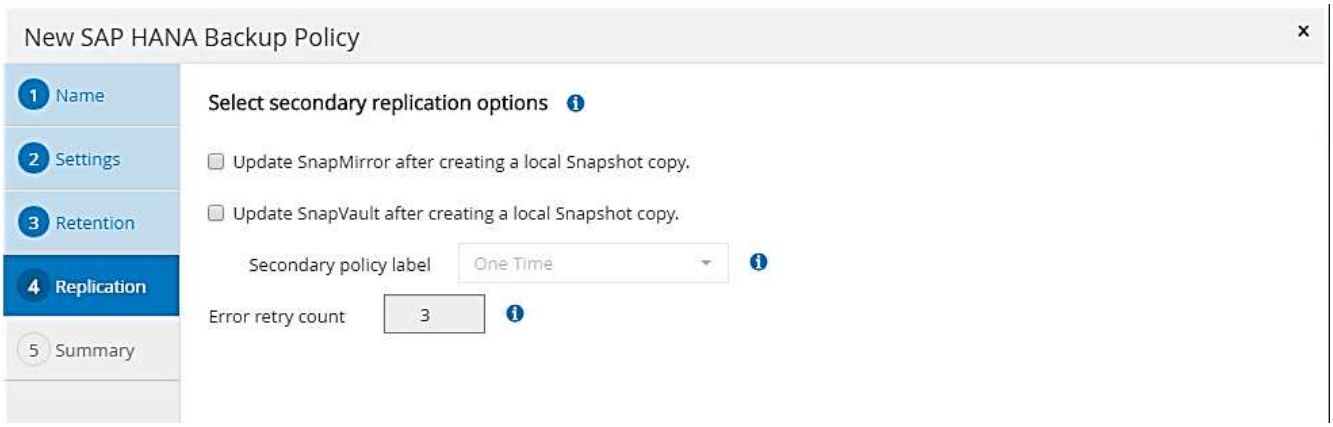

4. オンデマンドバックアップの保持を設定します。



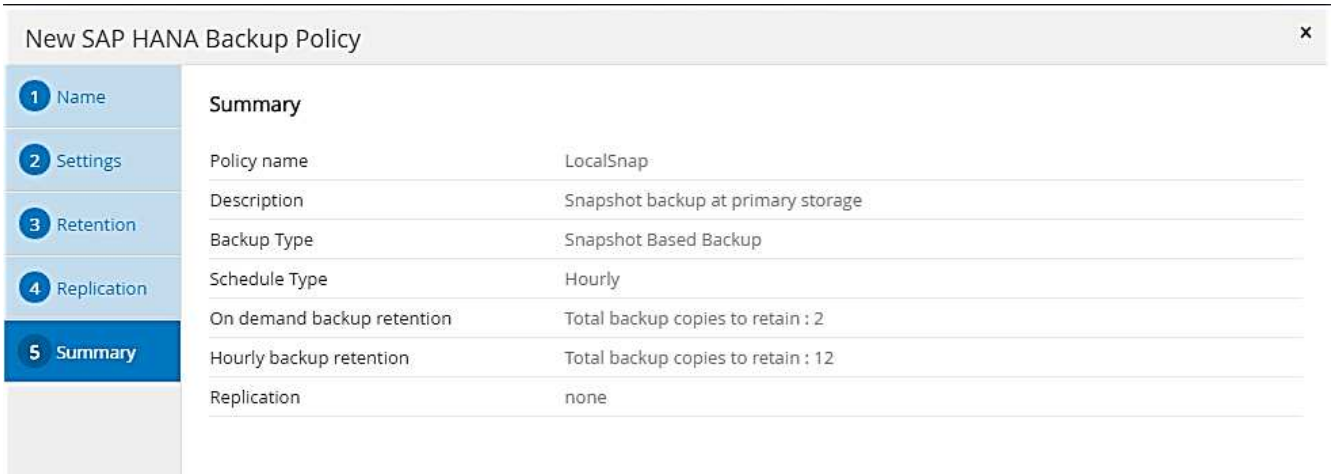

5. スケジュールされたバックアップの保持を設定します。




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。

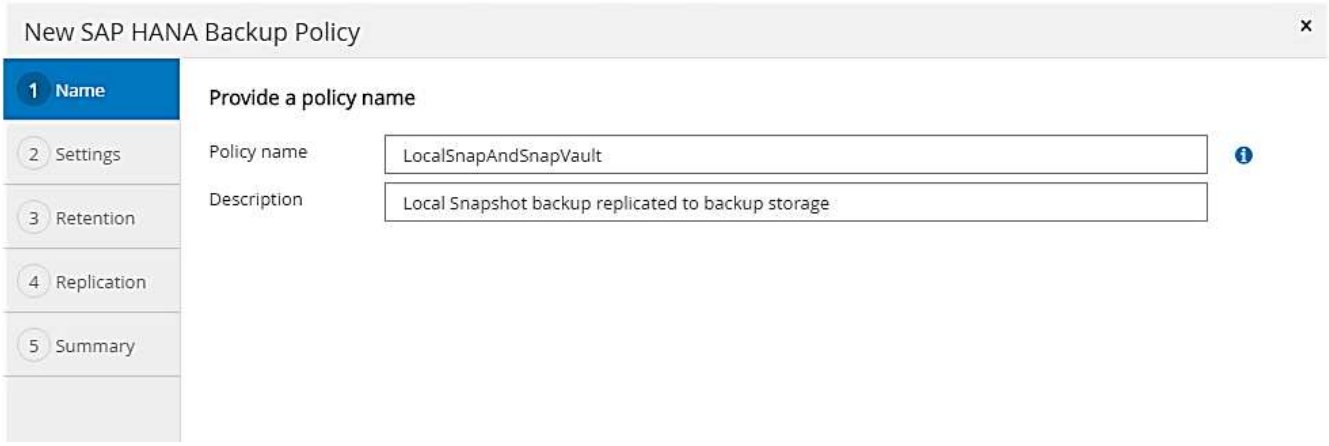



7. [ 概要 ] ページで、 [ 完了 ] をクリックします。

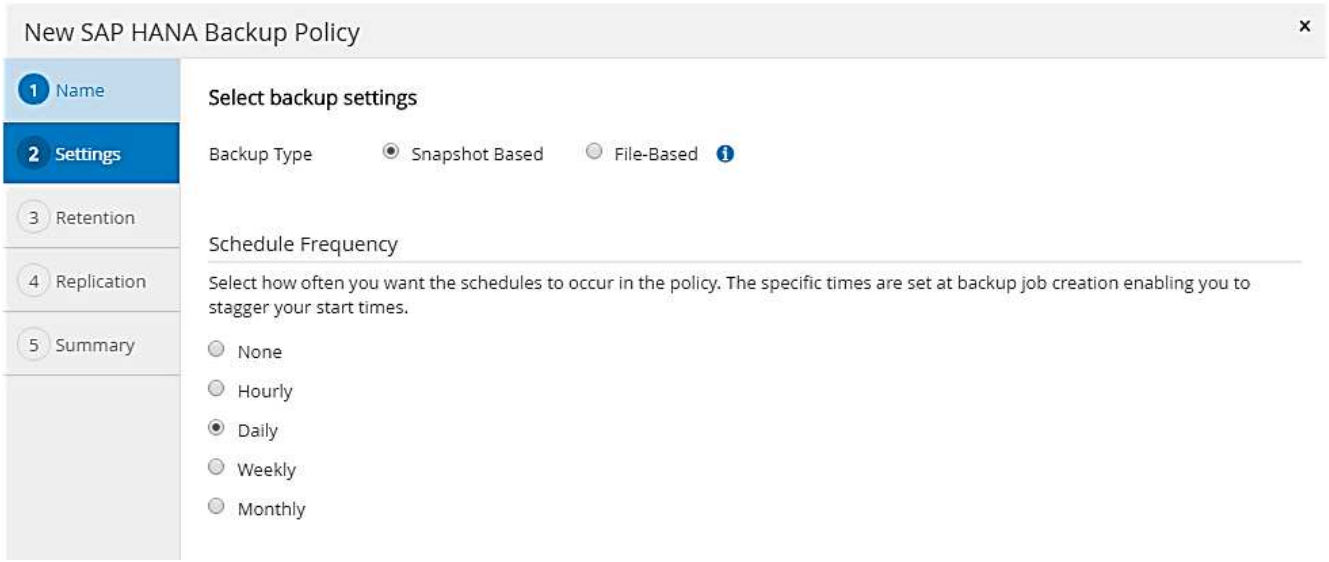



**SnapVault** レプリケーションを行う日次 **Snapshot** バックアップのポリシー

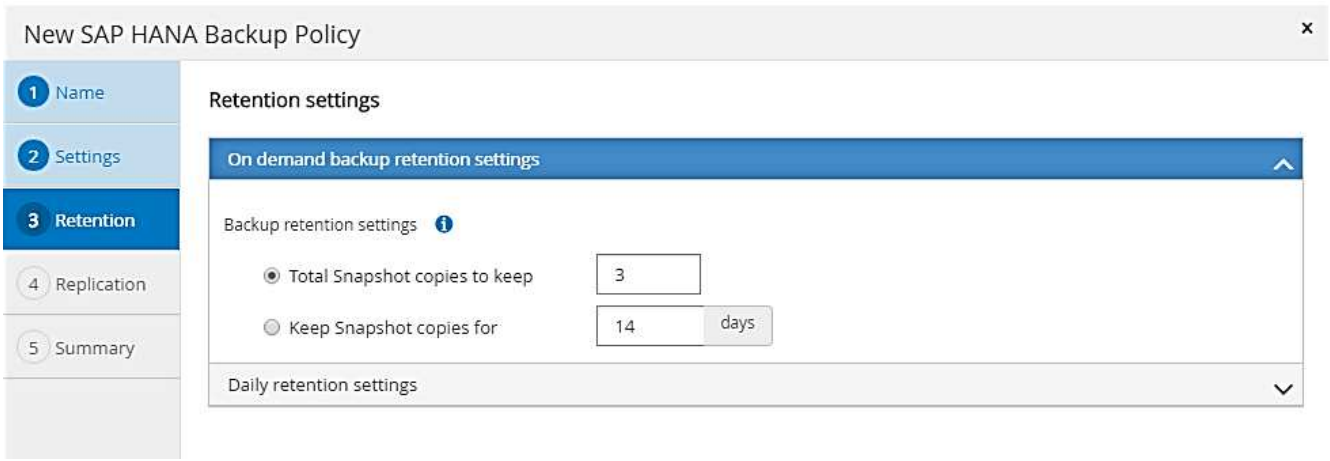
1. [ 設定 ] 、 [ ポリシー ] の順に移動し、 [ 新規 ] をクリックします
2. ポリシー名と概要を入力します。次へをクリックします。



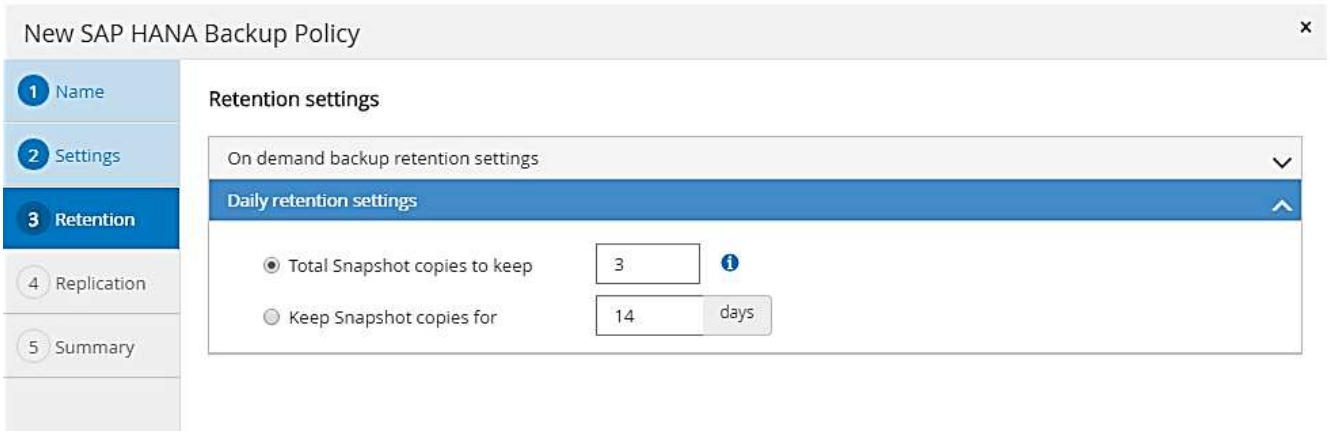

3. バックアップタイプを Snapshot ベースに、スケジュール頻度を「毎日」に設定します。




4. オンデマンドバックアップの保持を設定します。

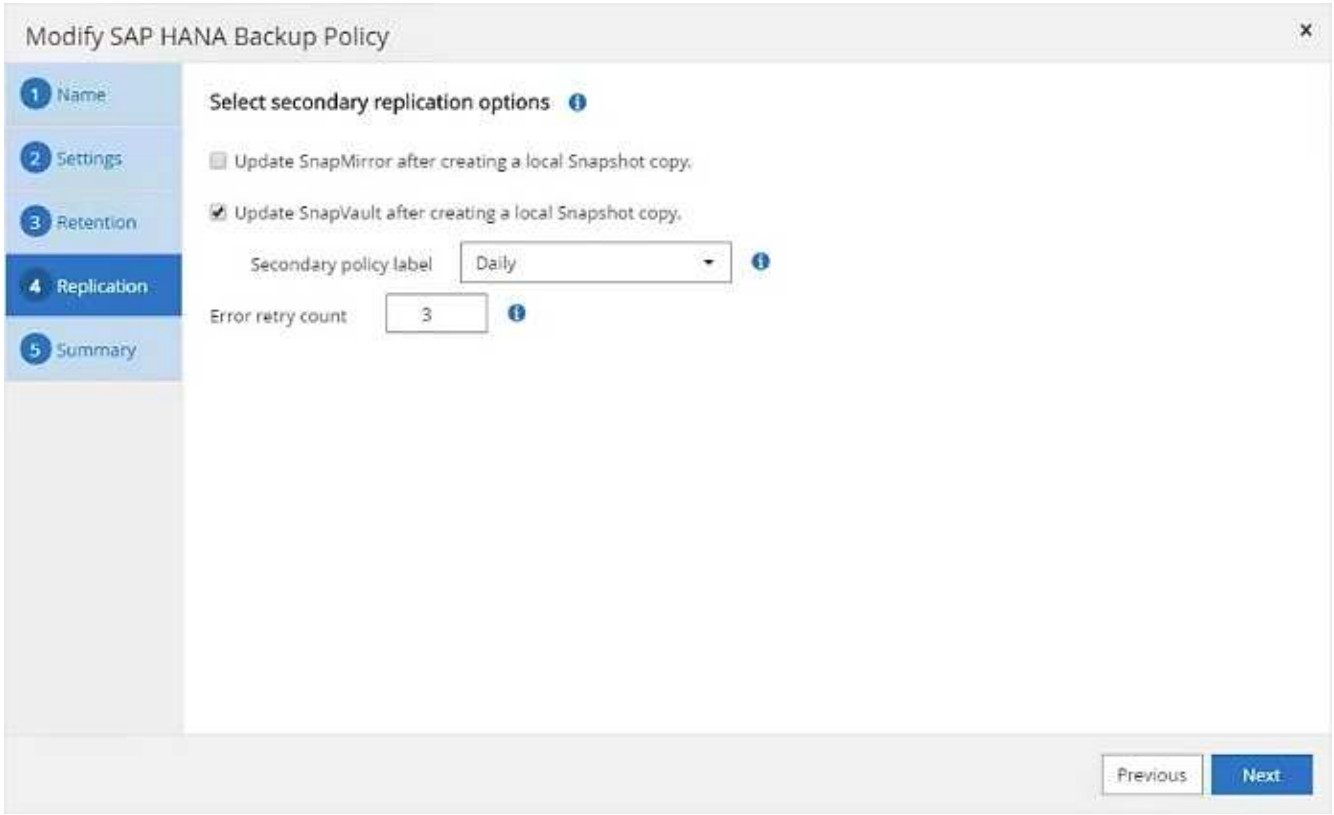



5. スケジュールされたバックアップの保持を設定します。

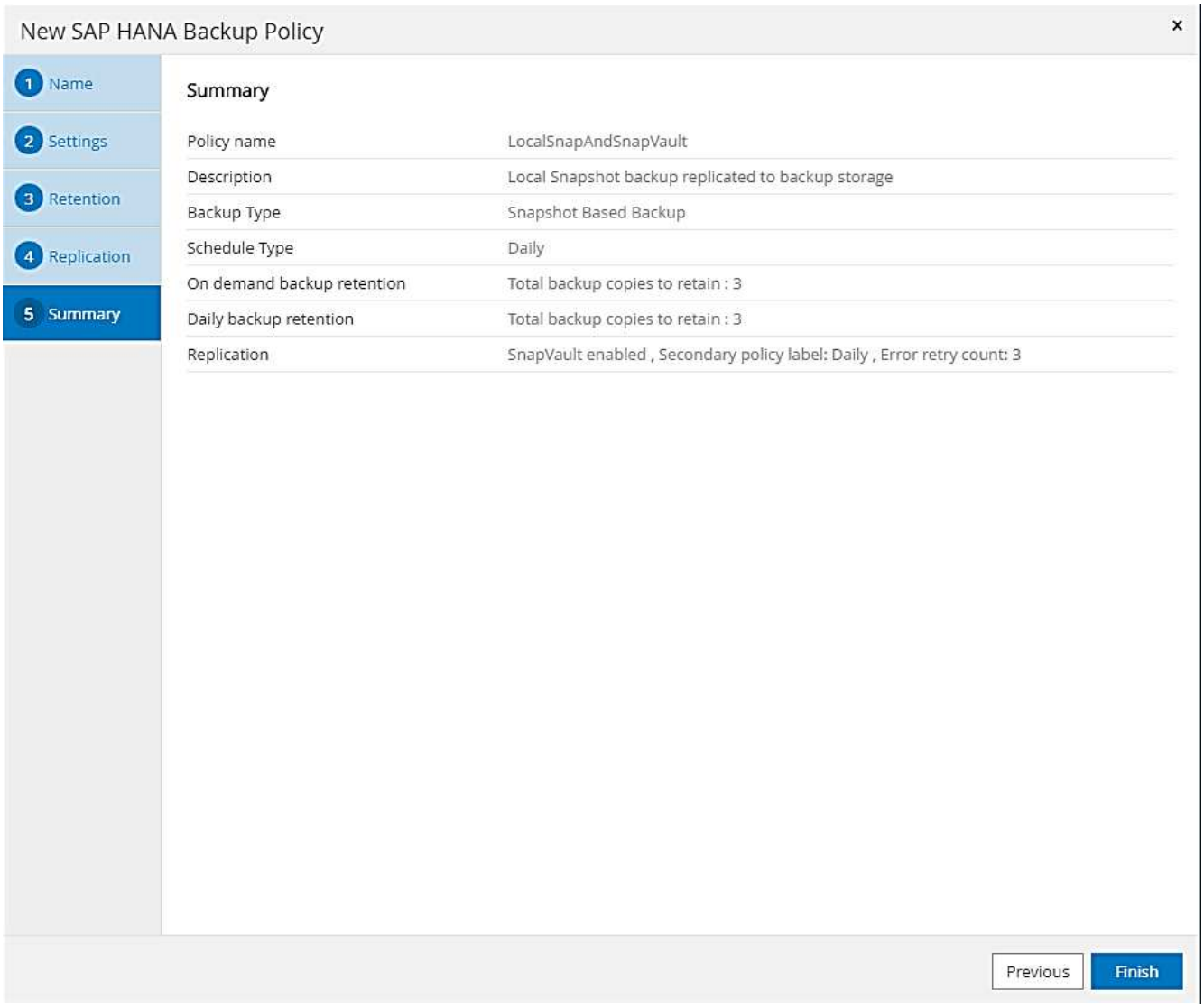



6. ローカル Snapshot コピーの作成後に SnapVault を更新するを選択します。

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」"

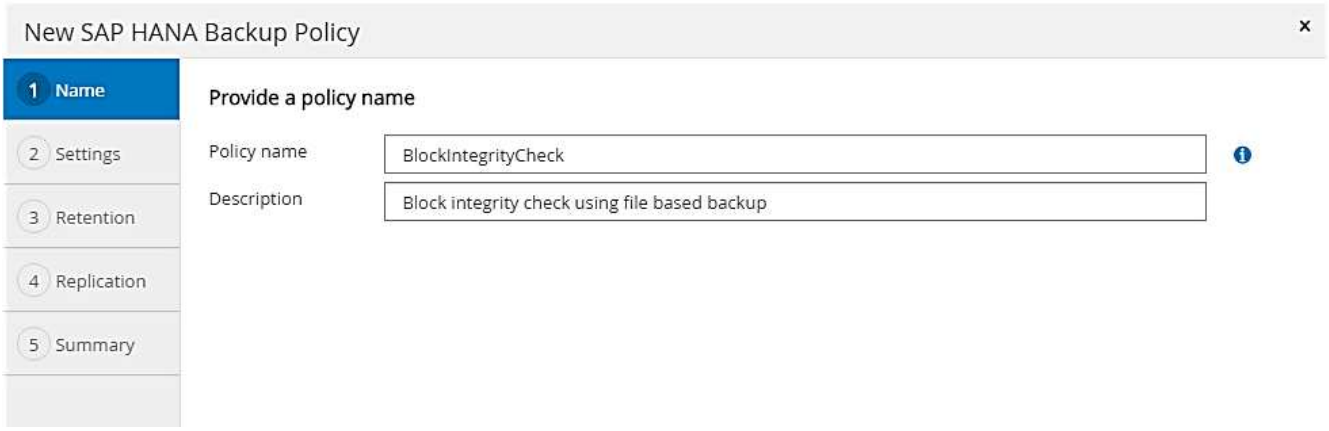



7. [ 概要 ] ページで、 [ 完了 ] をクリックします。

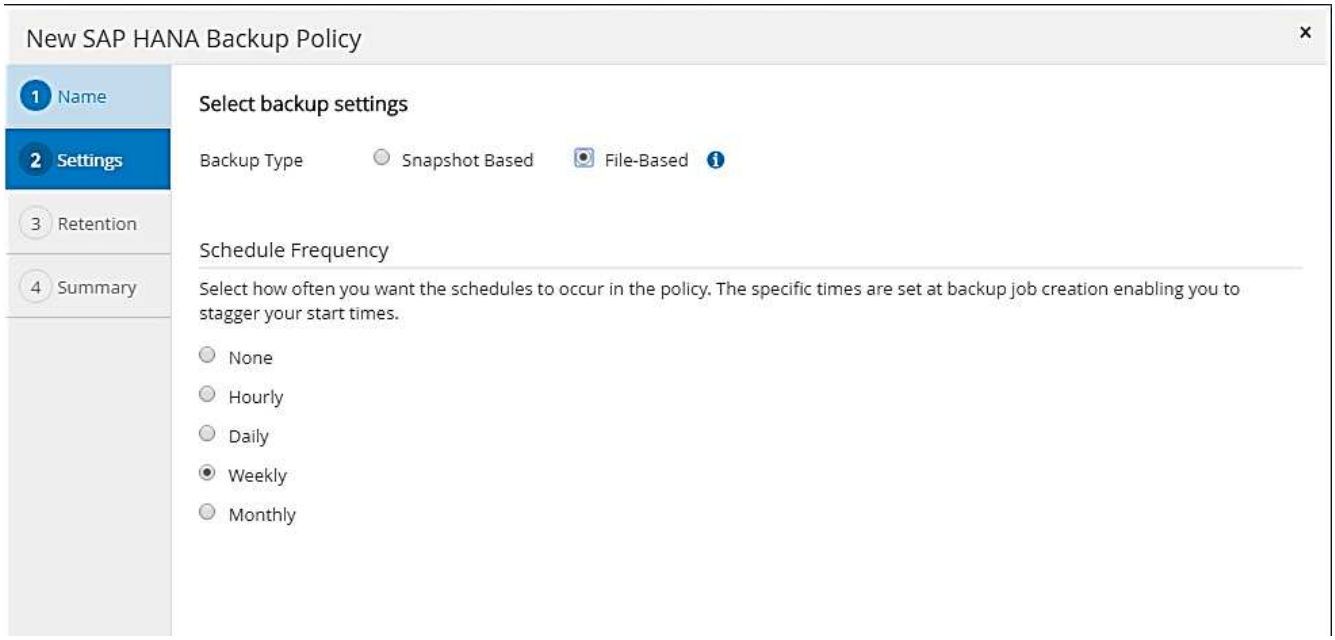



週次ブロック整合性チェックのポリシー

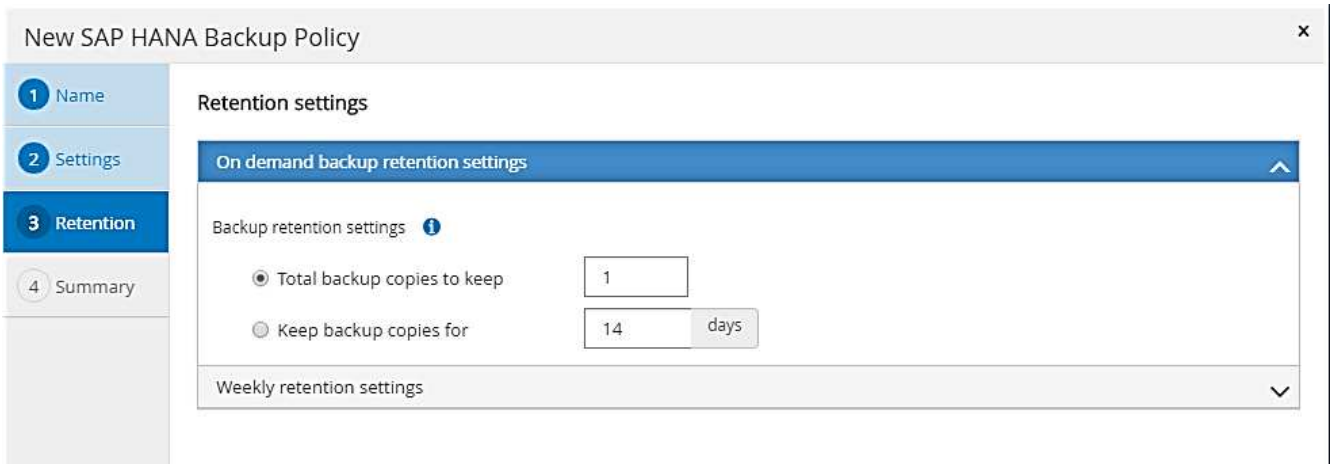
1. [ 設定 ] 、 [ ポリシー ] の順に移動し、 [ 新規 ] をクリックします
2. ポリシー名と概要を入力します。次へをクリックします。



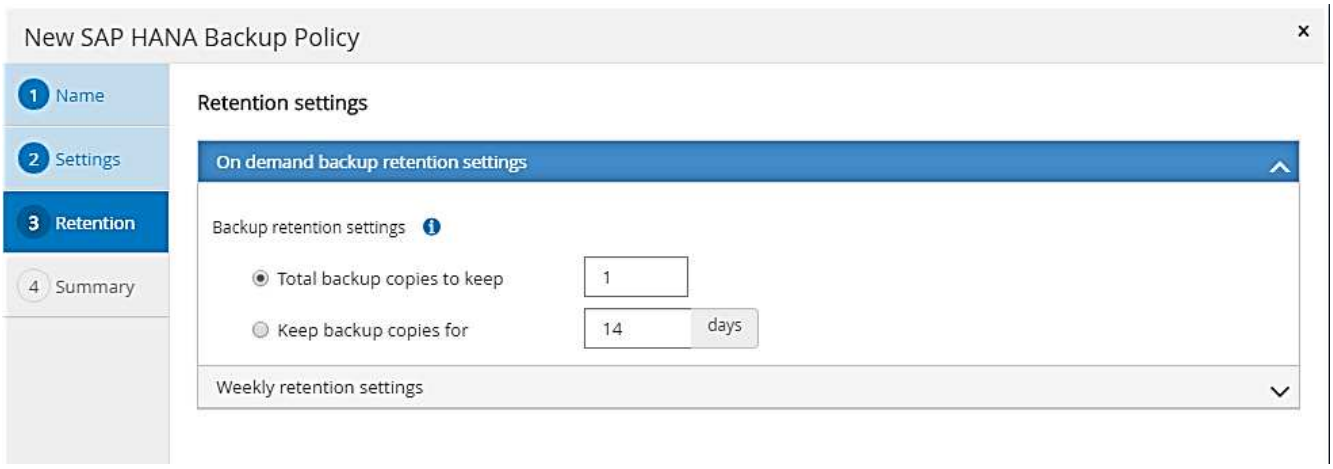

3. バックアップタイプを「ファイルベース」に、スケジュール頻度を「毎週」に設定します。



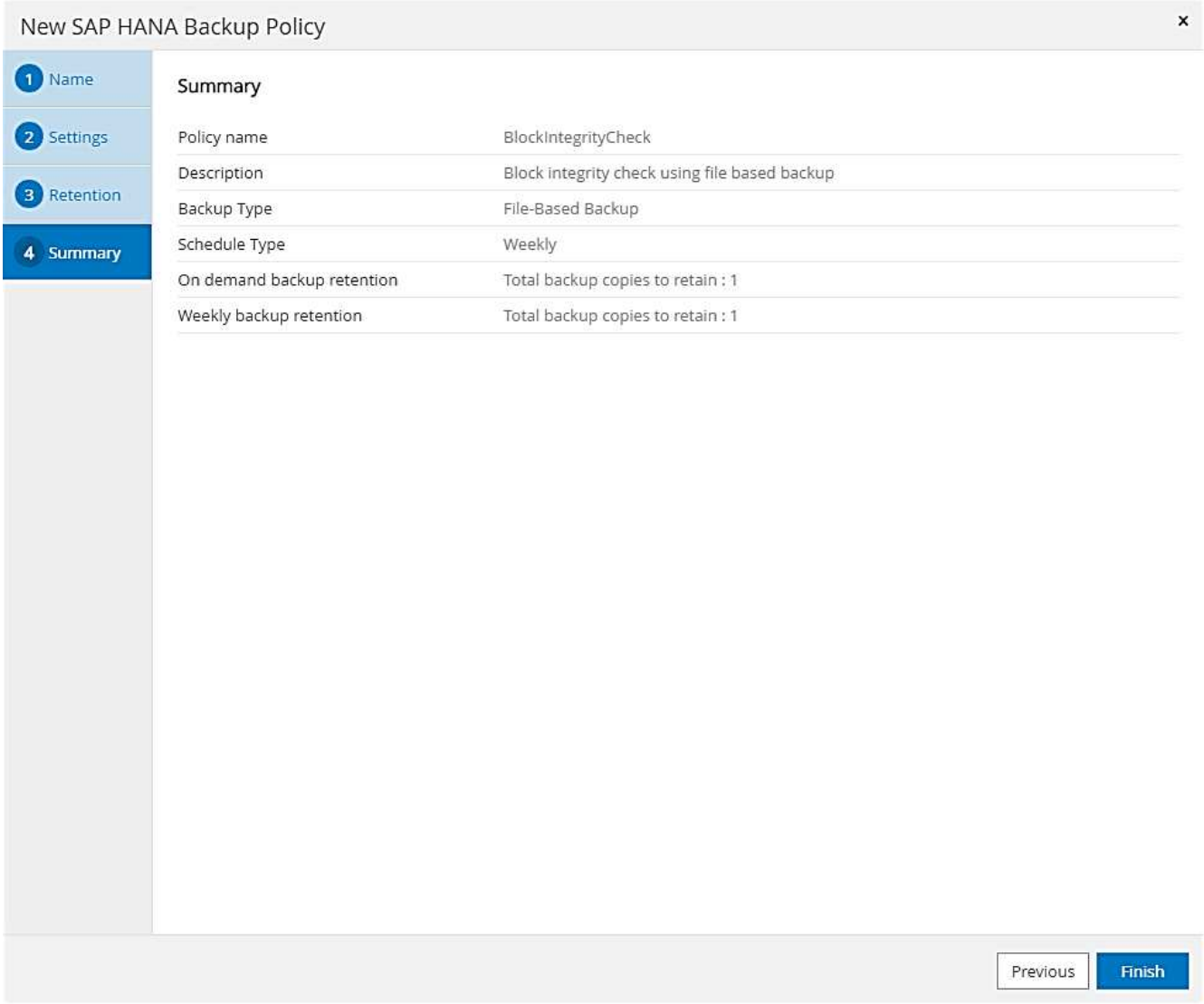

4. オンデマンドバックアップの保持を設定します。



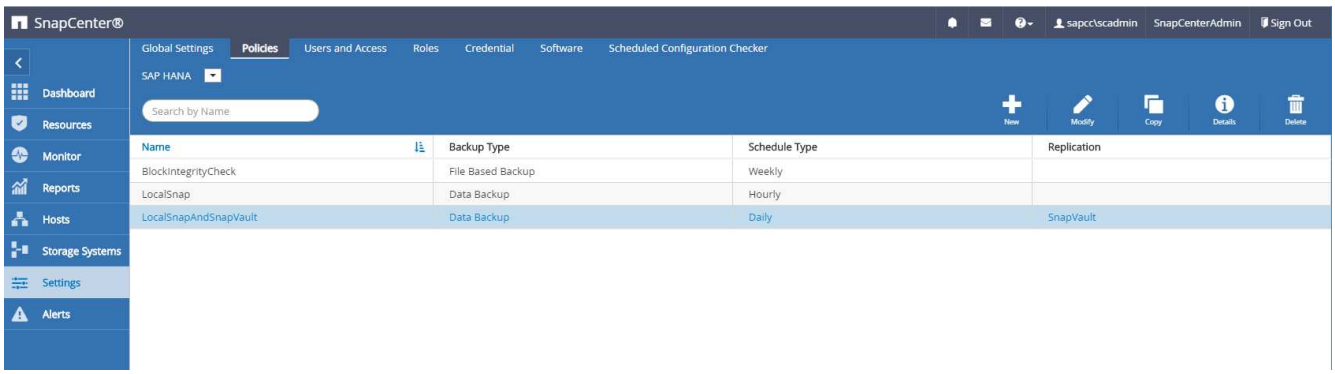

5. スケジュールされたバックアップの保持を設定します。




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。

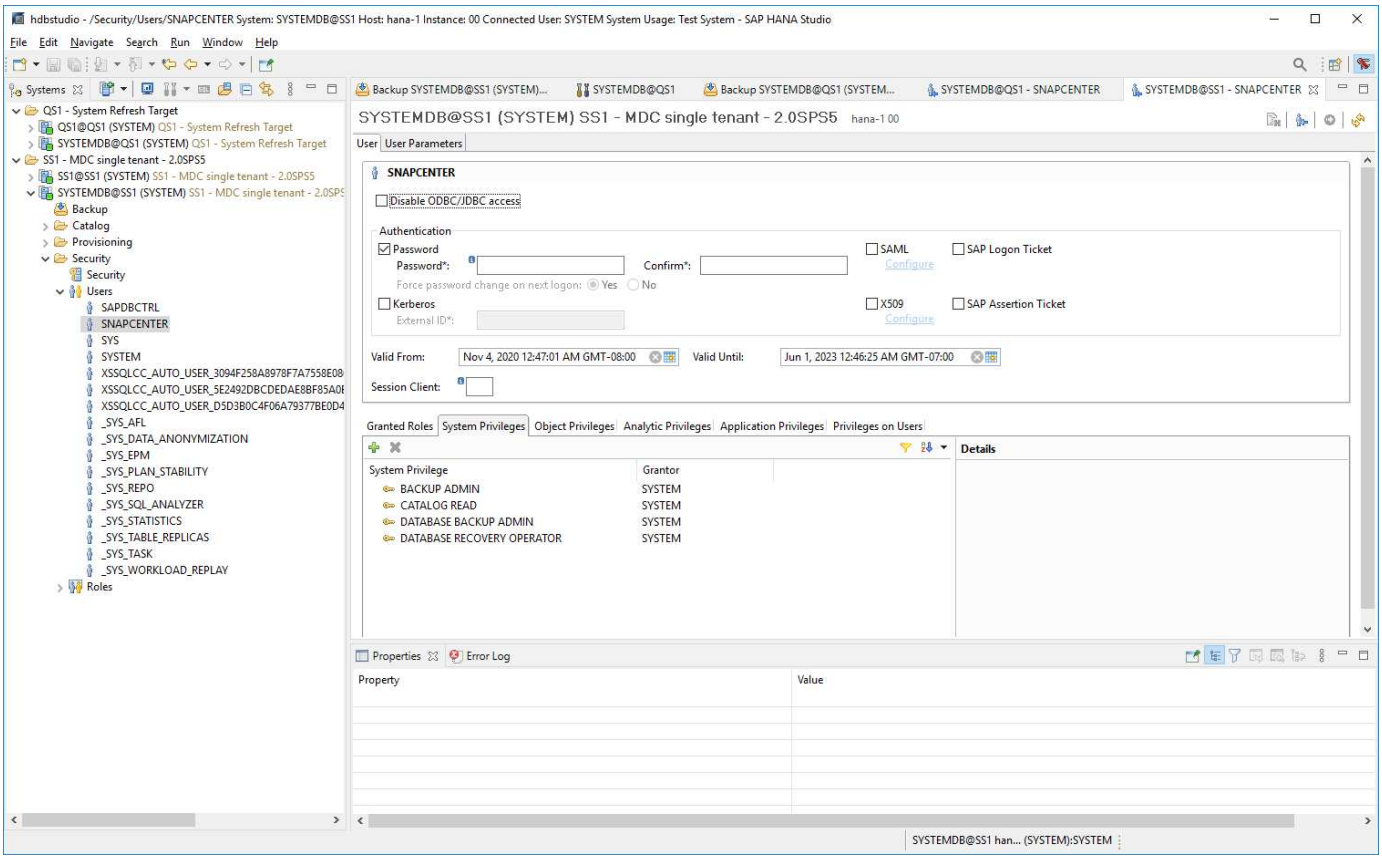
### **SAP HANA** のバックアップユーザと **hdbuserstore** の設定を指定します

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。

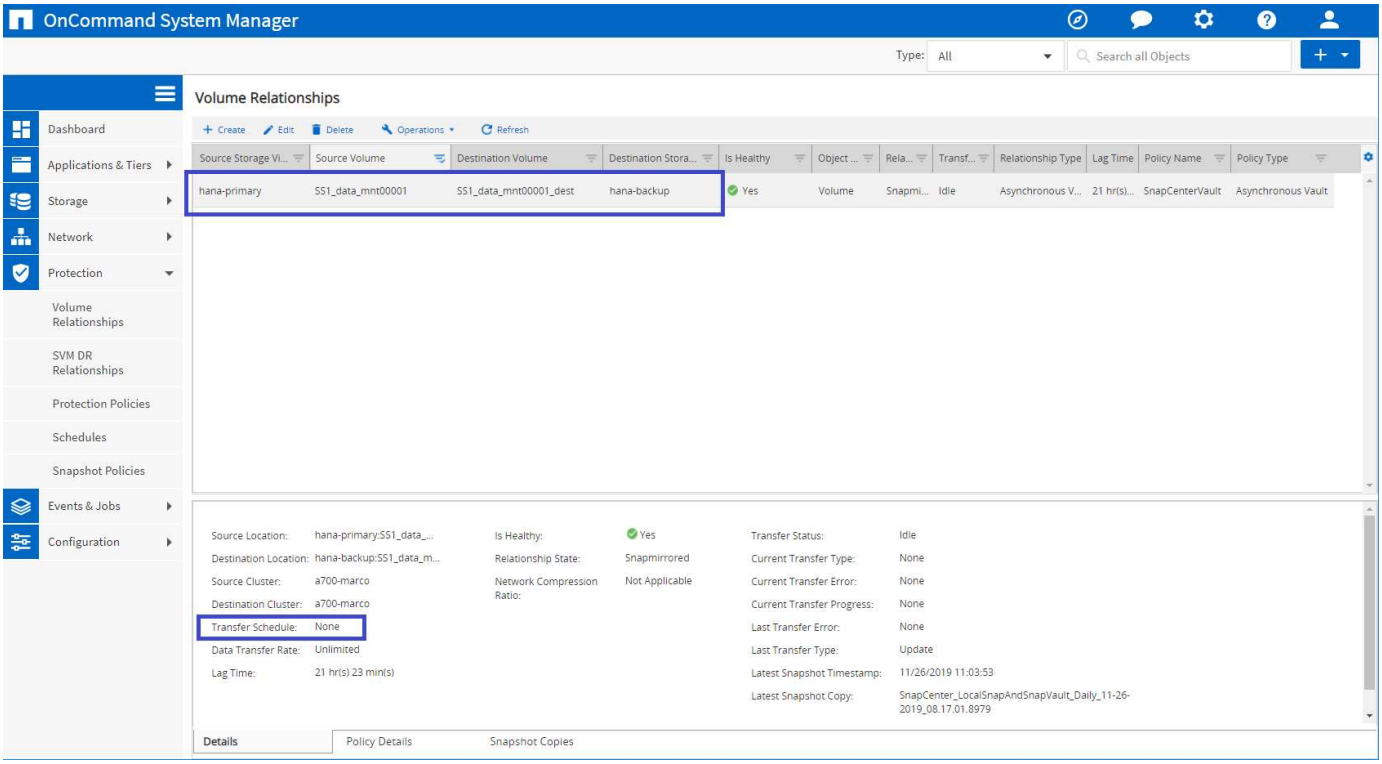
```
hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER
password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE       : 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。

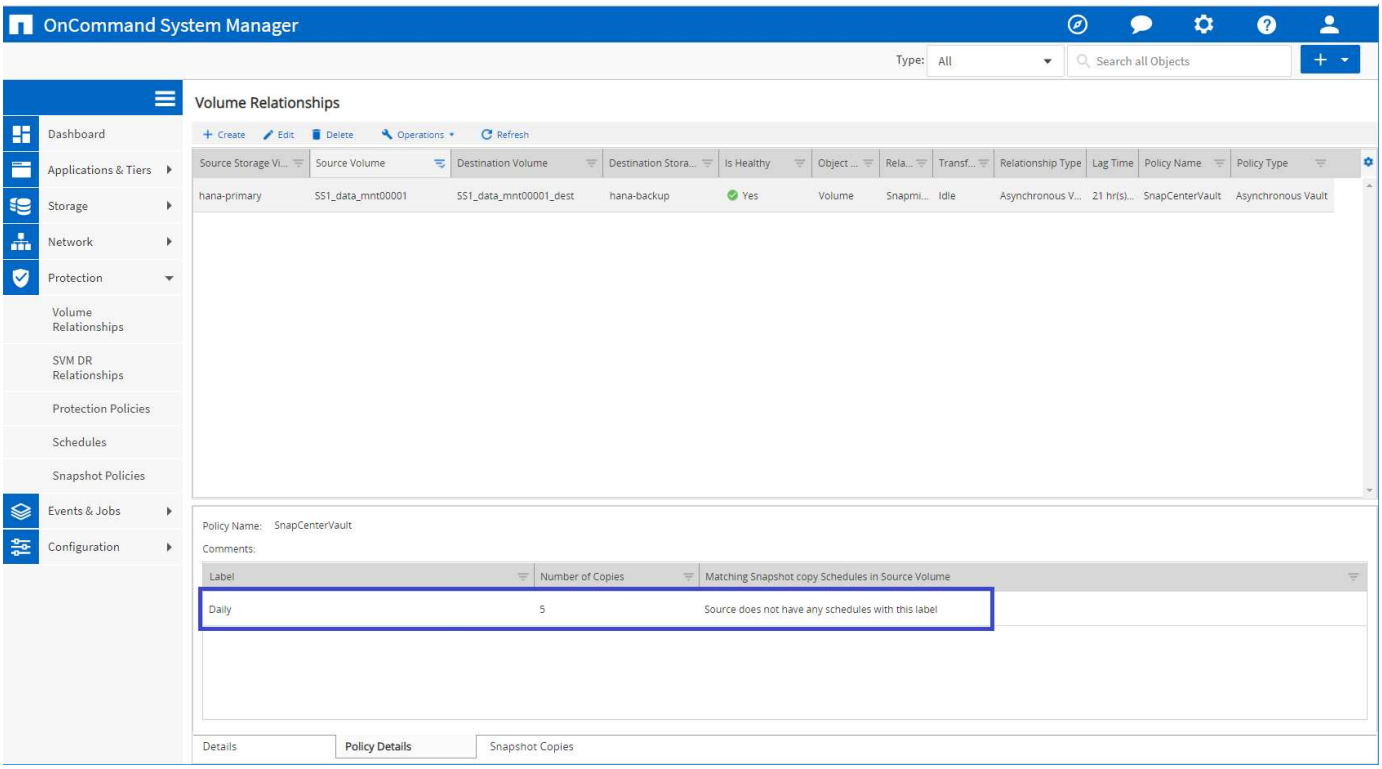
SnapCenter によって SnapVault の更新がトリガーされるため、関係のスケジュールは None に設定する必要があります。




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。

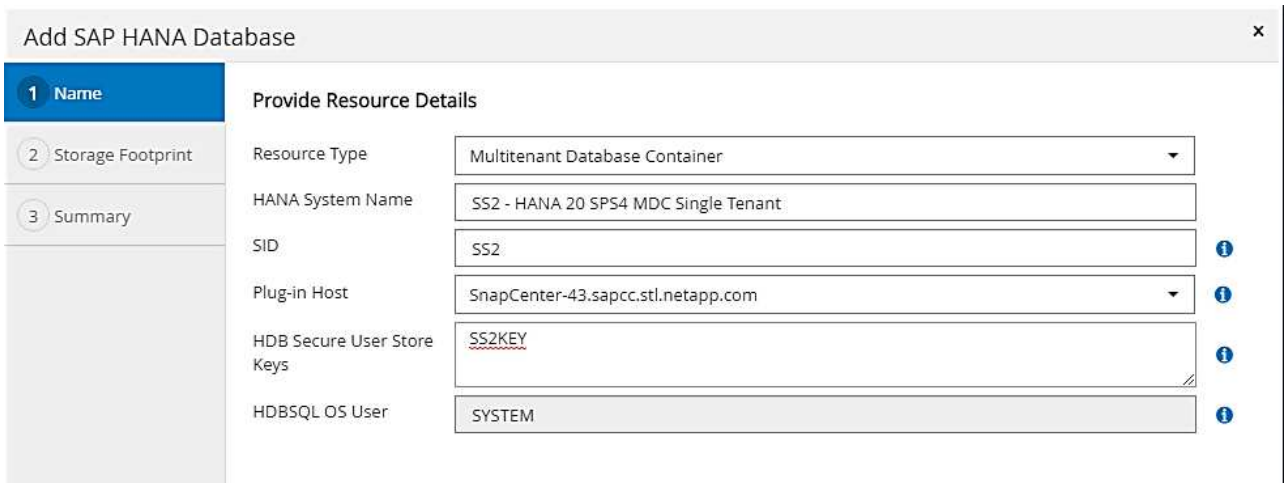
この例では、マルチテナントデータベースコンテナのリソースタイプを選択します。

> 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。

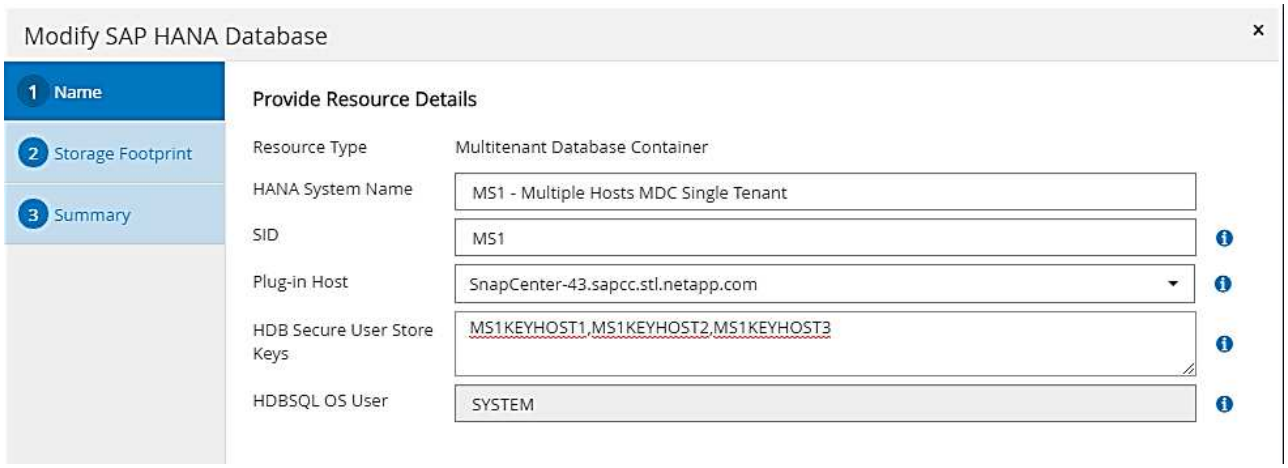
SAP HANA システムの場合、 SID は SS2 です。

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

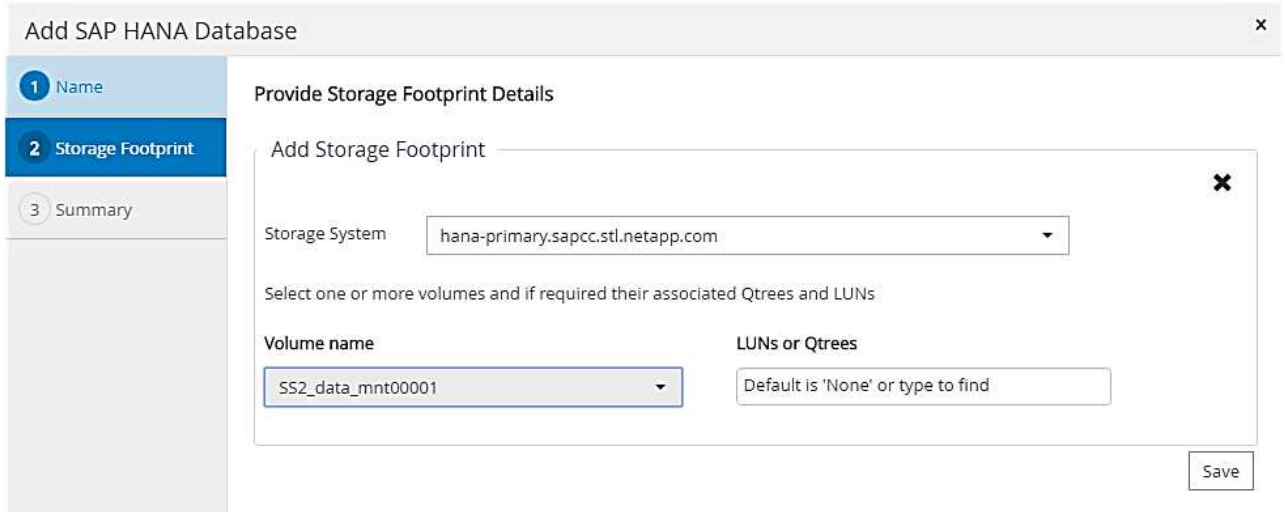
hdbuserstore キーは、 HANA データベース SS2 用に設定されたキーと一致している必要があります。この例では、 SS2KEY です。




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。

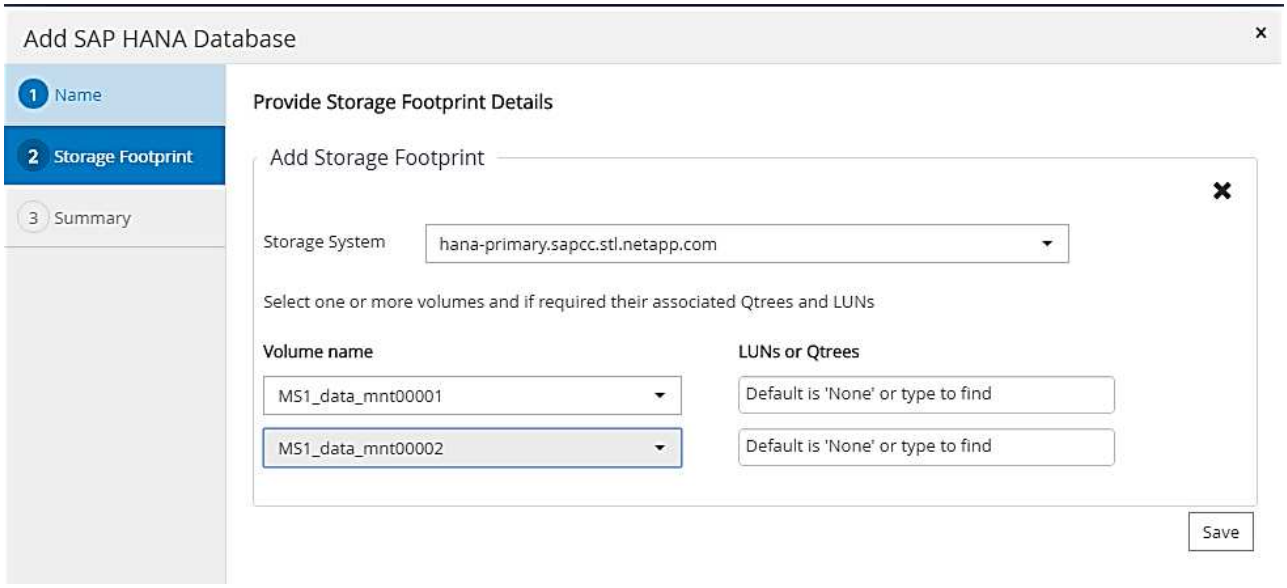



c. ストレージシステム（ SVM ）とボリューム名に必要なデータを選択します。



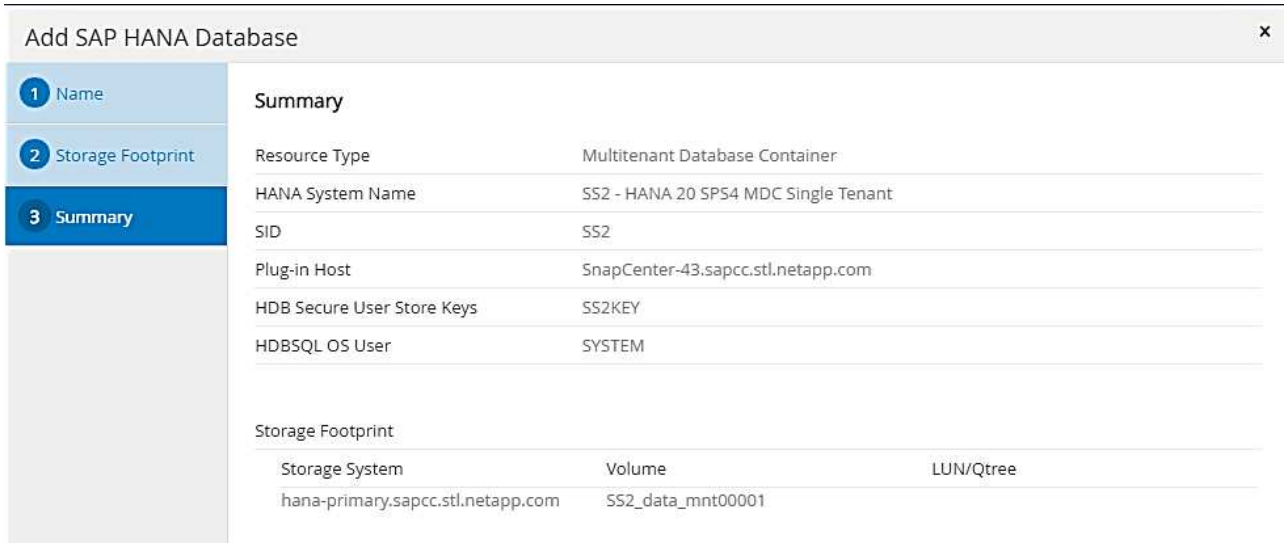
ファイバチャネル SAN 構成の場合は、 LUN も選択する必要があります。

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。



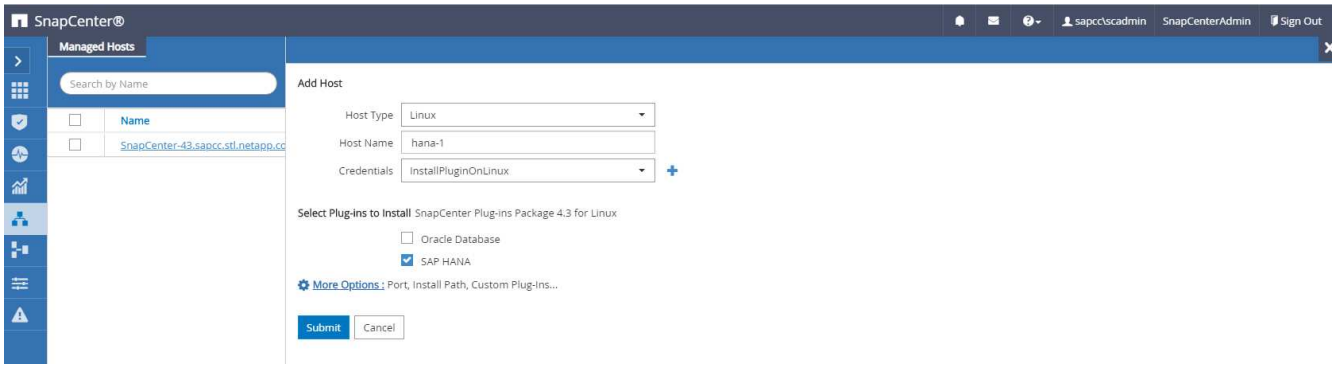

b. リソースの設定が完了したら、の説明に従ってリソース保護の設定を実行します"リソース保護の設定"。

**HANA** データベースの自動検出

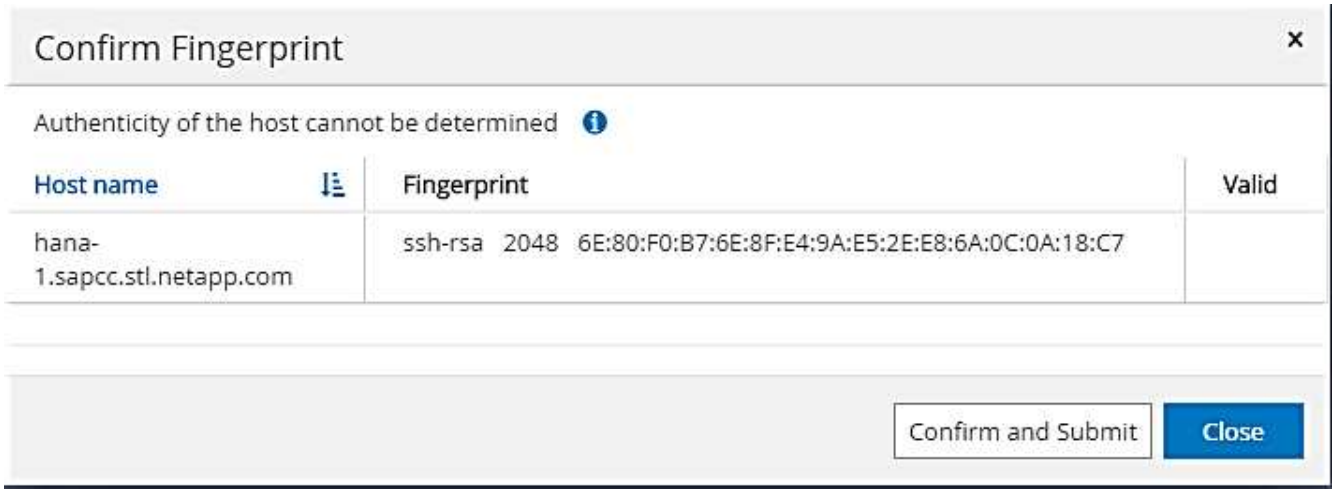
このセクションでは、 SAP HANA リソース SS1 （ NFS を使用するシングルホスト MDC シングルテナントシステム）の自動検出について説明します。ここで説明する手順はすべて、 HANA シングルコンテナ、 HANA MDC マルチテナントシステム、およびファイバチャネル SAN を使用する HANA システムで同じです。

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。

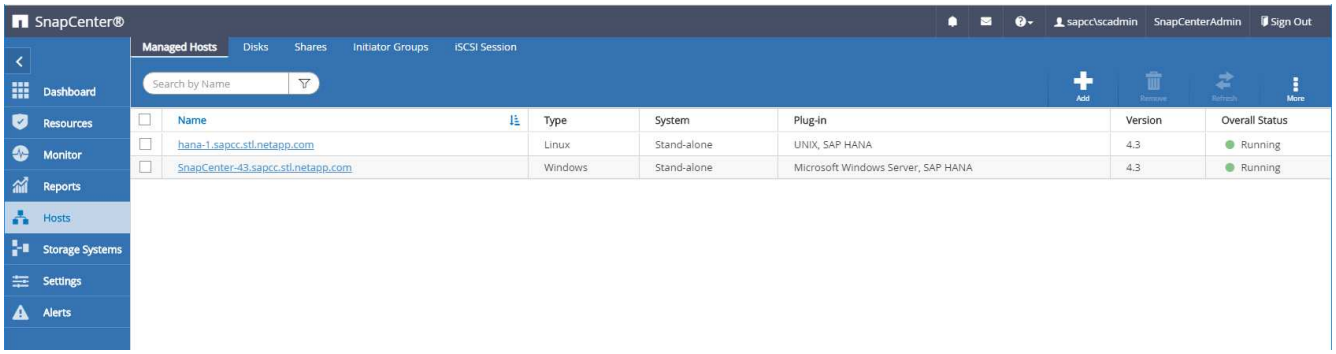
1. ホストタブで、追加をクリックします。
2. ホスト情報を入力し、インストールする SAP HANA プラグインを選択します。Submit をクリックします。




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。

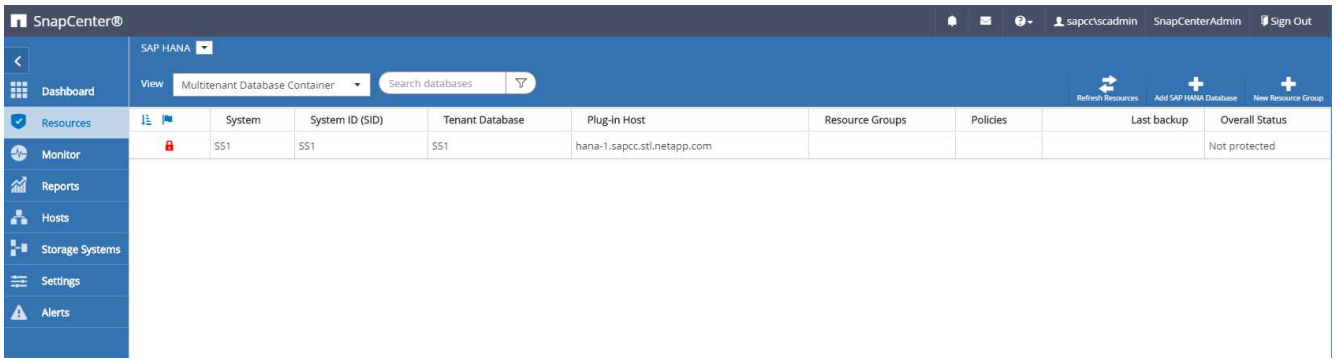



プラグインのインストール後、 HANA リソースの自動検出プロセスが自動的に開始されます。[ リソース ] 画面で、新しいリソースが作成されます。このリソースは、赤い南京錠のアイコンでロックされている

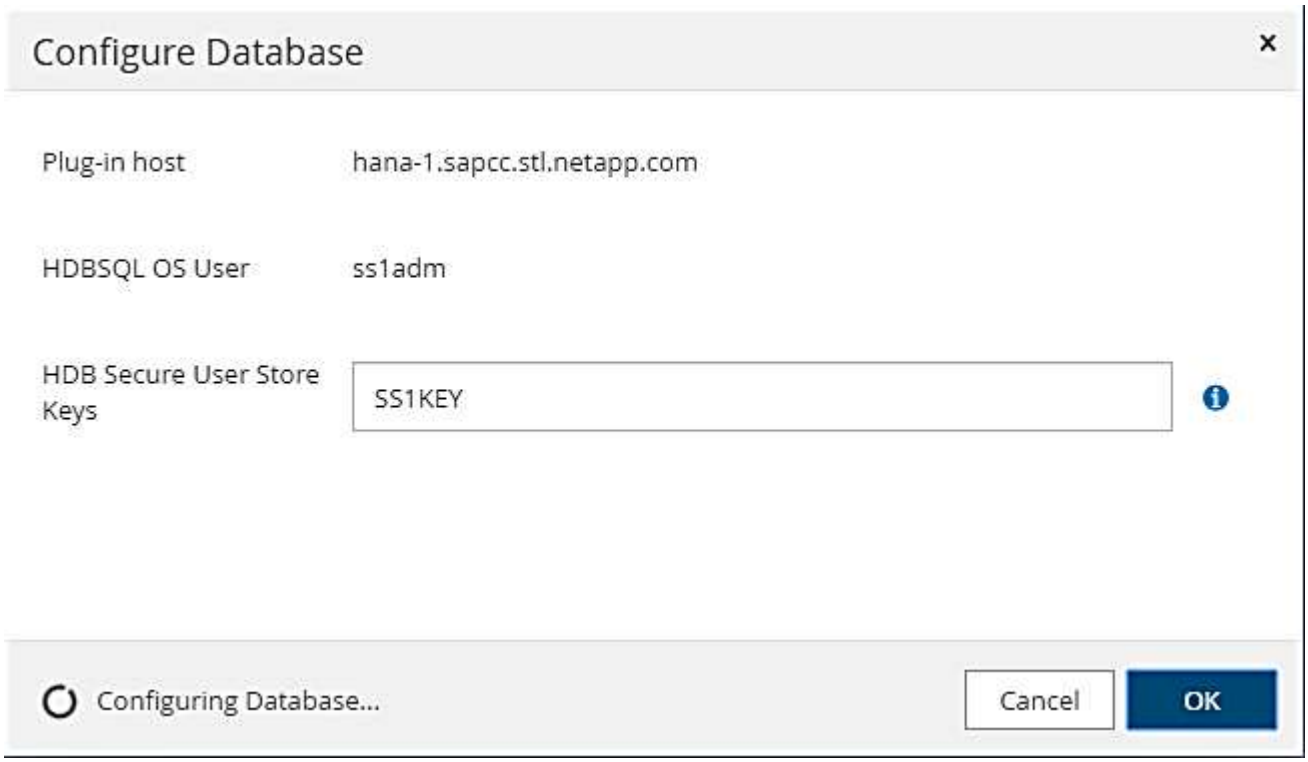
ことが示されます。

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。

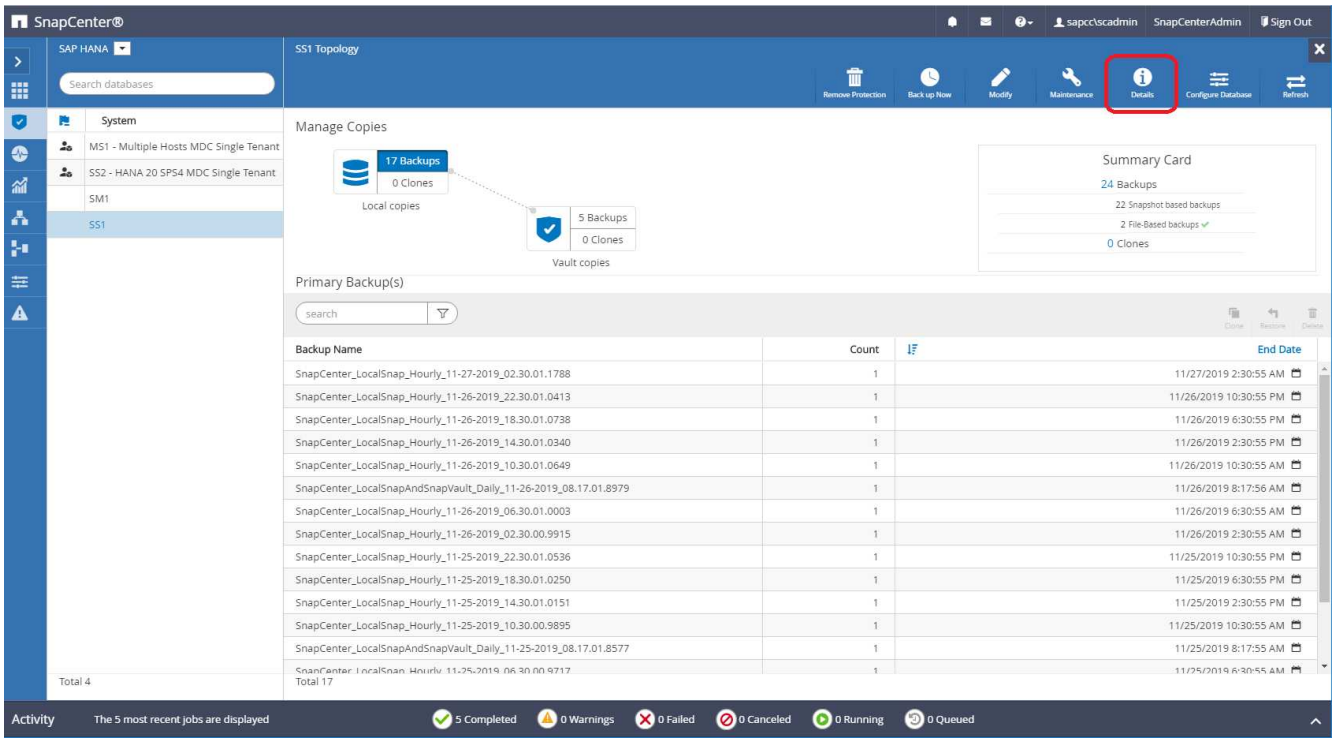


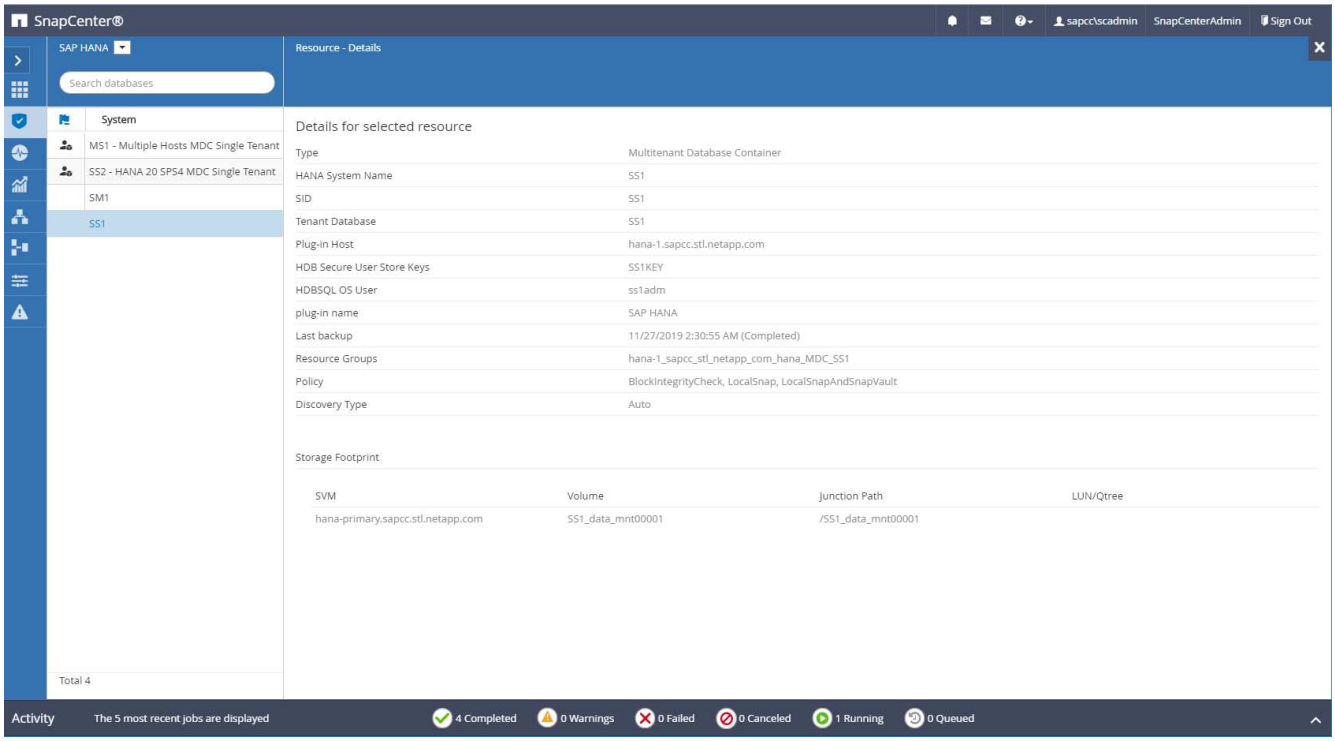

5. HANA データベースのユーザストアキーを指定します。




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。

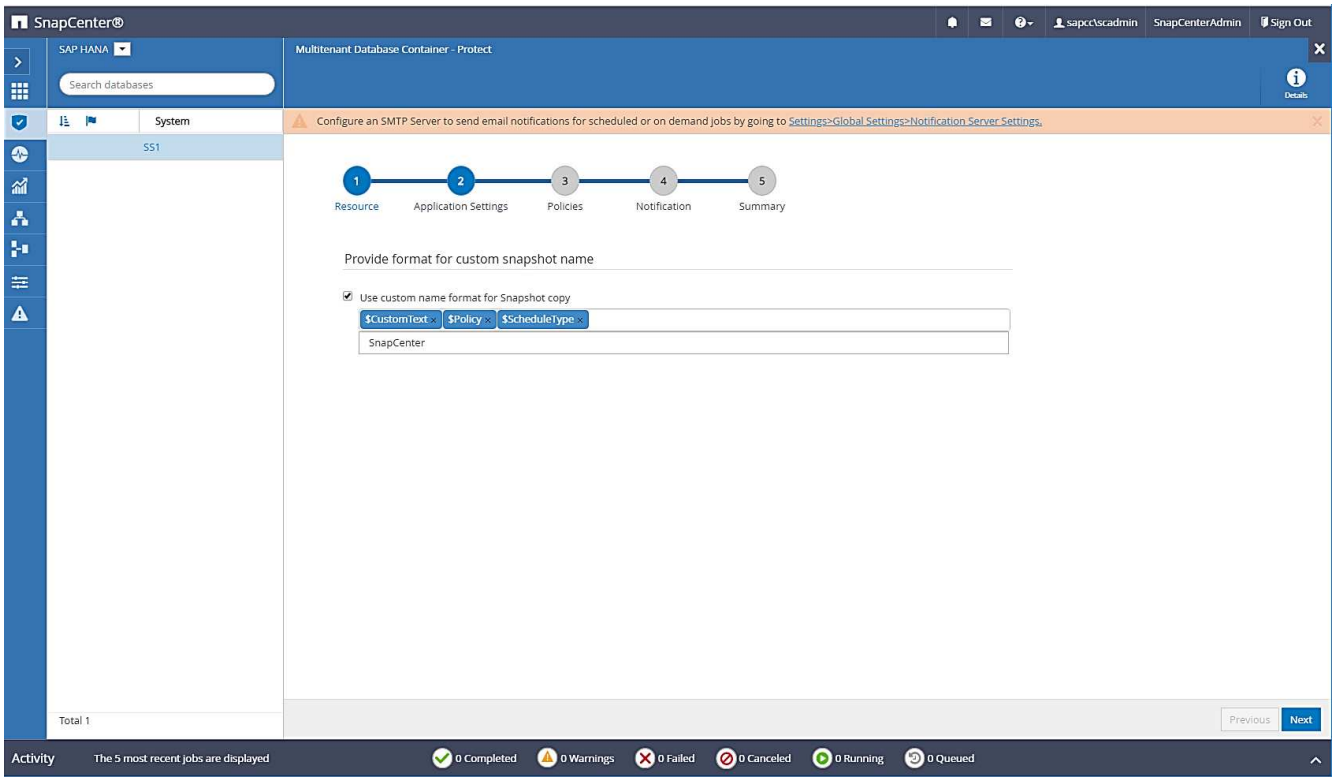
2. Snapshot コピーにカスタムの名前形式を設定します。

> 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。

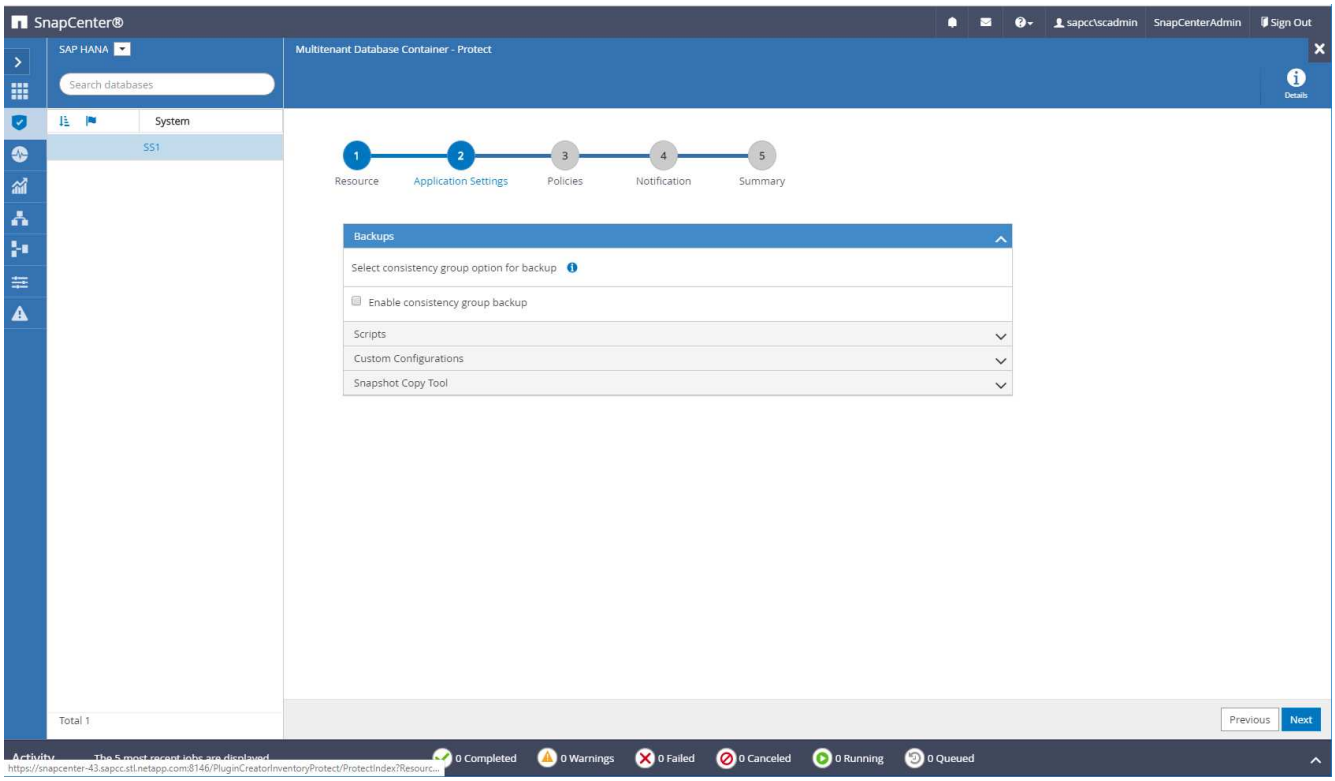
次の図に示す構成では、バックアップ名と Snapshot コピー名の形式は次のとおりです。

- 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>`

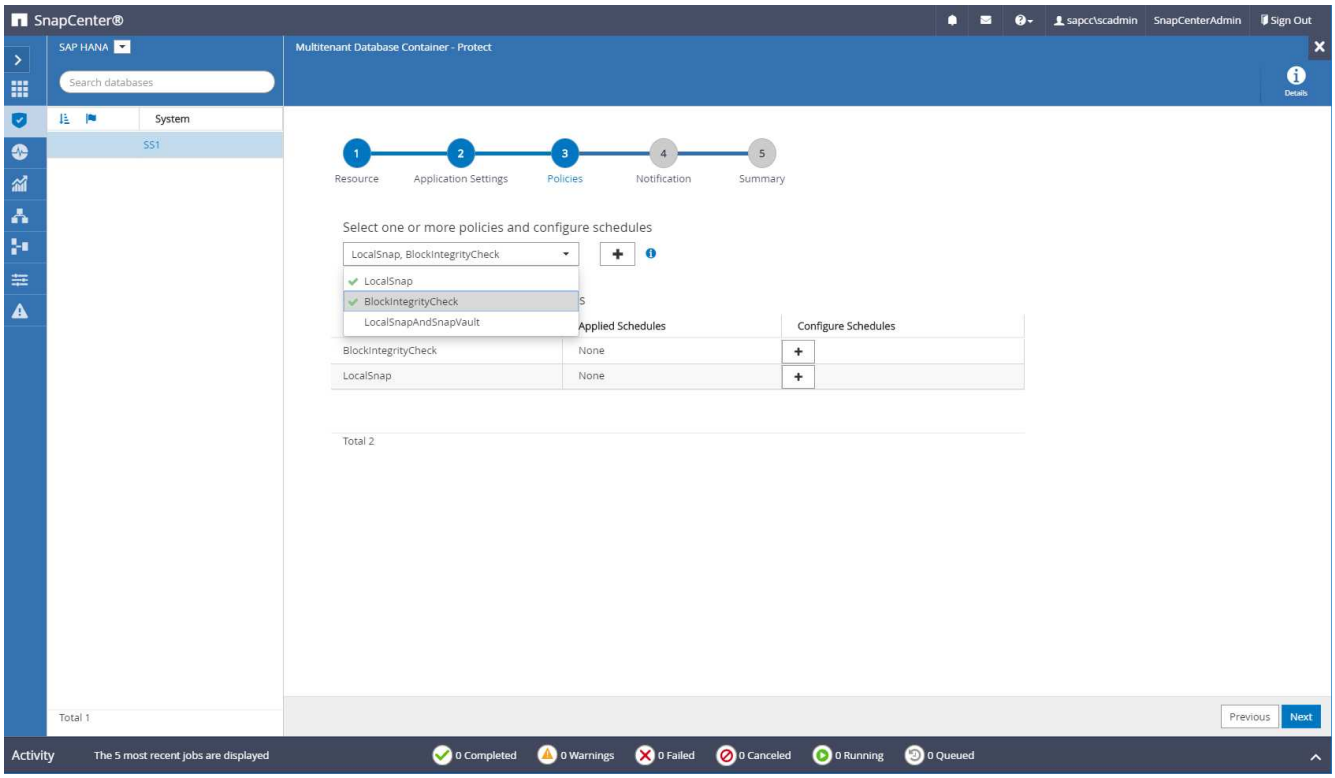
> ポリシー設定でオンデマンドバックアップに対して保持が定義されていても、不要なファイルの削除は別のオンデマンドバックアップが実行されたときにのみ実行されます。そのため、通常、 SnapCenter でオンデマンドバックアップを手動で削除して、これらのバックアップが SAP HANA バックアップカタログからも削除され、ログバックアップの不要な削除が古いオンデマンドバックアップに基づいて行われないようにする必要があります。



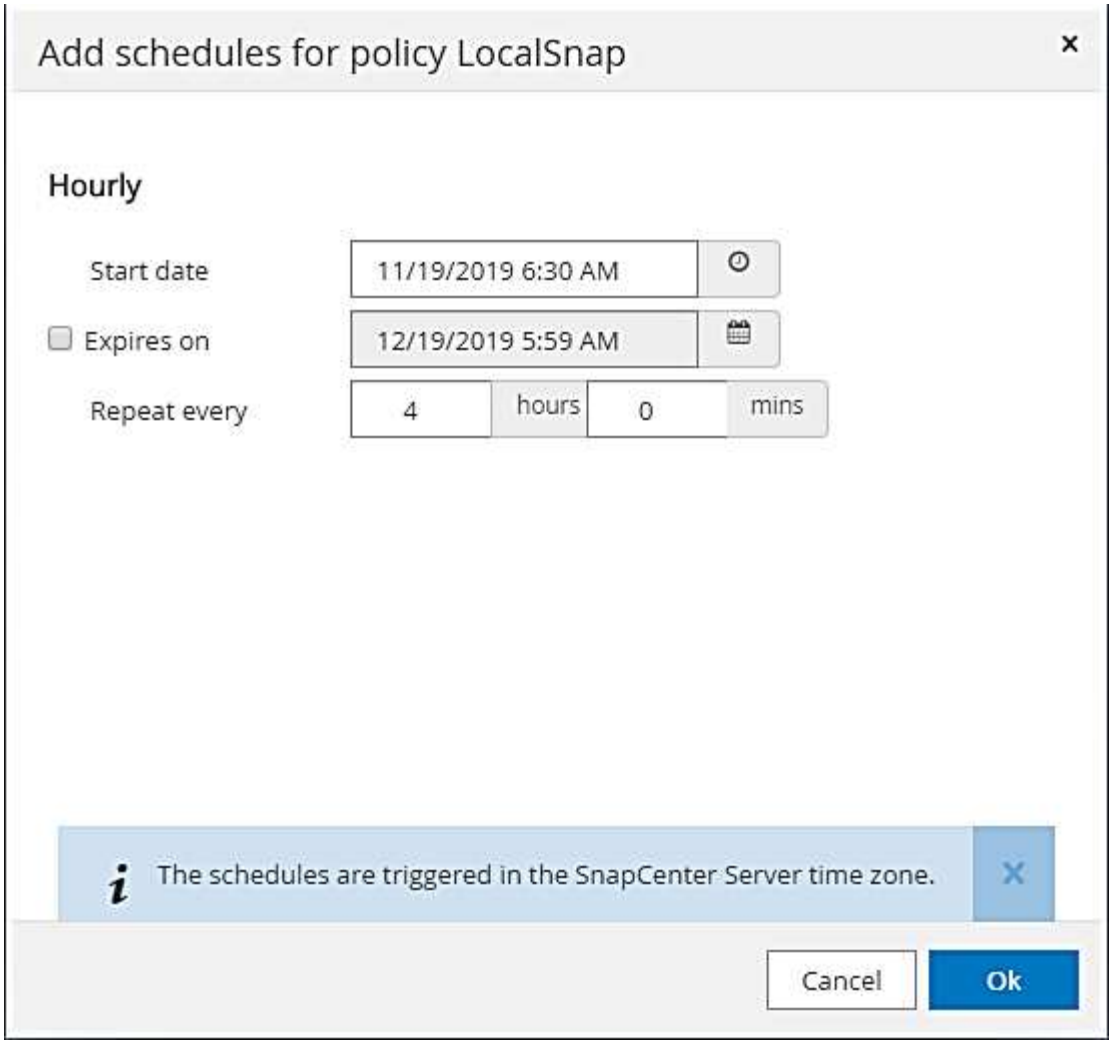

3. [ アプリケーションの設定 ] ページで、特定の設定を行う必要はありません。次へをクリックします。



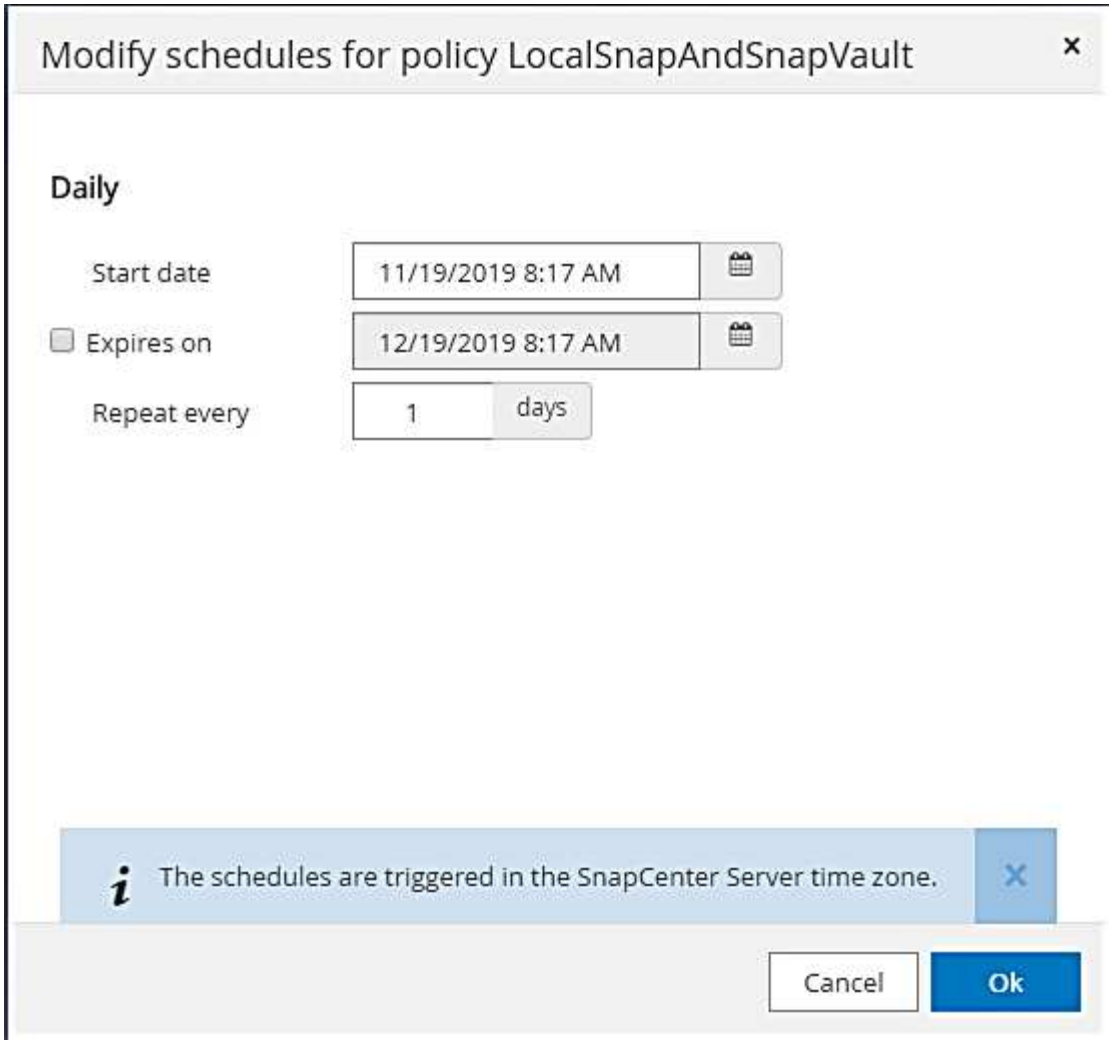

4. リソースに追加するポリシーを選択してください。



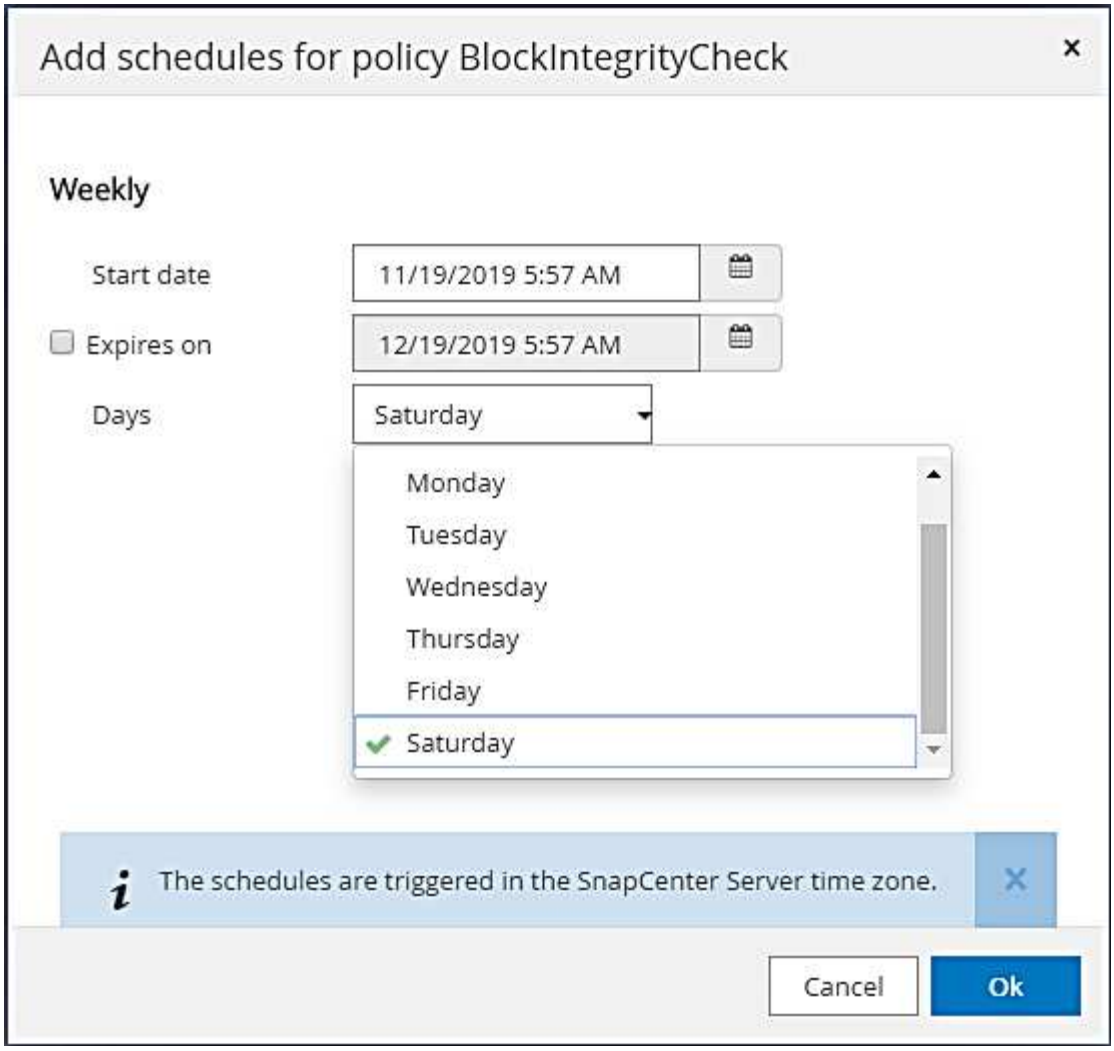

5. LocalSnap ポリシーのスケジュールを定義します（この例では 4 時間ごと）。



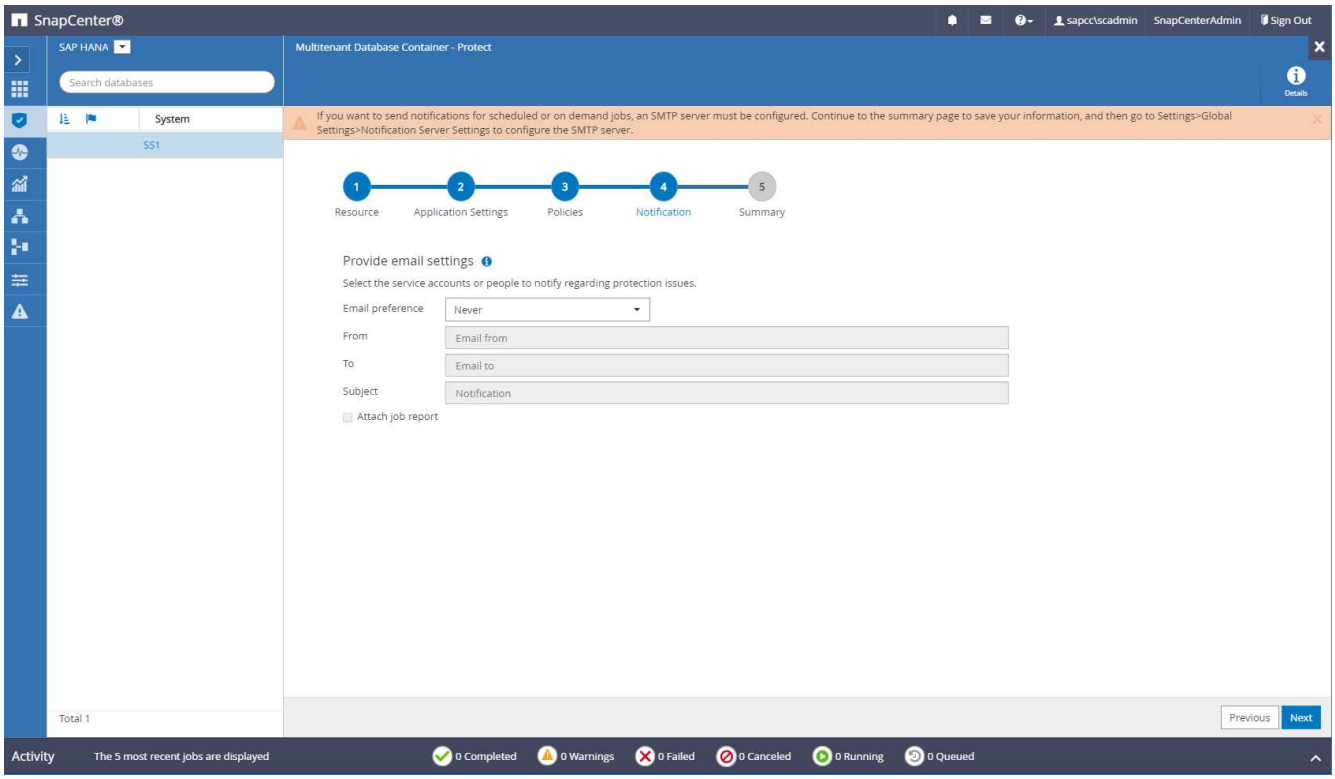

6. LocalSnapAndSnapVault ポリシーのスケジュールを定義します（この例では 1 日に 1 回）。



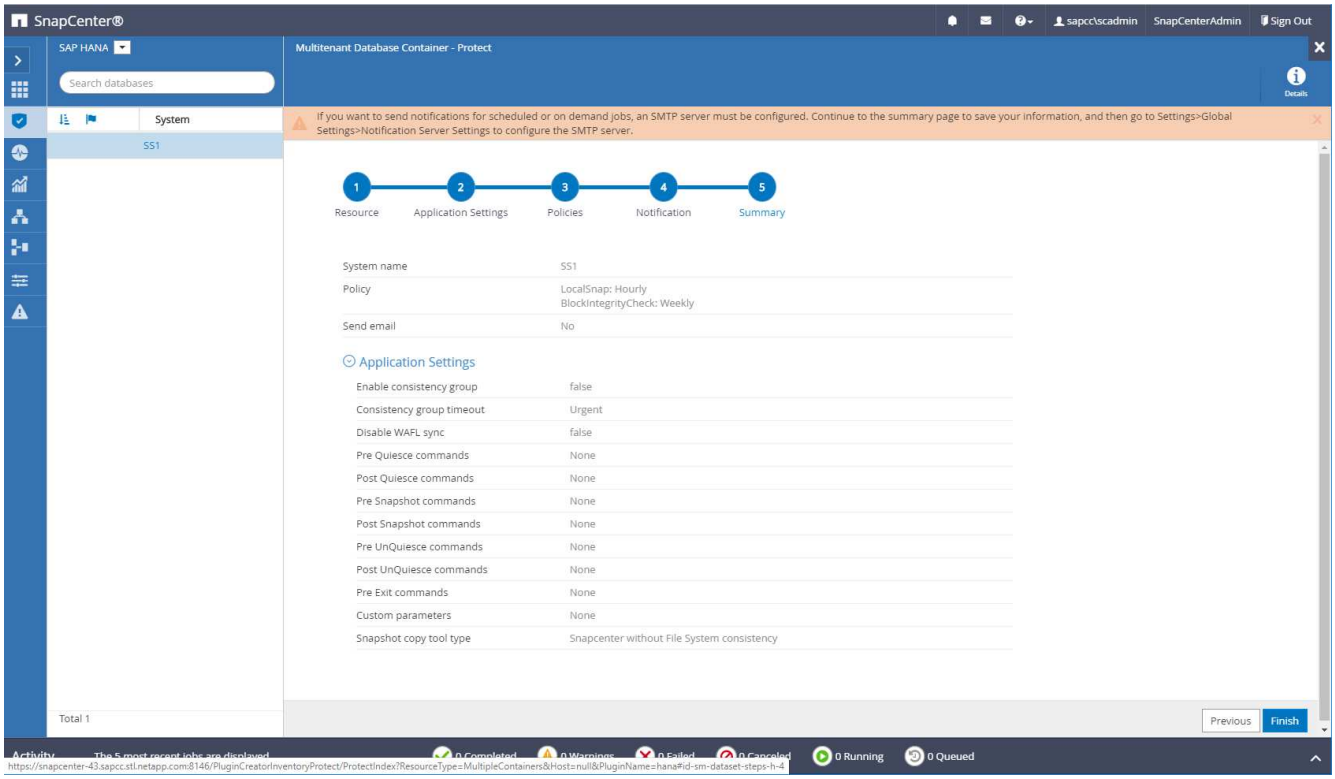

7. ブロック整合性チェックポリシーのスケジュールを定義します（この例では週に 1 回）。



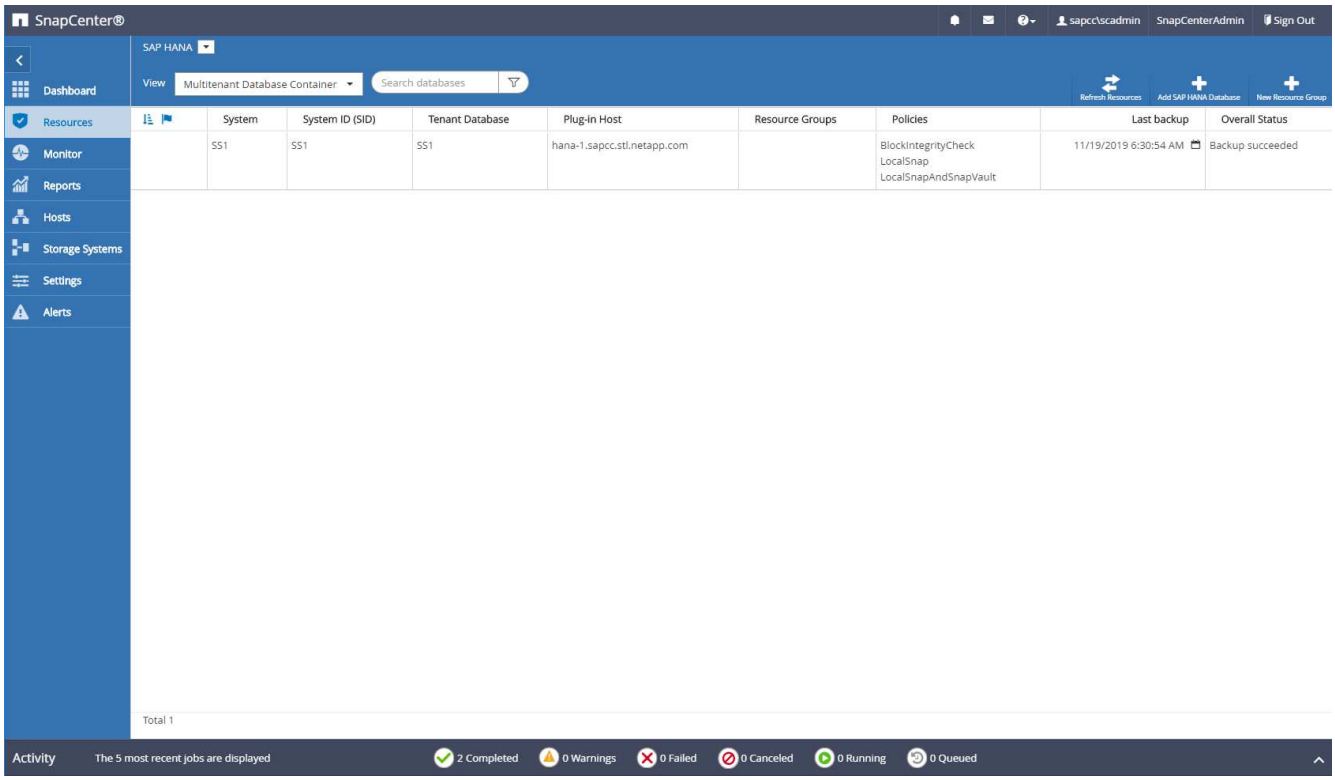

8. E メール通知に関する情報を指定します。




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。

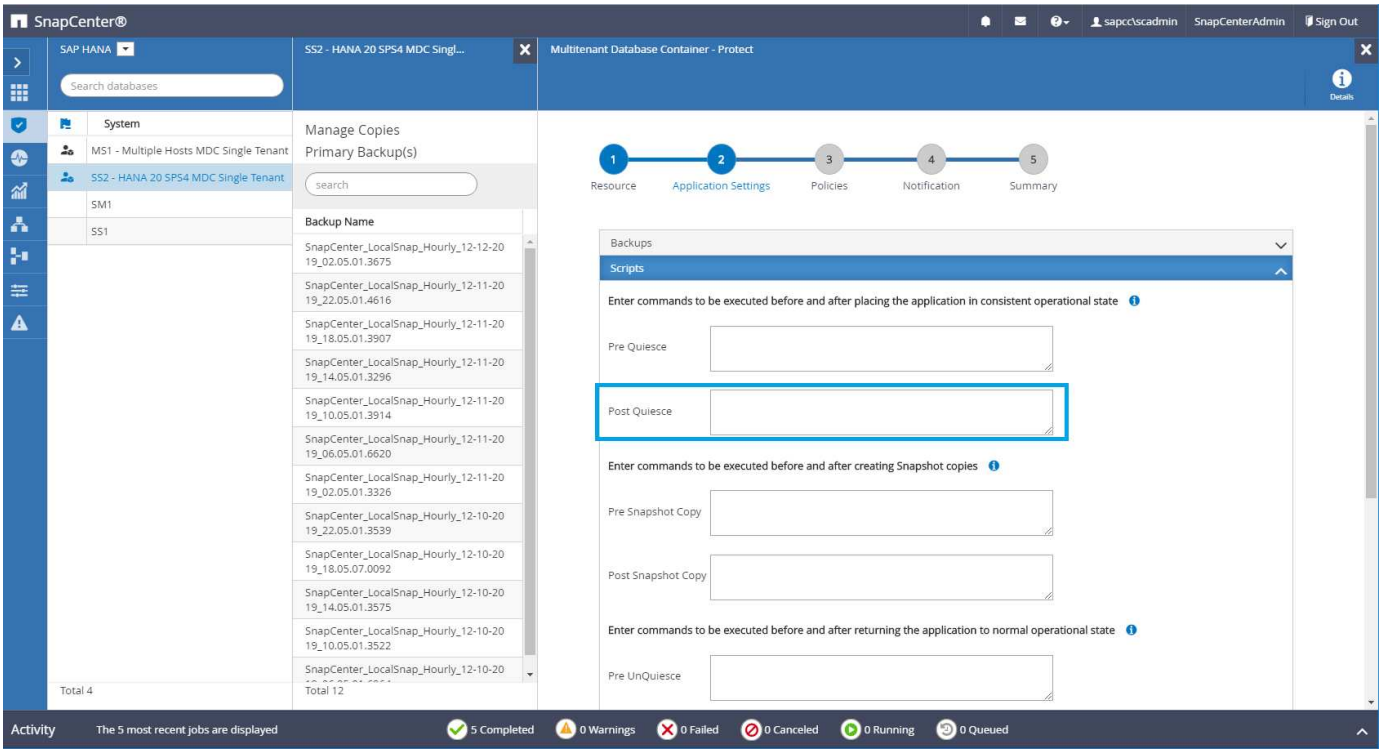
SnapCenter サーバが中央の HANA プラグインホストとして使用されている場合は、バッチファイルを使用できます。バッチファイルには、次の内容が含まれている必要があります。

```
@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。

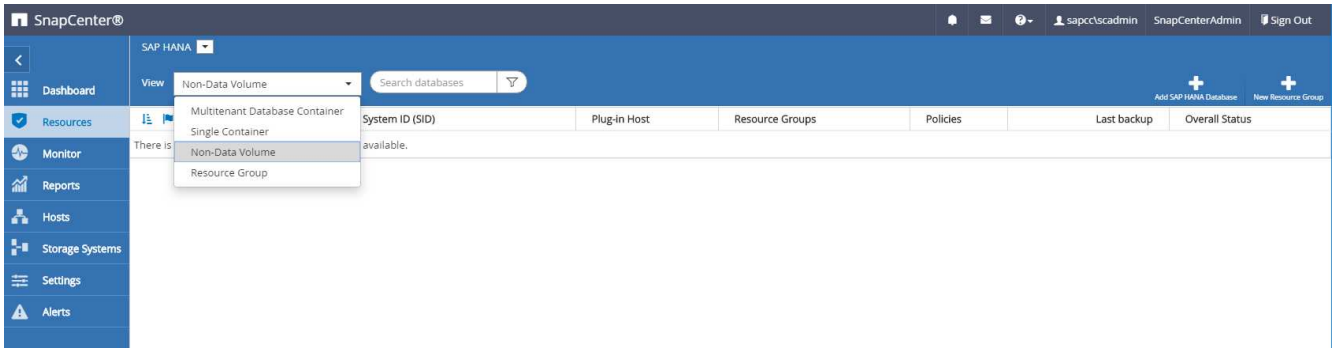
他のデータファイルのリストアが必要な状況からリカバリするには、 SAP HANA データベースのバックアップを補うために、データボリューム以外のボリュームに対する追加のバックアップ戦略を開発することを推奨します。固有の要件に応じて、非データボリュームのバックアップはスケジュールの頻度と保持の設定が異なる場合があります。また、非データファイルを変更する頻度も考慮する必要があります。たとえば、 HANA ボリューム「 /hana/shared 」には、実行可能ファイルと SAP HANA トレースファイルが格納されています。実行ファイルが変更されるのは SAP HANA データベースがアップグレー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

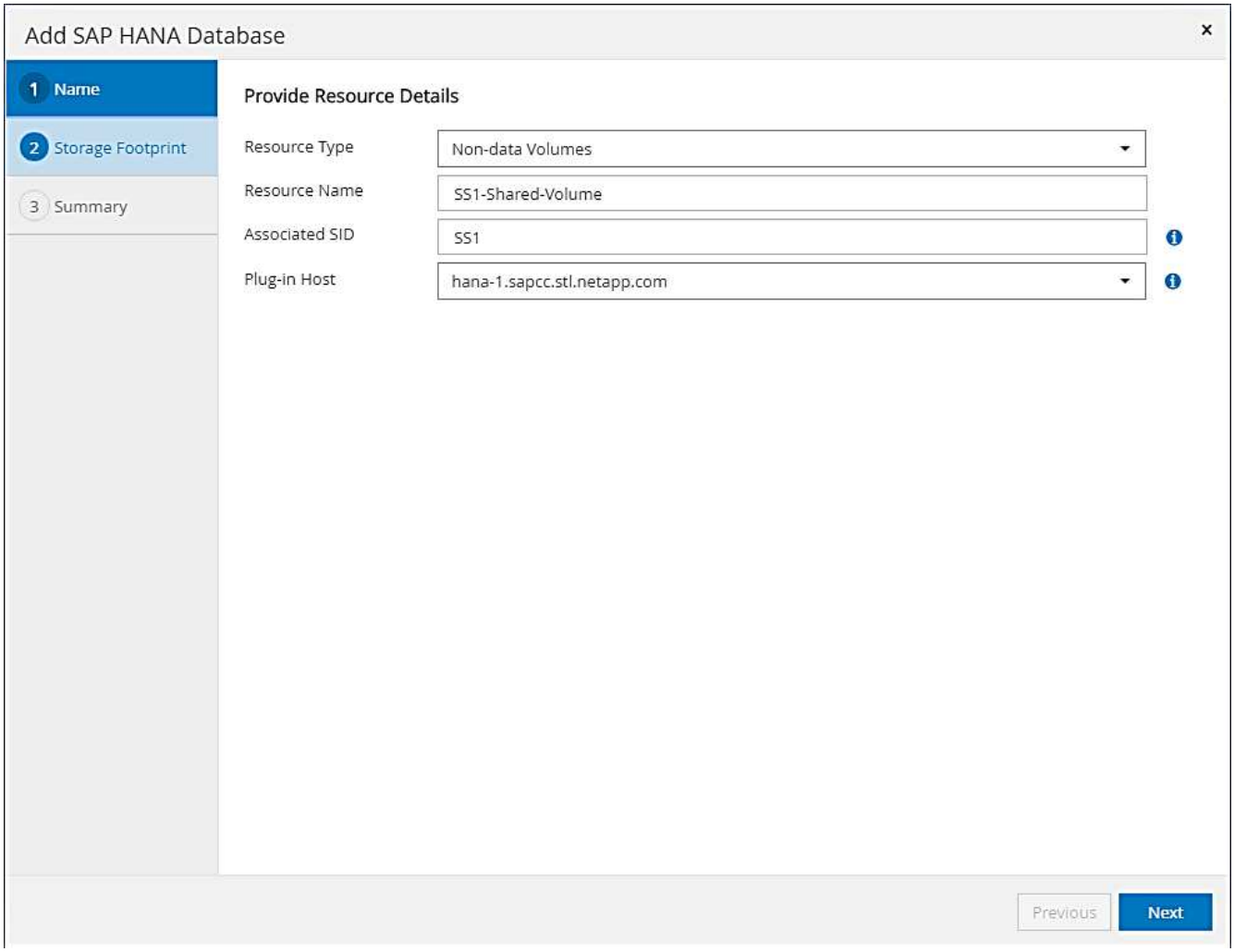
データボリューム以外のリソースの構成

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。

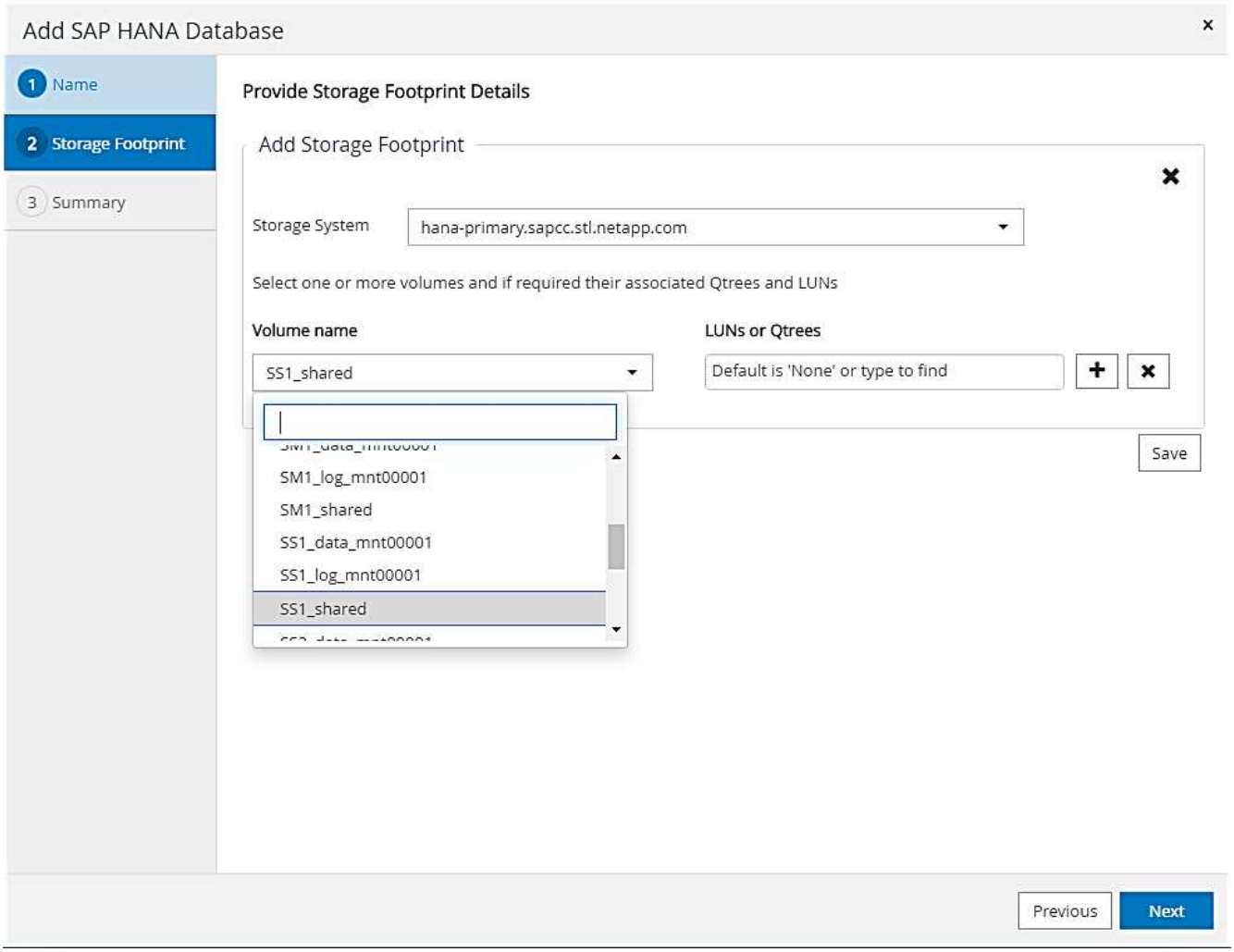
1. [ リソース ] タブで、 [ データボリュームではない ] を選択し、 [ SAP HANA データベースの追加 ] をクリックします。




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。



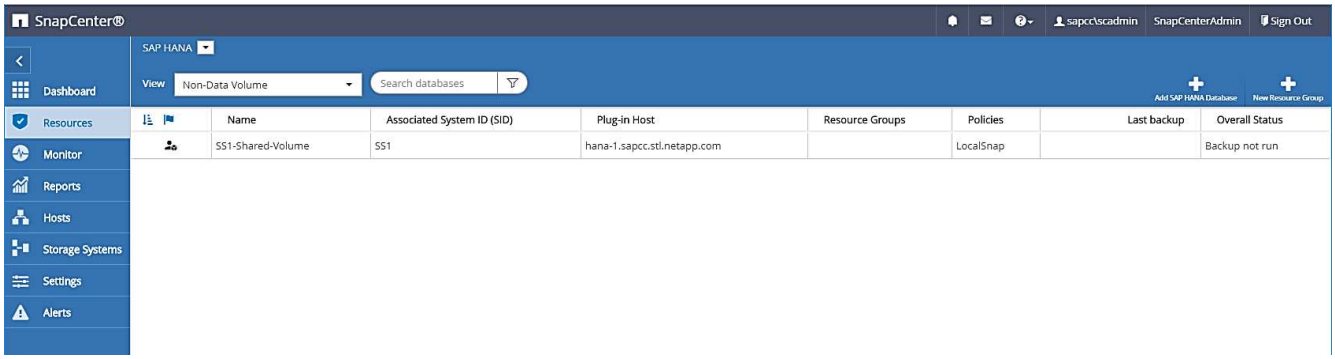

3. SVM とストレージボリュームをストレージ容量として追加し、次へをクリックします。




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。SAP LaMa向けNetApp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。

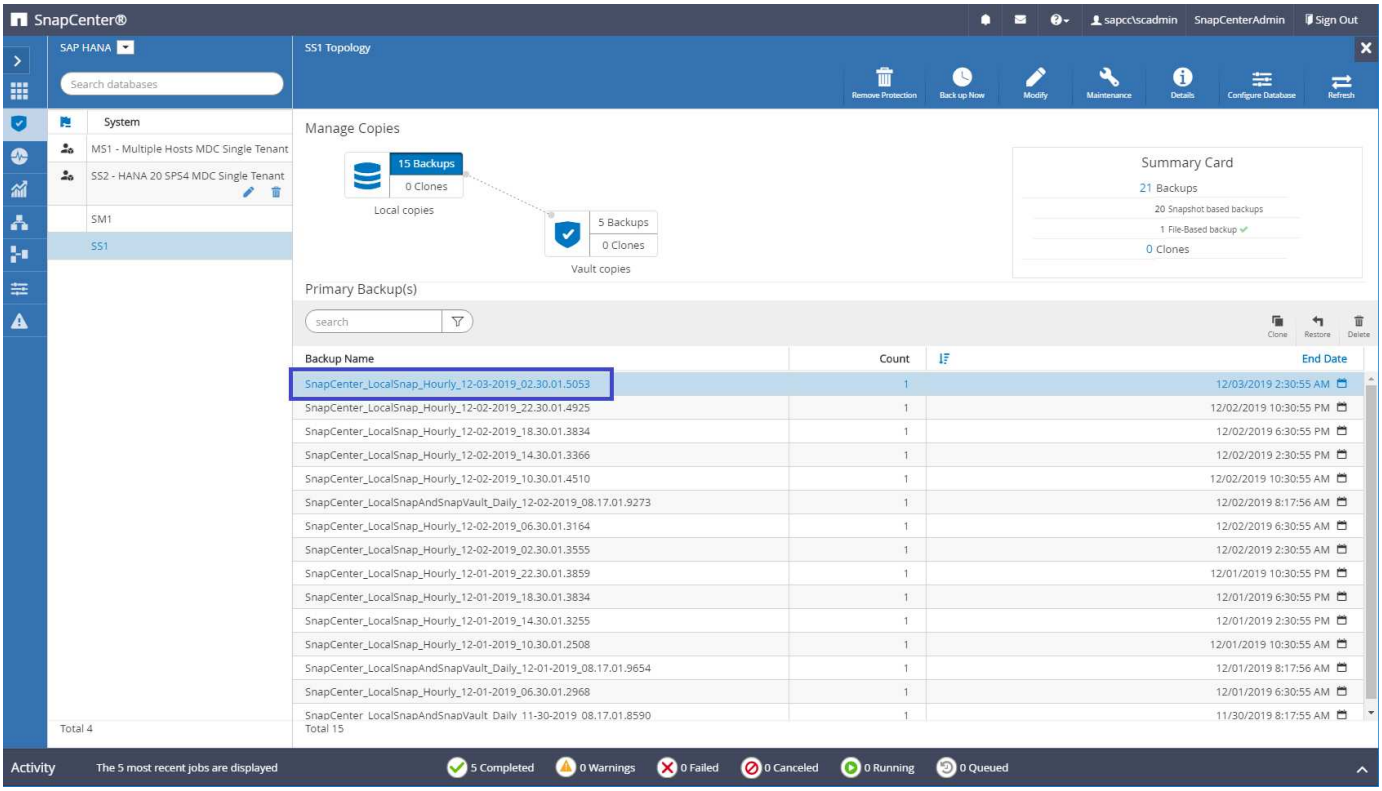
## データベースのバックアップ

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。



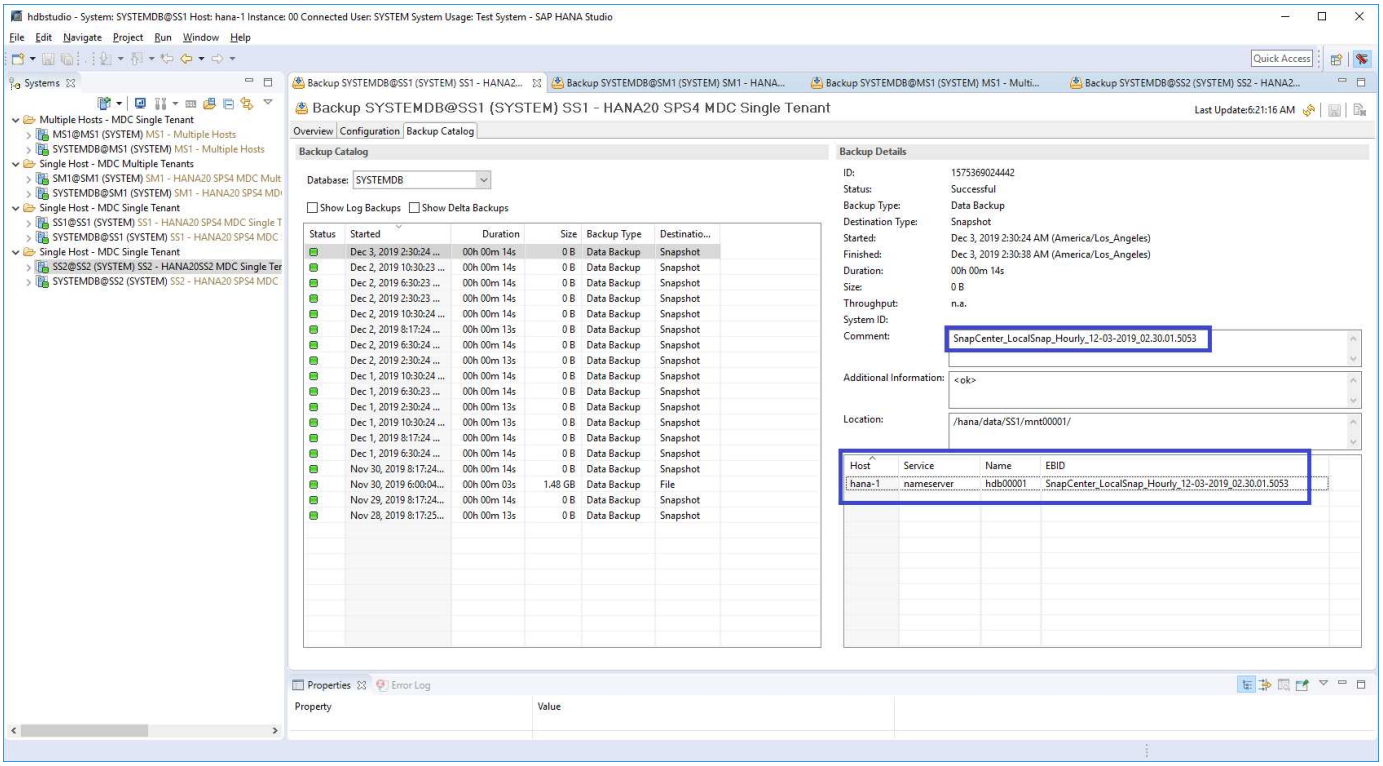

SAP HANA MDC システムのストレージ Snapshot コピーを使用したバックアップを実行する場合は、データボリュームの Snapshot コピーが作成されます。このデータボリュームには、システムデータベースのデータおよびすべてのテナントデータベースのデータが含まれます。この物理アーキテクチャを反映するため、 SnapCenter によって Snapshot バックアップがトリガーされるたびに、 SAP HANA はシステムデータベースとすべてのテナントデータベースの統合バックアップを内部的に実行します。その結果、 SAP HANA のバックアップカタログに、システムデータベース用と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

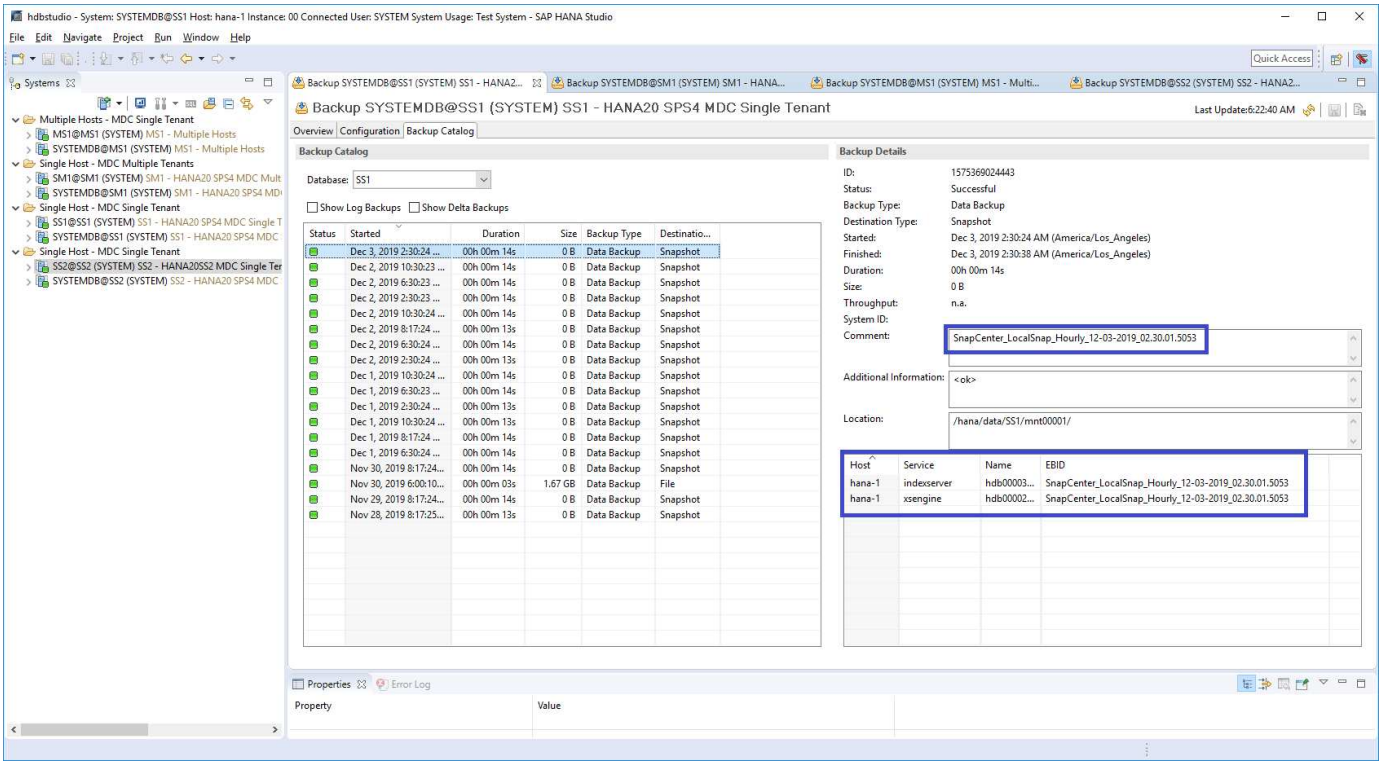
SAP HANA シングルコンテナシステムの場合、データベースボリュームにはデータベースが 1 つだけ格納され、 SAP HANA のバックアップカタログにはエントリが 1 つしかありません。

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"。

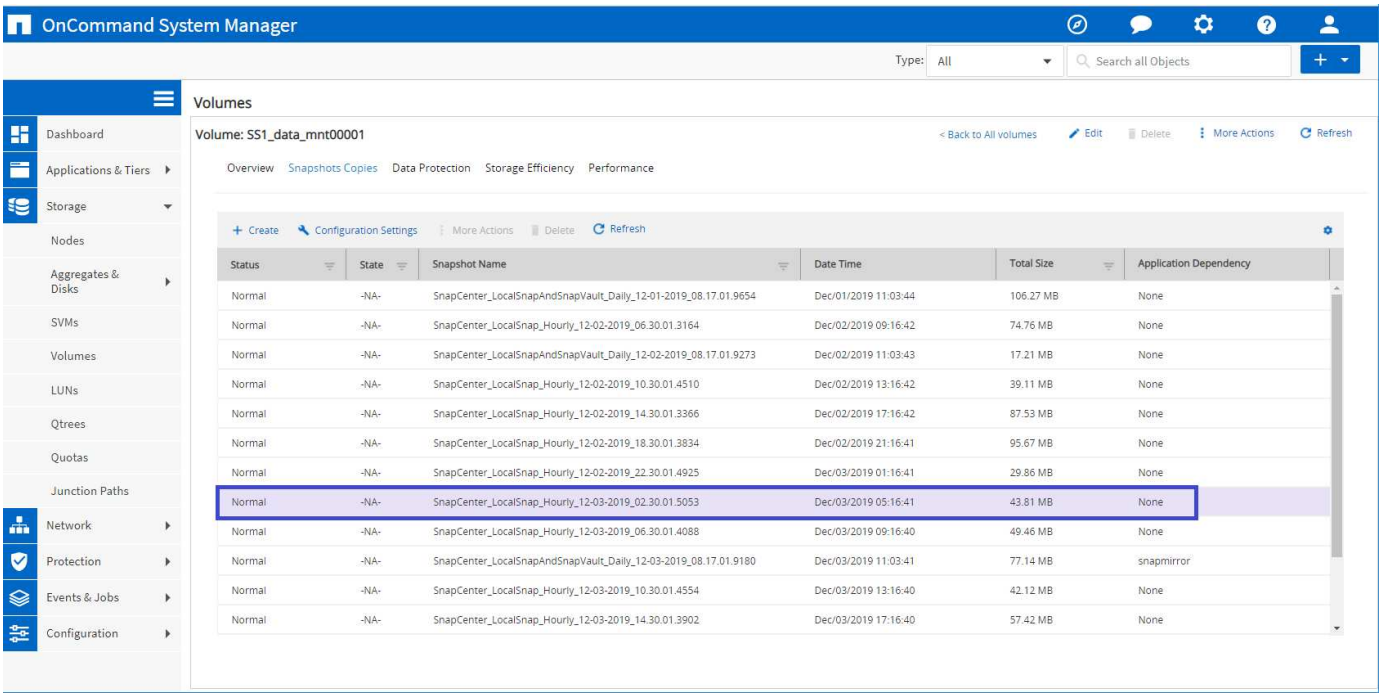


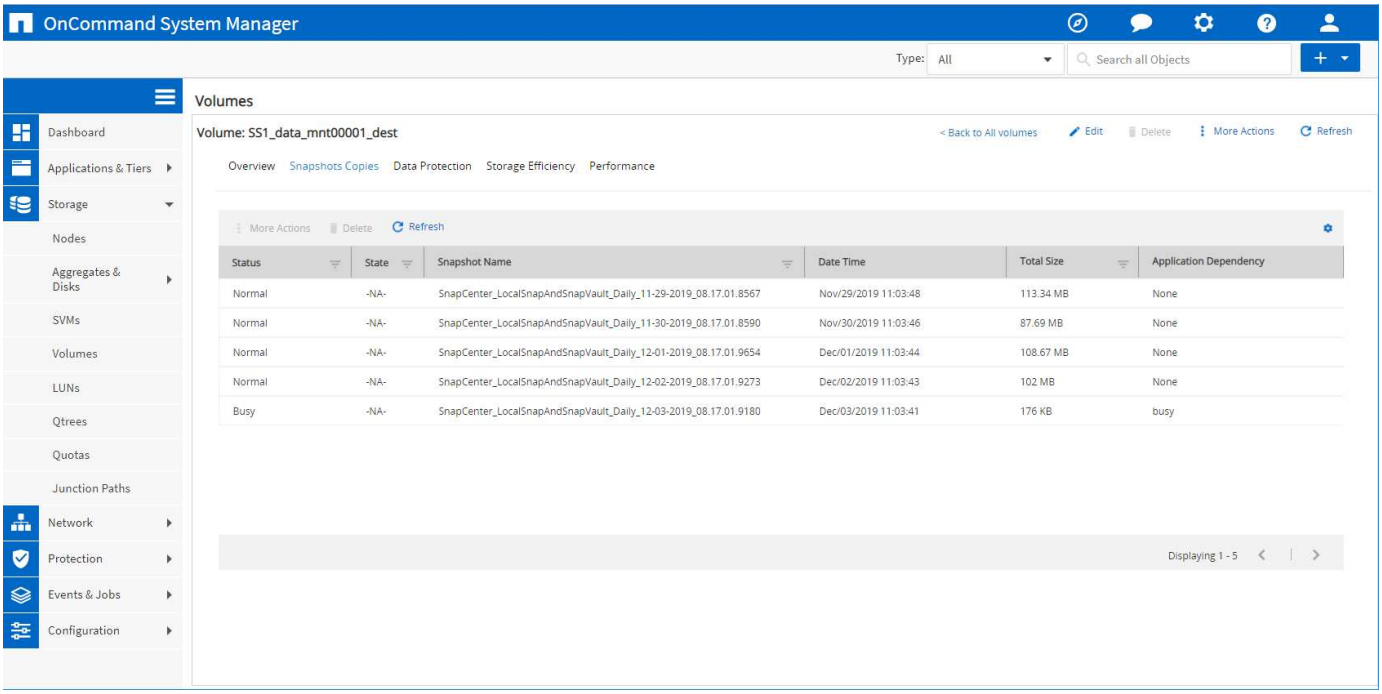
SnapCenter で認識されるのは、それ自体のバックアップだけです。SAP HANA Studio などで作成された追加のバックアップは、 SAP HANA のカタログには表示されますが、 SnapCenter には表示されません。

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。



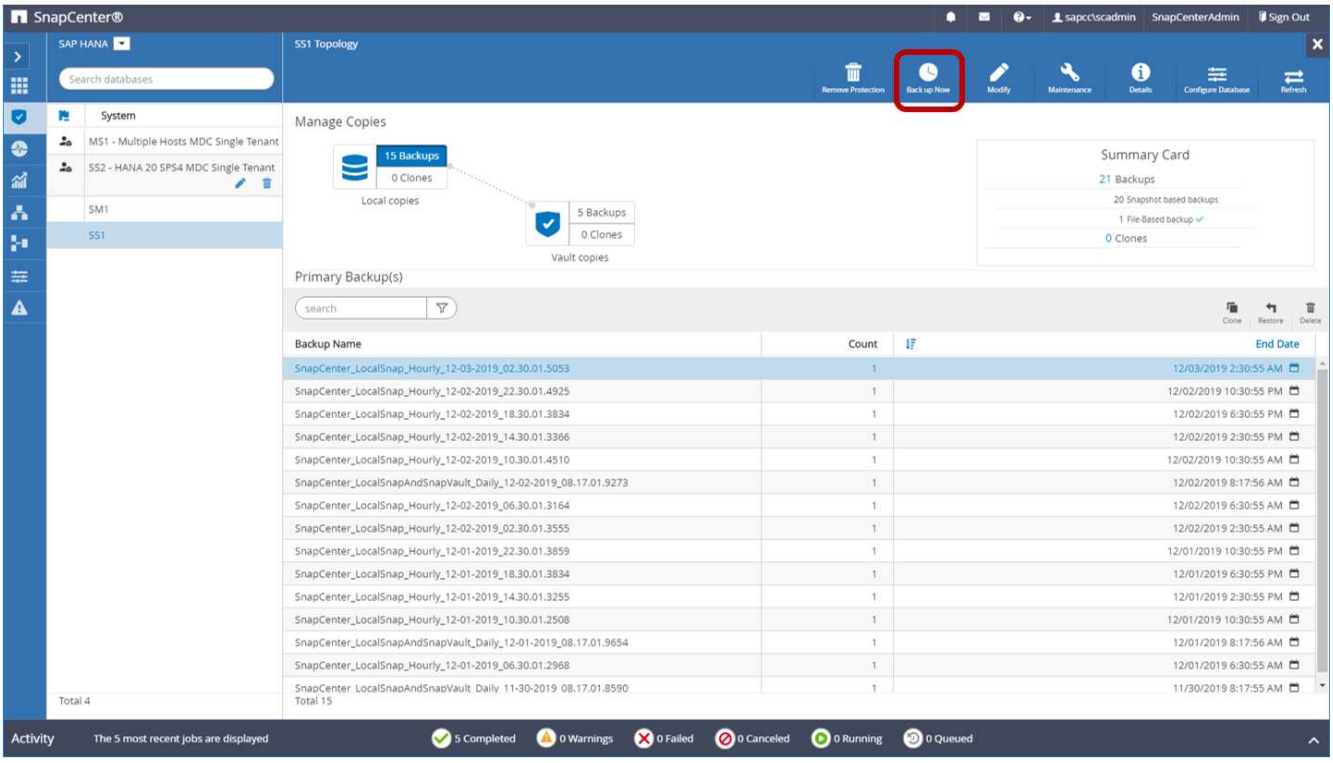

次のスクリーンショットは、セカンダリ・ストレージ・システムにあるレプリケーション・ターゲット・ボリューム「 hana_sa1_data_mnt00001_dest 」で使用可能なバックアップを示しています。




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

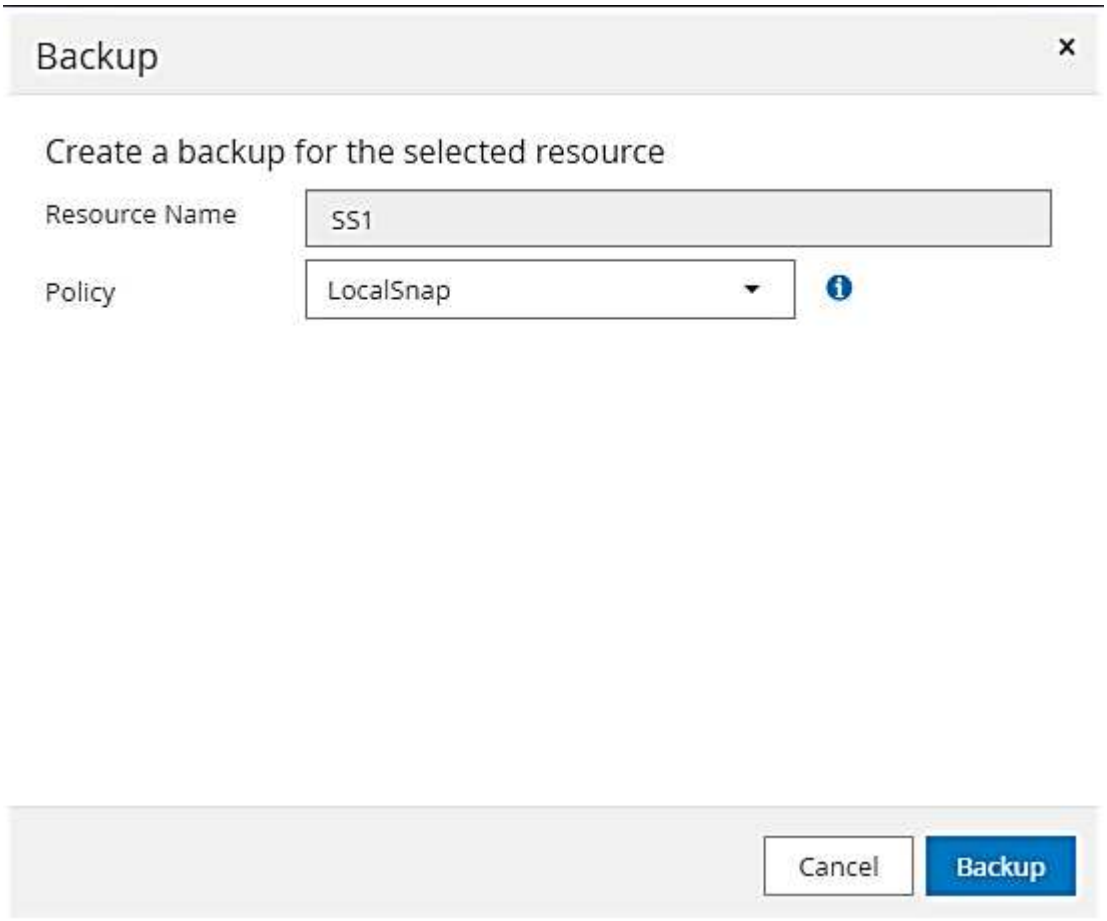
1. リソースビューでリソースを選択し、その行をダブルクリックしてトポロジビューに切り替えます。

   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。



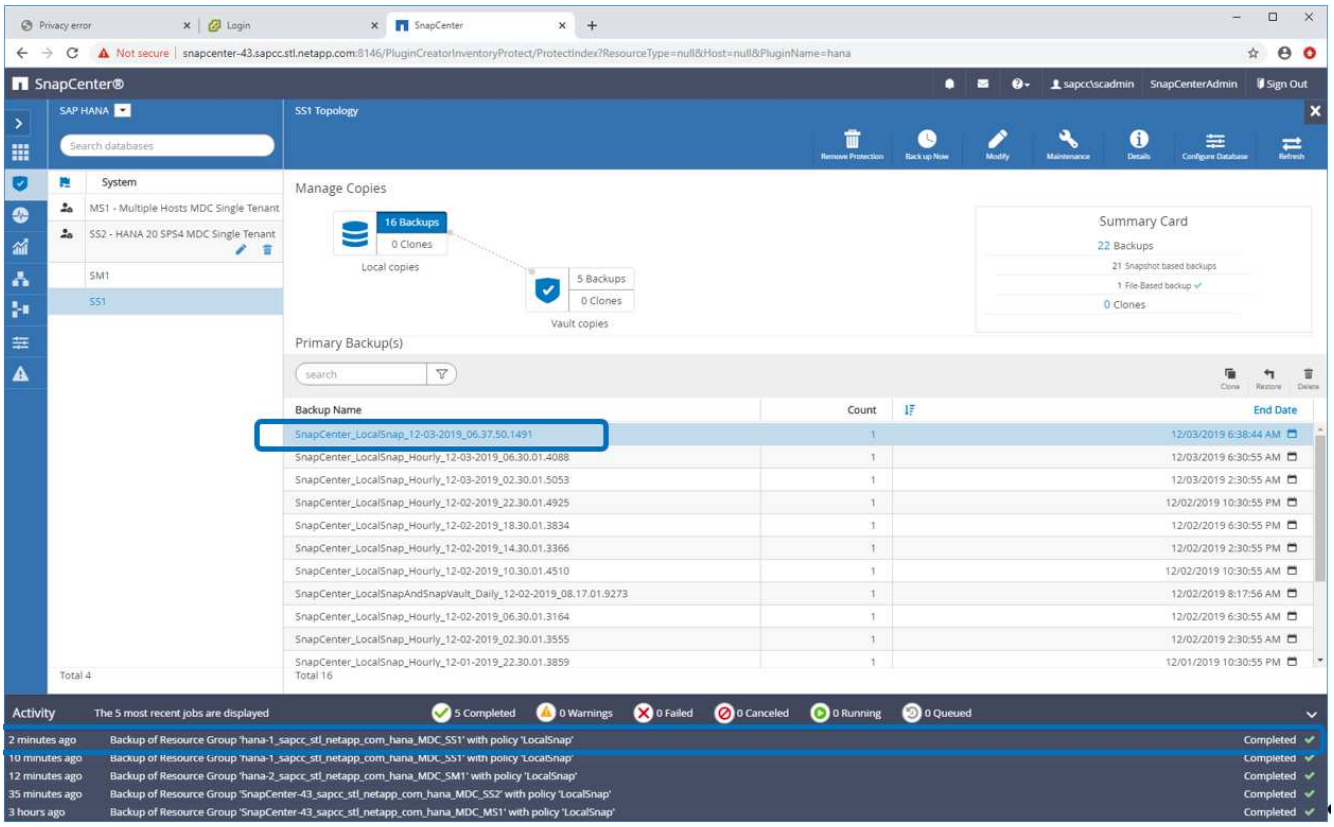

2. 一番上の行で、 Back Up Now （今すぐバックアップ）アイコンを選択して、オンデマンドバックアップ

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

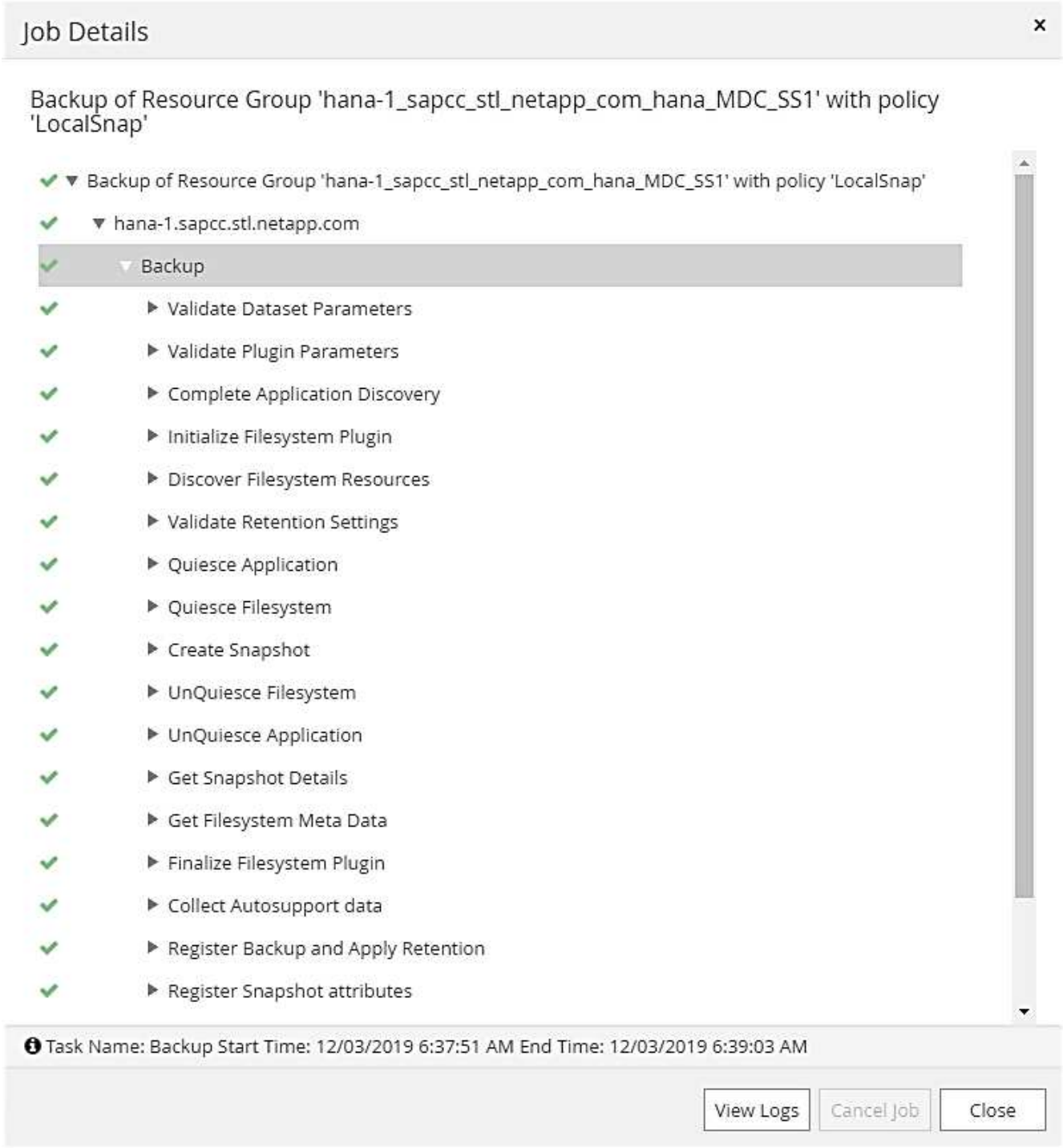



バックアップジョブが開始されます。トポロジビューの下のアクティビティ領域に、前の 5 つのジョブのログが表示されます。バックアップが完了すると、トポロジビューに新しいエントリが表示されます。バックアップ名は、セクションで定義したSnapshot名と同じ命名規則に従います。"「リソース保護の設定」"

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。



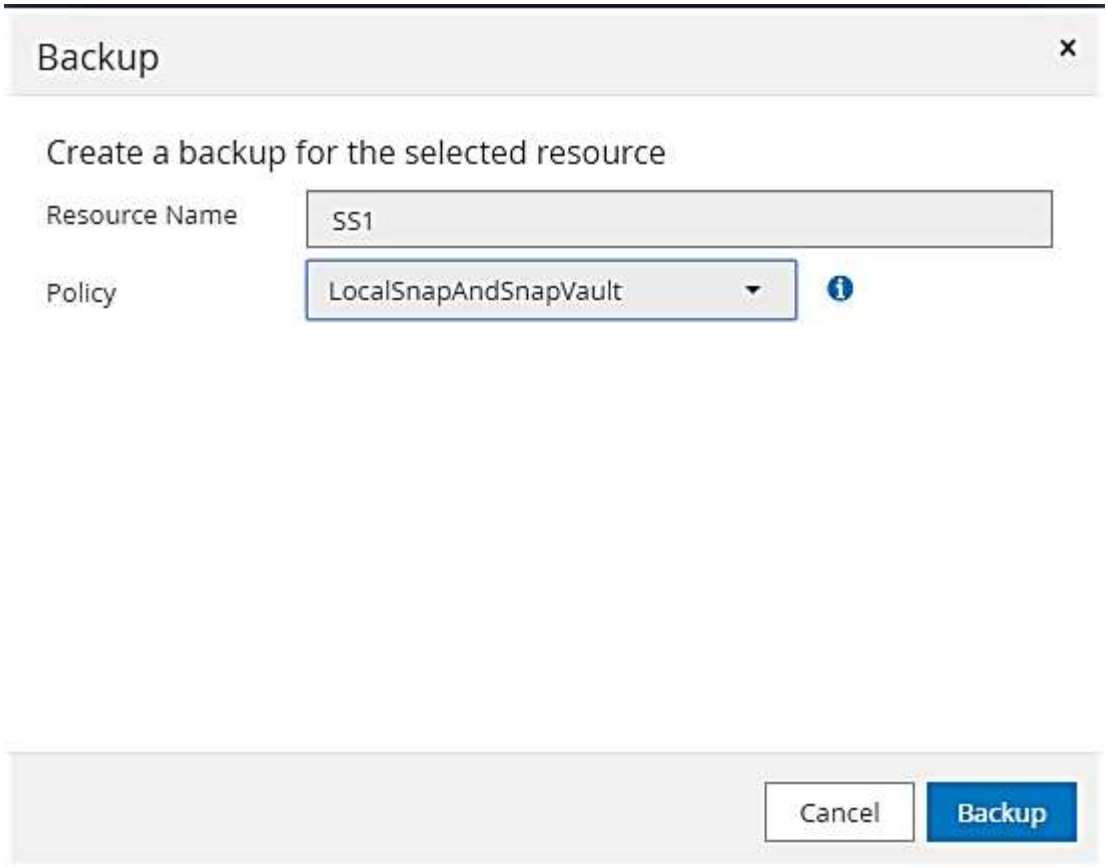

3. ジョブの詳細は、 [ アクティビティ ] 領域でジョブのアクティビティ行をクリックすると表示されます。ログの表示をクリックすると、詳細なジョブログを開くことができます。



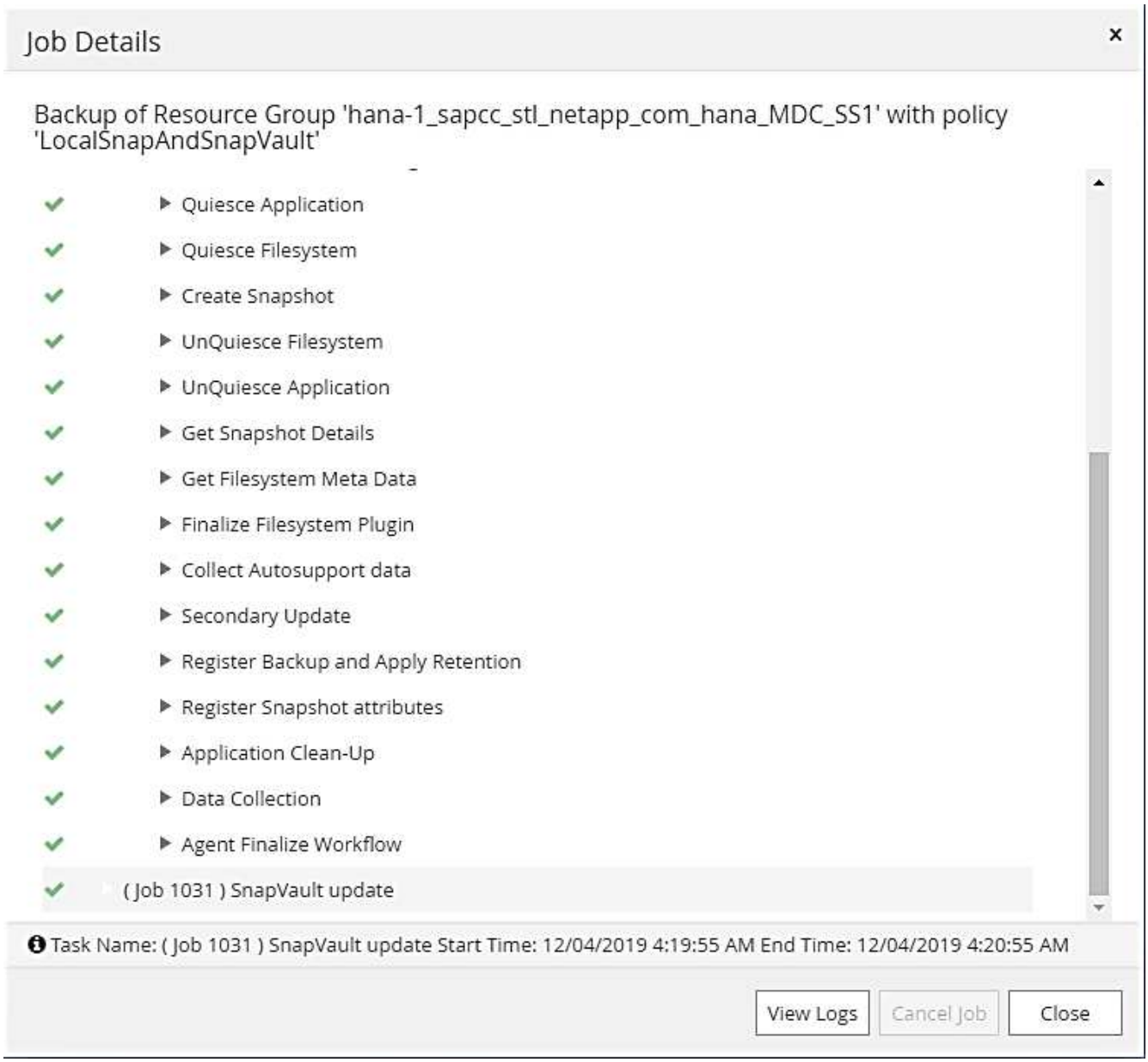

4. SAP HANA Studio では、バックアップカタログに新しいバックアップが表示されます。バックアップカタログのコメントフィールドと EBID フィールドには、 SnapCenter と同じバックアップ名が使用されます。

**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

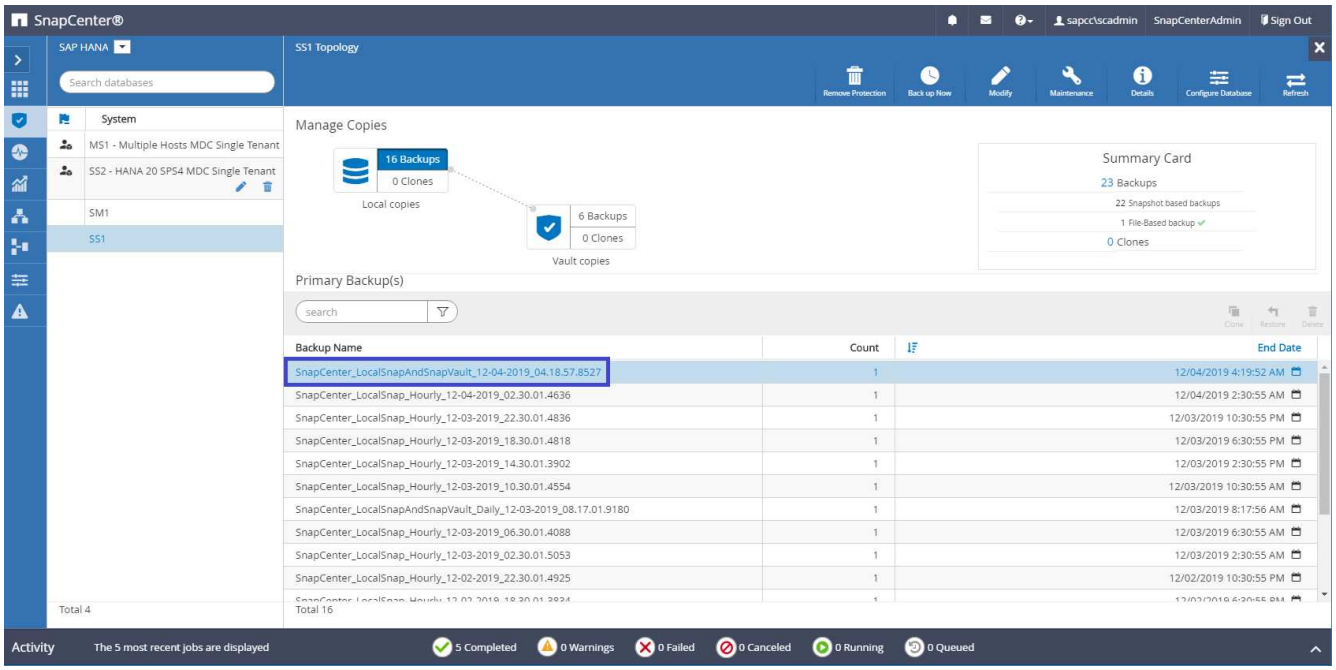



3. ジョブの詳細は、 [ アクティビティ ] 領域でジョブのアクティビティ行をクリックすると表示されます。

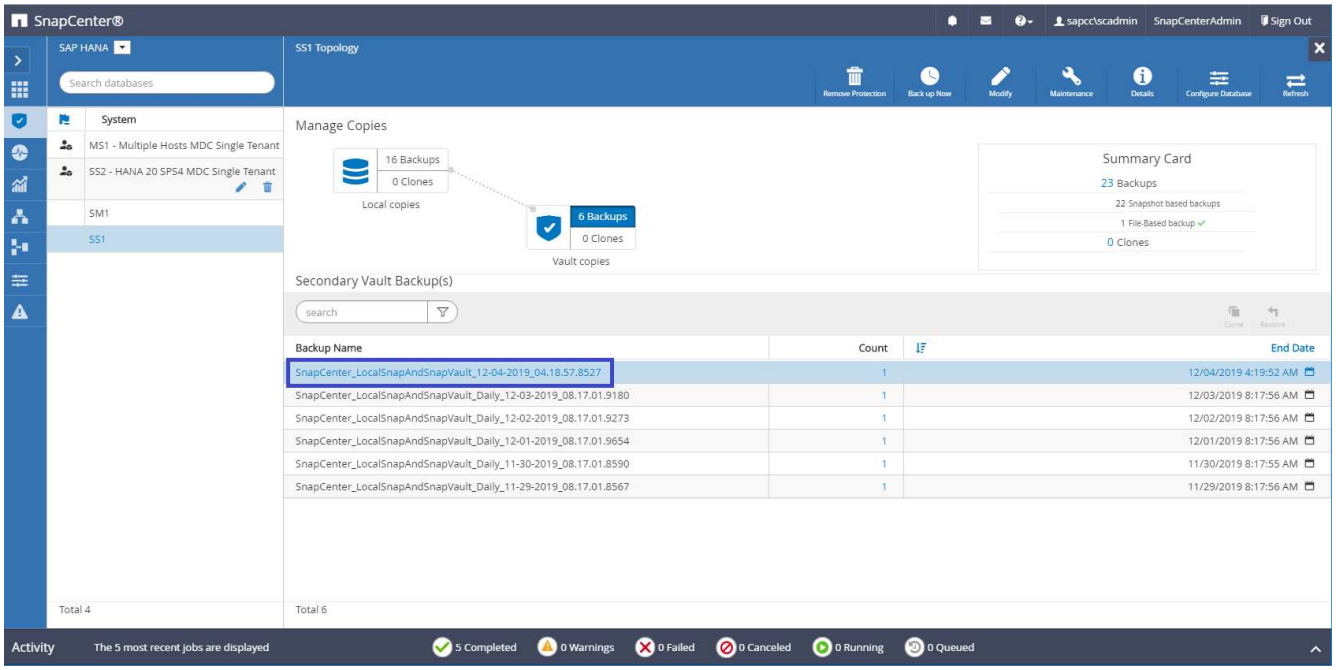



4. バックアップが完了すると、トポロジビューに新しいエントリが表示されます。バックアップ名は、セクションで定義したSnapshot名と同じ命名規則に従います。"「リソース保護の設定」"

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。

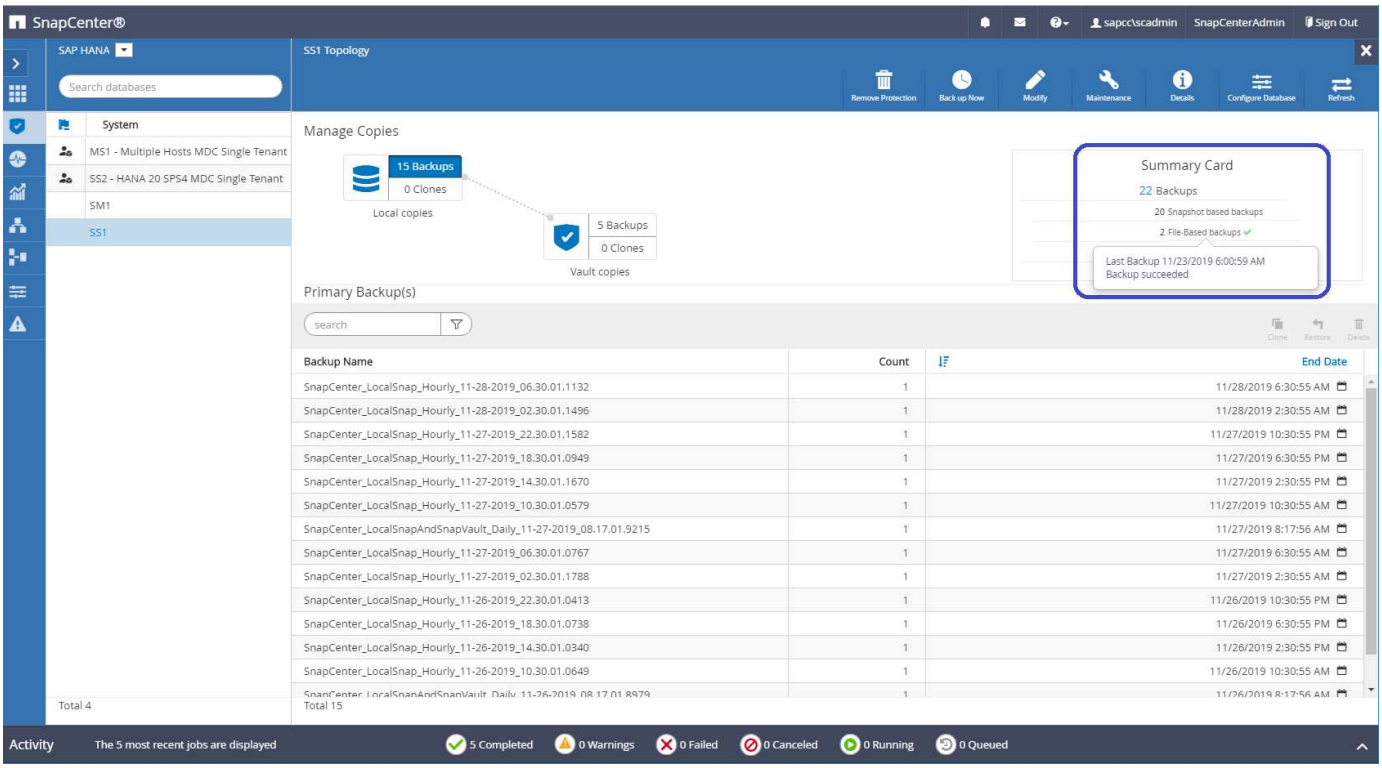
## ブロック整合性チェック

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

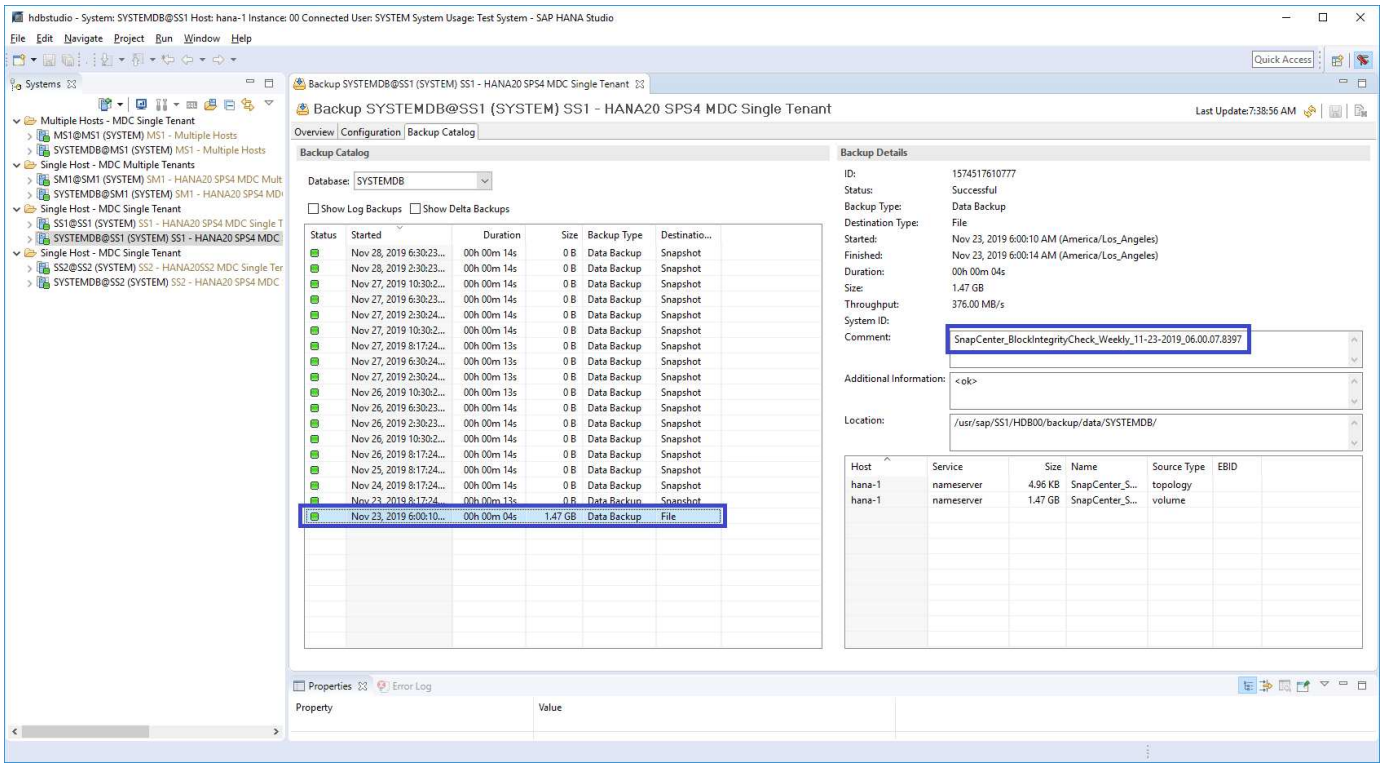
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"): y


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。

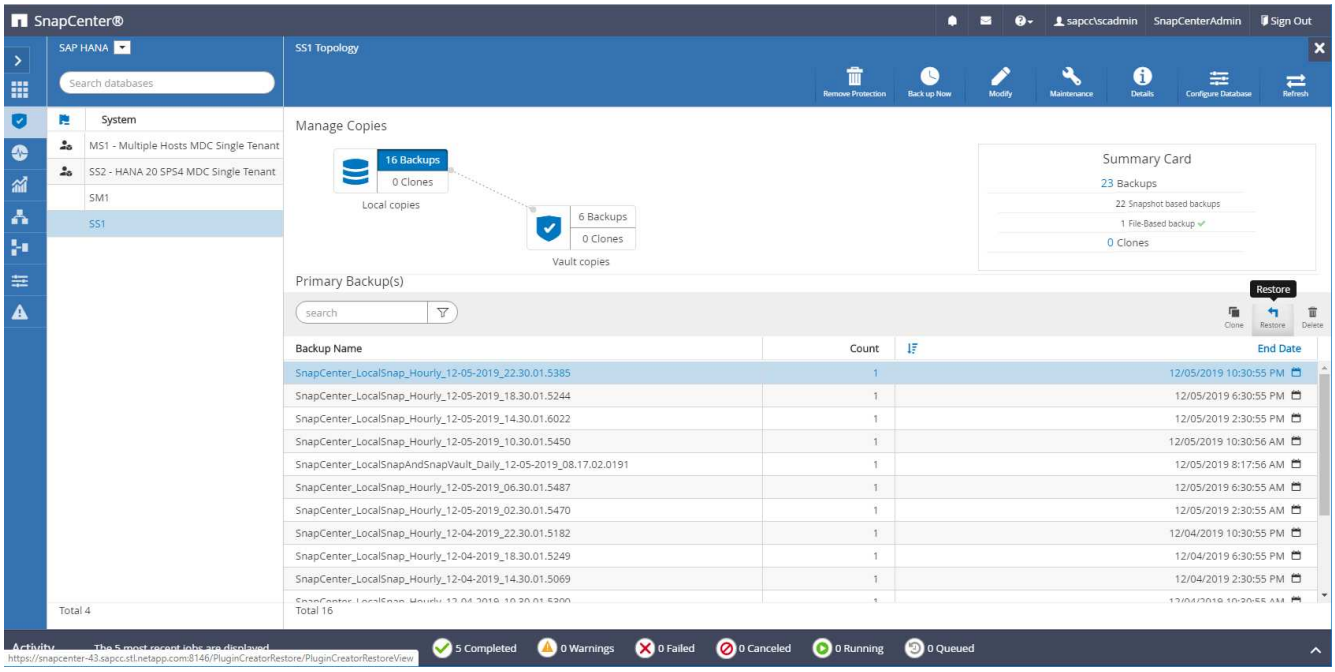
   c. HANA データベースが起動します。

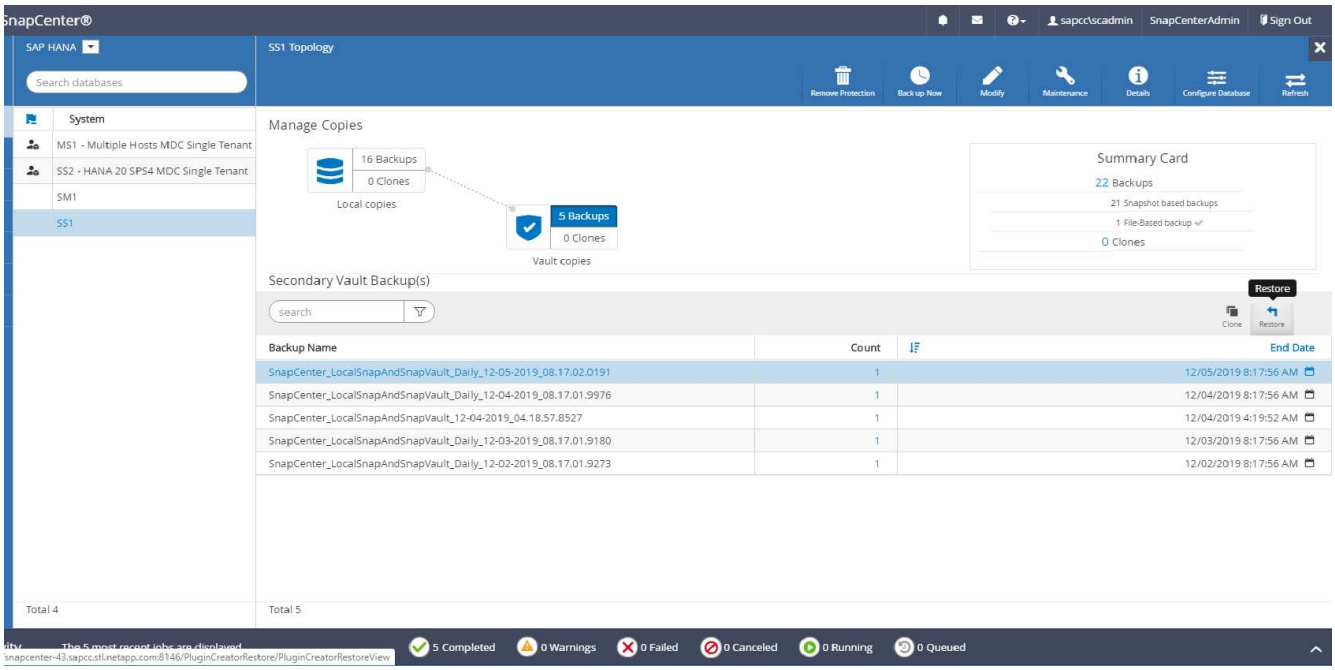
> リカバリなしを選択した場合は、 SnapCenter が終了し、システムとテナントデータベースのリカバリ処理を手動で実行する必要があります。

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。



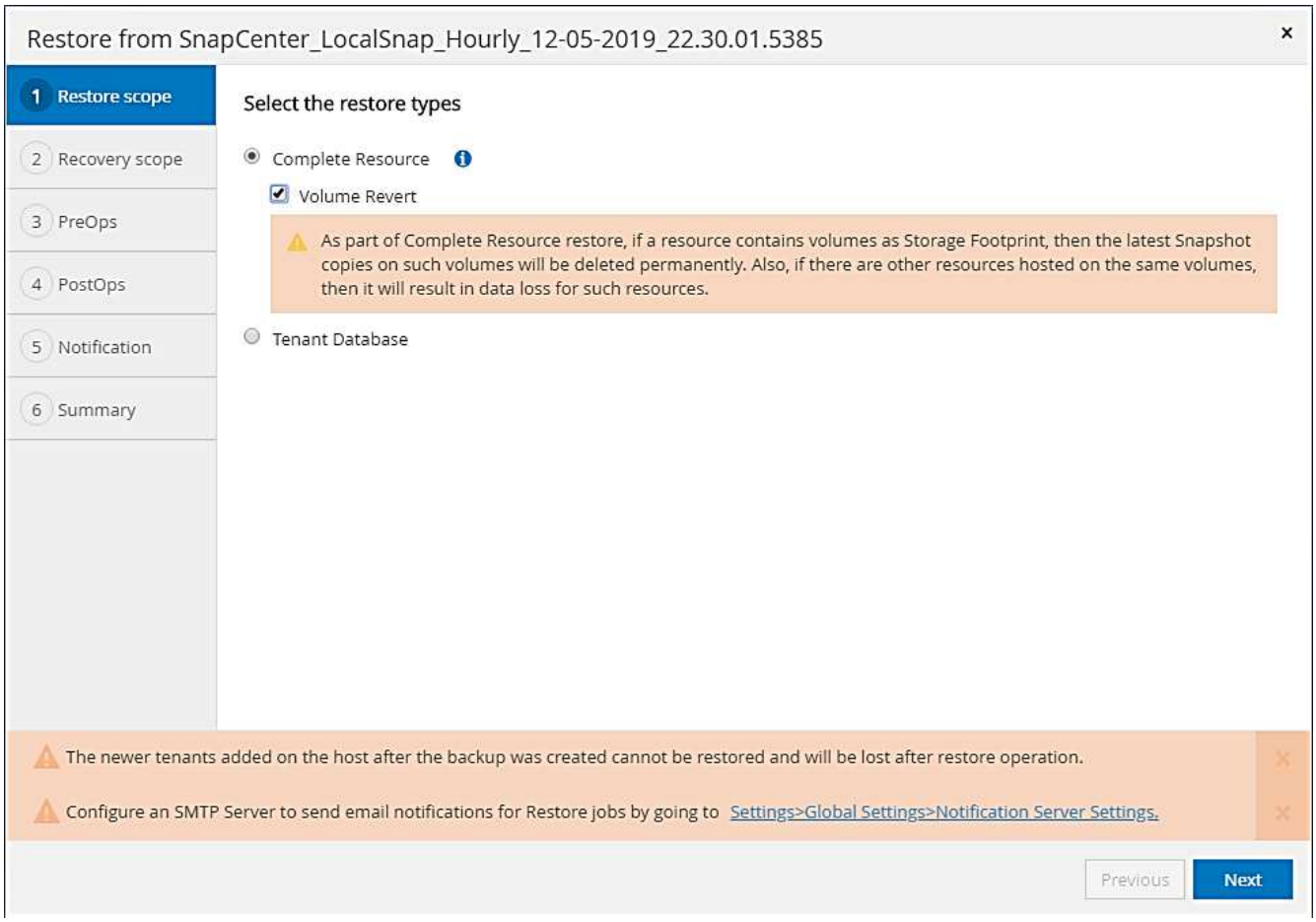



2. リストアの範囲とタイプを選択します。

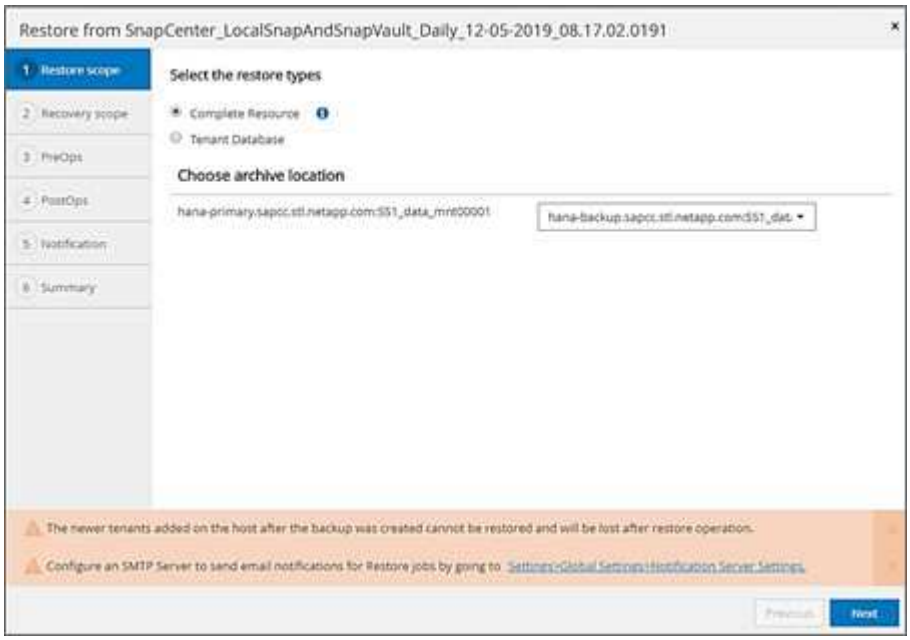
   次の 3 つのスクリーンショットは、 NFS を使用したプライマリからのリストア、 NFS を使用したセカンダリからのリストア、ファイバチャネル SAN を使用したプライマリからのリストアのリストアオプションを示しています。

   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。

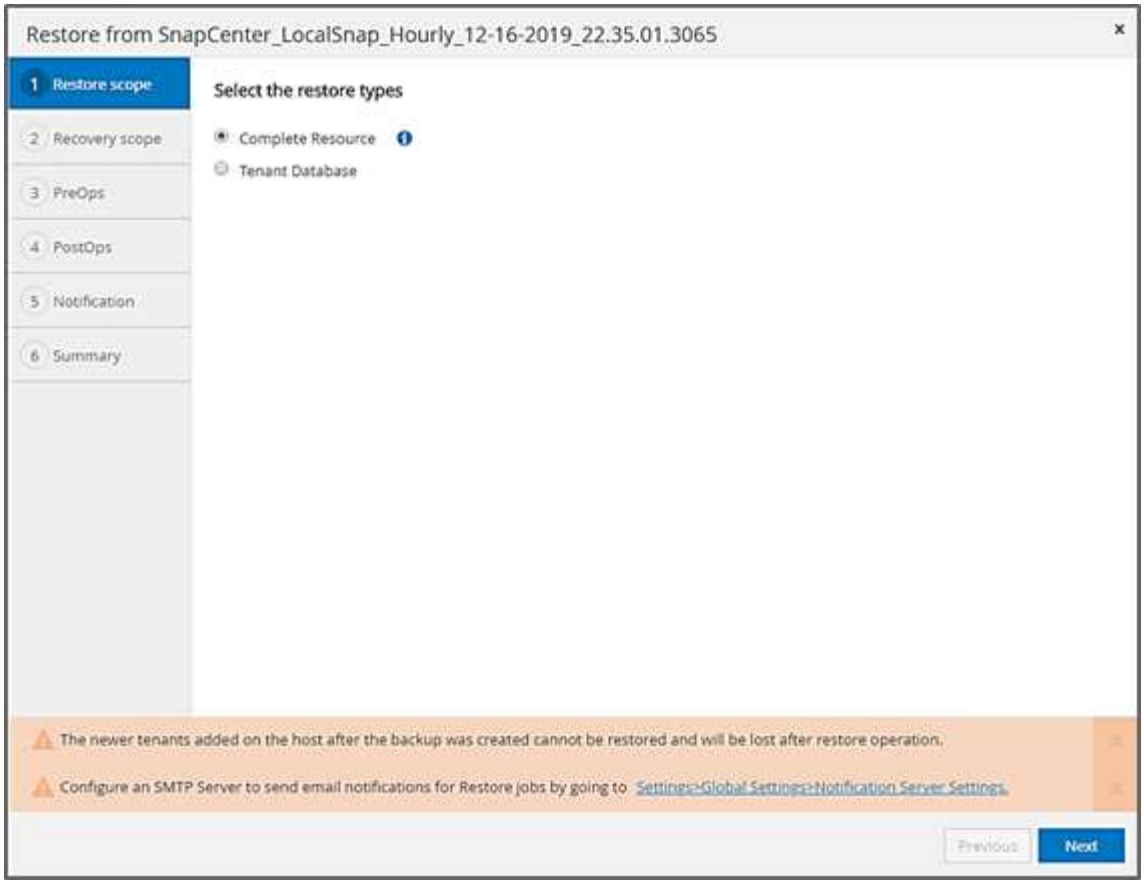
   ボリュームリバートオプションは、 NFS でプライマリからのリストア処理でのみ使用できます。




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。

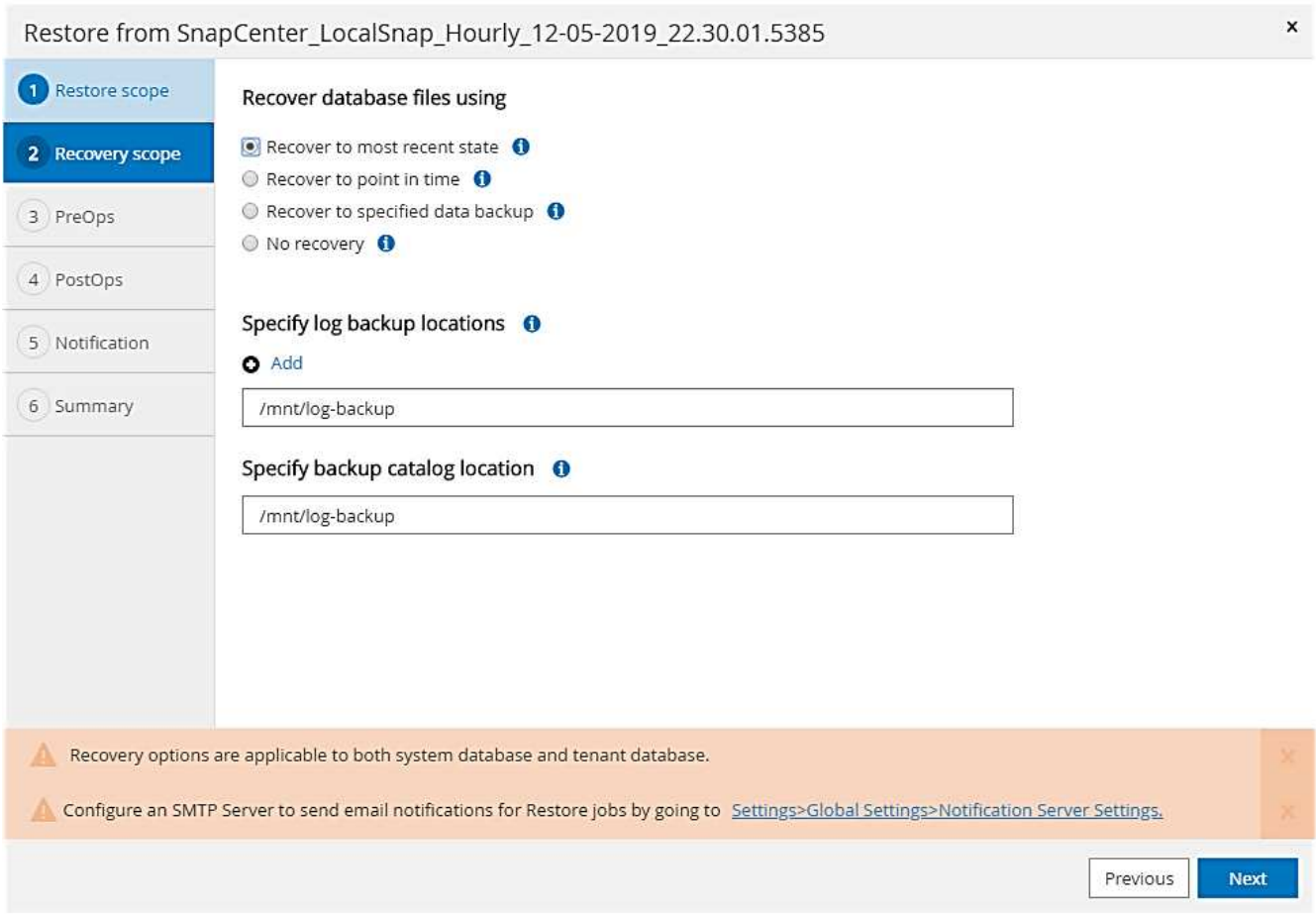



ファイバチャネル SAN を使用してプライマリストレージからリストアする場合のリストアタイプのオプション。

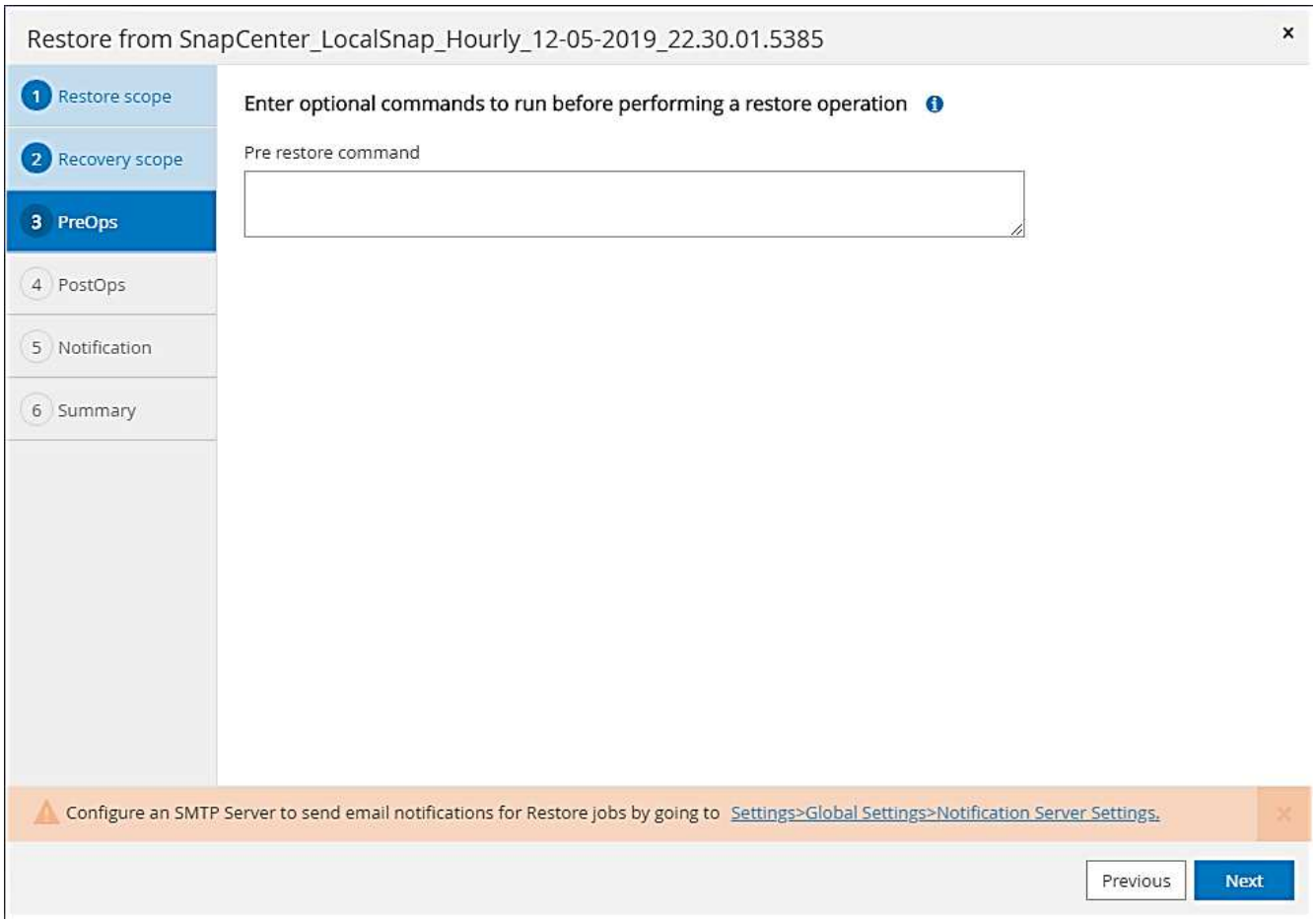



3. Recovery Scope を選択し、ログバックアップとカタログバックアップの場所を指定します。

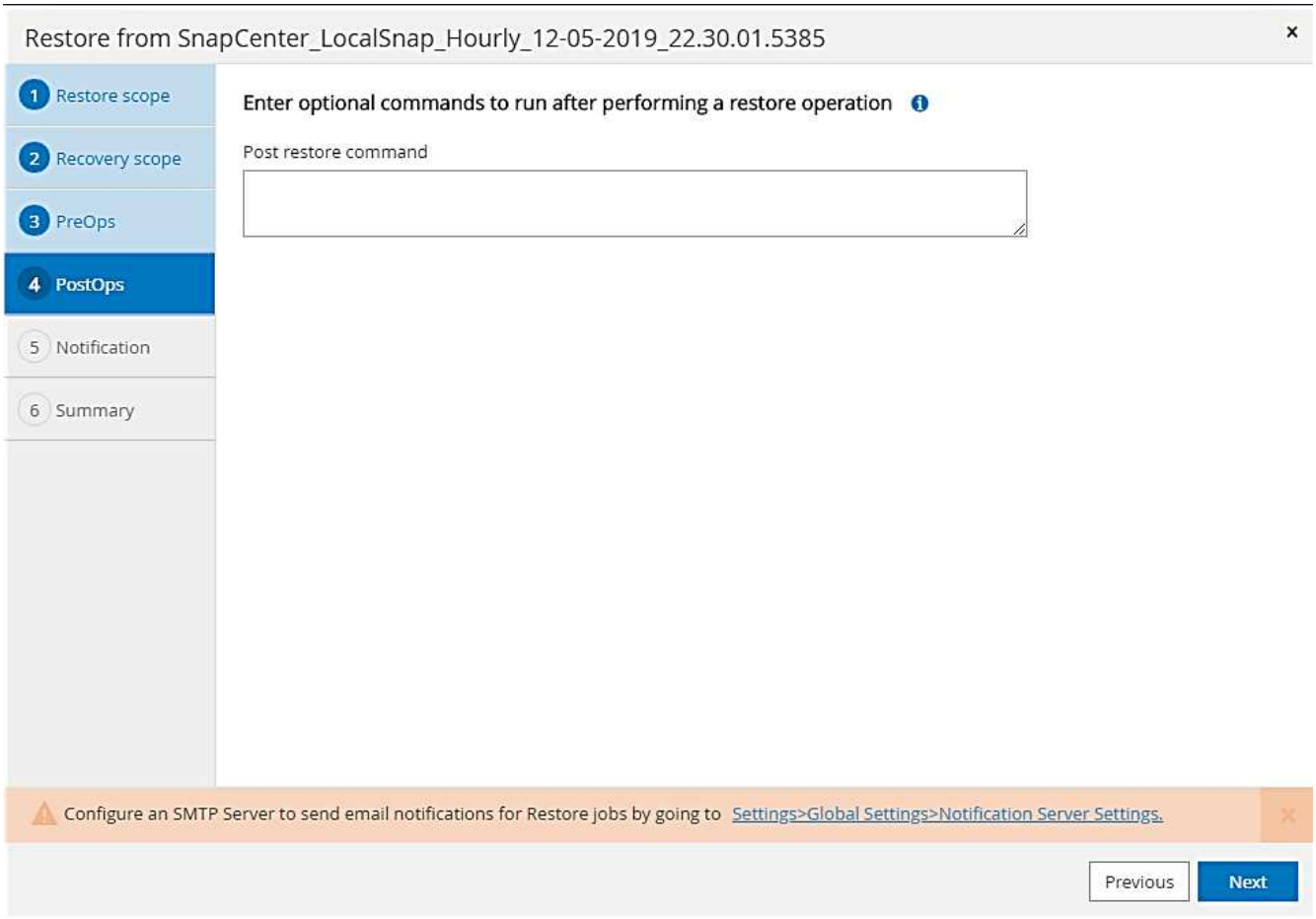
SnapCenter では、 HANA の global.ini ファイルのデフォルトパスまたは変更されたパスを使用して、ログとカタログのバックアップの場所が事前に入力されます。



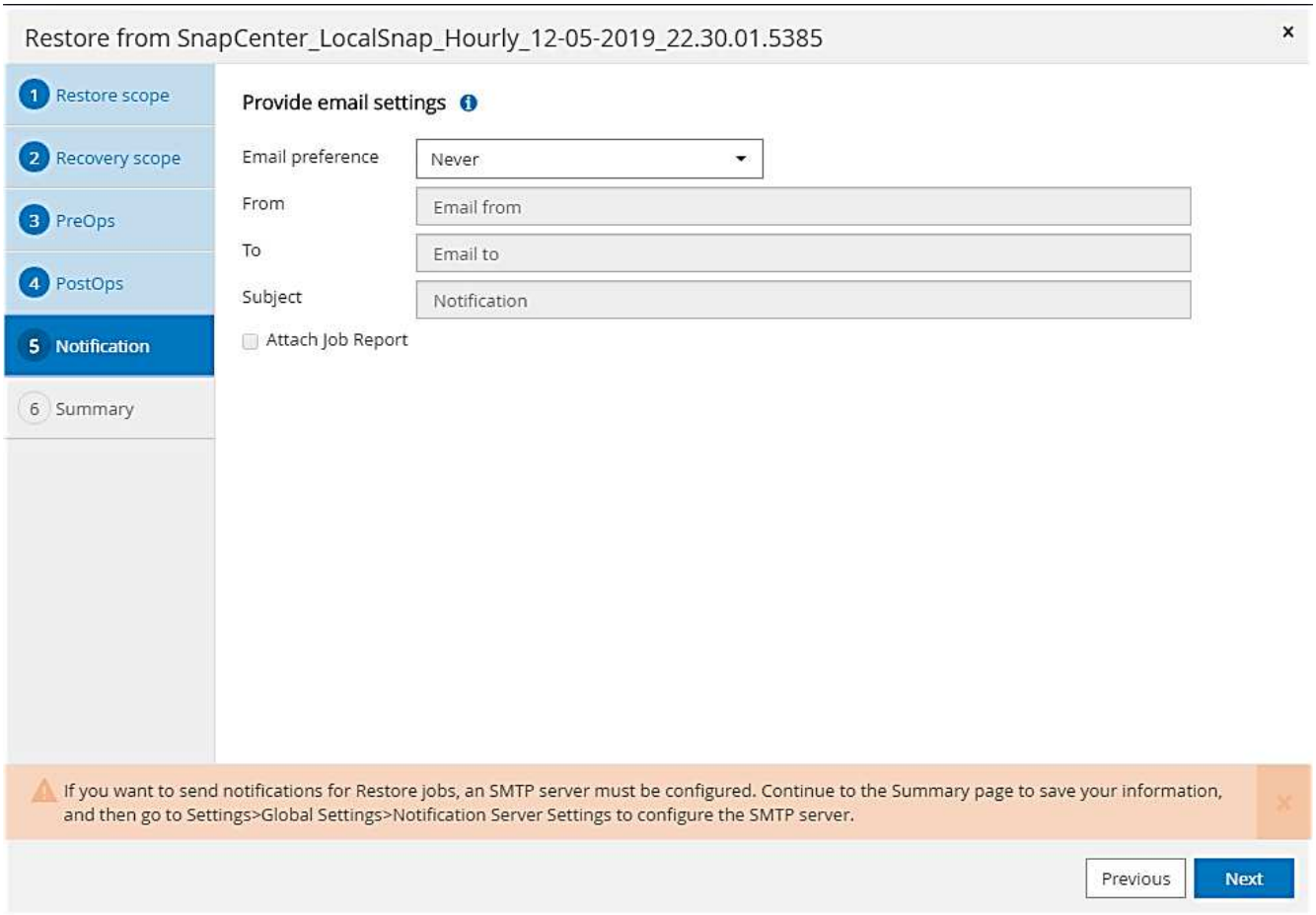

4. オプションのリストア前のコマンドを入力します



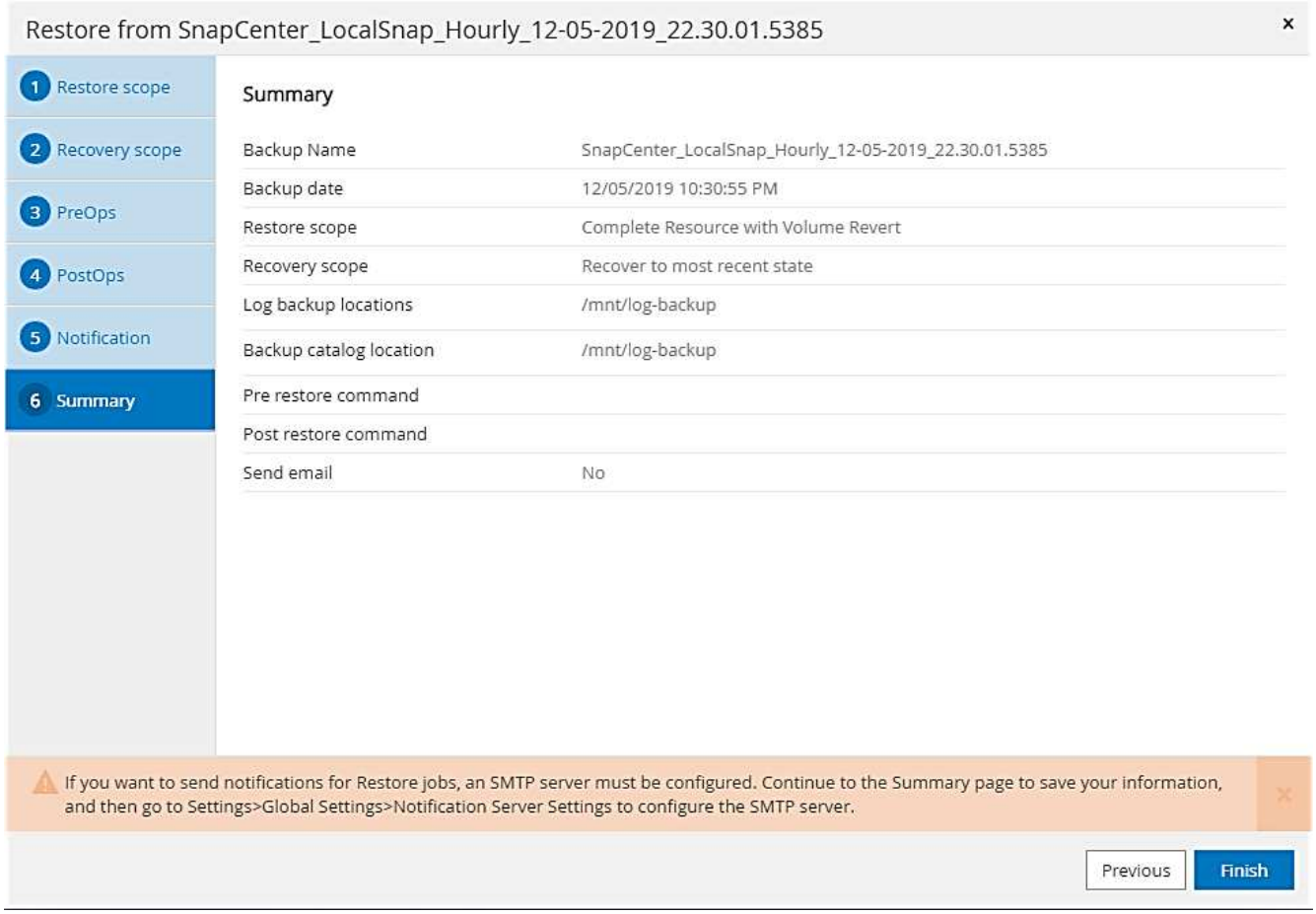

5. オプションのリストア後のコマンドを入力します。



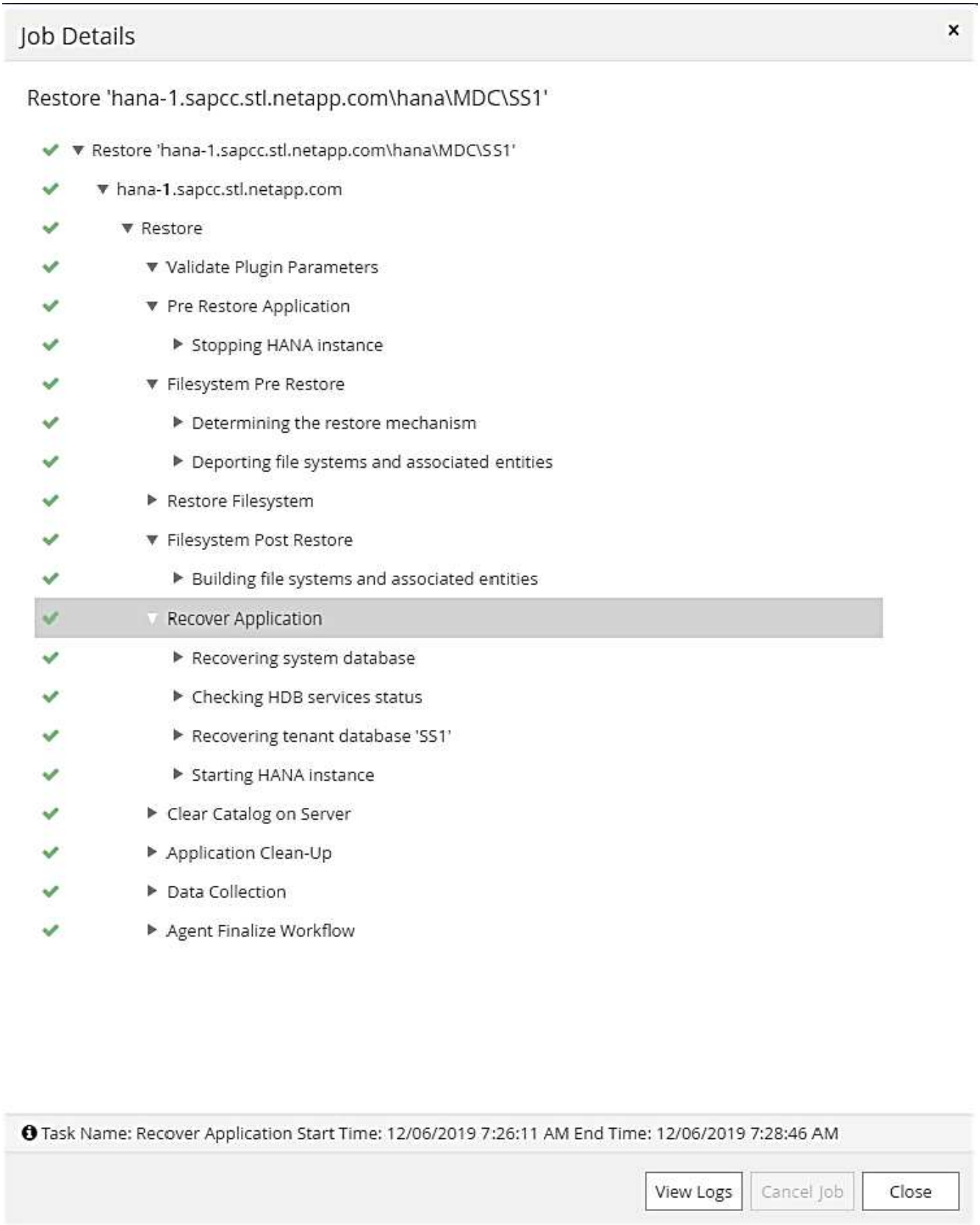

6. オプションの E メール設定を入力します。




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。

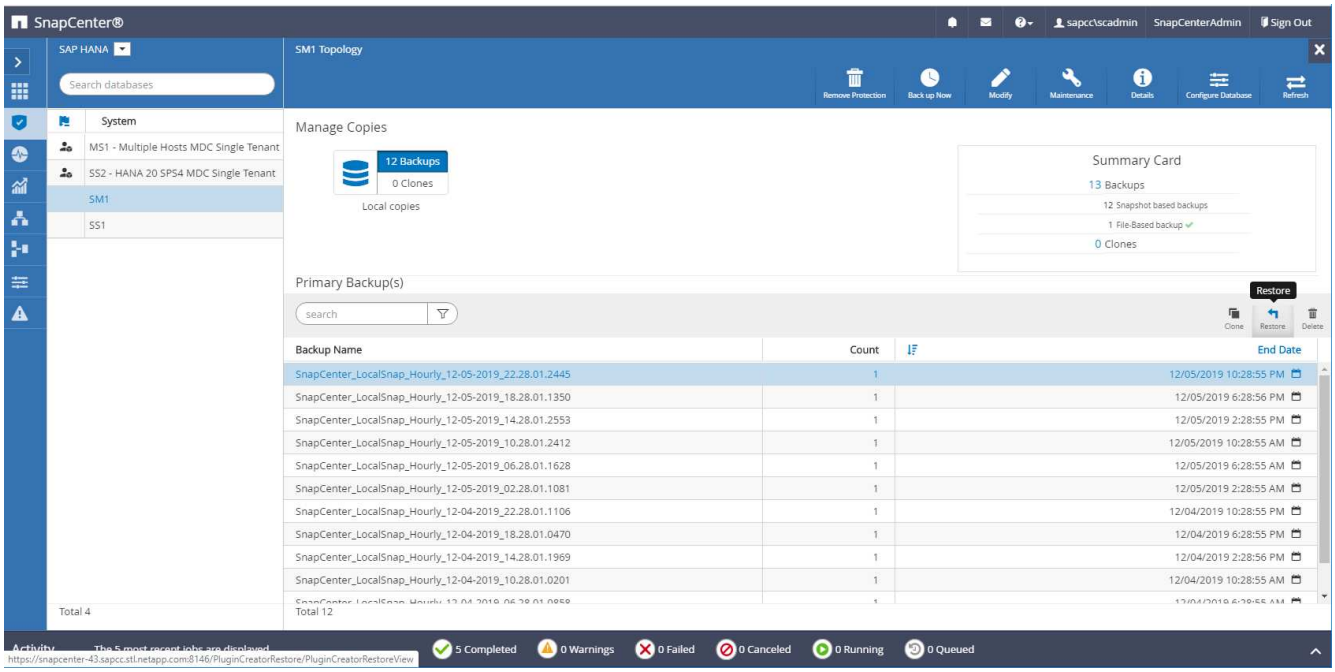
1. リストアおよびリカバリするテナントを停止します。
2. SnapCenter でテナントをリストアします。
   - プライマリストレージからリストアする場合、 SnapCenter は次の処理を実行します。
     - * NFS. * ストレージの単一ファイルの SnapRestore 操作は、テナントデータベースのすべてのファイルに対応しています。
     - * SAN. * LUN のクローンを作成してデータベースホストに接続し、テナント・データベースのすべてのファイルをコピーします。
   - セカンダリストレージからリストアする場合、 SnapCenter は次の処理を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

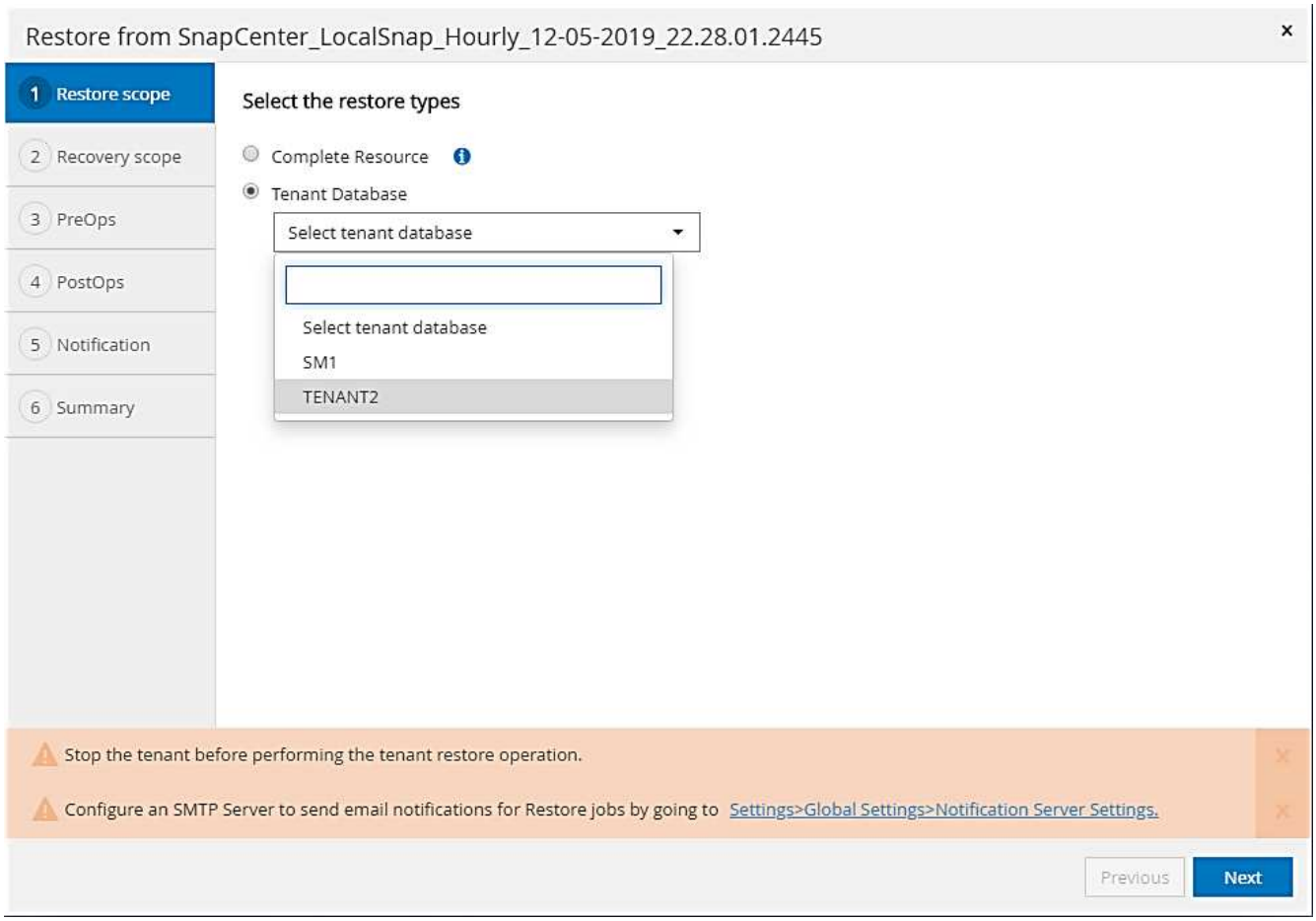
```
sm1adm@hana-2:/usr/sap/SM1/HDB00> hdbsql -U SYSKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql=>
hdbsql SYSTEMDB=> alter system stop database tenant2;
0 rows affected (overall time 14.215281 sec; server time 14.212629 sec)
hdbsql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

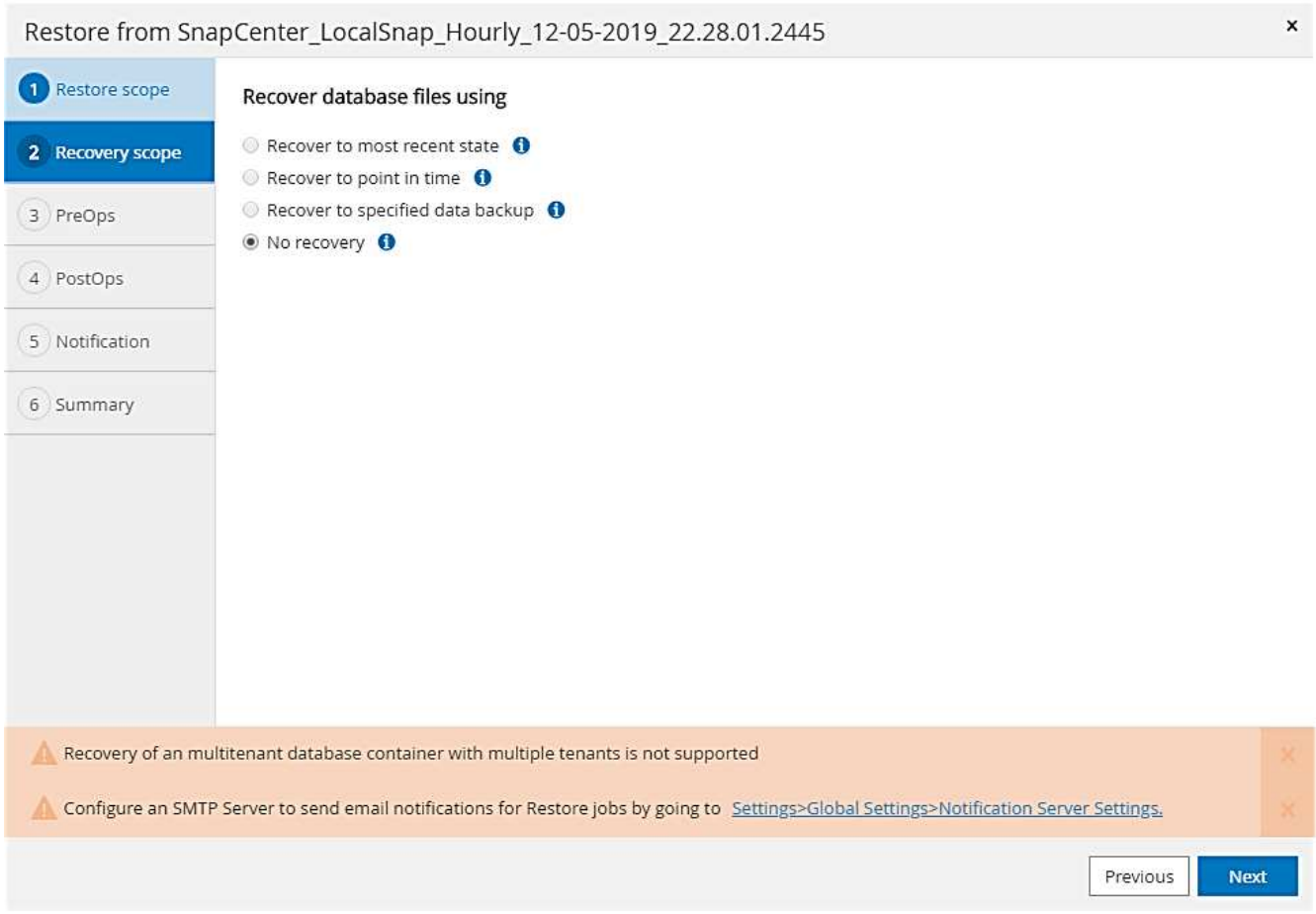



3. リストアするテナントを選択します。

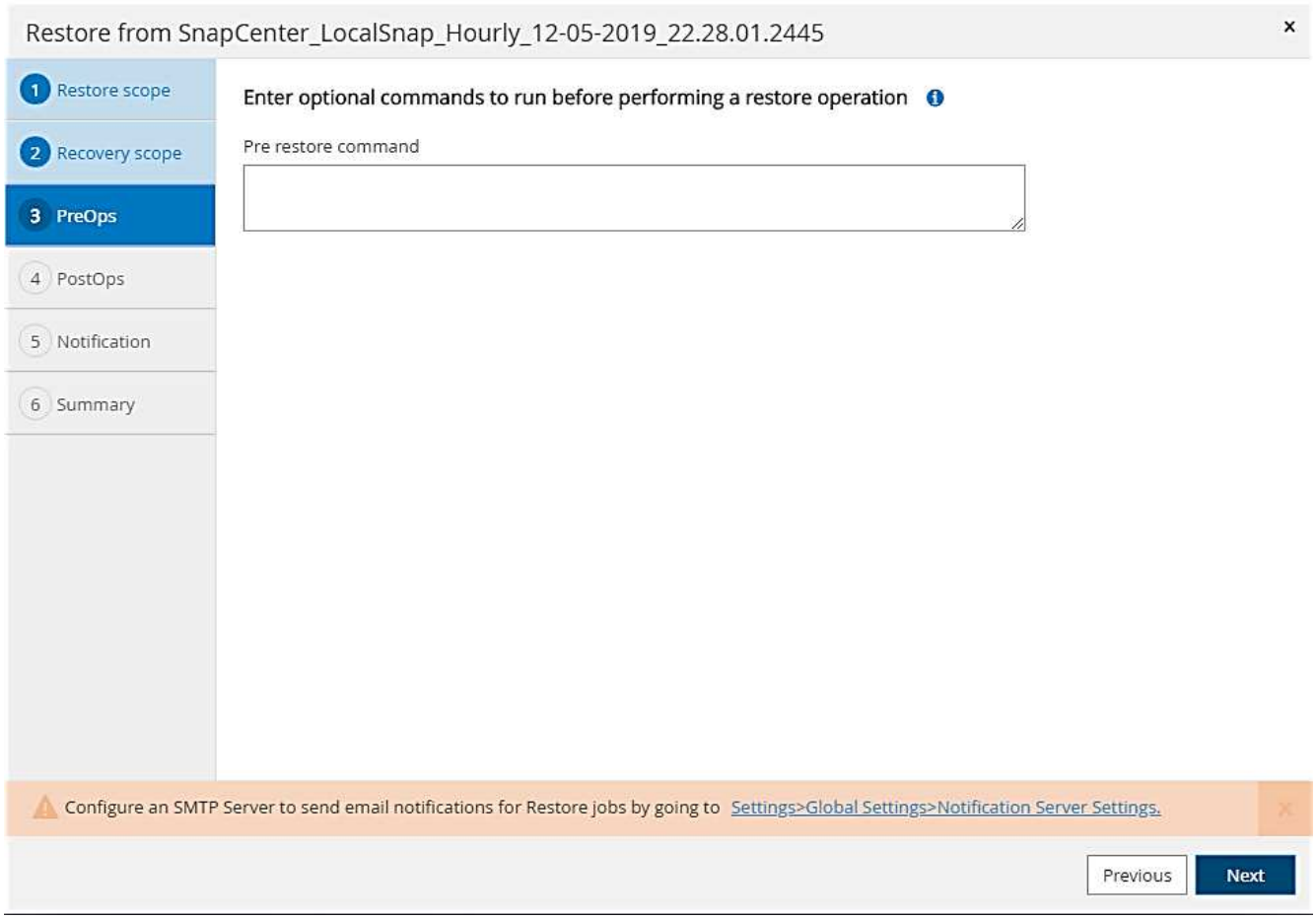
SnapCenter に、選択したバックアップに含まれるすべてのテナントのリストが表示されます。



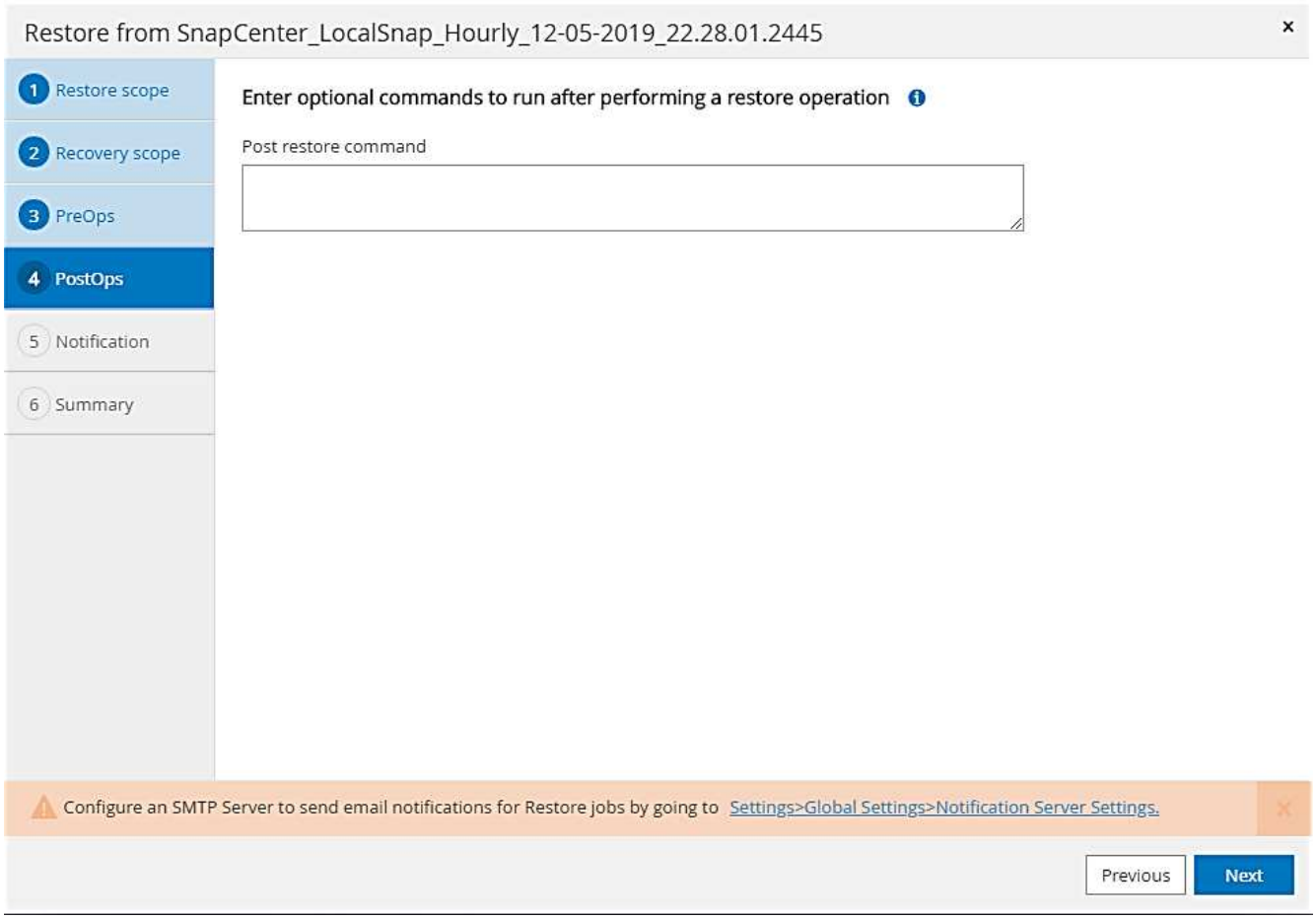
シングルテナントリカバリは、 SnapCenter 4.3 ではサポートされていません。リカバリは事前に選択されておらず、変更することはできません。



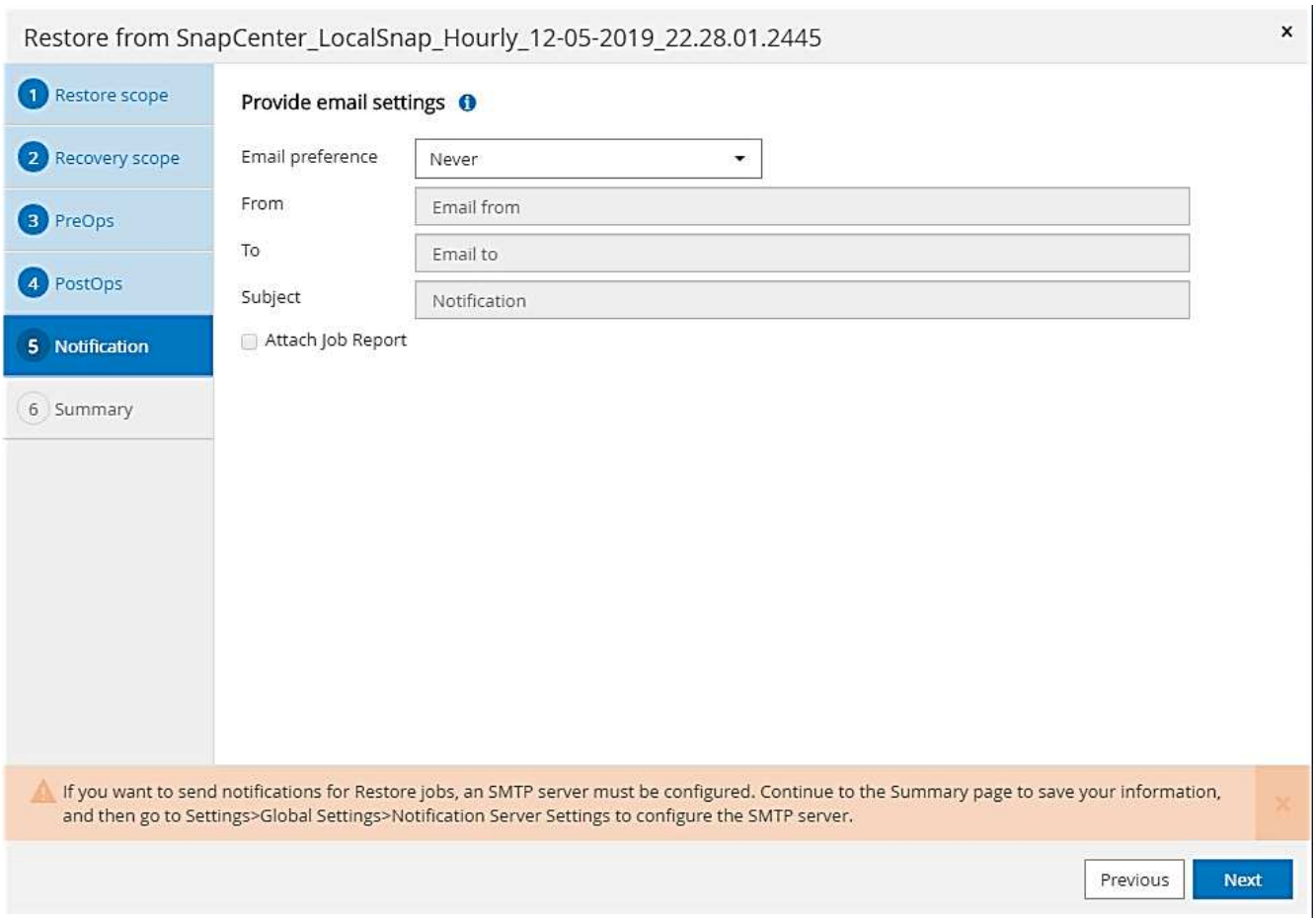

4. オプションのリストア前のコマンドを入力します



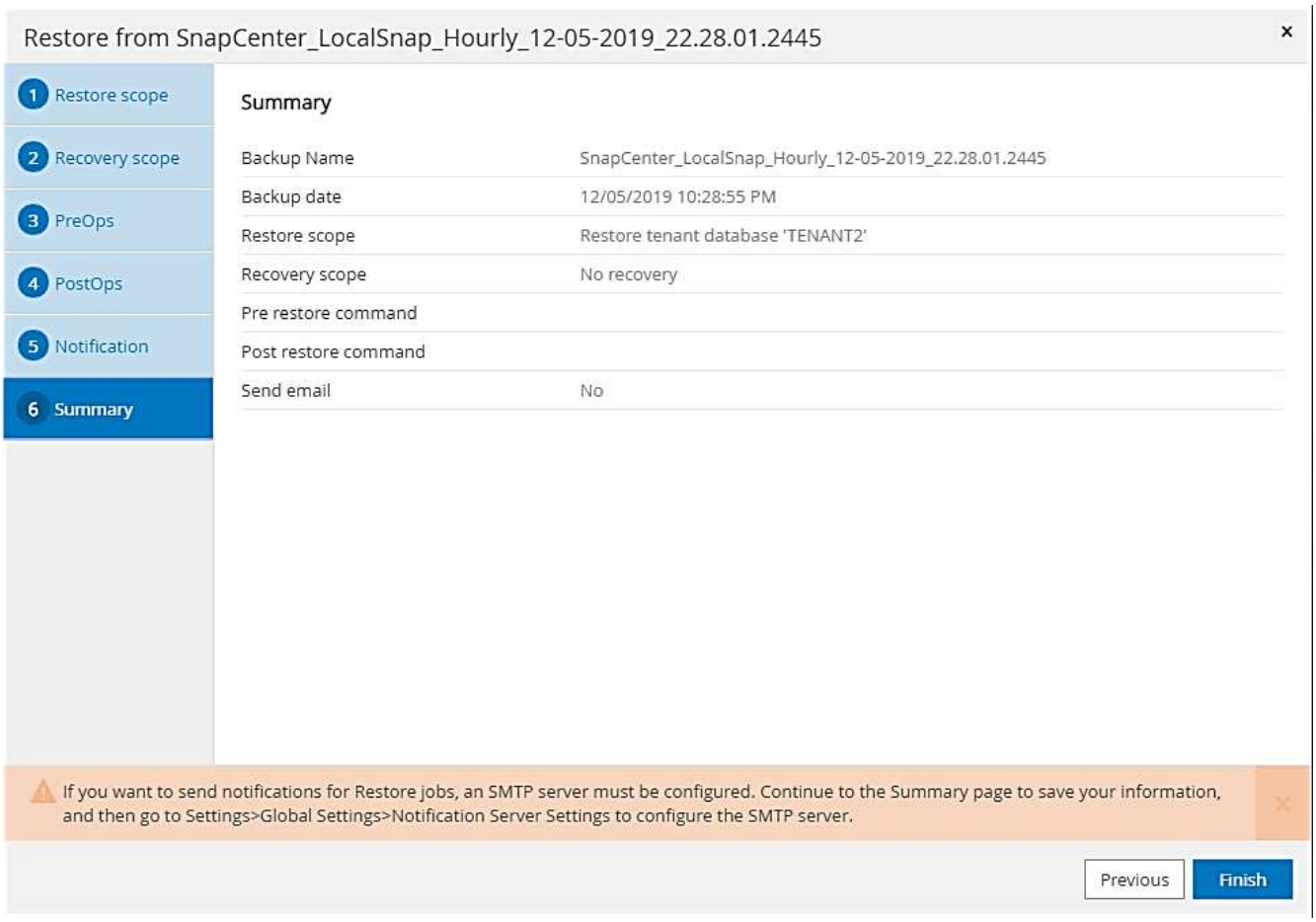

5. オプションのリストア後のコマンドを入力します。



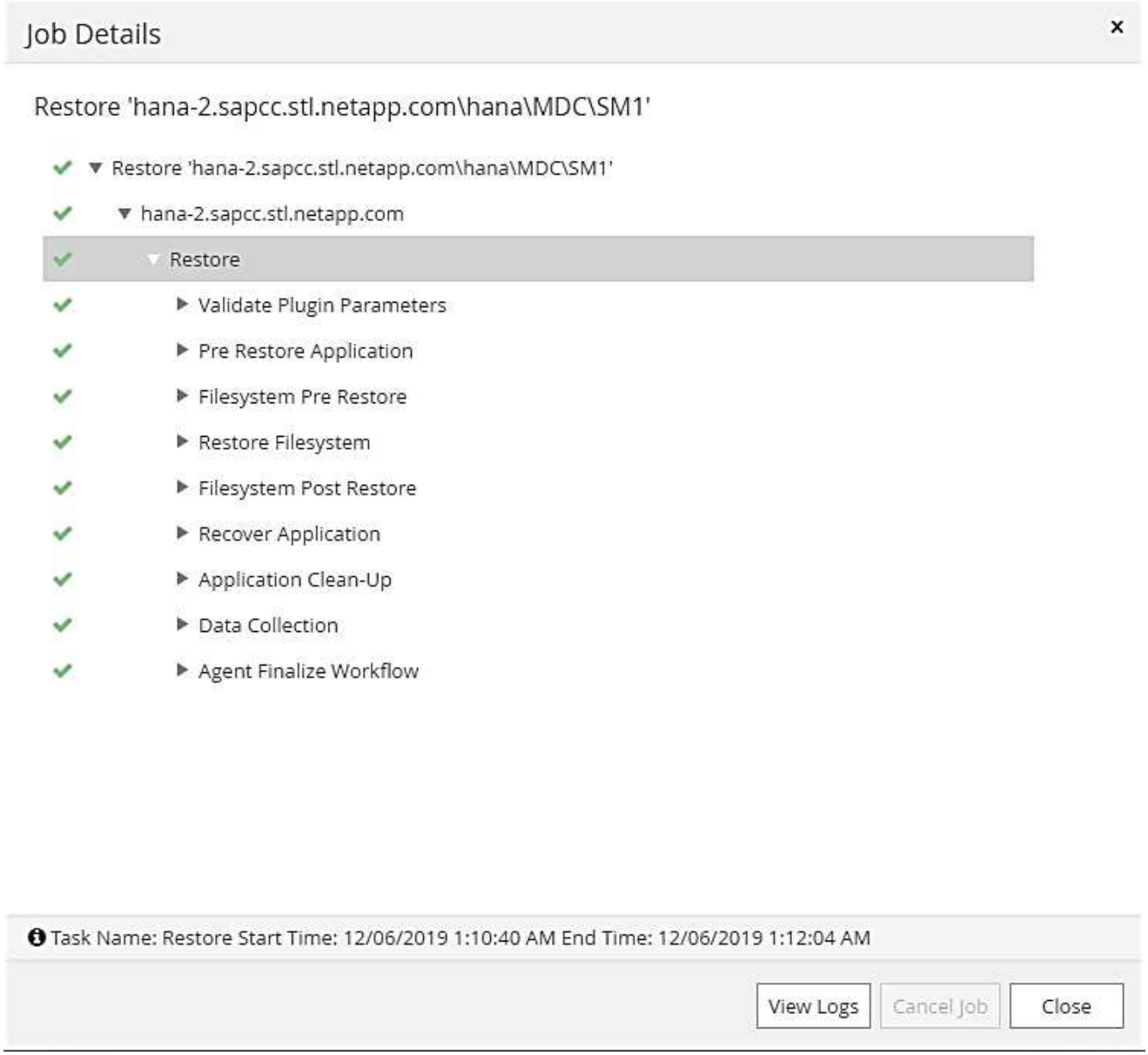

6. オプションの E メール設定を入力します。




7. リストア処理を開始するには、 [ 完了 ] をクリックします。



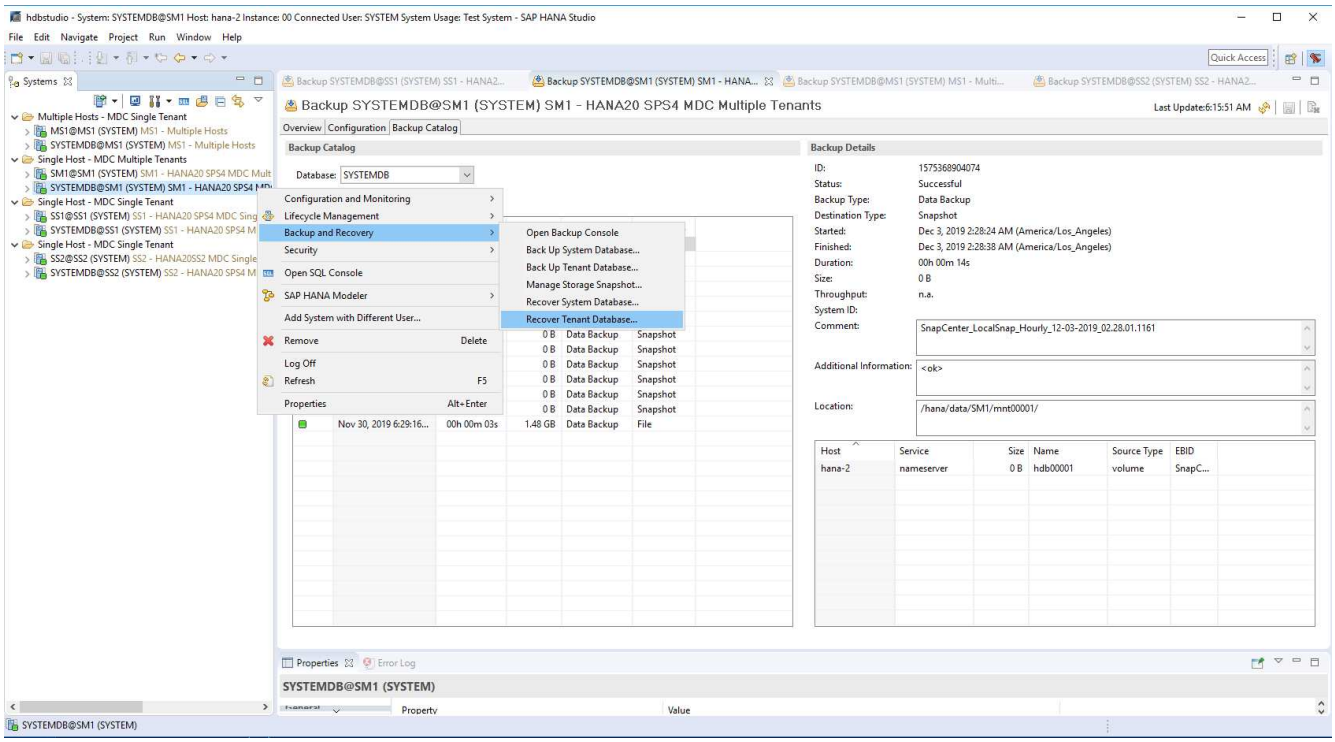

リストア処理は SnapCenter によって実行されます。この例は、リストアジョブのジョブの詳細を表示します。



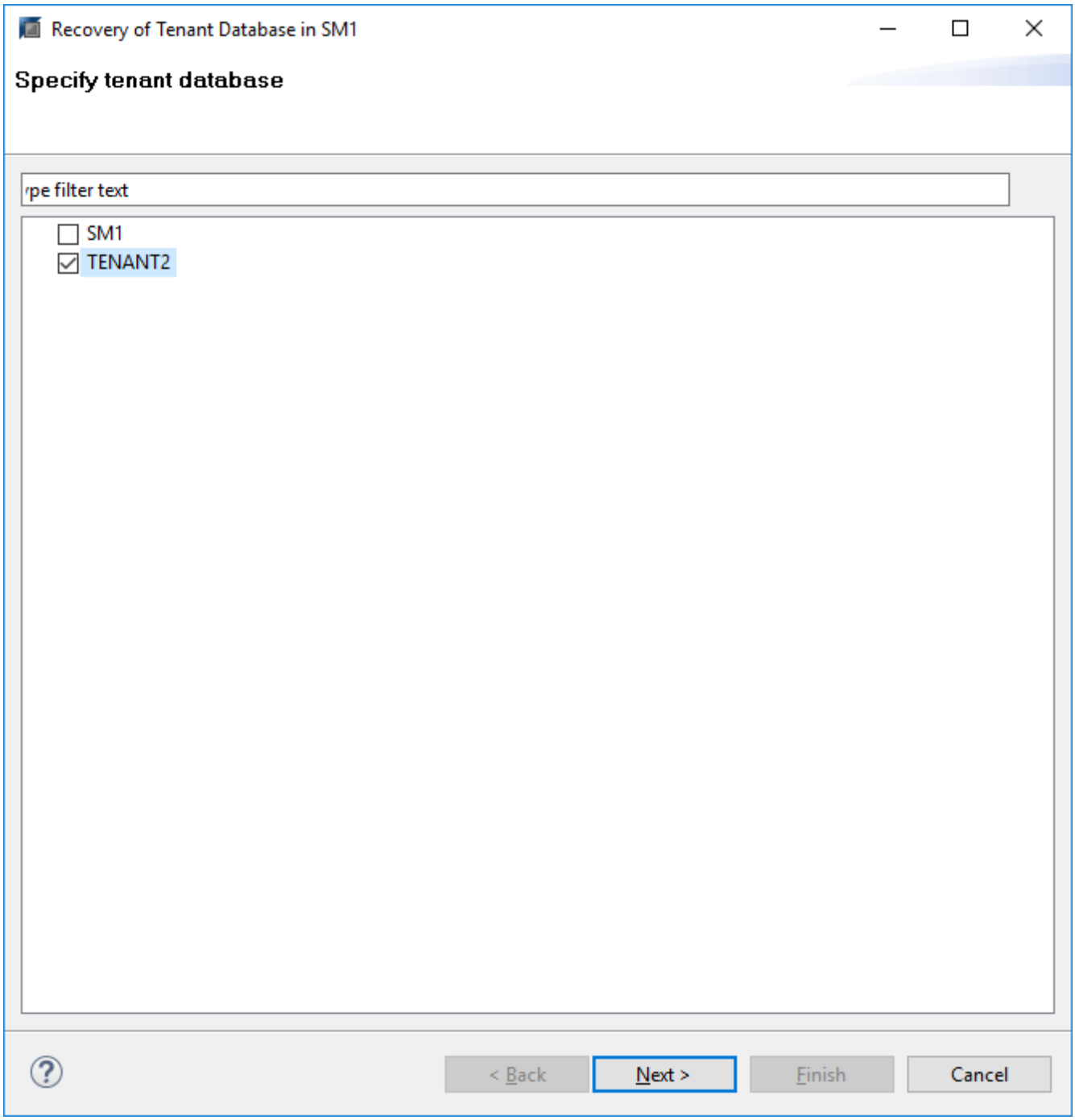

テナントのリストア処理が終了すると、テナントに関連するデータのみがリストアされます。HANA データベースホストのファイルシステムで、リストアしたデータファイルとテナントの Snapshot バックアップ ID ファイルを使用できます。

```
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>
```

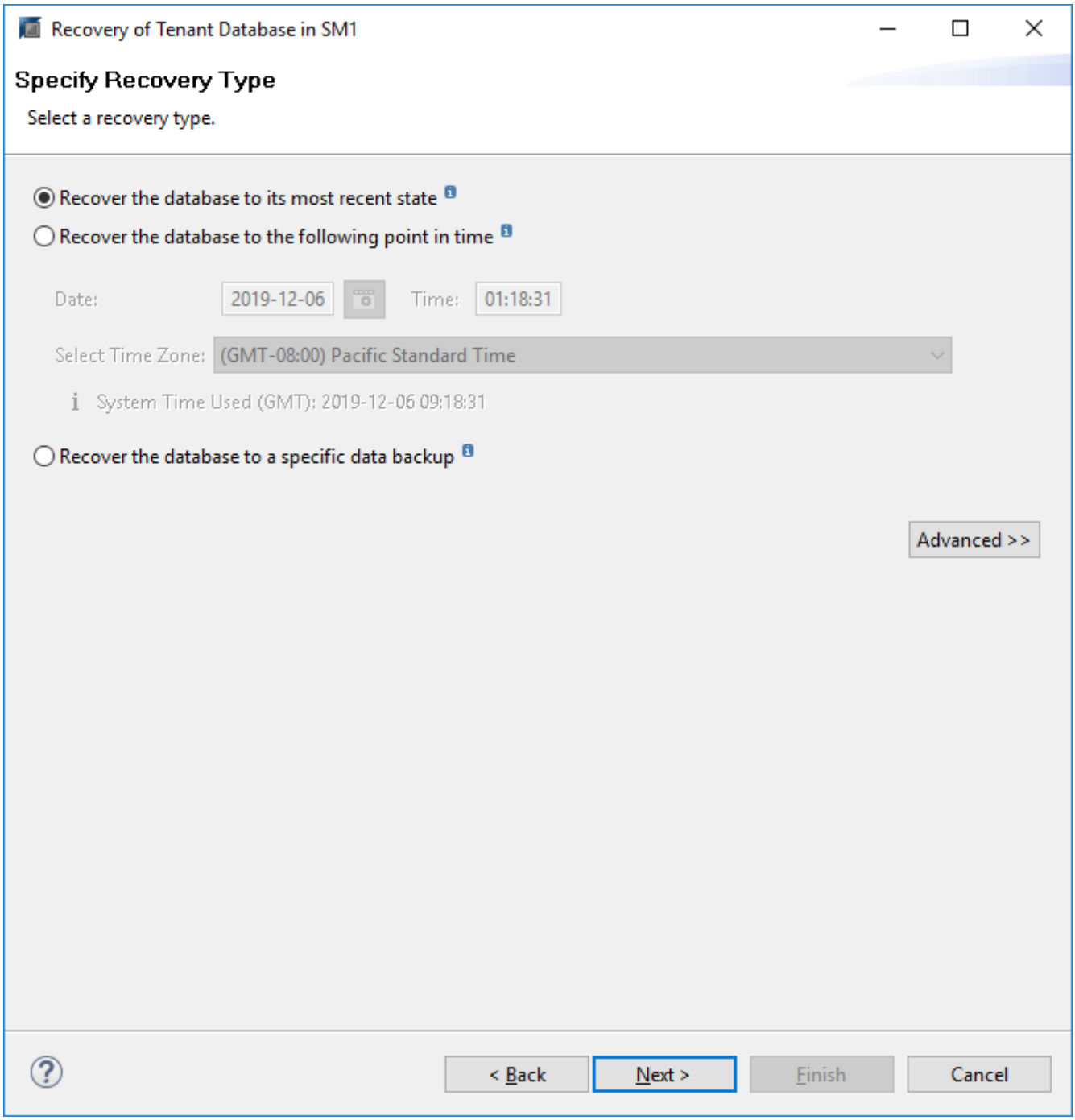
8. HANA Studio でリカバリを開始します。



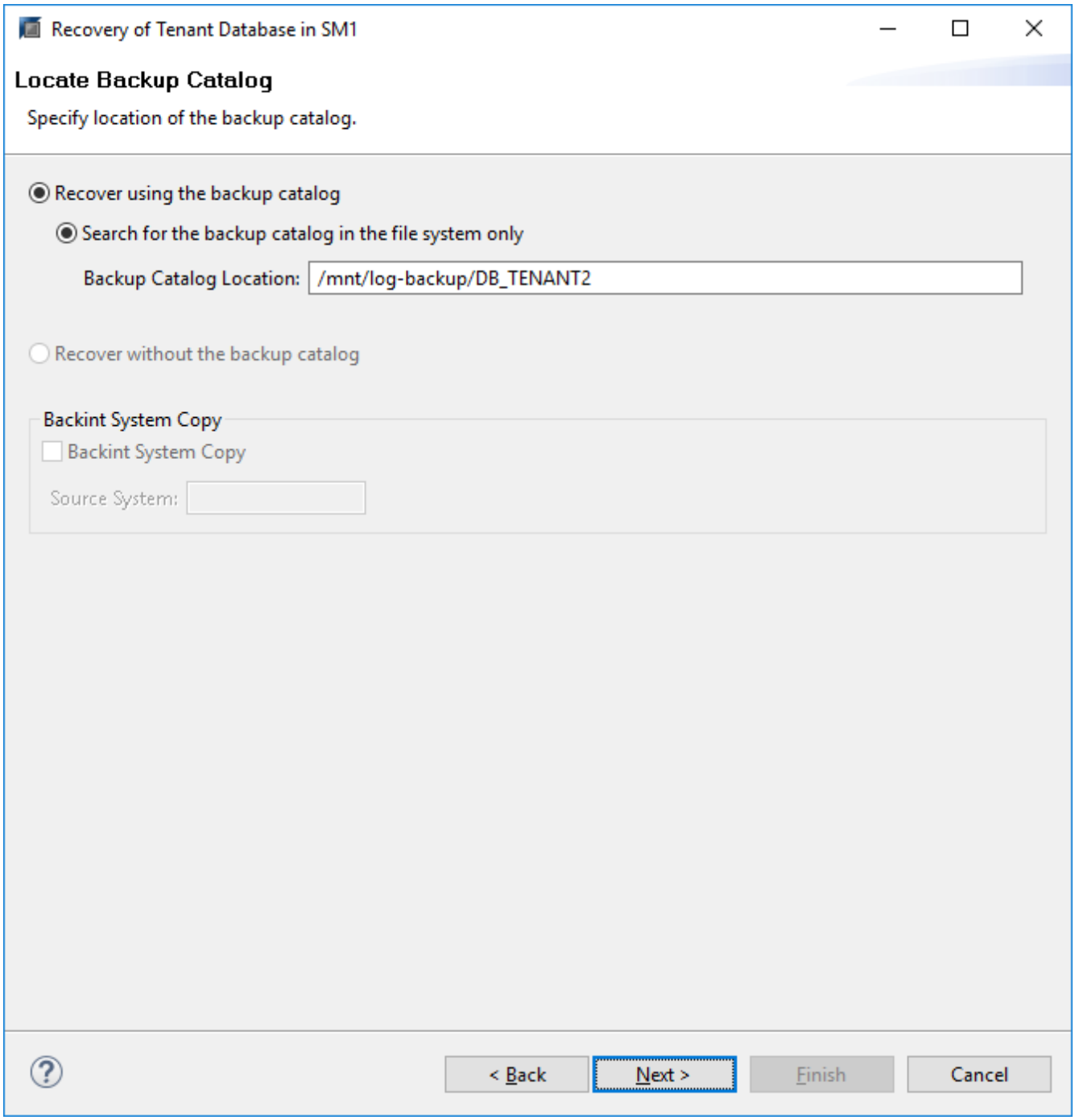

9. テナントを選択します。

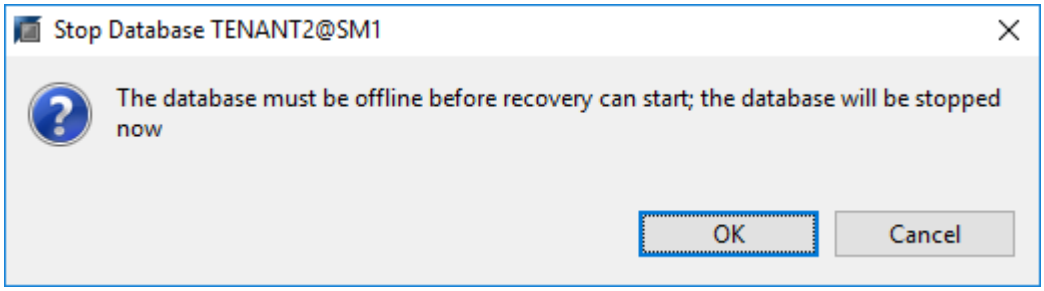



10. リカバリのタイプを選択します。



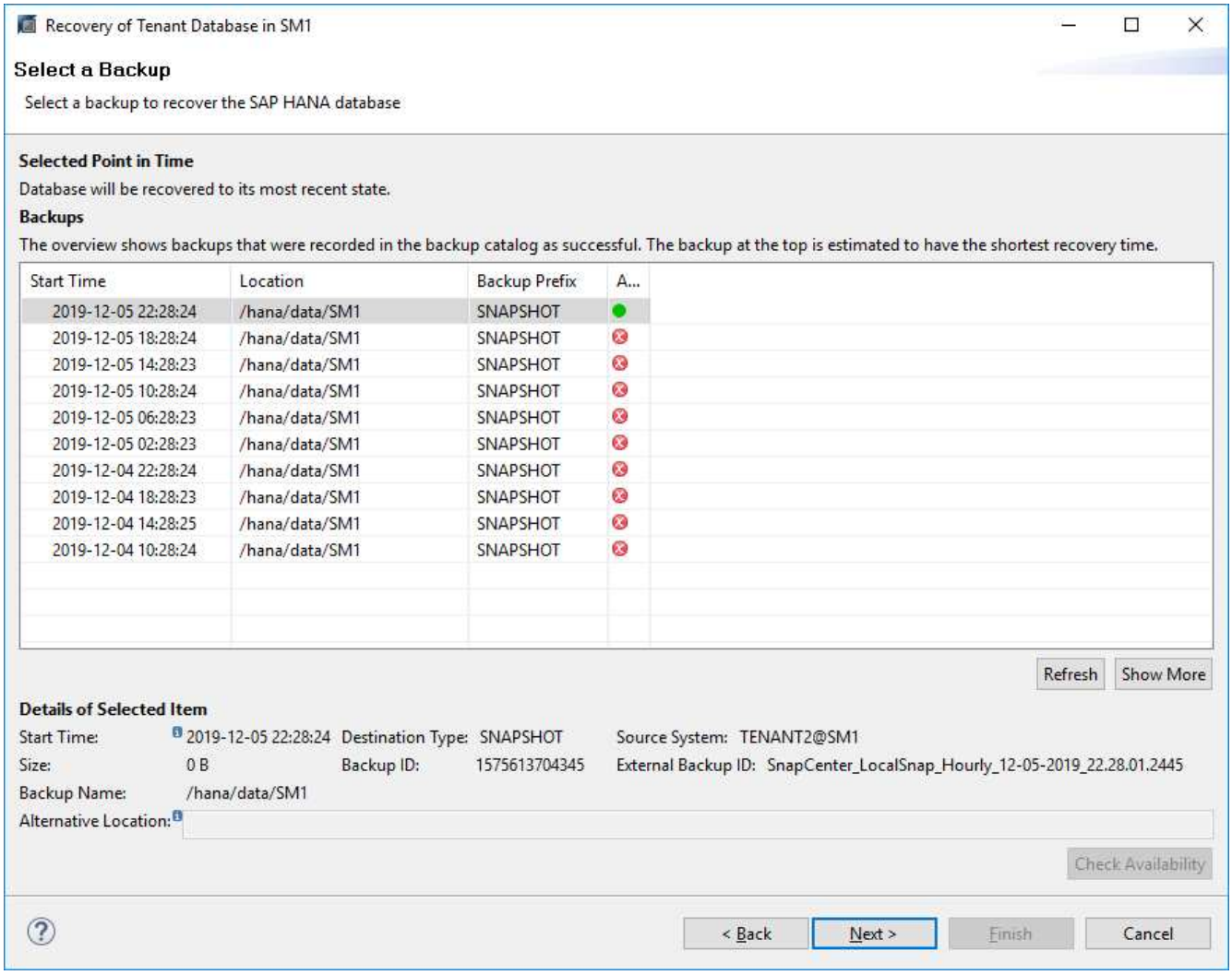

11. バックアップカタログの場所を指定します。



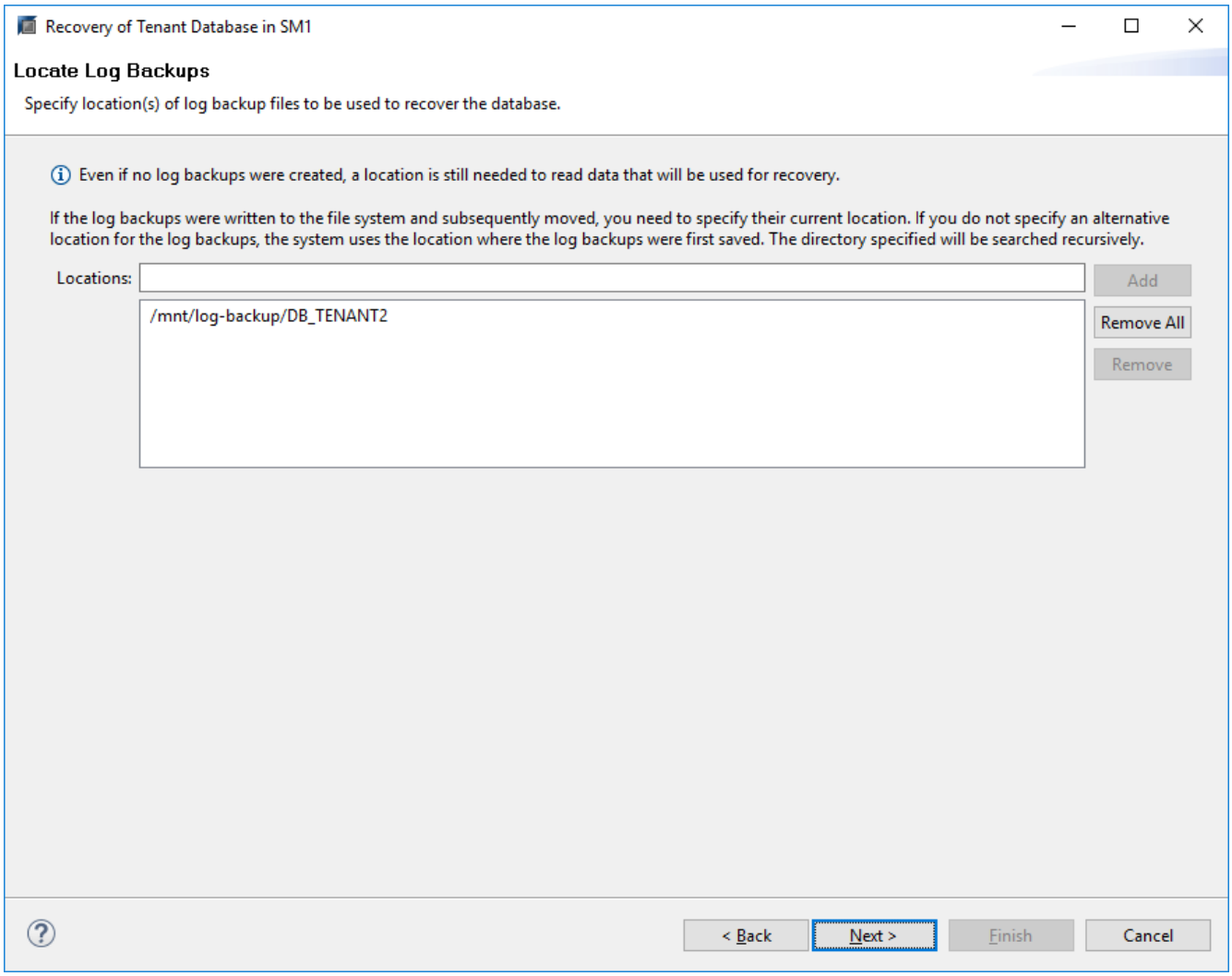




バックアップカタログ内で、リストアされたバックアップが緑のアイコンで強調表示されます。外部バックアップ ID には、 SnapCenter で以前に選択されたバックアップ名が表示されます。

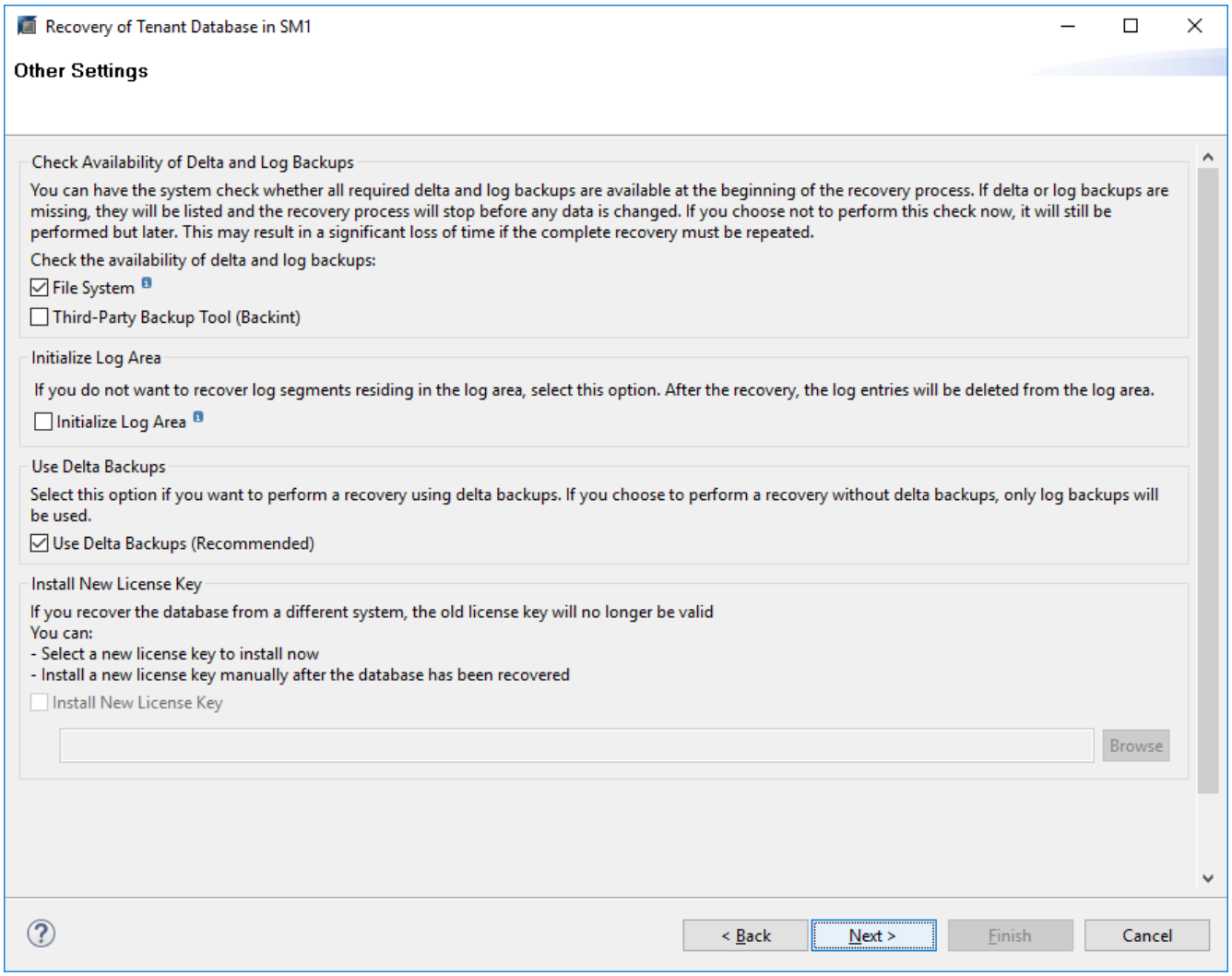
12. 緑のアイコンが表示されたエントリを選択し、次へをクリックします。



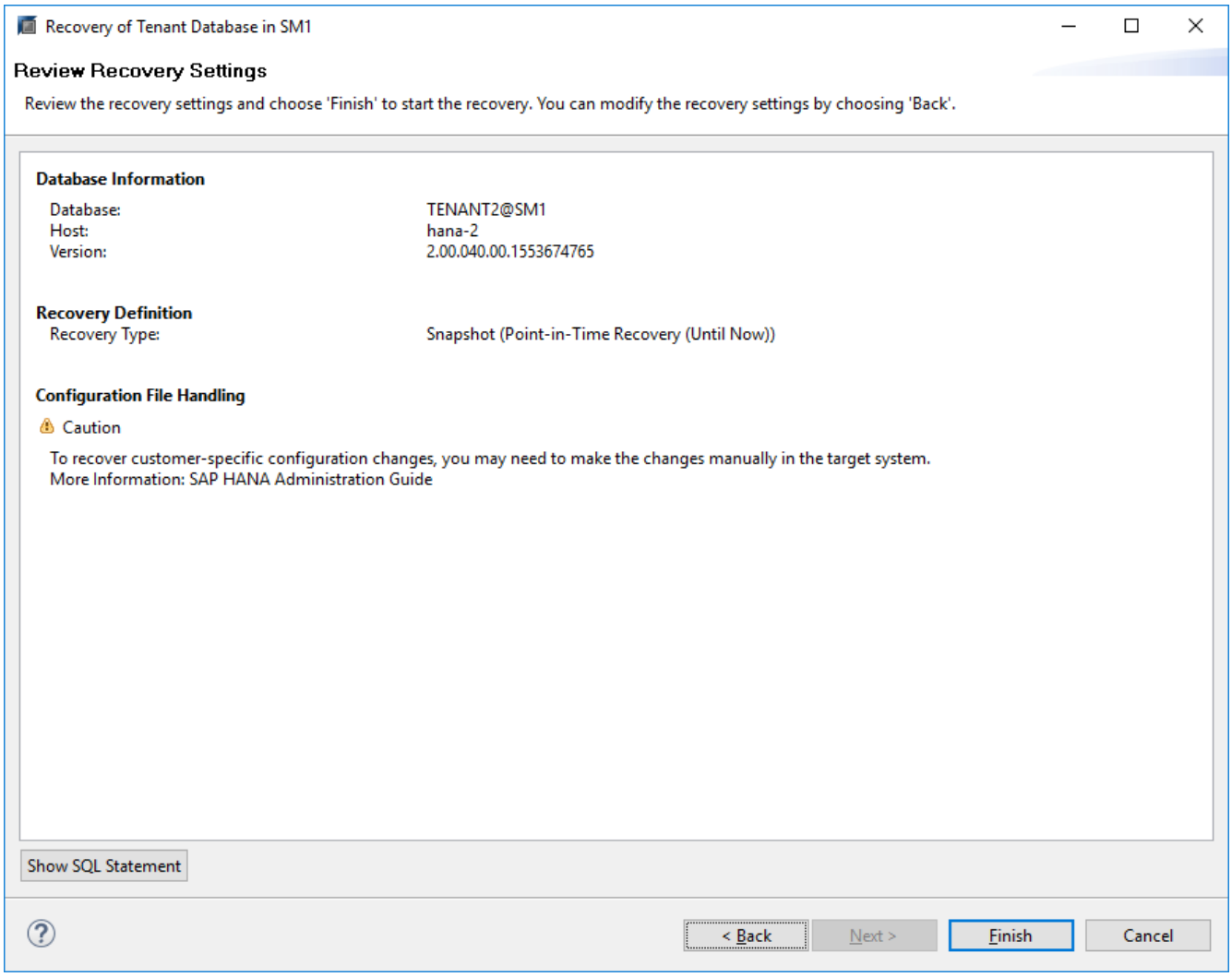

13. ログのバックアップ先を指定します。

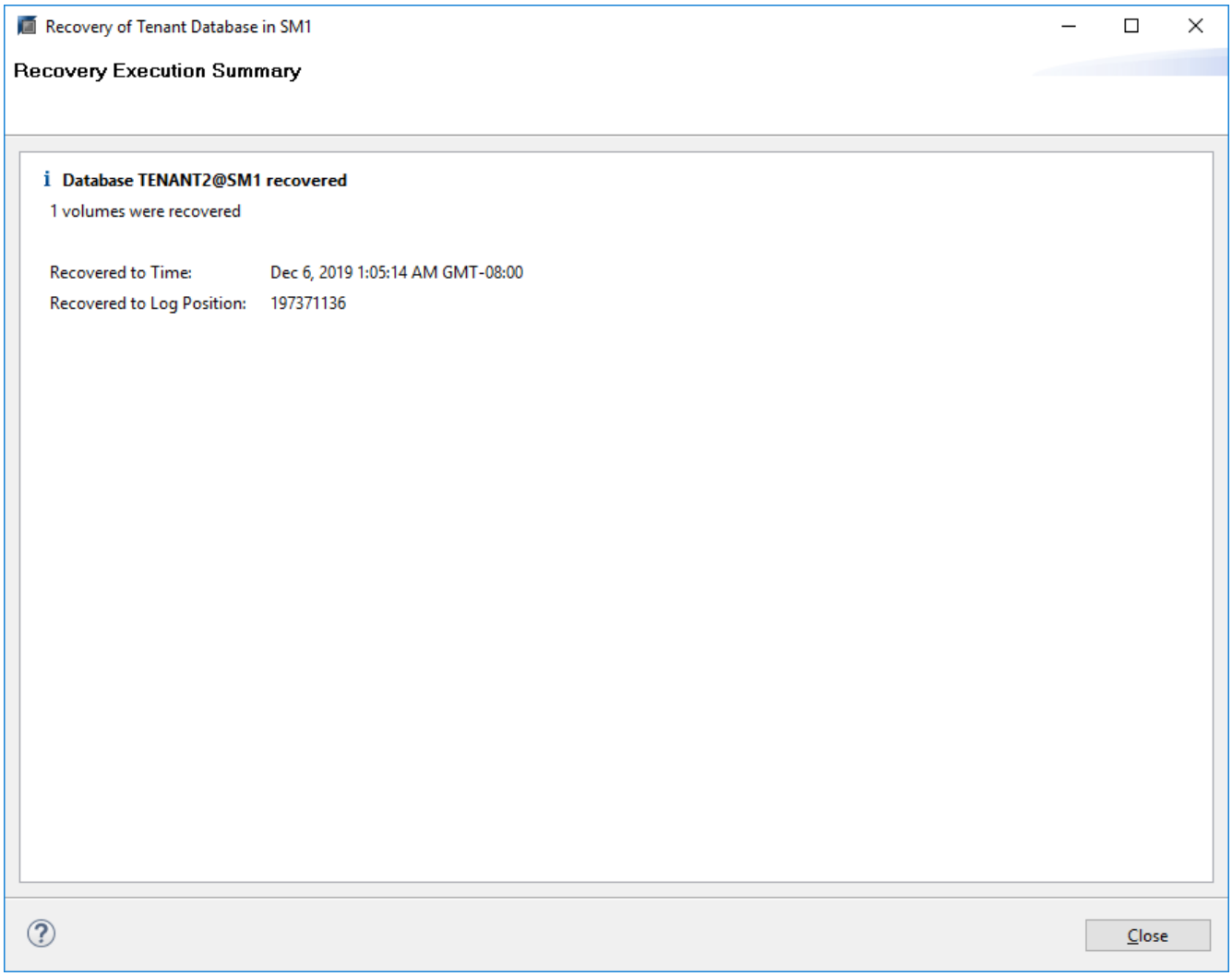



14. 必要に応じて、他の設定を選択します。




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。

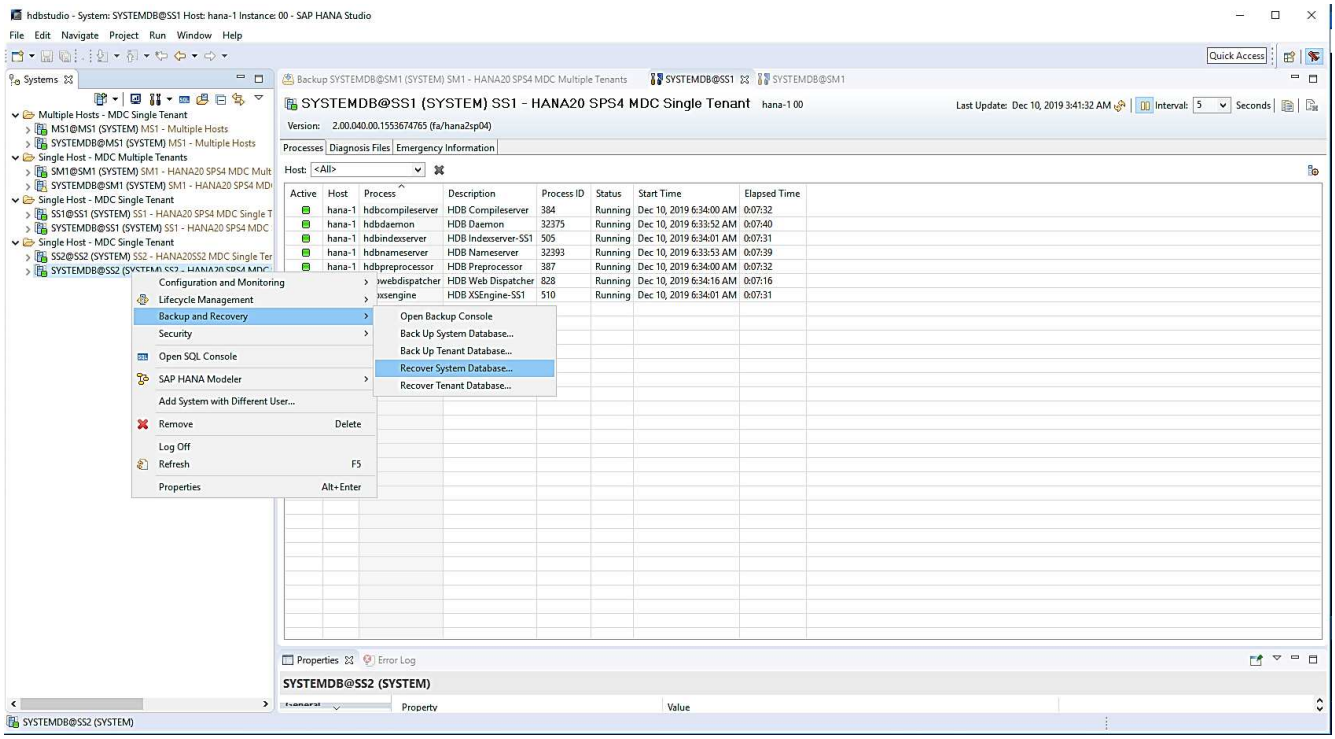
3. SAP HANA Studio を使用して、システムデータベースのリカバリプロセスを実行します。
   a. バックアップ・リストから [ 更新 ] をクリックし ' リカバリに使用できるバックアップを選択します（緑色のアイコンが表示されます）
   b. リカバリプロセスを開始します。リカバリプロセスが完了すると、システムデータベースが起動します。
4. SAP HANA Studio を使用してテナントデータベースのリカバリプロセスを実行します。
   a. [Recover Tenant Database] を選択して、リカバリするテナントを選択します。
   b. リカバリタイプ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

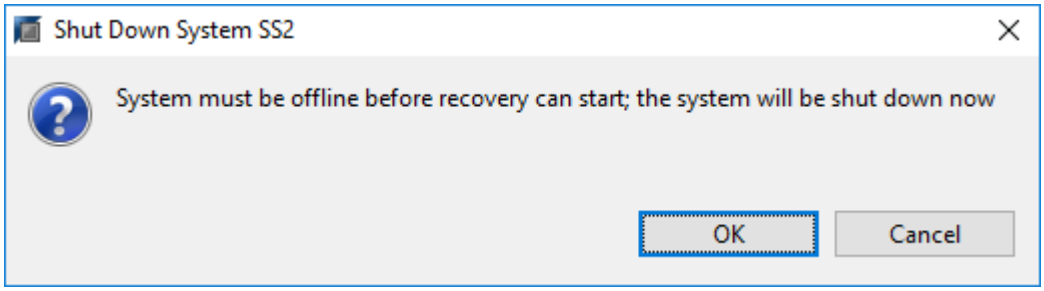
   c. このバックアップを選択し、リカバリプロセスを開始します。リカバリプロセスが完了すると、テナントデータベースが自動的に起動します。

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。

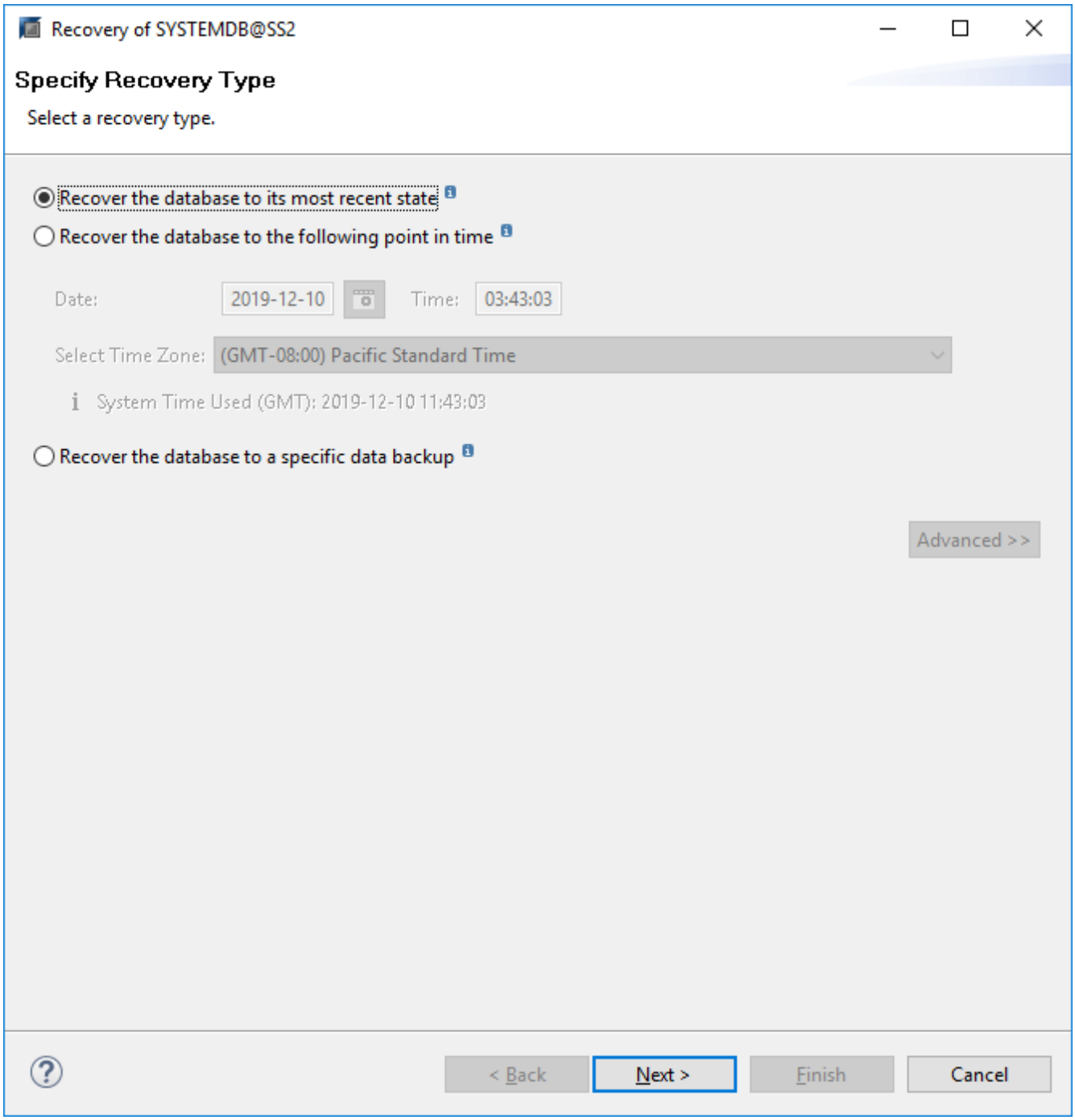


2. [OK] をクリックして、 SAP HANA データベースをシャットダウンします。

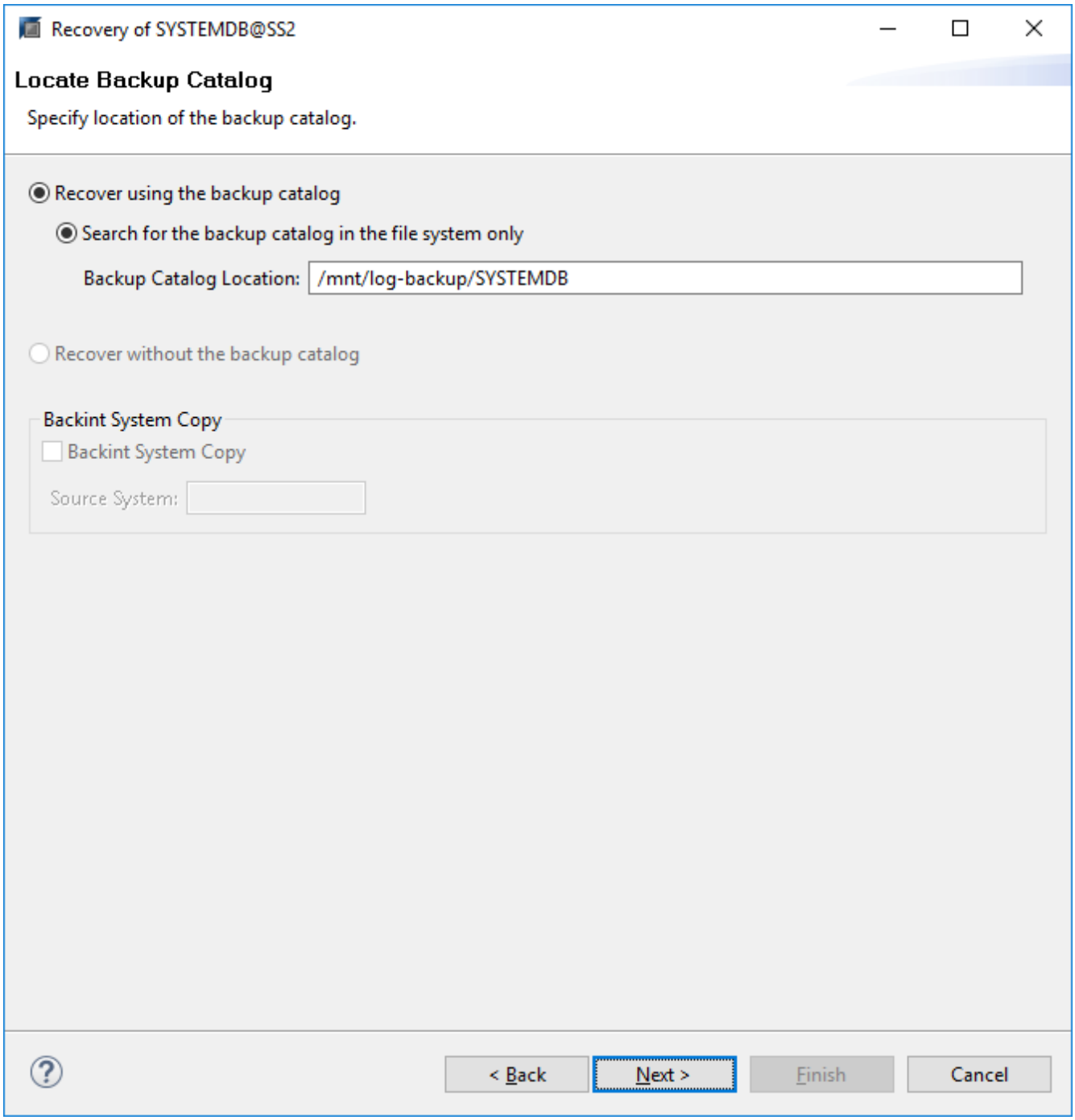



SAP HANA システムがシャットダウンし、リカバリウィザードが起動します。

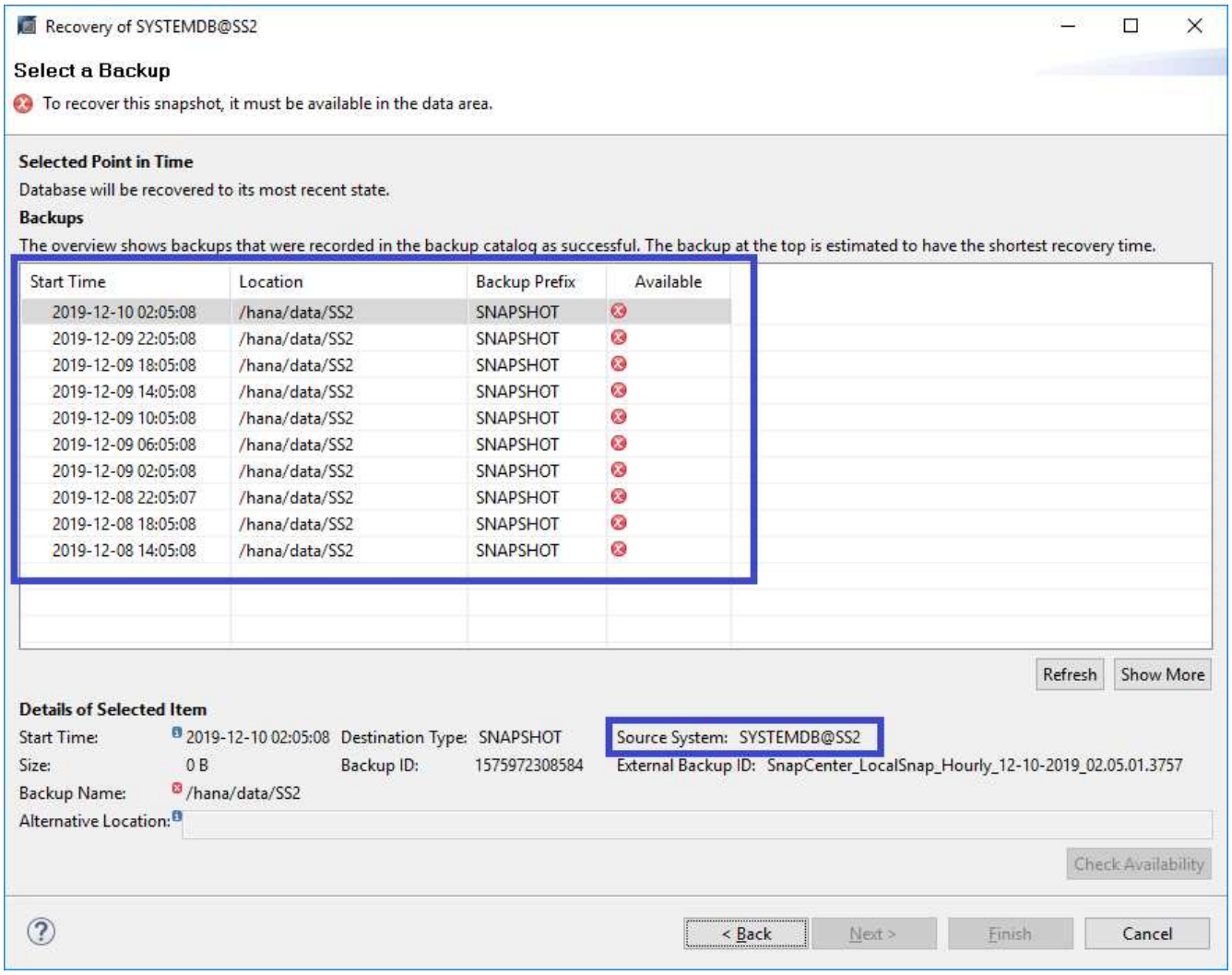
3. リカバリタイプを選択して、 Next （次へ）をクリックします。




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。



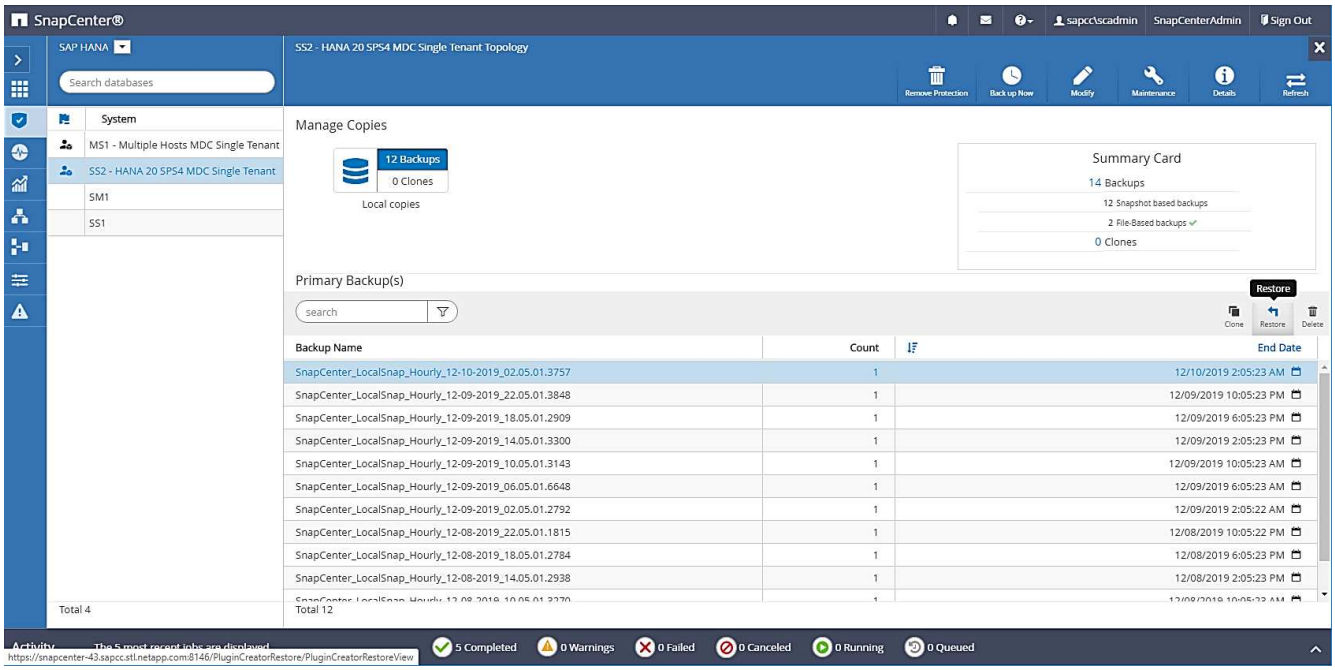

6. すべてのデータボリュームをアンマウントします。

```
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。

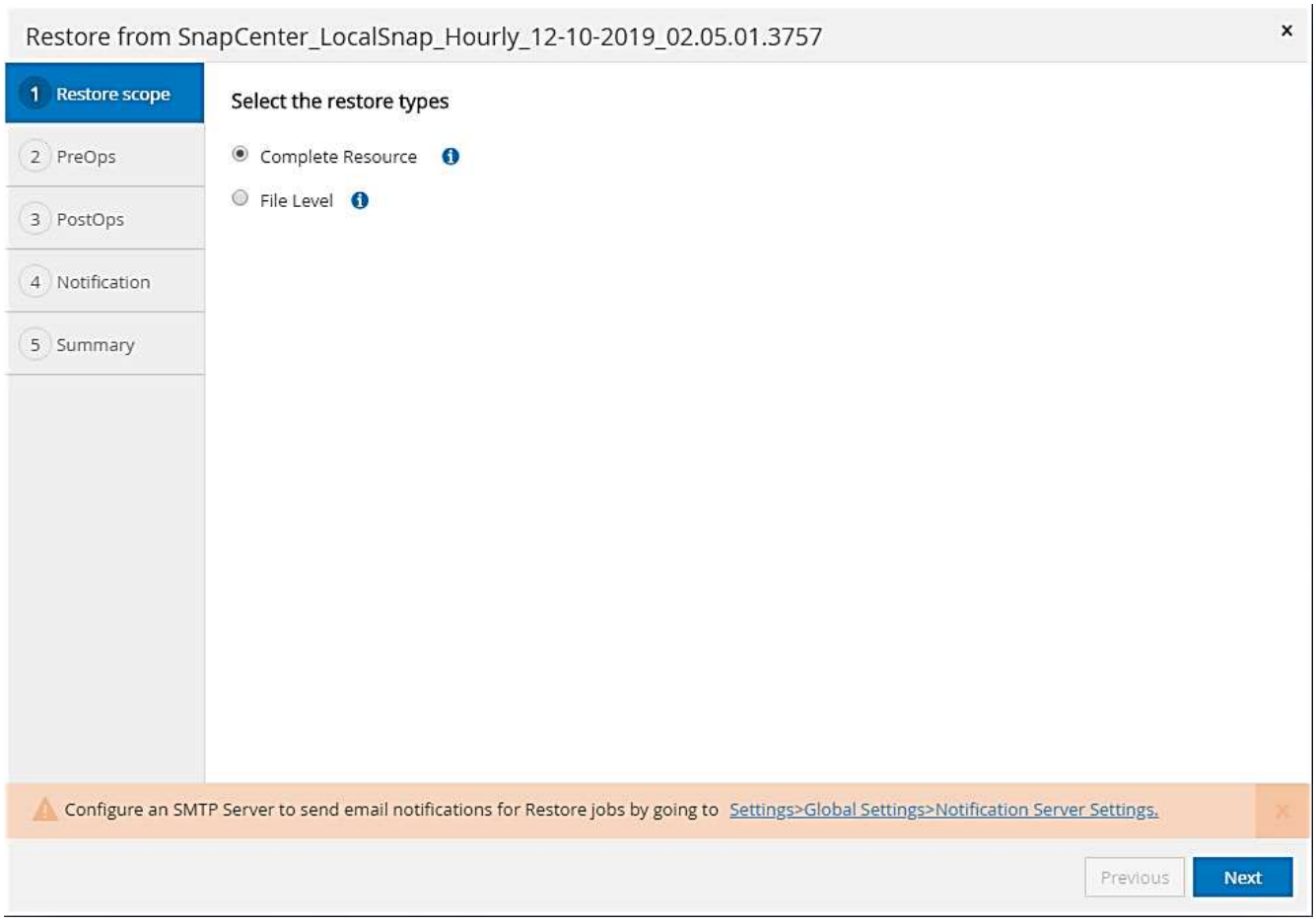
7. SnapCenter の GUI で、リソーストポロジビューを選択し、リストアするバックアップを選択します。この例では、最新のプライマリバックアップを選択します。リストアアイコンをクリックして、リストアを開始します。



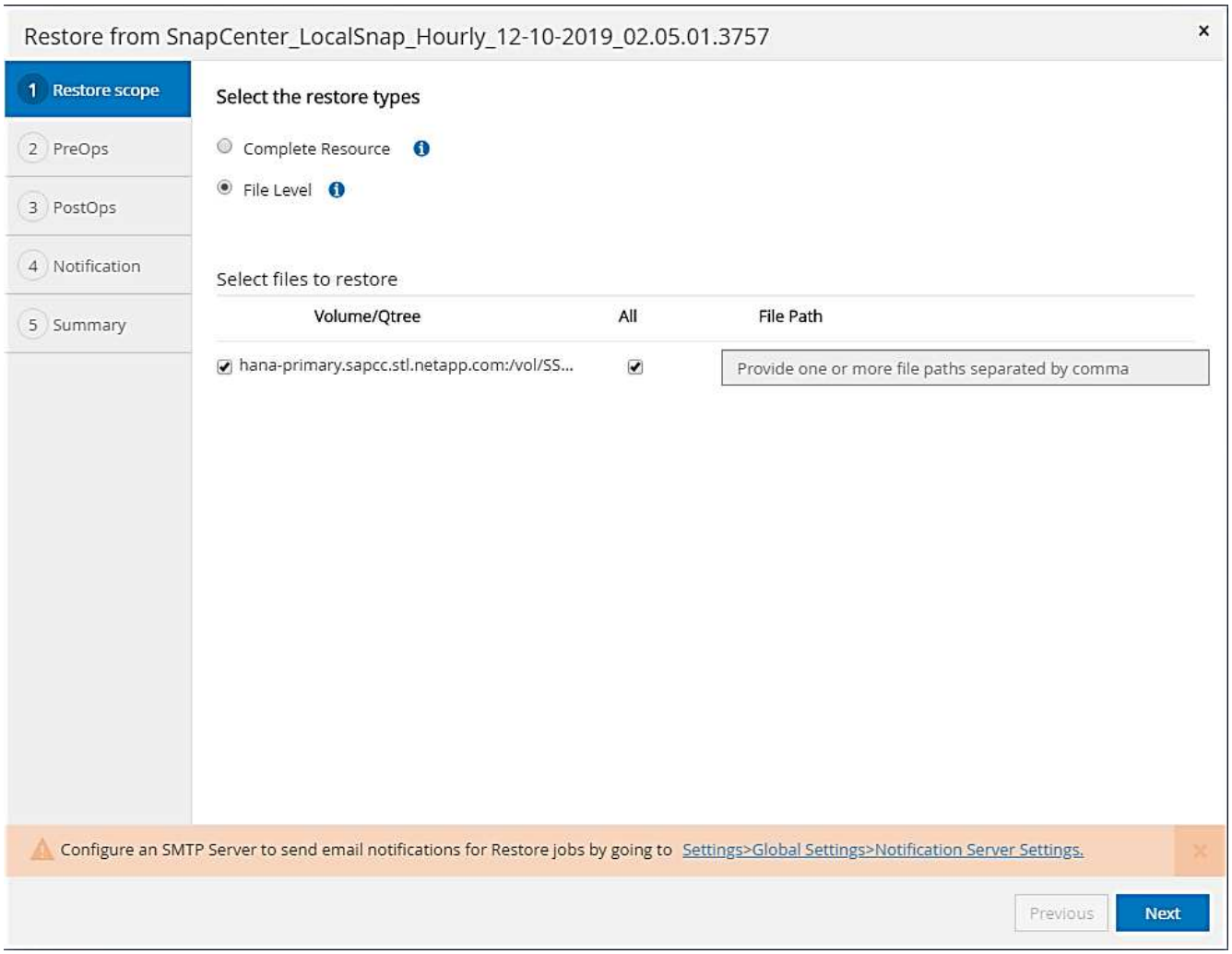

SnapCenter リストアウィザードが起動します。

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

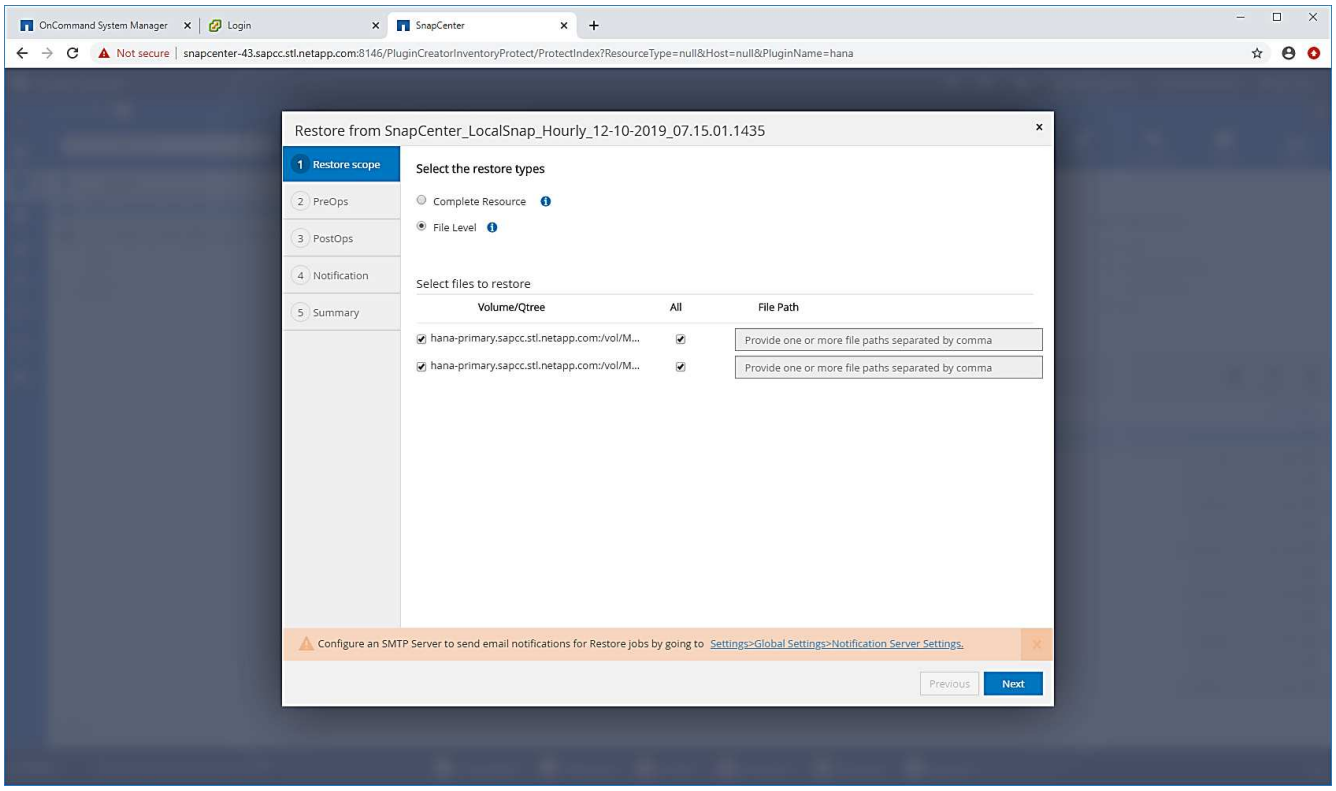
ボリュームベースのリストアを使用するには、 [ リソース全体 ] を選択します。



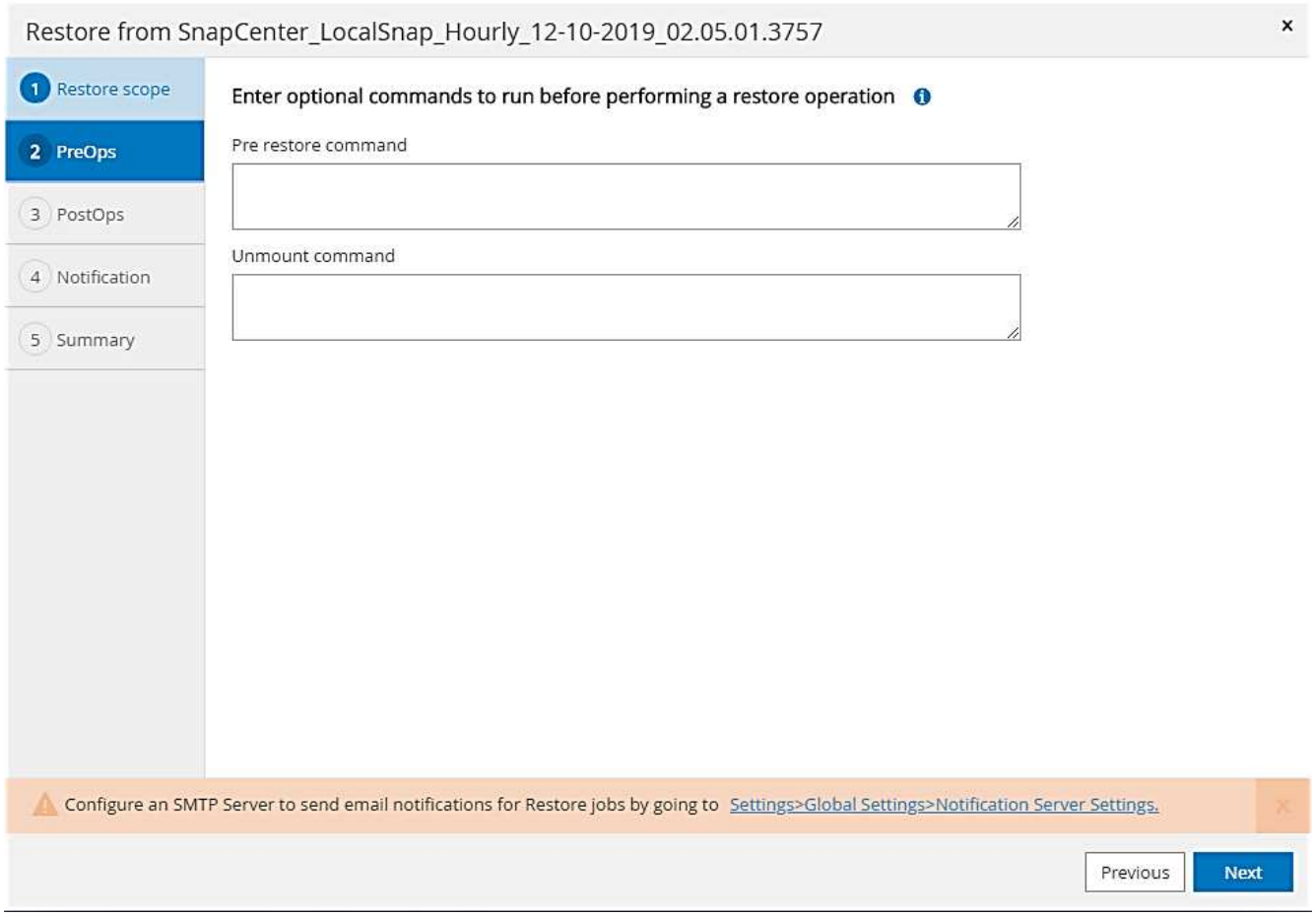
9. すべてのファイルに単一ファイルの SnapRestore 操作を使用するには、 [ ファイルレベルとすべて ] を選択します。



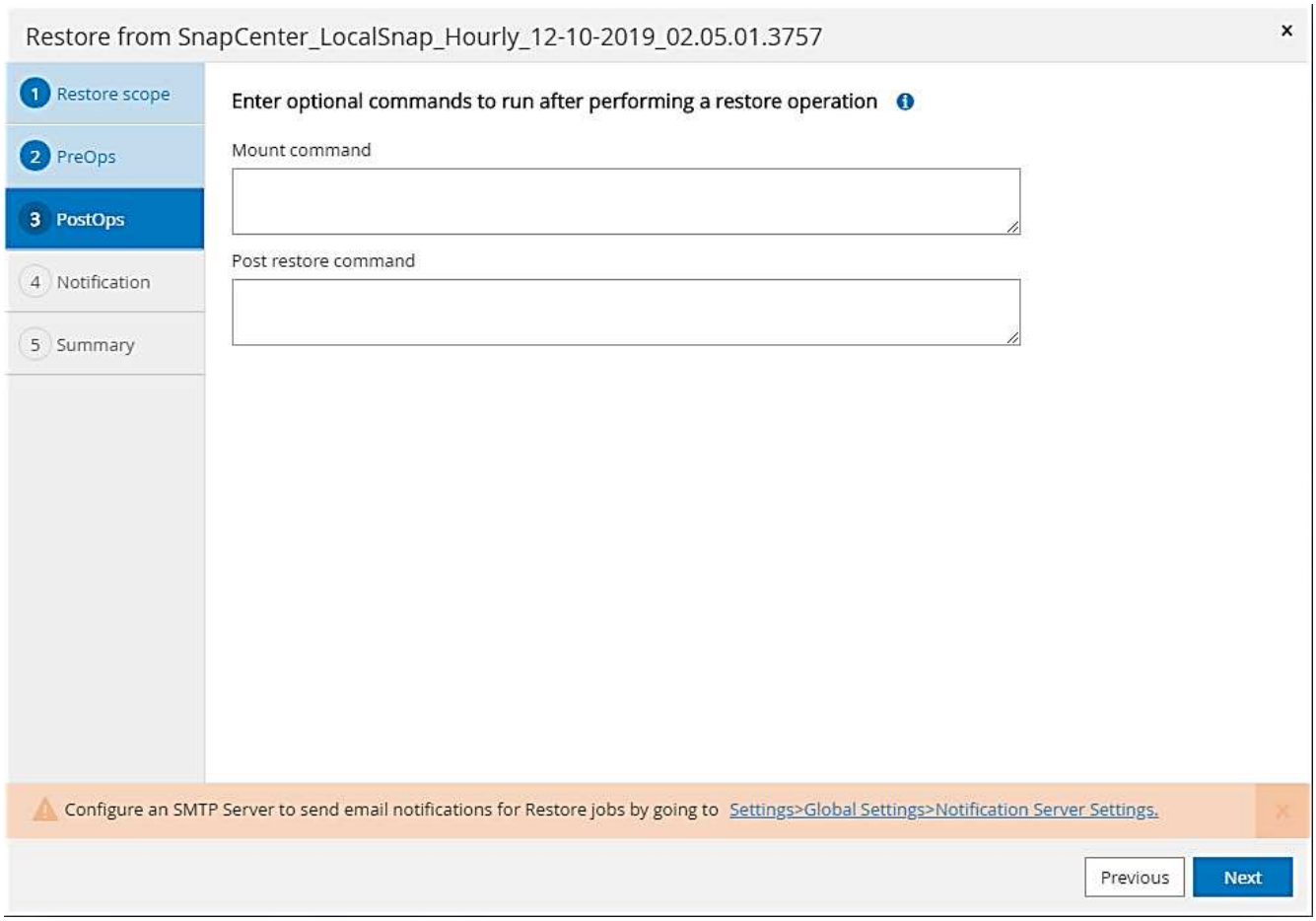

SAP HANA マルチホストシステムのファイルレベルのリストアを実行する場合は、すべてのボリュームを選択します。



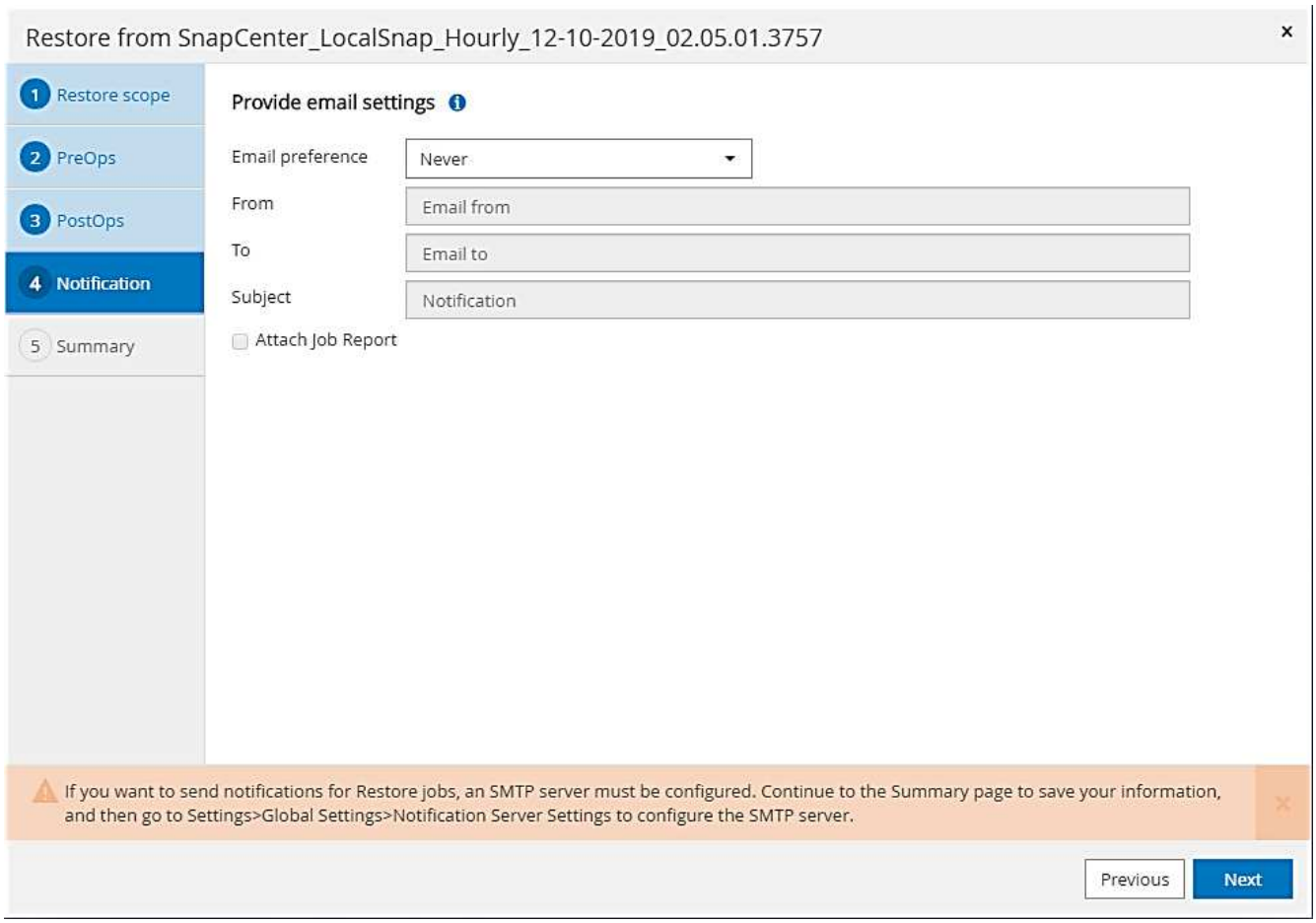

10. （オプション）中央の HANA プラグインホストで実行されている SAP HANA プラグインから実行するコマンドを指定します。次へをクリックします。



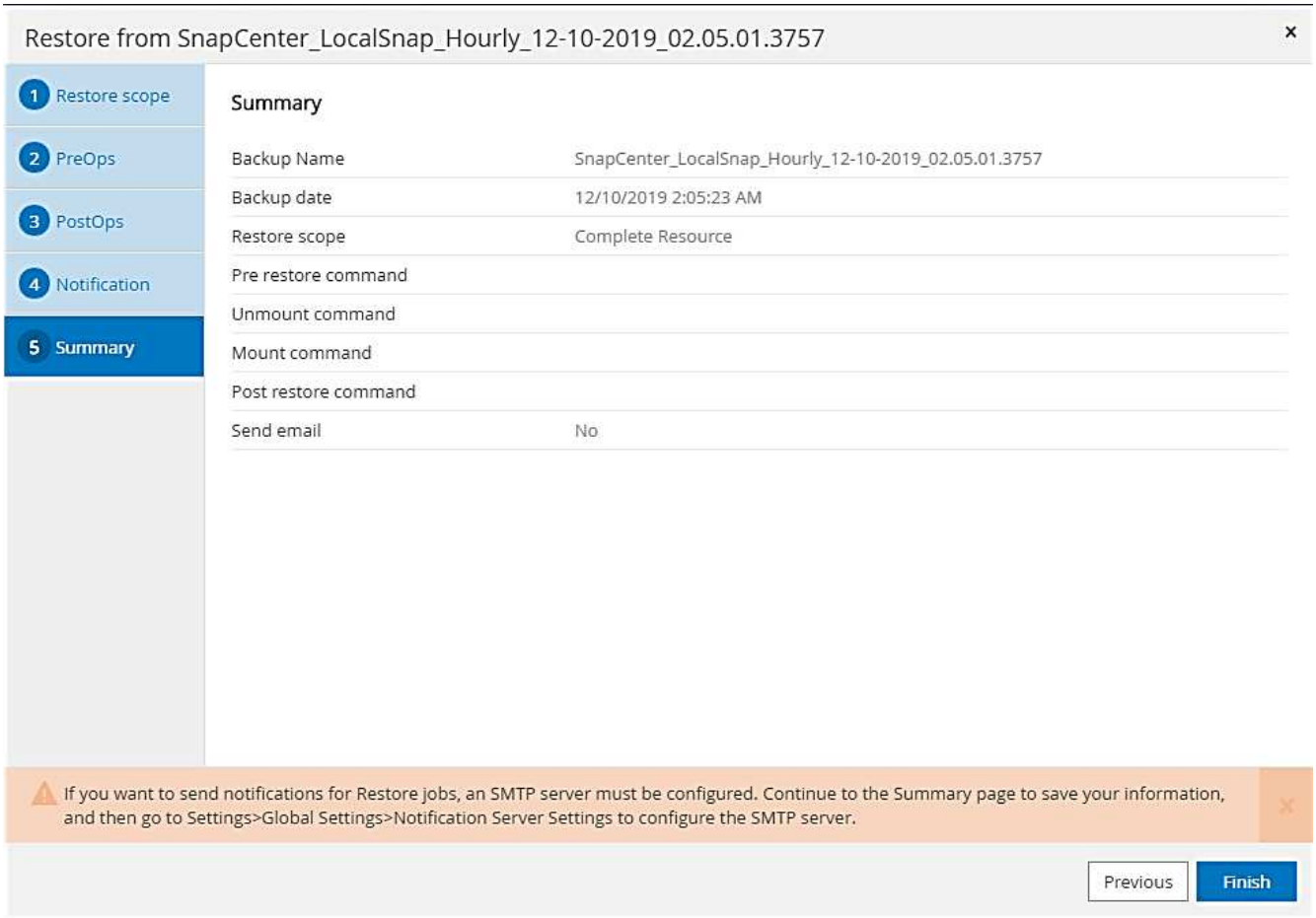
11. オプションのコマンドを指定し、次へをクリックします。



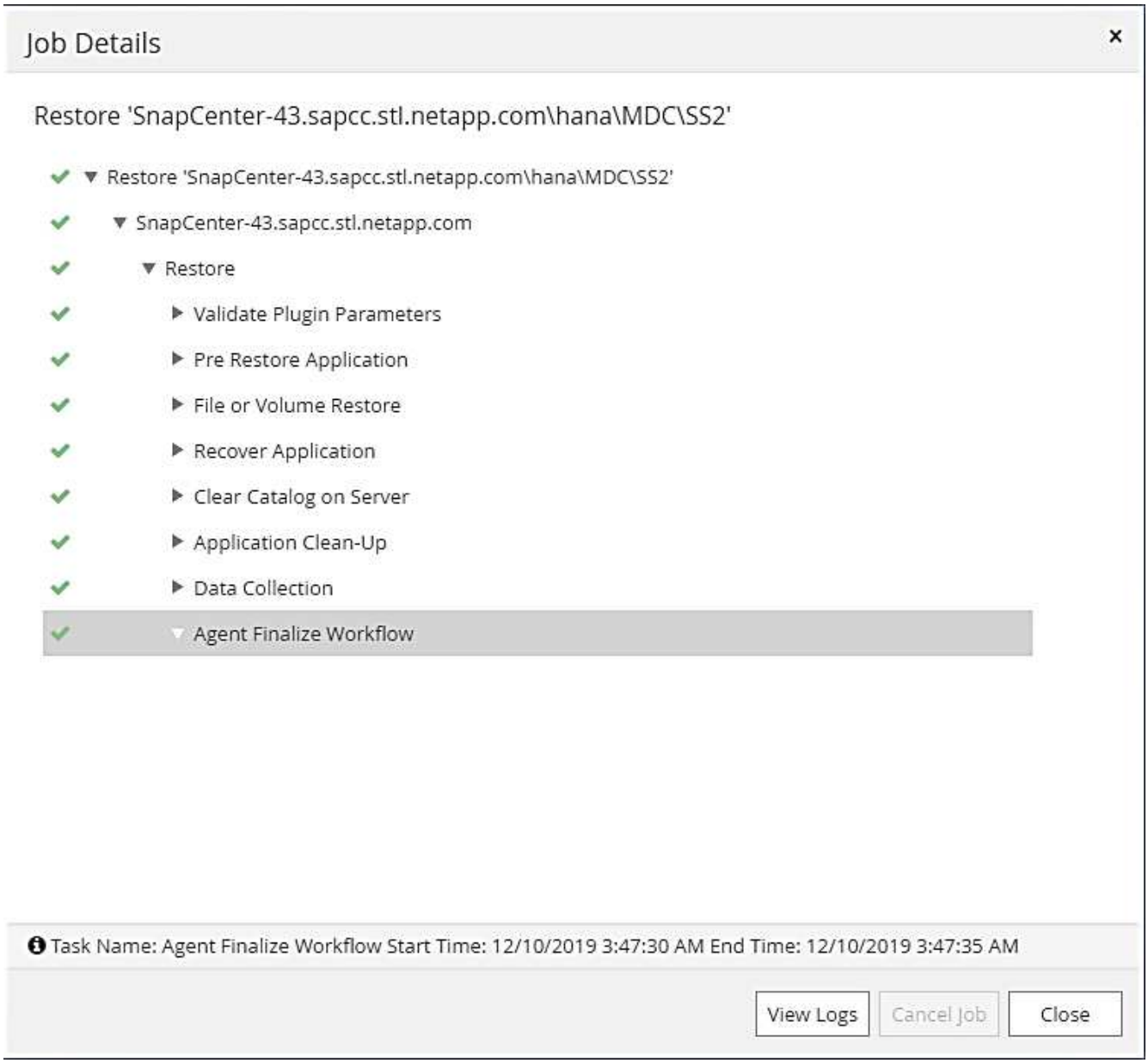

12. 通知設定を指定して、 SnapCenter からステータス E メールとジョブログを送信できるようにします。次へをクリックします。




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。



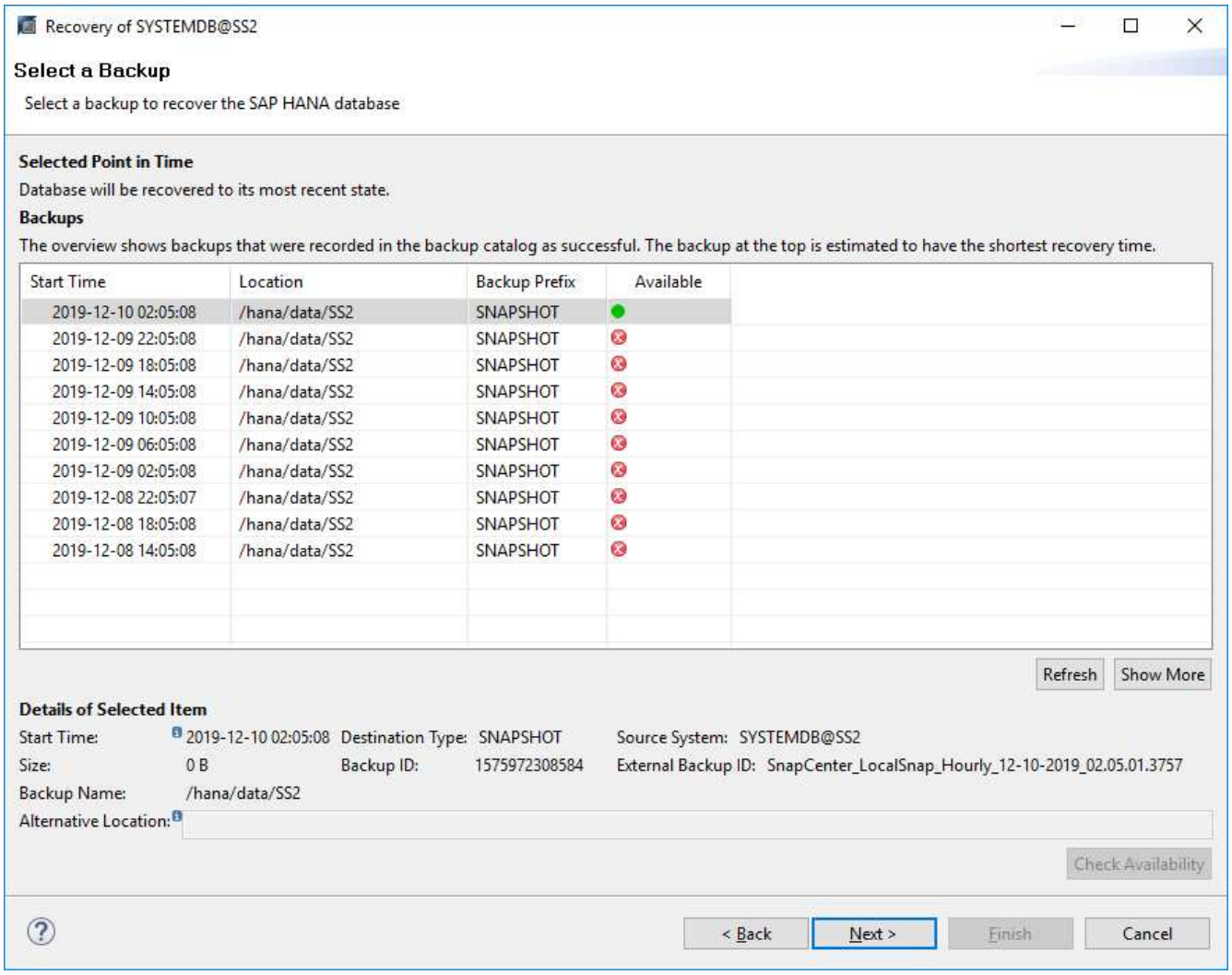

14. リストアジョブが開始され、アクティビティペインのログ行をダブルクリックするとジョブログが表示されます。



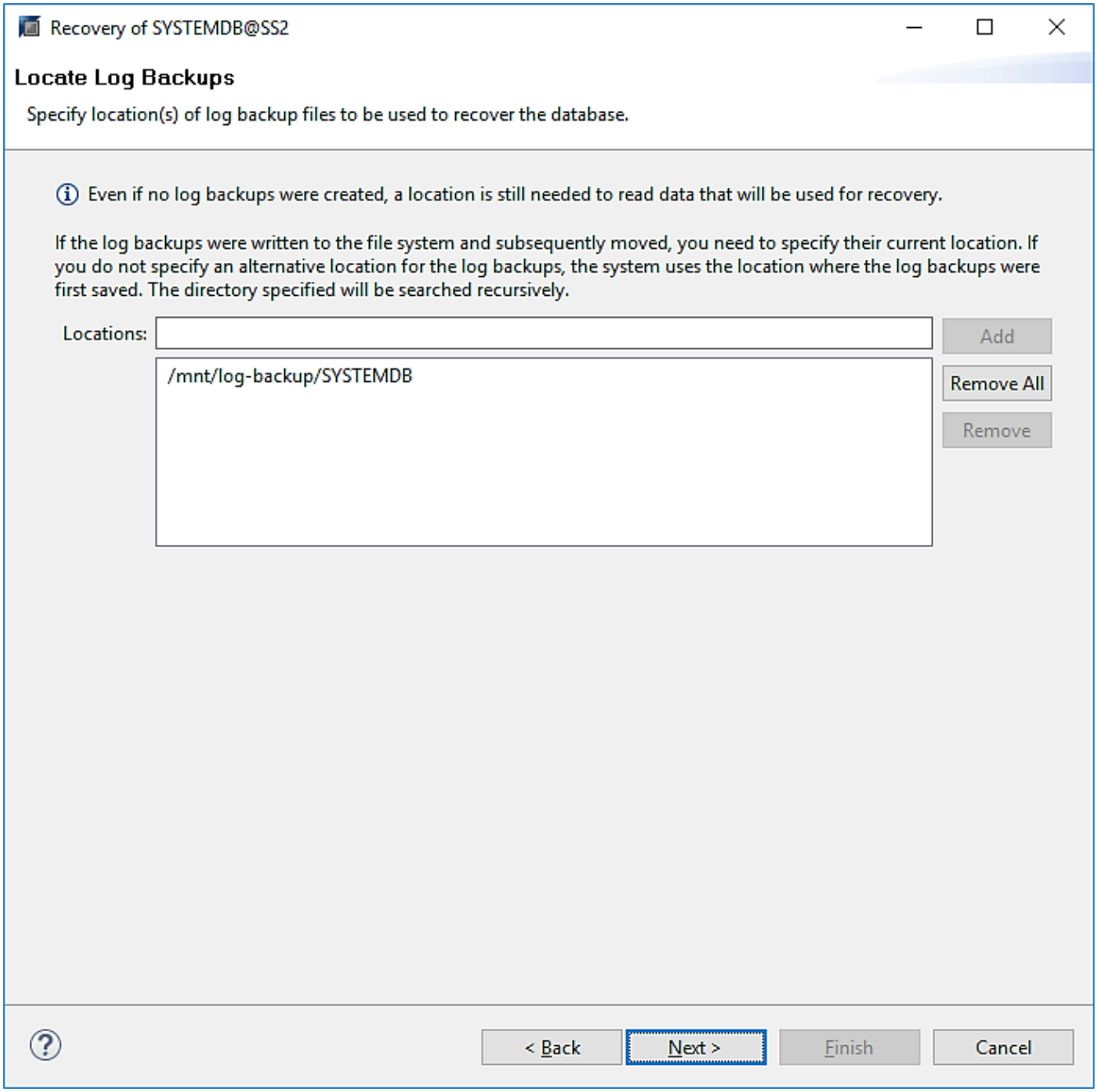

15. リストアプロセスが完了するまで待ちます。各データベースホストで、すべてのデータボリュームをマウントします。この例では、データベースホスト上で再マウントが必要なボリュームは 1 つだけです。

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

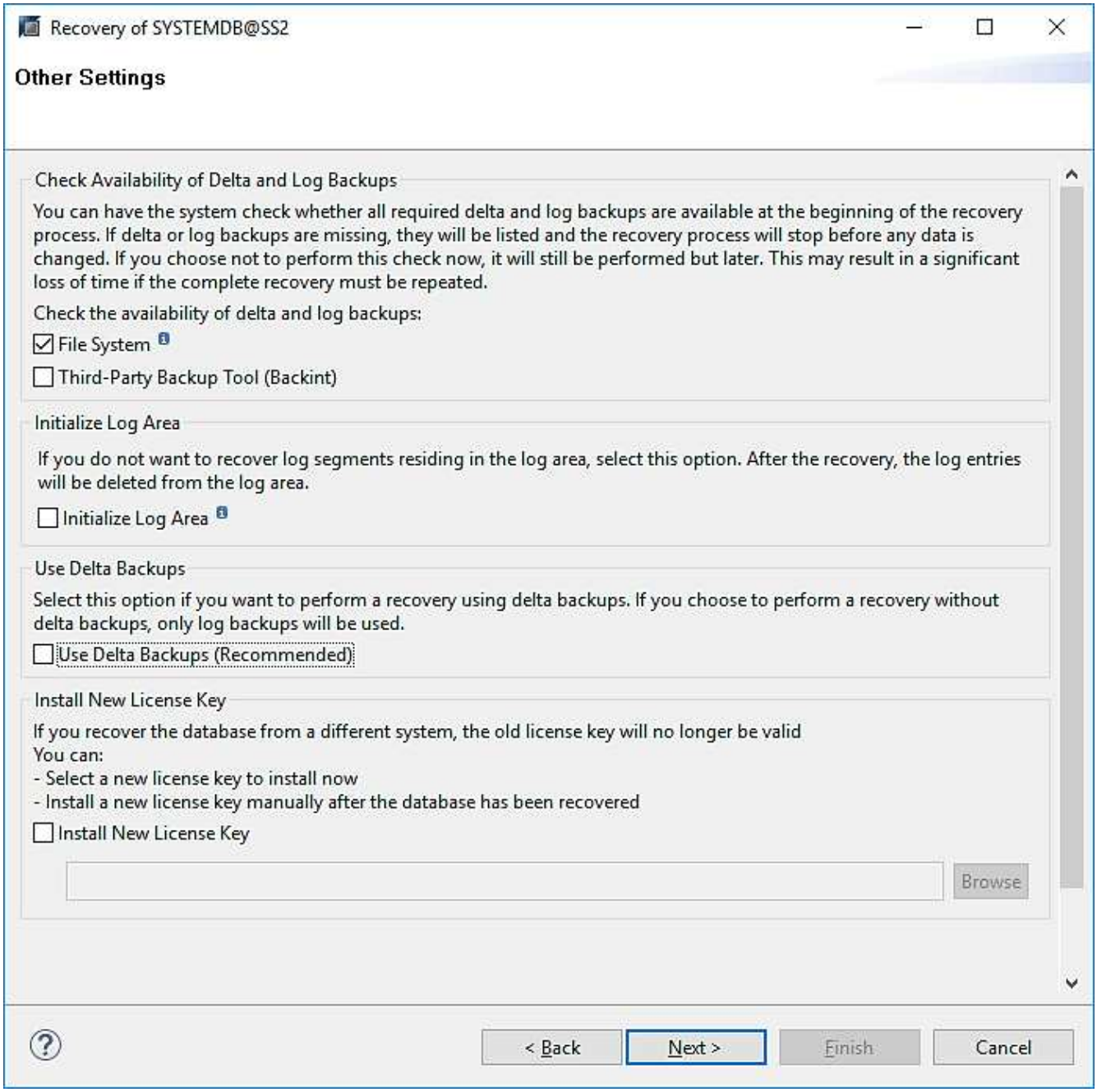
16. SAP HANA Studio に移動し、 Refresh をクリックして、使用可能なバックアップのリストを更新します。SnapCenter でリストアされたバックアップは、バックアップのリストに緑のアイコンで表示されます。バックアップを選択し、 Next （次へ）をクリックします。



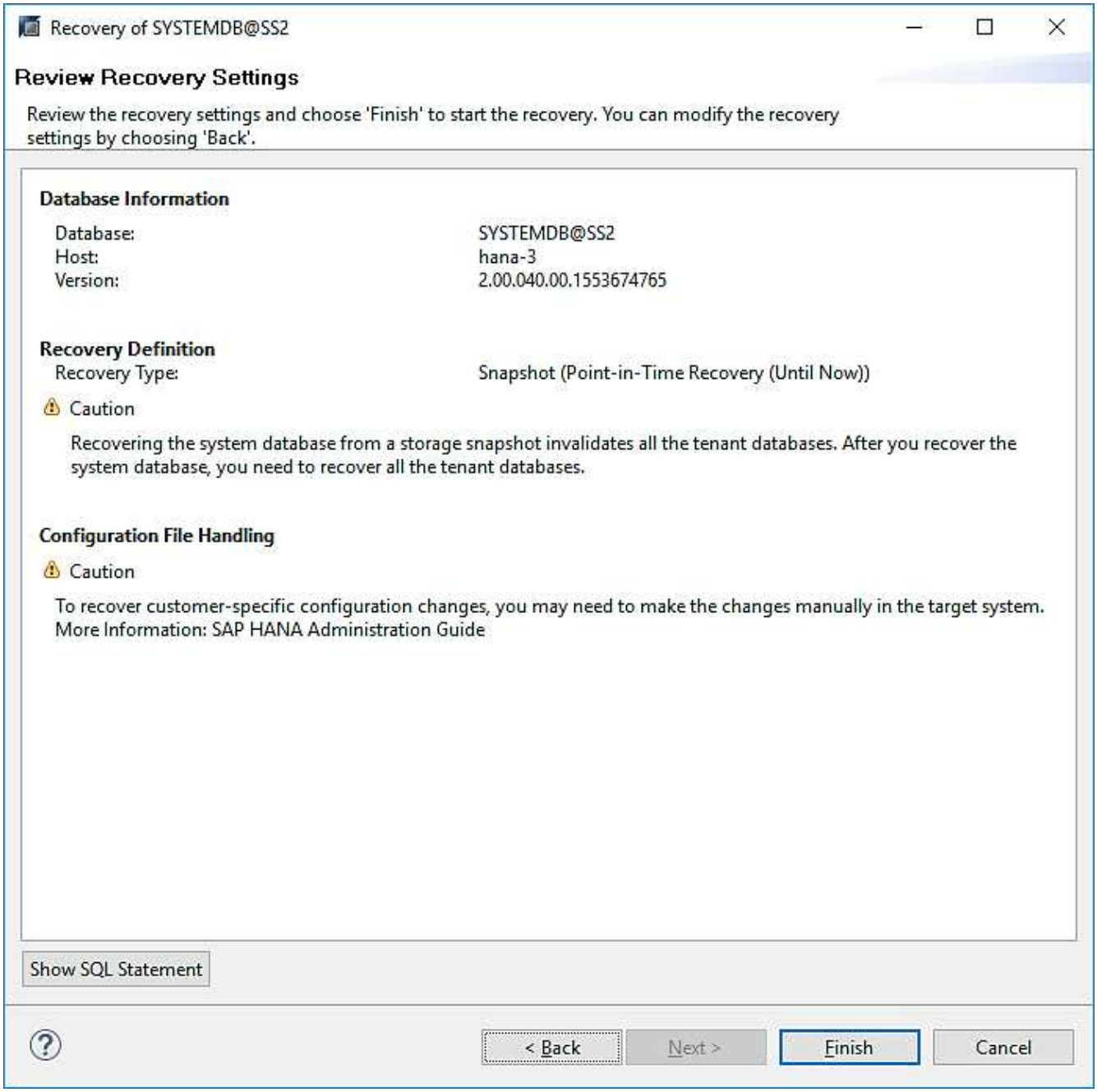

17. ログバックアップの場所を指定します。次へをクリックします。



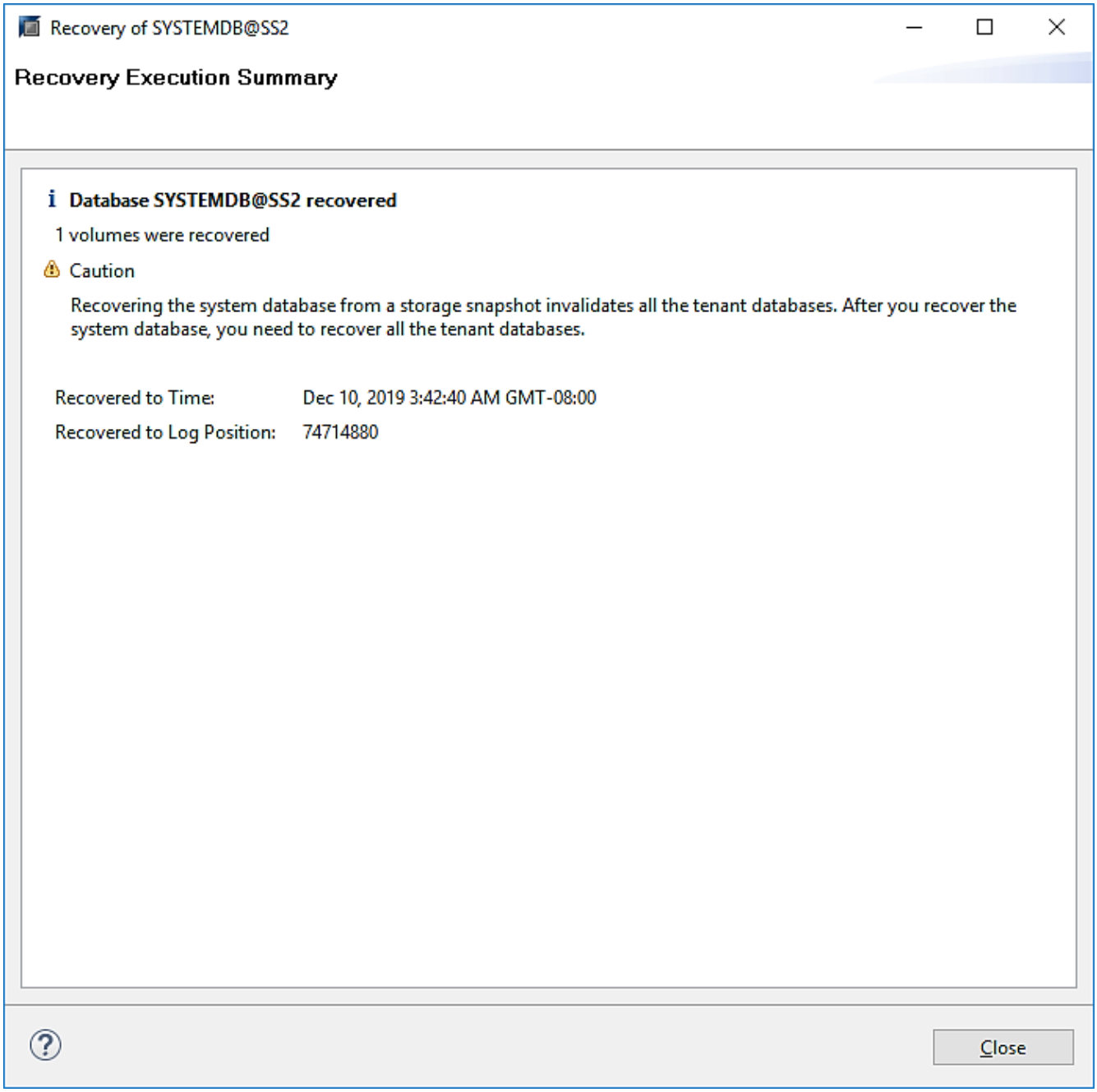

18. 必要に応じて、他の設定を選択します。［ デルタバックアップを使用 ］ が選択されていないことを確認します。次へをクリックします。



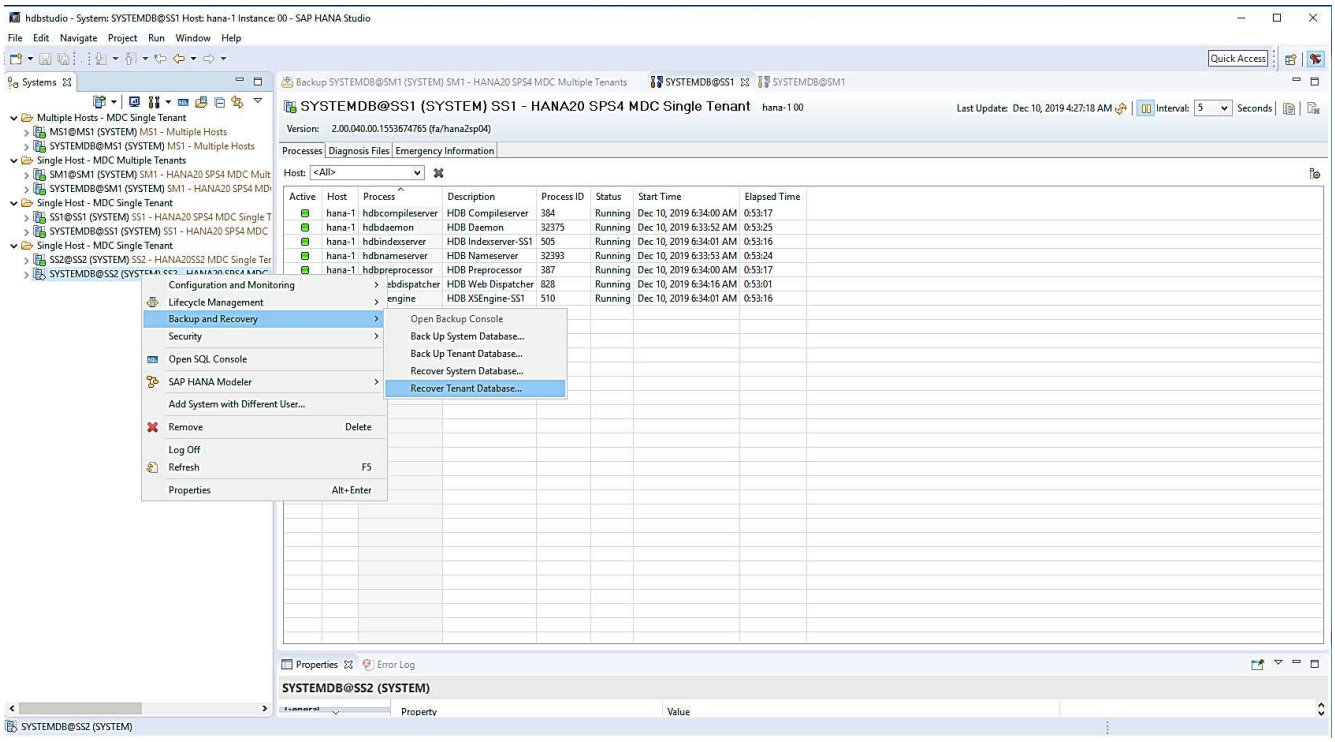

19. リカバリ設定を確認し、 [ 完了 ] をクリックします。



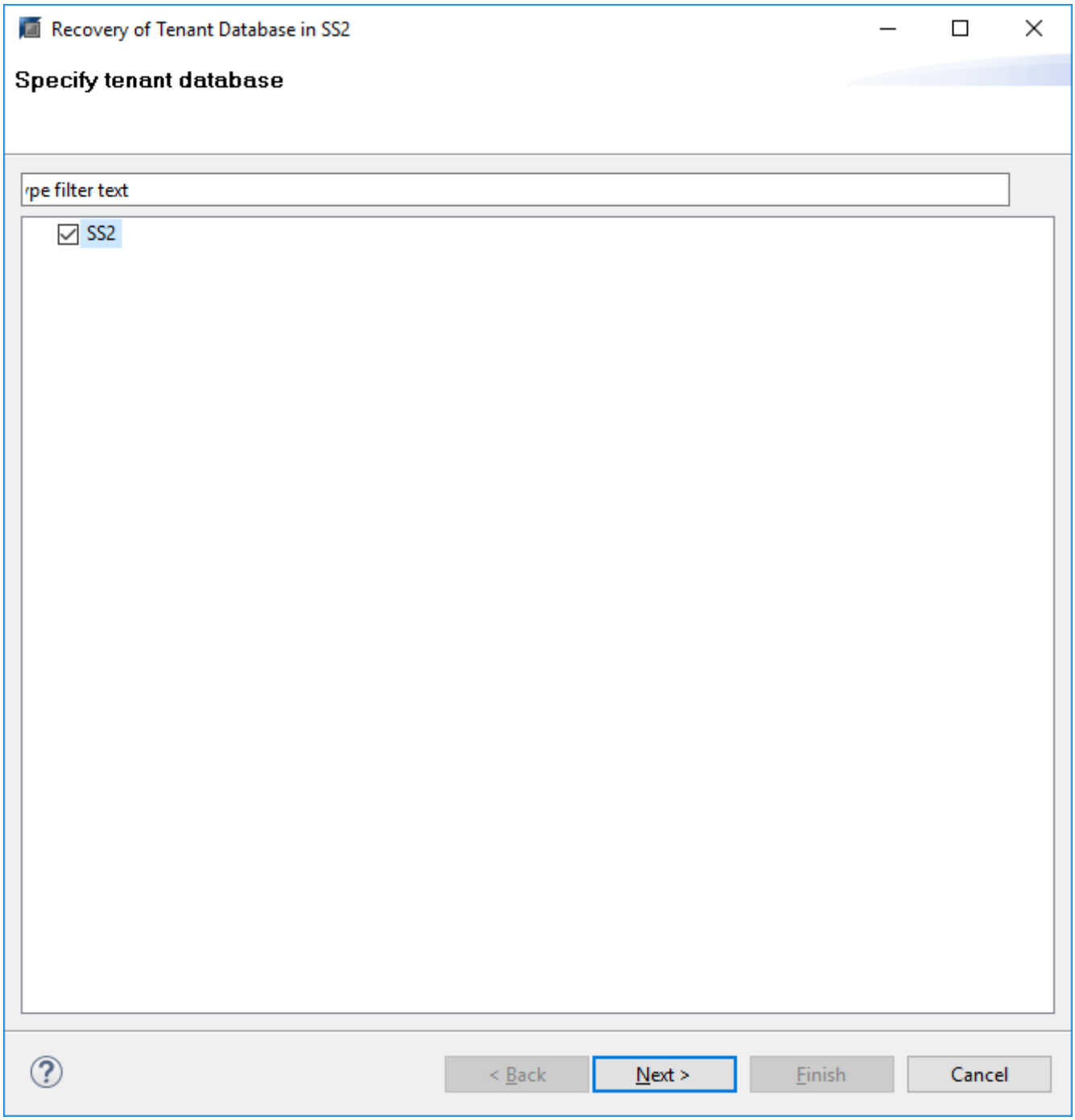

20. リカバリプロセスが開始されます。システムデータベースのリカバリが完了するまで待ちます。



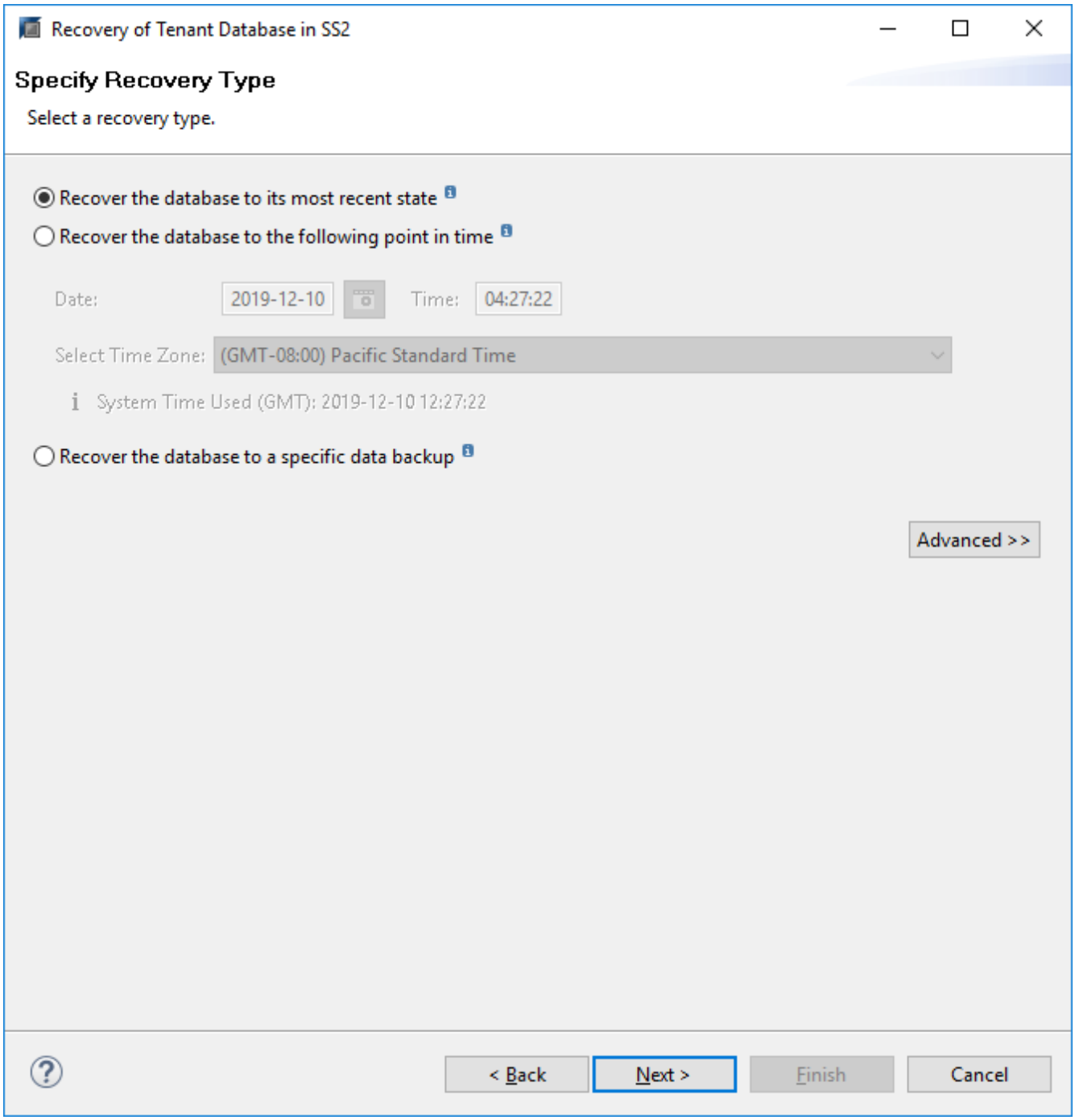

21. SAP HANA Studio で、システムデータベースのエントリを選択し、 Backup Recovery - Recover Tenant Database を開始します。



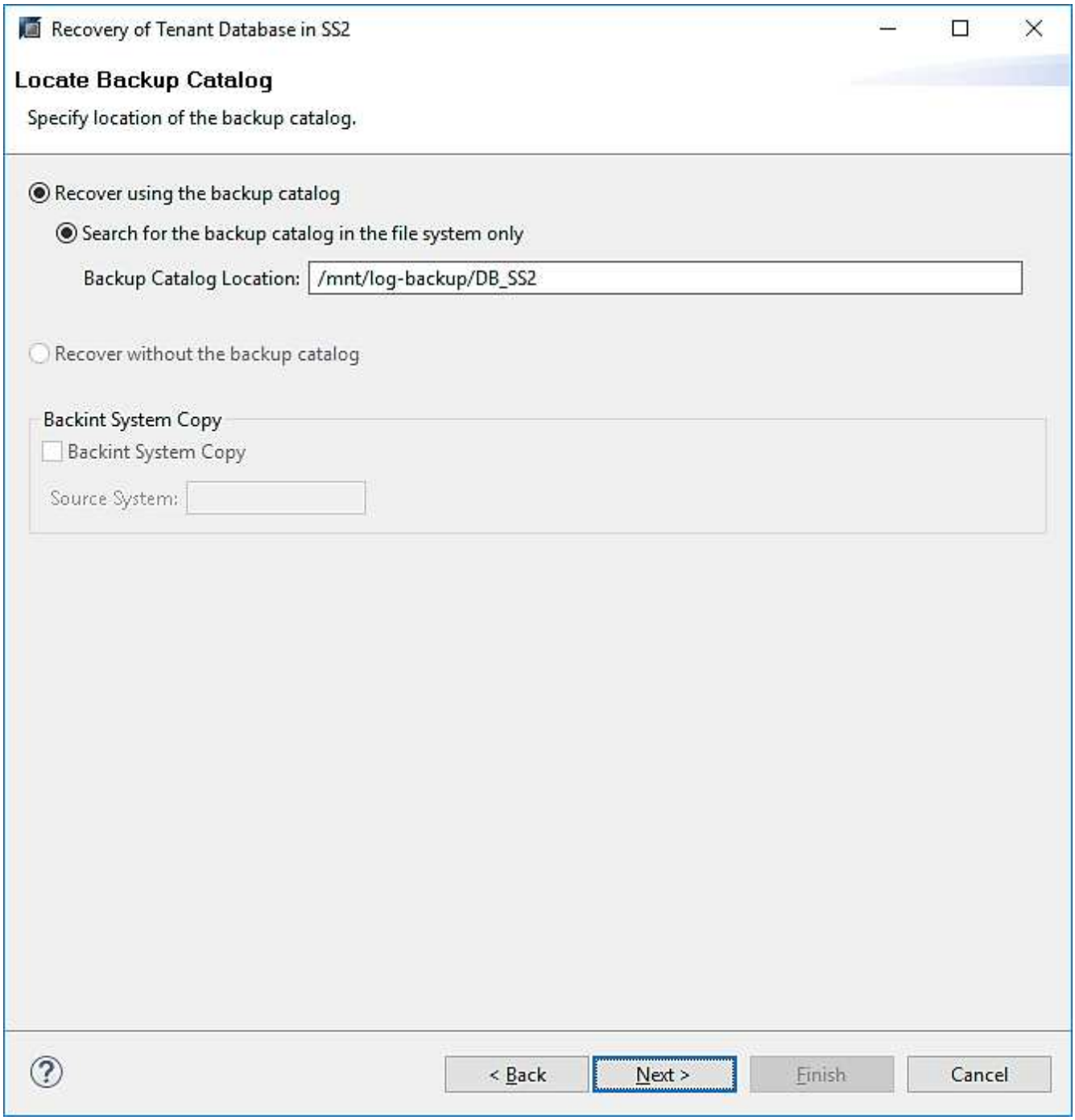

22. リカバリするテナントを選択し、 Next （次へ）をクリックします。



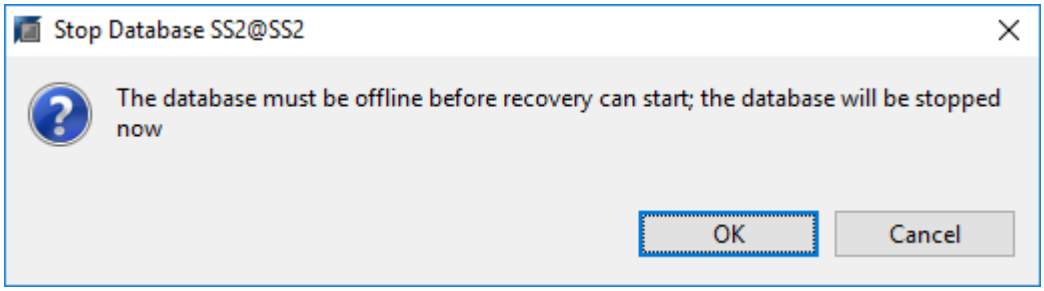

23. リカバリタイプを指定して、 Next （次へ）をクリックします。



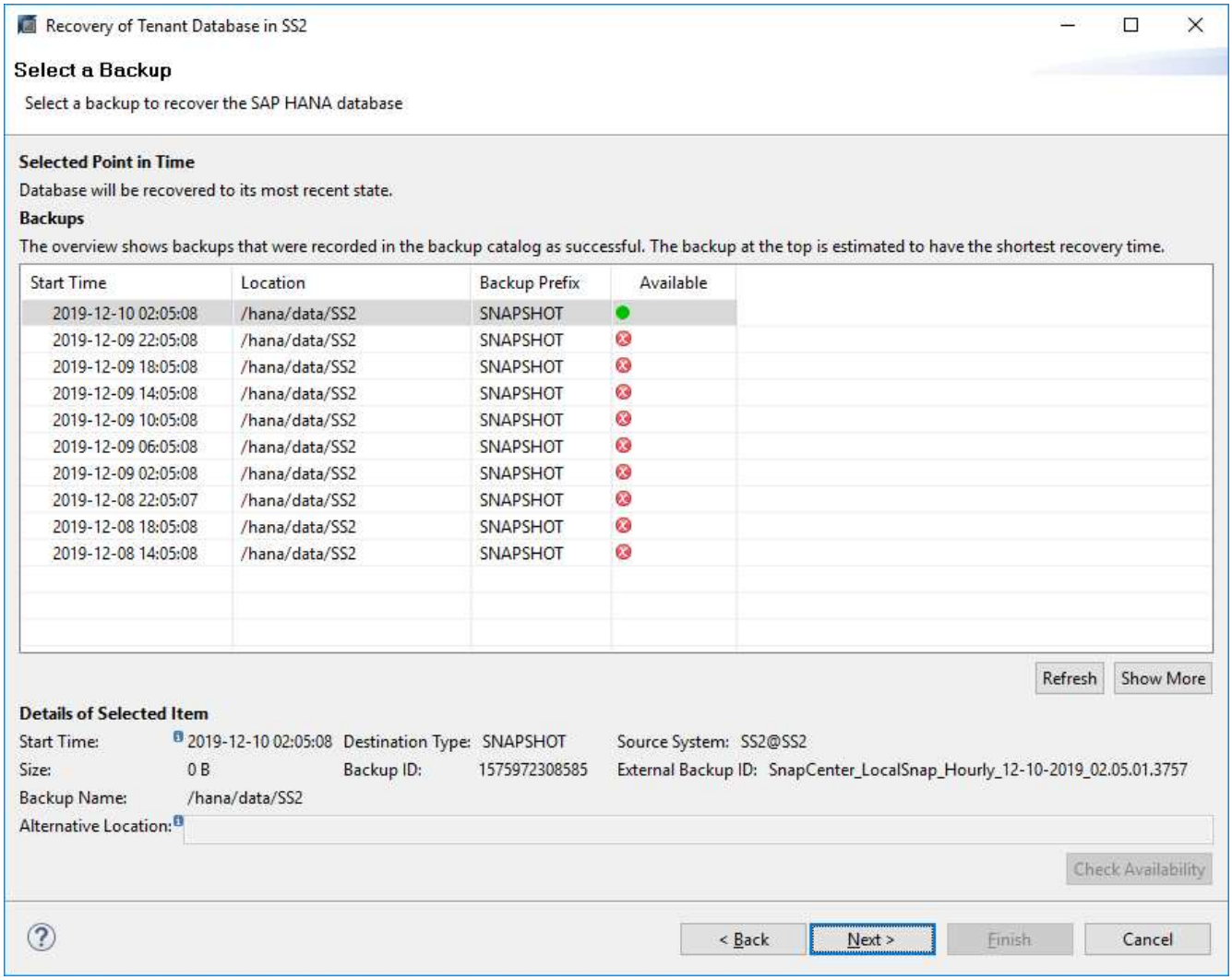

24. バックアップカタログの場所を確認し、 Next （次へ）をクリックします。



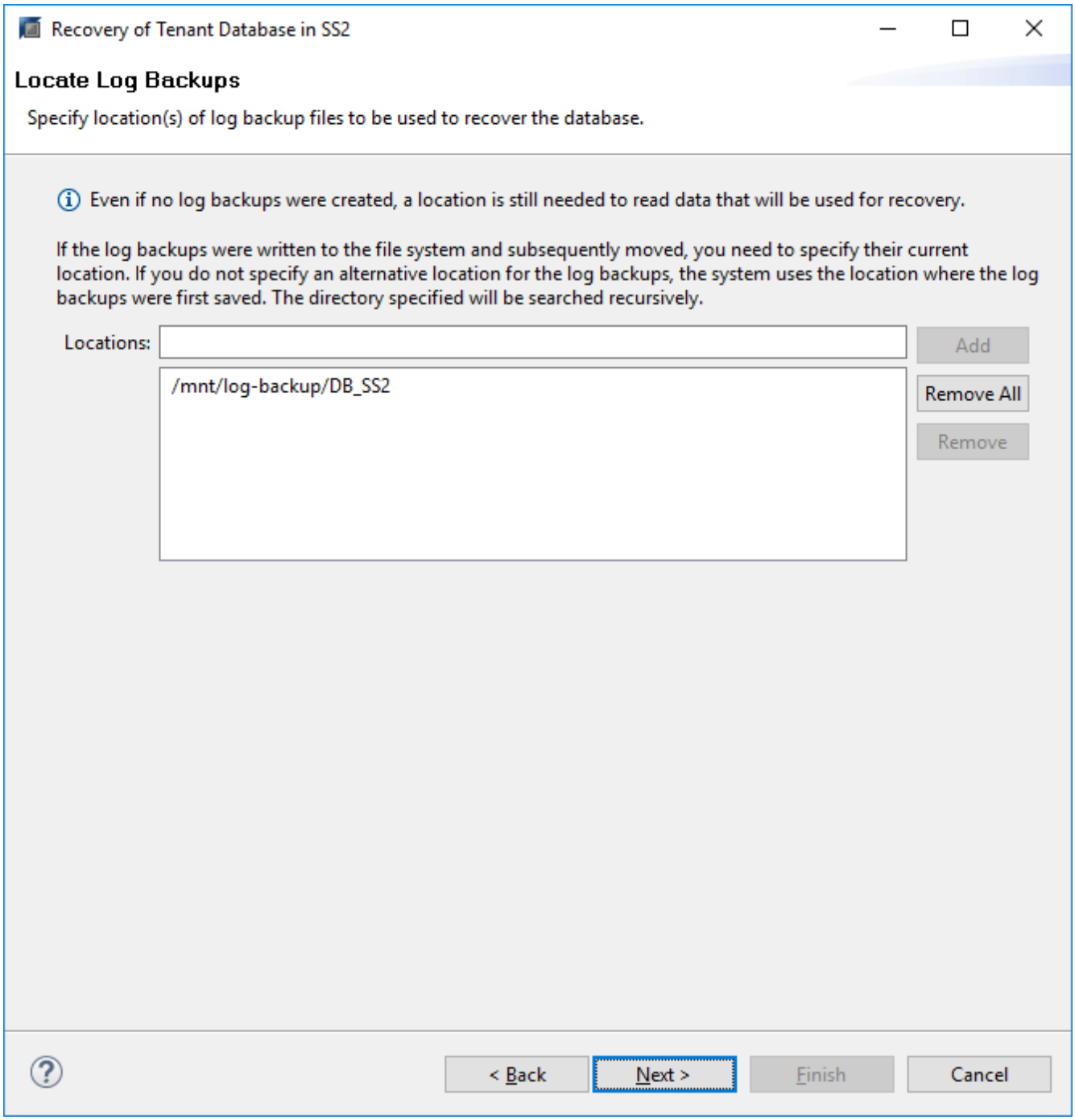

25. テナントデータベースがオフラインであることを確認します。[OK] をクリックして続行します。



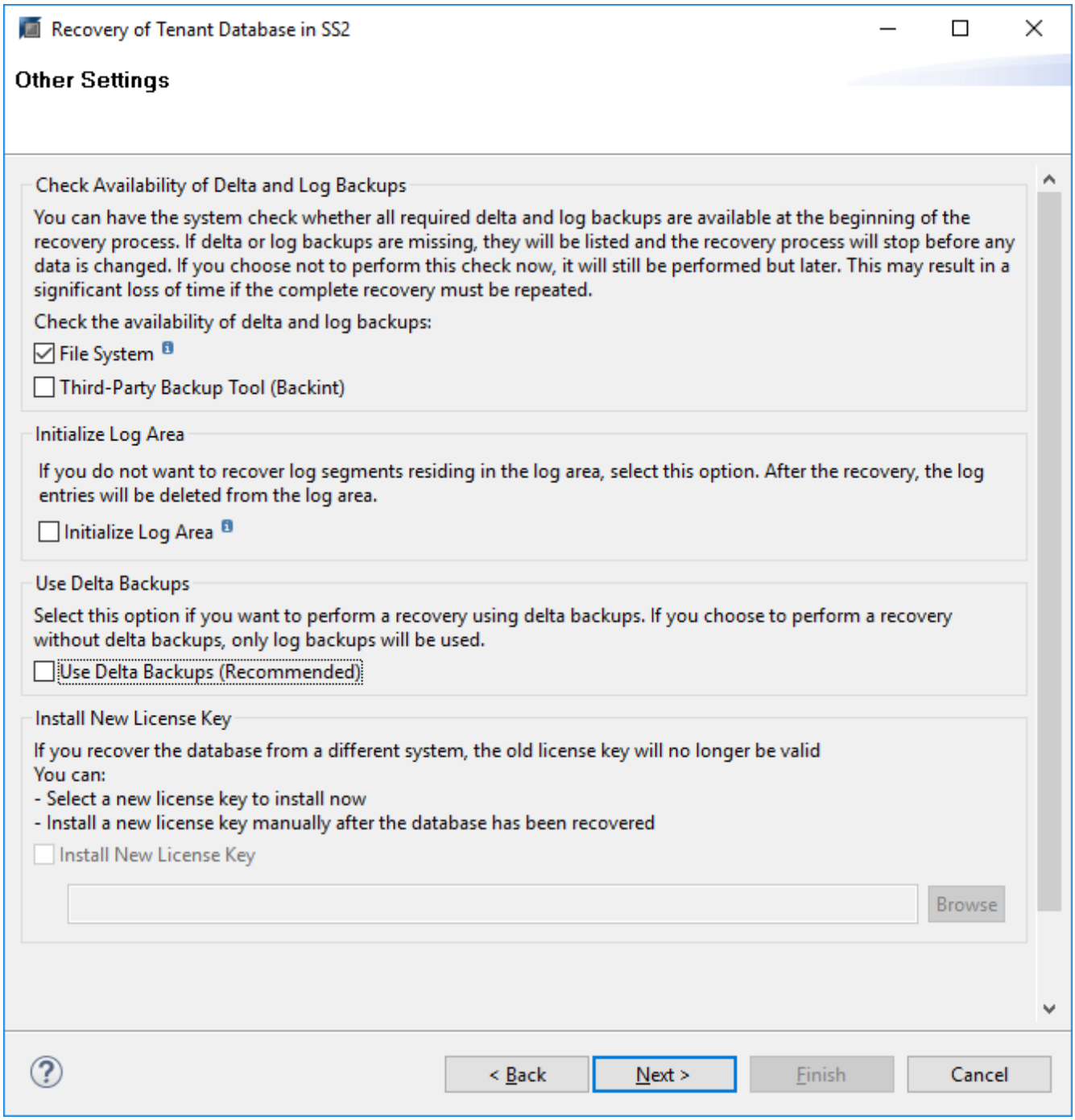

26. システムデータベースのリカバリ前にデータボリュームのリストアが実行されたため、テナントバックアップをすぐに使用できます。緑色でハイライトされたバックアップを選択し、次へをクリックします。



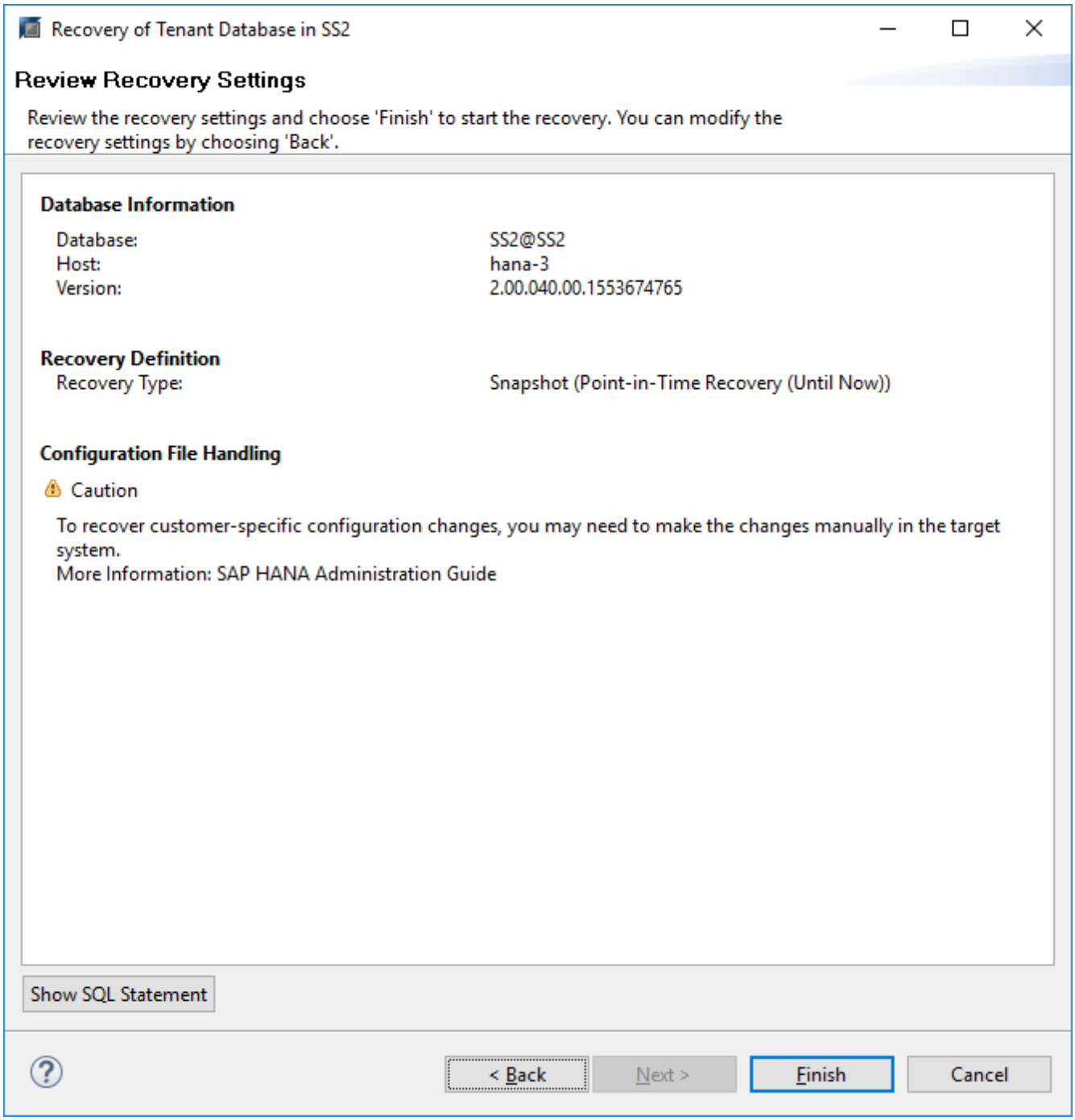

27. ログのバックアップ先を確認し、 Next （次へ）をクリックします。



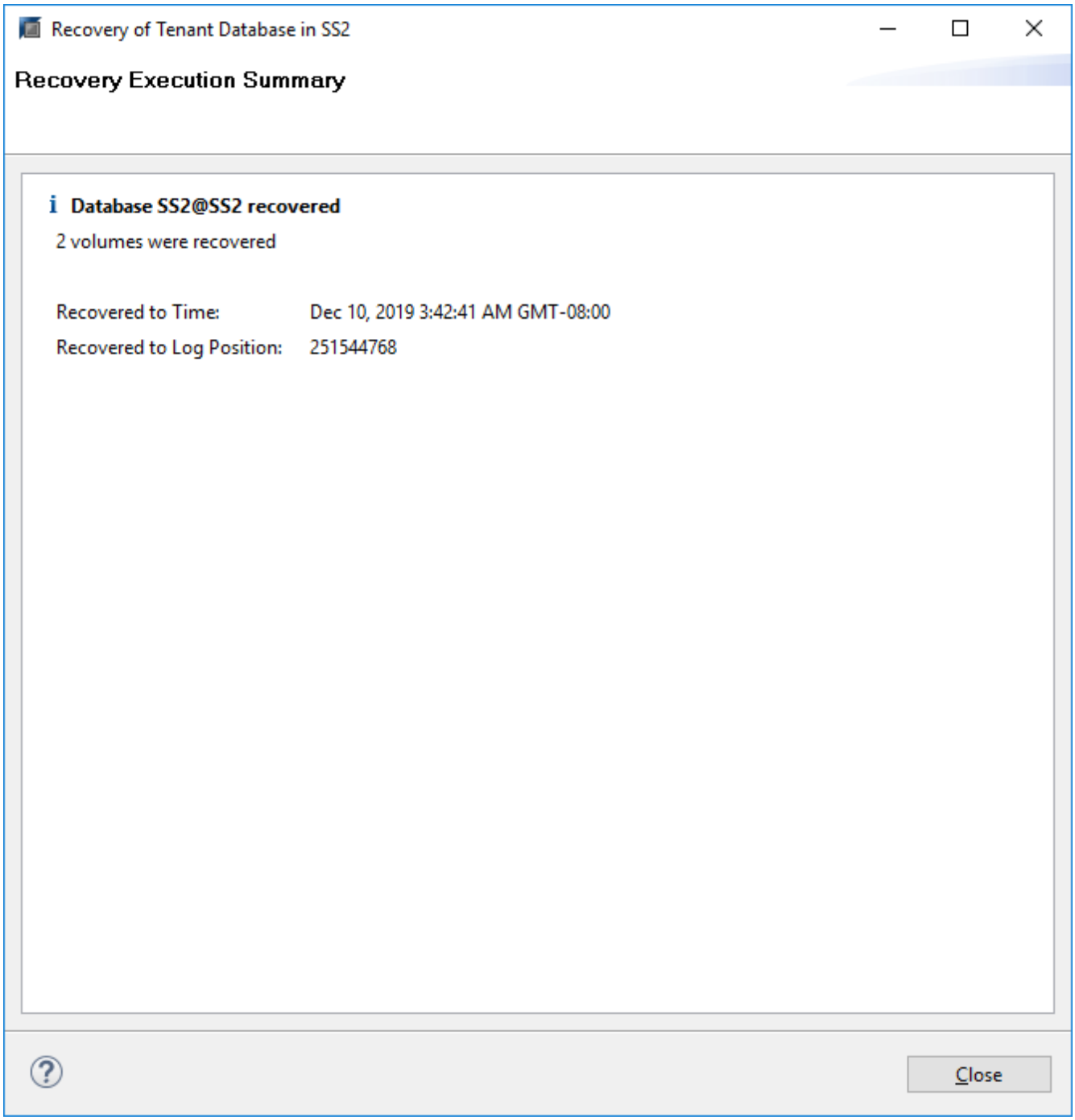

28. 必要に応じて、他の設定を選択します。［デルタバックアップを使用］が選択されていないことを確認します。次へをクリックします。




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

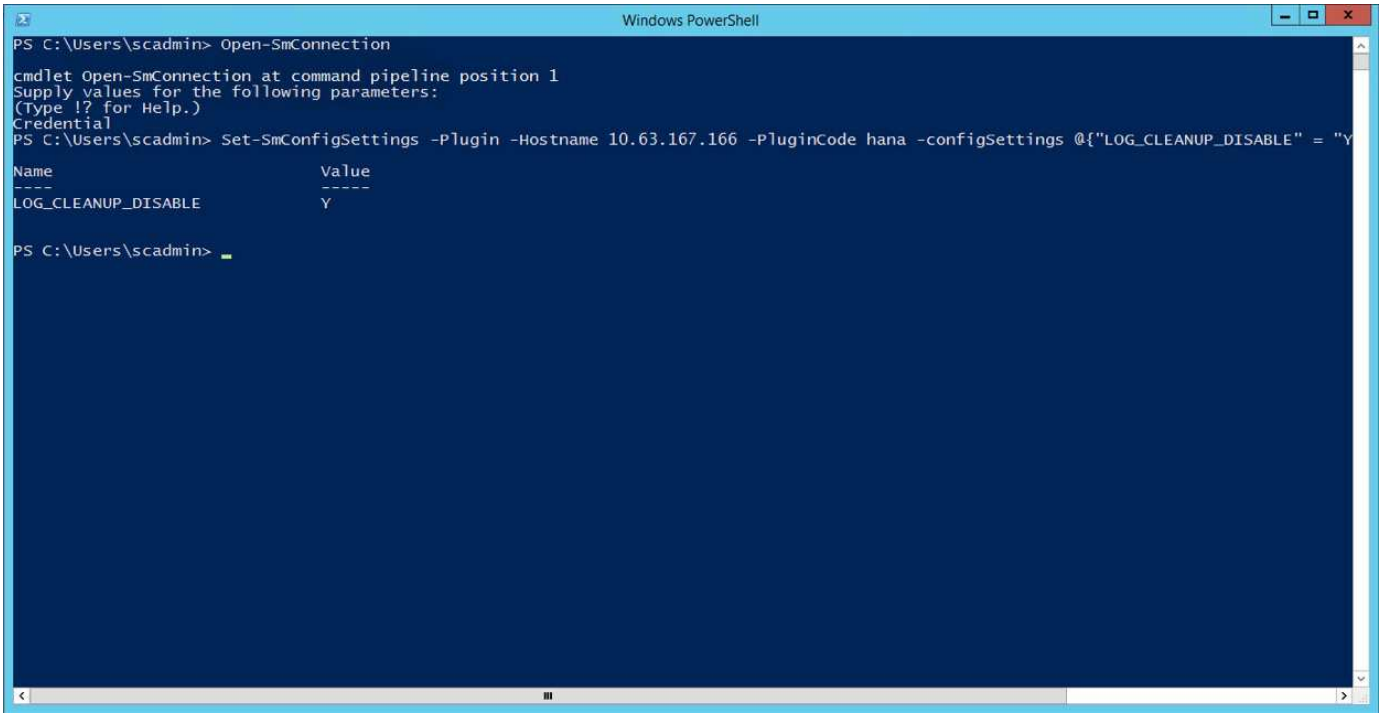
hana.property` 構成ファイルのパラメータ log_cleanup_disable=Y' を指定すると ' この SAP HANA プラグイン・ホストを通信ホストとして使用して ' すべてのリソースのログ・バックアップ・ハウスキーピングが無効になります

- 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

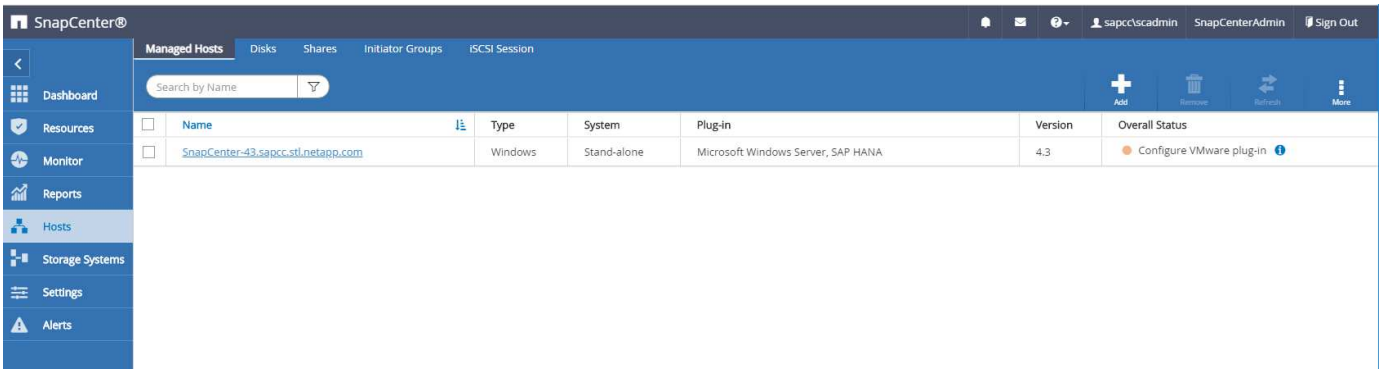
2 つ目のオプションでは、 SnapCenter PowerShell コマンドを使用します。

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

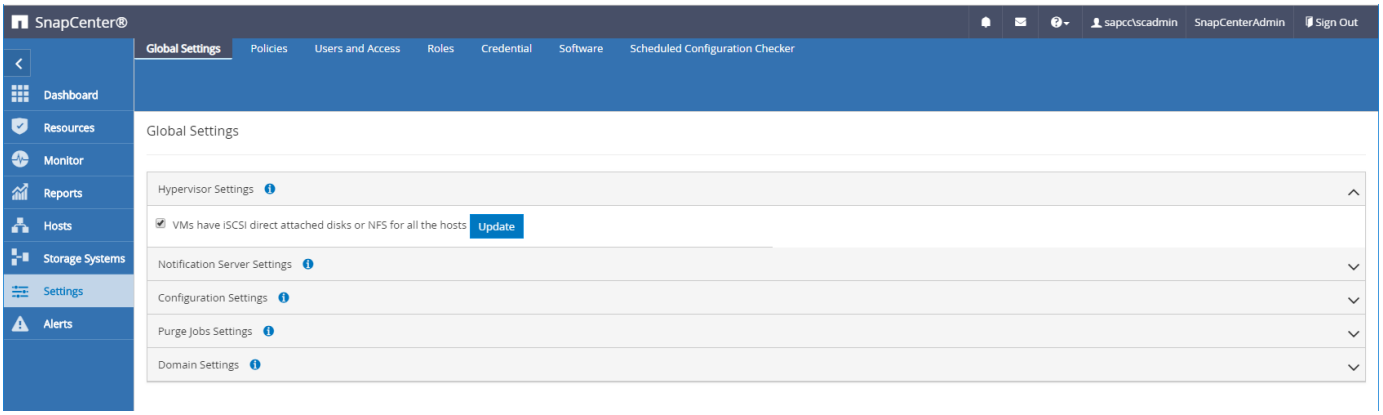
SnapCenter は、 SAP HANA プラグインが仮想環境にインストールされているかどうかを検出します。これは、パブリッククラウドプロバイダでの VMware 環境や SnapCenter 環境の場合があります。この場合、次の図に示すように、ハイパーバイザーの設定に関する警告が SnapCenter に表示されます。




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

セクションで説明したように、"「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によって処理されます。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。

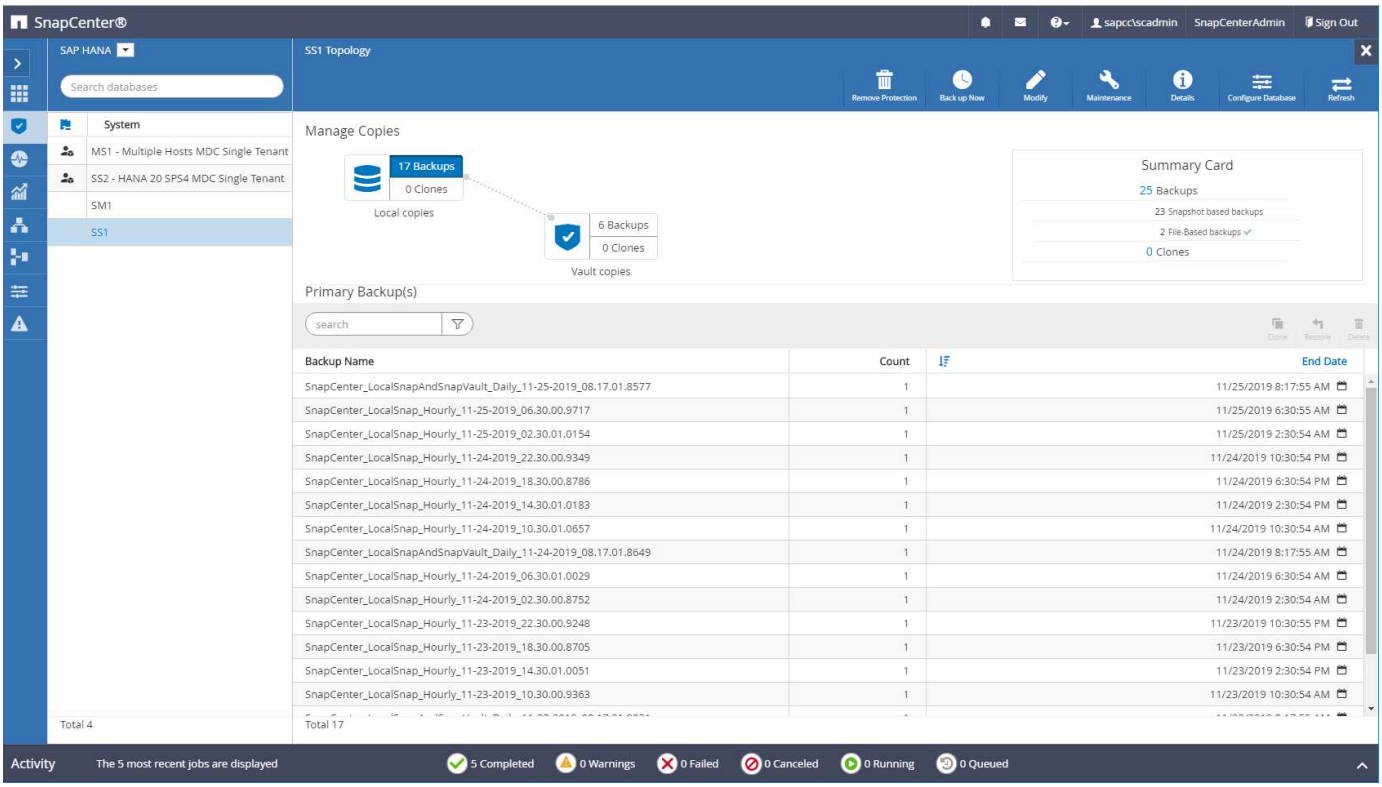
スケジュールされたこのクリーンアップが完了するまでの間、 SAP HANA と SnapCenter では、オフサイトのバックアップストレージからすでに削除されたバックアップが引き続き表示されることがあります。

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

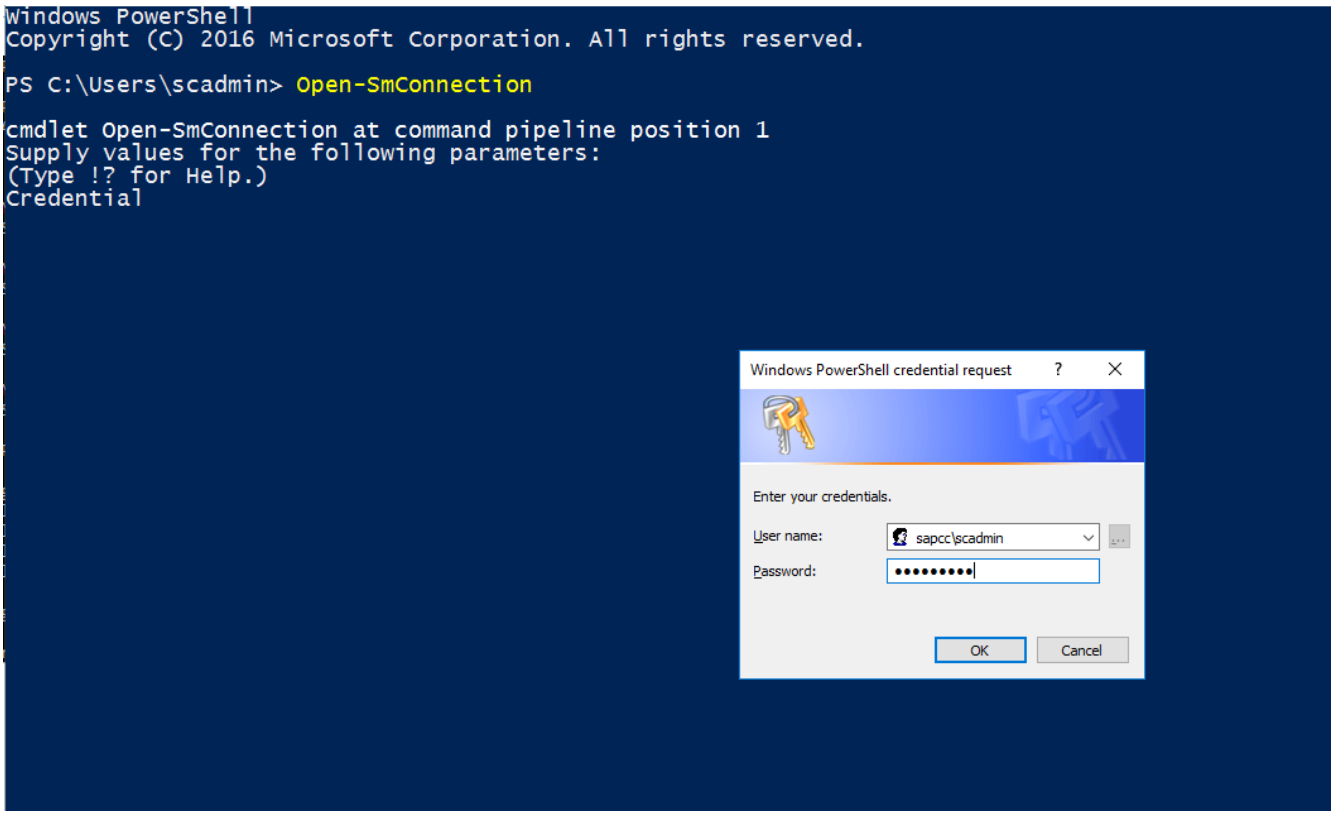
リソースのトポロジビューでは、次のスクリーンショットに示すように、セカンダリバックアップを選択する際に、 SnapCenter によってオフサイトのバックアップストレージにバックアップが表示されます。SnapCenter は、更新アイコンを使用してクリーンアップ処理を実行し、このリソースのバックアップを同期します。




**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。

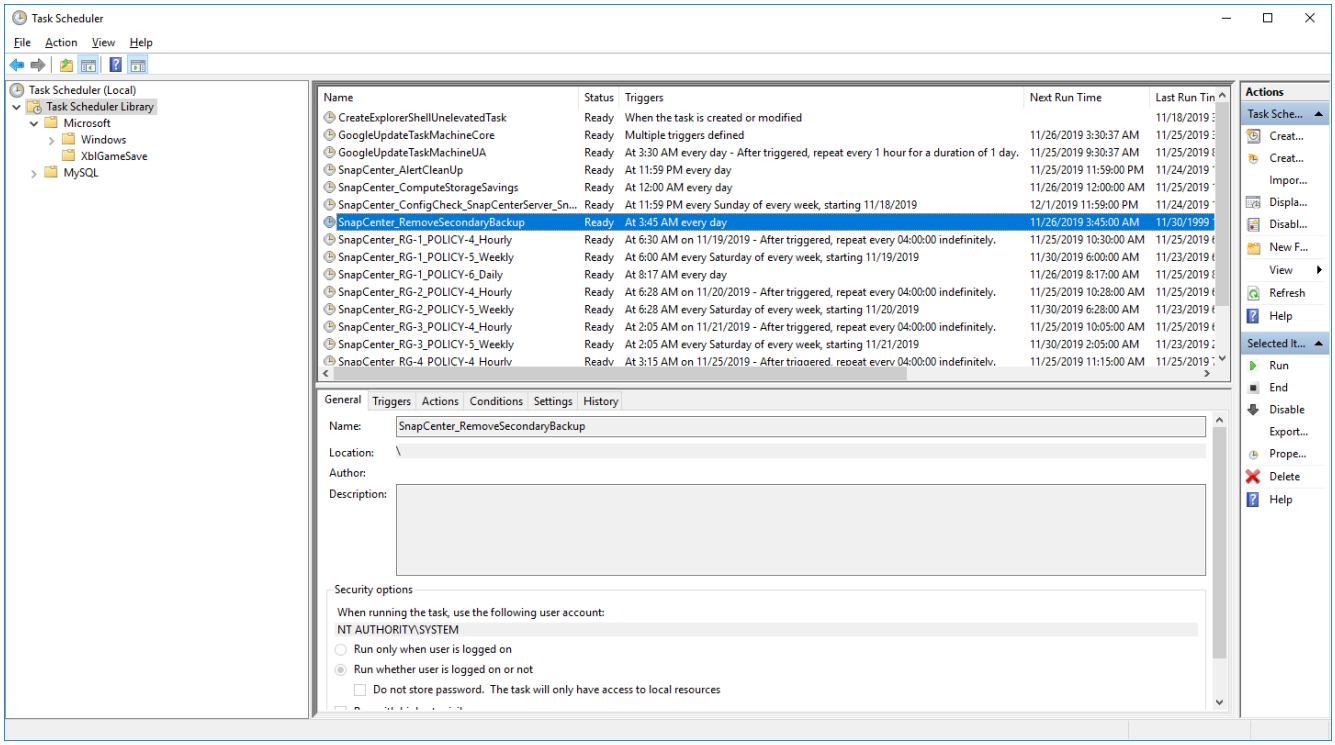
1. SnapCenter サーバで PowerShell コマンドウィンドウを起動します。
2. SnapCenter サーバへの接続を開き、ログインウィンドウに SnapCenter 管理者のクレデンシャルを入力します。




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 』

  "SnapCenterを使用したSAPシステムコピーの自動化"

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

  "SnapCenter を使用した SAP HANA システムのレプリケーション、バックアップ、リカバリ"

- 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。<br>• 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：<br>新しいデータボリュームリソース<br>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。<br>• SnapCenter 4.3を対象としたアップデート：<br>自動検出<br>リストアとリカバリの自動化<br>HANA MDCの複数テナントをサポート<br>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：<br>SnapCenter 4.3.1でのNFSv4のサポート<br>SSL通信の設定<br>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。<br>• 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。 |

# SnapCenter、SnapMirror Active Sync、VMware Metro Storage ClusterによるSAP HANAのデータ保護と高可用性

## SnapCenter、SnapMirror Active Sync、VMware Metro Storage ClusterによるSAP HANAのデータ保護と高可用性

このドキュメントでは、HANAストレージリソースの高可用性ソリューションとしてのSnapMirror Active Syncと組み合わせて、VMware環境でSnapCenterを使用したデータ保護のベストプラクティスを紹介します。

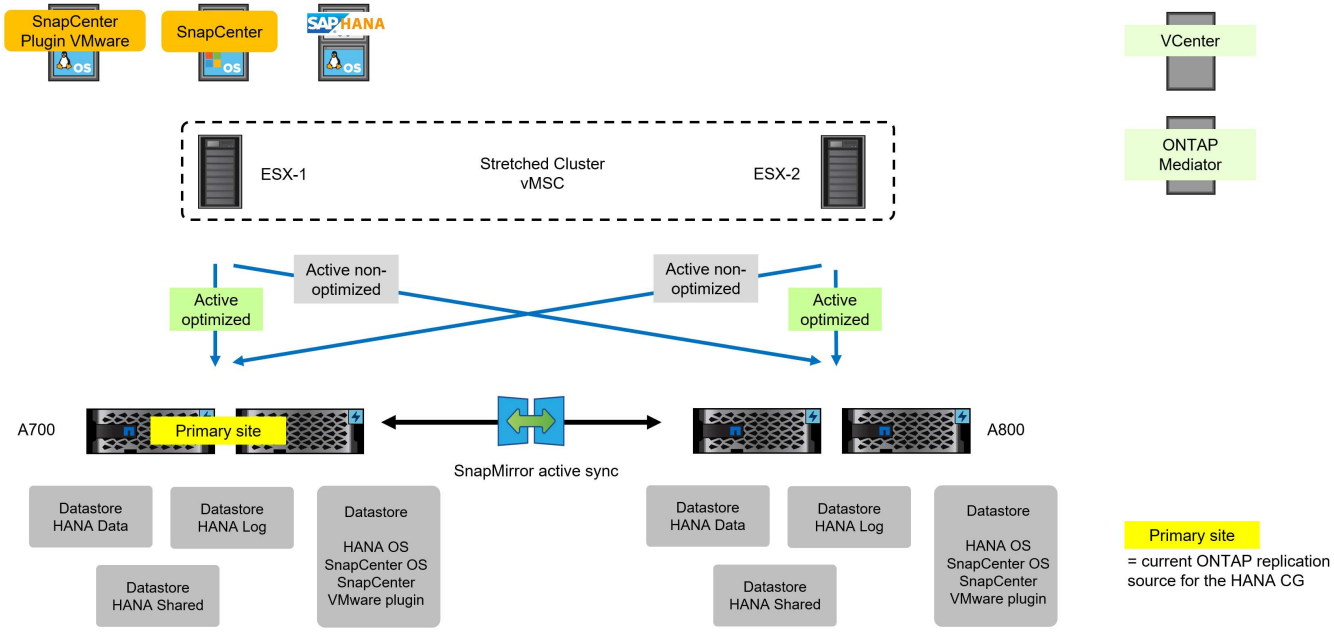
作成者：Nils Bauer、NetApp

本ドキュメントの内容

このドキュメントは、環境全体のセットアップ方法を段階的に説明することを目的としたものではありませんが、以下に関連する概念と関連する詳細について説明します。

- VMware VMFSを使用したSAP HANAシステムのセットアップ
- SAP HANA向けのSnapMirrorアクティブ同期構成
- VMFSを使用したVMware上のHANA向けのSnapCenter構成
- SnapMirrorアクティブ同期のためのSnapCenter設定
- VMware上のHANAでのSnapCenterの運用とSnapMirrorのアクティブな同期

ここでは、次の図に示すように、SnapMirrorアクティブ同期の統一されたアクセス設定を使用するVMware Metro Storage Cluster（vMSC）構成に焦点を当てますが、ベアメタルおよび不統一のアクセス設定についても簡単に説明します。




# SAP HANAの高可用性の概要

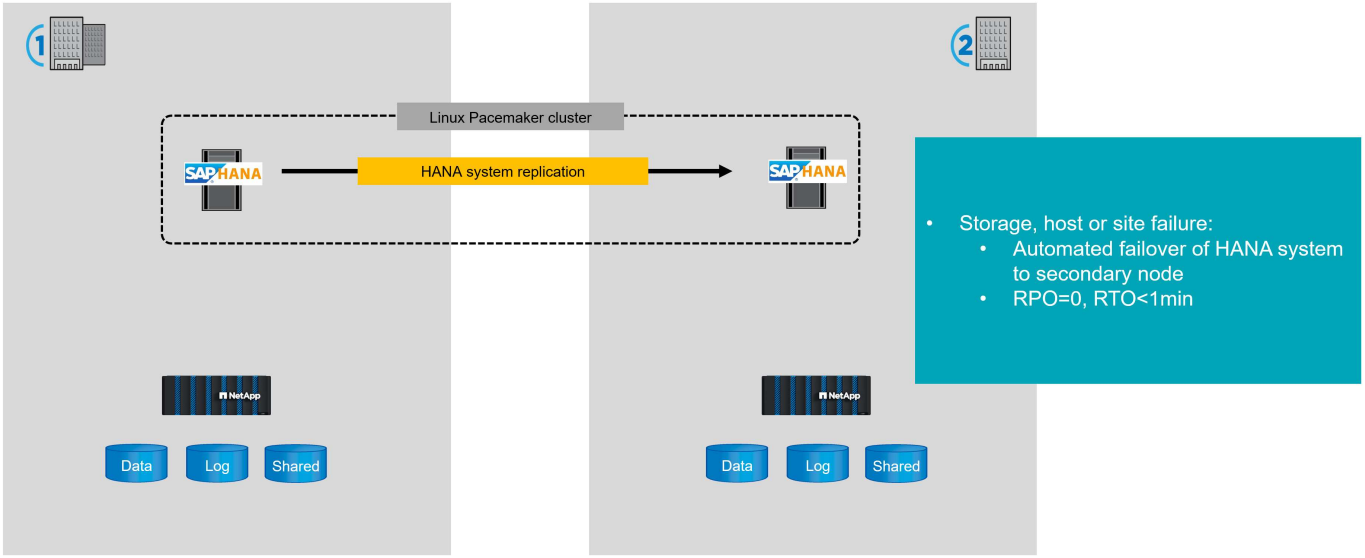
この章では、アプリケーションレイヤでのレプリケーションとストレージレプリケーションを比較した、SAP HANAの高可用性オプションの概要を説明します。

## SAP HANAシステムレプリケーション（HSR）

SAP HANAシステムレプリケーションでは、データが同期的にレプリケートされ、メモリにプリロードされ、セカンダリホストで継続的に更新される処理モードが提供されます。このモードでは、RTO値は約1分以下と非常に低くなりますが、ソースシステムからのレプリケーションデータの受信にのみ使用される専用サーバも必要です。フェイルオーバー時間が短いため、SAP HANAシステムのレプリケーションは、HANAソフトウェアのアップグレードなど、ダウンタイムがほぼゼロのメンテナンス処理にもよく使用されます。通常、Linux Pacemakerクラスタソリューションは、フェイルオーバー処理の自動化に使用されます。

プライマリサイト、ストレージ、ホスト、または完全なサイトで障害が発生した場合、HANAシステムはLinux Pacemakerクラスタで制御されているセカンダリサイトに自動的にフェイルオーバーします。

すべての設定オプションとレプリケーションシナリオの詳細については、を参照してください "SAP HANAシステムレプリケーション| SAPヘルプポータル"。




**NetApp SnapMirror**アクティブ同期

SnapMirror Active Syncを使用すると、サイト全体に障害が発生してもビジネスサービスの運用を継続できるため、アプリケーションがセカンダリコピーを使用して透過的にフェイルオーバーできるようになります。SnapMirrorアクティブ同期でフェイルオーバーをトリガーするための手動操作やカスタムスクリプトは必要ありません。SnapMirrorアクティブ同期は、AFFクラスタ、オールフラッシュSANアレイ（ASA）クラスタ、およびCシリーズ（AFFまたはASA）でサポートされます。SnapMirrorアクティブ同期は、iSCSI LUNまたはFCP LUNを使用してアプリケーションを保護します。

ONTAP 9.15.1以降では、SnapMirrorアクティブ同期で対称アクティブ/アクティブ機能がサポートされます。対称アクティブ/アクティブ：双方向同期レプリケーションにより、保護されたLUNの両方のコピーからの読み取りおよび書き込みI/O処理を有効にし、両方のLUNコピーがローカルでI/O処理を処理できるようにします。

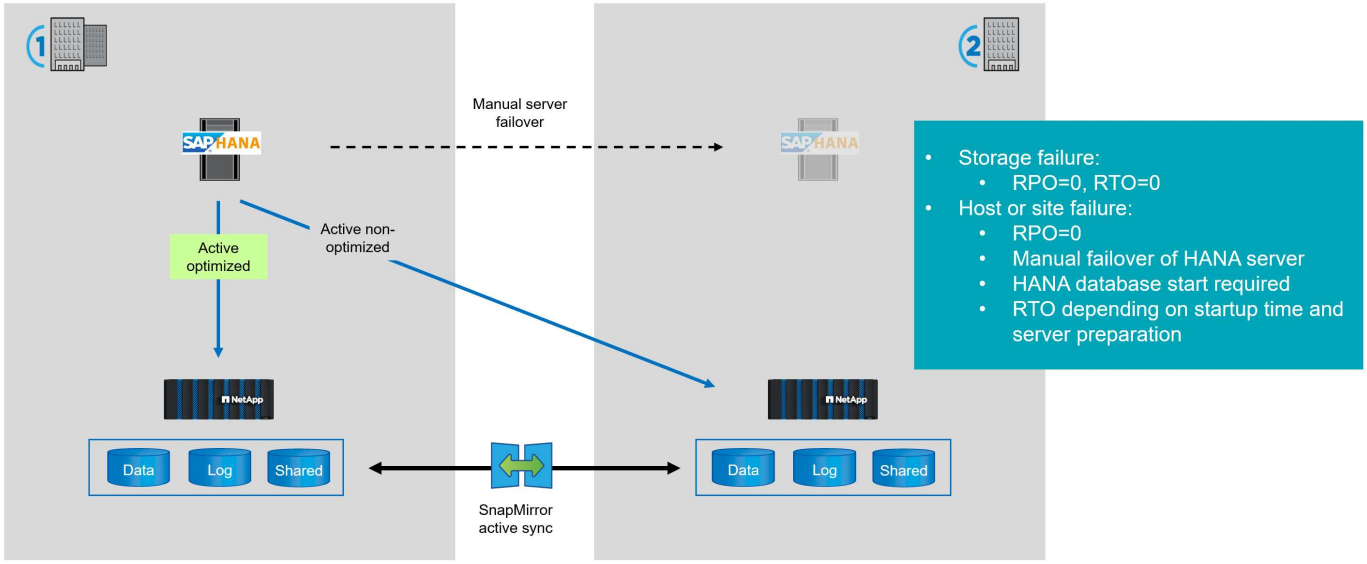
詳細については、を参照してください "ONTAPでのSnapMirrorアクティブ同期の概要"。

#### **HANA**ベアメタル

ベアメタルサーバでSAP HANAを実行している場合は、SnapMirrorアクティブ同期を使用して可用性の高いストレージソリューションを提供できます。データは同期的にレプリケートされるため、RPO=0になります。

ストレージ障害が発生した場合、HANAシステムは2つ目のFCPパスを使用してセカンダリサイトのミラーコピーに透過的にアクセスし、RTO = 0を実現します。

ホストまたはサイト全体に障害が発生した場合は、障害が発生したホストのデータにアクセスするために、セカンダリサイトに新しいサーバを用意する必要があります。これは通常、本番システムと同じサイズのテストシステムまたはQAシステムで、シャットダウンして本番システムの実行に使用します。セカンダリサイトのLUNを新しいホストに接続したら、HANAデータベースを起動する必要があります。そのため、合計RTOは、ホストのプロビジョニングに必要な時間とHANAデータベースの起動時間に左右されます。

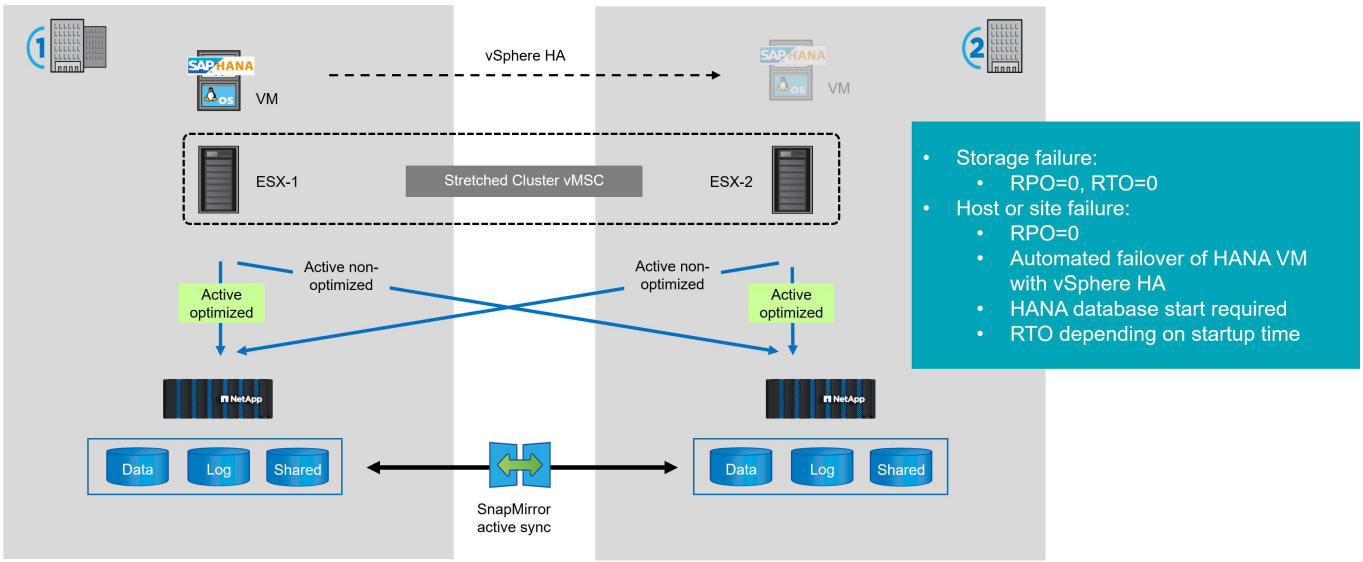



**vSphere Metro Storage Cluster（vMSC）**

FCPに接続されたデータストアを使用するVMware環境でSAP HANAを実行している場合は、SnapMirrorのアクティブ同期を使用してVMware Metroストレージクラスタを構築できます。このようなセットアップでは、HANAシステムで使用されるデータストアがセカンダリサイトに同期的にレプリケートされます。

ストレージに障害が発生した場合、ESXホストはセカンダリサイトのミラーコピーに自動的にアクセスし、RTO = 0を実現します。

ホストまたはサイト全体に障害が発生した場合は、vSphere HAを使用してセカンダリESXホストでHANA VMを起動します。HANA VMを実行したら、HANAデータベースを起動する必要があります。そのため、総RTOは主にHANAデータベースの起動時間に依存します。



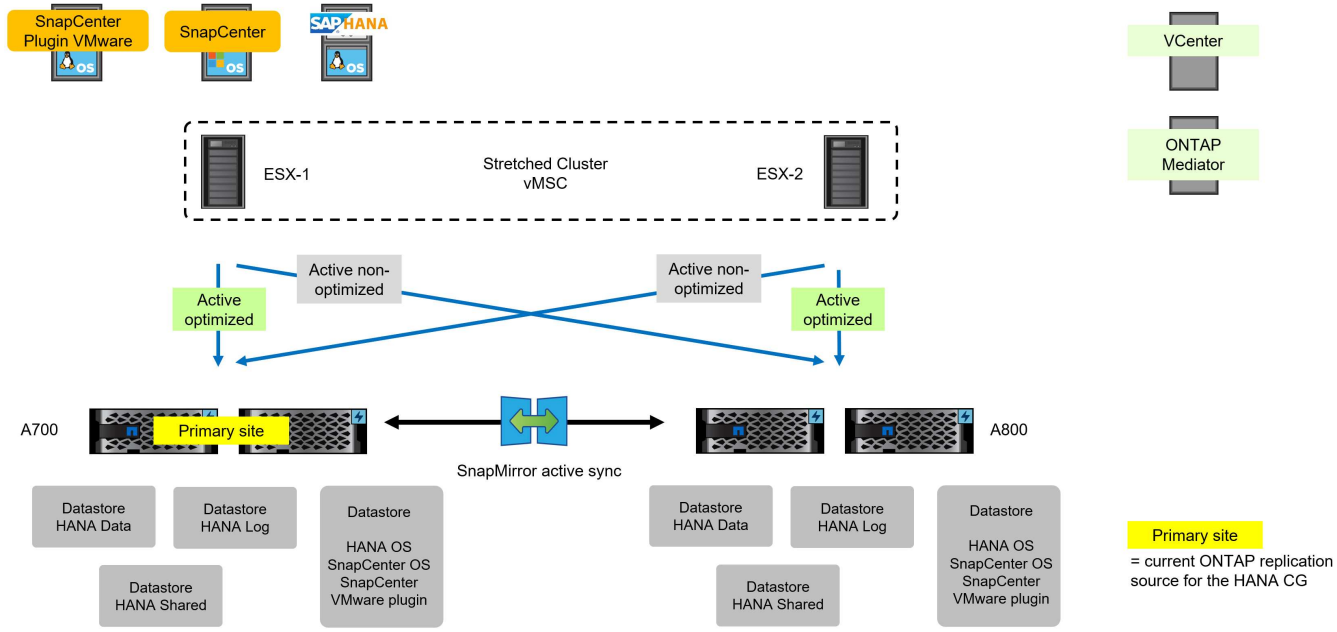

ソリューションの比較

次の表は、上記のソリューションの主な特徴をまとめたものです。

| | **HANA** システムレプリケーション | **SnapMirror**アクティブ同期**–**ベアメタル | **SnapMirror**アクティブ同期**–VMware vMSC** |
|---|---|---|---|
| 障害発生時のRPO | RPO = 0 +同期レプリケーション | | |
| ストレージ障害時のRTO | RTO <1分 | RTO = 0 +透過的なストレージフェイルオーバー | |
| サイトまたはホストの障害が発生した場合のRTO + | RTO <1分 | RTO：サーバの準備とHANAデータベースの起動に必要な時間によって異なります。 | RTO：HANAデータベースの起動に必要な時間によって異なります。 |
| フェイルオーバーの自動化 | はい、<br><br>セカンダリHSRホストへの自動フェイルオーバー<br><br>Pacemakerクラスタによって制御されます。 | ○（ストレージ障害の場合）<br><br>いいえ（ホストまたはサイトの障害）<br><br>（ホストのプロビジョニング、ストレージリソースの接続、HANAデータベースの起動） | ○（ストレージ障害の場合）<br><br>○（ホストまたはサイトの障害時）<br><br>（他のサイトへのVMのフェイルオーバーは、vSphere HAとHANAデータベースの起動によって自動化されます） |
| セカンダリサイトに専用サーバが必要 | はい、<br><br>データをメモリにプリロードし、データベースの起動なしで高速フェイルオーバーを実現するために必要です。 | いいえ、<br><br>サーバは、フェールオーバーの場合にのみ必要です。通常、QAに使用されるサーバは本番環境に使用されます。 | いいえ、<br><br>ESXホストのリソースは、フェイルオーバーの場合にのみ必要です。通常、QAリソースは本番環境に使用されます。 |

## セツテイノカイヨウレイ

ラボのセットアップでは、両方のESXホストが両方のストレージクラスタにアクセスできる、統一されたアクセス構成を使用します。次のセクションでは、ユニフォームアクセス設定について説明しますが、ユニフォーム設定ではない場合の違いについても説明します。




ソフトウェアバージョン

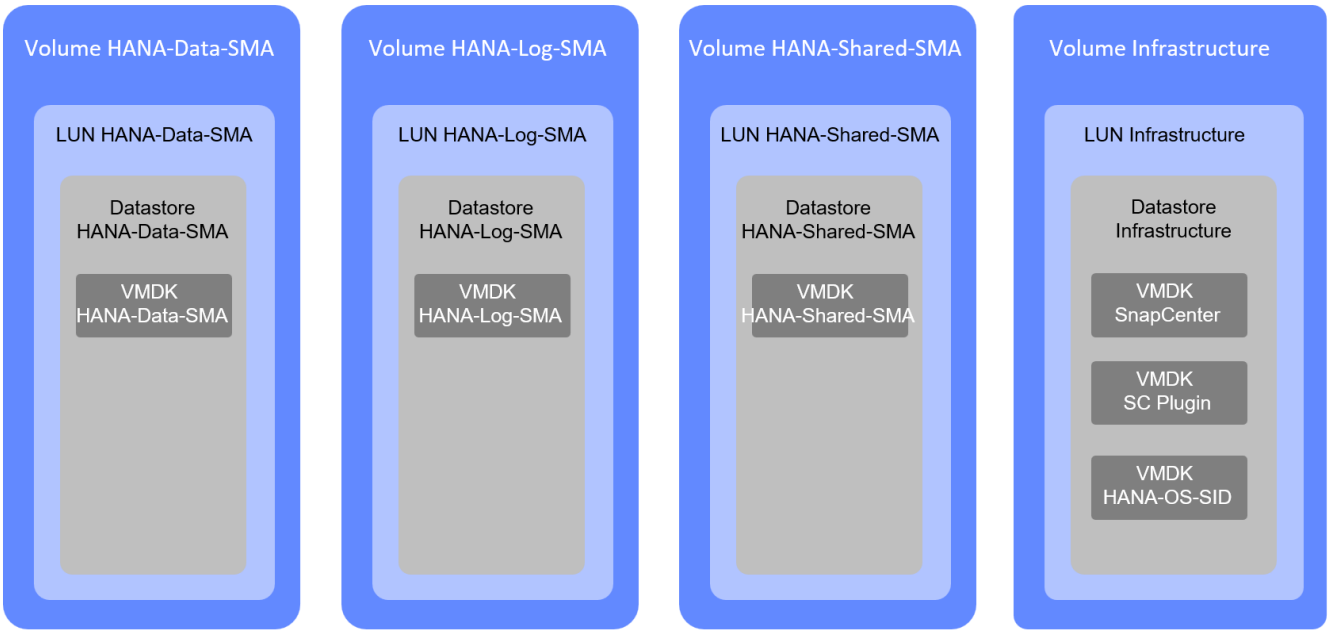
| ソフトウェア | バージョン |
| --- | --- |
| ONTAP | A700：9.15.1P7、A800：9.16.1RC1 |
| vSphereクライアント | 8.0.3 |
| ESXi | 8.0.3 |
| vSphere用SnapCenterプラグイン | 6.0.1 |
| Linux OS | SLES for SAP 15 SP5 |
| SAP HANA のサポート | 2.0 SPS8 |
| SnapCenter | 6.0.1 |

## HANAシステムのプロビジョニングとインストール

この章では、VMFSを使用するVMware環境に固有のSAP HANAシステムのインストールと設定について説明します。その他の一般的なベストプラクティスについては、を参照してください"『 SAP HANA on NetApp AFF Systems with Fibre Channel Protocol 』を参照してください"。

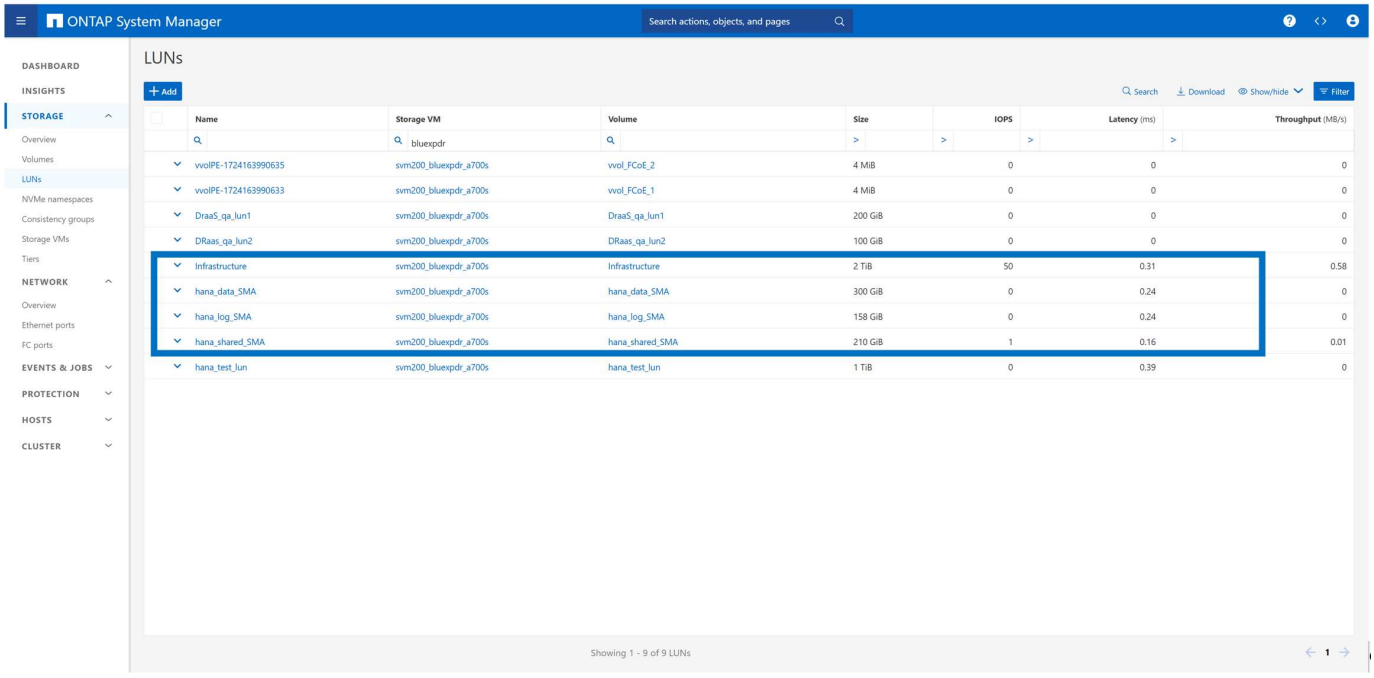
ストレージ構成

次の図は、HANAシステムのストレージとデータストアの構成を示しています。HANAシステムのファイルシステムごとに専用のボリューム、LUN、データストアを設定する必要があります。複数のHANAシステム間やその他のワークロード間でデータストアを共有しないでください。




HANAシステムの3つのLUN（hana_+data+*SMA*、*hana_+LOG* +SAMおよびhana_+shared_SMA）と、OSイメージ用のLUNとSnapCenterコンポーネント用のLUNがすべてA700ストレージクラスタでプロビジョニングされている。

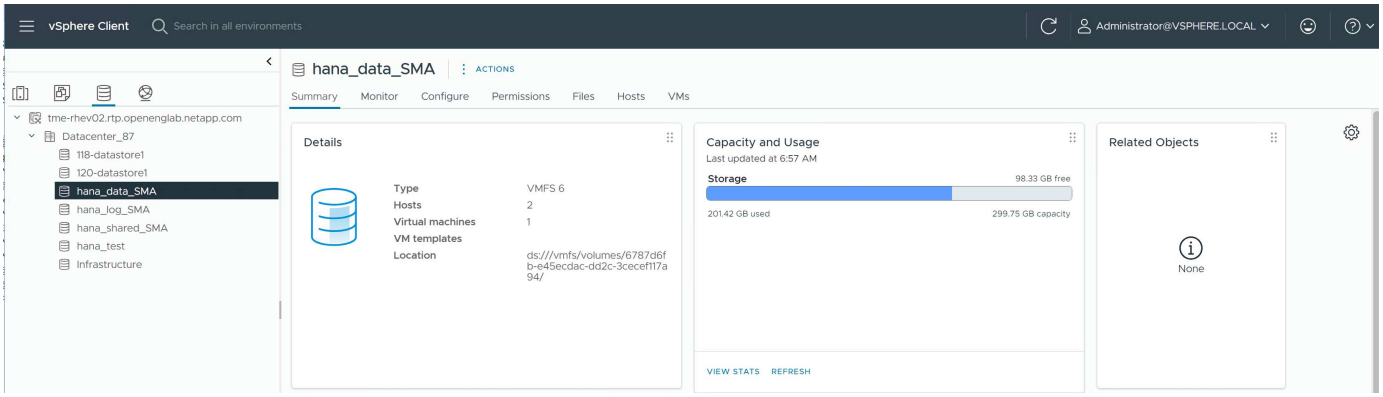
HANAシステムのボリュームは、すべて同じSVM内にプロビジョニングする必要があります。後述するSnapMirrorアクティブ同期構成では、3つのHANAボリュームすべてにわたって整合グループを作成します。そのためには、ボリュームが同じSVM内にある必要があります。インフラボリュームは別の整合グループに配置されるため、別のSVMに配置することもできます。




イニシエータグループを設定し、このラボ環境のA700ストレージシステムのすぐ近くにあるESX-1ホストに上記のLUNをマッピングする必要があります。

データストアのプロビジョニング

以前にプロビジョニングした3つのLUNを使用して、HANAシステム用に3つのデータストアを作成しました。また、インフラLUNを使用してインフラデータストアを作成しました。

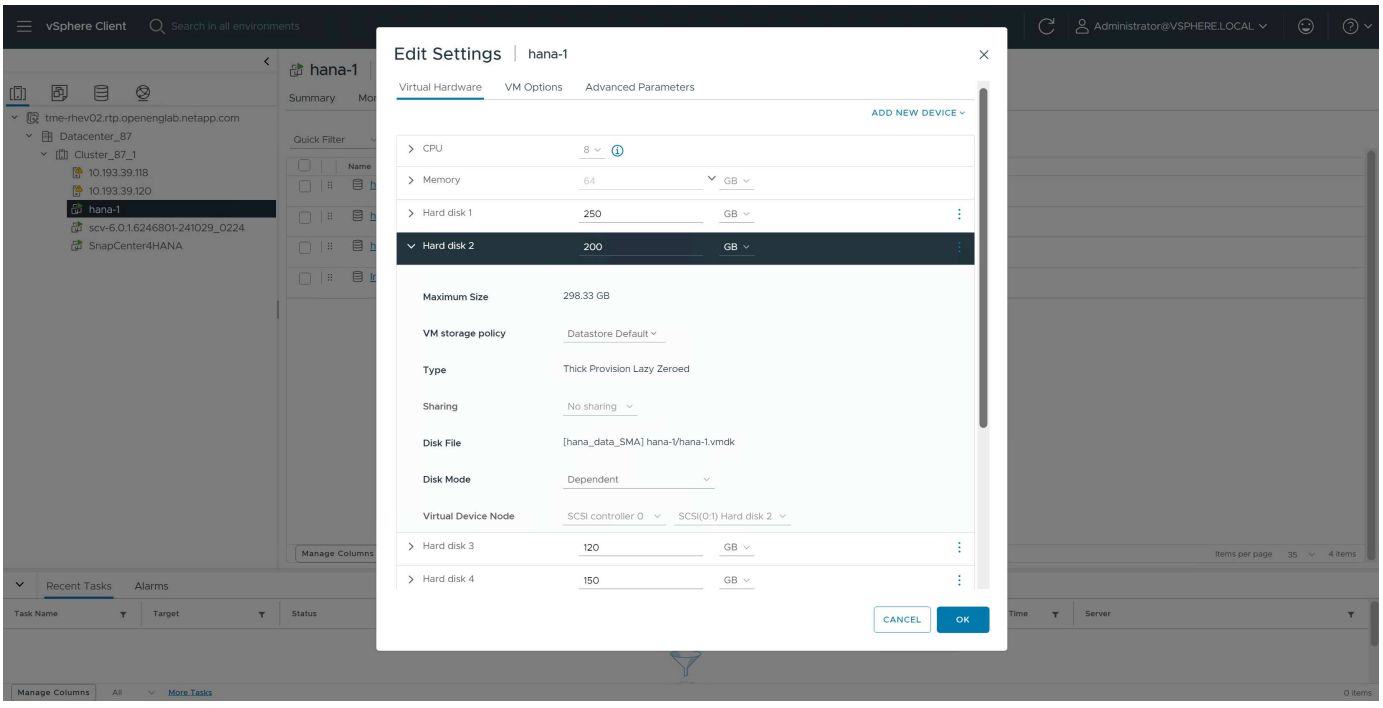



**VM**のプロビジョニングと**OS**のインストール

ラボのセットアップでは、新しいVMを導入し、Linux OS用のVMDKをインフラデータストアに配置しました。

**VM**ディスク構成

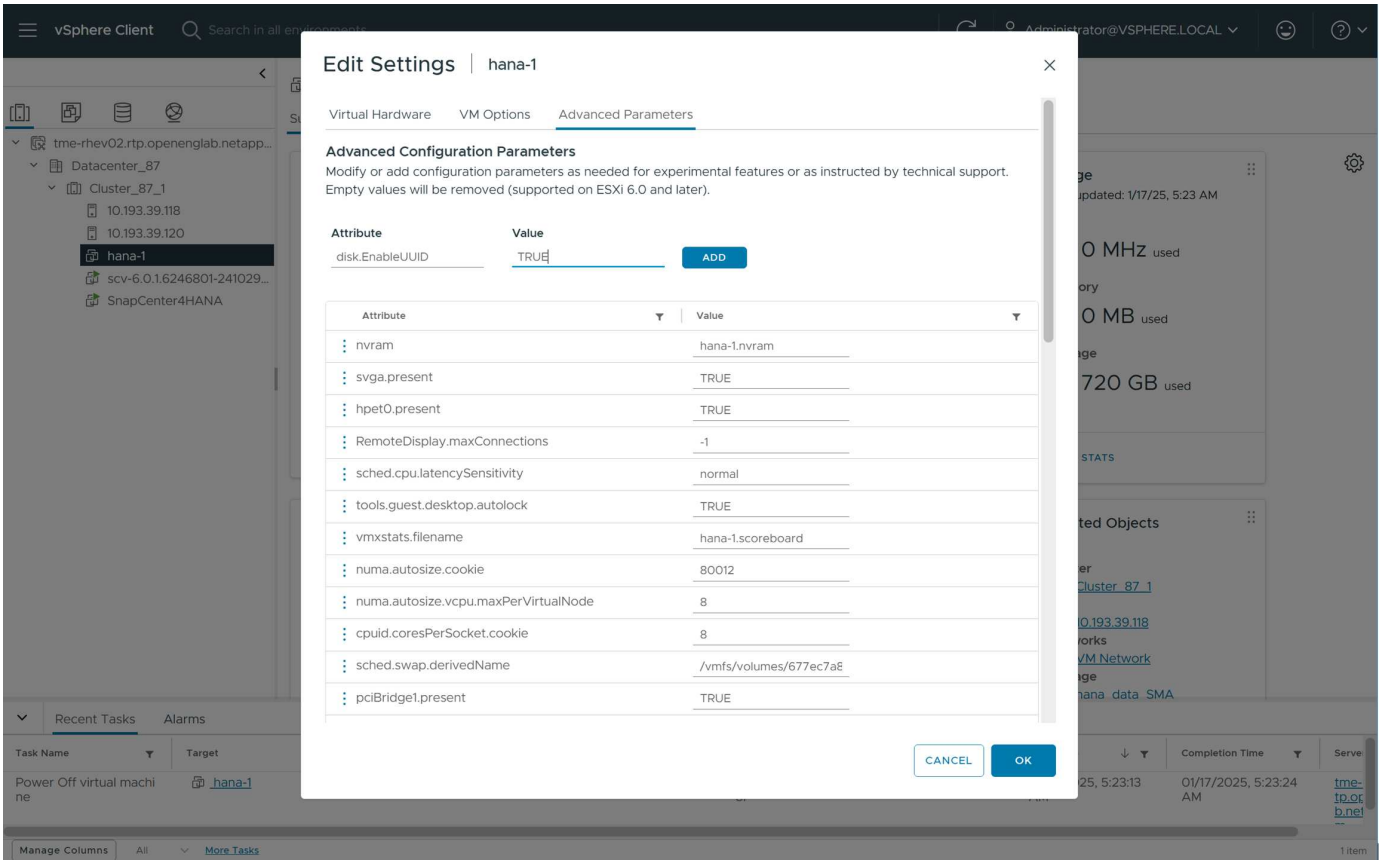
HANA VMに3本の新しいディスクが追加されました。各ディスクは、HANAシステム用に作成されたいずれかのデータストア内にあります。




**VM**パラメータの設定

パラメータdisk.EnableUUIDを追加し、trueに設定する必要があります。SnapCenterではパラメータは必須です。設定しないと、SnapCenterの[Discover virtual resource]処理が失敗します。

パラメータを追加する前に、VMを停止する必要があります。




この機能は、以下のコマンドで確認できます。

```
hana-1:~ # sg_inq /dev/sdd
standard INQUIRY:
PQual=0 PDT=0 RMB=0 LU_CONG=0 hot_pluggable=0 version=0x06 [SPC-4]
[AERC=0] [TrmTsk=] NormACA=0 HiSUP=0 Resp_data_format=2
SCCS=0 ACC=0 TPGS=0 3PC=0 Protect=0 [BQue=0]
EncServ=0 MultiP=0 [MChngr=0] [ACKREQQ=0] Addr16=0
[RelAdr=0] WBus16=1 Sync=1 [Linked=0] [TranDis=0] CmdQue=1
length=36 (0x24) Peripheral device type: disk
Vendor identification: VMware
Product identification: Virtual disk
Product revision level: 2.0
Unit serial number: 6000c293fecf25ac6bc457af67fe1f54
```

### **Linux**ホストテノフアイルシステムノシユンヒ

新しいディスクでの**xfs**ファイルシステムの作成

新しいディスクのデバイス名は、以下のコマンドで確認できます。

```
hana-1:/install # lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 250G 0 disk
├─sda1 8:1 0 256M 0 part /boot/efi
└─sda2 8:2 0 82G 0 part
├─system-root 254:0 0 60G 0 lvm /root
│ /var
│ /usr/local
│ /tmp
│ /srv
│ /opt
│ /home
│ /boot/grub2/x86++_++64-efi
│ /boot/grub2/i386-pc
│ /.snapshots
│ /
└─system-swap 254:1 0 2G 0 lvm SWAP
sdb 8:16 0 200G 0 disk
sdc 8:32 0 120G 0 disk
sdd 8:48 0 150G 0 disk
sr0 11:0 1 1024M 0 rom
hana-1:/install #
```

3つの新しいディスクそれぞれにxfsファイルシステムが作成されている。

```
hana-1:/install # mkfs.xfs /dev/sdb
meta-data=/dev/sdb isize=512 agcount=4, agsize=7864320 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=31457280, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=15360, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0

hana-1:/install # mkfs.xfs /dev/sdc
meta-data=/dev/sdc isize=512 agcount=4, agsize=7864320 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=31457280, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=15360, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0

hana-1:/install # mkfs.xfs /dev/sdd
meta-data=/dev/sdd isize=512 agcount=4, agsize=9830400 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=39321600, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=19200, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
hana-1:/install #
```

マウントポイントの作成

```
hana-1:/ # mkdir -p /hana/data/SMA/mnt00001
hana-1:/ # mkdir -p /hana/log/SMA/mnt00001
hana-1:/ # mkdir -p /hana/shared
hana-1:/ # chmod –R 777 /hana/log/SMA
hana-1:/ # chmod –R 777 /hana/data/SMA
hana-1:/ # chmod -R 777 /hana/shared
```

**/etc/fstab**の設定

```
hana-1:/install # cat /etc/fstab
/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=/@/var 0 0
/dev/system/root /usr/local btrfs subvol=/@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=/@/tmp 0 0
/dev/system/root /srv btrfs subvol=/@/srv 0 0
/dev/system/root /root btrfs subvol=/@/root 0 0
/dev/system/root /opt btrfs subvol=/@/opt 0 0
/dev/system/root /home btrfs subvol=/@/home 0 0
/dev/system/root /boot/grub2/x86_64-efi btrfs subvol=/@/boot/grub2/x86_64-
efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=/@/.snapshots 0 0
UUID=2E8C-48E1 /boot/efi vfat utf8 0 2
/dev/sdb /hana/data/SMA/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/SMA/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
hana-1:/install #

hana-1:/install # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 4.0K 49G 1% /dev/shm
tmpfs 13G 26M 13G 1% /run
tmpfs 4.0M 0 4.0M 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 35G 25G 58% /
/dev/mapper/system-root 60G 35G 25G 58% /.snapshots
/dev/mapper/system-root 60G 35G 25G 58% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 35G 25G 58% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 35G 25G 58% /home
/dev/mapper/system-root 60G 35G 25G 58% /opt
/dev/mapper/system-root 60G 35G 25G 58% /srv
/dev/mapper/system-root 60G 35G 25G 58% /tmp
/dev/mapper/system-root 60G 35G 25G 58% /usr/local
/dev/mapper/system-root 60G 35G 25G 58% /var
/dev/mapper/system-root 60G 35G 25G 58% /root
/dev/sda1 253M 5.1M 247M 3% /boot/efi
tmpfs 6.3G 56K 6.3G 1% /run/user/0
/dev/sdb 200G 237M 200G 1% /hana/data/SMA/mnt00001
/dev/sdc 120G 155M 120G 1% /hana/log/SMA/mnt00001
/dev/sdd 150G 186M 150G 1% /hana/shared
hana-1:/install #
```

**HANA**のインストール

これで、HANAのインストールを実行できます。

> ここで説明した設定では、OS VMDK上に/usr/sap/smaディレクトリが作成されます。/usr/sap/smaを共有VMDKに格納する必要がある場合は、HANA共有ディスクをパーティショニングして、/usr/sap/smaに別のファイルシステムを提供できます。

**SnapCenter**のユーザストアキー

システムデータベースユーザのユーザストアを作成し、SnapCenterで使用する必要があります。通信ポートに応じてHANAインスタンス番号を設定する必要があります。セットアップでは、インスタンス番号「00」が使用されます。

詳細については、を参照してください。"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"

```
smaadm@hana-1:/usr/sap/SMA/HDB00> hdbuserstore set SMAKEY hana-1:30013
SNAPCENTER <password>
Operation succeed.
```

接続は、以下のコマンドで確認できます。

```
smaadm@hana-1:/usr/sap/SMA/HDB00> hdbsql -U SMAKEY
Welcome to the SAP HANA Database interactive terminal.
Type: \h for help with commands
\q to quit
hdbsql SYSTEMDB=> exit
smaadm@hana-1:/usr/sap/SMA/HDB00
```

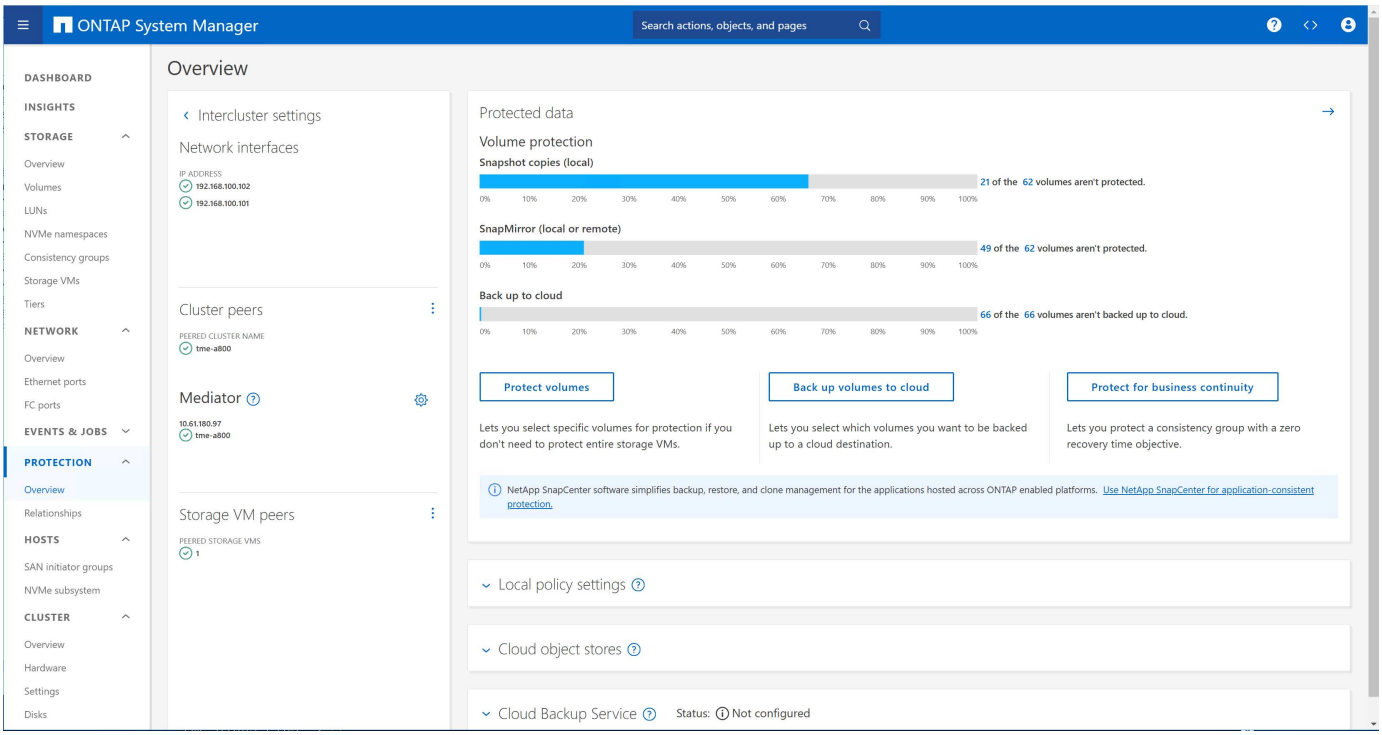
## **SnapMirror**のアクティブな同期設定

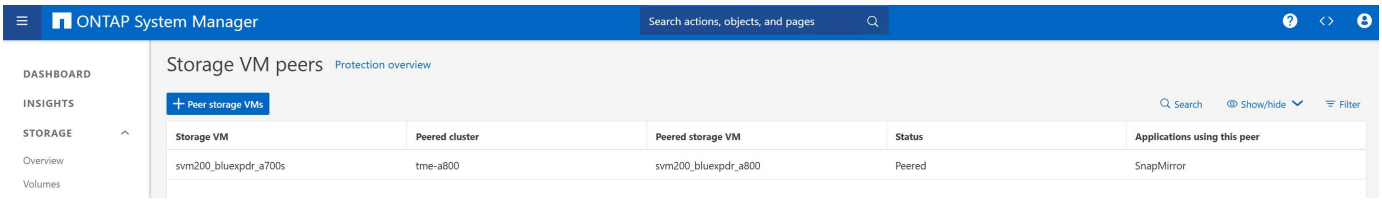
この記事では、このソリューションに必要な設定手順について説明します。

前提条件

ストレージクラスタと関連するSVMのピア関係が確立されている必要があります。

両方のストレージクラスタでONTAPメディエーターが使用可能で設定されている必要があります。



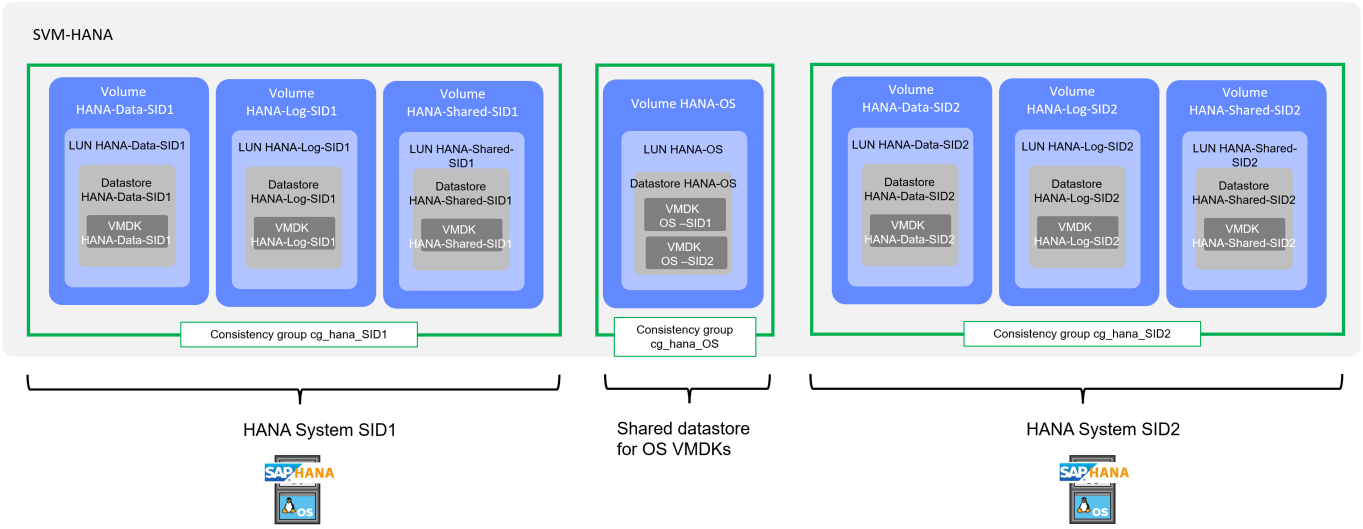

ストレージレイアウトと整合グループの設定

ONTAPのドキュメントでは "ONTAPでのSnapMirrorアクティブ同期の概要"、SnapMirrorアクティブ同期を使用する整合グループの概念を次のように説明しています。

整合グループはFlexVolボリュームの集まりで、ビジネス継続性のために保護する必要があるアプリケーションワークロードの整合性を保証します。

整合性グループの目的は、複数のボリュームのSnapshotイメージを同時に作成して、ある時点における一連のボリュームのcrash-consistentコピーを作成することです。整合グループを使用すると、データセットのすべてのボリュームが休止され、正確に同じポイントインタイムにスナップされます。これにより、データセットをサポートするボリューム間でデータ整合性のあるリストアポイントが提供されます。これにより、整合グループは従属書き込み順序の整合性を維持します。ビジネス継続性のためにアプリケーションを保護する場合は、ソースとデスティネーションの整合グループの間にデータ保護関係を確立できるように、このアプリケーションに対応するボリュームグループを整合グループに追加する必要があります。ソース整合性とデスティネーション整合性には、同じ数とタイプのボリュームが含まれている必要があります。

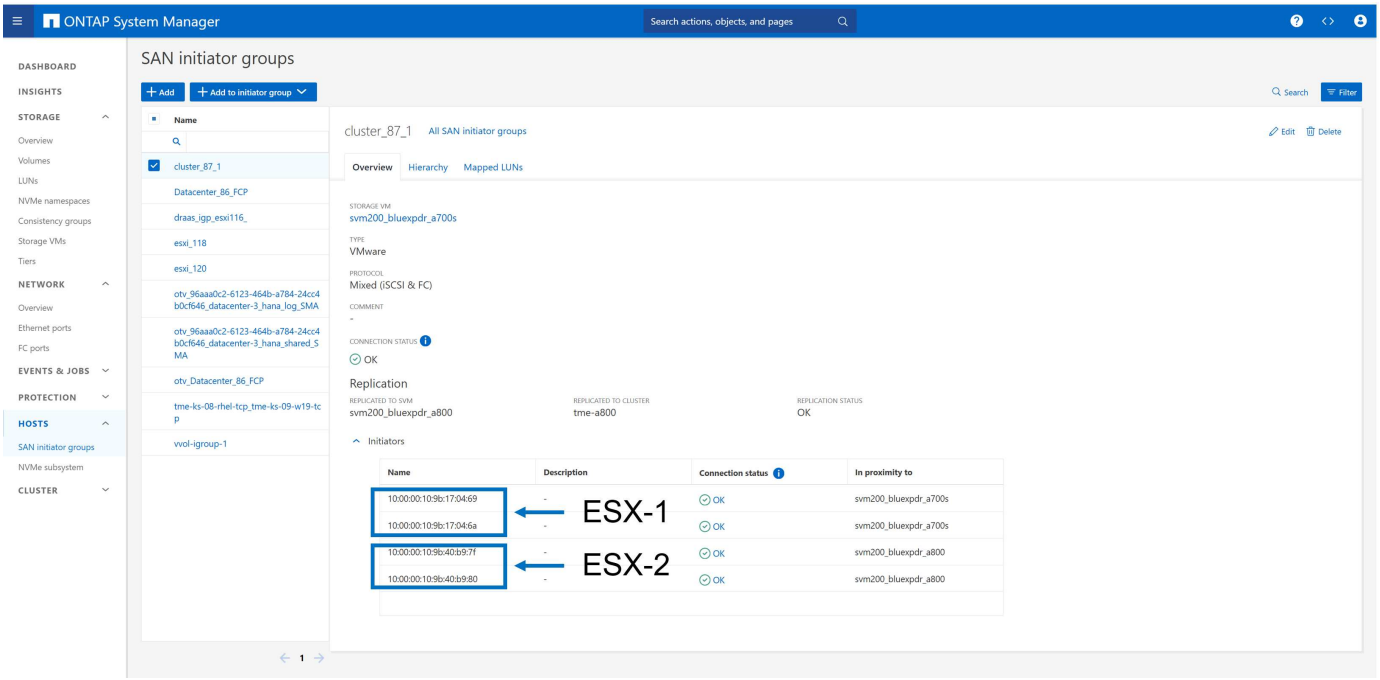
HANAシステムのレプリケーションでは、整合性グループに、個 々 のHANAシステムで使用されるすべてのボリューム（データ、ログ、共有）が含まれている必要があります。整合グループに含めるボリュームは、同じSVMに格納する必要があります。オペレーティングシステムイメージは、独自の整合グループを持つ別のボリュームに格納できます。次の図は、2つのHANAシステムを使用した構成例を示しています。

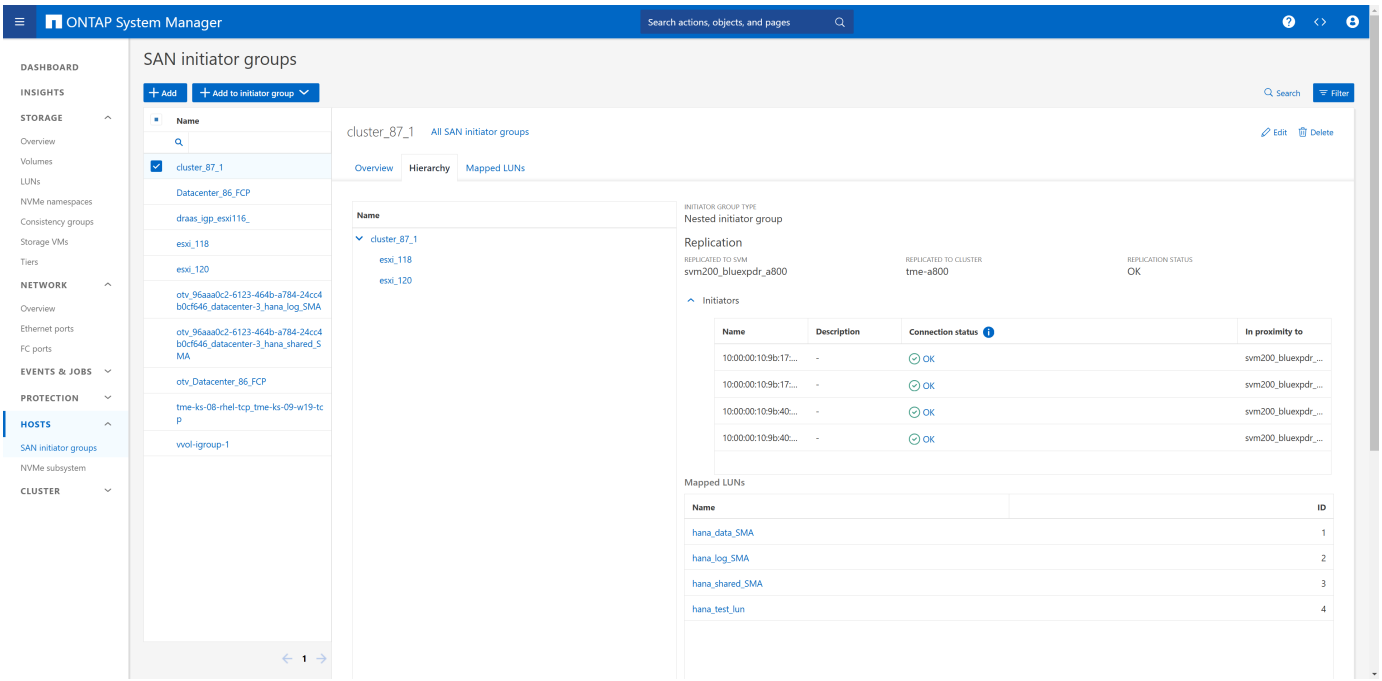



イニシエータグループの構成

このラボのセットアップでは、SnapMirrorのアクティブな同期レプリケーションに使用する両方のストレージSVMを含むイニシエータグループを作成しました。後述するSnapMirrorのアクティブな同期設定では、イニシエータグループをレプリケーションの一部として定義します。

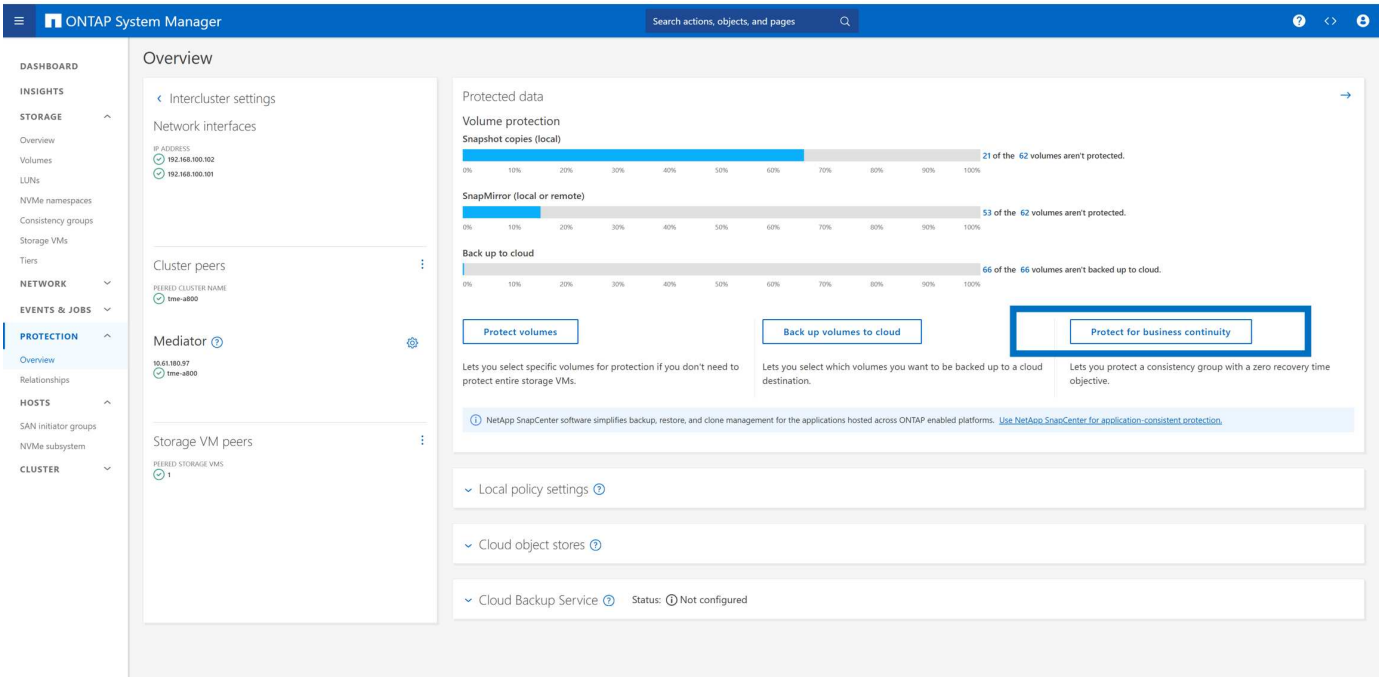
このプロキシミティ設定を使用して、どのESXホストがどのストレージクラスタに近いかを定義しました。この例では、A700はESX-1に近く、A800はESX-2に近くなっています。






統一されていないアクセス設定では、プライマリストレージクラスタ（A700）のイニシエータグループにESX-1ホストのイニシエータのみを含める必要があります。これは、ESX-2へのSAN接続がないためです。また、2つ目のストレージクラスタ（A800）に、ESX-2ホストのイニシエータのみを含む別のイニシエータグループを設定する必要があります。プロキシミティ構成とイニシエータグループのレプリケーションは必要ありません。

## ONTAP System Managerを使用した保護の設定

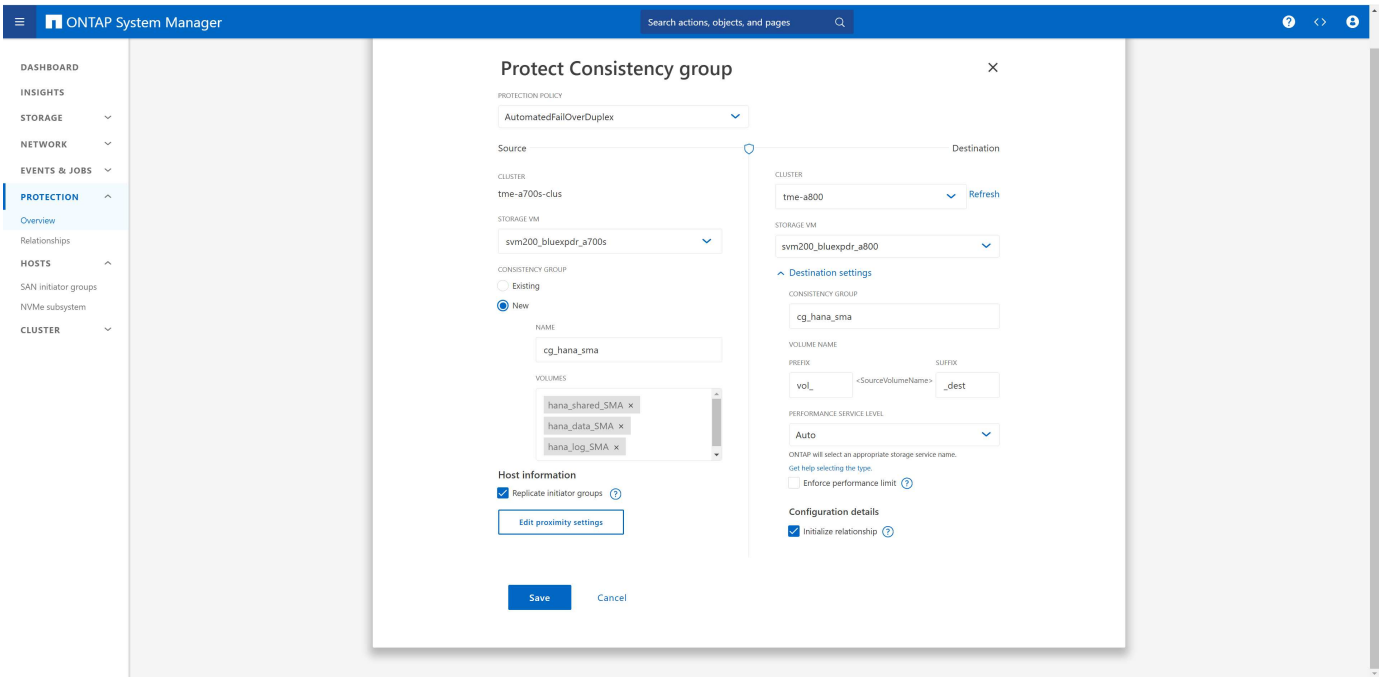



整合グループとイニシエータグループのレプリケーション

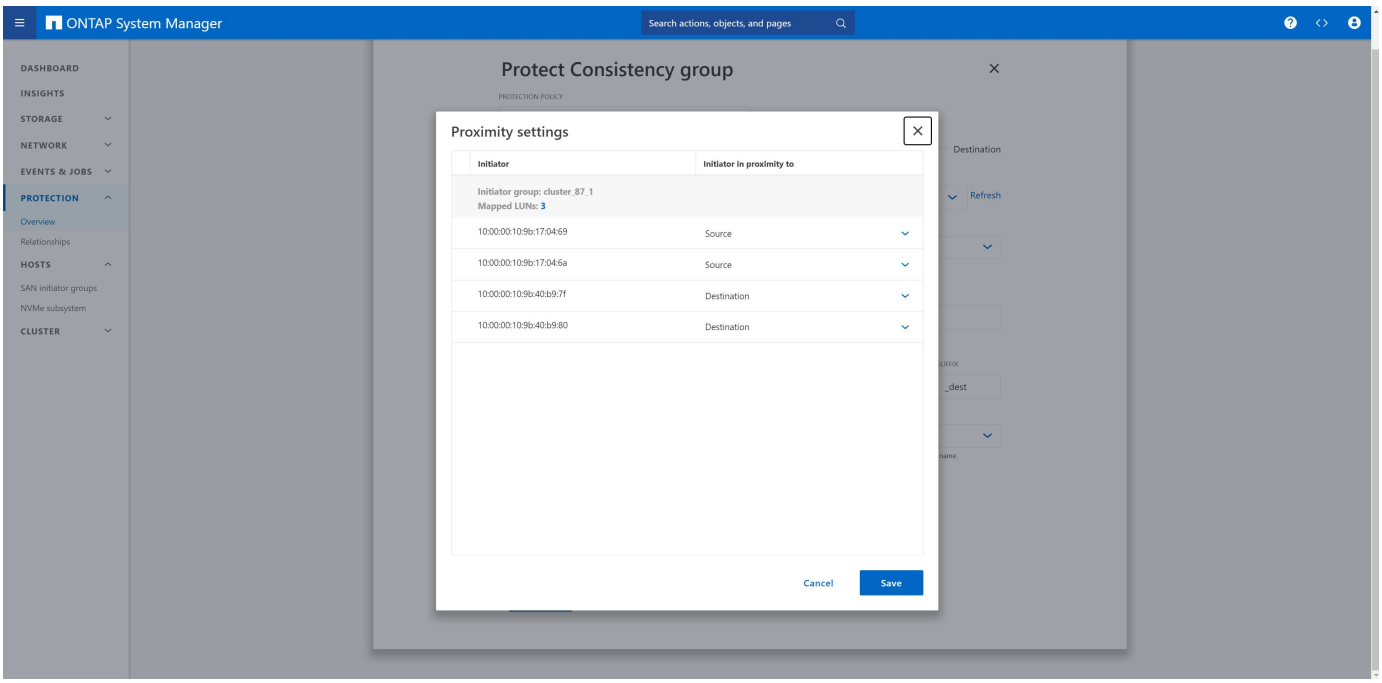
新しい整合グループを作成し、HANAシステムの3つのLUNをすべて整合グループに追加する必要があります。

[イニシエータグループのレプリケート]が有効になりました。その後、イミテータグループは、変更が行われた場所で独立して同期されたままになります。

異なるアクセス設定では、別のイニシエータグループを2つ目のストレージクラスタに設定する必要があるため、イニシエータグループをレプリケートしないでください。



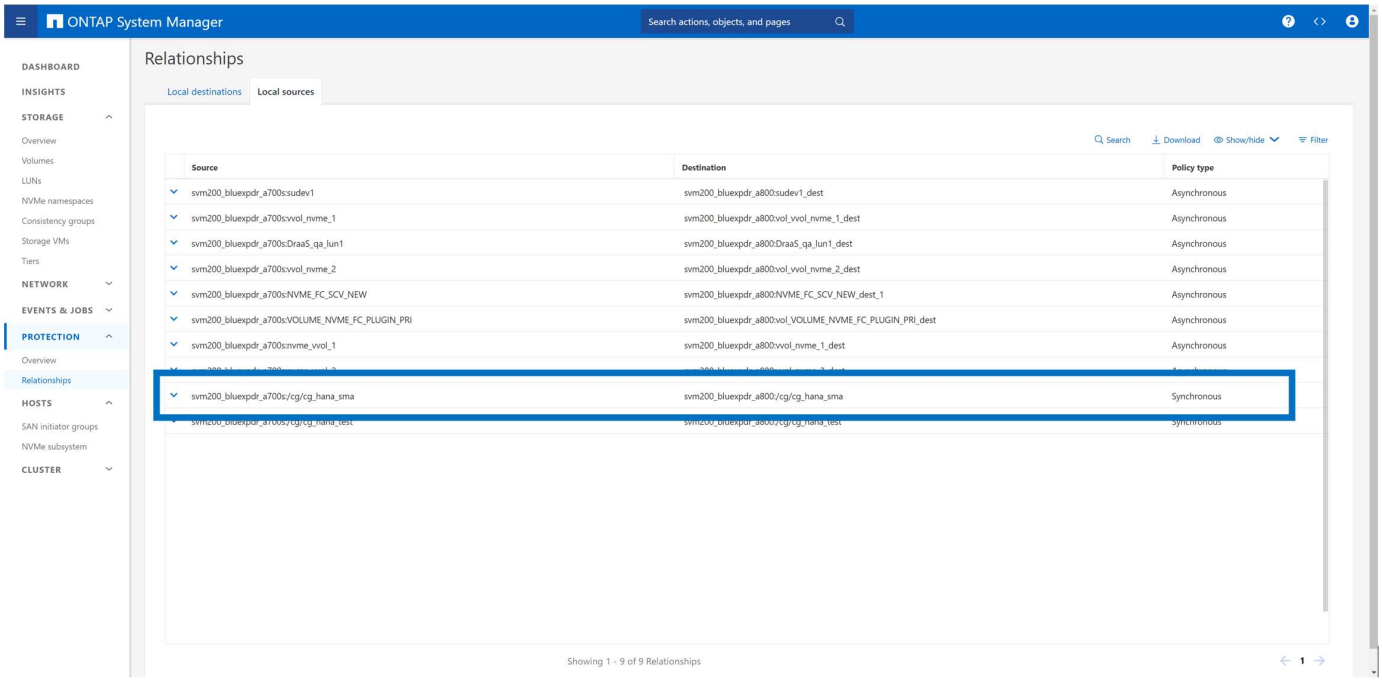

近接設定をクリックすると、イニシエータグループのセットアップで実行された設定を確認できます。



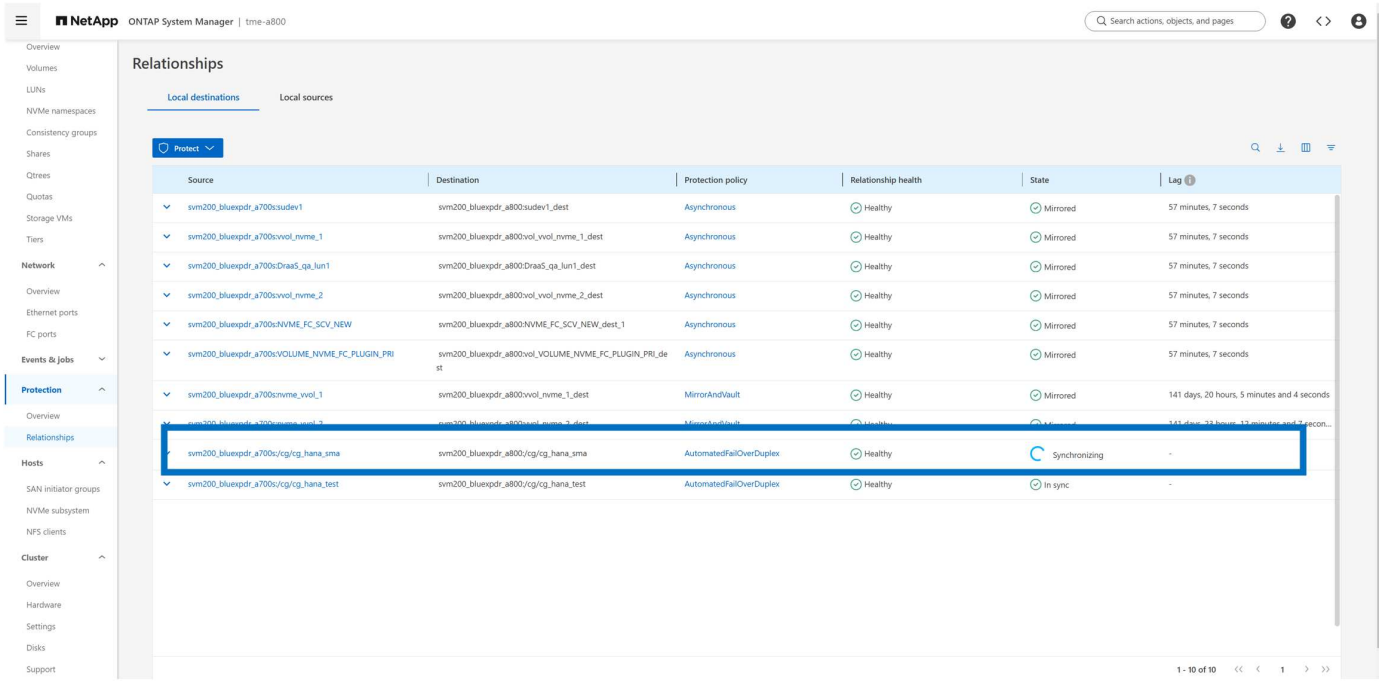

デスティネーションストレージクラスタを設定し、「関係の初期化」を有効にする必要があります。

同期

A700ストレージクラスタ（ソース）に新しい関係が表示されます。




A800ストレージクラスタ（デスティネーション）で、新しい関係とレプリケーションのステータスが表示されます。




## **Infrastructure**データストア

HANAシステム、SnapCenter、vSphereプラグインのOSイメージが格納されるデータストアは、HANAデータベースデータストアの場合と同じ方法でレプリケートされます。

プライマリサイト

SnapMirrorのアクティブな同期の動作は対称ですが、重要な例外が1つあります（プライマリサイトの設定）。

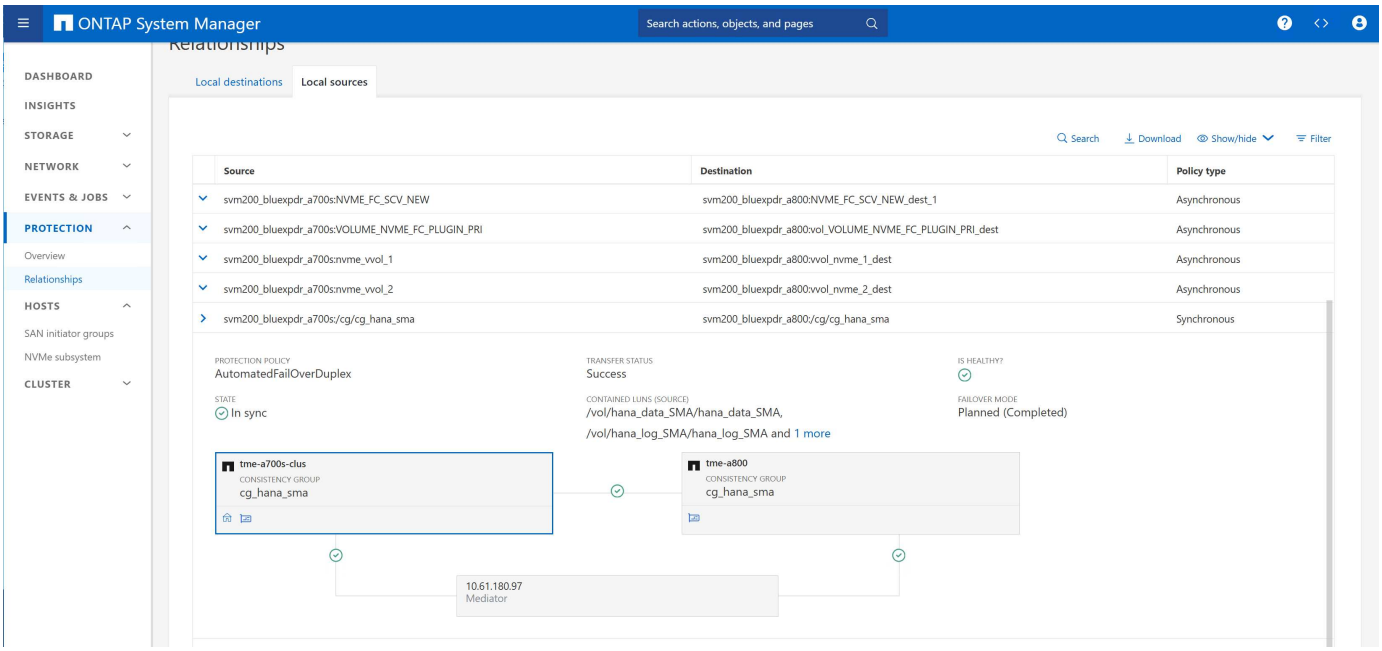
SnapMirrorアクティブ同期では、一方のサイトが「ソース」で、もう一方が「デスティネーション」と見なされます。これは一方向のレプリケーション関係を意味しますが、IO動作には適用されません。レプリケーションは双方向であり、対称であり、IO応答時間はミラーの両側で同じです。

レプリケーションリンクが失われた場合、ソースコピー上のLUNパスは引き続きデータを提供しますが、デスティネーションコピー上のLUNパスは、レプリケーションが再確立されてSnapMirrorが同期状態に戻るまで使用できなくなります。その後、パスでデータの提供が再開されます。

1つのクラスタをソースとして指定すると、レプリケーションリンクが失われた場合に、どのクラスタが読み取り/書き込みストレージシステムとして残っているかが制御されます。

プライマリサイトはSnapCenterによって検出され、バックアップ、リストア、クローニングの各処理に使用されます。

ソースとデスティネーションはSVMまたはストレージクラスタに関連付けられていませんが、レプリケーション関係ごとに異なる場合があることに注意してください。




## SnapCenter 構成

本ドキュメントの冒頭で説明したように、VMwareとVMFSおよびSnapMirrorのアクティブ同期を使用するHANA環境のベストプラクティスを紹介することを目的としています。ここでは、この特定のソリューションに関連する詳細と重要な手順についてのみ説明します。SnapCenterの一般的な概念については説明しません。SnapCenterに関するこれらの概念およびその他の追加情報については、次のサイトを参照してください。

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

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

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

前提条件

一般に、保護されたリソースをSnapCenterに追加する前に、SnapMirrorアクティブ同期を設定する必要があります。SnapMirror Active Syncのセットアップ前に作成されたバックアップは、元のプライマリストレージにのみ存在し、その後はレプリケートされません。

#### SnapCenter HANAリソースを自動検出する必要があります

VMware VMFSで構成されているリソース、またはSnapMirror Active Syncで保護されているリソースは、SnapCenterによって自動検出され、これらの構成に必要な特定の処理を実行できるようにする必要があります。

HANAの非データボリュームは、SnapCenterでは常に手動で設定されたリソースであるため、SnapCenterでは即座にサポートされません。データボリューム以外のボリュームのオプションと回避策については、このドキュメントの後半で説明します。

SAP HANAマルチホストシステムは、中央のHANAプラグインを使用して設定する必要があるため、デフォルトでリソースを手動で設定します。VMware VMFSまたはSnapMirrorのアクティブ同期を使用している場合、このようなHANAシステムはSnapCenterでサポートされません。

#### SnapCenter for VMware vSphere プラグイン

SnapCenter for VMware vSphereプラグインをVMware環境に導入する必要があります。

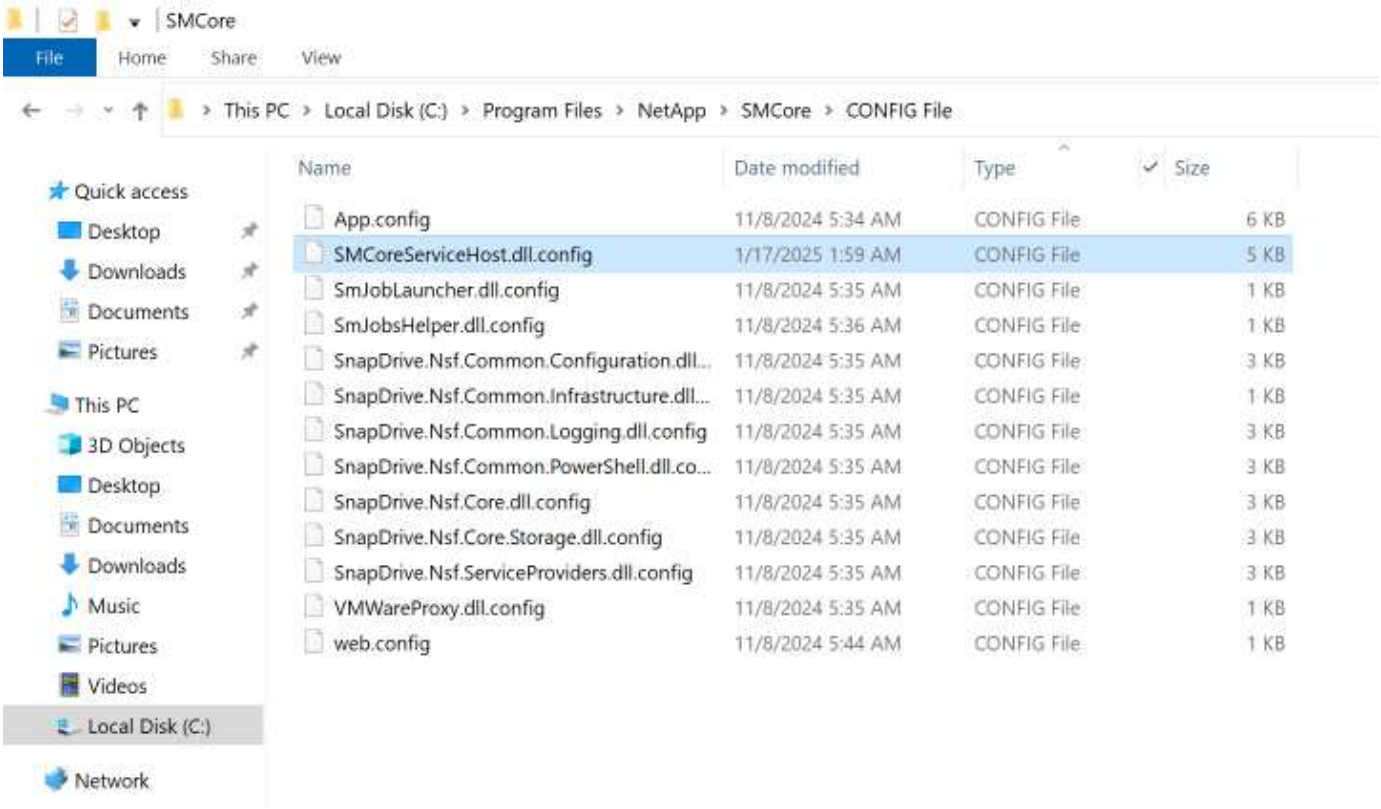
#### ボリュームをホストしているSVMの管理IPアドレス

クラスタをSnapCenterに追加する場合でも、ソースボリュームとデスティネーションボリュームをホストするSVMに管理IPアドレスを設定する必要があります。

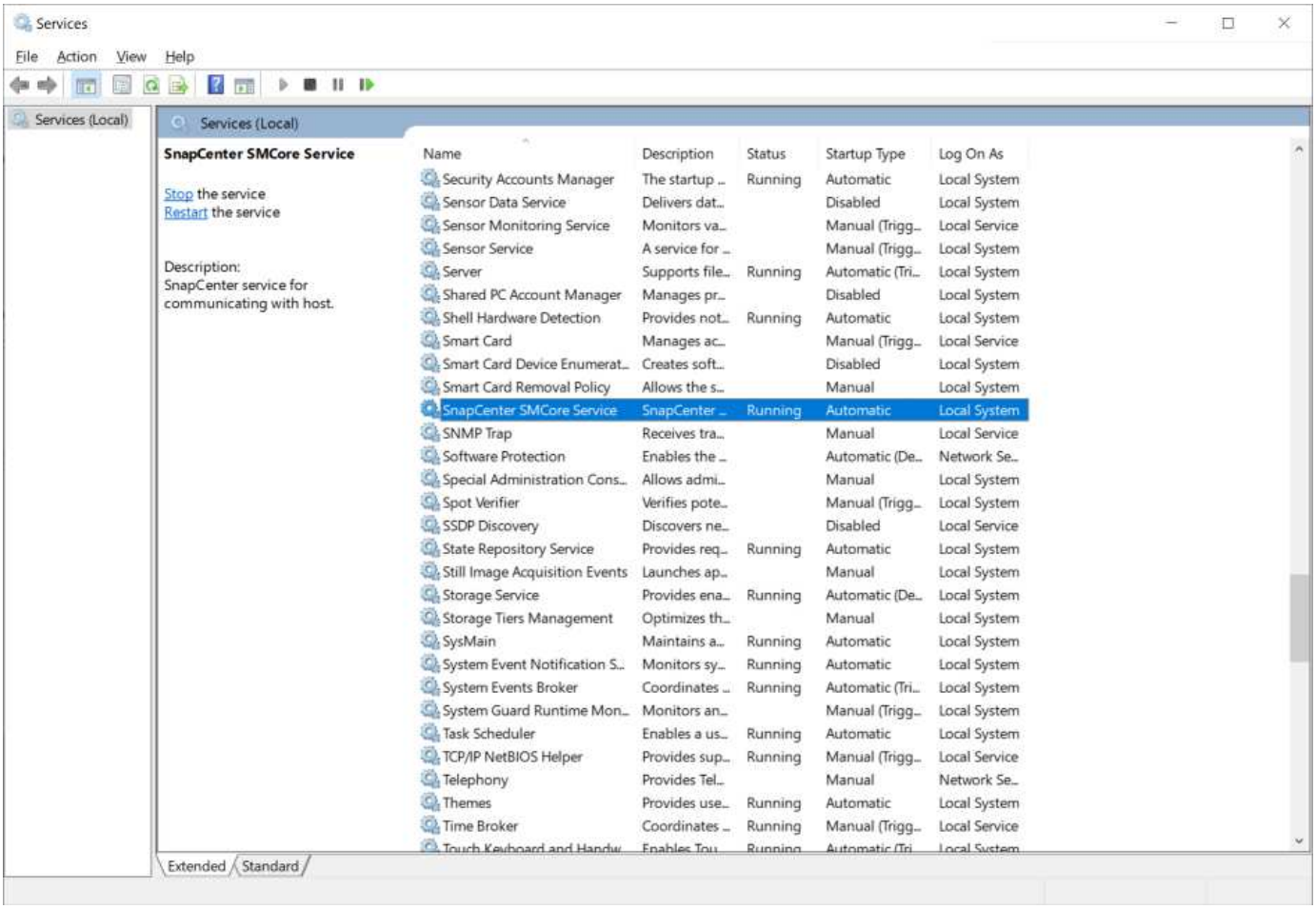
#### ストレージ通信用のREST API

SnapMirrorのアクティブな同期の管理と監視には、REST APIアクセスが必要です。そのため、ストレージ通信にREST APIを使用するようにSnapCenterを設定する必要があります。構成ファイル+C：\\+Program NetApp +\\+SMCore\\+SMCoreServiceHost.dll.configのパラメータ「IsRestEnabledForStorageConnection」をtrueに設定する必要があります。

```
<add key="IsRestEnabledForStorageConnection" value="true">
```

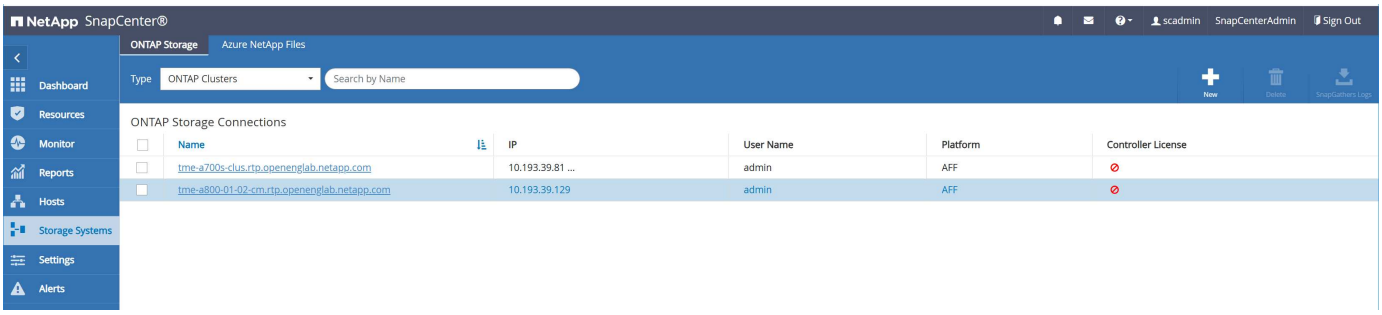


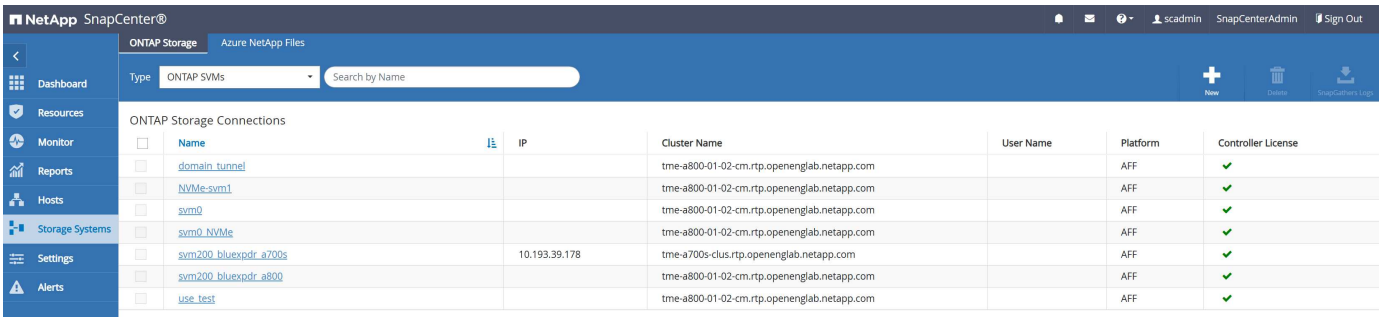

パラメータを変更したら、SnapCenter SMCoreサービスを再起動する必要があります。



ストレージシステムを追加する

SnapCenterでREST APIを有効にしたあとにストレージシステムを追加できます。個 々 のSVMではなく、両方のストレージクラスタを追加する必要があります。



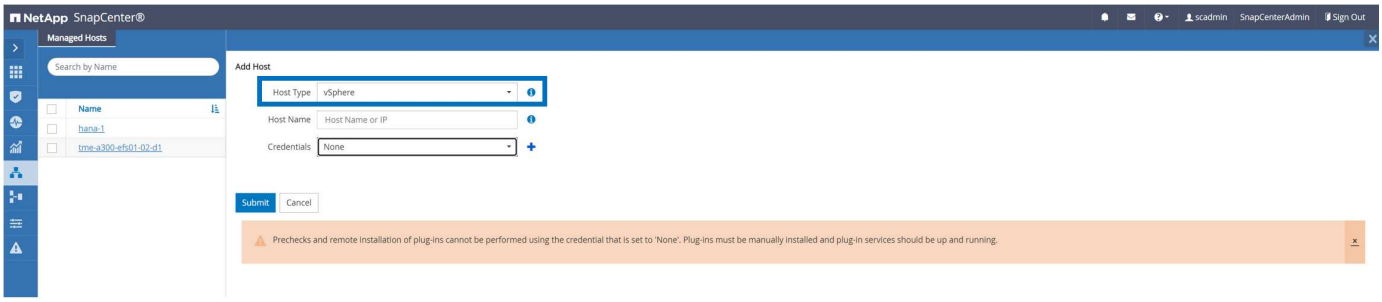



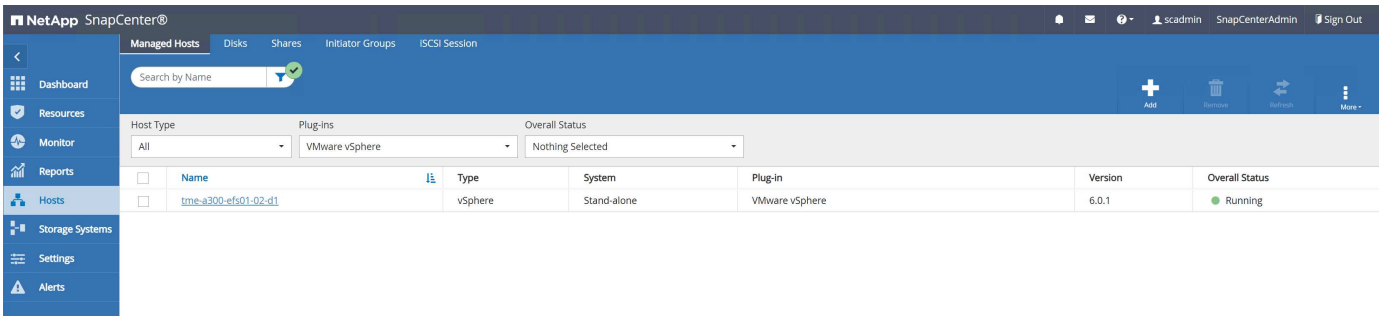

ホストの追加–**SnapCenter for VMware vSphere**プラグイン

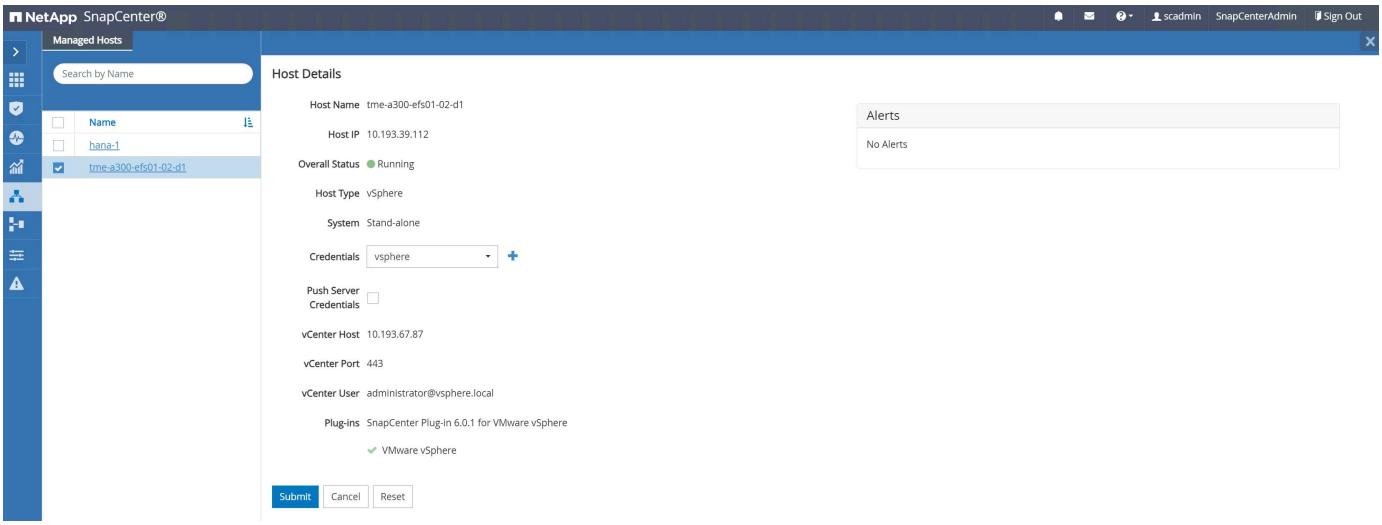
SnapCenterのリソースが仮想化されたVMware環境で実行されている場合、SnapCenterはSnapCenter Plug-in for VMware vSphereを利用して、SnapCenterのバックアップ、リストア、クローニングのワークフローを拡張し、VMwareレイヤで必要な手順を実行します。

ホストをSnapCenterに追加する前に、VMware vSphere用SnapCenterプラグインをVMware環境に導入する必要があります。

クレデンシャルはホスト追加ワークフローで設定する必要があります。ホストタイプとしてvSphereを選択できます。






SnapCenter for vSphereプラグイン自体で追加の設定は必要ありません。

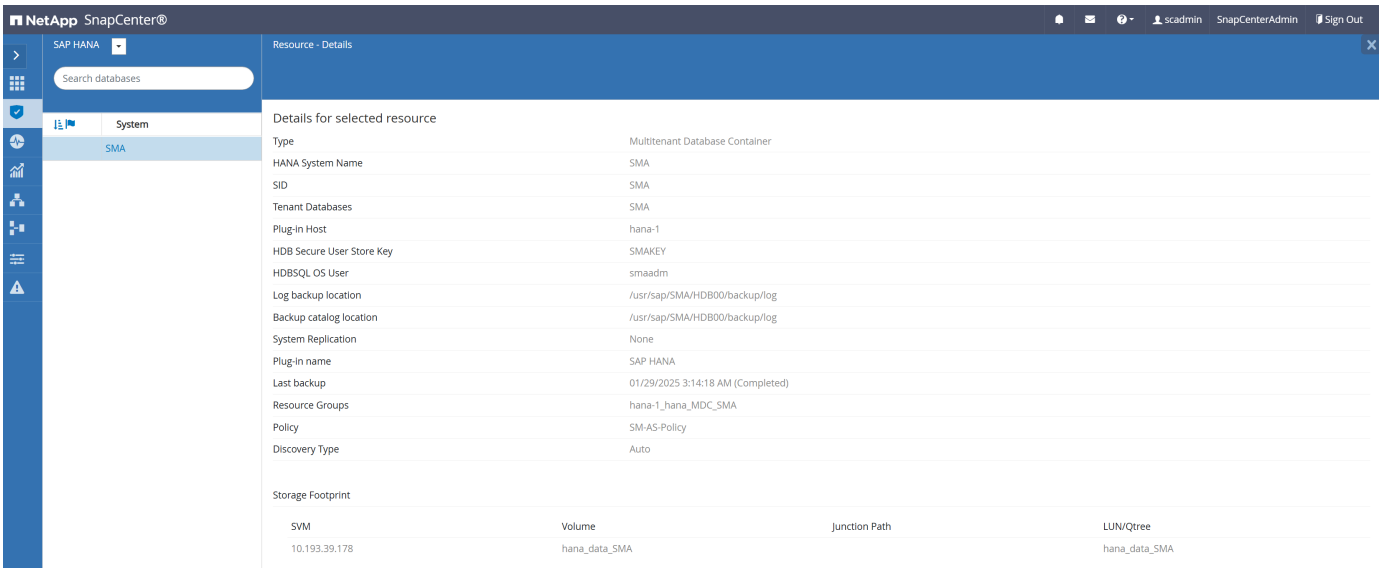
ホストを追加–**HANA**システム

具体的な要件はありません。プラグインの導入と自動検出は通常どおり実行されます。

自動検出プロセスにより、SnapCenterは、HANAリソースがVMFS/VMDKで仮想化された状態で実行されていることを検出します。また、SnapCenterはSnapMirrorのアクティブな同期設定を検出し、現在のプライマリサイトを特定します。

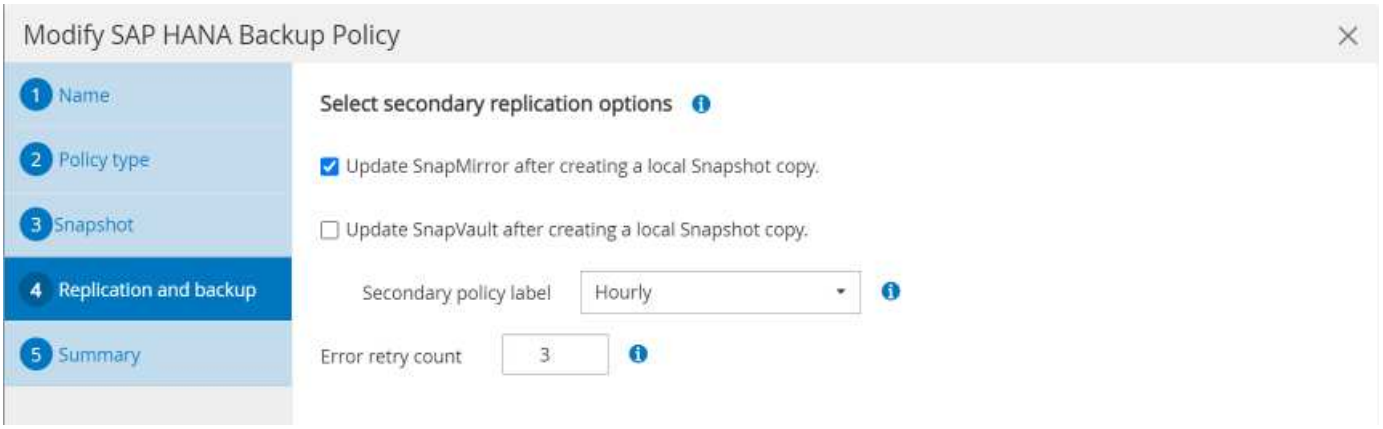
リソースの自動検出後、リソースビューのストレージフットプリントセクションに現在のプライマリサイトが表示されます。どのストレージシステムがマスターであるかは、SnapCenterで使用されるONTAPコマンドの出力に基づいて検出されます。

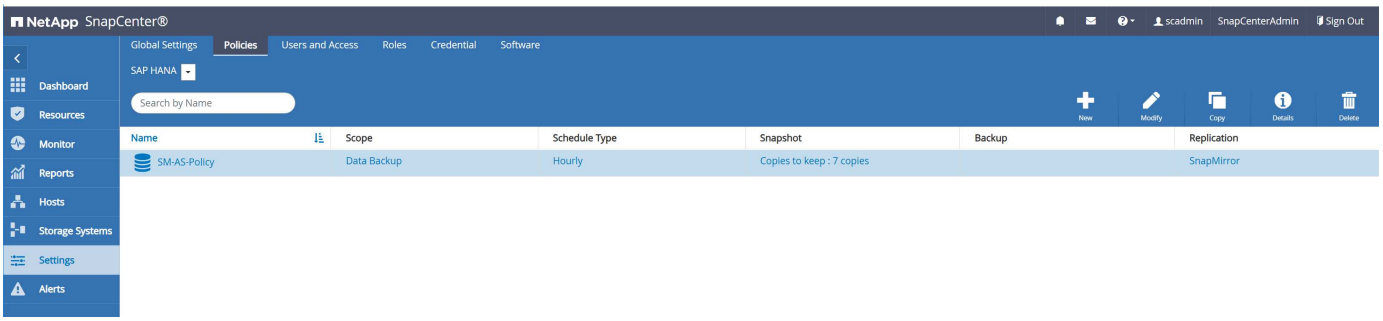
```
volume show -vserver <vs> -volume <vol> -fields smbc-consensus,is-smbc-
master
```




ポリシー設定

SnapMirrorアクティブ同期で保護されているリソースに使用されるポリシーは、SnapMirrorレプリケーションを使用して設定する必要があります。ただし、SnapCenterではSnapMirror更新処理がトリガーされません。



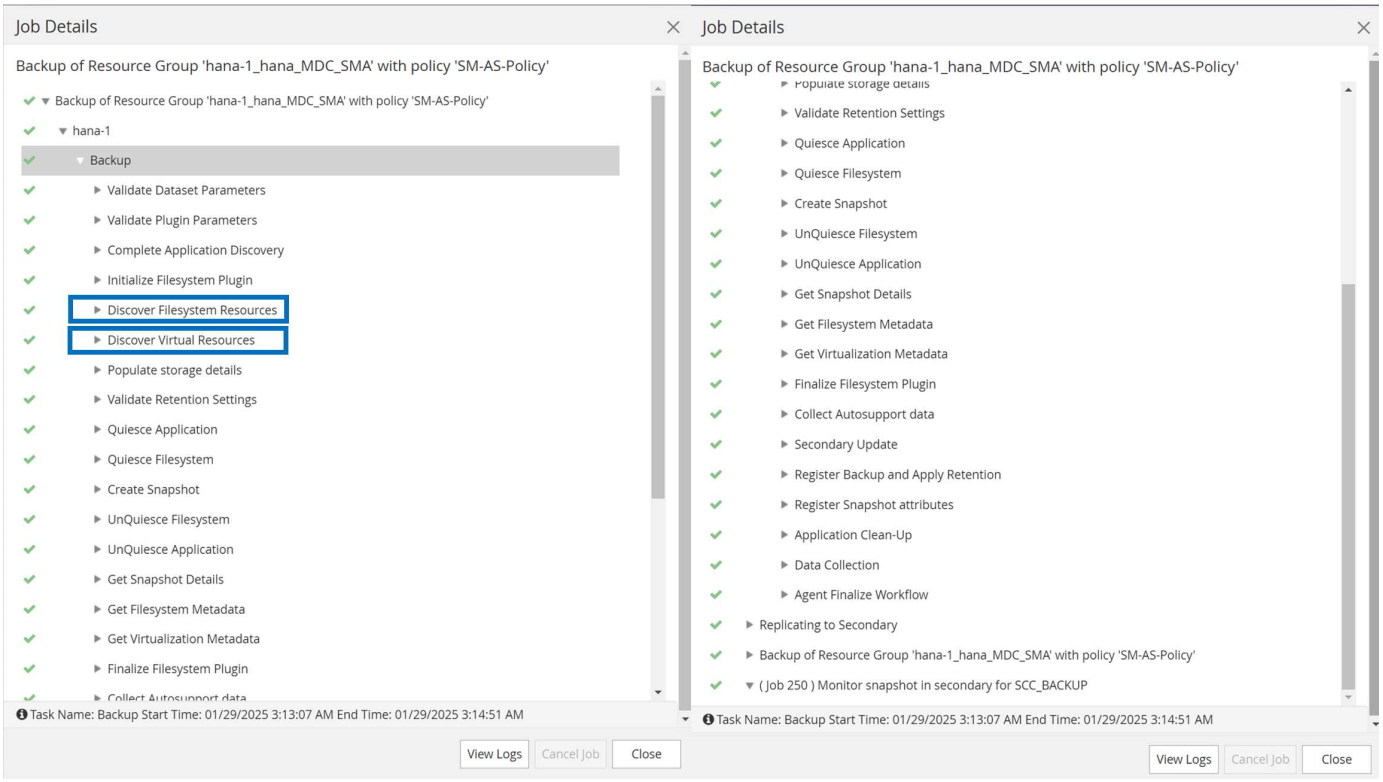

**HANA**リソース保護構成

具体的な要件はありません。リソース保護の設定は通常どおり行われます。

## SnapCenter バックアップ処理

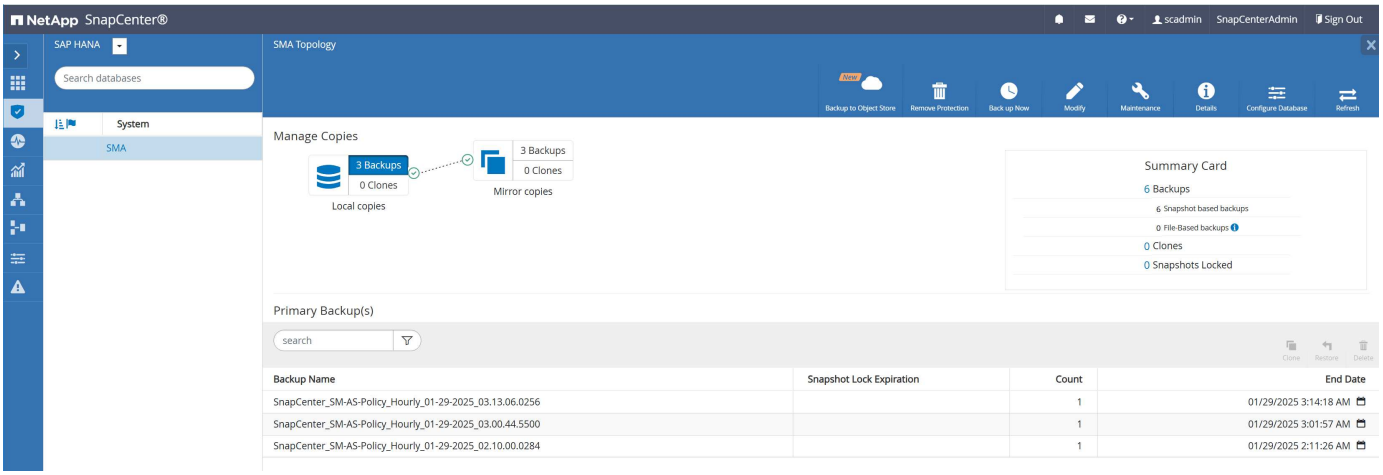
バックアップ処理のたびに、SnapCenterはVMware側での検出とプライマリサイトの検

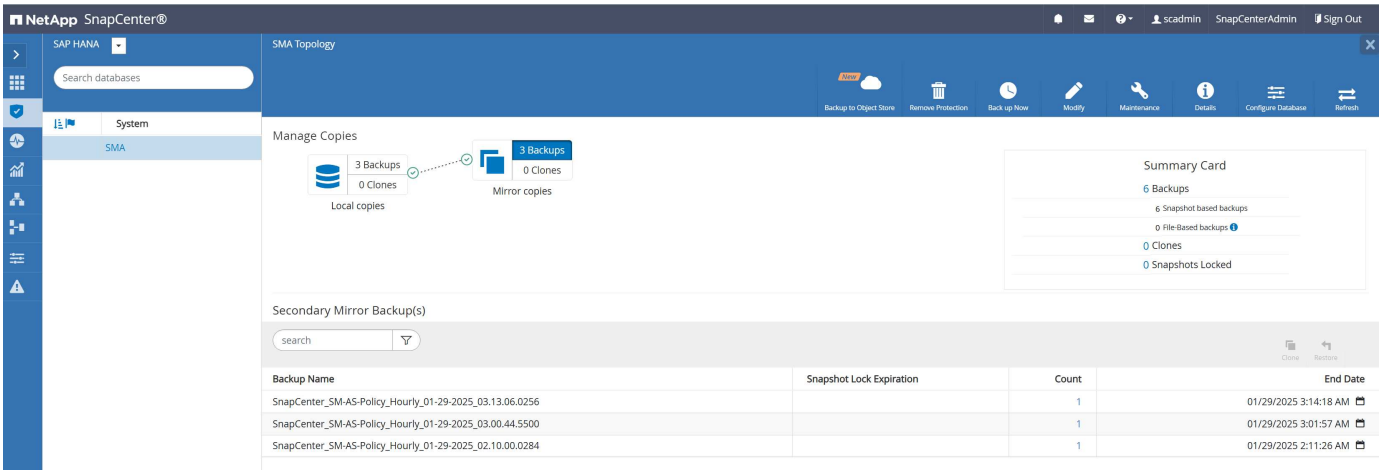
出を実行します。ストレージフェイルオーバーが発生した場合、SnapCenterはリソースのバックアップが実行されるとすぐに新しいプライマリサイトを検出します。




## [Topology]ビュー

トポロジビュー内のSnapCenterには、ソースとデスティネーションの両方のストレージクラスタのバックアップが表示されます。





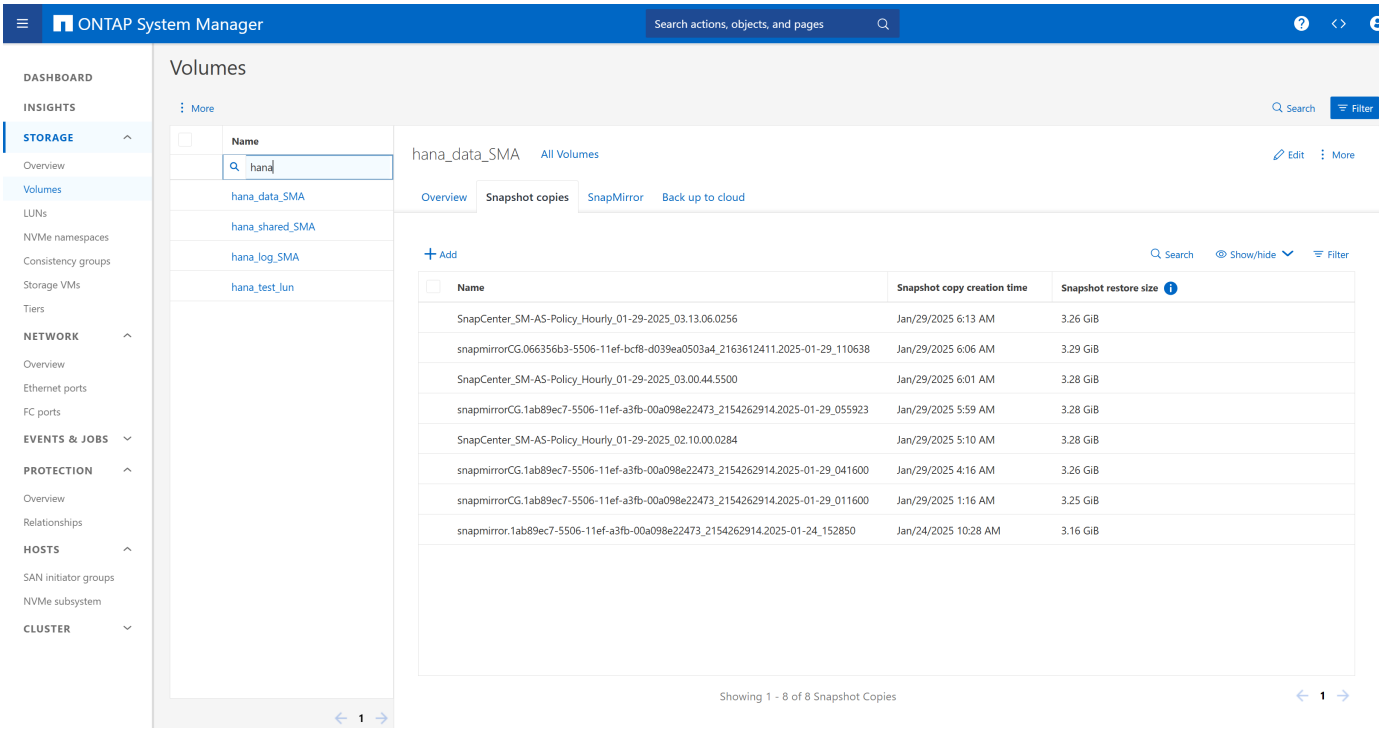

セカンダリストレージの数をクリックすると、現在の関係とレプリケーションの方向が表示されます。ソースは常に現在のプライマリサイトです。ストレージフェイルオーバーが発生すると、プライマリサイトが変化し、それに応じて表示が変更されます。どのストレージシステムが現在プライマリサイトであるかに応じて、すべてのバックアップの関係は常に同じです。



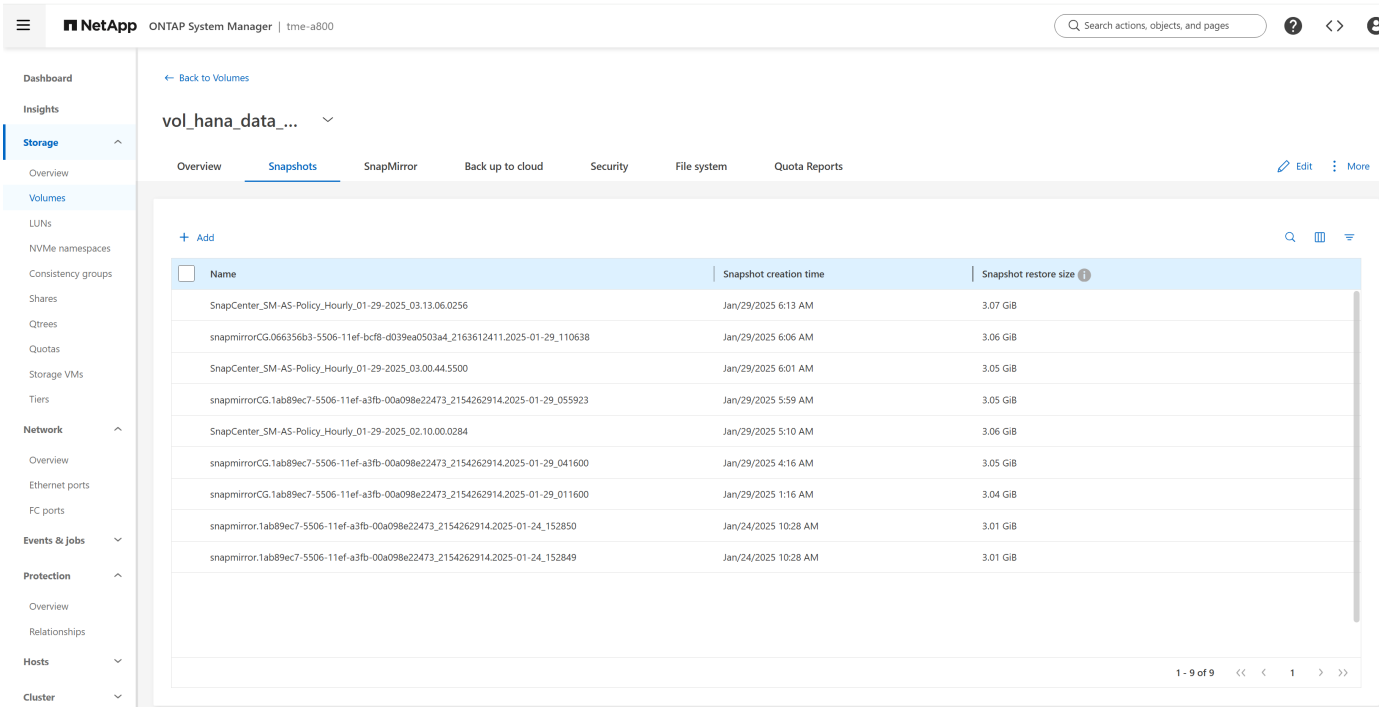

ストレージシステムに**Snapshot**を作成

SnapCenterで作成されたSnapshotバックアップは、両方のストレージシステムの両方のHANAデータボリュームで使用できます。ONTAPでは、整合グループレベルで追加のSnapshotが作成され、他のすべてのHANAボリュームでも使用できます。

次の図は、A700クラスタのHANAデータボリュームのSnapshotを示しています。




次の図は、A800クラスタのHANAデータボリュームのSnapshotを示しています。




## SnapCenterノリストアトリカハリ

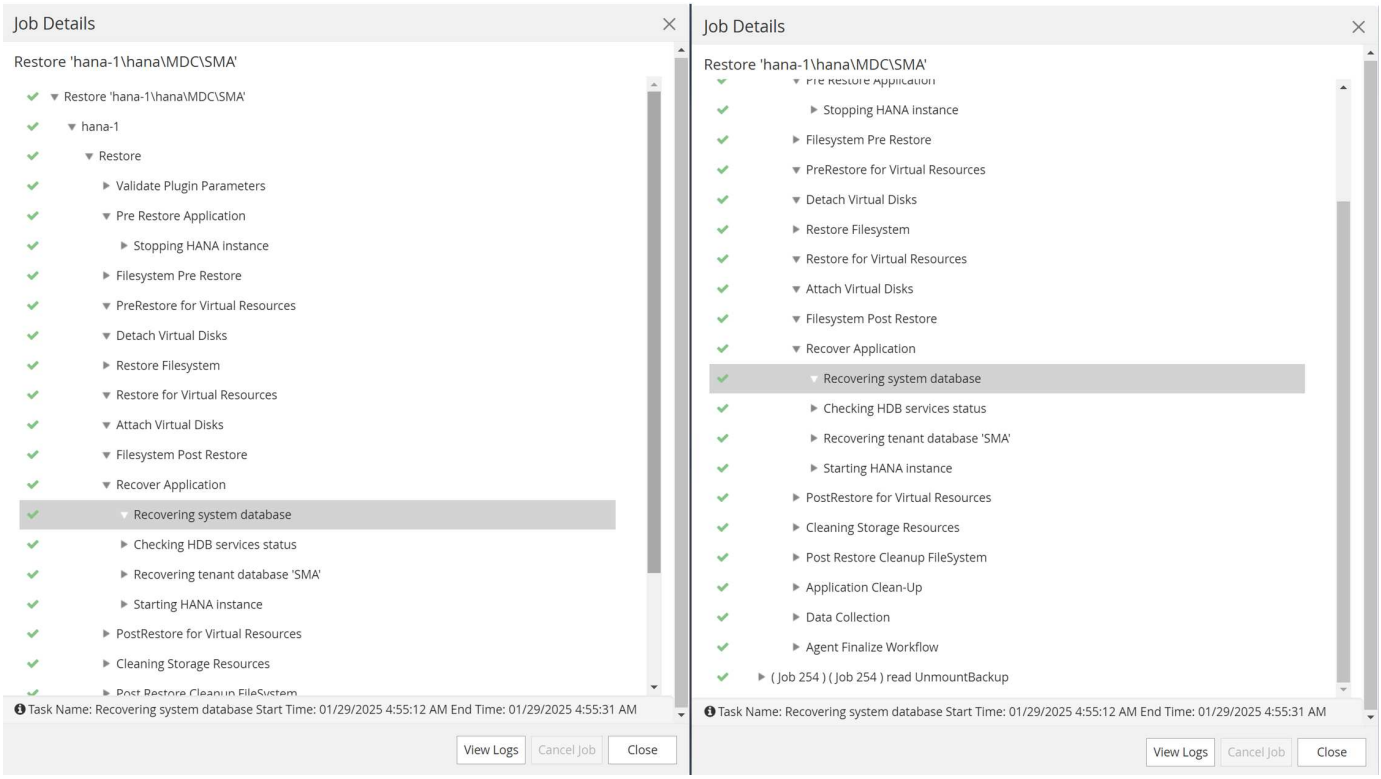
仮想リソースがVMFS/VMDKに格納されている場合、SnapCenterのリストア処理は、常にクローン、マウント、コピーの各処理によって実行されます。

1. SnapCenterは、選択したSnapshotを基にボリュームクローンを作成します。
2. SnapCenterは、クローンボリューム内のLUNを新しいデータストアとしてESXホストにマウントします。

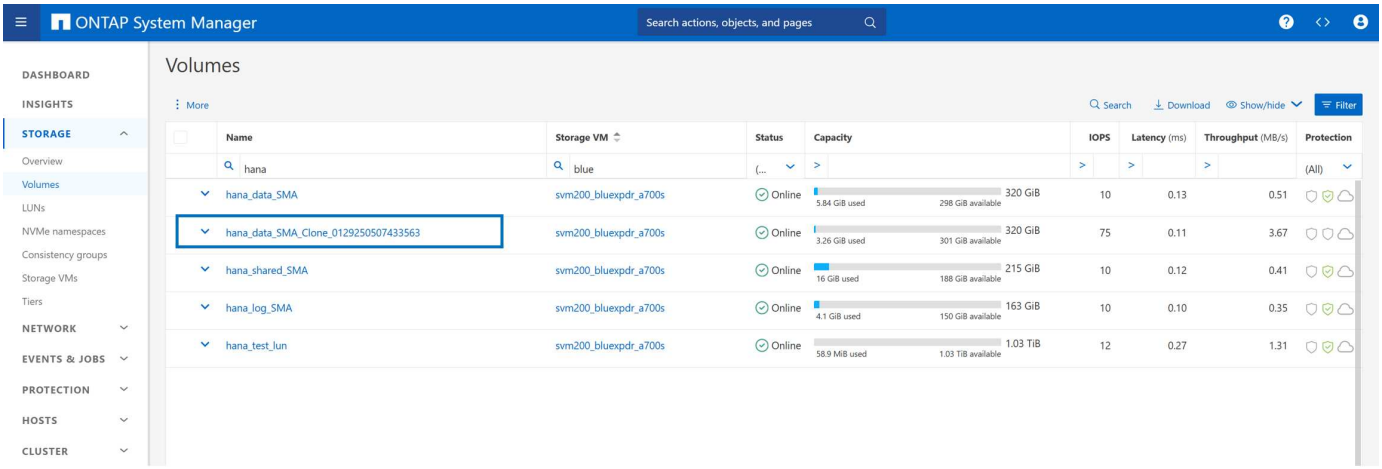
3. SnapCenterは、データストア内のVMDKを新しいディスクとしてHANA VMに追加
4. SnapCenterが新しいディスクをLinux OSにマウント
5. SnapCenterは、新しいディスクから元の場所にデータをコピーします。
6. コピー操作が終了すると、上記のリソースはすべて再度削除されます。
7. HANAのリカバリは通常どおり実行

したがって、リストア処理の全体的な実行時間は、データベースのサイズと、ストレージクラスタとESXホスト間のFC接続のスループットに左右されます。

また、リソースにSnapMirrorアクティブ同期が設定されている場合、SnapCenterリストア処理は現在のプライマリサイトでのみ選択できます。




リストアとリカバリ処理の実行中に、現在のプライマリサイトに作成された新しいクローンボリュームが表示されます。



HANA Linuxホストでは、ホストにマウントされた新しいディスクが表示されます。リストア処理が完了すると、SnapCenterによってデータストアとボリュームが再び削除されます。

```
hana-1:~ # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 4.0K 49G 1% /dev/shm
tmpfs 13G 58M 13G 1% /run
tmpfs 4.0M 0 4.0M 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 36G 24G 60% /
/dev/mapper/system-root 60G 36G 24G 60% /.snapshots
/dev/mapper/system-root 60G 36G 24G 60% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 36G 24G 60% /home
/dev/mapper/system-root 60G 36G 24G 60% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 36G 24G 60% /opt
/dev/mapper/system-root 60G 36G 24G 60% /srv
/dev/mapper/system-root 60G 36G 24G 60% /usr/local
/dev/mapper/system-root 60G 36G 24G 60% /tmp
/dev/mapper/system-root 60G 36G 24G 60% /root
/dev/mapper/system-root 60G 36G 24G 60% /var
/dev/sdb 200G 8.0G 192G 4% /hana/data/SMA/mnt00001
/dev/sdc 120G 7.0G 113G 6% /hana/log/SMA/mnt00001
/dev/sda1 253M 5.1M 247M 3% /boot/efi
/dev/sdd 150G 28G 123G 19% /hana/shared
tmpfs 6.3G 48K 6.3G 1% /run/user/467
tmpfs 6.3G 28K 6.3G 1% /run/user/0
/dev/sde 200G 8.0G 192G 4%
/var/opt/snapcenter/scu/clones/hana_data_SMAmnt00001_255_scu_clone_1
hana-1:~ #
```

## SAPシステムの更新処理

クローニング処理は、プライマリサイトまたはセカンダリストレージで実行できます。

クローンボリュームはHANA整合性グループには含まれず、SnapMirrorのアクティブな同期ではレプリケートされません。

システム更新ワークフローの詳細については、次のサイトを参照してください。"TR-4667：『Automating SAP HANA System Copy and Clone Operations with SnapCenter』"

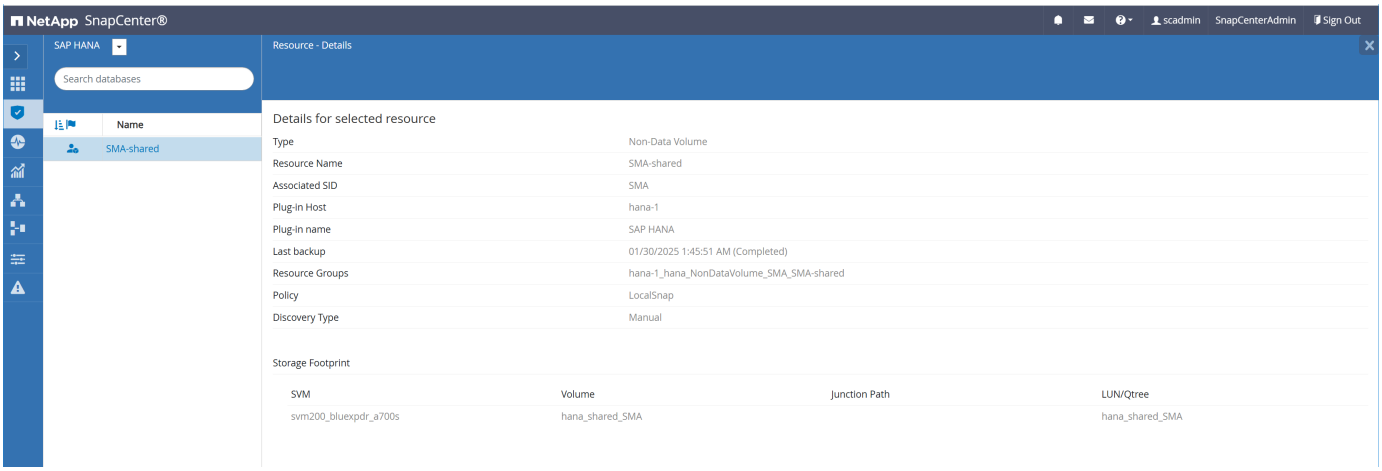
## SnapCenterデータボリューム以外のボリューム

リソースがSnapCenterで手動で設定され、自動検出されない場合、SnapCenterはVMwareとSnapMirrorのアクティブな同期を認識しません。そのため、SnapCenterではネイティブにサポートされていません。

HANA共有のようなデータボリューム以外のボリュームでは、追加の手動手順を検討する場合でも、SnapCenterを使用してバックアップとリストアの処理を実行できます。

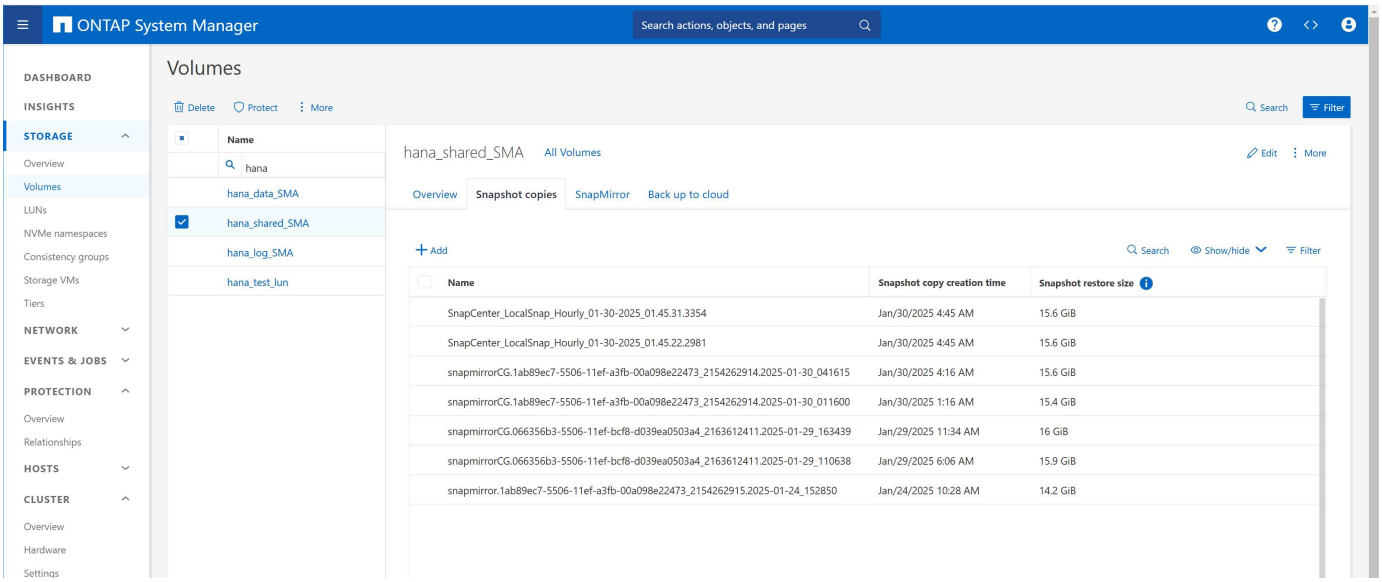
### SnapCenterで設定されたストレージシステムの障害

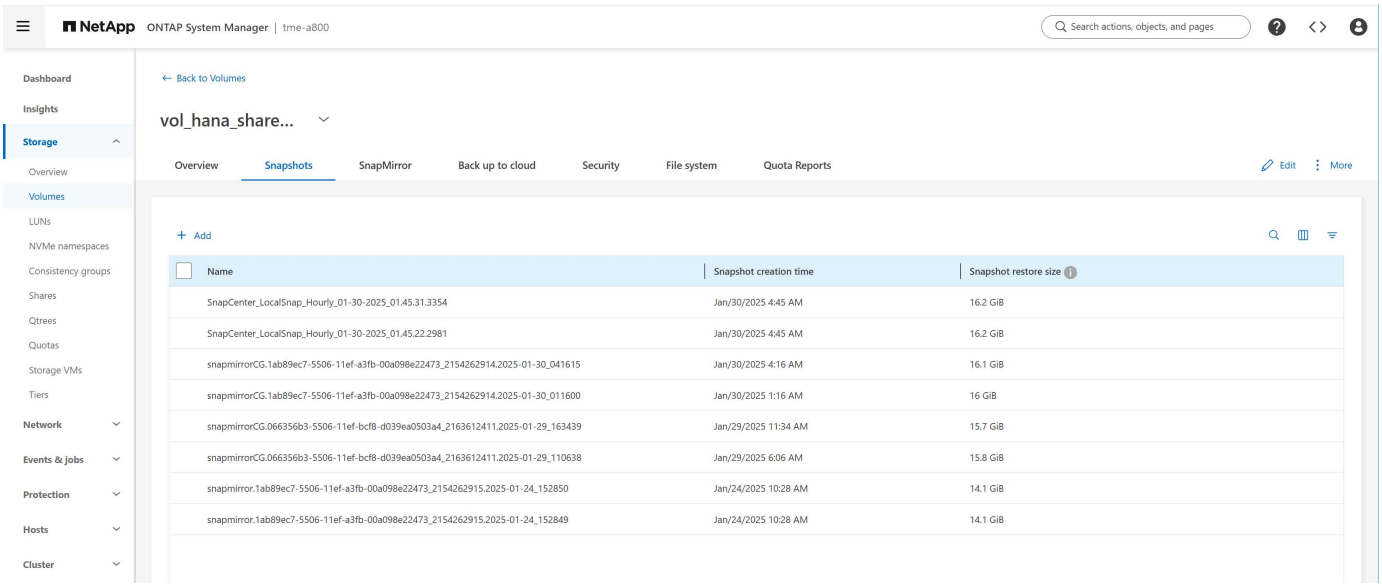
SnapCenterで設定されたストレージ・システムに障害が発生しても、SnapCenterは自動的にもう一方のストレージ・システムに切り替わりません。ボリュームのミラーコピーをバックアップおよびリストア処理に使用するには、データボリューム以外のリソースを手動で調整する必要があります。




### バックアップ処理

SnapCenterはHANA共有ボリュームのSnapMirrorアクティブ同期設定を認識しませんが、Snapshotは両方のサイトにレプリケートされます。






リストア処理を実行します

リストアの場合、SnapCenterでは、VMware固有の手順を実行せずにボリュームのリストアが実行されます。通常は、LinuxホストでHANA共有ボリュームをアンマウントし、データストアを切断してからボリュームのリストアを実行し、データストアを再度接続してから、Linuxホストでファイルシステムをマウントする必要があります。手動操作では、HANA VMを停止し、SnapCenterでHANA共有ボリュームをリストアしてから、VMを再起動できます。

## フェイルオーバーのシナリオ

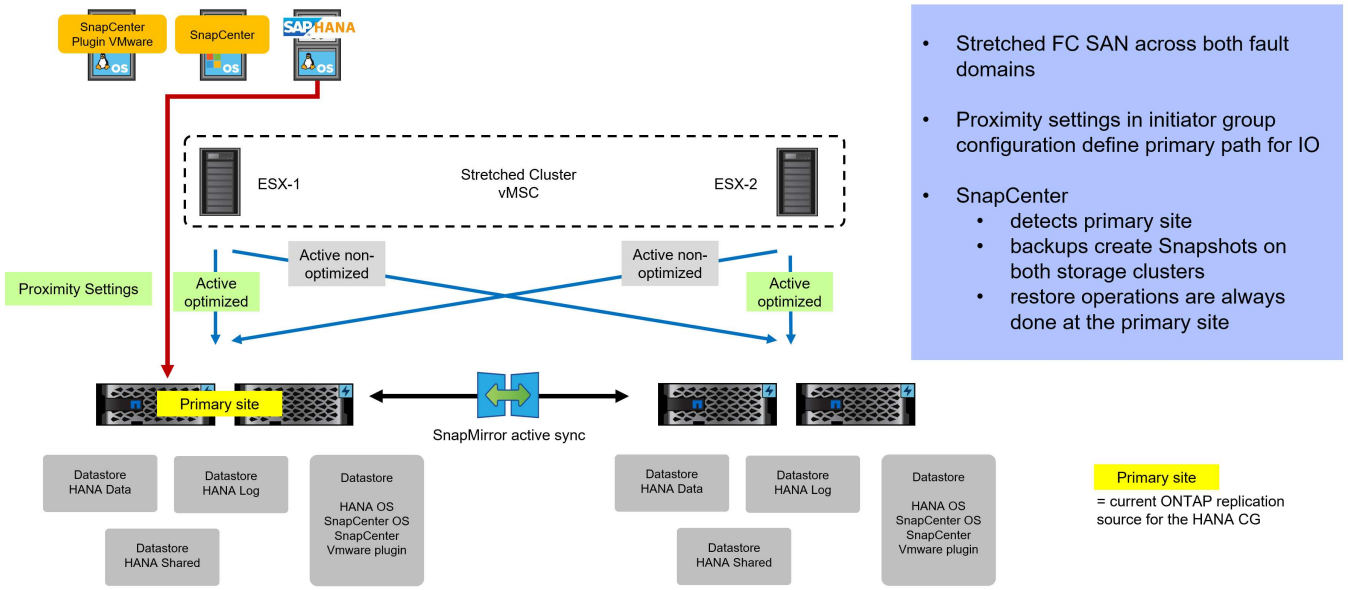
この記事では、このソリューションのフェイルオーバーシナリオについて説明します。

### 統一されたアクセス設定

統一されたアクセス構成では、ファイバチャネルSANが両方のサイトに拡張されます。両方のサイトのESXホストは、データセットの両方のコピーにアクセスできます。通常運用時、HANAシステムを実行するESXホストは、イニシエータグループ構成の近接設定に基づいてデータのローカルコピーにアクセスします。各ESXホストには、ローカルコピーへのアクティブな最適パスと、ミラーコピーへのアクティブな非最適パスがあります。

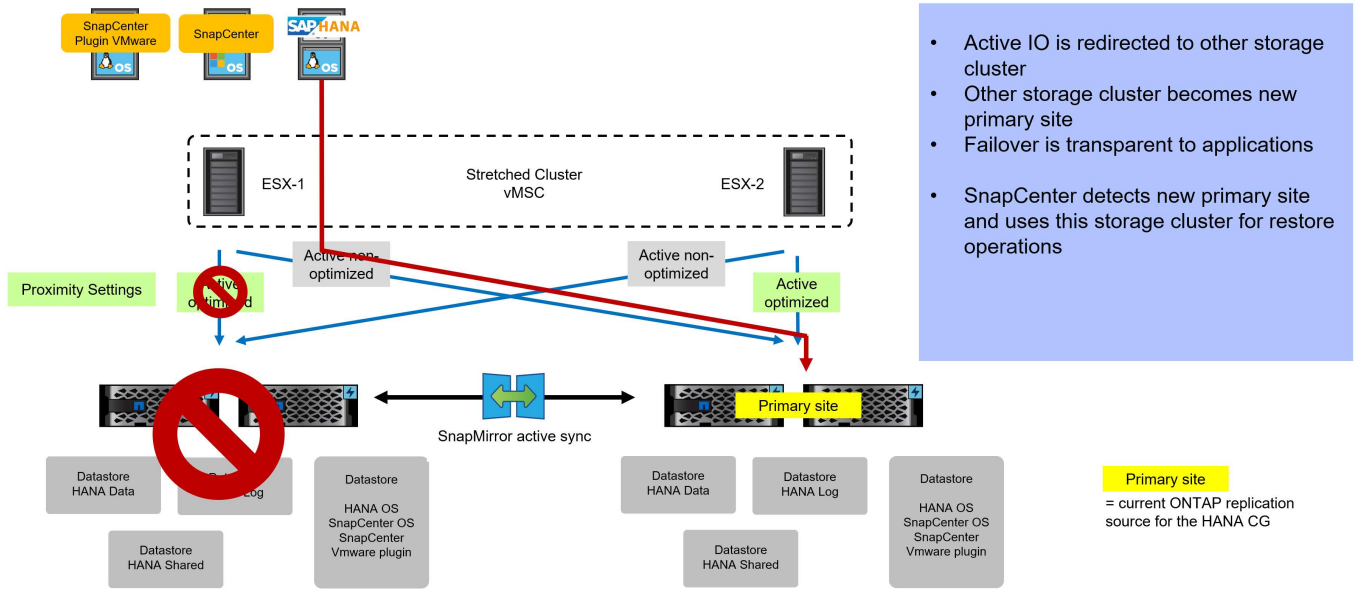
#### 通常運用時

通常運用時には、HANAシステムはESXホストESX-1からのアクティブな最適パスに基づいてローカルコピーの読み取りと書き込みを行います。各バックアップ処理で、SnapCenterはレプリケーション関係の現在のプライマリサイトを検出し、プライマリサイトに対してバックアップ処理を実行します。Snapshotはミラーコピーにレプリケートされ、両方のサイトで使用できます。プライマリサイトでSnapCenterリストア処理を実行します。



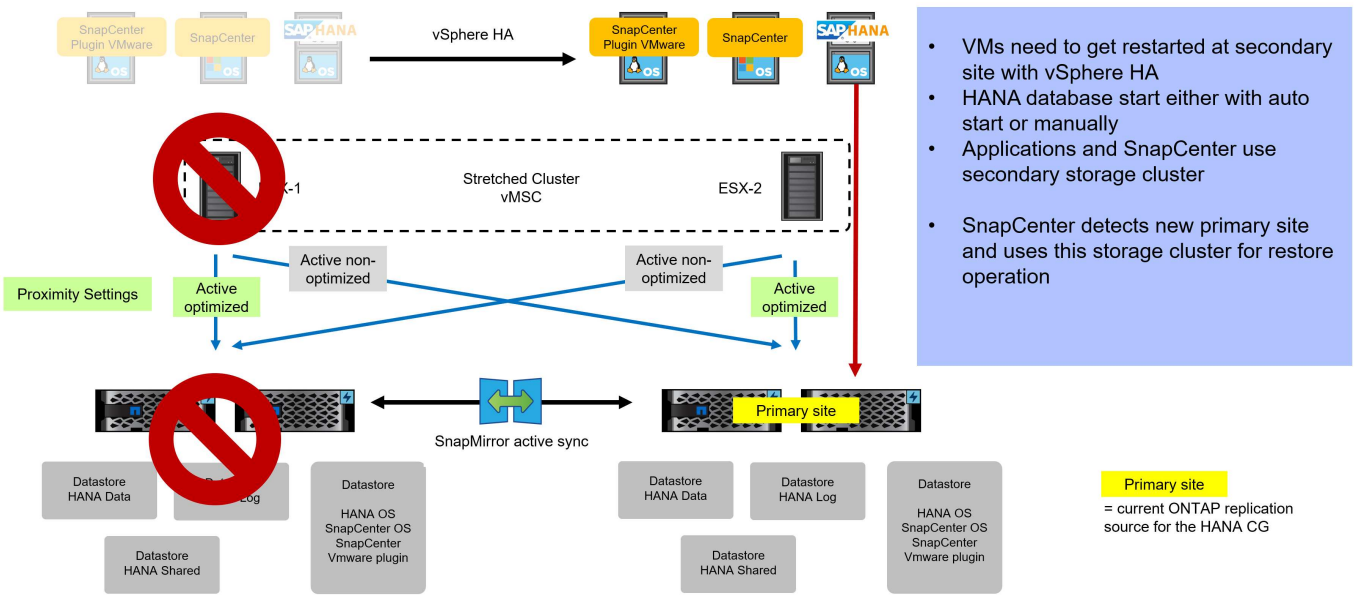

ストレージ障害

サイト1のストレージシステムに障害が発生した場合、HANAシステムはサイト2のミラーコピーにアクセスして処理を続行します。プライマリサイトがセカンダリサイトに切り替わり、SnapCenterが新しいプライマリサイトでバックアップとリストアの処理を実行するようになります。




サイト障害

サイト障害が発生した場合、HANA VMとSnapCenterおよびSnapCenter for VMwareプラグインVMは、vSphere HAを使用してセカンダリサイトのESXホストにフェイルオーバーします。HANAデータベースを起動し、セカンダリサイトのミラーコピーにアクセスする必要があります。プライマリサイトがセカンダリサイトに切り替わり、SnapCenterが新しいプライマリサイトでバックアップとリストアの処理を実行するようになります。

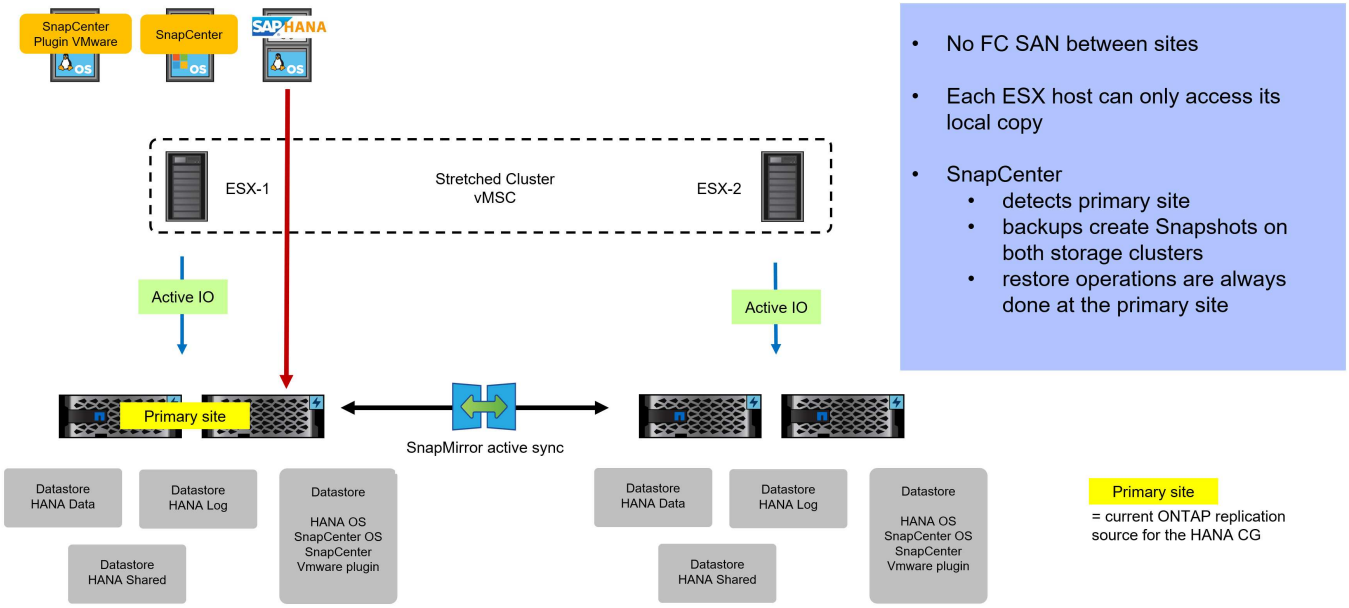



不均一なアクセス設定

統一されていないアクセス構成では、ファイバチャネルSANは両方のサイトに拡張されません。各サイトの各ESXホストは、データセットのローカルコピーにのみアクセスできます。

通常運用時

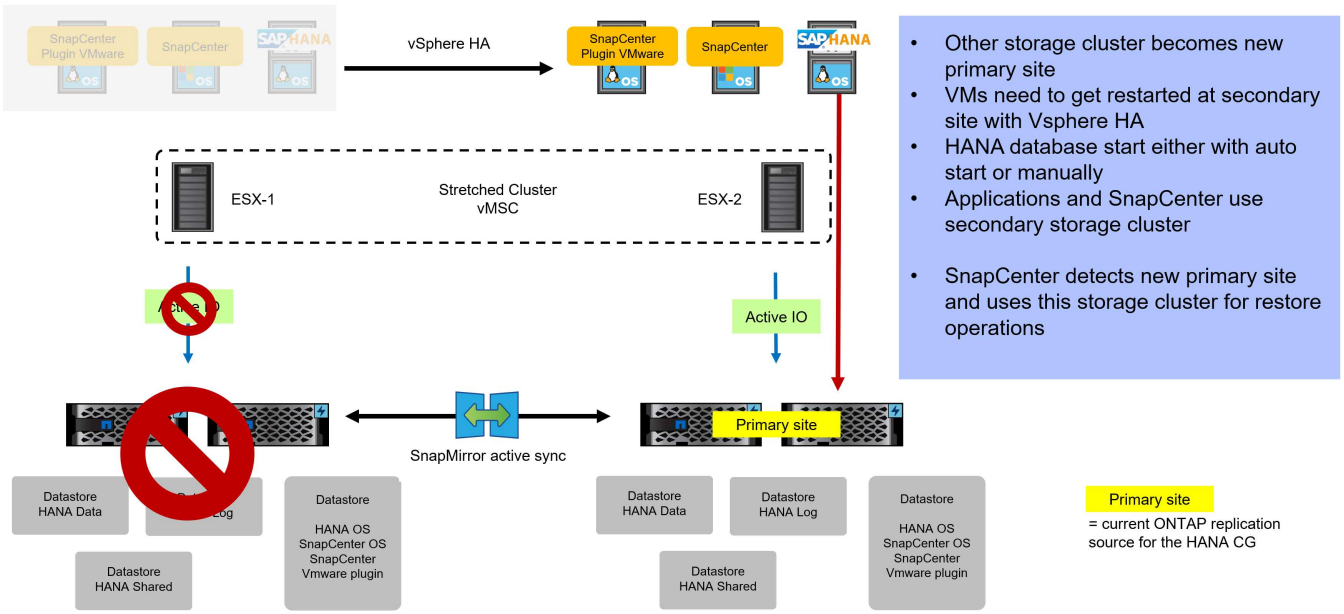
通常運用時、HANAシステムはローカルコピーとの間で読み取りと書き込みを行います。各バックアップ処理で、SnapCenterはレプリケーション関係の現在のプライマリサイトを検出し、プライマリサイトに対してバックアップ処理を実行します。Snapshotはミラーコピーにレプリケートされ、両方のサイトで使用できます。プライマリサイトでSnapCenterリストア処理を実行します。




ストレージ障害

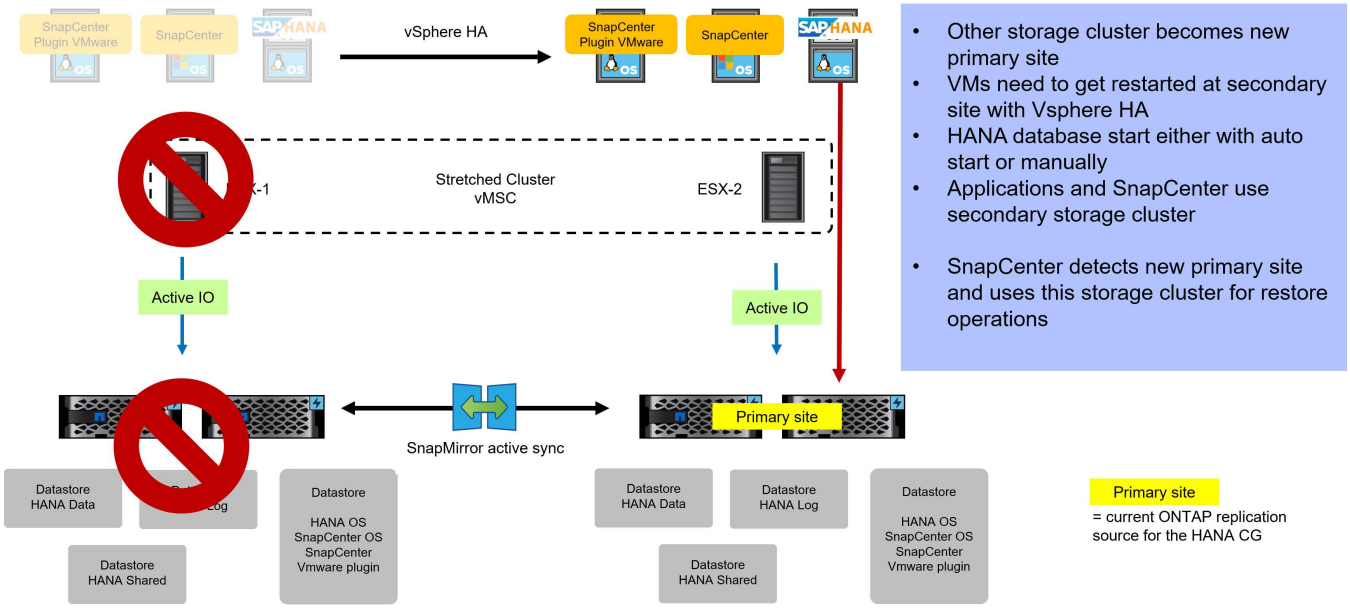
ストレージに障害が発生した場合、HANA VMとSnapCenterおよびSnapCenter for VMwareプラグインVMは、vSphere HAを使用してセカンダリサイトのESXホストにフェイルオーバーします。HANAデータベース

を起動し、セカンダリサイトのミラーコピーにアクセスする必要があります。プライマリサイトがセカンダリサイトに切り替わり、SnapCenterが新しいプライマリサイトでバックアップとリストアの処理を実行するようになります。




サイト障害

ストレージ障害と同じ。

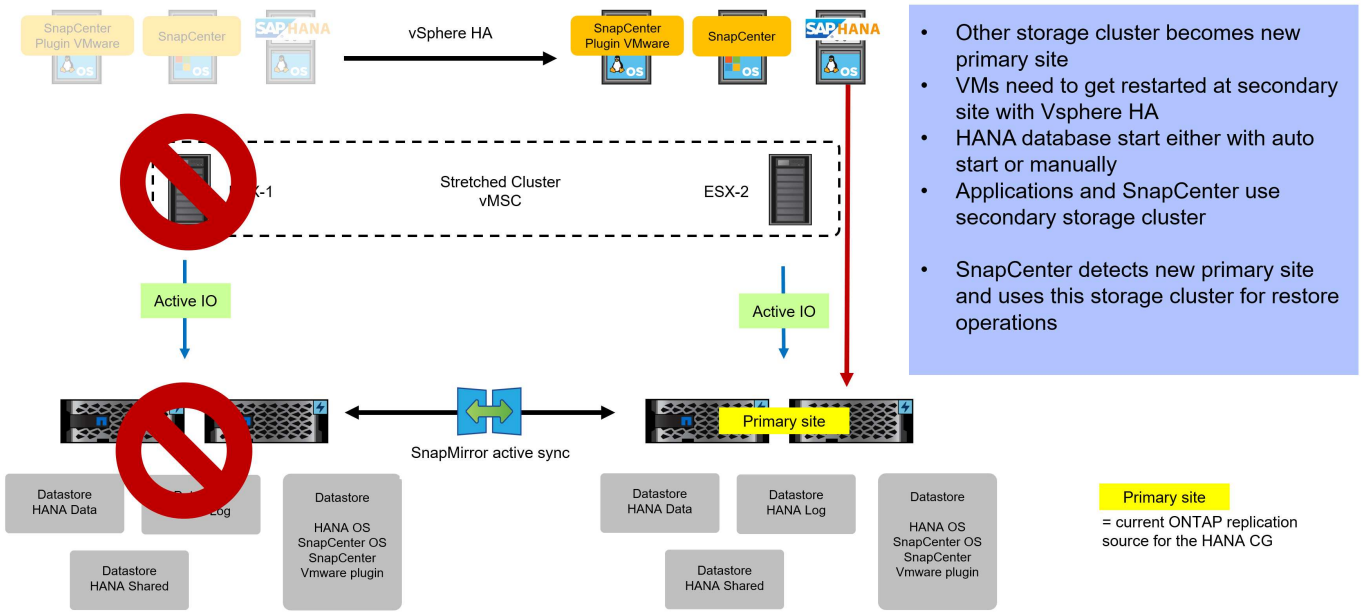



**HANA VM**またはプライマリサイトの再配置

HANA VMを他のESXホストに再配置し、ストレージのプライマリサイトを変更しないと、SnapCenterを使用したリストア処理は失敗します。SnapCenterはリストア処理を実行するためにプライマリサイトを使用するため、クローンは左側に作成され、HANA VMは右側で実行されます。サイト間にデータパスがないため、SnapCenterはデータをコピーしません。

この問題を回避するには、VMとプライマリ側の再配置を同時に実行するか、SnapCenterを使用したリストア

処理の前にプライマリサイトをフェイルオーバーする必要があります。




## 追加情報とバージョン履歴

この記事では、このソリューションに関連するその他のリソースへのリンクを示します。

SnapCenter ：

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

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

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

"SnapCenter ソフトウェアのドキュメント"

SnapMirrorアクティブ同期：

"ONTAPでのSnapMirrorアクティブ同期の概要"

"NetApp ONTAPとNetApp SnapMirrorは、VMware vSphere Metro Storage Cluster（vMSC）とアクティブに同期されます。"

"SnapMirrorアクティブ同期を使用したVMware vSphere Metroストレージクラスタ"

"VMware vSphere Metro Storage Cluster （ vMSC ）"

バージョン履歴：

| バージョン | 日付 | コメント |
| --- | --- | --- |
| バージョン 1.0 以降 | 2025年3月 | 初版 |

# VMware VMFSおよびNetApp ASAシステムを使用したSnapCenterによるSAP HANAデータ保護

## VMware VMFSおよびNetApp ASAシステムを使用したSnapCenterによるSAP HANAデータ保護

このドキュメントでは、VMware 上で実行され、VMFS を使用するデータストアとNetApp ASAシステムに保存された LUN を備えた HANA システムに対してSnapCenterを使用したデータ保護のベスト プラクティスについて説明します。

作成者：Nils Bauer、NetApp

本ドキュメントの内容

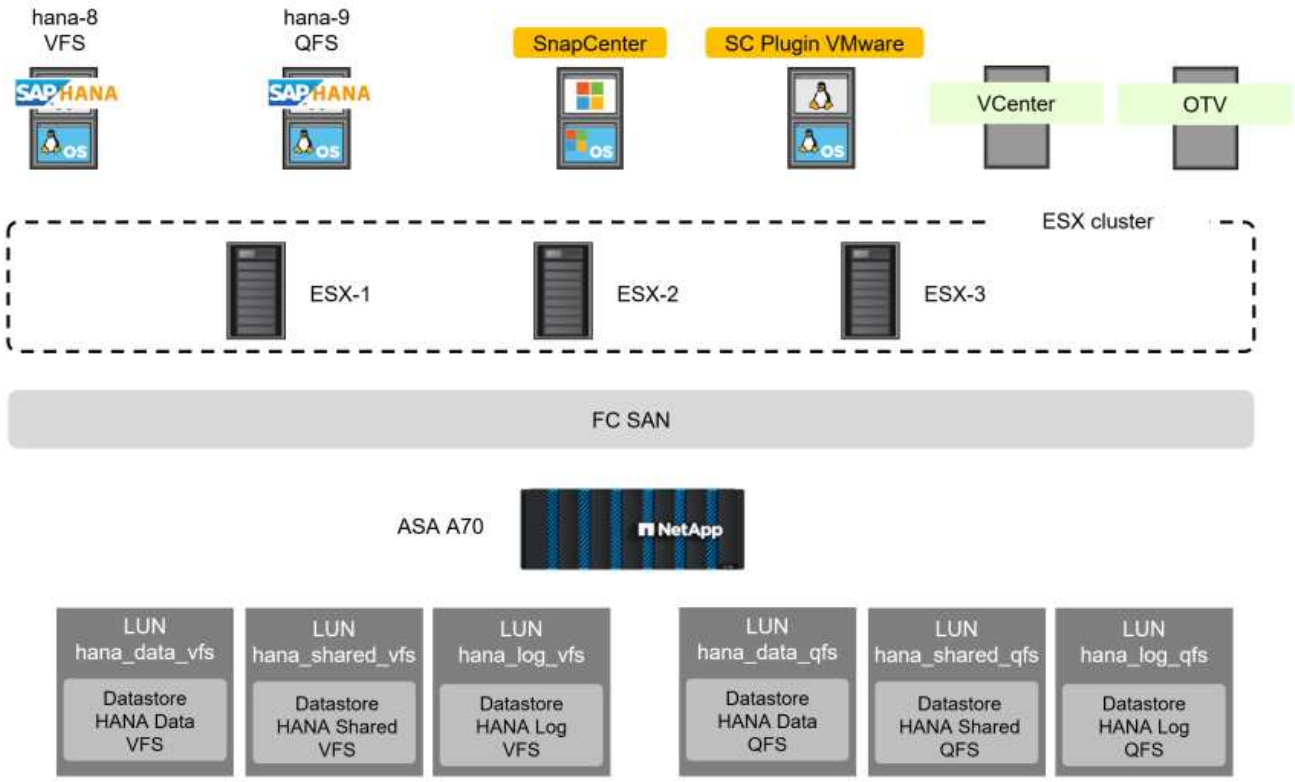
これは、環境全体を構成するためのステップバイステップのガイドではありませんが、次のような VMFS 上のSnapCenterおよび HANA に固有の詳細に重点を置いています。

- VMware VMFS を使用した SAP HANA システムのセットアップ
- VMFS を使用した VMware 上の HANA 向けの特定のSnapCenter構成
- VMFS を使用した VMware 上の HANA のSnapCenterバックアップ、リストア、リカバリ操作
- VMFS を使用した VMware 上の HANA 向けSnapCenter SAP システム更新操作

詳細情報および詳細な設定手順については、 ""追加情報""章。

## このドキュメントで使用したラボのセットアップ

下の図は、使用したラボのセットアップの概要を示しています。2つの単一ホストHANA MDCシステムを使用して、様々な操作をデモンストレーションしています。HANAシステムVFSはバックアップ、リストア、リカバリ操作の実行用に指定され、HANAシステムQFSはSAPシステムリフレッシュ操作のターゲットシステムとして機能します。VMware向けSnapCenterプラグインは、VMware VMFSで構成されたHANAリソースをSnapCenterで管理するために不可欠です。HANAシステムのストレージユニットのプロビジョニングにはVMware向けONTAPツールを使用しましたが、必須コンポーネントではありません。




ソフトウェアバージョン

| ソフトウェア | バージョン |
| --- | --- |
| ONTAP | ASA A70 ONTAP 9.16.1 |
| vSphereクライアント | 8.0.3 |
| ESXi | 8.0.3 |
| vSphere用SnapCenterプラグイン | 6.1.0 |
| ONTAP tools for VMware vSphere | 10.4 |
| Linux OS | SLES for SAP 15 SP6 |
| SAP HANA のサポート | 2.0 SPS8 |
| SnapCenter | 6.1P1 |

## HANAシステムのプロビジョニングとインストール

この章では、VMFSを使用するVMware環境に固有のSAP HANAシステムのインストールと設定について説明します。その他の一般的なベストプラクティスについては、を参照してください "『 SAP HANA on NetApp ASA Systems with Fibre Channel Protocol 』を参照してください"。

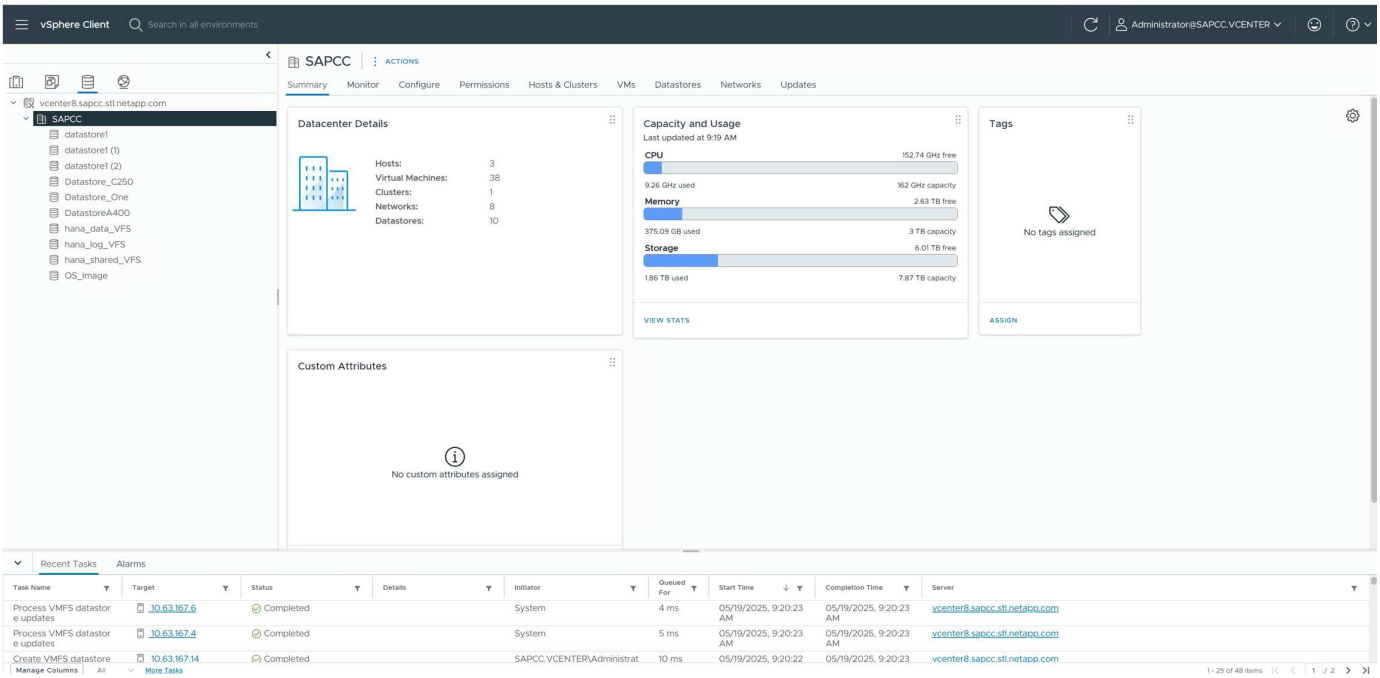
ストレージ構成

SAPが本番環境のHANAシステム向けに定義したストレージパフォーマンスKPIを満たすには、HANAシステムのデータおよびログファイルシステム用に専用のLUNとデータストアを構成する必要があります。データストアは、複数のHANAシステムや他のワークロード間で共有しないでください。

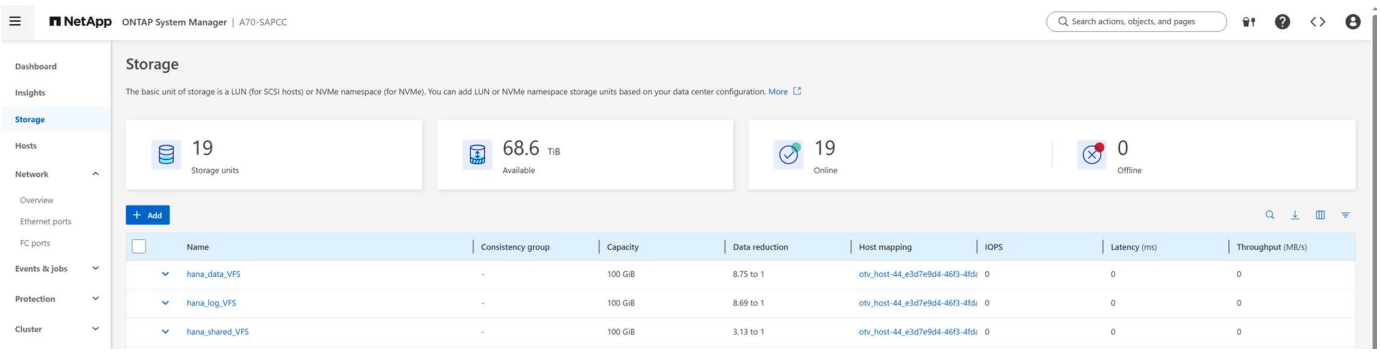
HANA システム VFS の 3 つのデータストアをプロビジョニングするために、 ONTAP Tools for VMware (OTV) が使用されています。

- ハナ+_データ+___VFS
- hana+_log++VFS
- hana+_共有++VFS

HANA 共有ファイルシステムのデータストアは、複数の HANA システム間で共有することもできます。

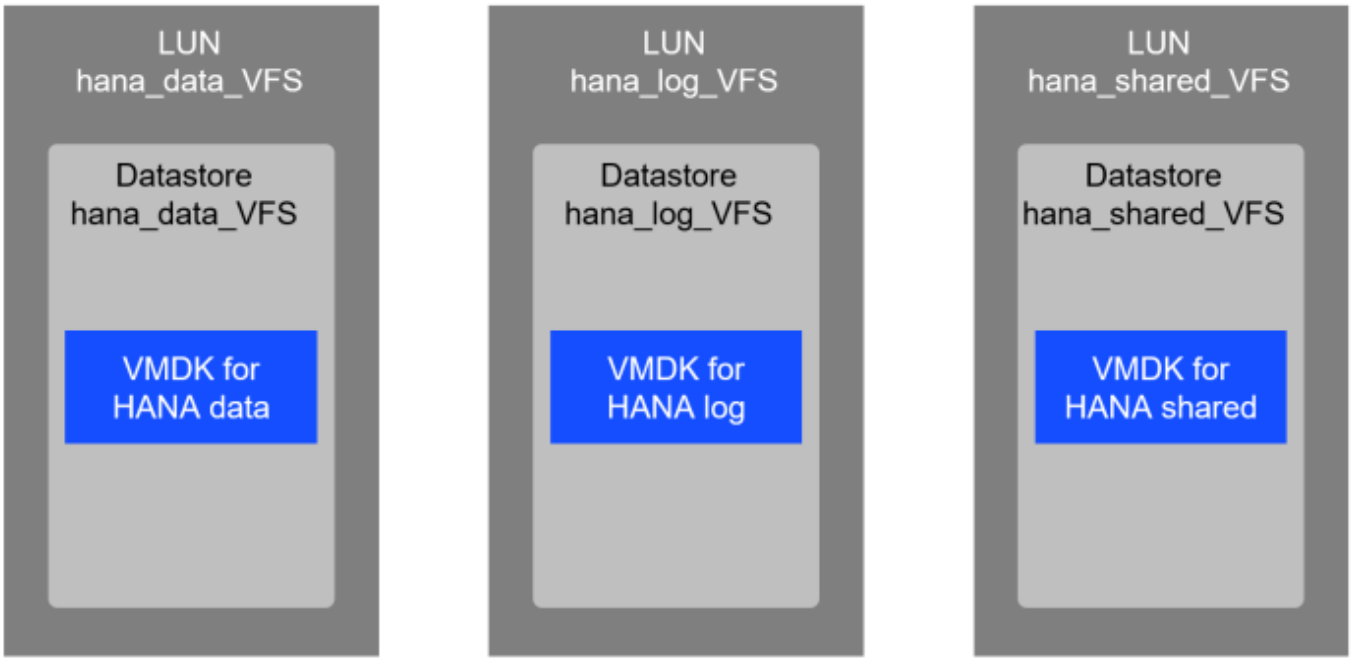


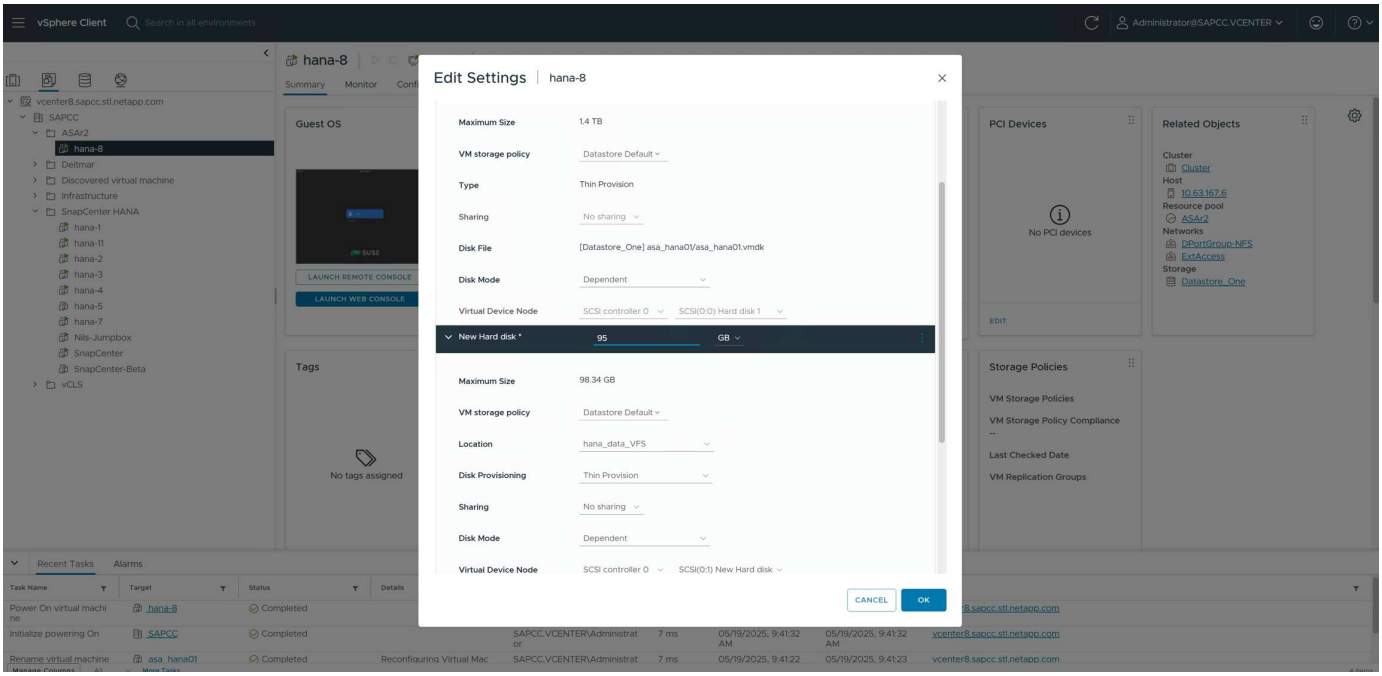

ストレージ システムでは、OTV によって 3 つの LUN が作成されています。

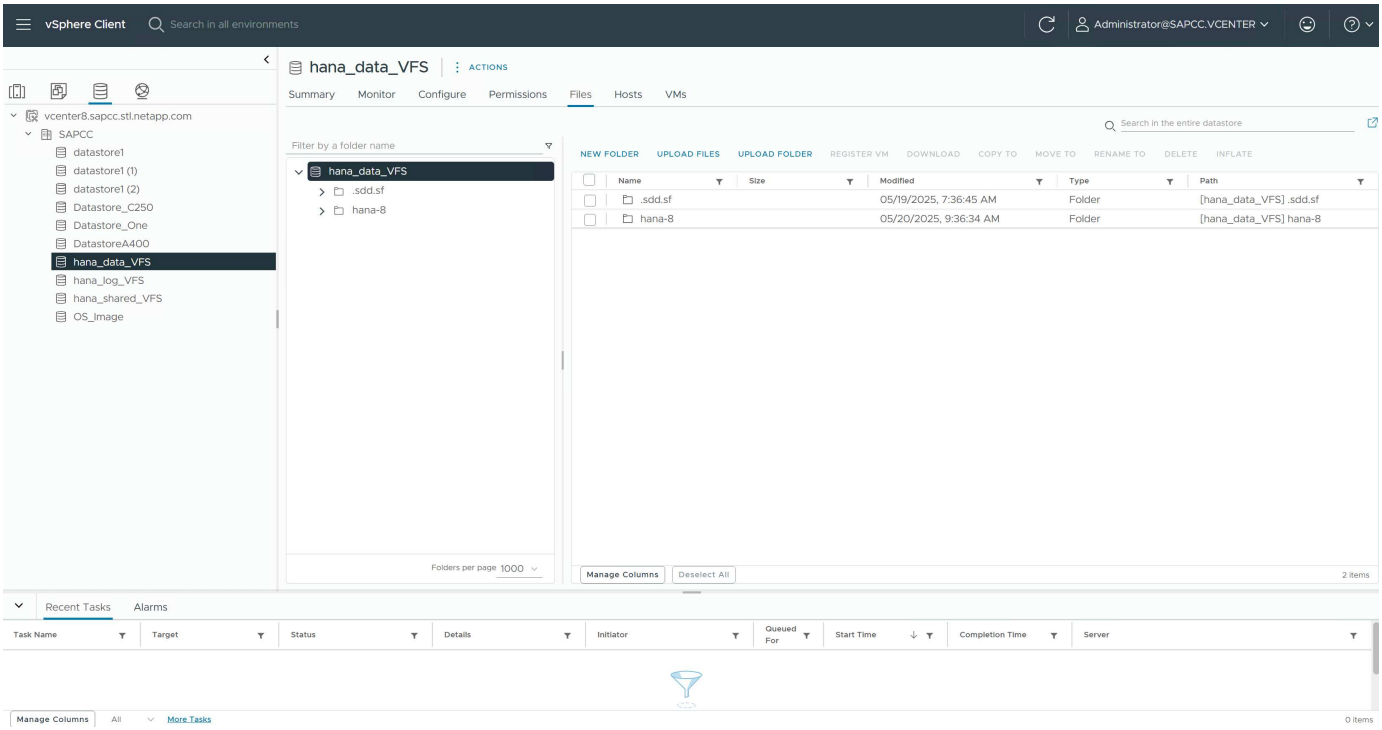



## VMディスク構成

HANA VMに3つの新しいディスク（VMDK）を追加する必要があります。各ディスクは、下図に示すように、以前に作成されたデータストアのいずれかに格納されます。


LUN
hana_data_VFS
Datastore
hana_data_VFS
VMDK for
HANA data
LUN
hana_log_VFS
Datastore
hana_log_VFS
VMDK for
HANA log
LUN
hana_shared_VFS
Datastore
hana_shared_VFS
VMDK for
HANA shared


vSphere Client
Edit Settings
hana-8
Maximum Size
1.4 TB
VM storage policy
Datastore Default
Type
Thin Provision
Sharing
No sharing
Disk File
[Datastore_One] asa_hana01/asa_hana01.vmdk
Disk Mode
Dependent
Virtual Device Node
SCSI controller 0
SCSI(0:0) Hard disk 1
New Hard disk *
95
GB
Maximum Size
98.34 GB
VM storage policy
Datastore Default
Location
hana_data_VFS
Disk Provisioning
Thin Provision
Sharing
No sharing
Disk Mode
Dependent
Virtual Device Node
SCSI controller 0
SCSI(0:1) New Hard disk
CANCEL
OK



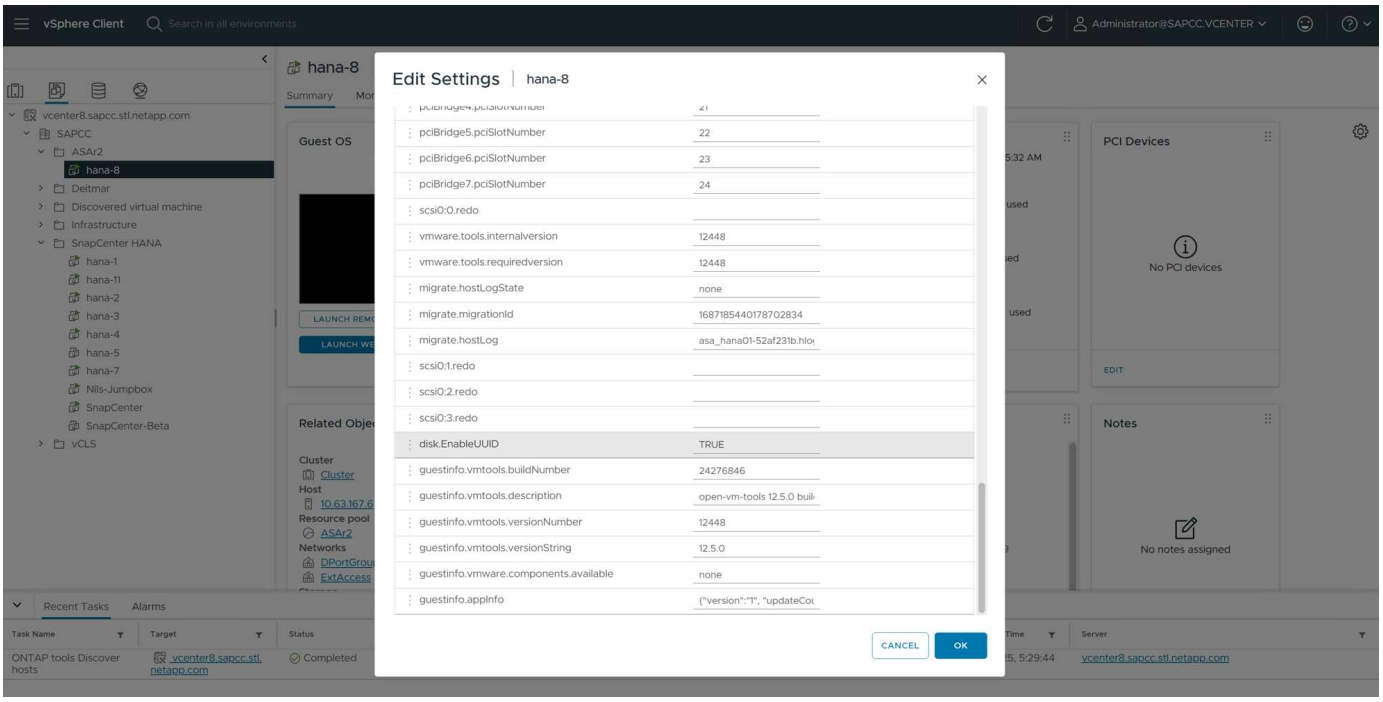

3 つのディスクが VM に追加されると、OS レベルでリストできるようになります。

```
hana-8:~ # lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 100G 0 disk
├─sda1 8:1 0 256M 0 part /boot/efi
└─sda2 8:2 0 82G 0 part
├─system-root 254:0 0 60G 0 lvm /root
│ /var
│ /usr/local
│ /tmp
│ /srv
│ /opt
│ /home
│ /boot/grub2/x86++_++64-efi
│ /boot/grub2/i386-pc
│ /.snapshots
│ /
└─system-swap 254:1 0 2G 0 lvm [SWAP]
sdb 8:16 0 95G 0 disk
sdc 8:32 0 95G 0 disk
sdd 8:48 0 95G 0 disk
sr0 11:0 1 17.1G 0 rom
```

### VMパラメータdisk.EnableUUID

このパラメータを適切に設定する必要があります。そうしないと、 SnapCenterデータベースの自動検出は失敗します。

1. VMのシャットダウン
2. 新しいパラメータ「disk.EnableUUID」を追加し、「TRUE」に設定します
3. Start VM




### Linuxホストテノフアイルシステムノシユンヒ

新しいディスクでのxfsファイルシステムの作成

3つの新しいディスクそれぞれにxfsファイルシステムが作成されている。

```
hana-8:~ # mkfs.xfs /dev/sdb
meta-data=/dev/sdb isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nrext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.

hana-8:~ # mkfs.xfs /dev/sdc
meta-data=/dev/sdc isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nrext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.

hana-8:~ # mkfs.xfs /dev/sdd
meta-data=/dev/sdd isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nrext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.

hana-8:~ #
```

マウントポイントの作成

```
hana-8:/ # mkdir -p /hana/data/VFS/mnt00001
hana-8:/ # mkdir -p /hana/log/VFS/mnt00001
hana-8:/ # mkdir -p /hana/shared
hana-8:/ # chmod –R 777 /hana/log/SMA
hana-8:/ # chmod –R 777 /hana/data/SMA
hana-8:/ # chmod -R 777 /hana/shared
```

**/etc/fstab**の設定

```
hana-8:/ # cat /etc/fstab

/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=/@/var 0 0
/dev/system/root /usr/local btrfs subvol=/@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=/@/tmp 0 0
/dev/system/root /srv btrfs subvol=/@/srv 0 0
/dev/system/root /root btrfs subvol=/@/root 0 0
/dev/system/root /opt btrfs subvol=/@/opt 0 0
/dev/system/root /home btrfs subvol=/@/home 0 0
/dev/system/root /boot/grub2/x86++_++64-efi btrfs
subvol=/@/boot/grub2/x86++_++64-efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=/@/.snapshots 0 0
UUID=FB79-24DC /boot/efi vfat utf8 0 2
### SAPCC_share
192.168.175.86:/sapcc_share /mnt/sapcc-share nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
/dev/sdb /hana/data/VFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/VFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
hana-8:/ #

hana-8:/ # df -h
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 4.4G 54G 8% /
devtmpfs 4.0M 0 4.0M 0% /dev
tmpfs 49G 0 49G 0% /dev/shm
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 18M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
```

```
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/mapper/system-root 60G 4.4G 54G 8% /.snapshots
/dev/mapper/system-root 60G 4.4G 54G 8% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 4.4G 54G 8% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 4.4G 54G 8% /home
/dev/mapper/system-root 60G 4.4G 54G 8% /opt
/dev/mapper/system-root 60G 4.4G 54G 8% /srv
/dev/mapper/system-root 60G 4.4G 54G 8% /tmp
/dev/mapper/system-root 60G 4.4G 54G 8% /usr/local
/dev/mapper/system-root 60G 4.4G 54G 8% /var
/dev/sda1 253M 5.9M 247M 3% /boot/efi
/dev/mapper/system-root 60G 4.4G 54G 8% /root
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
192.168.175.86:/sapcc_share 1.4T 840G 586G 59% /mnt/sapcc-share
/dev/sdb 95G 1.9G 94G 2% /hana/data/VFS/mnt00001
/dev/sdc 95G 1.9G 94G 2% /hana/log/VFS/mnt00001
/dev/sdd 95G 1.9G 94G 2% /hana/shared

hana-8:/ #
```

#### HANAのインストール

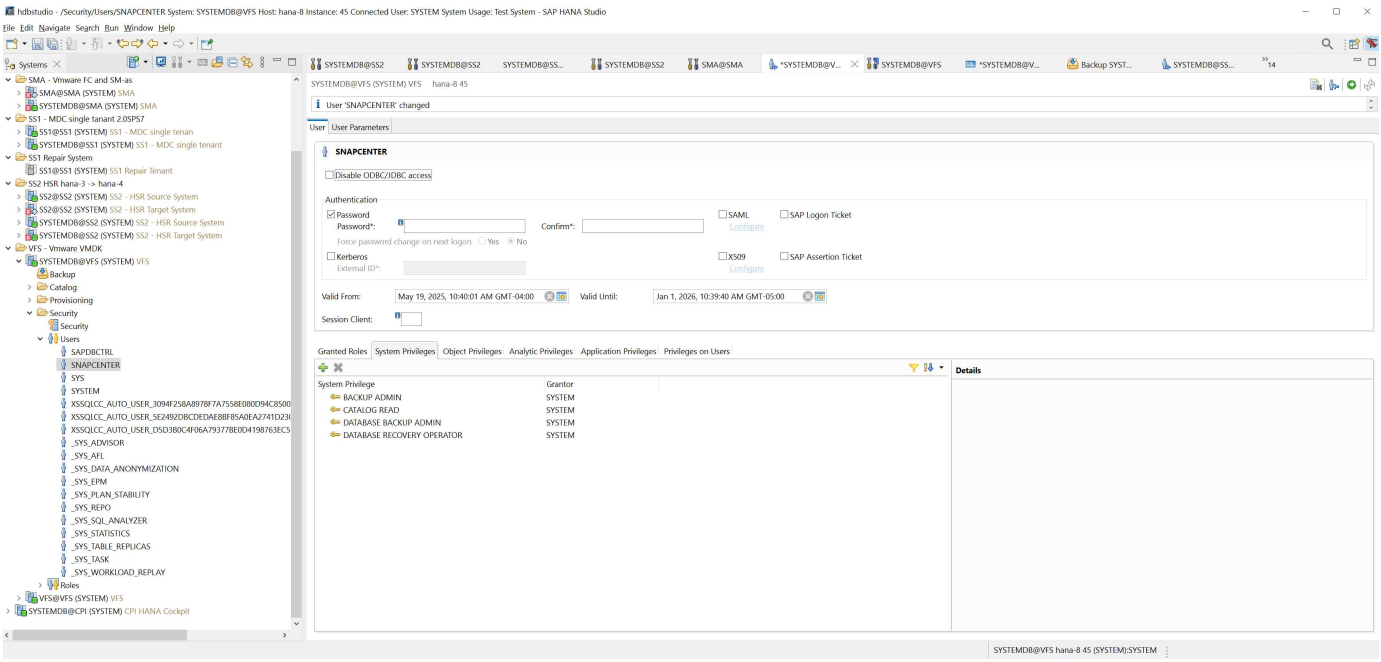
これで、HANAのインストールを実行できます。

> 上記の設定では、/usr/sap/VFS ディレクトリは OS VMDK 上に配置されます。/usr/sap/VFS を共有 VMDK 上に保存する必要がある場合は、hana 共有ディスクをパーティション分割して、/usr/sap/VFS 用の別のファイルシステムを提供することができます。

## HANA構成

#### SnapCenterデータベースユーザーを構成する

システムデータベースユーザのユーザストアを作成し、SnapCenterで使用する必要があります。




### HDBユーザーストアキーを設定する

ユーザーvfsadmのユーザーストアキーを作成する必要があります。ポート通信のために、HANAインスタンス番号を適切に設定する必要があります。セットアップでは、インスタンス番号「45」が使用されます。

```
vfsadm@hana-8:/usr/sap/VFS/HDB45> hdbuserstore SET VFSKEY hana-8:34513
SNAPCENTER <password>

Retroactive report: Operation succeed.
```

アクセスを確認するには:

```
vfsadm@hana-8:/usr/sap/VFS/HDB45> hdbsql -U VFSKEY

Welcome to the SAP HANA Database interactive terminal.
Type: \h for help with commands
\q to quit
hdbsql SYSTEMDB=> exit

vfsadm@hana-8:/usr/sap/VFS/HDB45>
```

## SnapCenter 構成

前提条件

**SnapCenter HANA**リソースを自動検出する必要があります

VMware VMFS で構成されたリソースは、これらの構成に必要な特定の操作を有効にするために、

SnapCenterによって自動検出される必要があります。

HANA 非データ ボリュームはSnapCenterで常に手動で構成されるリソースであるため、VMFS を使用したSnapCenterではサポートされません。

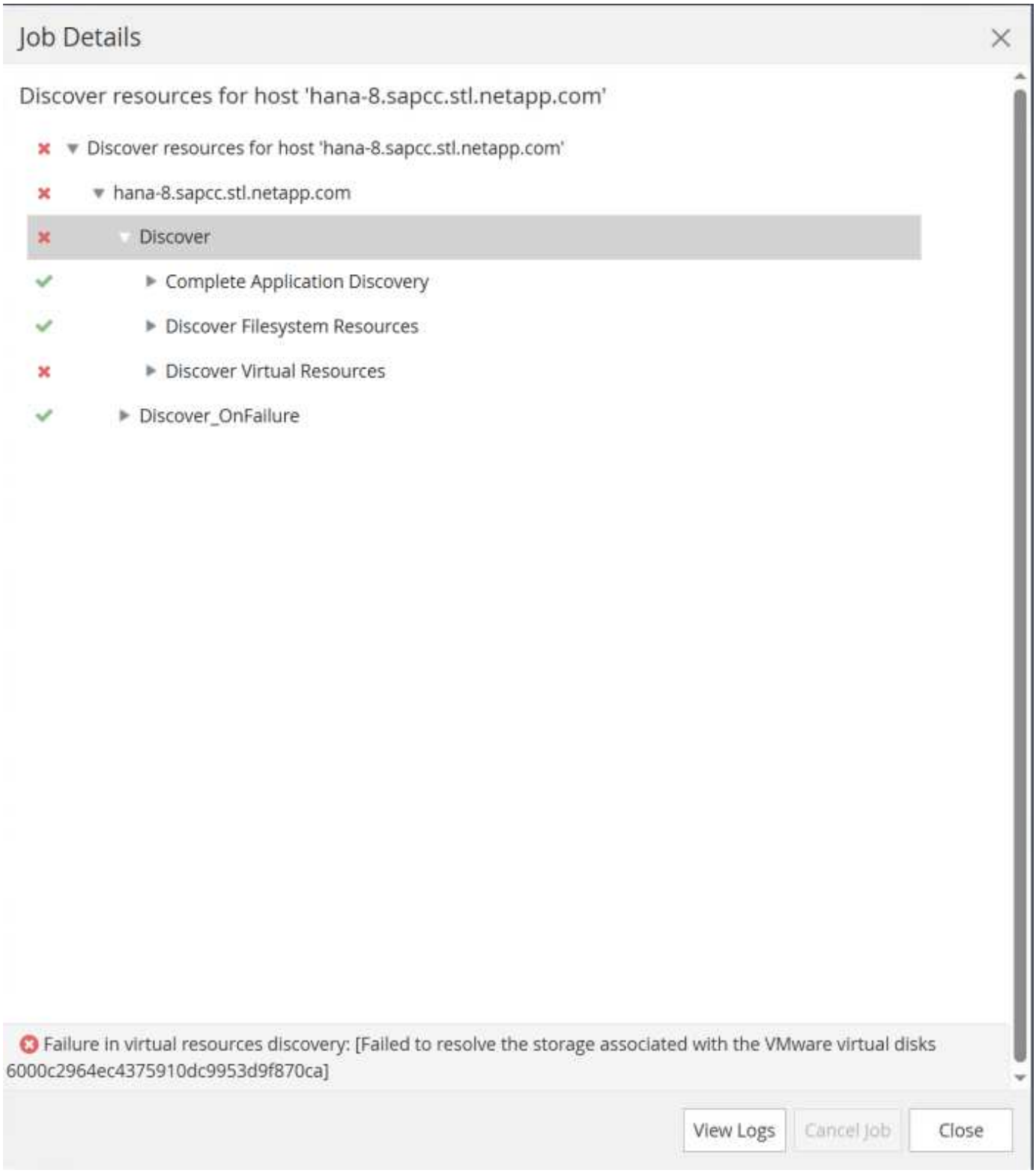
SAP HANAのマルチホストシステムは、中央のHANAプラグインを使用して設定する必要があるため、デフォルトでは手動で設定されます。また、VMware VMFSを使用する場合、このようなシステムはSnapCenterではサポートされません。

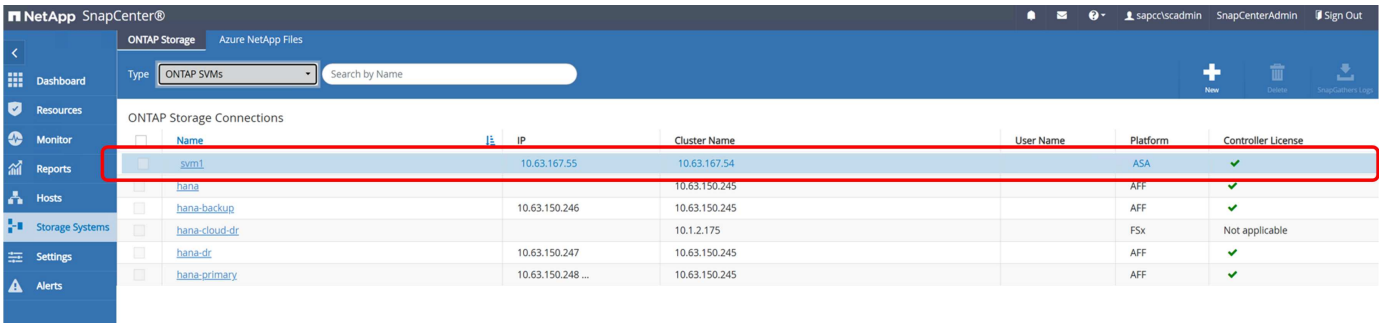
#### SnapCenter for VMware vSphereプラグイン

SnapCenter for VMware vSphereプラグインをVMware環境に導入する必要があります。

#### Storage SVM 管理 IP

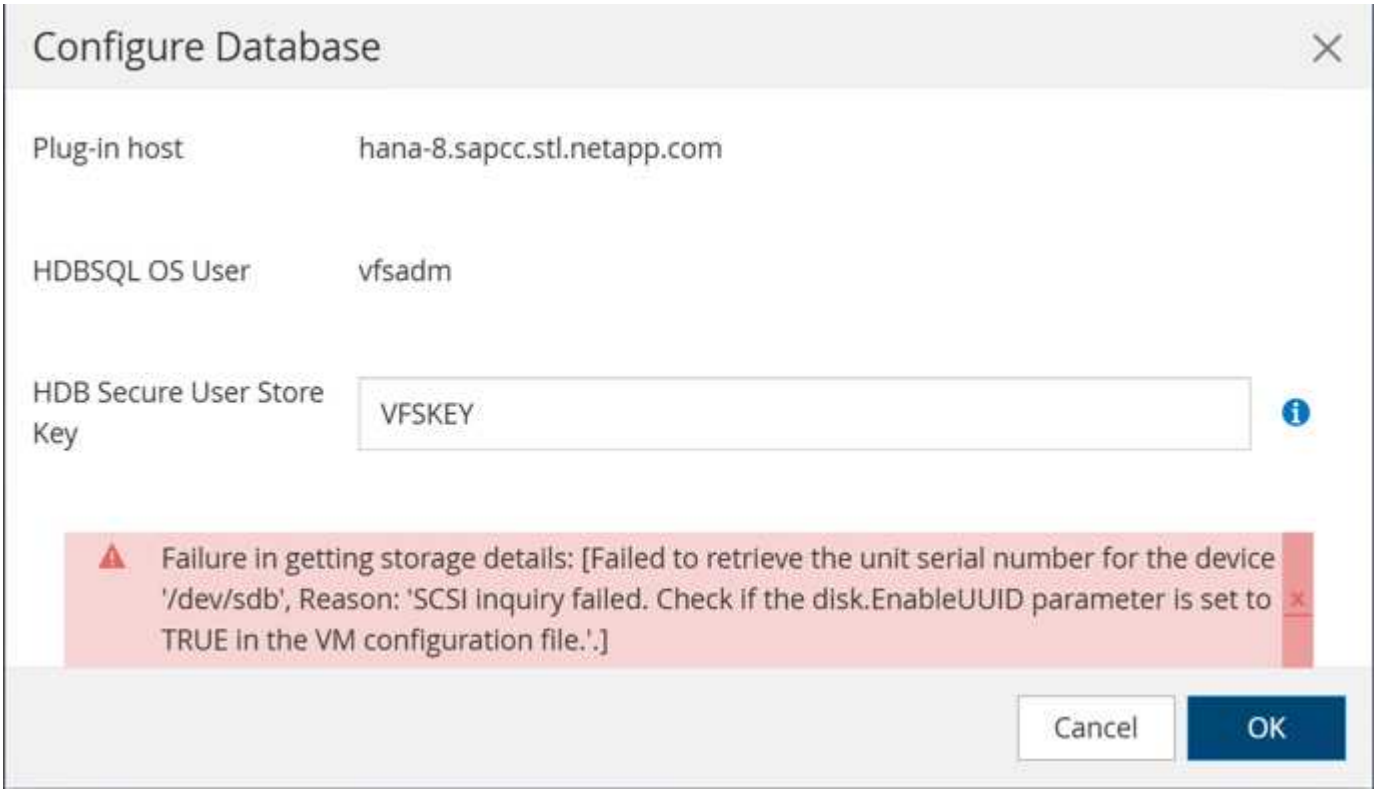
LUN をホストするストレージ SVM には管理インターフェイスが設定されている必要があります。そうでないと、「クラスターの追加」オプションを使用してストレージを追加したときに SVM がSnapCenterにリストされず、自動検出操作が失敗します。


Job Details
Discover resources for host 'hana-8.sapcc.stl.netapp.com'
Discover resources for host 'hana-8.sapcc.stl.netapp.com'
hana-8.sapcc.stl.netapp.com
Discover
Complete Application Discovery
Discover Filesystem Resources
Discover Virtual Resources
Discover_OnFailure
Failure in virtual resources discovery: [Failed to resolve the storage associated with the VMware virtual disks 6000c2964ec4375910dc9953d9f870ca]
View Logs
Cancel Job
Close




**VM**ディスクパラメータ

パラメータは、章で説明されているように設定する必要があります。 "「VMパラメータdisk.EnableUUID」"そうしないと、 SnapCenterデータベースの自動検出は失敗します。



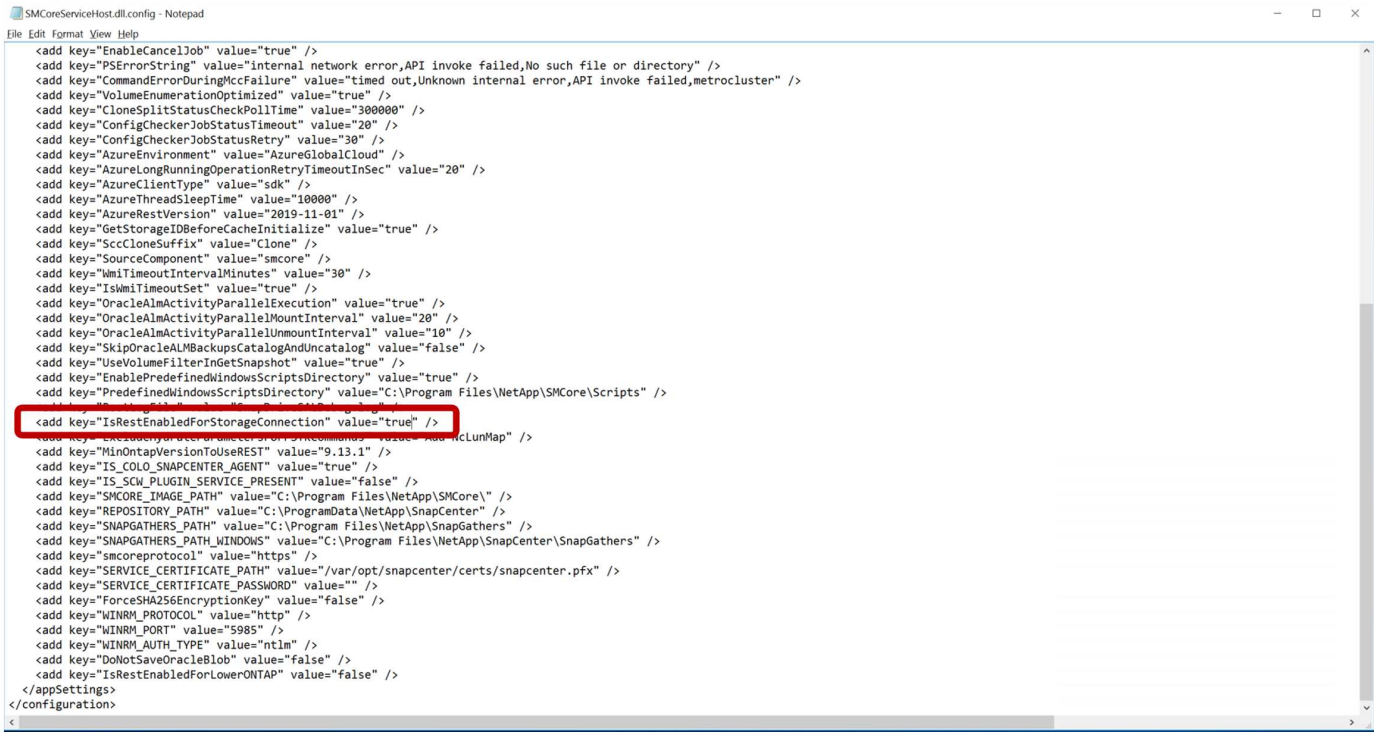

ストレージ通信に**REST API**を使用するように**SnapCenter**を構成する

SnapCenterは、ストレージ通信にREST APIを使用するように設定する必要があります。設定されていない場合、スナップショット作成操作は失敗し、以下のエラーメッセージが表示されます。

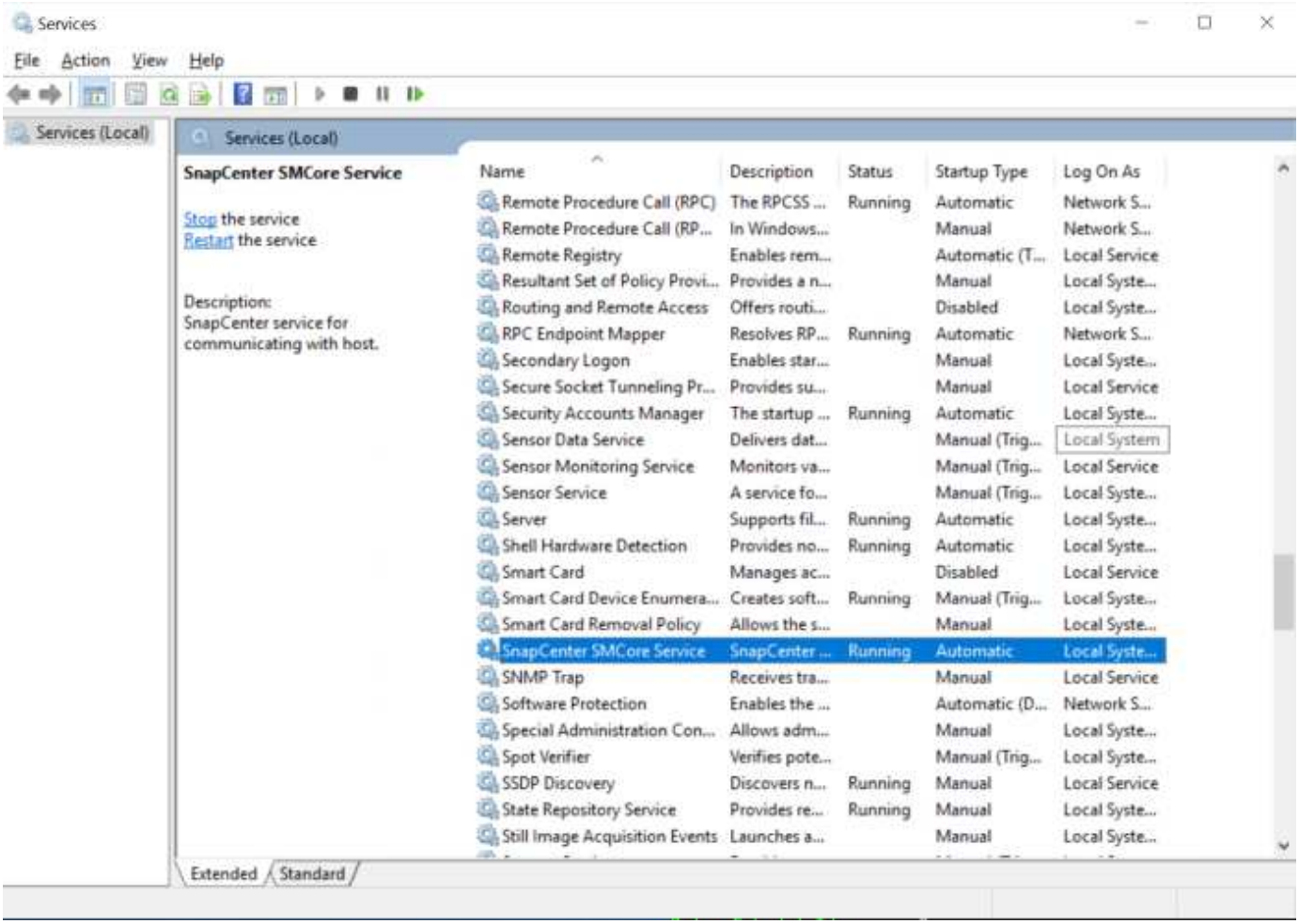



構成ファイル + C:\Program Files\NetApp\SMCore\SMCoreServiceHost.dll.config 内のパラメーター「IsRestEnabledForStorageConnection」を「true」に設定する必要があります。

<キー="IsRestEnabledForStorageConnection" 値="true" を追加 />



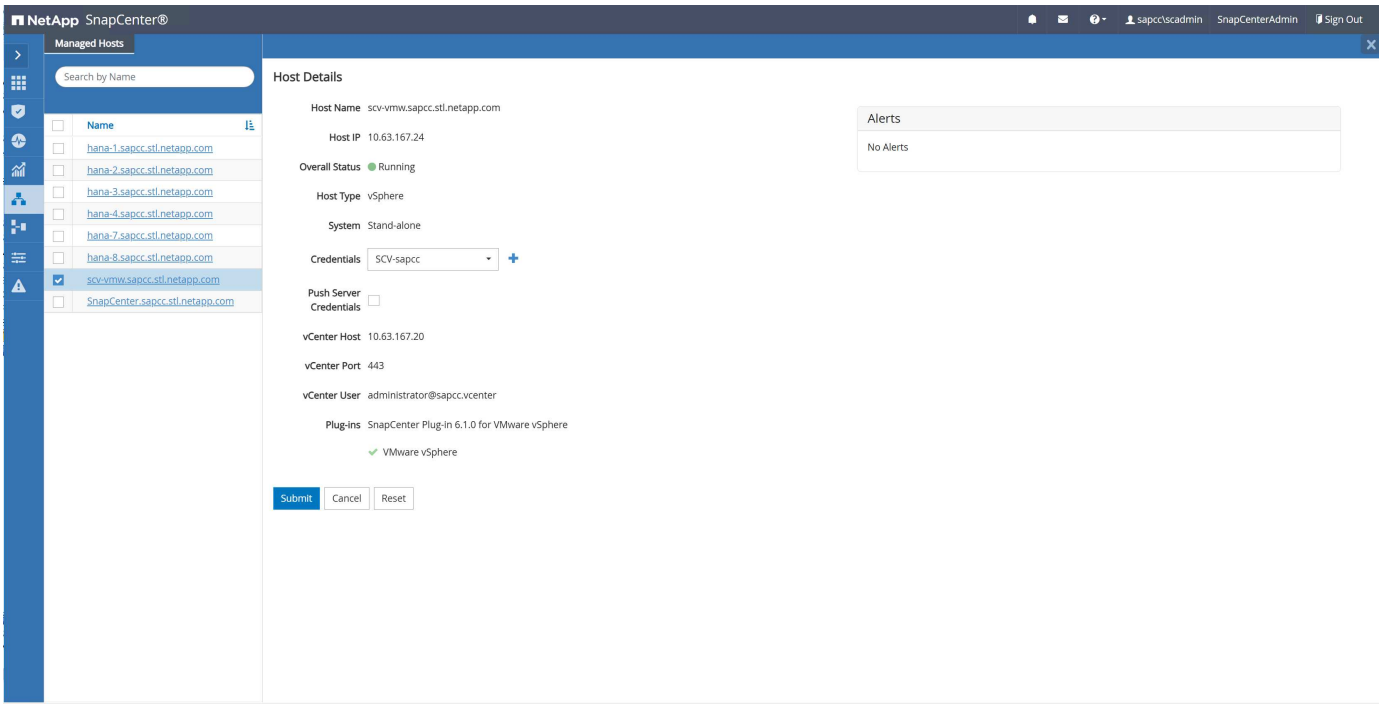

変更を行った後、 SnapCenter SMCore サービスを停止して起動する必要があります。



### SnapCenterにVMwareプラグインを追加する

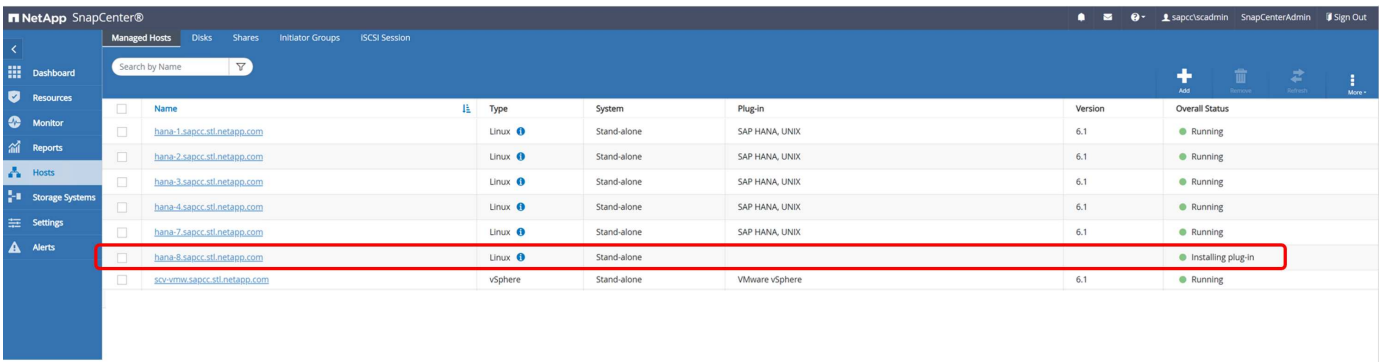
ホストをSnapCenterに追加する前に、VMware vSphere用SnapCenterプラグインをVMware環境に導入する必要があります。も参照してください "SnapCenter Plug-in for VMware vSphereの導入"。

クレデンシャルはホスト追加ワークフローで設定する必要があります。ホストタイプとしてvSphereを選択できます。

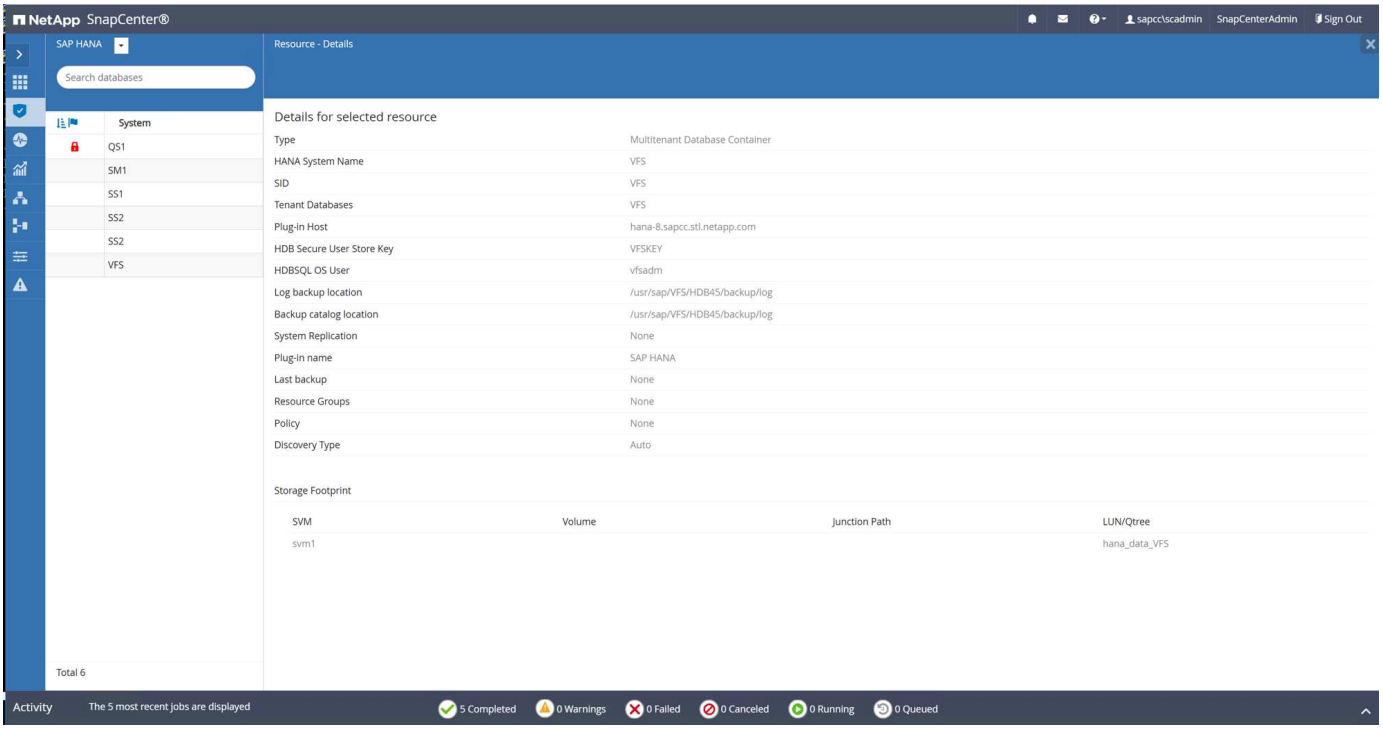



### HANAホストを追加する

具体的な要件はありません。プラグインの導入と自動検出は通常どおり実行されます。




自動検出プロセスにより、 SnapCenter はHANA リソースが VMFS で仮想化されて実行されていることを検出します。

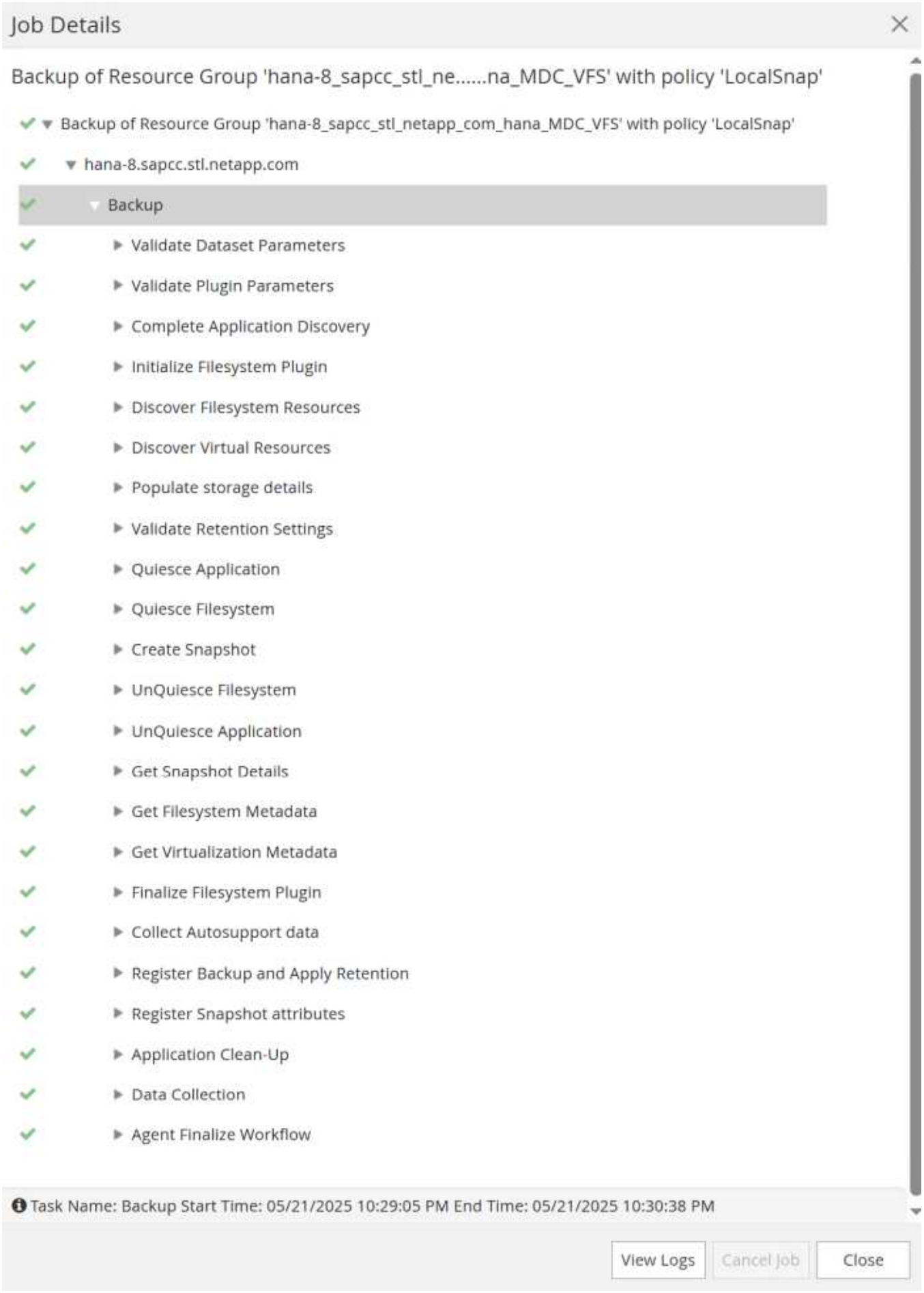


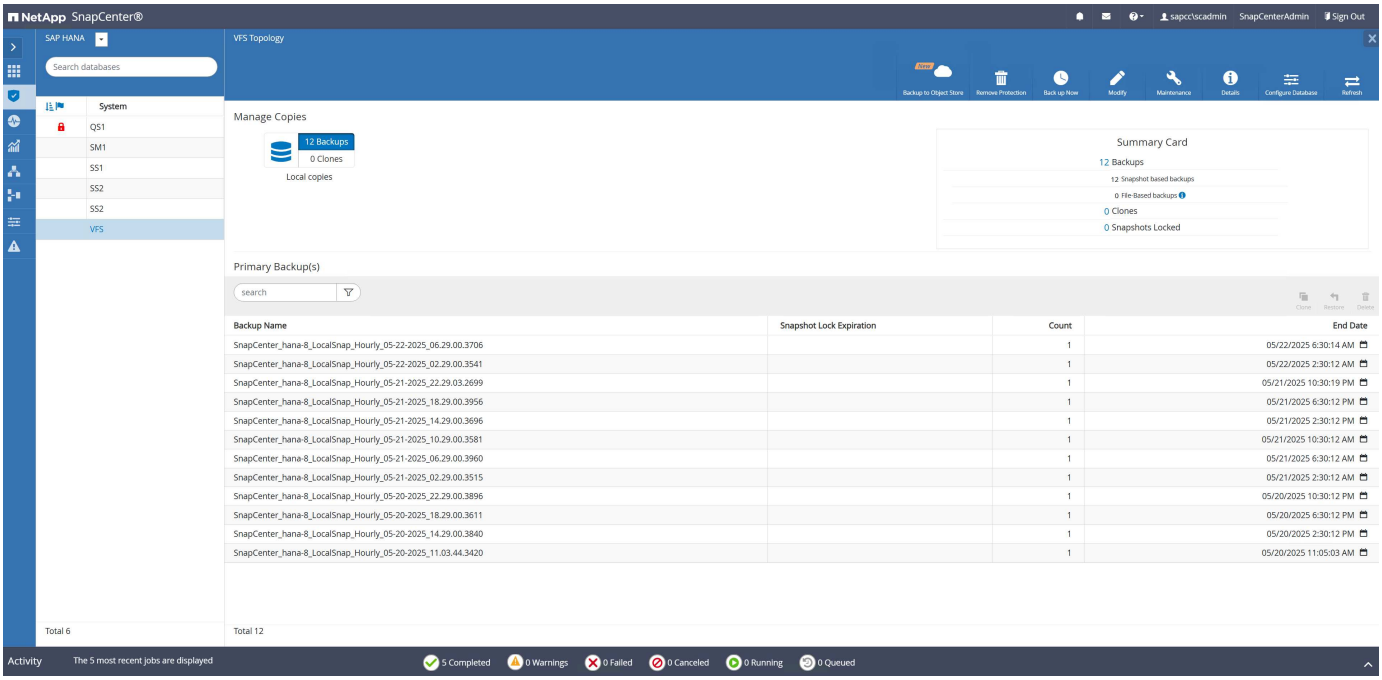

ポリシーとリソース保護の構成

VMFS を使用する VMware に固有のものはありません。

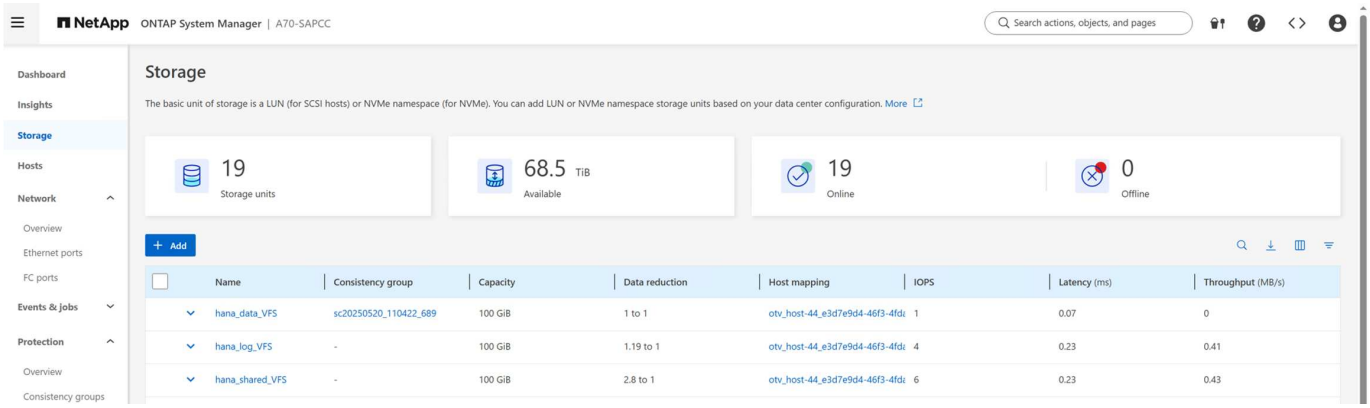
## バックアップ処理

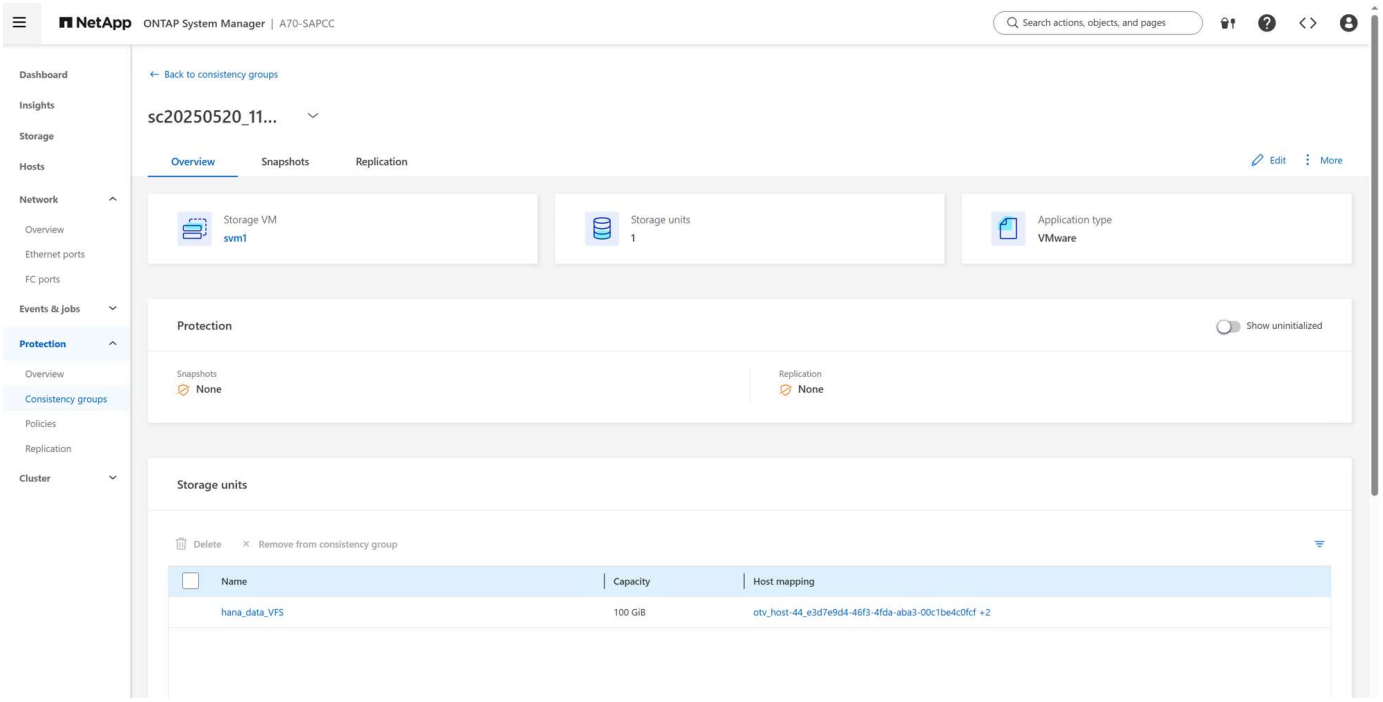
VMFS を使用する VMware に固有のものはありません。

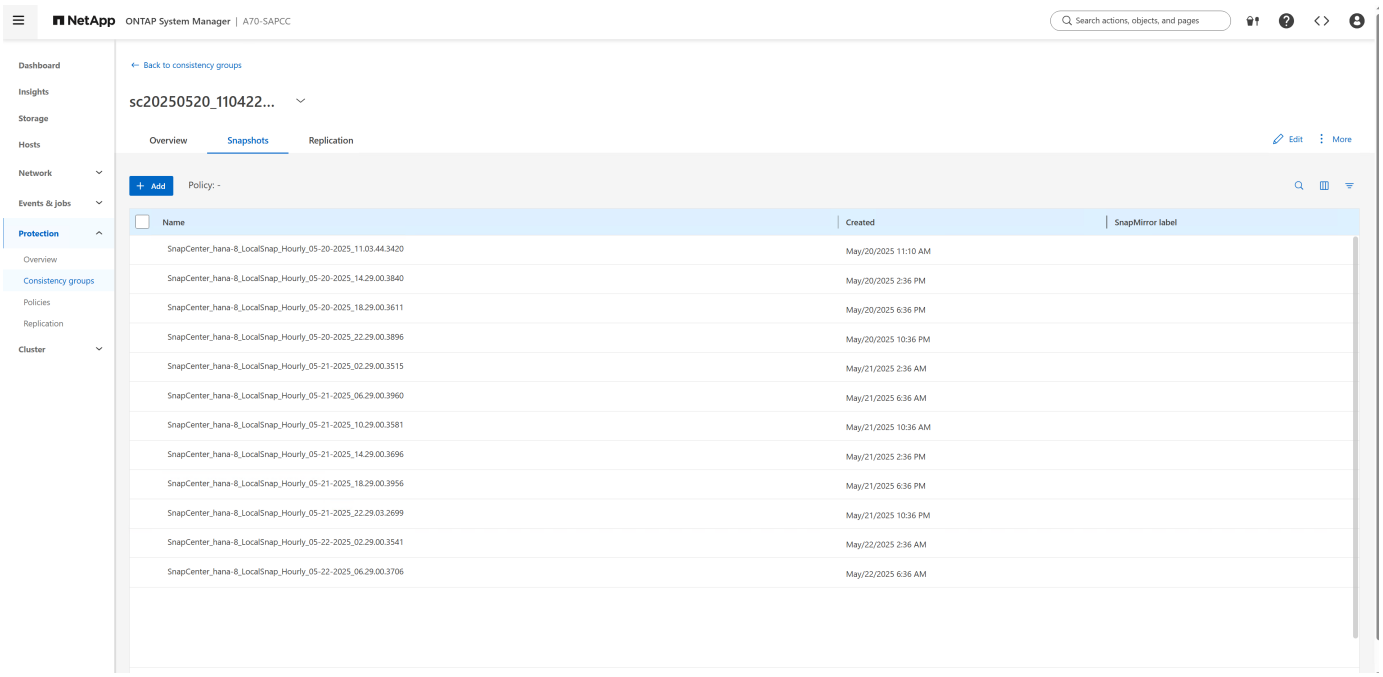

Job Details
Backup of Resource Group 'hana-8_sapcc_stl_ne.....na_MDC_VFS' with policy 'LocalSnap'
Backup of Resource Group 'hana-8_sapcc_stl_netapp_com_hana_MDC_VFS' with policy 'LocalSnap'
hana-8.sapcc.stl.netapp.com
Backup
Validate Dataset Parameters
Validate Plugin Parameters
Complete Application Discovery
Initialize Filesystem Plugin
Discover Filesystem Resources
Discover Virtual Resources
Populate storage details
Validate Retention Settings
Quiesce Application
Quiesce Filesystem
Create Snapshot
UnQuiesce Filesystem
UnQuiesce Application
Get Snapshot Details
Get Filesystem Metadata
Get Virtualization Metadata
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: 05/21/2025 10:29:05 PM End Time: 05/21/2025 10:30:38 PM
View Logs
Cancel Job
Close




SnapCenterはコンシステンシーグループ（CG）を作成し、ストレージユニットhana++data+++VFSをCGに追加します。スナップショットはCGレベルで作成されます。






## リストア処理とリカバリ処理

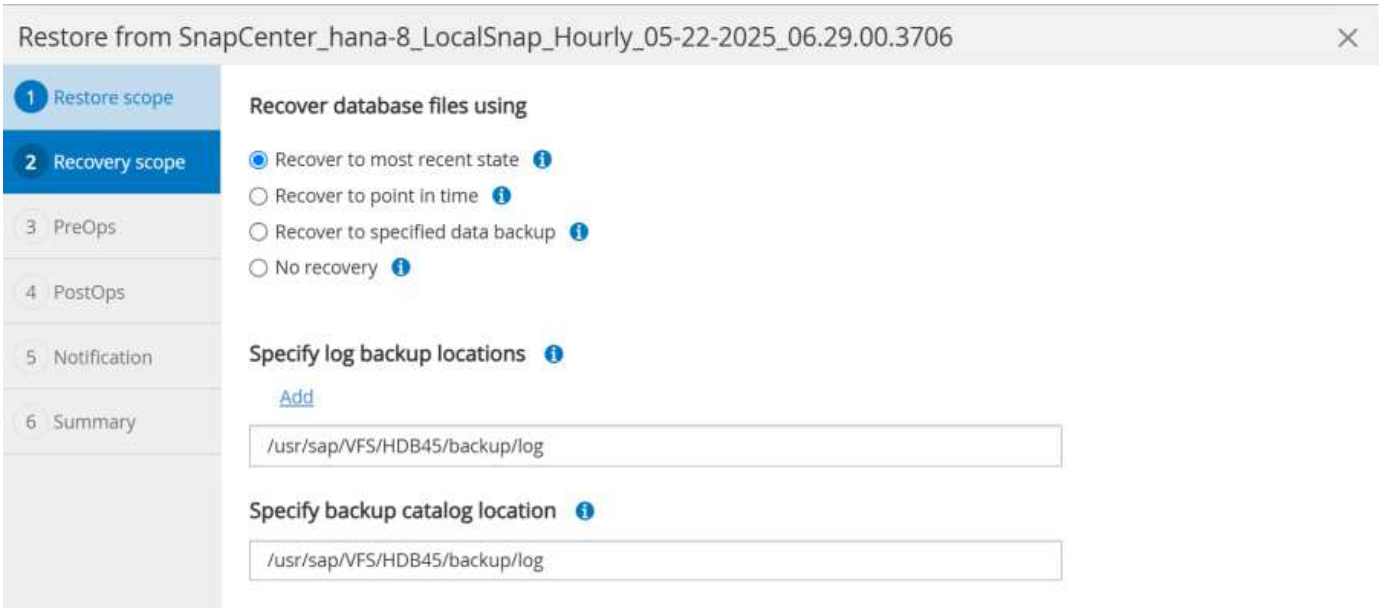
VMFS/VMDK のSnapCenterに保存された仮想リソースの場合、復元操作は常にクローン、マウント、コピー操作によって実行されます。

1. SnapCenterは選択したスナップショットに基づいてストレージクローンを作成します
2. SnapCenterはLUNを新しいデータストアとしてESXホストにマウントします。
3. SnapCenterは、データストア内のVMDKを新しいディスクとしてHANA VMに追加
4. SnapCenterが新しいディスクをLinux OSにマウント
5. SnapCenterは、新しいディスクから元の場所にデータをコピーします。

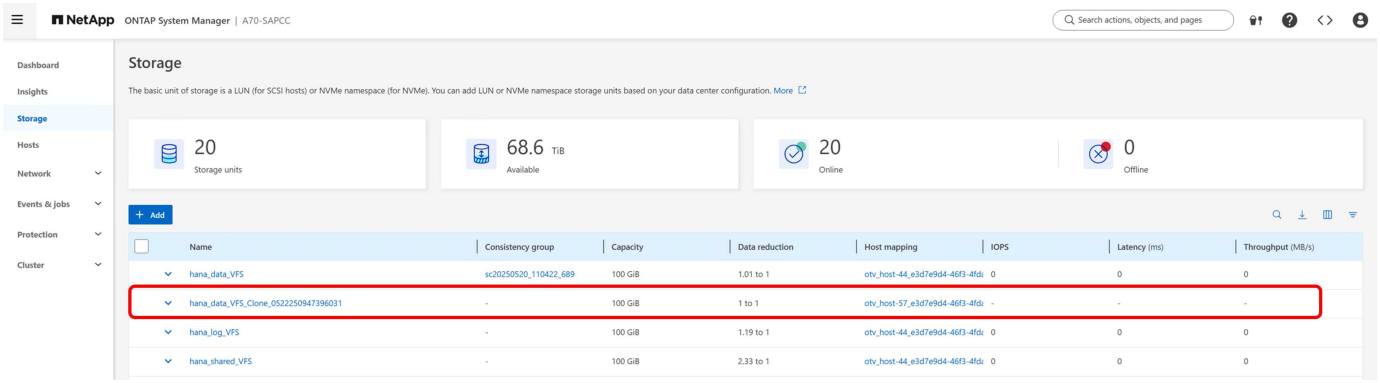
6. コピー操作が終了すると、上記のリソースはすべて再度削除されます。
7. SnapCenterはHANAシステムデータベースのリカバリを実行します
8. SnapCenterはHANAテナントデータベースのリカバリを実行します

リストア操作の全体的な実行時間は、データベースのサイズと、ストレージクラスターとESXホスト間のFC接続のスループットに依存します。当社のラボ環境（初期HANAインストール時）では、実行時間は約12分でした。

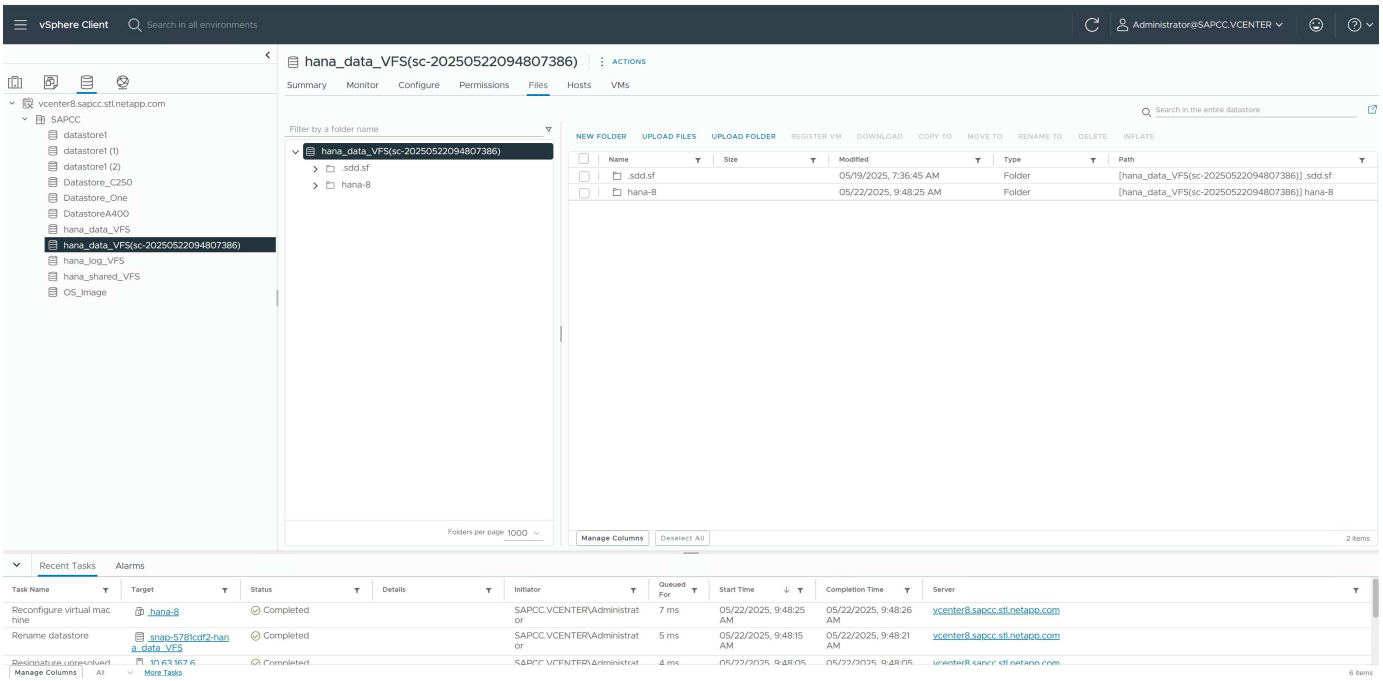



復元およびリカバリ操作の実行中に、新しいクローン ストレージ ユニットが表示されます。




クローン作成されたストレージ ユニットに基づく新しい LUN (データストア) が ESX クラスターに接続されます。

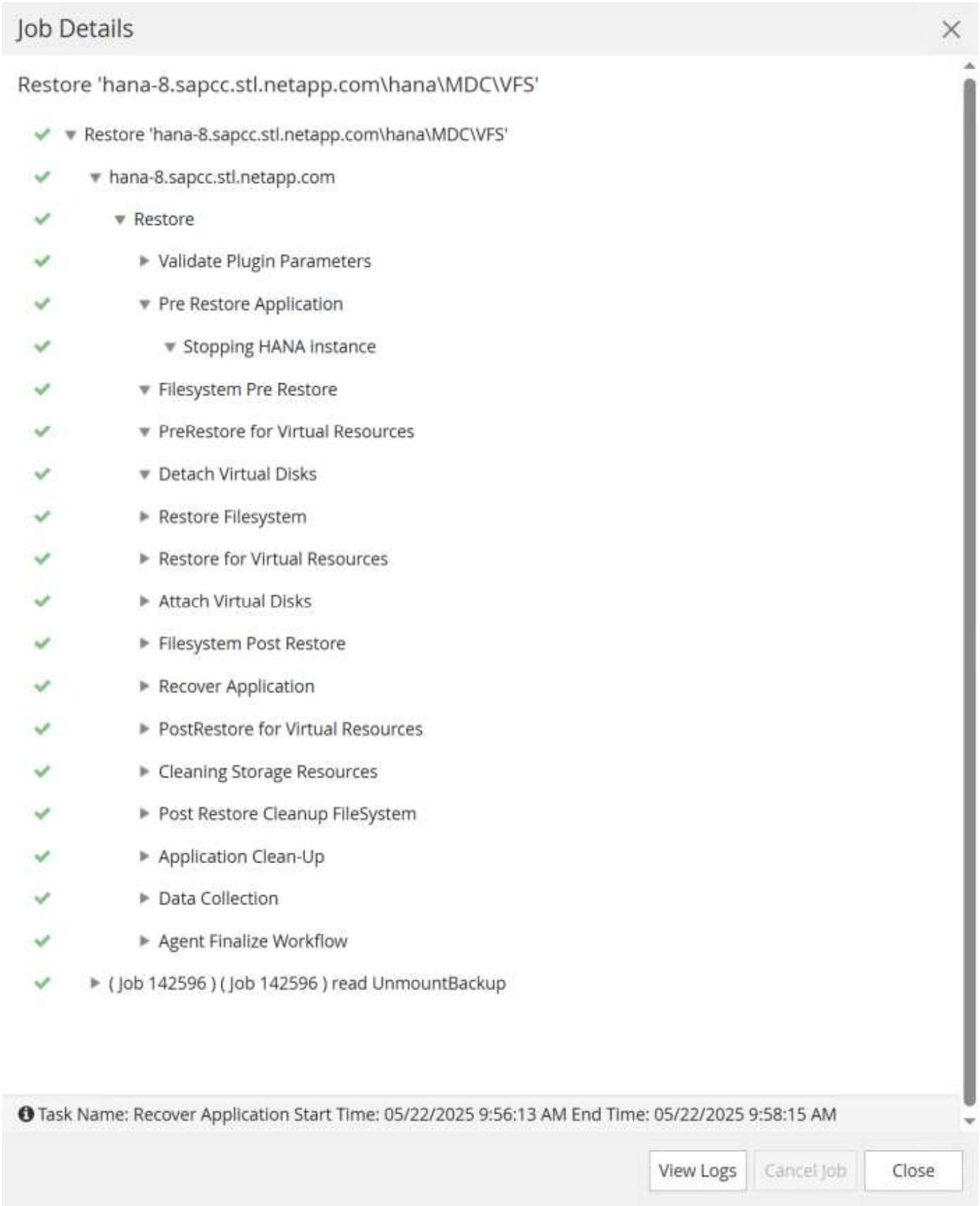



データストア内の VMDK はターゲットの HANA VM にマップされ、HANA システムにマウントされます。

```
hana-8:~ # df -h

Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 5.3G 54G 9% /
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 0 49G 0% /dev/shm
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 26M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysusers.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
/dev/mapper/system-root 60G 5.3G 54G 9% /.snapshots
/dev/mapper/system-root 60G 5.3G 54G 9% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 5.3G 54G 9% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 5.3G 54G 9% /home
/dev/mapper/system-root 60G 5.3G 54G 9% /opt
/dev/mapper/system-root 60G 5.3G 54G 9% /root
/dev/mapper/system-root 60G 5.3G 54G 9% /srv
/dev/mapper/system-root 60G 5.3G 54G 9% /usr/local
/dev/mapper/system-root 60G 5.3G 54G 9% /tmp
/dev/mapper/system-root 60G 5.3G 54G 9% /var
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/sdc 95G 8.9G 87G 10% /hana/log/VFS/mnt00001
/dev/sdb 95G 7.6G 88G 8% /hana/data/VFS/mnt00001
/dev/sdd 95G 15G 81G 16% /hana/shared
/dev/sda1 253M 5.9M 247M 3% /boot/efi
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
192.168.175.86:/sapcc_share 1.4T 858G 568G 61% /mnt/sapcc-share
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
/dev/sde 95G 9.2G 86G 10%
/var/opt/snapcenter/scu/clones/hana_data_VFS_mnt00001_142592_scu_clone_1

hana-8:~ #
```




## SAP システムリフレッシュ

SnapCenterを使用したSAPシステムリフレッシュ操作の詳細については、以下を参照してください。 "TR-4667：『Automating SAP HANA System Copy and Clone Operations with SnapCenter 』" 。

2番目のHANAシステムのQFSは、第1章で説明したのと同じ方法でプロビジョニングされています。 "「HANAシステムのプロビジョニングとインストール」" 。

前提条件

SnapCenterの現在のバージョン (6.1P1) にはいくつかの制限がありますが、次のリリースで修正される予定です。

1. 各「クローン作成」および「クローン削除」ワークフローの後に、ターゲット HANA ホストでコマンド「systemctl restart spl」を使用して spl プロセスを再起動する必要があります。
2. SAP システム更新操作のソースとターゲットとして使用される HANA VM は、同じ ESX ホスト上で実行する必要があります。

ワークフローの概要

最初の SAP システム更新処理を実行する前に、ターゲット HANA システムをインストールし、ホストを SnapCenter に追加する必要があります。次に、HANA システムをシャットダウンし、HANA データ ディスクをホストからアンマウントする必要があります。

**SnapCenter** クローン作成ワークフロー

1. ストレージクローンを作成
2. ストレージクローンのホストマッピングを設定します
3. ストレージクローン(データストア)をESXホストに接続します
4. データストアからターゲットHANA VMに新しいディスクを追加する
5. HANA VM OS へのディスクのマウント
6. 事後スクリプトを使用したHANAシステムの回復

上映時間:12分

リストア処理と比較すると、クローン処理の実行時間は HANA データベースのサイズに依存しません。ステップ 1 から 5 の実行時間は、非常に大規模なデータベースでも同様です。もちろん、大規模なHANAシステムでは回復に時間がかかります。

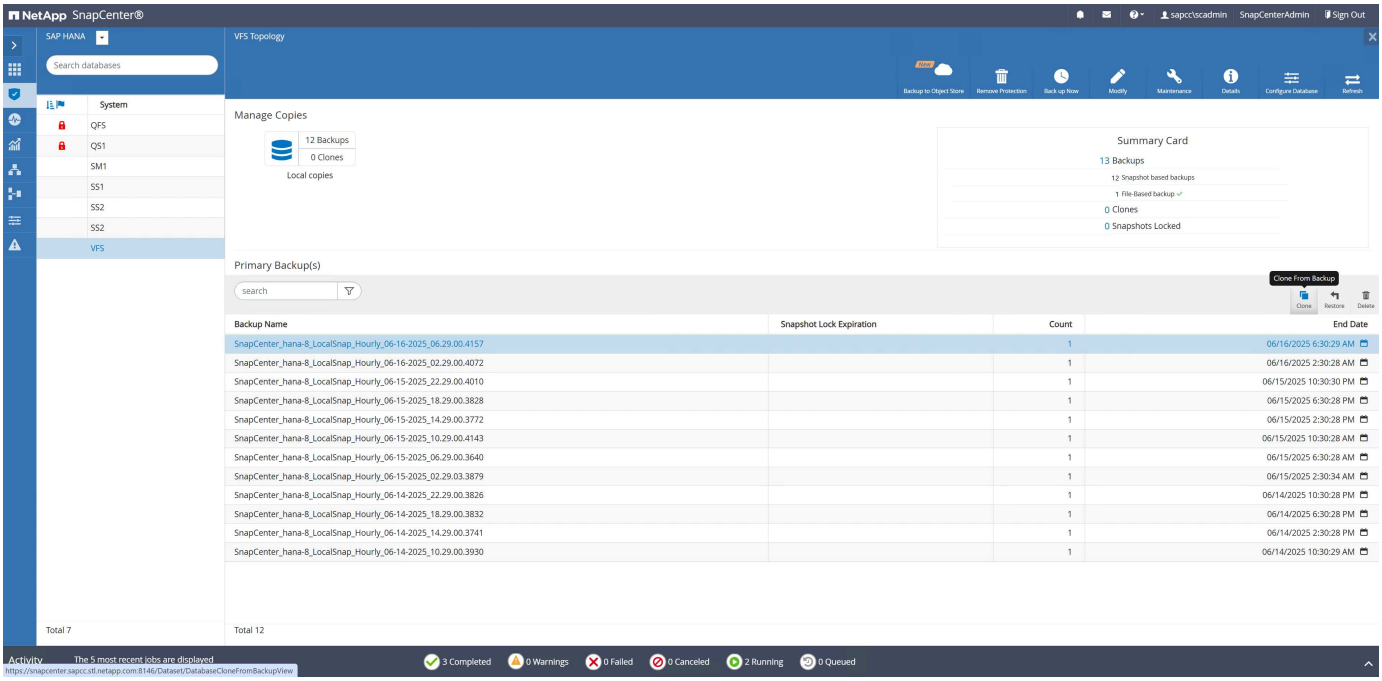
**SnapCenter** クローン削除ワークフロー

1. 事前スクリプトを使用したHANAシステムのシャットダウン
2. HANA VM OS からディスクをアンマウントする
3. HANA VM からディスクを削除する
4. ESX ホストからデータストアを削除する
5. ストレージクローンの削除

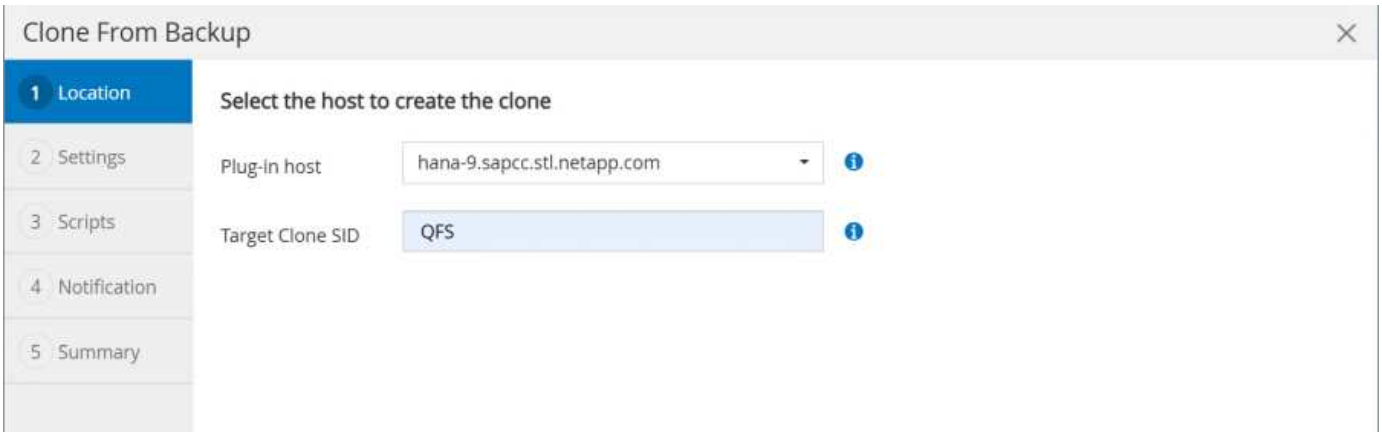
上映時間:11分

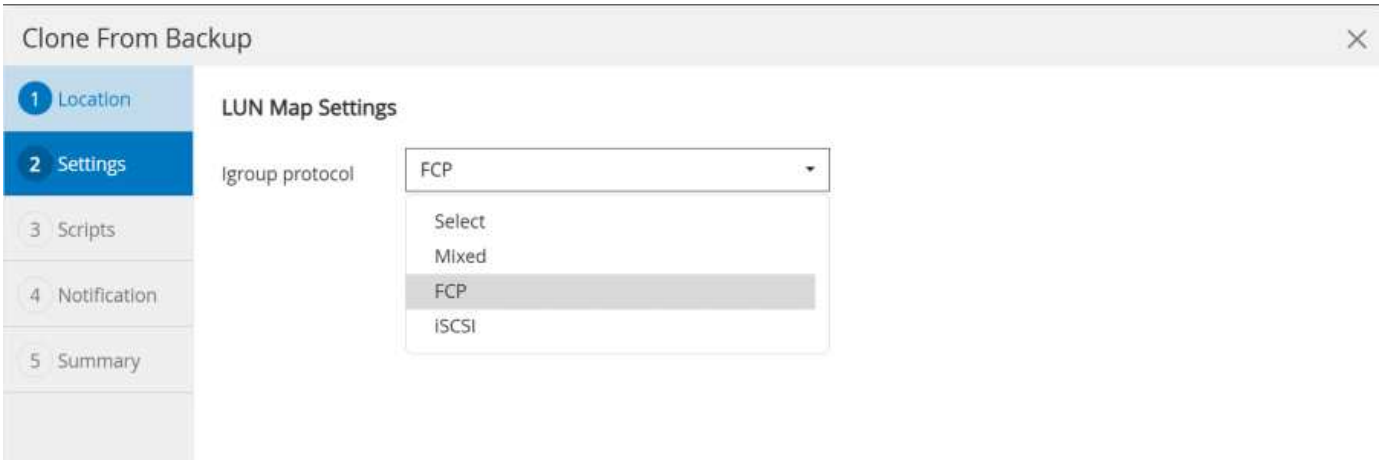
**SnapCenter** クローン作成ワークフロー

クローン作成ワークフローは、目的のスナップショットを選択し、クローン・ボタンをクリックすると開始されます。

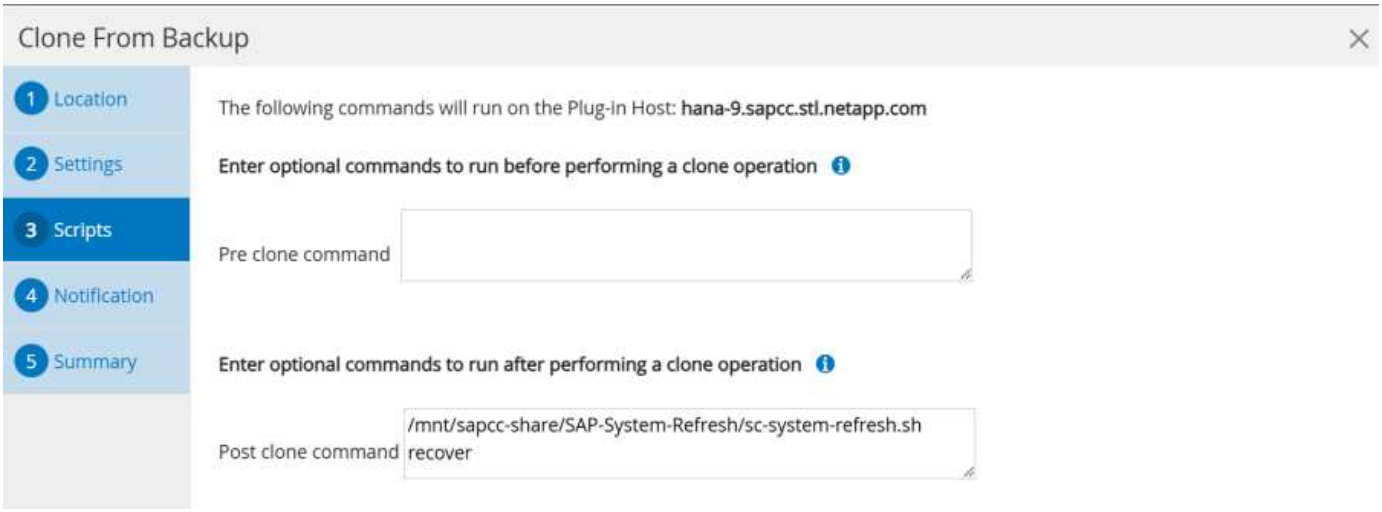



ターゲット ホストと SID を指定する必要があります。

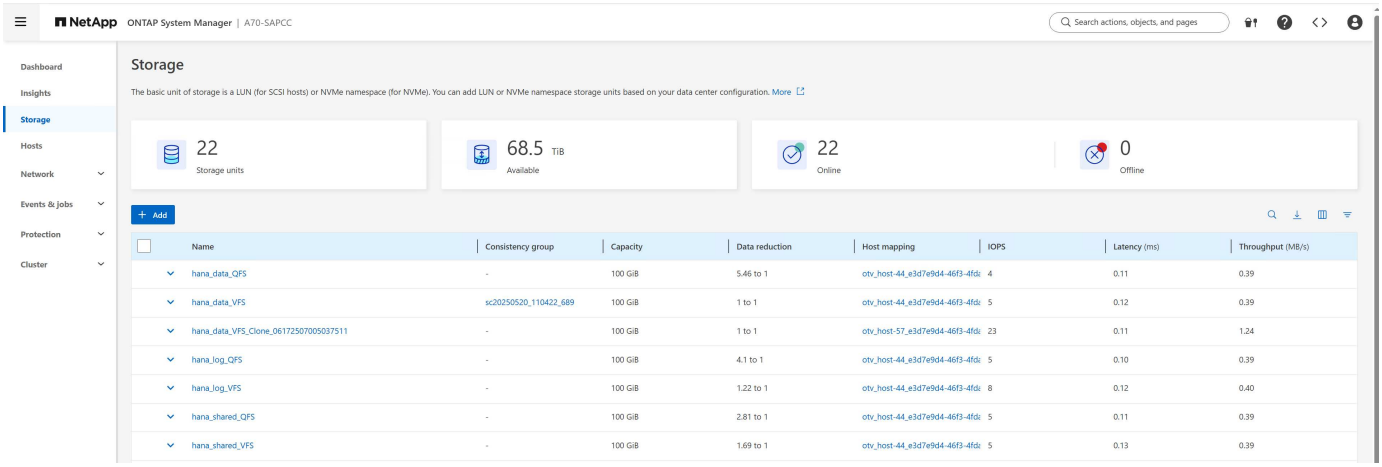


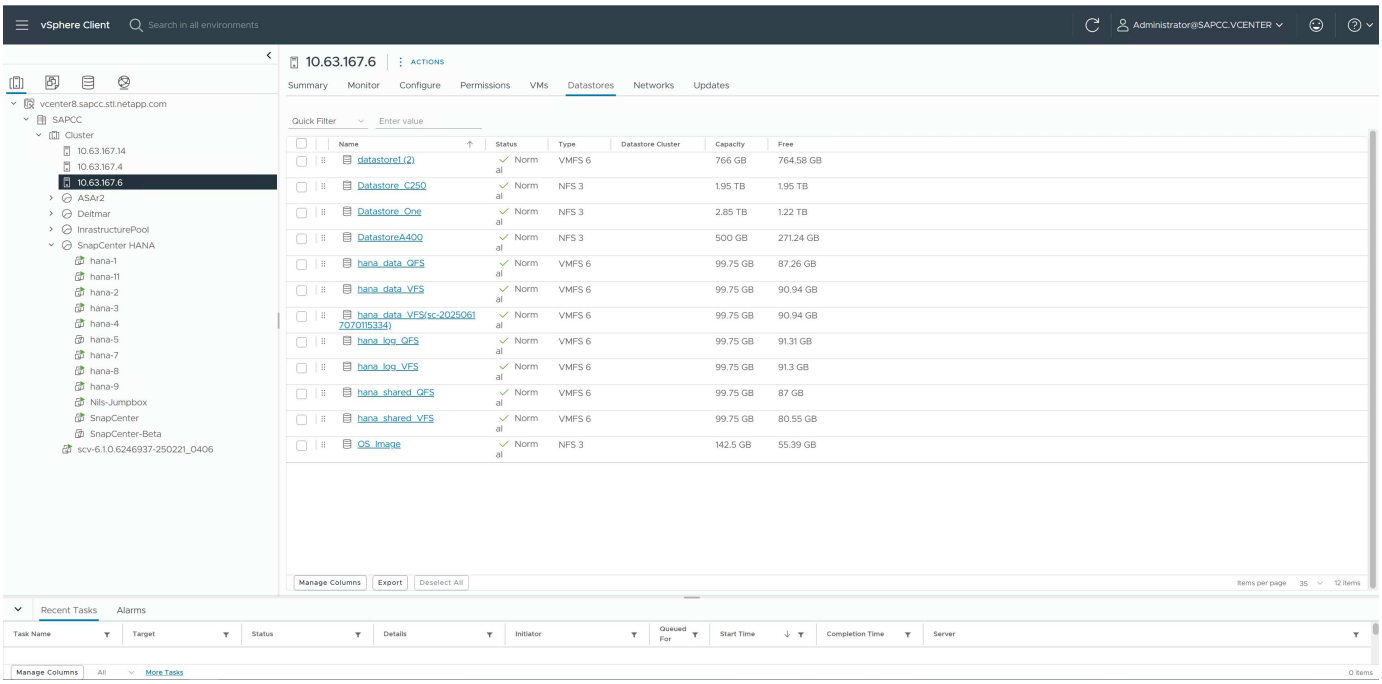
この例では、ポストスクリプトを使用して、ターゲットホストでリカバリを実行しています。



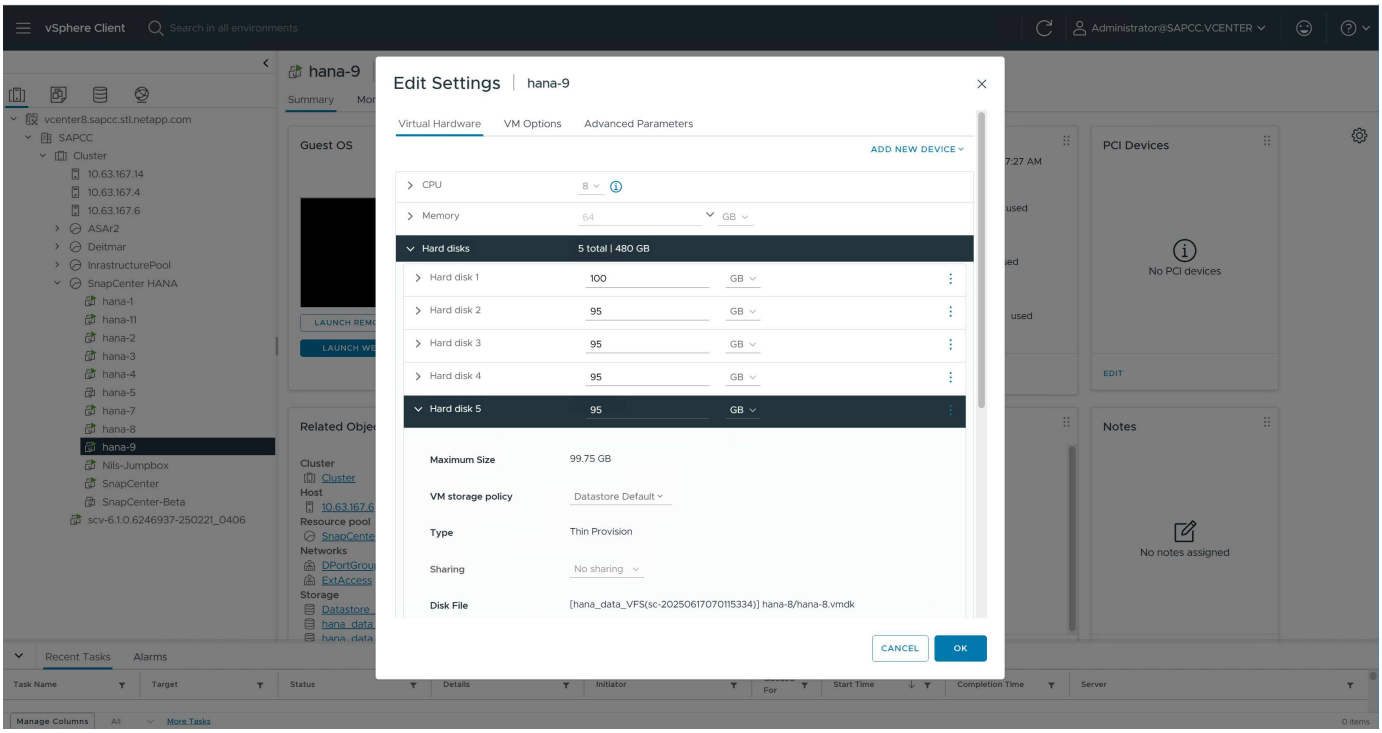

ワークフローが開始されると、 SnapCenter は選択した Snapshot に基づいてクローニングされたストレージユニットを作成します。




その後、 SnapCenter は、ターゲット HANA VM が実行されている ESX ホストに LUN (データストア)を接続します。




その後、新しいデータストア内の VMDK が HANA VM に追加されます。




その後、 SnapCenter は新しいディスクを HANA Linux システムに設定してマウントします。

```
hana-9:/mnt/sapcc-share/SAP-System-Refresh # df -h

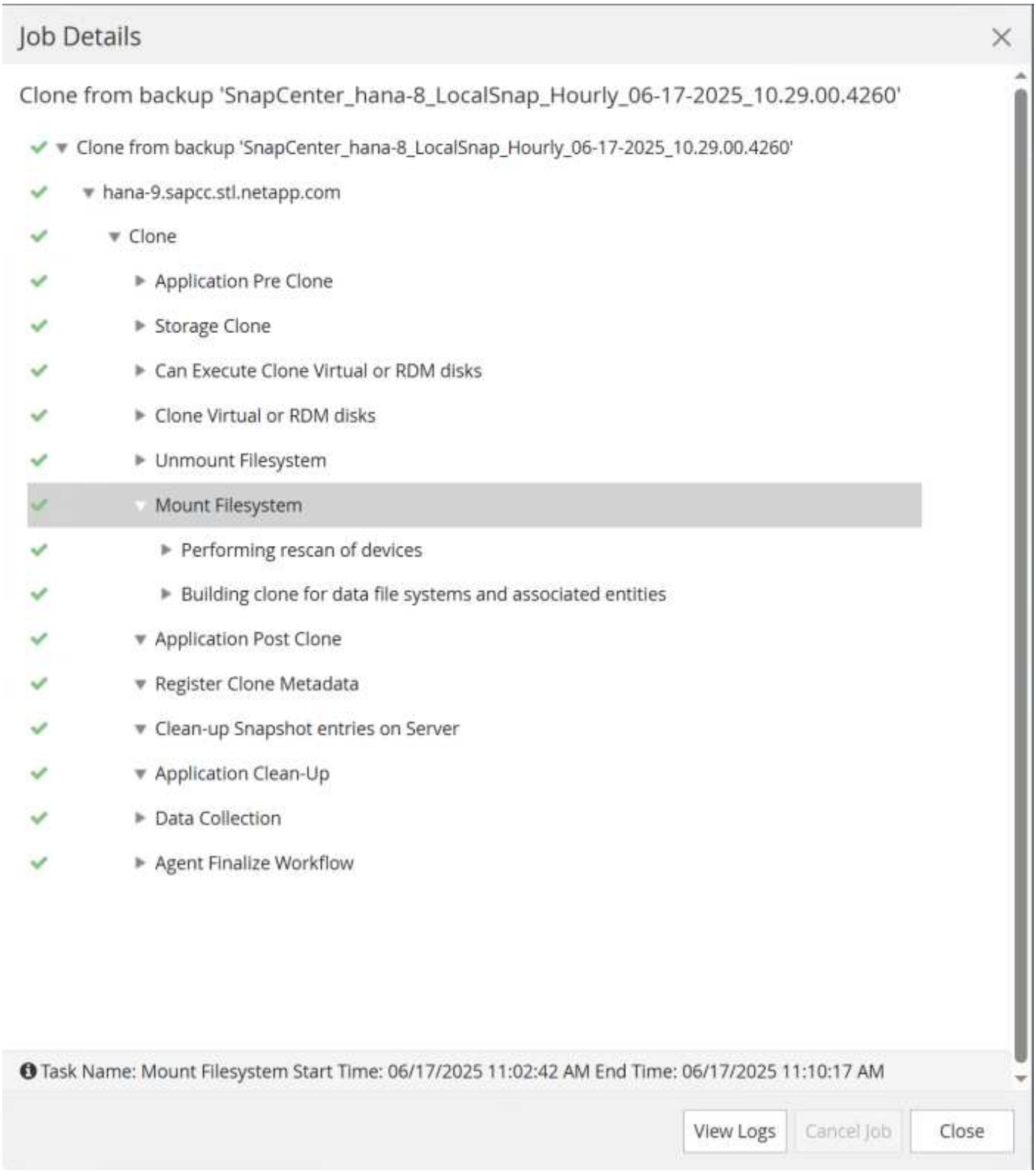
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 5.2G 52G 10% /
devtmpfs 4.0M 4.0K 4.0M 1% /dev
tmpfs 49G 0 49G 0% /dev/shm
```

```
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 26M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysusers.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
/dev/mapper/system-root 60G 5.2G 52G 10% /.snapshots
/dev/mapper/system-root 60G 5.2G 52G 10% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 5.2G 52G 10% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 5.2G 52G 10% /home
/dev/mapper/system-root 60G 5.2G 52G 10% /opt
/dev/mapper/system-root 60G 5.2G 52G 10% /srv
/dev/mapper/system-root 60G 5.2G 52G 10% /root
/dev/mapper/system-root 60G 5.2G 52G 10% /tmp
/dev/mapper/system-root 60G 5.2G 52G 10% /usr/local
/dev/mapper/system-root 60G 5.2G 52G 10% /var
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/sdc 95G 8.9G 87G 10% /hana/log/QFS/mnt00001
/dev/sdd 95G 14G 82G 14% /hana/shared
/dev/sda1 253M 5.9M 247M 3% /boot/efi
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
192.168.175.86:/sapcc++_++share 1.4T 858G 568G 61% /mnt/sapcc-share
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
/dev/sde 95G 9.2G 86G 10% /hana/data/QFS/mnt00001
tmpfs 6.3G 56K 6.3G 1% /run/user/1001
hana-9:/mnt/sapcc-share/SAP-System-Refresh #

hana-9:/mnt/sapcc-share/SAP-System-Refresh # cat /etc/fstab
/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=/@/var 0 0
/dev/system/root /usr/local btrfs subvol=/@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=/@/tmp 0 0
/dev/system/root /srv btrfs subvol=/@/srv 0 0
/dev/system/root /root btrfs subvol=/@/root 0 0
/dev/system/root /opt btrfs subvol=/@/opt 0 0
/dev/system/root /home btrfs subvol=/@/home 0 0
/dev/system/root /boot/grub2/x86++_++64-efi btrfs
subvol=/@/boot/grub2/x86++_++64-efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=/@/.snapshots 0 0
UUID=FB79-24DC /boot/efi vfat utf8 0 2
```

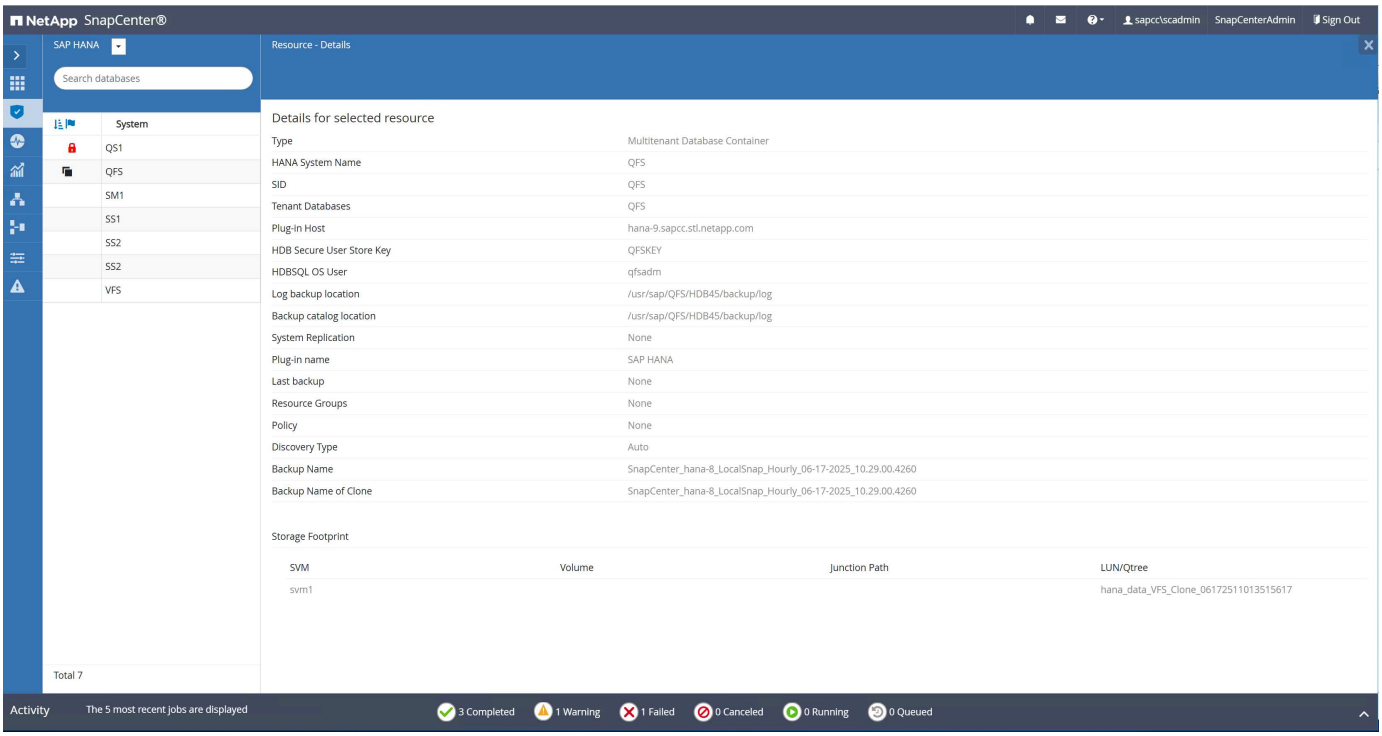
```
192.168.175.86:/sapcc++_++share /mnt/sapcc-share nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
#/dev/sdb /hana/data/QFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/QFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
# The following entry has been added by NetApp (SnapCenter Plug-in for
UNIX)
/dev/sde /hana/data/QFS/mnt00001 xfs
rw,relatime,attr2,inode64,logbufs=8,logbsize=32k,noquota 0 0
hana-9:/mnt/sapcc-share/SAP-System-Refresh #
```

次のスクリーンショットは、 SnapCenter によって実行されるジョブステップを示しています。



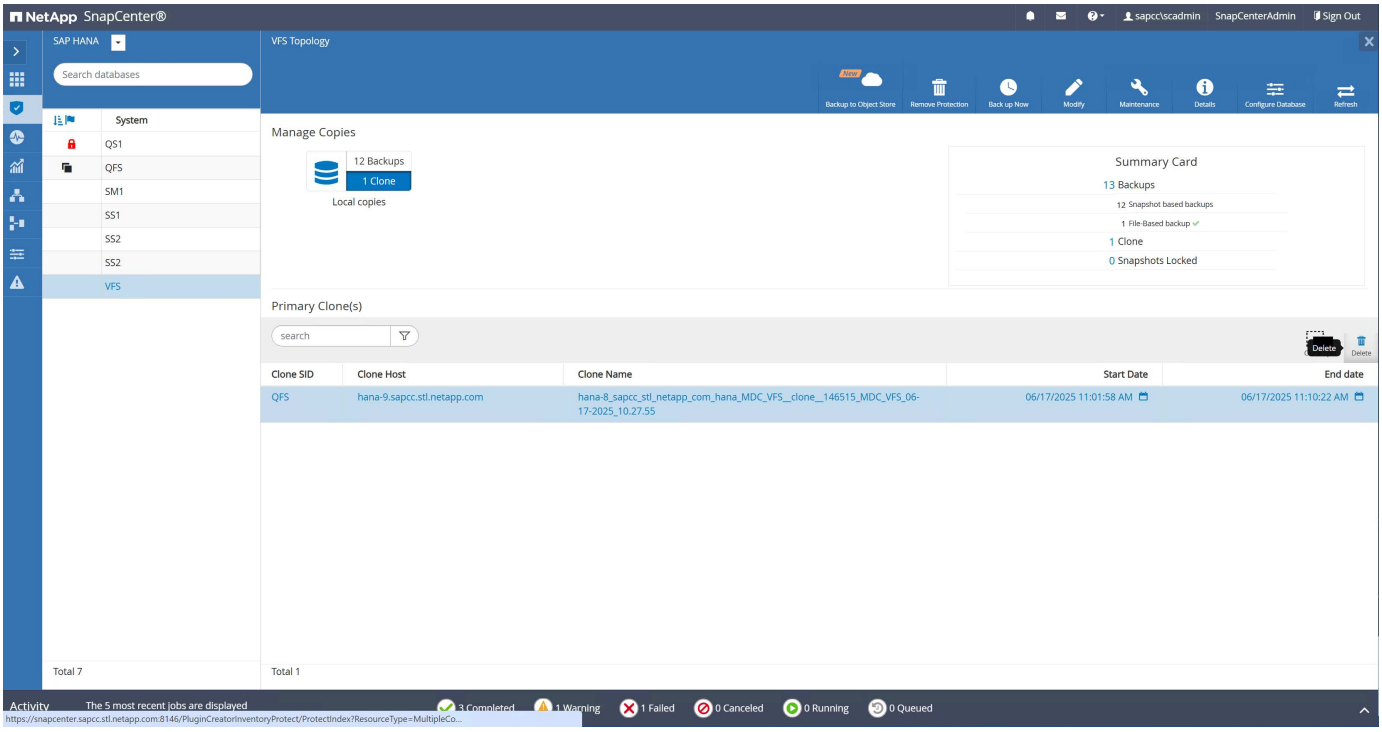

で説明したように "前提条件" セクションでは、適切なクリーンアップを開始するには、 HANA ホストの SnapCenter spl サービスを「 systemctl restart spl 」コマンドを使用して再起動する必要があります。これは、ジョブが終了したときに行う必要があります。

クローンワークフローが完了したら、リソース QFS をクリックして自動検出を開始できます。自動検出プロセスが完了すると、新しいストレージフットプリントがリソースの詳細ビューに一覧表示されます。

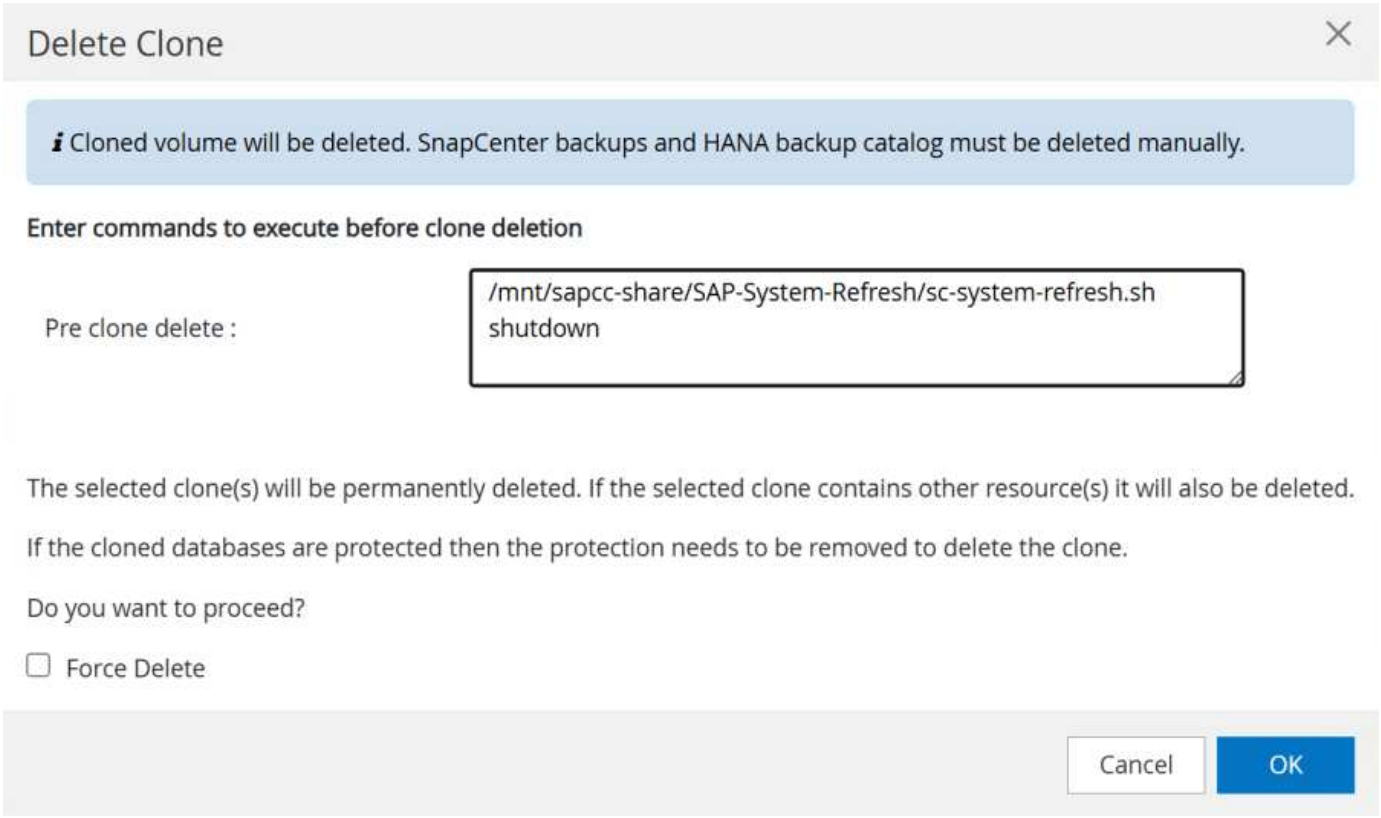



**SnapCenter** クローン削除ワークフロー

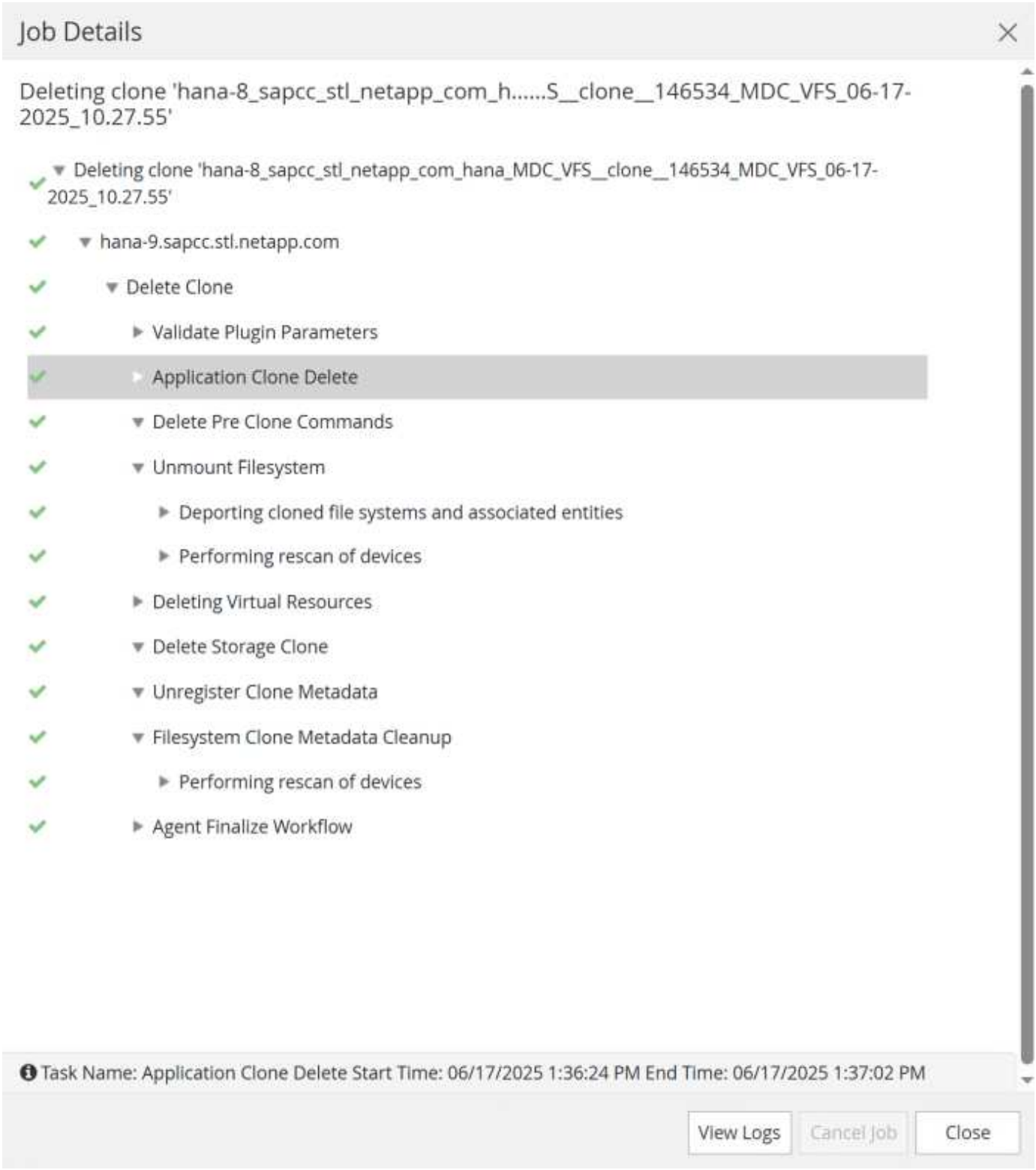
クローン削除ワークフローは、ソース HANA リソースでクローンを選択し、削除ボタンをクリックして開始します。




この例では、事前スクリプトを使用してターゲットHANAデータベースをシャットダウンしています。




次のスクリーンショットは、 SnapCenter によって実行されるジョブステップを示しています。




で説明したように "前提条件" セクションでは、適切なクリーンアップを開始するには、 HANA ホストの SnapCenter spl サービスを「 systemctl restart spl 」コマンドを使用して再起動する必要があります。

## 追加情報とバージョン履歴

HANA のベストプラクティス:

- "『 SAP HANA on NetApp ASA Systems with Fibre Channel Protocol 』を参照してください"です。

SnapCenter ：

- "TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"
- "TR-4719 ：『 SAP HANA System Replication - Backup and Recovery with SnapCenter 』"
- "TR-4667：『Automating SAP HANA System Copy and Clone Operations with SnapCenter 』"
- "SnapCenter SnapMirror Active Sync と VMware Metro Storage Cluster による SAP HANA のデータ保護と高可用性"
- "SnapCenter ソフトウェアのドキュメント"

バージョン履歴：

| バージョン | 日付 | コメント |
| --- | --- | --- |
| バージョン 1.0 以降 | 07/2025 | 初版 |

# BlueXP Backup and Recovery for SAP HANA -バックアップ先としてのクラウドオブジェクトストレージ

## BlueXP Backup and Recovery for SAP HANA -バックアップ先としてのクラウドオブジェクトストレージ

このテクニカルレポートでは、NetApp BlueXP Backup NAD Recovery for Applicationを使用したSAP HANAのデータ保護のベストプラクティスを紹介します。このドキュメントでは、概念、構成に関する推奨事項、処理のワークフロー（設定、バックアップ処理など）について説明します。 およびリストア処理

概要

このドキュメントでは、NetApp BlueXPを使用してオンプレミスからクラウドベースのオブジェクトストアへのデータ保護のためにSAP HANAをセットアップおよび設定する方法について説明します。このコースでは、解決策のBlueXPのバックアップとリカバリについて説明します。この解決策は、NetApp Snap Centerを使用してオンプレミスのSAP HANAバックアップ解決策を強化したもので、コスト効率に優れた方法でSAP HANAバックアップをクラウドベースのオブジェクトストレージに長期アーカイブできます。また、オブジェクトストレージをAWS Glacier/Deep Glacierなどのアーカイブストレージに階層化するオプションも用意されています。 Microsoft Azure Blob Archive、GCP Archive Storageの略。

オンプレミスのSAP HANAバックアップ/リカバリソリューションのセットアップと構成については、を"TR-4614：『SAP HANA backup and recovery with SnapCenter』（netapp.com）"参照してください。

このテクニカルレポートでは、AWS S3オブジェクトストレージを使用したBlueXPのSAP HANA向けバックアップ/リカバリ機能を使用して、オンプレミスのSnapCenterベースのSAP HANAバックアップ/リカバリ解決策を強化する方法のみを説明します。AWS S3ではなくMicrosoft AzureとGCPオブジェクトストレージを使用したセットアップと設定は似ていますが、本ドキュメントでは説明しません。

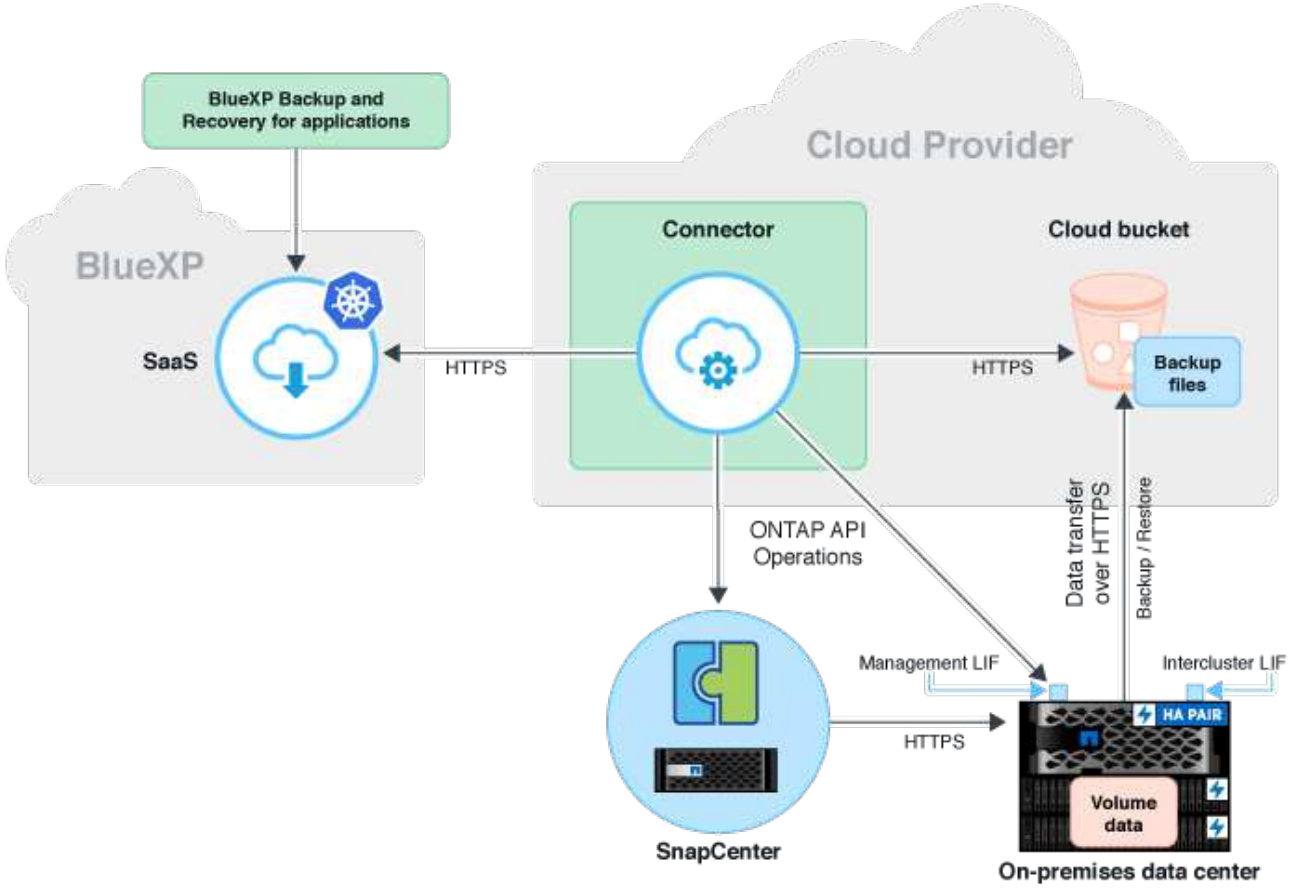
**BlueXP**のバックアップとリカバリのアーキテクチャ

BlueXPのバックアップとリカバリは、NetAppオンプレミスストレージで実行されるアプリケーションにクラウドでデータ保護機能を提供するSaaS解決策です。NetAppストレージを使用して、アプリケーションと整合性のある効率的なポリシーベースのSAP HANA保護を実現します。さらに、BlueXPのバックアップとリカバリ機能では、一元的な管理と監視が可能になると同時に、アプリケーション固有のバックアップとリストア処理の管理もユーザに委譲できます。

BlueXPのバックアップとリカバリは、NetApp BlueXP内でSaaSとして実行され、フレームワークとUIを活用します。BlueXP作業環境フレームワークを使用して、NetApp ONTAPベースのオンプレミスストレージとNetApp SnapCenterサーバのクレデンシャルを設定、管理します。

BlueXP Connectorは、お客様の仮想ネットワーク内に導入する必要があります。サイト間VPN接続など、オンプレミス環境とクラウド環境を接続する必要があります。NetApp SaaSコンポーネントとお客様の環境の間の通信は、コネクタを介してのみ行われます。コネクタは、ONTAPおよびSnapCenter管理APIを使用してストレージ処理を実行しています。

オンプレミスストレージとクラウドバケット間のデータ転送は、保存中のAES 256ビット暗号化、転送中のTLS / HTTPS暗号化、顧客管理キー（CMK）のサポートによってエンドツーエンドで保護されます。[+]バックアップされたデータは、書き換えや削除が不可能なWORM状態で保存できます。オブジェクトストレージからデータにアクセスする唯一の方法は、NetApp CVOを含むNetApp ONTAPベースのストレージにデータをリストアすることです。



インストールと設定の手順の概要

必要なインストールと設定の手順は、3つの領域に分けることができます。+ NetApp Snap CenterでSAP HANAのバックアップ構成が設定されていることを前提条件としています。Snap Center for SAP HANAの最初のセットアップについては、を参照してください"SnapCenterの設定（netapp.com）"。

1. NetApp BlueXPコンポーネントのインストールと設定

   データ保護解決策の初期セットアップ時に1回実行する必要があります。

2. NetApp SnapCenterでの準備手順

   保護が必要なSAP HANAデータベースごとに実行する必要があります。

3. BlueXPのバックアップとリカバリの設定手順

   保護が必要なSAP HANAデータベースごとに実行する必要があります。

#### NetApp BlueXPハイブリッドアプリケーションバックアップのインストールと設定

NetApp BlueXPのコンポーネントのインストールと設定については、を参照してください "オンプレミスアプリケーションデータの保護| NetAppドキュメント"。

1. BlueXPにサインアップし、次のURLでNetAppアカウントを設定してください：https://bluexp.netapp.com/。
2. BlueXP Connectorを環境に導入します。概要は、 "コネクタの詳細| NetAppのドキュメント"。
3. BlueXPでCloud Backupライセンスを追加/購入： https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-licensing-cloud-backup.html。
4. オンプレミスストレージを追加して、BlueXPでNetAppオンプレミス環境とクラウドデスティネーションの作業環境を作成します。
5. オンプレミスストレージの新しいオブジェクトストア関係をAWS S3バケットに作成します。
6. SnapCenterでSAP HANAシステムリソースを設定します。
7. 作業環境にSnap Centerを追加します。
8. 環境に応じたポリシーを作成します。
9. SAP HANAシステムを保護

## BlueXP Backup and Recovery for SAP HANAの設定

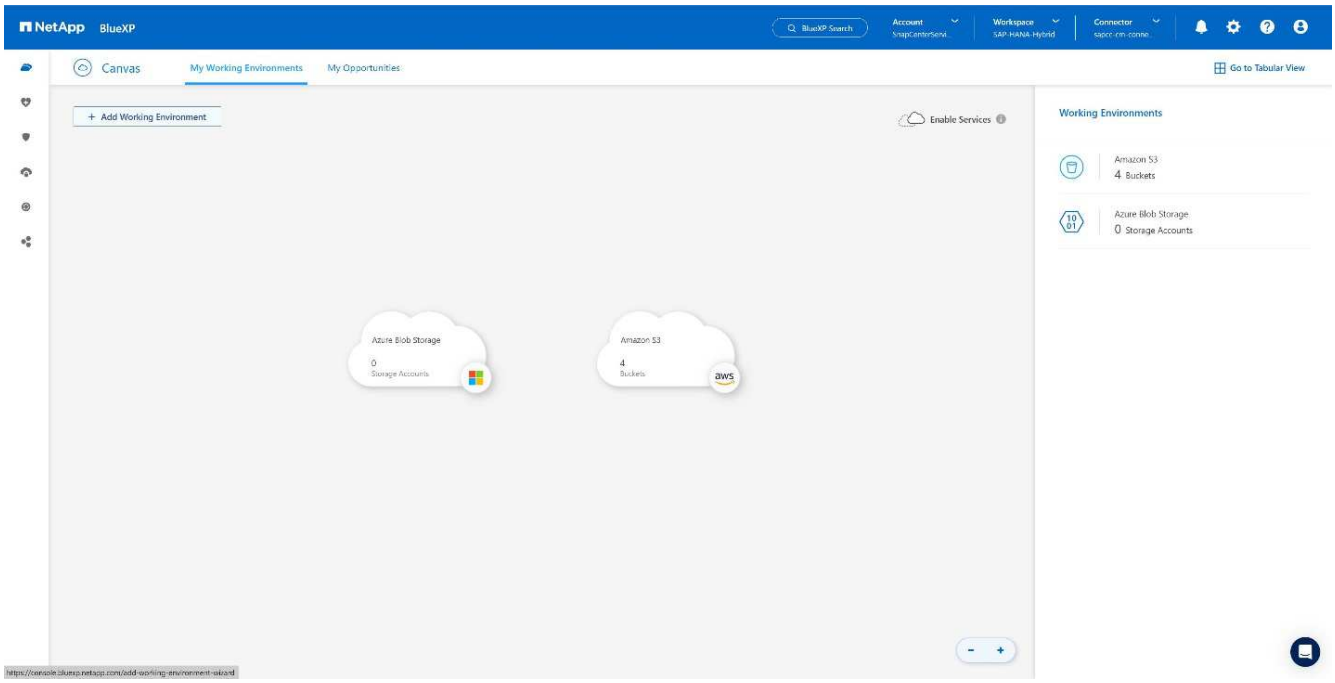
このセクションでは、作業環境のセットアップ方法、SnapCenterの設定方法、およびBlueXPでSAP HANAバックアップを設定してアクティブ化する方法について説明します。

#### BlueXPの作業環境の作成

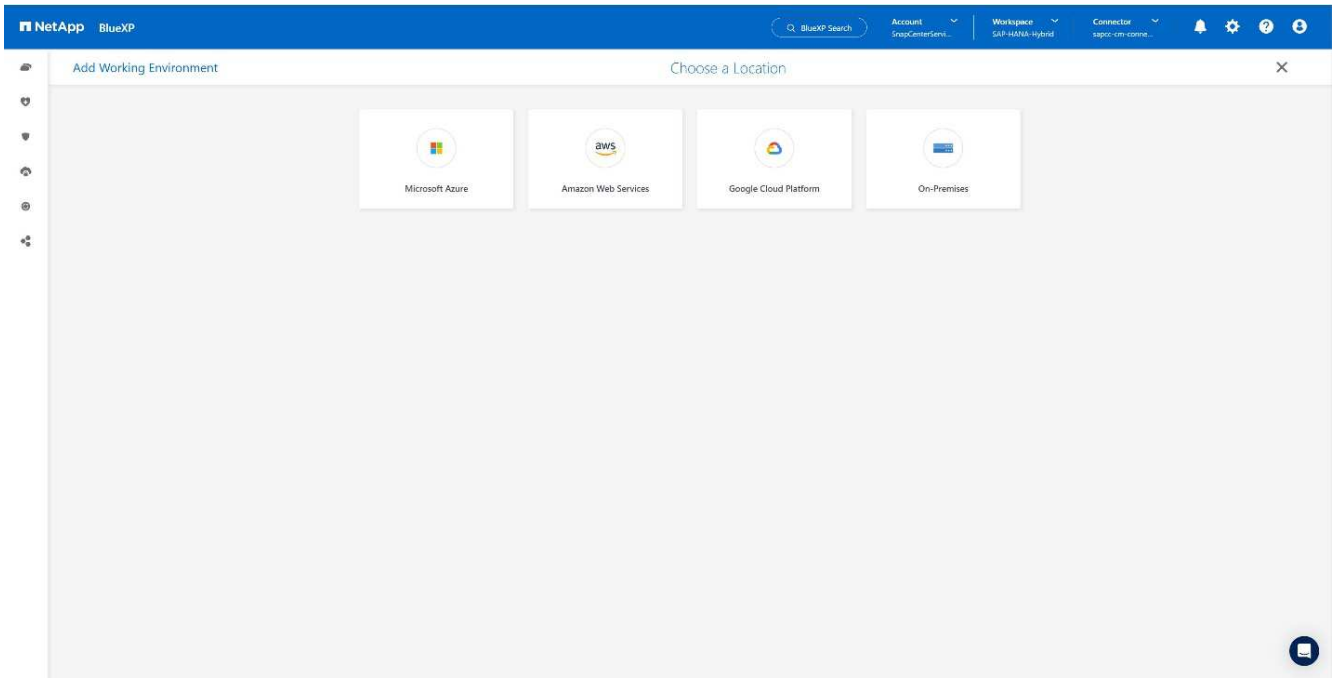
社内ストレージシステムを作業環境に追加します。

1. 左側のメニューで、**[ストレージ]>*>**[マイ作業環境]を選択します。

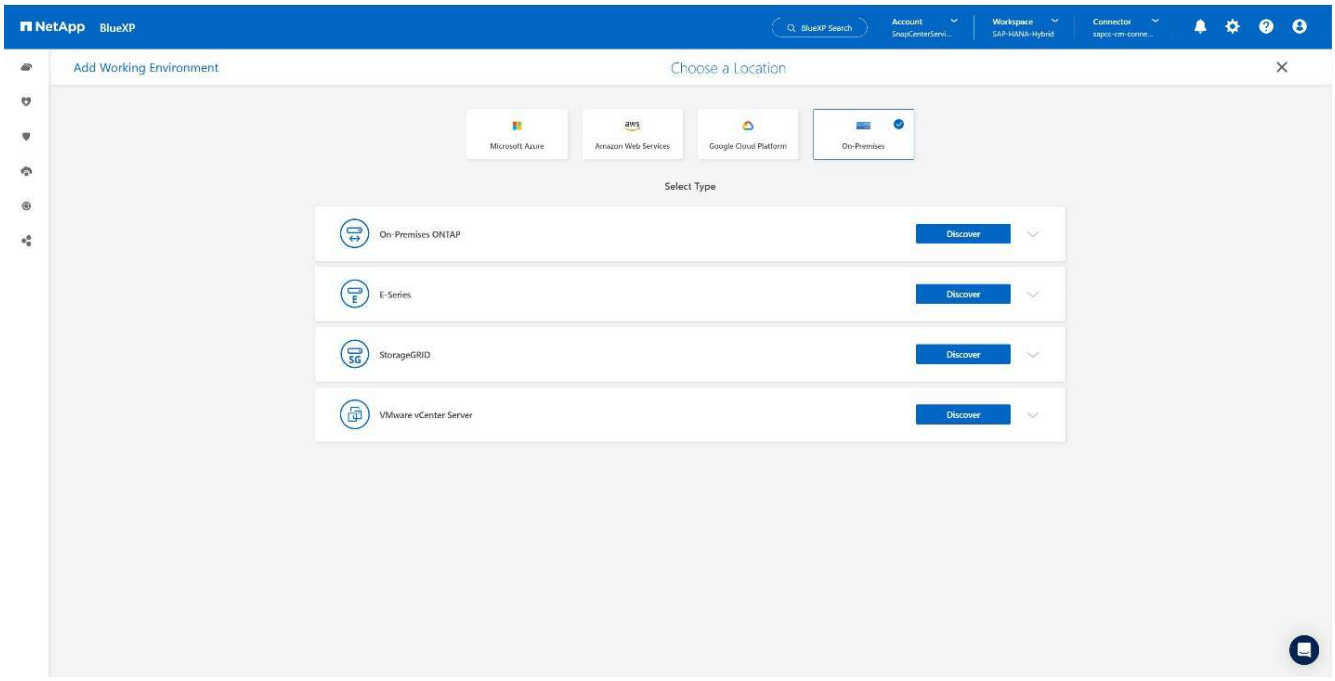
2. +作業環境の追加*を押します。
+



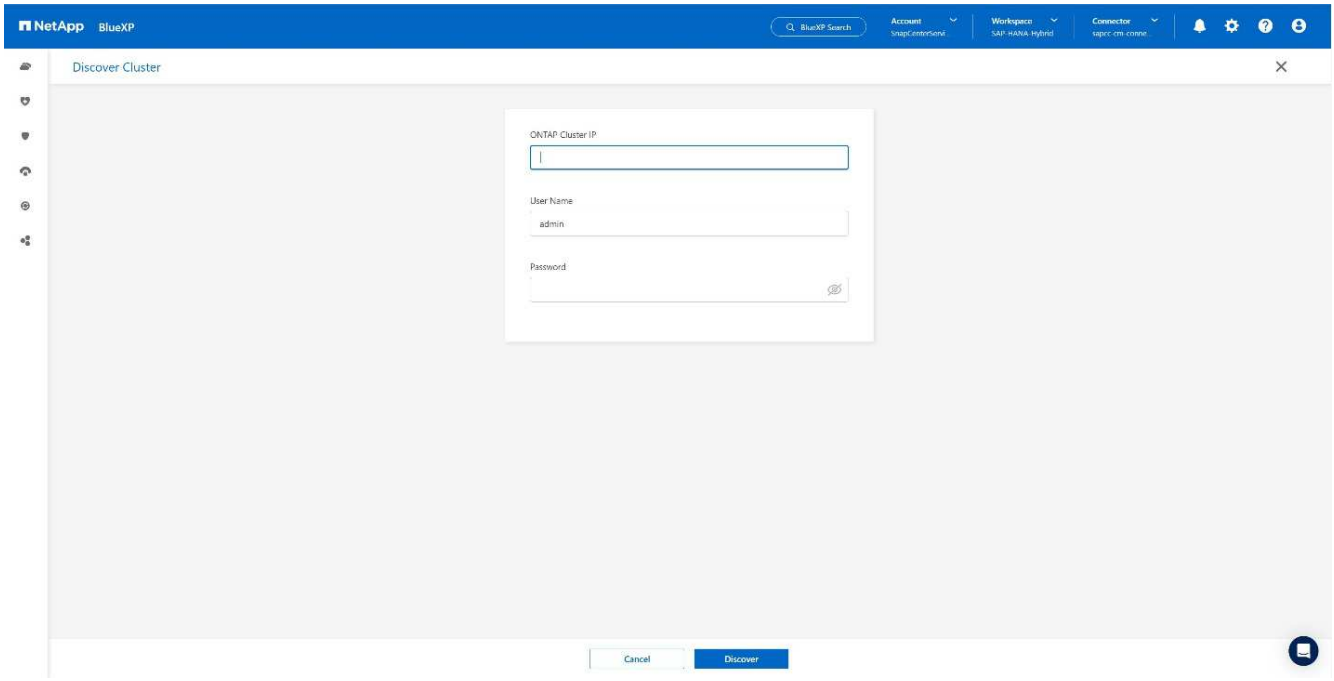

3. [オンプレミス]を選択します。
+



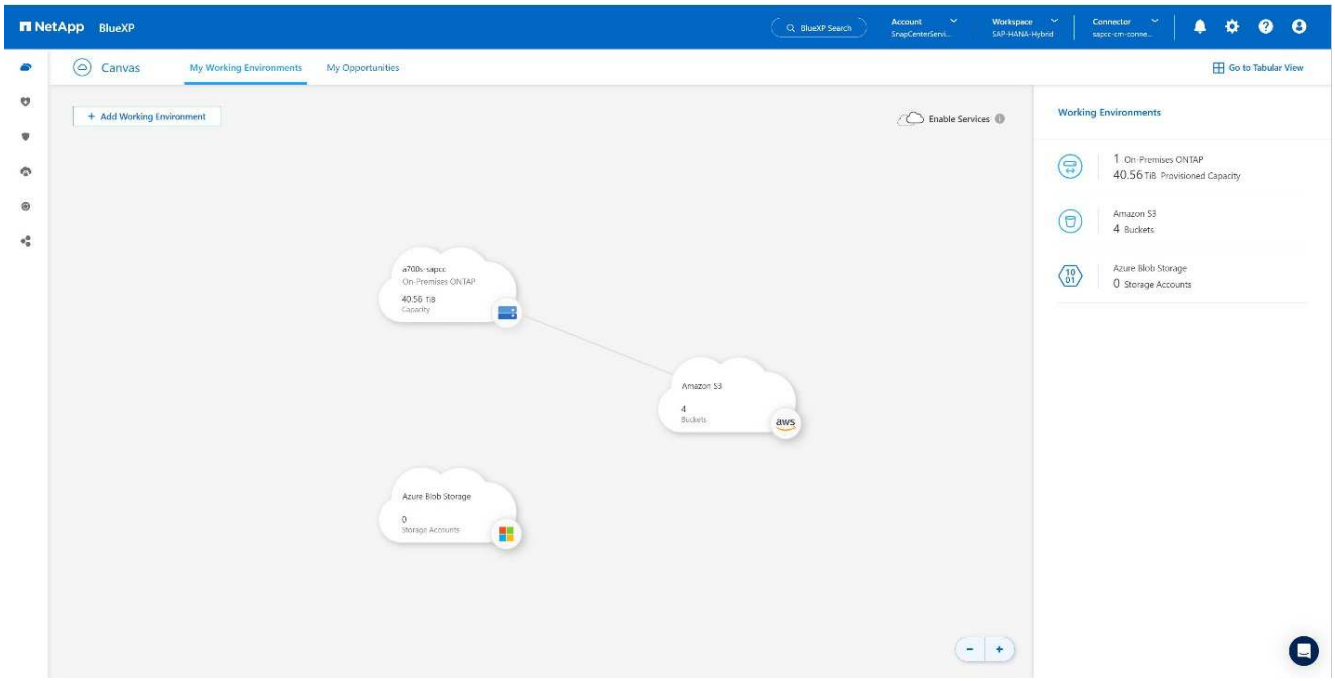

4. [オンプレミスのONTAPを検出]*を選択します。
+




5. ONTAPクラスタのIPアドレスとパスワードを追加し、*[検出]*を押します。
+




6. これでONTAPクラスタが使用可能になります。
+

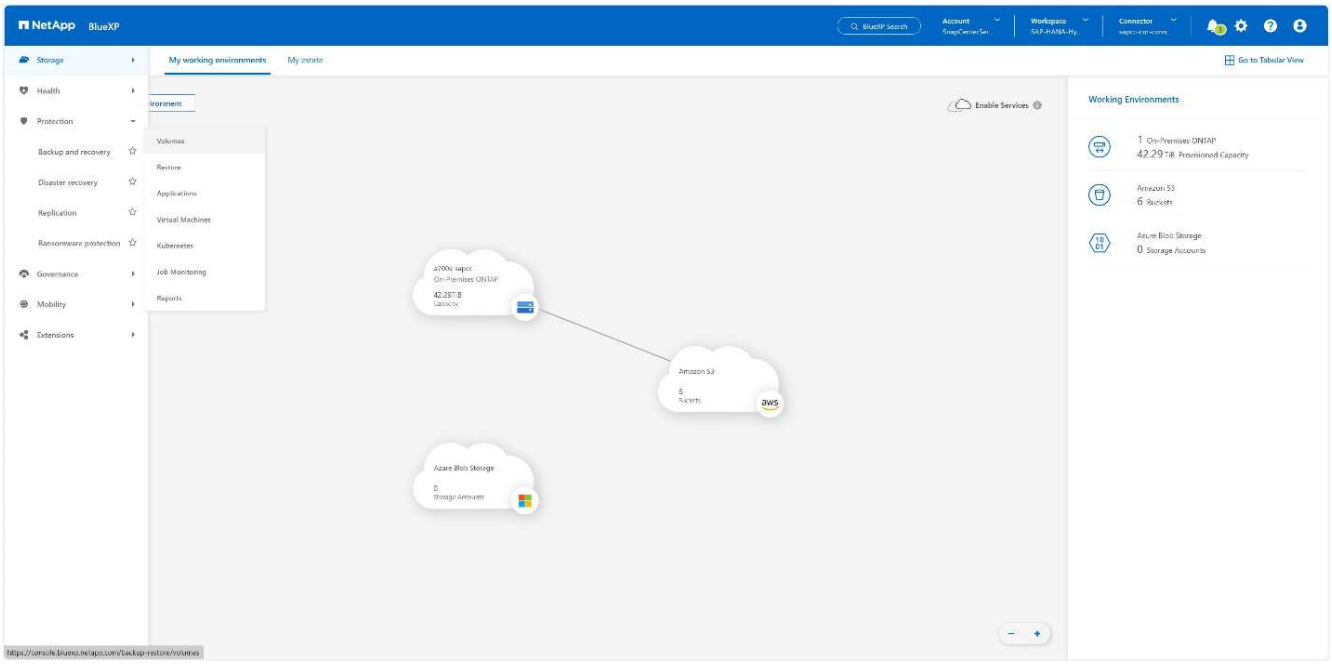



オンプレミスのストレージシステムとオブジェクトストレージバケット間の関係を作成

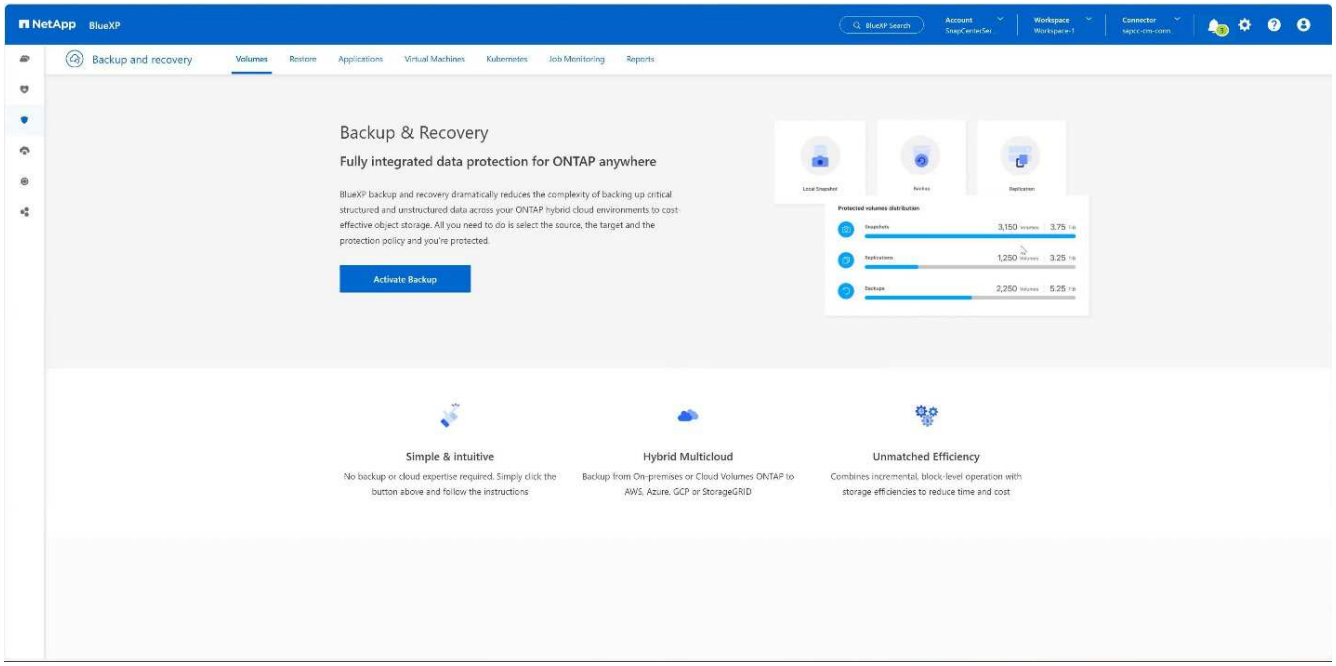
オンプレミスストレージとS3バケットの関係は、ボリュームのバックアップを作成するか、アプリケーションのバックアップをアクティブ化することで確立されます。既存のサイト間VPNを使用してオンプレミスからS3へデータを転送する場合は、VPCエンドポイントを使用する必要があるため、ボリュームバックアップを使用してオンプレミスストレージとS3バケット間の関係を作成する必要があります。[] このドキュメントの作成時、アプリケーションバックアップワークフローでは、S3バケットにアクセスするためのVPCエンドポイントの選択は提案されていません。[]
を参照してください "Amazon S3のゲートウェイエンドポイント- Amazon Virtual Private Cloud" VPC内でS3のVPCエンドポイントをセットアップする方法

最初のボリュームのバックアップを作成するには、次の手順を実行します。

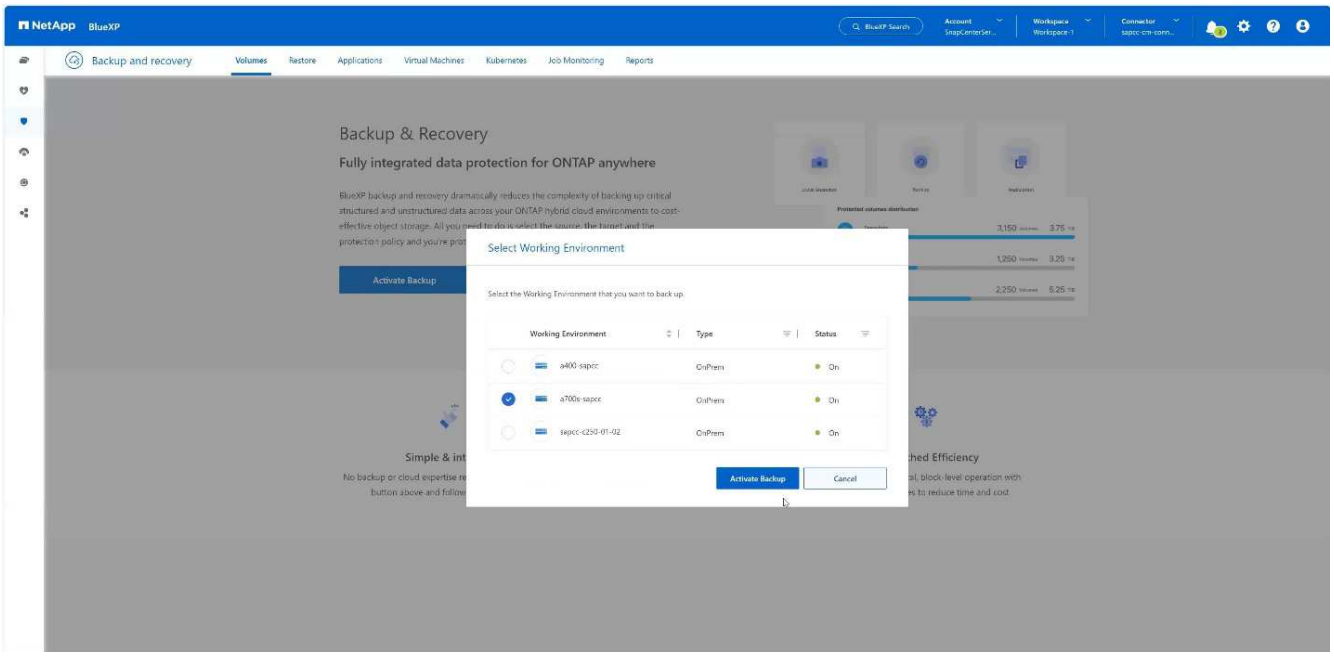
1. から[バックアップとリカバリ]に移動し、[ボリューム]*を選択します。
+



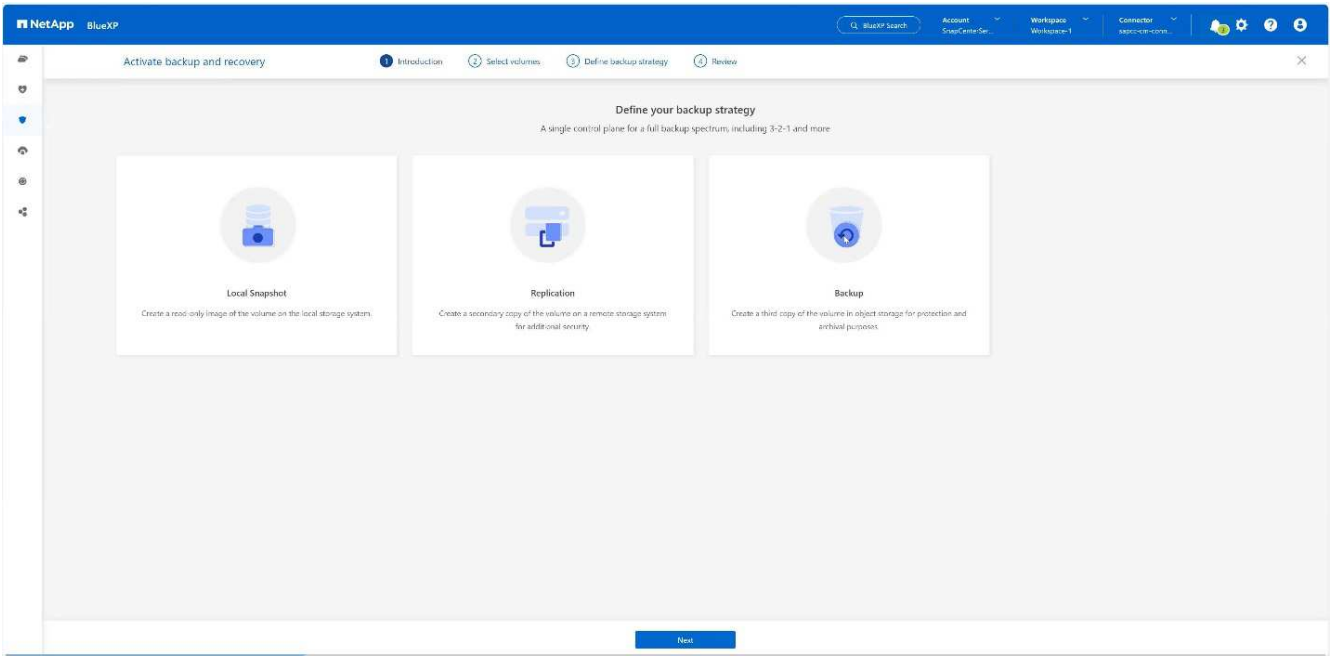

2. [Activate Backup]ボタンを押します。
+



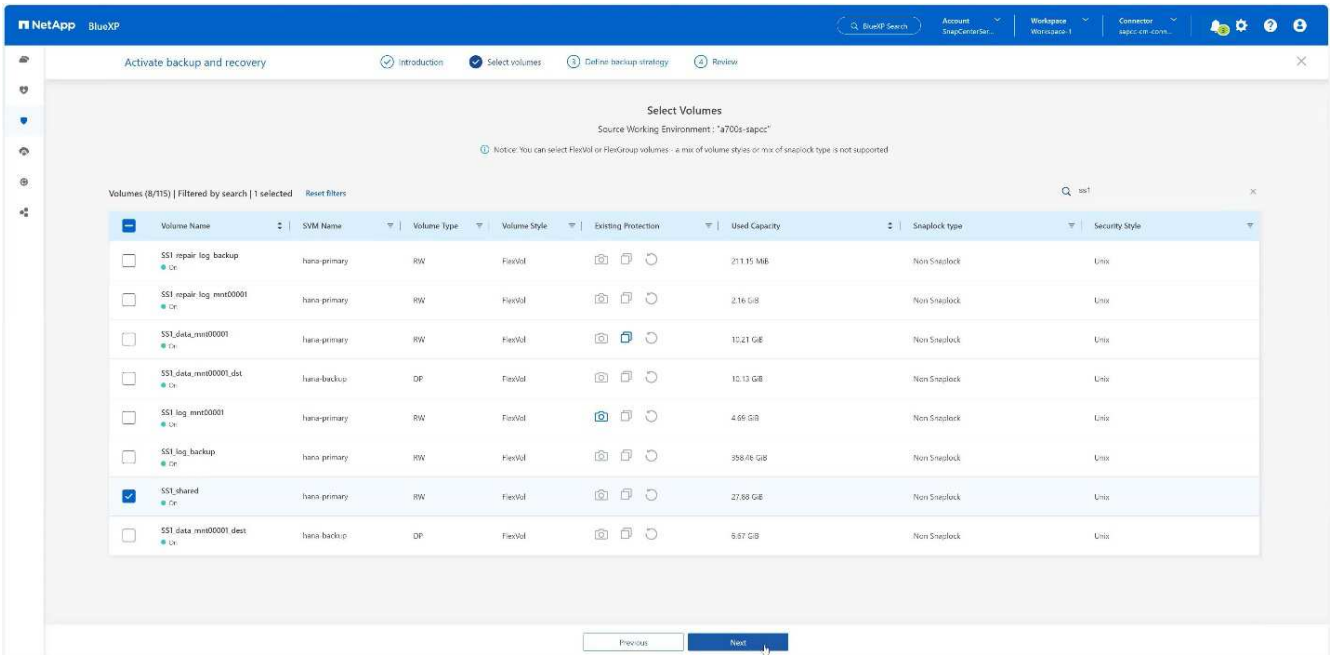

3. 目的のオンプレミスストレージシステムを選択し、*[バックアップのアクティブ化]*をクリックします。
+



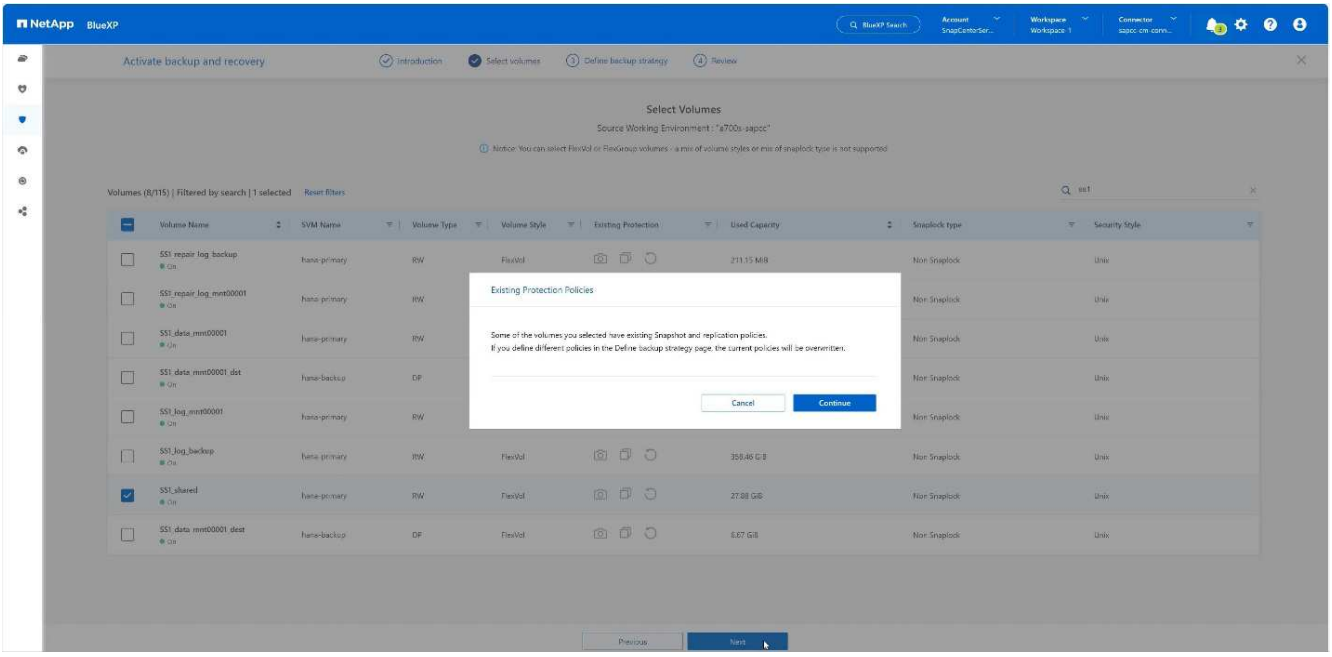

4. [バックアップ]*を選択します。
+



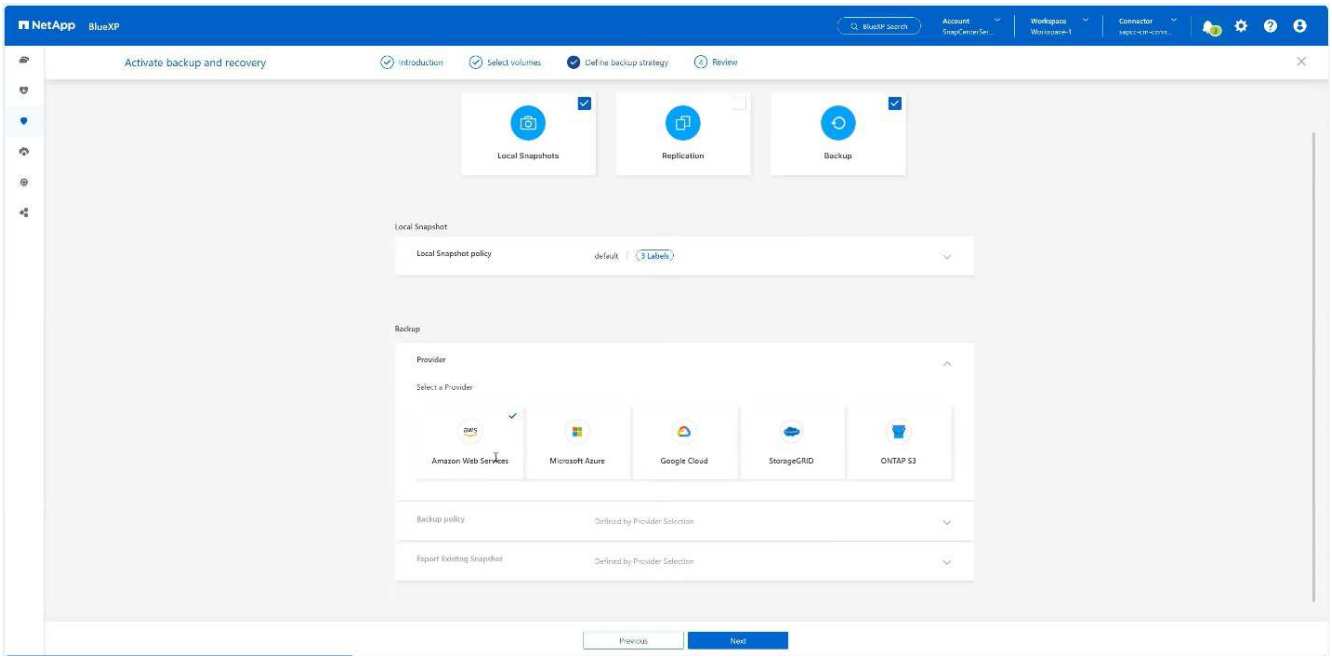

5. SAP HANAデータファイルと同じSVMに格納されているボリュームを選択し、*[次へ]*を押します。この例では、/hana/sharedのボリュームが選択されています。
+



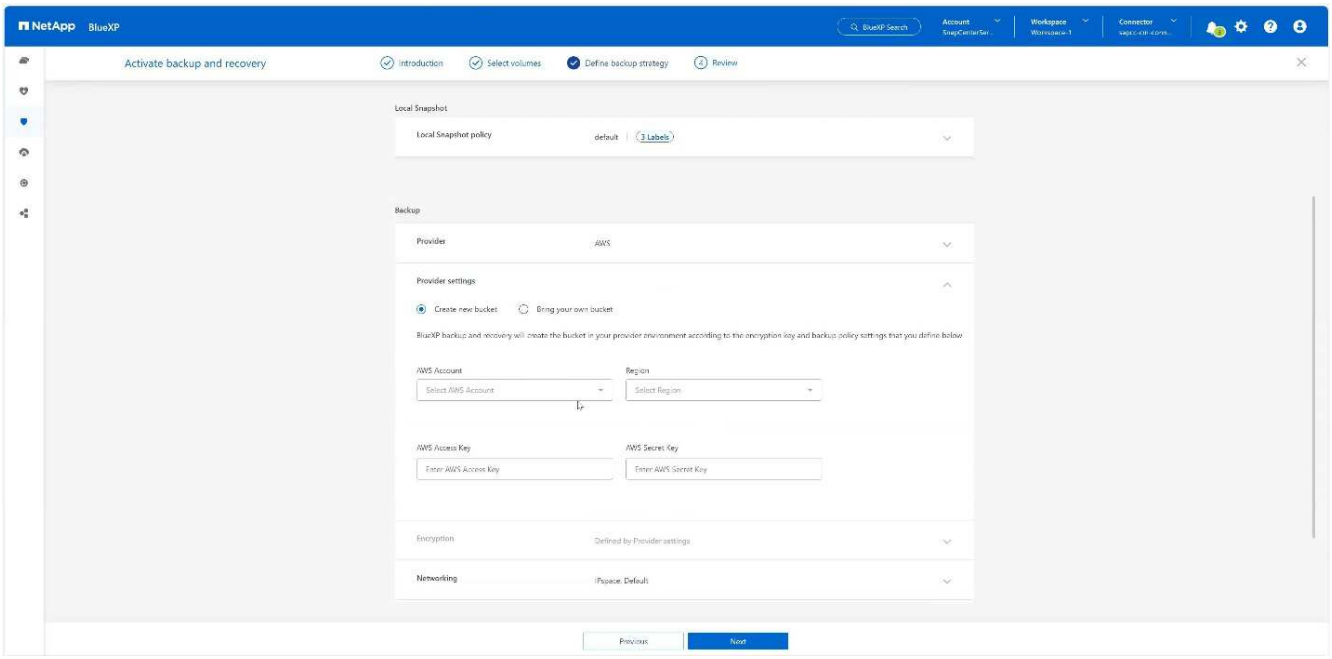

6. 既存のポリシーが存在する場合は、[続行]*をクリックします。
+



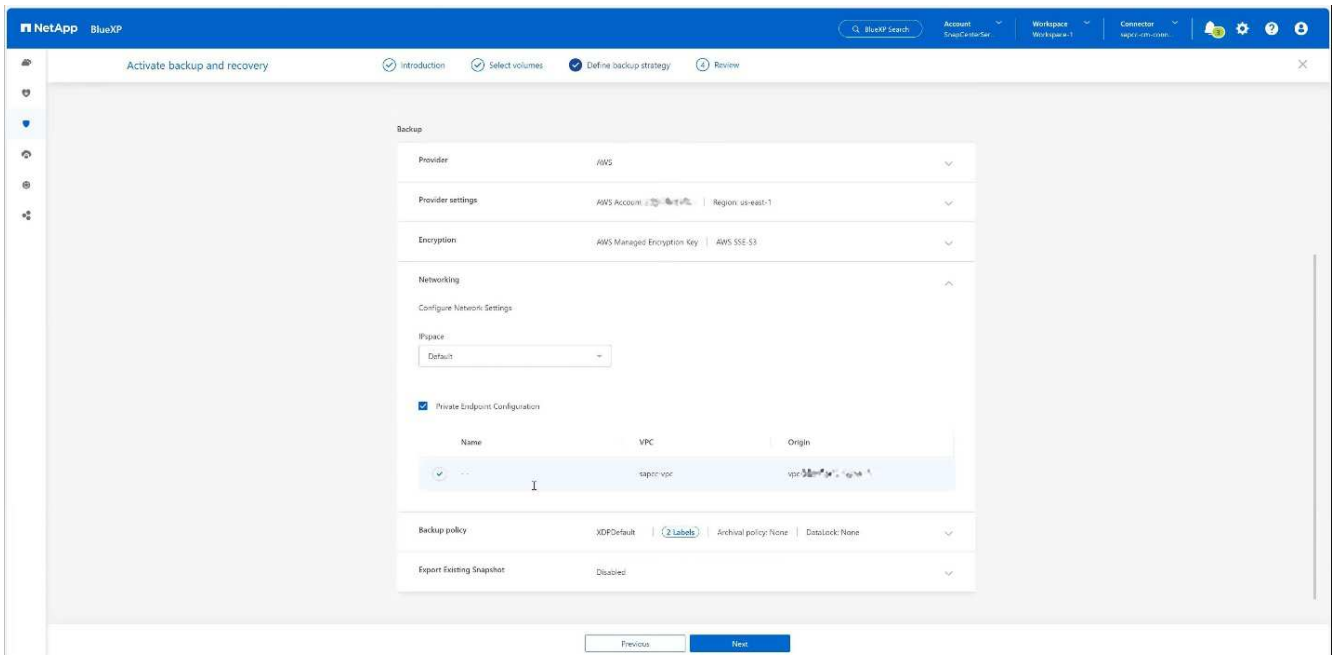

7. [バックアップオプション]*にチェックを入れ、目的のバックアッププロバイダを選択します。この例ではAWSです。+既存のポリシーについては、このオプションをオンのままにします。+使用しないオプションのチェックを外します。
+



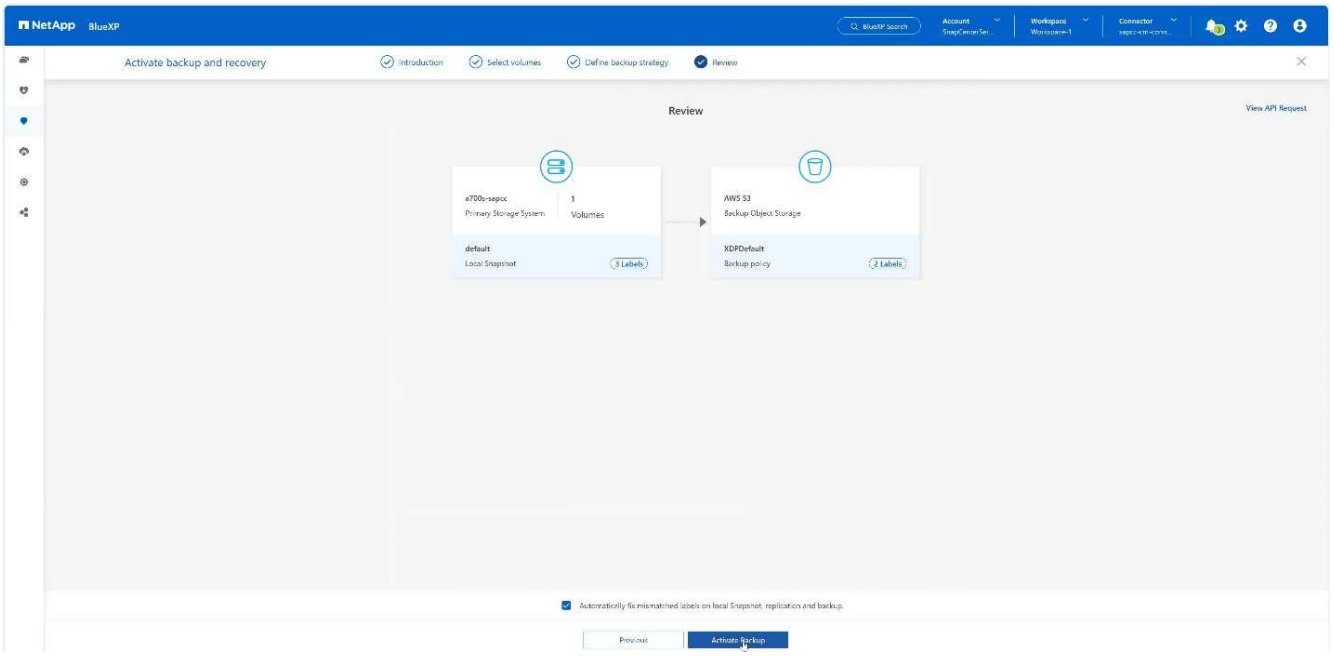

8. 新しいバケットを作成するか、既存のバケットを選択します。AWSアカウント設定、regio、アクセスキー、シークレットキーを指定します。[次へ]*を押します。
+



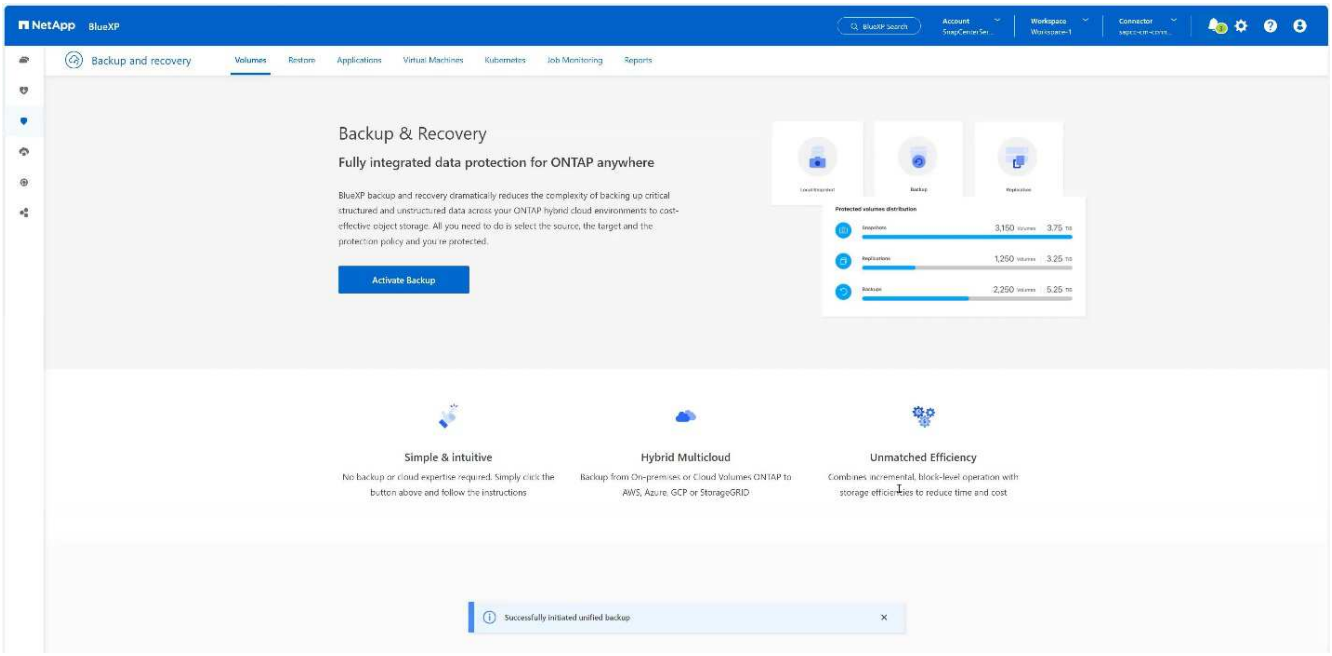

9. オンプレミスストレージシステムの正しいIPspaceを選択し、* Privat Endpoint Configuration *を選択してS3のVPCエンドポイントを選択します。[次へ]*を押します。
+



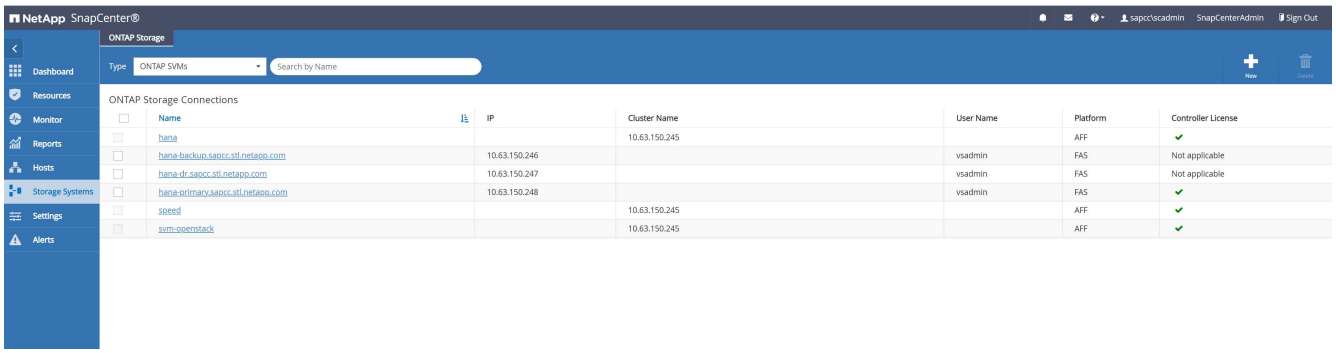

10. 構成を確認し、*[バックアップのアクティブ化]*を押します。
+

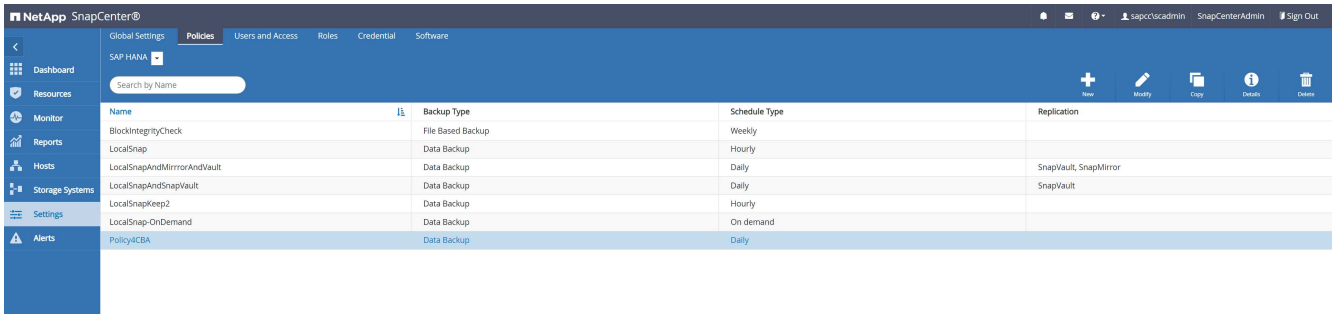


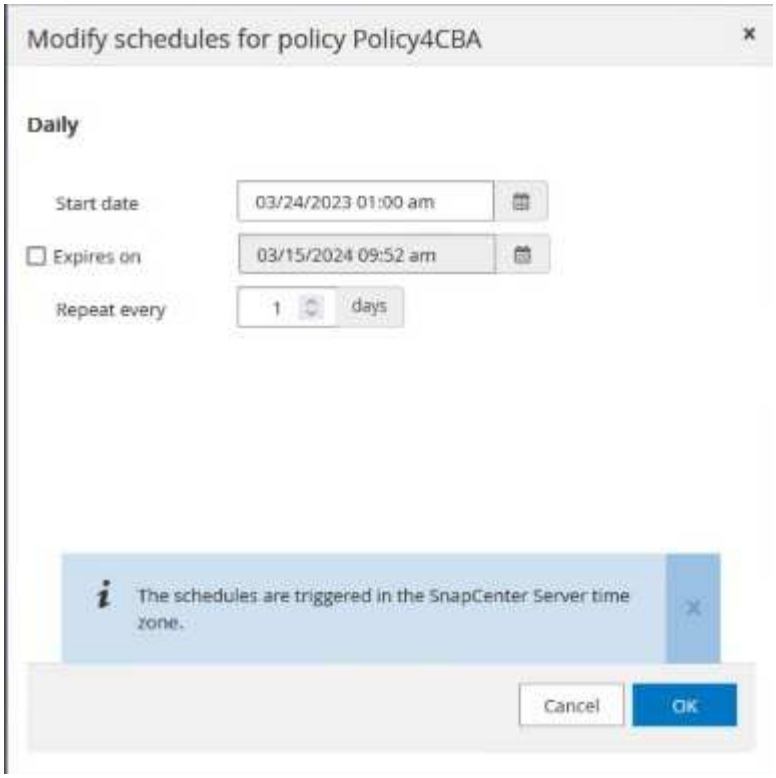

11. バックアップが開始されました。
+



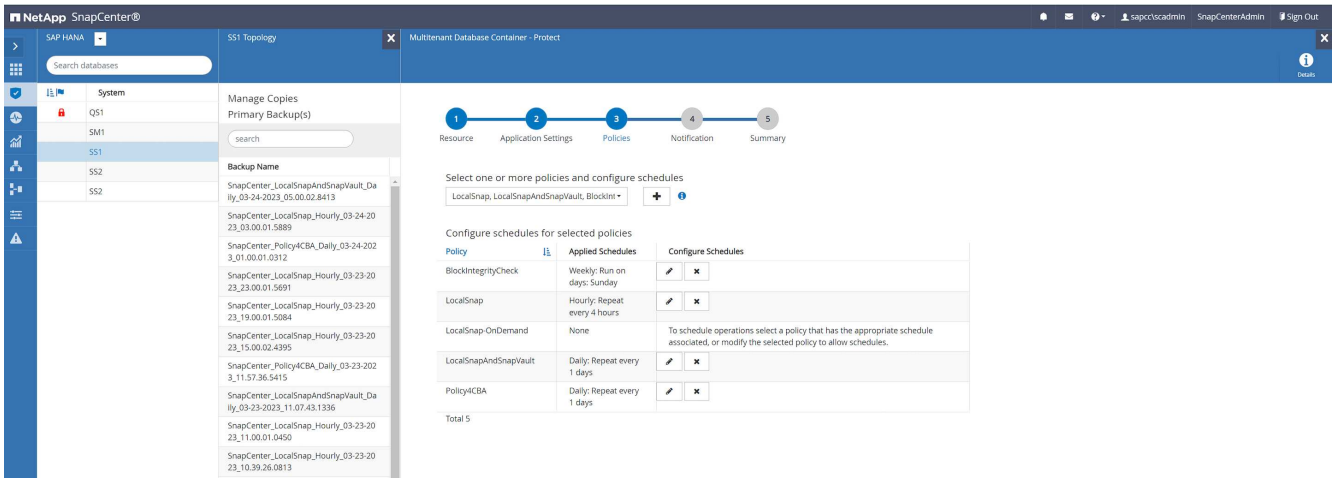

## SnapCenterでのSAP HANAシステムリソースの設定

1. SAP HANAシステムが格納されているSVM（この例ではHANA）がクラスタ経由で追加されているかどうかを確認します。SVMのみが追加されている場合は、クラスタを追加します。
+


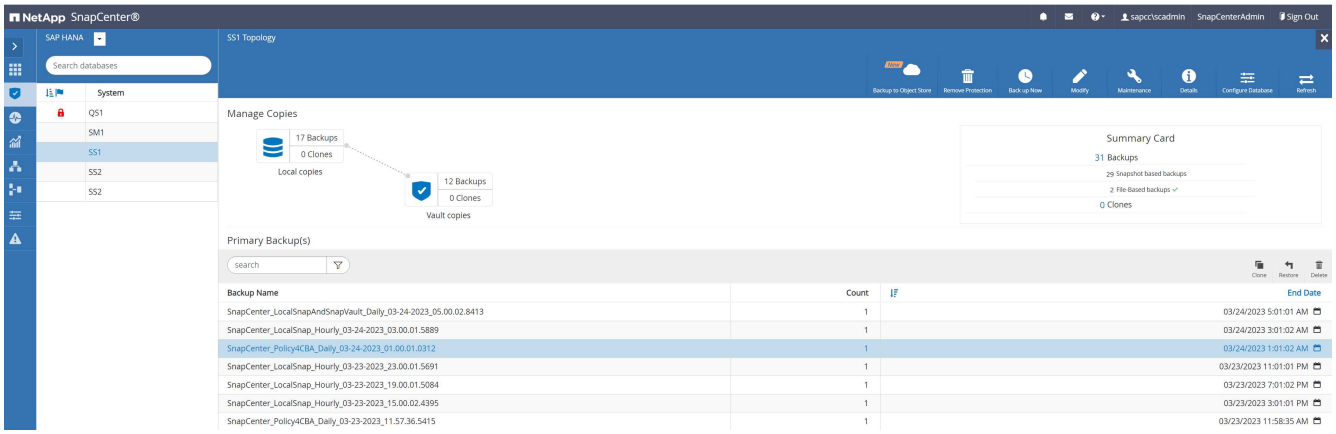

2. daily、weekly、またはmonthlyスケジュールタイプでスケジュールポリシーを定義します。
+





3. 新しいポリシーをSAP HANAシステムに追加し、日次スケジュールを割り当てます。
+

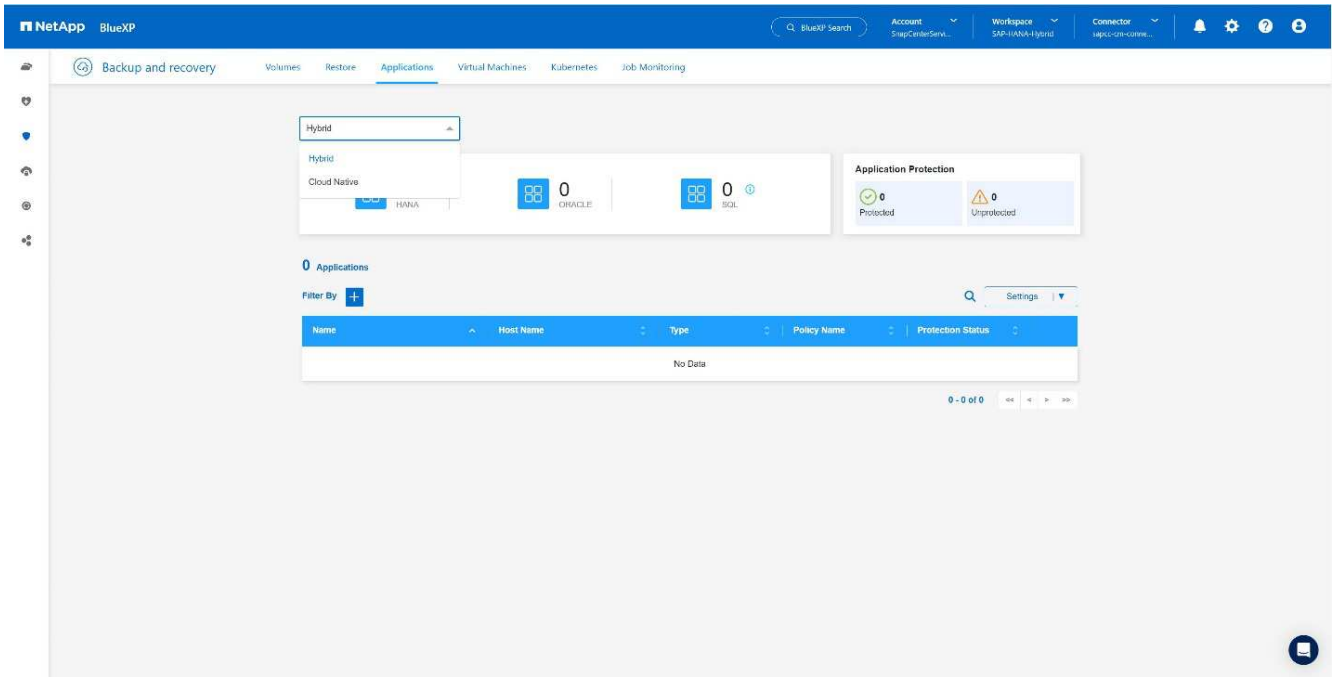



4. 設定された新しいバックアップは、定義されたスケジュールに従ってポリシーが実行されたあとに使用できるようになりま
す。

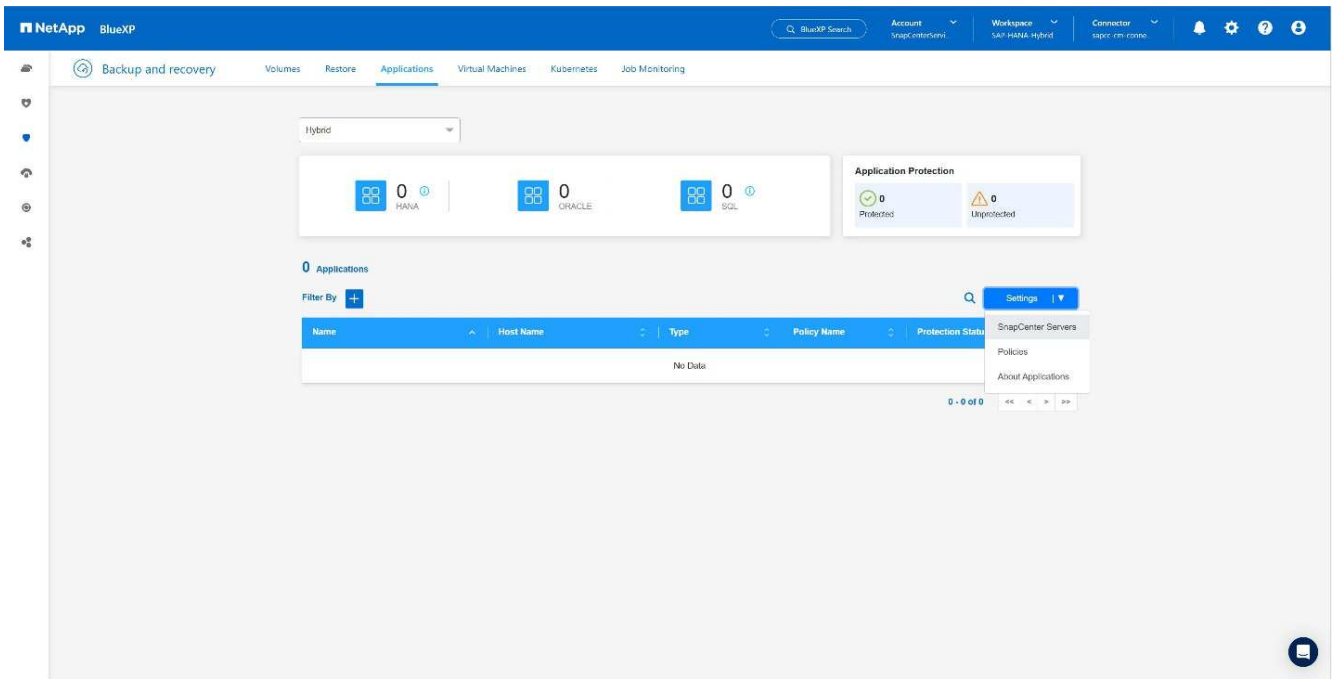


## BlueXP作業環境へのSnapCenterの追加

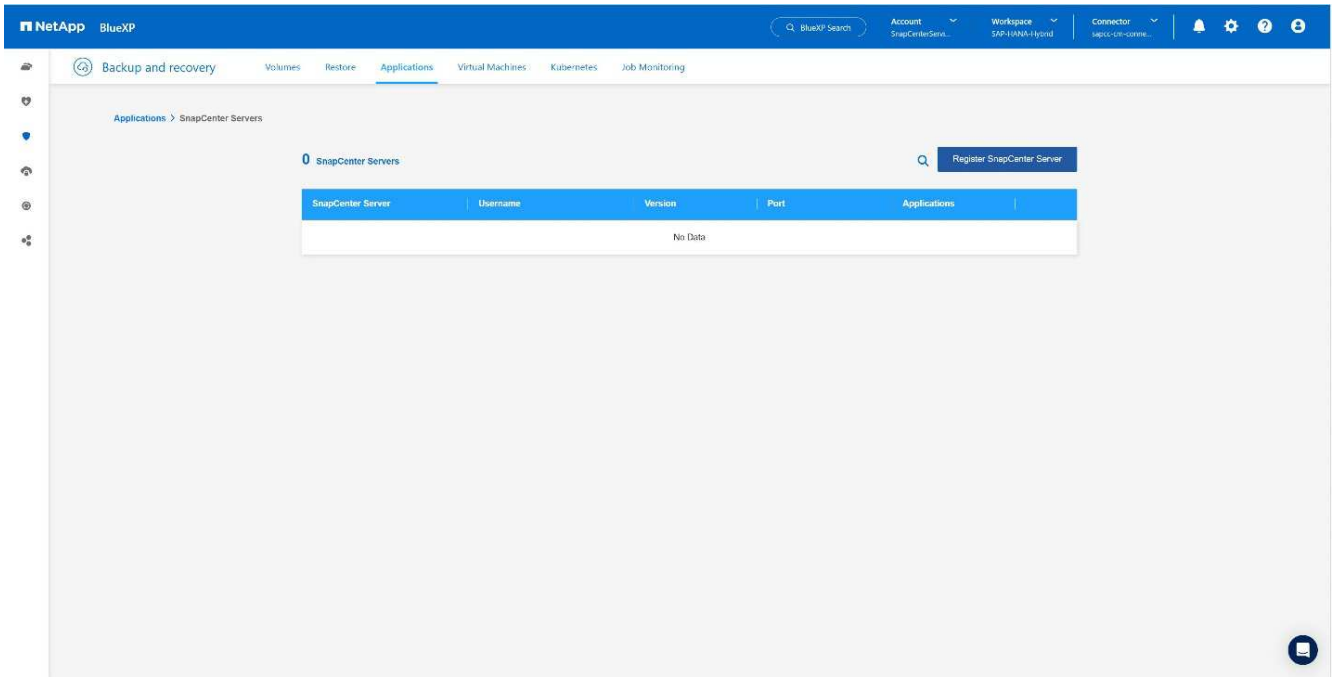
1. 左側のメニューで、[保護]→*→[アプリケーション]*を選択します。
2. プルダウンメニューから* Hybrid *を選択します。
+



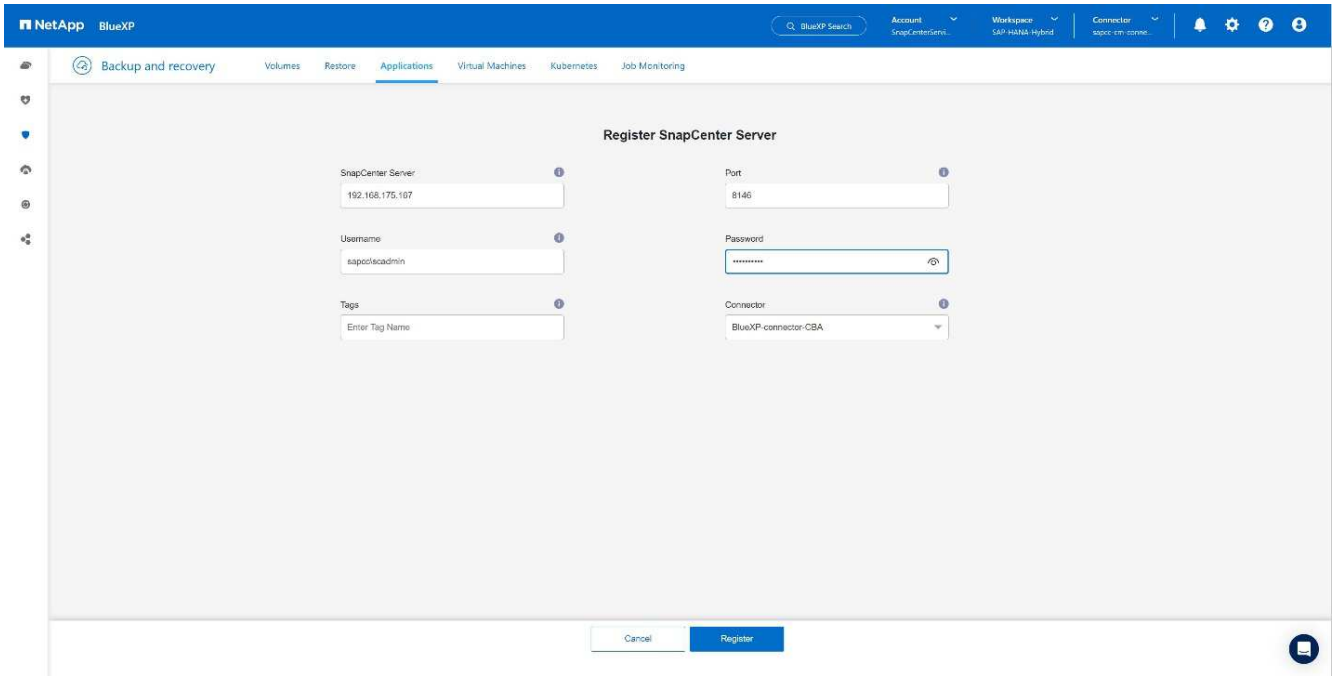

3. 設定メニューで* SnapCenter Servers *を選択します。
+



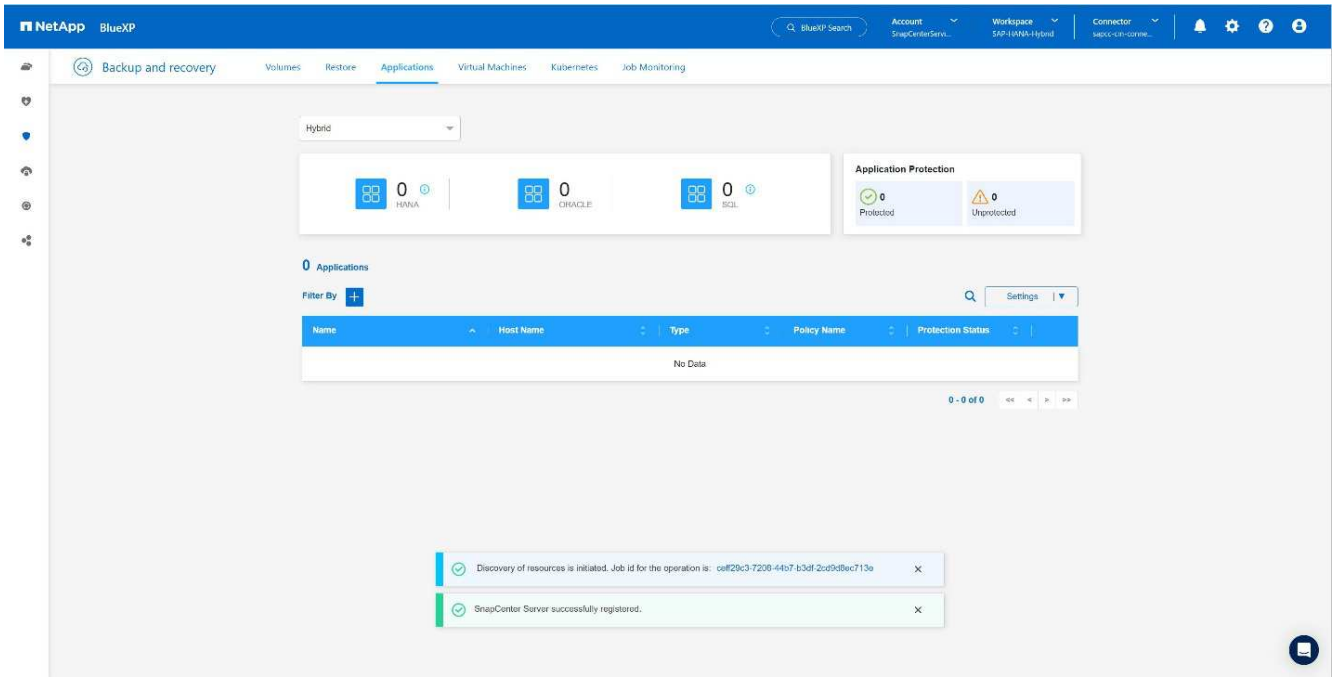

4. SnapCenterサーバを登録します。
+



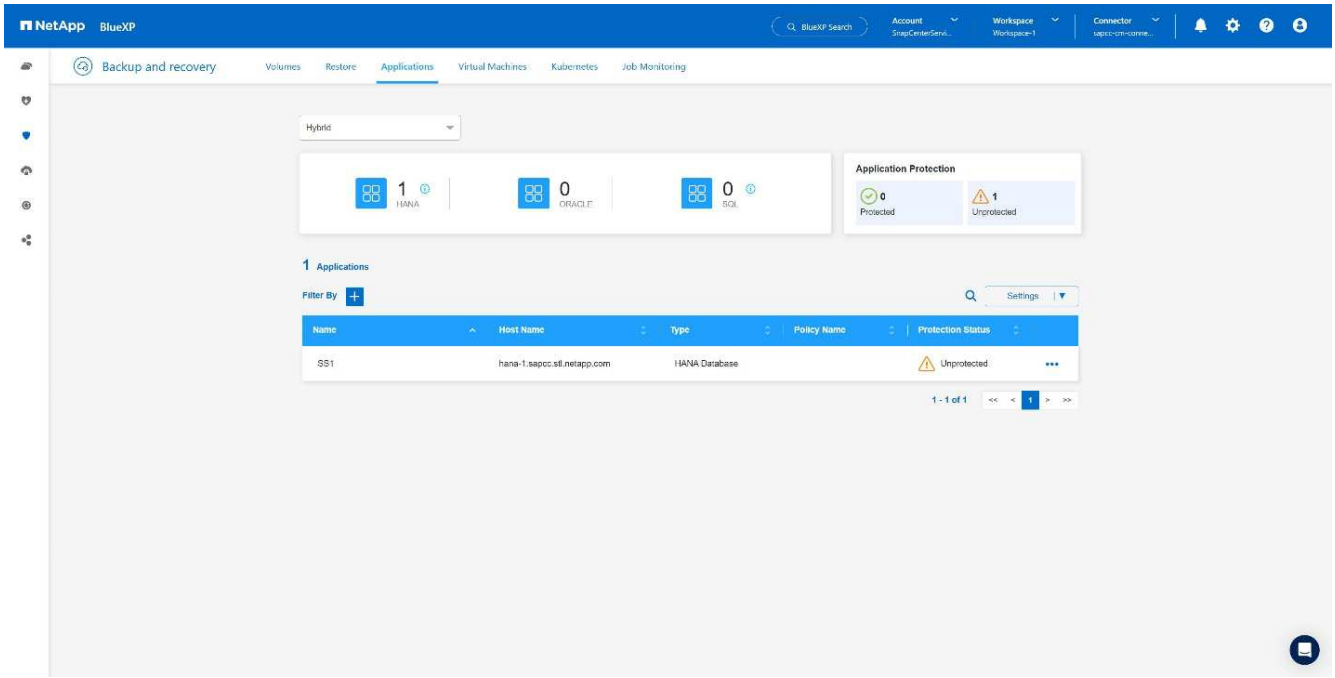

5. SnapCenterサーバのクレデンシャルを追加します。
+




6. SnapCenterサーバが追加され、データが検出されます。
+

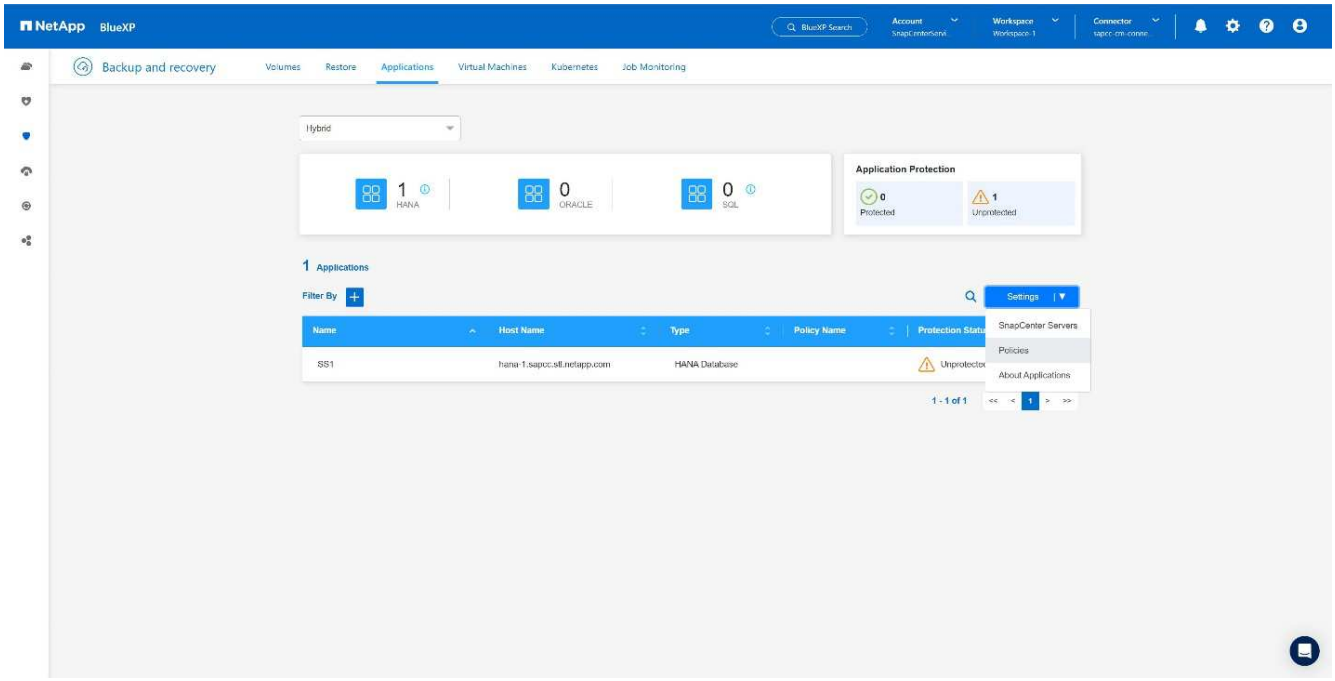



7. 検出ジョブが完了すると、SAP HANAシステムが使用可能になります。
+

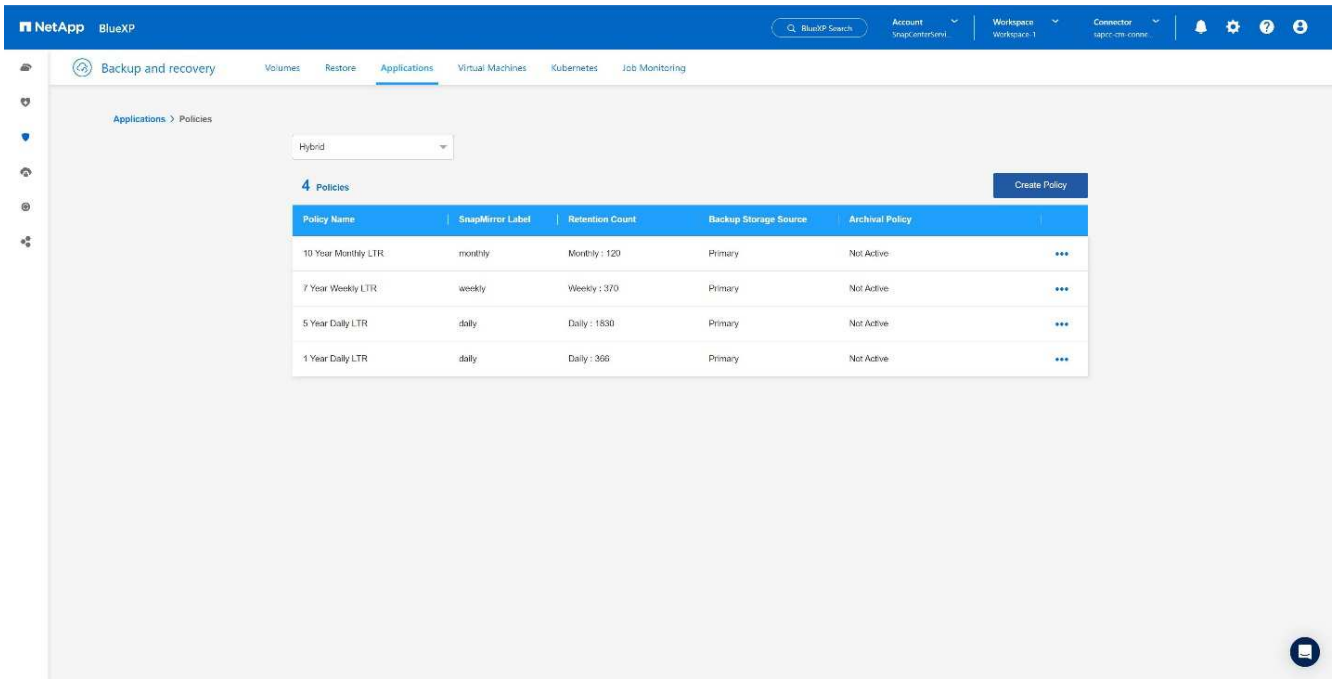



アプリケーションバックアップのバックアップポリシーの作成

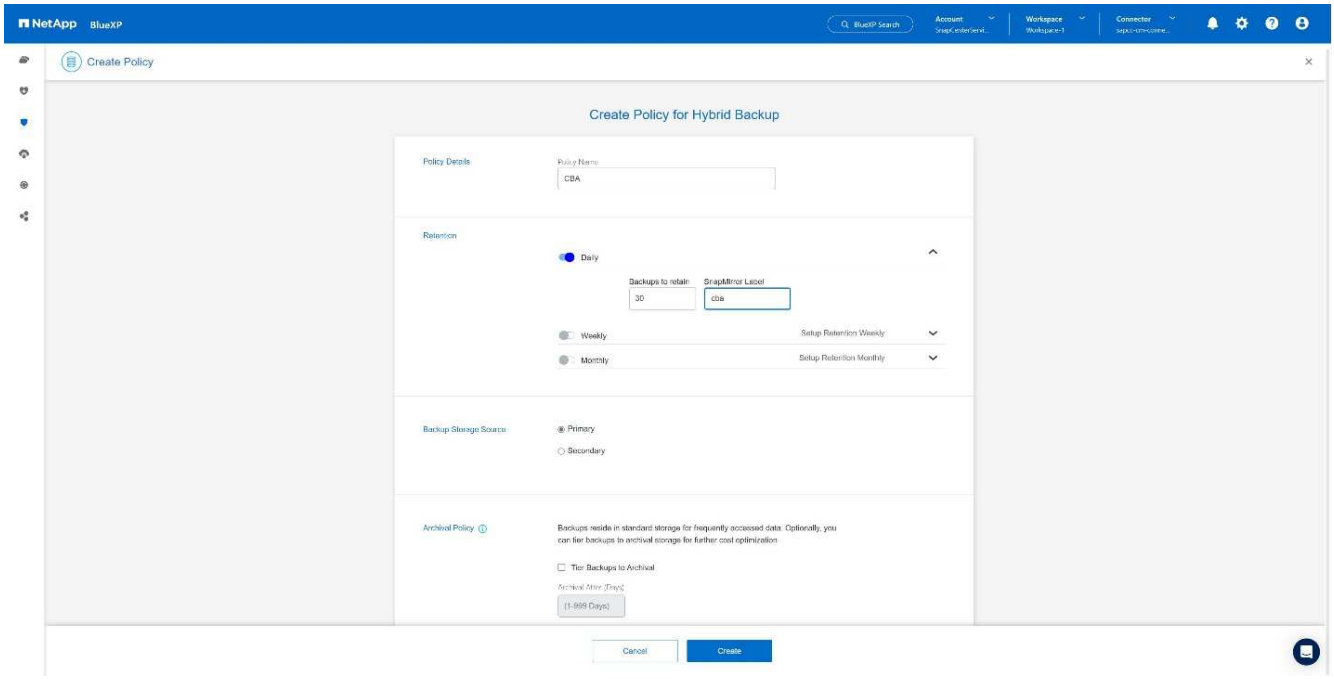
1. 設定メニューの*ポリシー*を選択します。
+



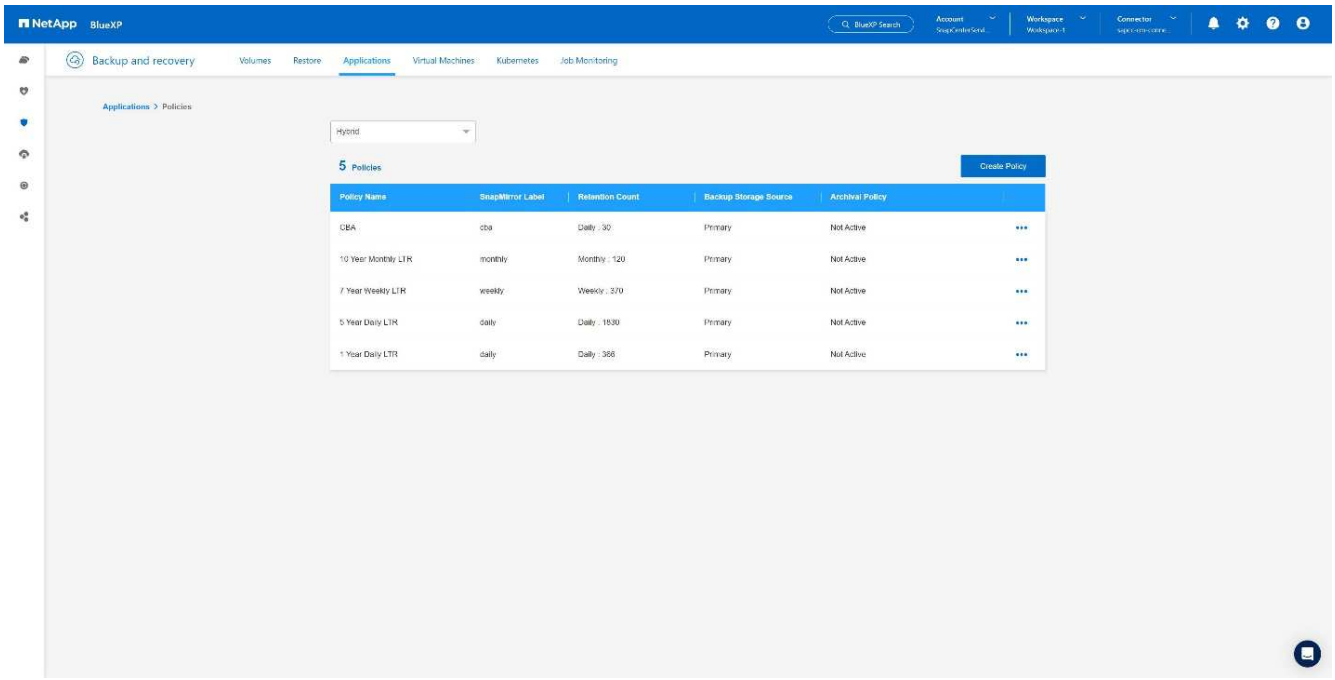

2. 必要に応じて、[ポリシーの作成]*をクリックして新しいポリシーを作成します。
+




3. ポリシー名と目的のSnapMirrorラベルを指定し、必要なオプションを選択して*[作成]*を押します。
+

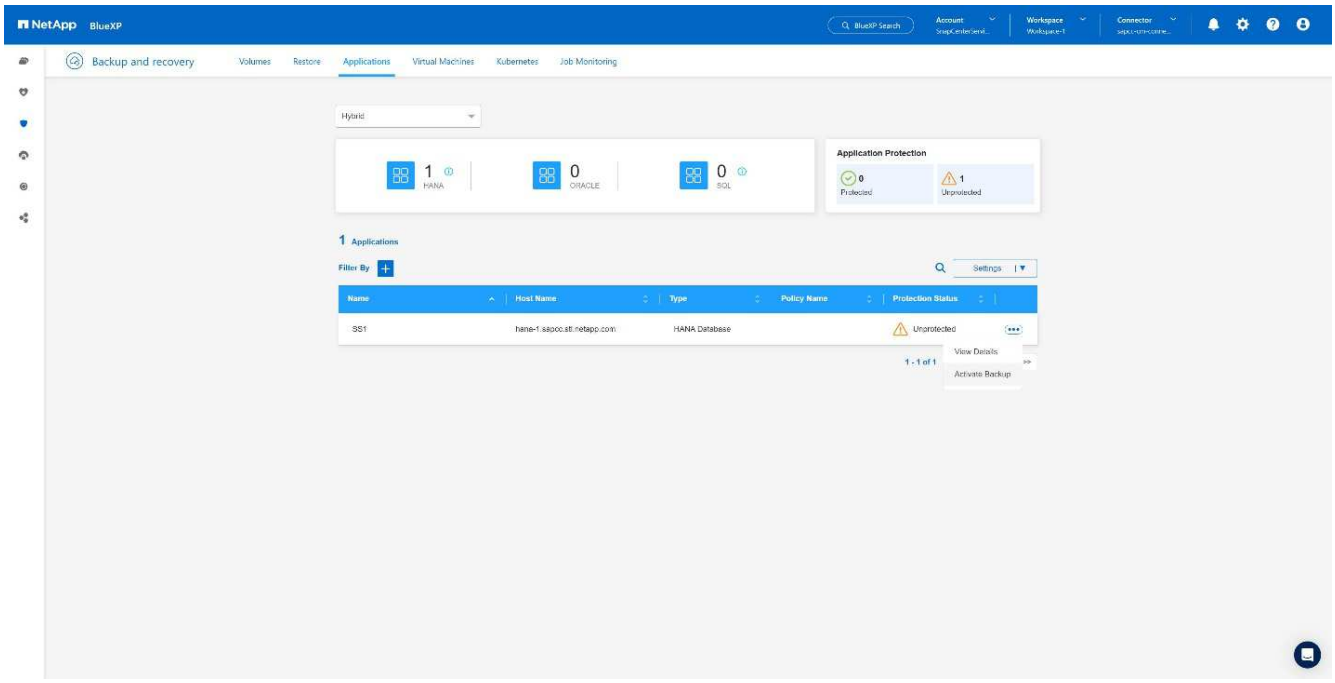



4. 新しいポリシーが使用可能になります。
+

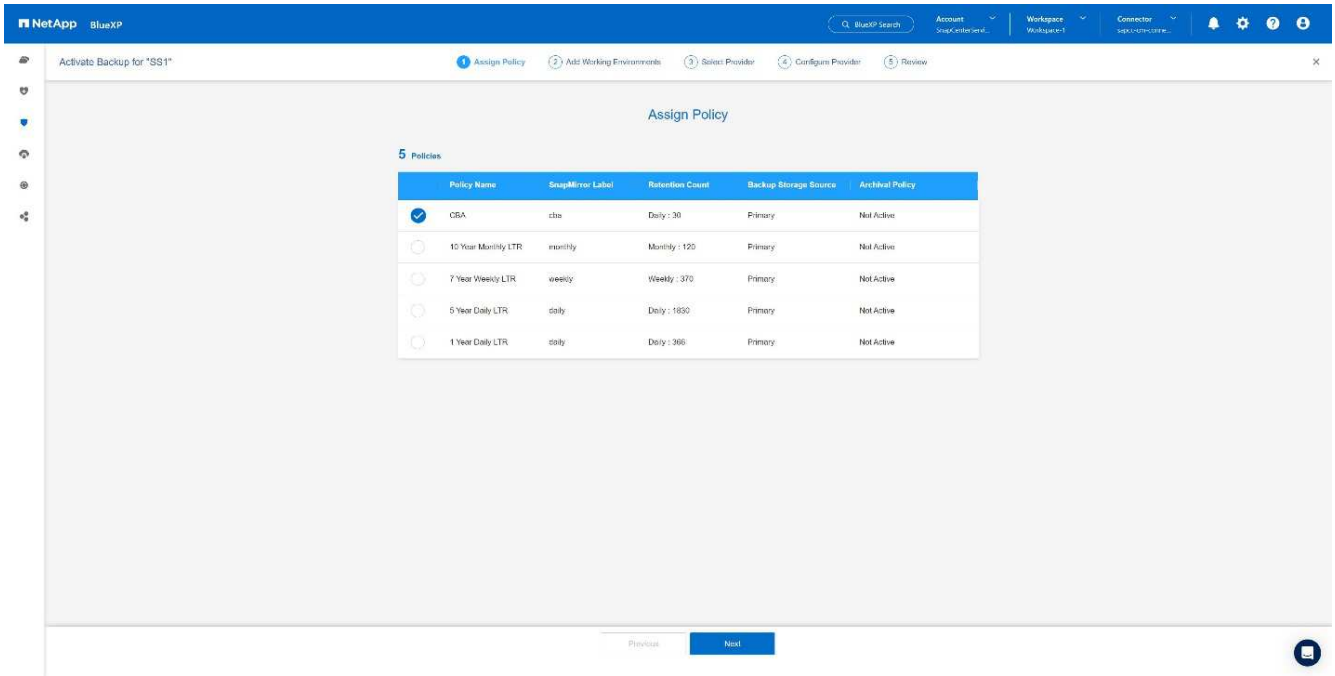



## Cloud Backup for ApplicationsによるSAP HANAデータベースの保護

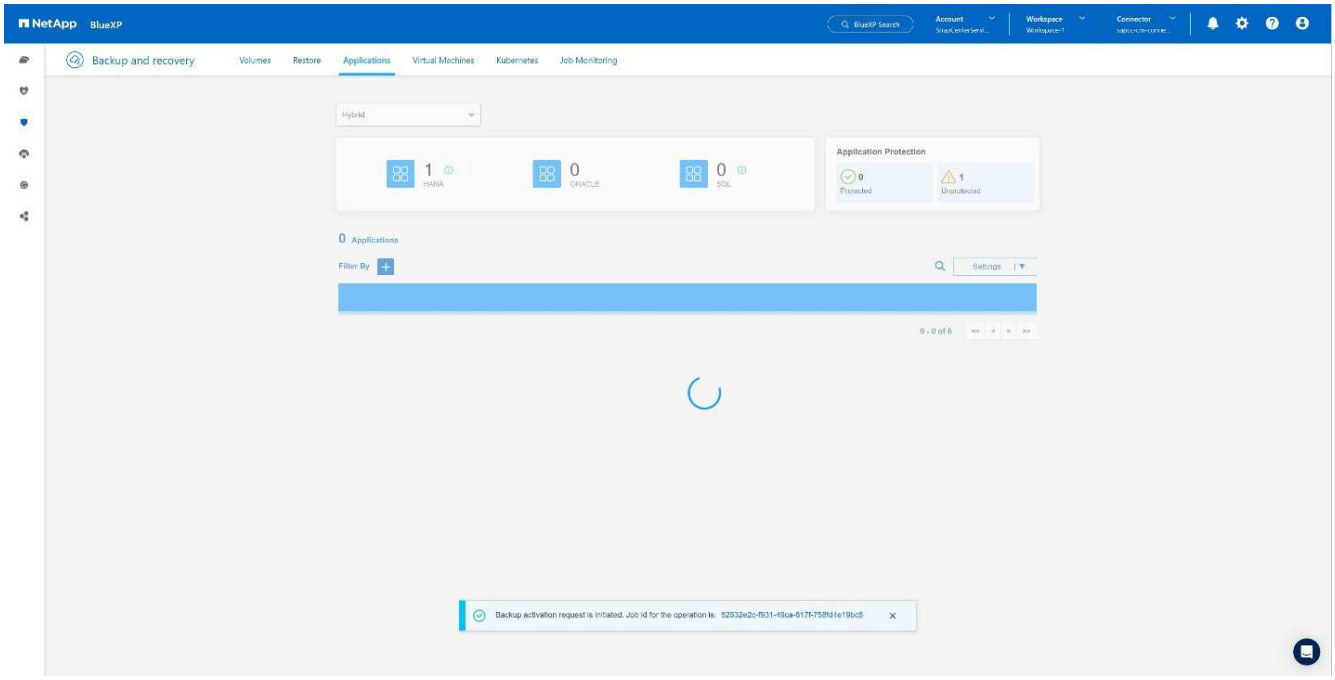
1. SAP HANAシステムの*[バックアップのアクティブ化]*を選択します。
+



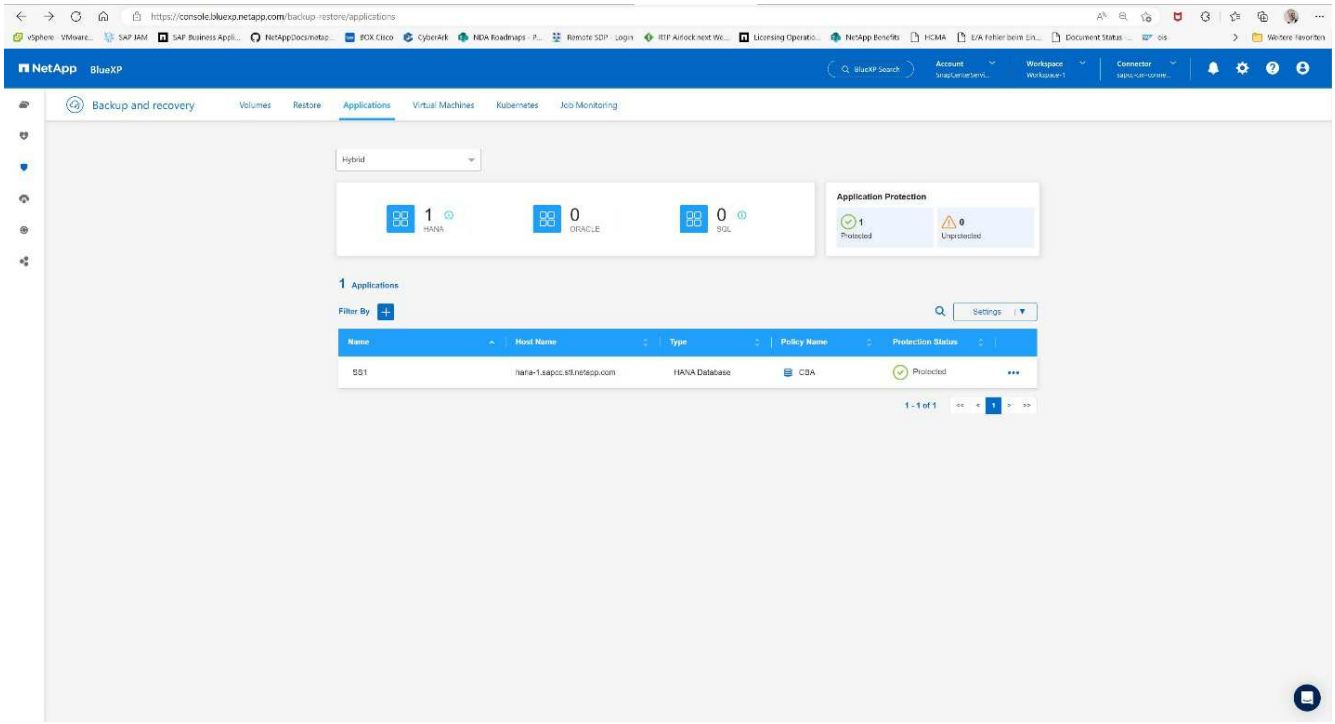

2. 前の手順で作成したポリシーを選択し、*[次へ]*をクリックします。
+



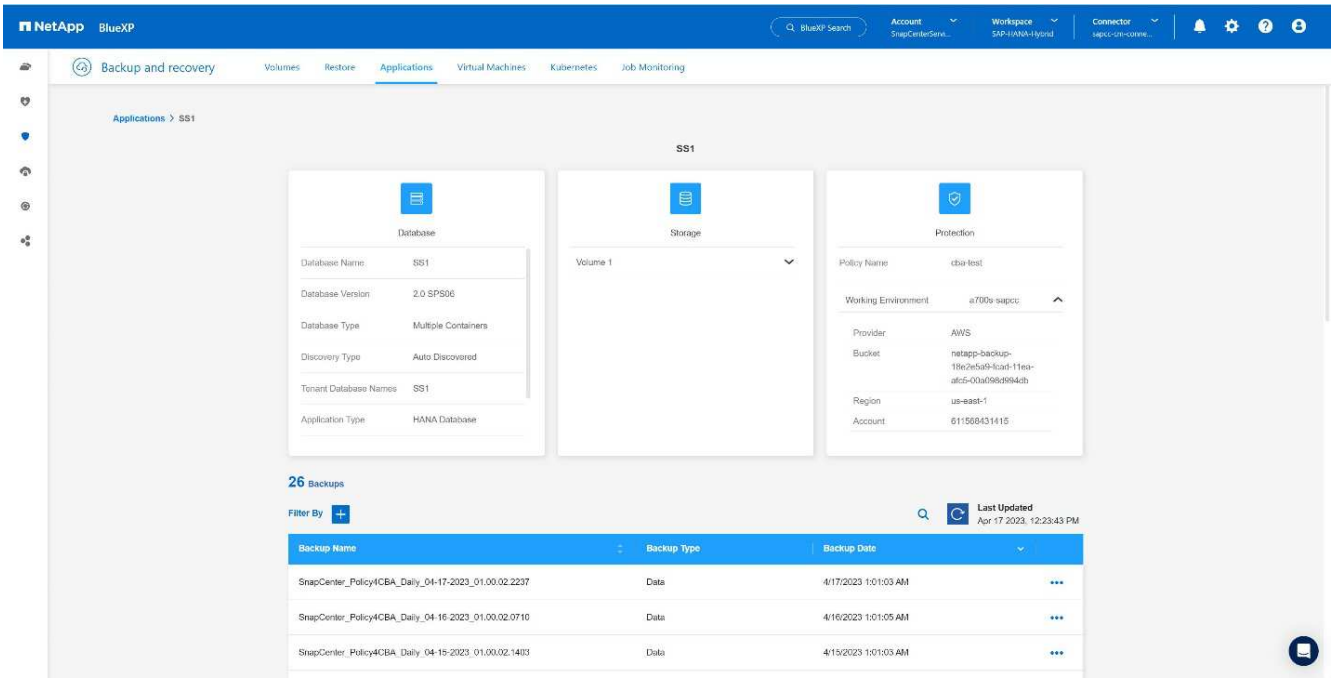

3. ストレージシステムとコネクタが事前に設定されているため、バックアップがアクティブ化されます。
+




4. ジョブが完了すると、システムが表示されます。
+




5. しばらくすると、バックアップがSAP HANAシステムの詳細ビューに表示されます。+日次バックアップが翌日に表示されます。
+

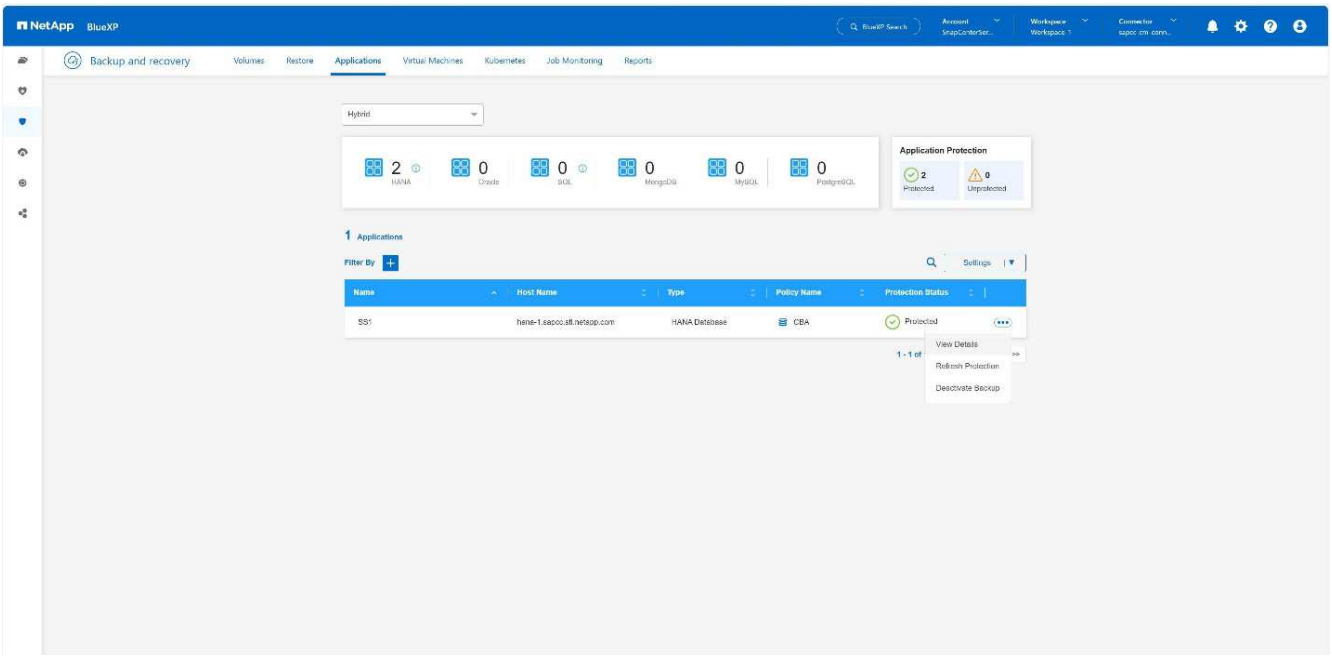



環境によっては、SnapMirrorソースの既存のスケジュール設定を削除しなければならない場合があります。そのためには、ソースONTAPシステムで次のコマンドを実行します。*snapmirror modify -destination-path <hana-cloud-svm>：<SID_data_mnt00001>* copy -schedule ""_。

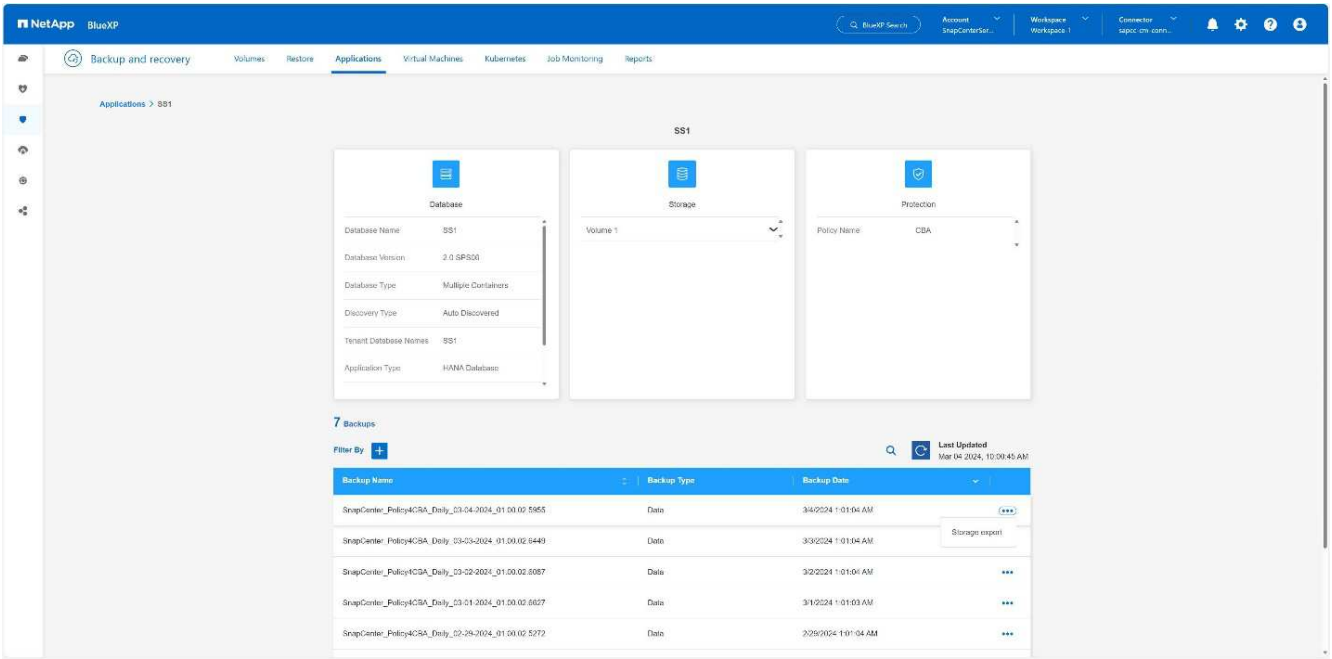
## SAP HANA BlueXPのバックアップのリストア

バックアップからのリストアは、オンプレミスのNetApp ONTAPベースのストレージシステムまたはクラウド内のNetApp CVOに対してのみ実行できます。リストアを実行するには、次の手順を実行します。

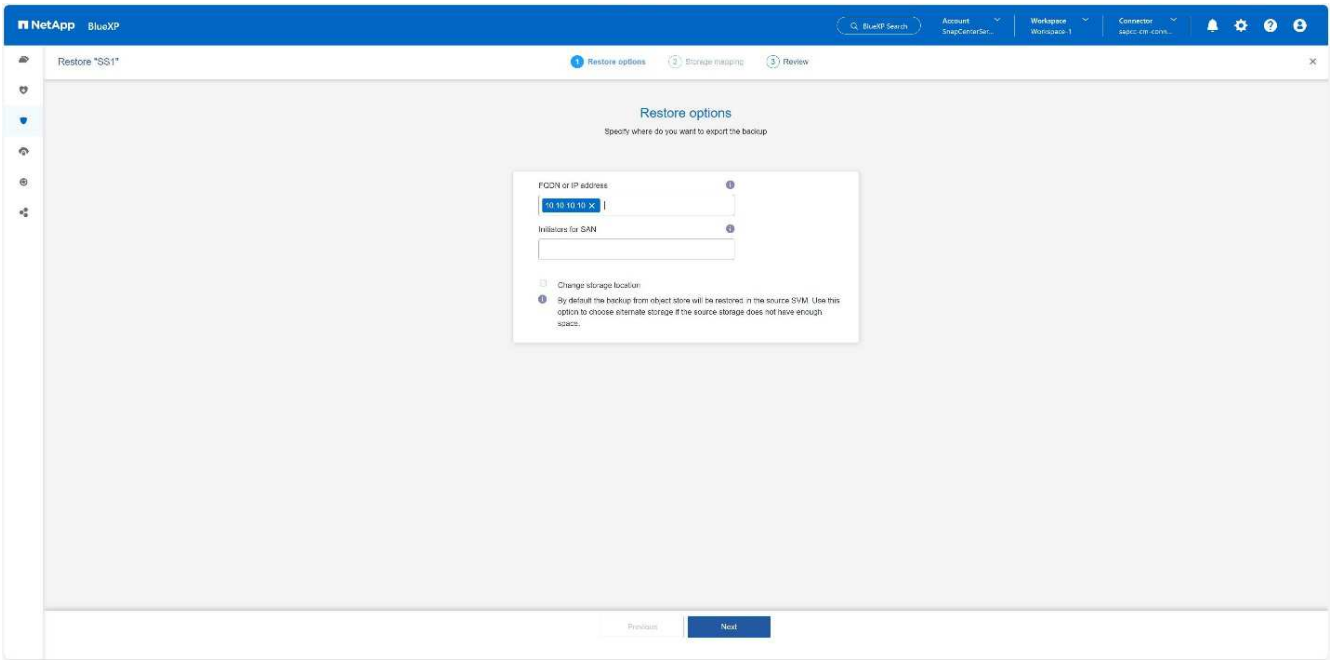
1. BlueXP UIで 、**[保護]** > **[**バックアップとリカバリ**]**>*[アプリケーション]*をクリックし、[ハイブリッド]を選択します。
2. [Filter by] フィールドで、フィルタ Type を選択し 、ドロップダウンから HANA *を選択します。
3. リストアするデータベースの*[詳細の表示]*をクリックします。
+




4. 目的のバックアップを選択し、[ストレージ][エクスポート]を選択します。
+




5. 必要なオプションを指定します。
+




a. NAS環境の場合は、オブジェクトストアからリストアするボリュームのエクスポート先となるホストのFQDNまたはIPアドレスを指定します。

b. SAN環境の場合、オブジェクトストアからリストアするボリュームのLUNをマッピングするホストのイニシエータを指定します。

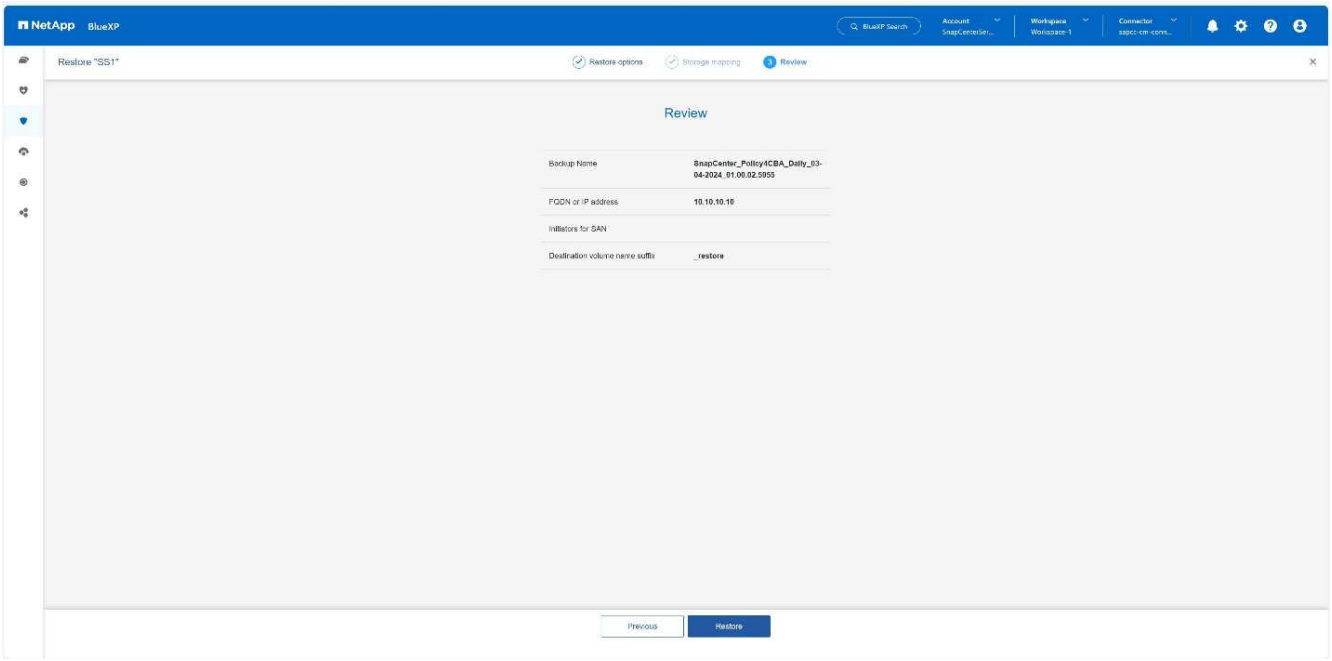
6. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。

7. ソースストレージに十分なスペースがないか、ソースストレージが停止している場合は 、*[ストレージの場所を変更]*を選択します。

8. [ストレージの場所の変更]*を選択した場合は、デスティネーションボリュームにサフィックスを追加できます。このチェックボックスをオンにしていない場合、デフォルトでは デスティネーションボリュームに*_restore *が追加されます。 [次へ]*をクリックします。

9. [ストレージの場所を変更]を選択した場合は、オブジェクトストアからリストアするデータを格納する代替ストレージの場所の詳細を[ストレージマッピング]ページで指定し、*[次へ]*をクリックします。

10. 詳細を確認し、 *[リストア]*をクリックします。




++この処理では、指定したホストのリストアされたバックアップのストレージエクスポートのみが実行されます。ホストでファイルシステムを手動でマウントし、データベースを起動する必要があります。ボリュームを利用したあと、ストレージ管理者はONTAP クラスタからボリュームを削除できます。

## 追加情報とバージョン履歴

このセクションでは、追加情報の参照先とバージョン履歴を示します。

### 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。

- NetApp BlueXPバックアップ/リカバリの製品ドキュメント+
"オンプレミスアプリケーションデータの保護| NetAppドキュメント"
- "SnapCenter を使用した SAP HANA の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 | 2024年3月 | 初版 |

を参照してください "Interoperability Matrix Tool （ IMT ）" NetApp Support Siteで、本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかを確認してください。NetApp IMT には、ネットアップがサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

# SnapCenter を使用した SAP HANA システムレプリケーションのバックアップとリカバリ

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

SAP HANA システムレプリケーションは、一般に、 SAP HANA データベースの高可用性またはディザスタリカバリ解決策として使用されます。SAP HANA システムレプリケーションには、ユースケースや可用性の要件に応じて、さまざまな動作モードが用意されています。

作成者：Nils Bauer、NetApp

組み合わせて使用できる主なユースケースは次の 2 つです。

- 専用のセカンダリ SAP HANA ホストを使用した、ゼロの Recovery Point Objective （ RPO ；目標復旧時点）と最小の Recovery Time Objective （ RTO ；目標復旧時間）による高可用性。
- 遠隔地での災害復旧。セカンダリ SAP HANA ホストは、通常運用時の開発やテストにも使用できます。

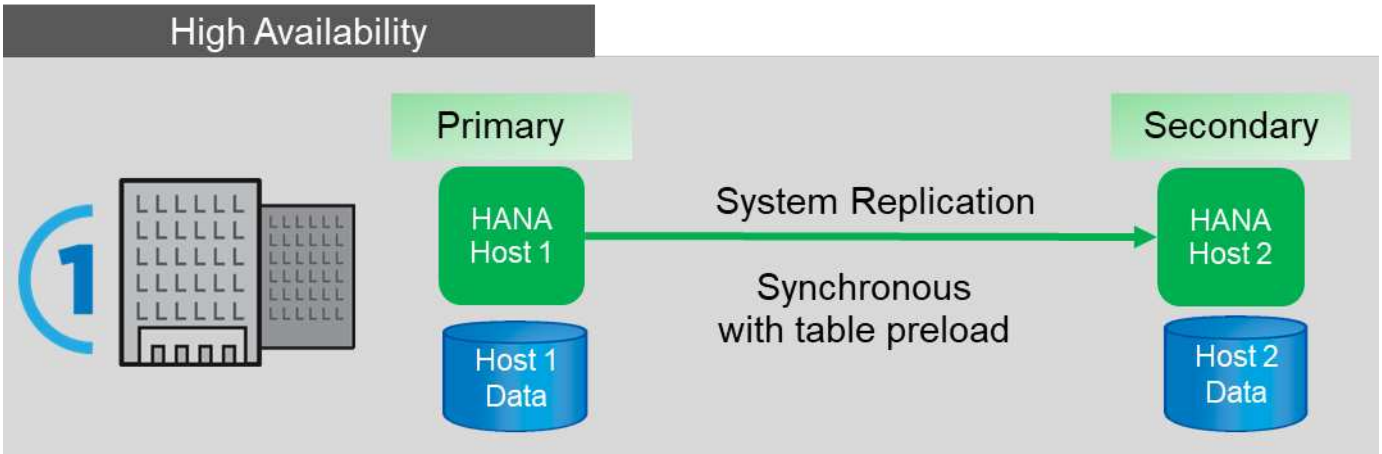
**RPO** がゼロで **RTO** が最小限のハイアベイラビリティ

システムレプリケーションでは、セカンダリ SAP HANA ホストのメモリにプリロードされたテーブルを使用して同期レプリケーションが設定されます。この高可用性解決策を使用して、ハードウェアやソフトウェアの障害に対処できるほか、 SAP HANA ソフトウェアのアップグレード中の計画的停止（ダウンタイムはほぼゼロ）を軽減できます。

フェイルオーバー処理は、多くの場合、サードパーティ製のクラスタソフトウェアを使用するか、 SAP Landscape Management ソフトウェアでワンクリックで実行することで自動化されます。

バックアップ要件の観点では、どの SAP HANA ホストがプライマリまたはセカンダリであるかに関係なく、バックアップを作成できる必要があります。バックアップを作成したホストに関係なく、共有バックアップインフラを使用してバックアップがリストアされます。

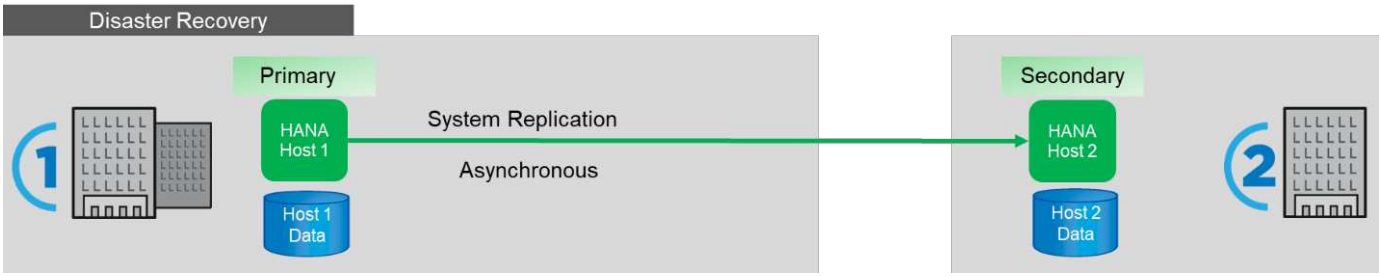
このドキュメントの残りの部分では、ハイアベイラビリティ解決策として構成された SAP システムレプリケーションを使用したバックアップ処理について説明します。



遠隔地での災害復旧

システムレプリケーションは、セカンダリホストのメモリにテーブルがプリロードされていない非同期レプリケーションで構成できます。この解決策はデータセンターの障害に対処するために使用され、通常は手動でフェイルオーバー処理が実行されます。

バックアップ要件に関しては、データセンター 1 での通常運用中、およびデータセンター 2 でのディザスタリカバリ中に、バックアップを作成できる必要があります。データセンター 1 と 2 には独立したバックアップインフラがあり、ディザスタフェイルオーバーの一環としてバックアップ処理がアクティブ化されます。通常、バックアップインフラは共有されません。もう一方のデータセンターで作成されたバックアップをリストアすることはできません。



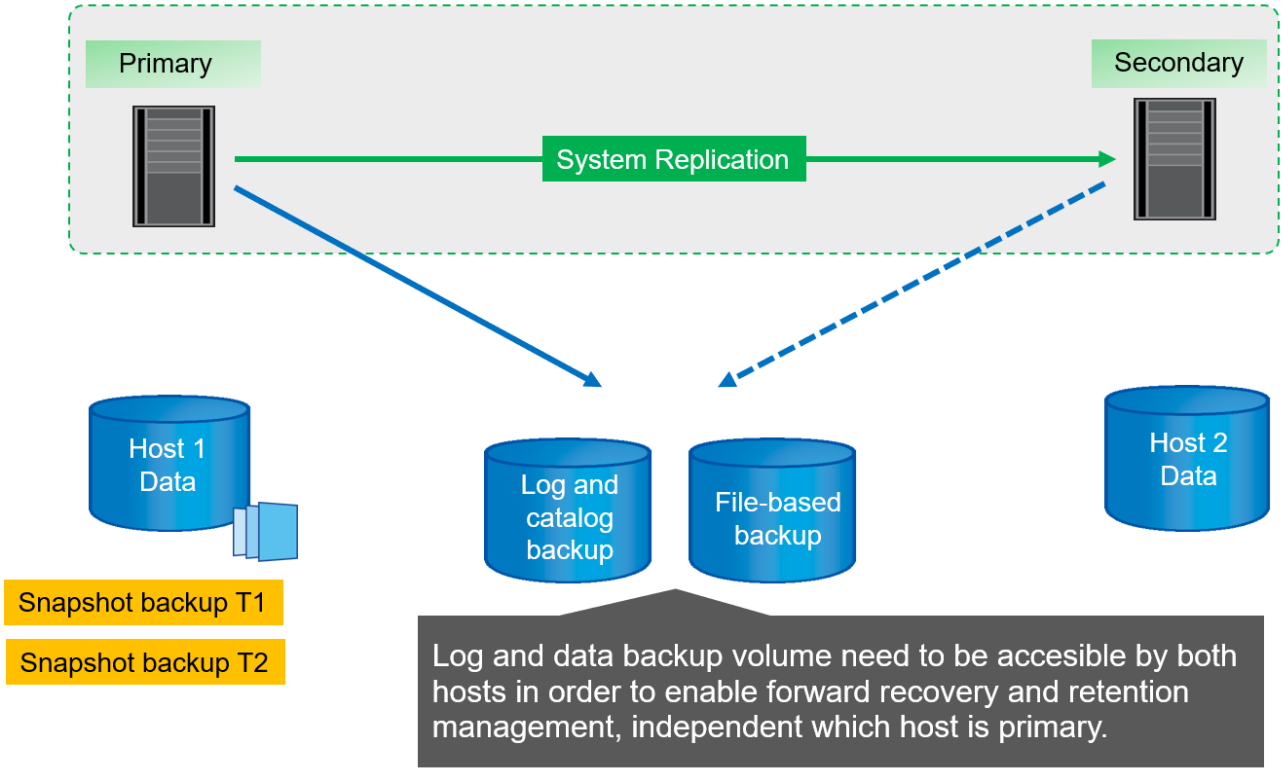

## ストレージ **Snapshot** バックアップと **SAP** システムレプリケーション

### バックアップ処理は常にプライマリ SAP HANA ホストで実行されます。バックアップ処理に必要な SQL コマンドをセカンダリ SAP HANA ホストで実行することはできません。

SAP HANA のバックアップ処理では、プライマリとセカンダリの SAP HANA ホストが単一のエンティティになります。バックアップがプライマリ SAP HANA ホストとセカンダリ SAP HANA ホストのどちらで作成されたかに関係なく、 SAP HANA は同じバックアップカタログを共有し、リストアとリカバリにバックアップを使用します。

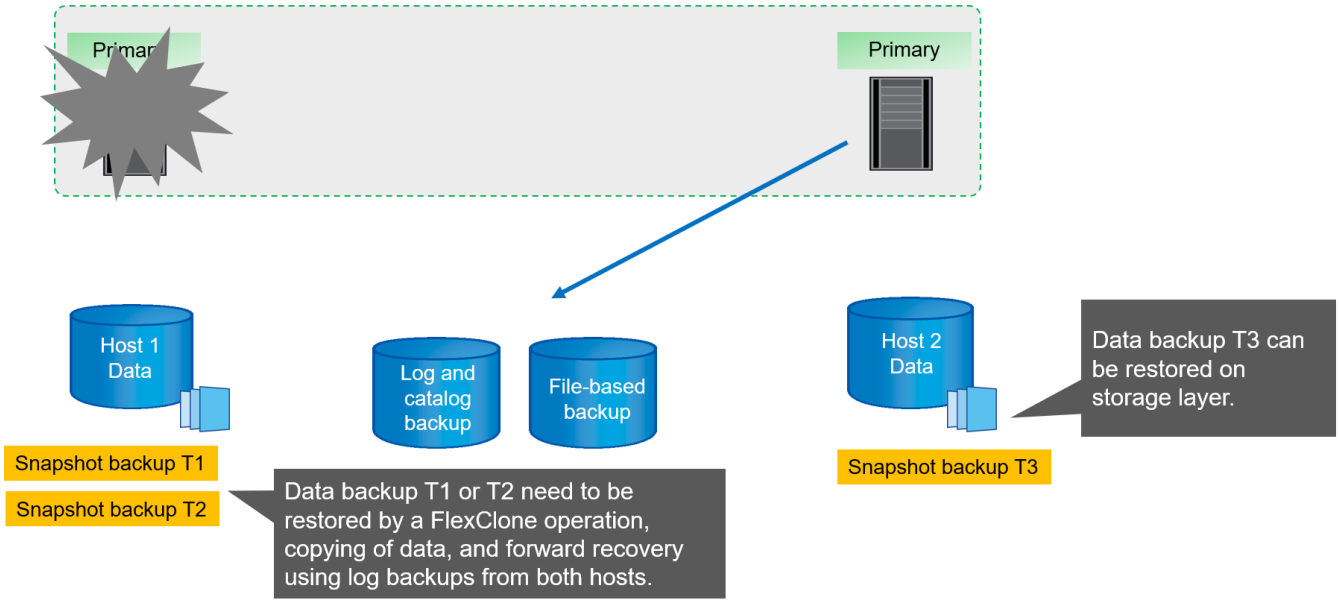
いずれかのバックアップをリストアに使用したり、両方のホストからログバックアップを使用してリカバリを転送したりするには、両方のホストからアクセスできる共有ログバックアップの場所が必要です。共有ストレージボリュームを使用することを推奨します。ただし、ログバックアップのデスティネーションは、共有ボリューム内のサブディレクトリに分ける必要があります。

各 SAP HANA ホストには、独自のストレージボリュームがあります。ストレージベースの Snapshot を使用してバックアップを実行すると、データベースと整合性のある Snapshot がプライマリ SAP HANA ホストのストレージボリューム上に作成されます。




ホスト 2 へのフェイルオーバーが実行されると、ホスト 2 がプライマリホストになり、ホスト 2 でバックアップが実行され、ホスト 2 のストレージボリュームに Snapshot バックアップが作成されます。

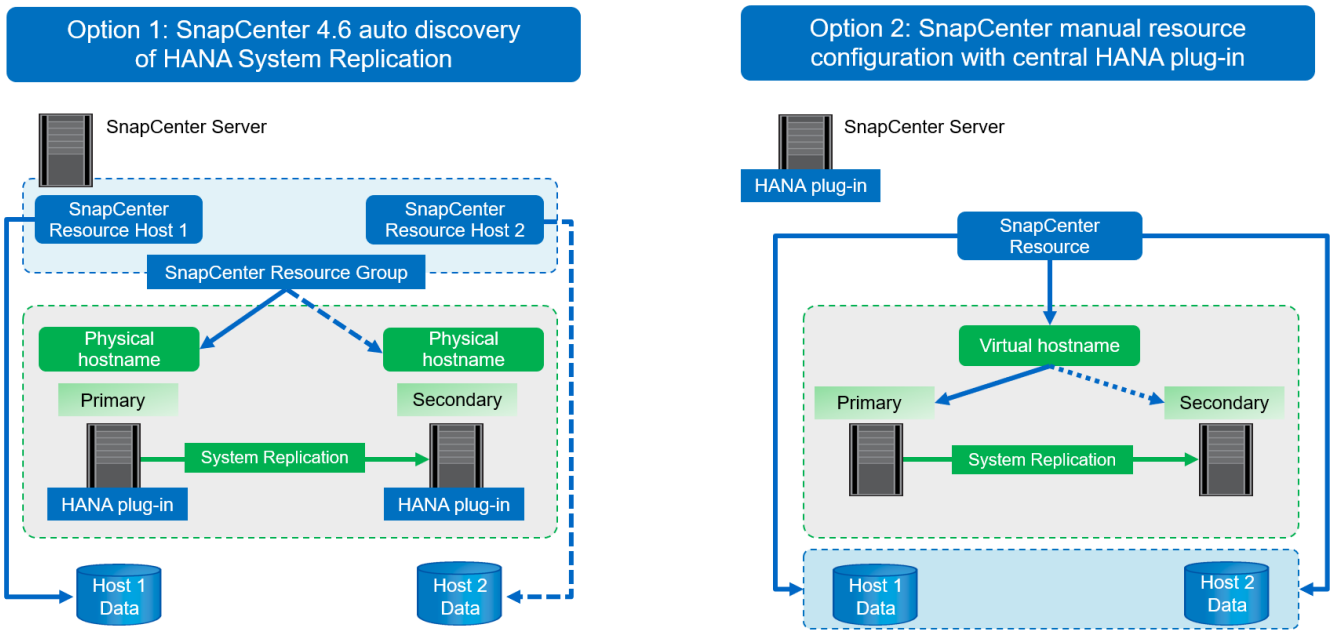
ホスト 2 で作成されたバックアップは、ストレージレイヤで直接リストアできます。ホスト 1 に作成したバックアップを使用する場合は、ホスト 1 のストレージボリュームからホスト 2 のストレージボリュームにバックアップをコピーする必要があります。フォワードリカバリでは、両方のホストからのログバックアップが使用されます。



## SAP システムレプリケーションの SnapCenter 設定オプション

SAP HANA システムレプリケーション環境で NetApp SnapCenter ソフトウェアを使用してデータ保護を設定するには、次の 2 つの方法があります。

- SnapCenter リソースグループ。 SAP HANA ホストと SnapCenter バージョン 4.6 以降を使用した自動検出の両方が含まれます。
- 仮想 IP アドレスを使用する、両方の SAP HANA ホスト用の単一の SnapCenter リソース。




SnapCenter 4.6 以降では、 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 SnapCenter でサポートされます。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まとめられ、プライマリまたはセカンダリのホストが SnapCenter によって自動的に識別され、必要なバックアップ処理が適宜実行されます。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るため、現在のセカンダリホストでも古いバックアップを削除できます。

両方の SAP HANA ホストに単一リソース構成を使用する場合、単一の SnapCenter リソースは、 SAP HANA システムレプリケーションホストの仮想 IP アドレスを使用して構成されます。SAP HANA ホストの両方のデータボリュームが SnapCenter リソースに含まれています。SnapCenter のリソースは 1 つであるため、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管理は、現在プライマリとセカンダリのどちらのホストにも依存しません。このオプションは、すべての SnapCenter リリースで使用できます。

次の表に、 2 つの設定オプションの主な違いをまとめます。

| | **SnapCenter 4.6** を使用したリソースグループ | 単一の **SnapCenter** リソースと仮想 **IP** アドレス |
|---|---|---|
| バックアップ処理（ Snapshot およびファイルベース） | リソースグループ内のプライマリホストの自動識別 | 仮想 IP アドレスを自動的に使用する |
| 保持管理（ Snapshot とファイルベース） | 両方のホストで自動的に実行されます | 単一のリソースを自動的に使用します |

| | **SnapCenter 4.6** を使用したリソースグループ | 単一の **SnapCenter** リソースと仮想 **IP** アドレス |
|---|---|---|
| バックアップ容量の要件 | バックアップはプライマリホストボリュームでのみ作成されます | バックアップは両方のホストボリュームで常に作成されます。2 番目のホストのバックアップはクラッシュ整合性のみであり、ロールフォワードには使用できません。 |
| リストア処理を実行します | 現在のアクティブホストのバックアップをリストア処理に使用できます | リストアに使用できる有効なバックアップを特定するためのバックアップ前スクリプト |
| リカバリ処理 | 自動検出されたすべてのリソースと同じリカバリオプションを使用できます | 手動でリカバリする必要があります |

一般に、リソースグループ構成オプションを SnapCenter 4.6 に設定して、 HANA システムのレプリケーションを有効にして HANA システムを保護することを推奨します。単一の SnapCenter リソース構成が必要になるのは、 SnapCenter の処理アプローチが中央のプラグインホストに基づいており、 HANA プラグインが HANA データベースホストに導入されていない場合だけです。

この 2 つのオプションについては、以降のセクションで詳しく説明します。

## リソースグループを使用した **SnapCenter 4.6** の設定

SnapCenter 4.6 では、 HANA システムレプリケーションが設定された HANA システムの自動検出がサポートされます。SnapCenter 4.6 には、バックアップ処理中にプライマリおよびセカンダリの HANA ホストを識別し、両方の HANA ホスト間で保持管理を処理するロジックが含まれています。また、 HANA システムレプリケーション環境でも自動リストアと自動リカバリが利用できるようになりました。

#### **SnapCenter 4.6 HANA** システムレプリケーション環境の構成

次の図に、この章で使用するラボのセットアップを示します。HANA システムレプリケーションを使用して、HANA ホストを 2 台、 HANA を 3 台、 HANA を 4 台構成しました。

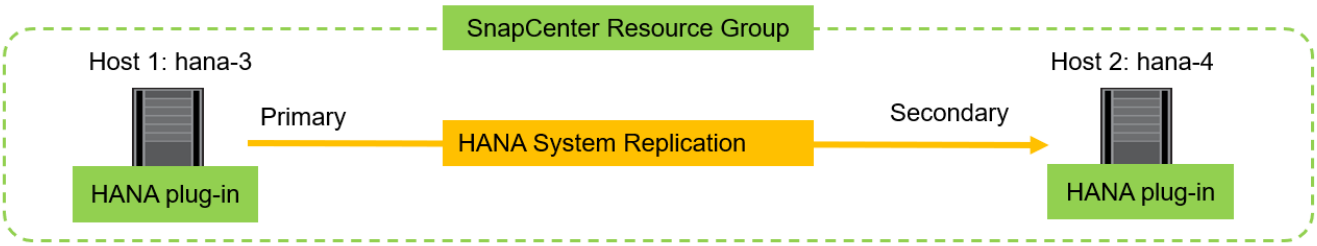
バックアップとリカバリ処理を実行するために必要なPrivilegesを使用して、HANAシステムデータベース用にデータベースユーザ「SnapCenter」"SnapCenter を使用した SAP HANA のバックアップとリカバリ"を作成しました（を参照）。HANA のユーザストアキーは、上記のデータベースユーザを使用して両方のホストで設定する必要があります。

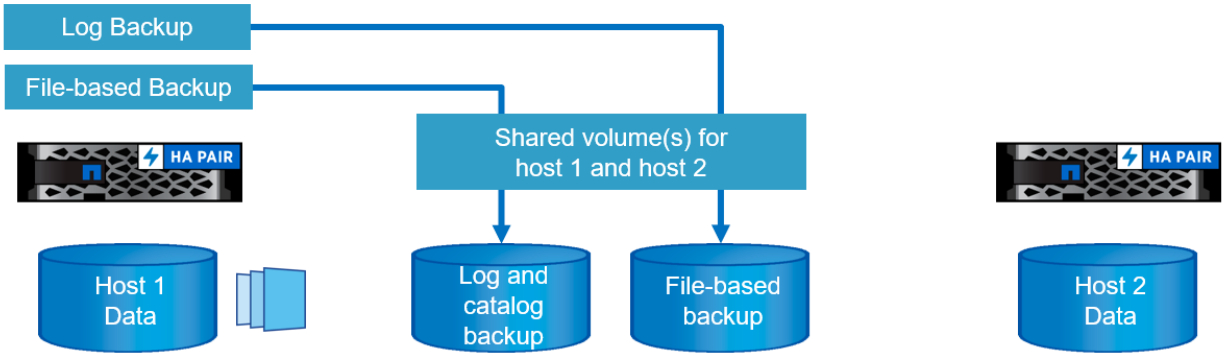
```
ss2adm@hana- 3: / > hdbuserstore set SS2KEY hana- 3:33313 SNAPCENTER
<password>
```

```
ss2adm@hana- 4:/ > hdbuserstore set SS2KEY hana-4:33313 SNAPCENTER
<password>
```

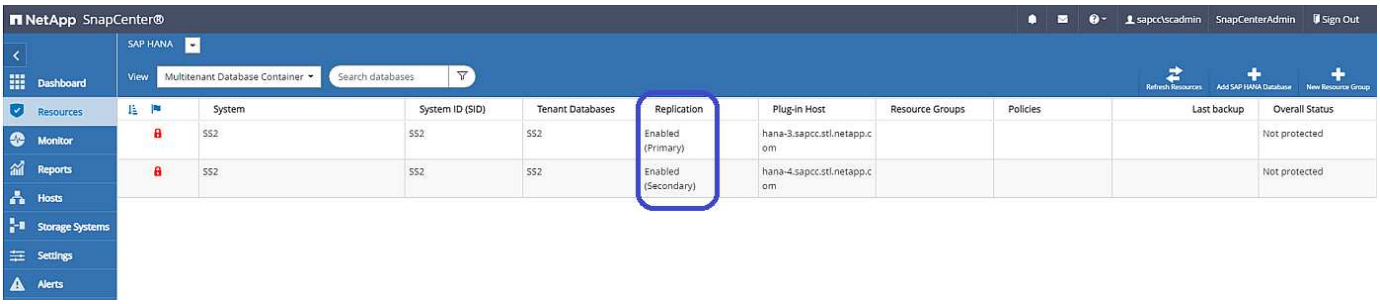
SnapCenter で HANA システムのレプリケーションを設定するには、大まかに見て次の手順を実行する必要があります。

1. HANA プラグインをプライマリホストとセカンダリホストにインストールします。自動検出が実行され、各プライマリホストまたはセカンダリホストで HANA システムのレプリケーションステータスが検出されます。
2. SnapCenter の configure database を実行し 'hdbuserstore キーを指定しますさらに自動検出操作が実行されます。
3. 両方のホストを含むリソースグループを作成し、保護を設定します。

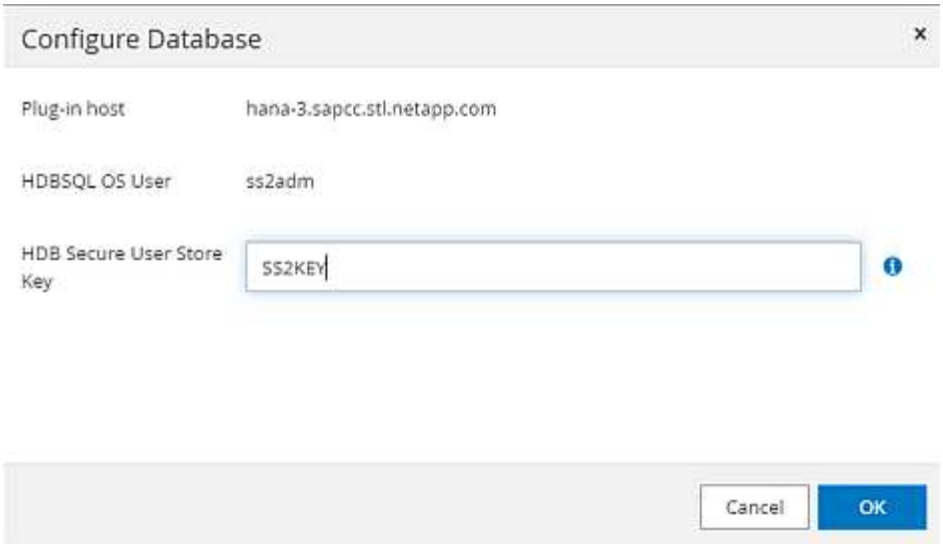


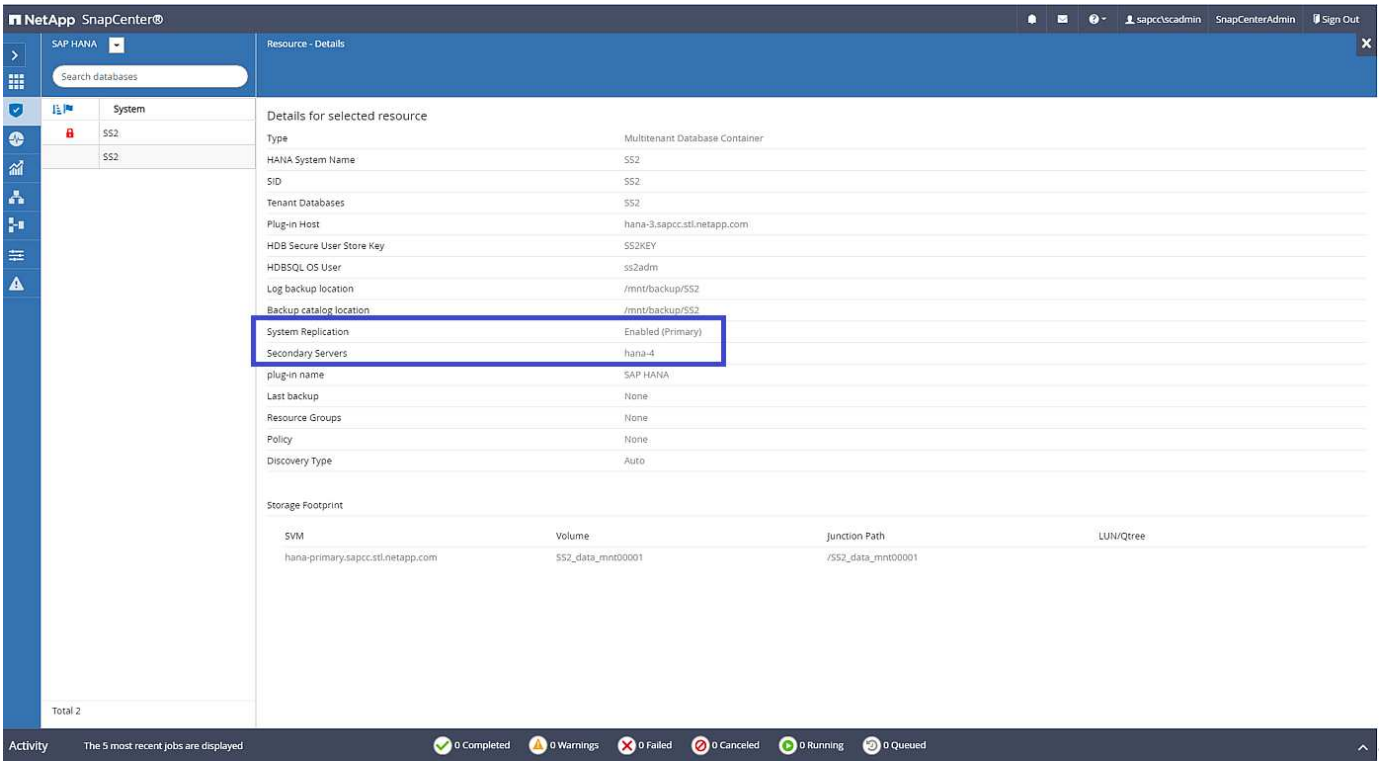

両方の HANA ホストに SnapCenter HANA プラグインをインストールすると、他の自動検出されたリソースと同じように、 HANA システムが SnapCenter リソースビューに表示されます。SnapCenter 4.6 以降では、追加の列に HANA システムレプリケーション（有効 / 無効、プライマリ / セカンダリ）のステータスが表示されます。




リソースをクリックすると、 SnapCenter は HANA システムの HANA ユーザストアキーを要求します。



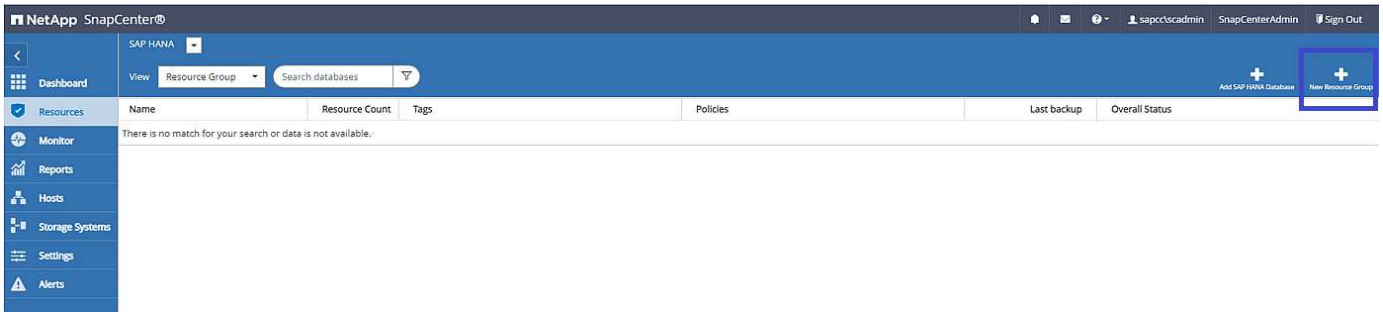

追加の自動検出ステップが実行され、 SnapCenter にリソースの詳細が表示されます。SnapCenter 4.6 では、システムレプリケーションのステータスとセカンダリサーバがこのビューに表示されます。



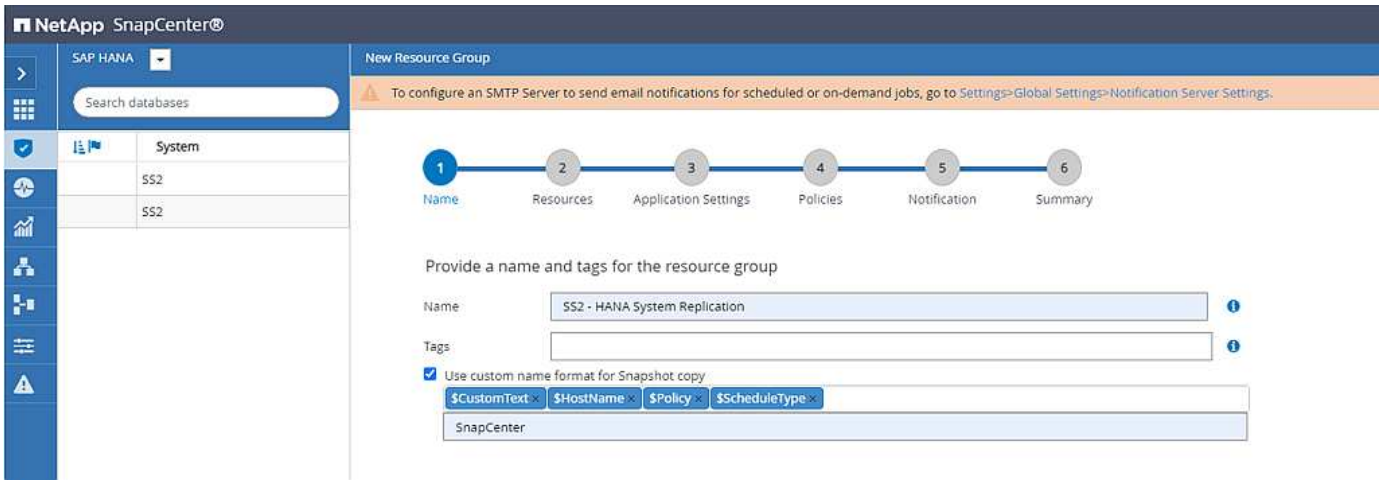

2 つ目の HANA リソースに対して同じ手順を実行すると、自動検出プロセスが完了し、両方の HANA リソースが SnapCenter で構成されます。



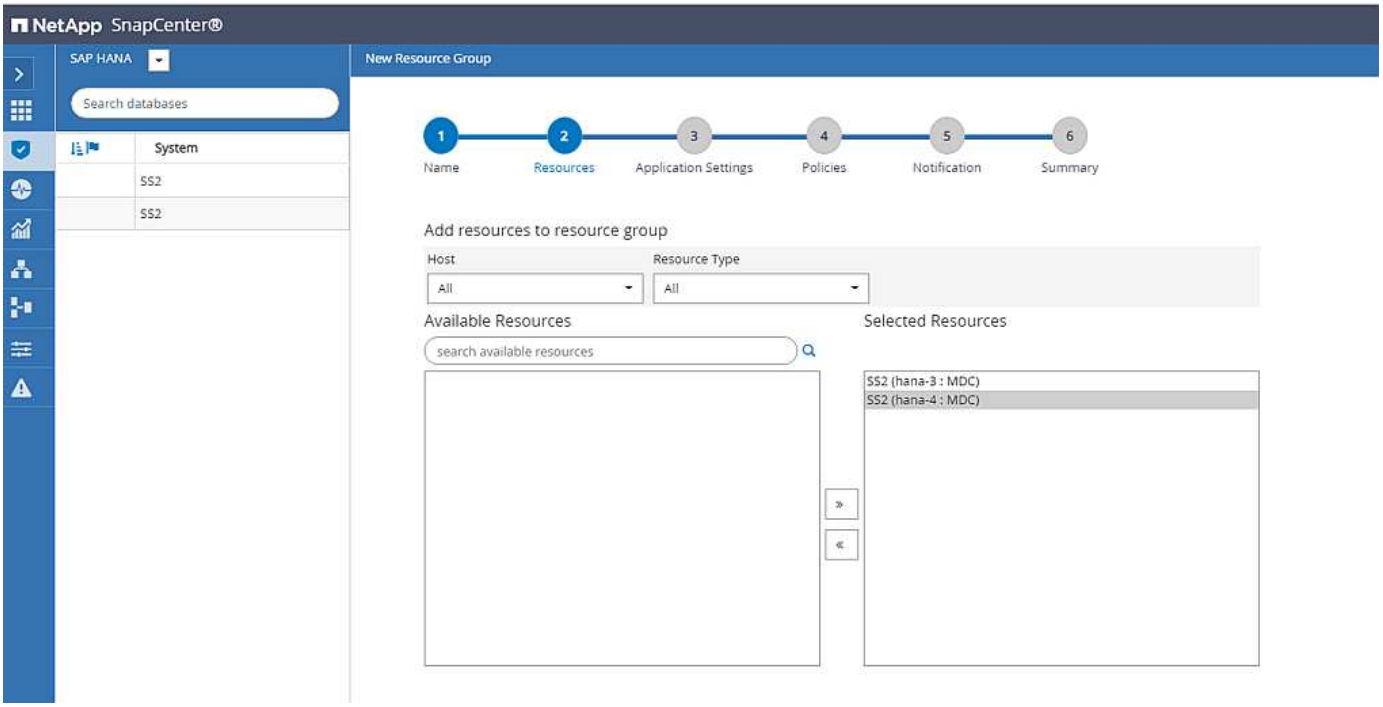

HANA システムレプリケーションを有効にしたシステムでは、両方の HANA リソースを含む SnapCenter リソースグループを設定する必要があります。




Snapshot 名には、ホスト名、ポリシー、スケジュールなどを含めるカスタムの名前形式を使用することを推奨します。

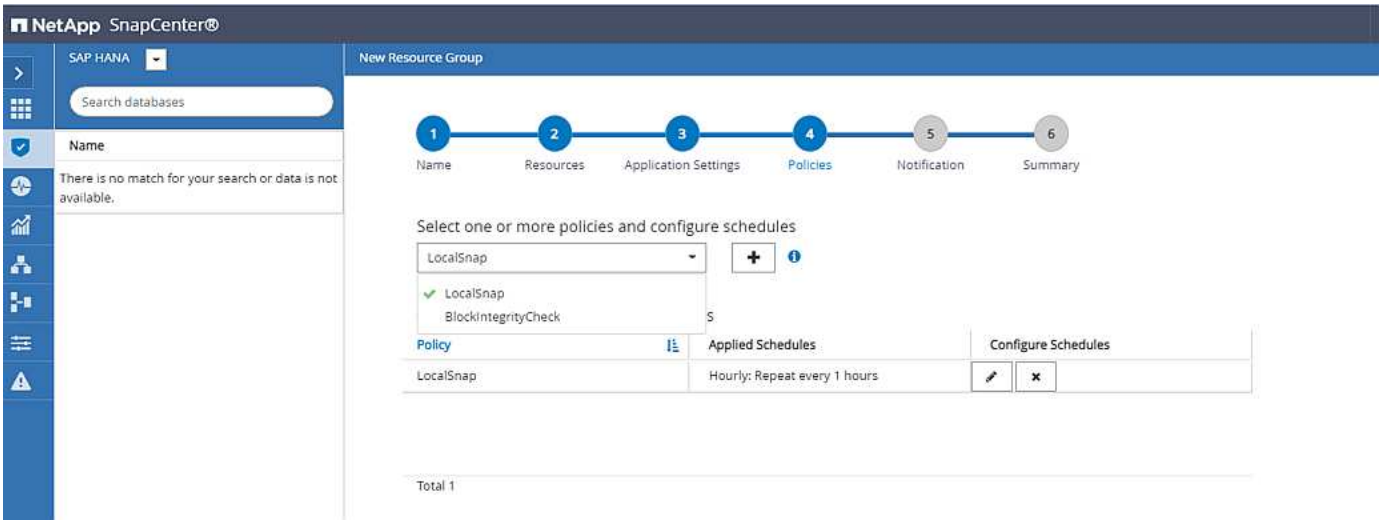



リソースグループに両方の HANA ホストを追加する必要があります。

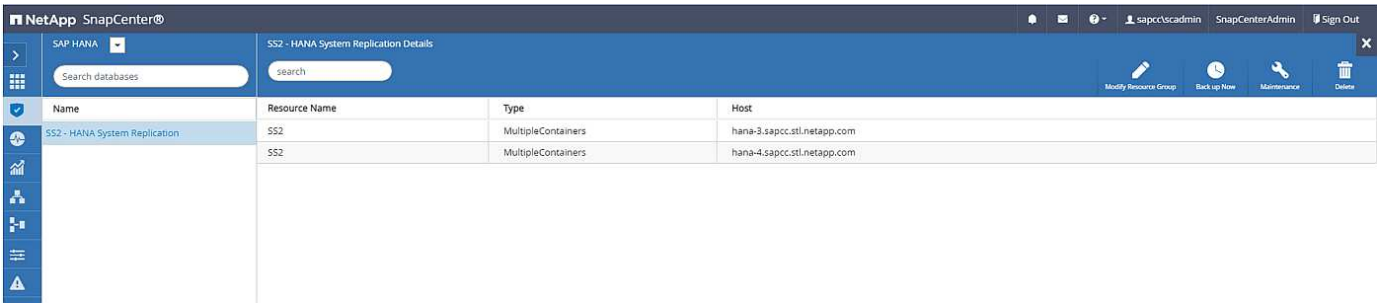



リソースグループにはポリシーとスケジュールが設定されます。

ポリシーで定義された保持設定は、両方の HANA ホストで使用されます。たとえば、ポリシーで保持数が 10 に定義されている場合、両方のホストのバックアップの合計がバックアップ削除の基準として使用されます。SnapCenter は、現在のプライマリホストまたはセカンダリホストに作成された最も古いバックアップを個別に削除します。




これでリソースグループの設定が終了し、バックアップを実行できるようになります。

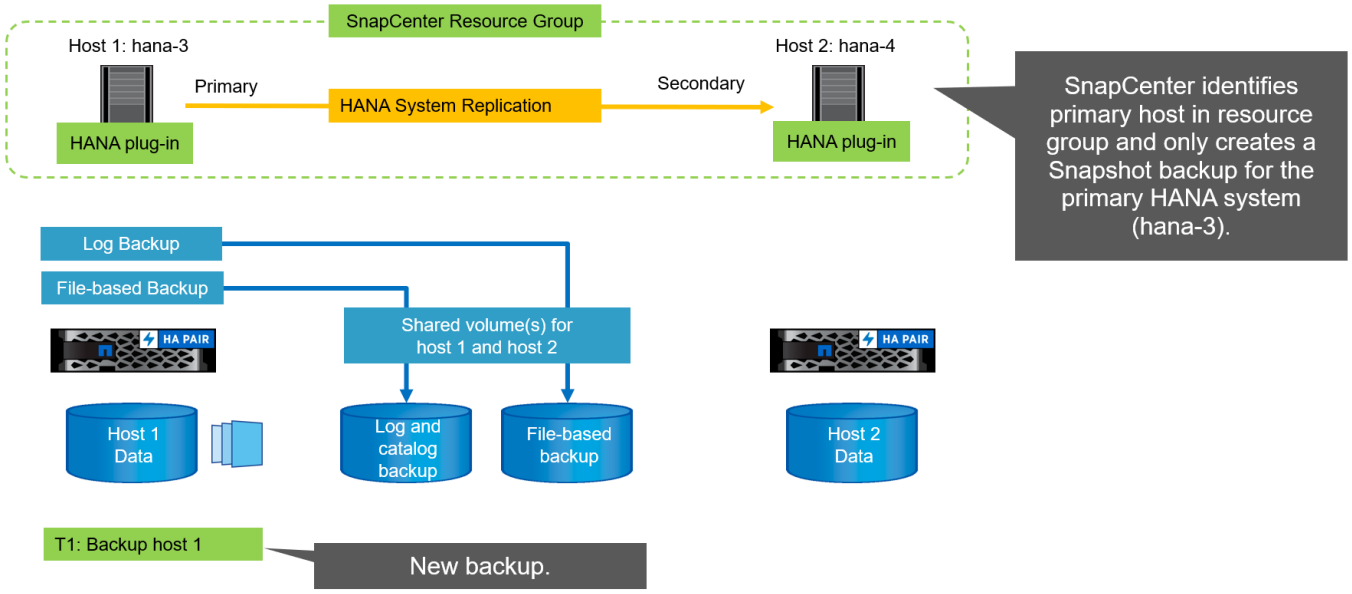




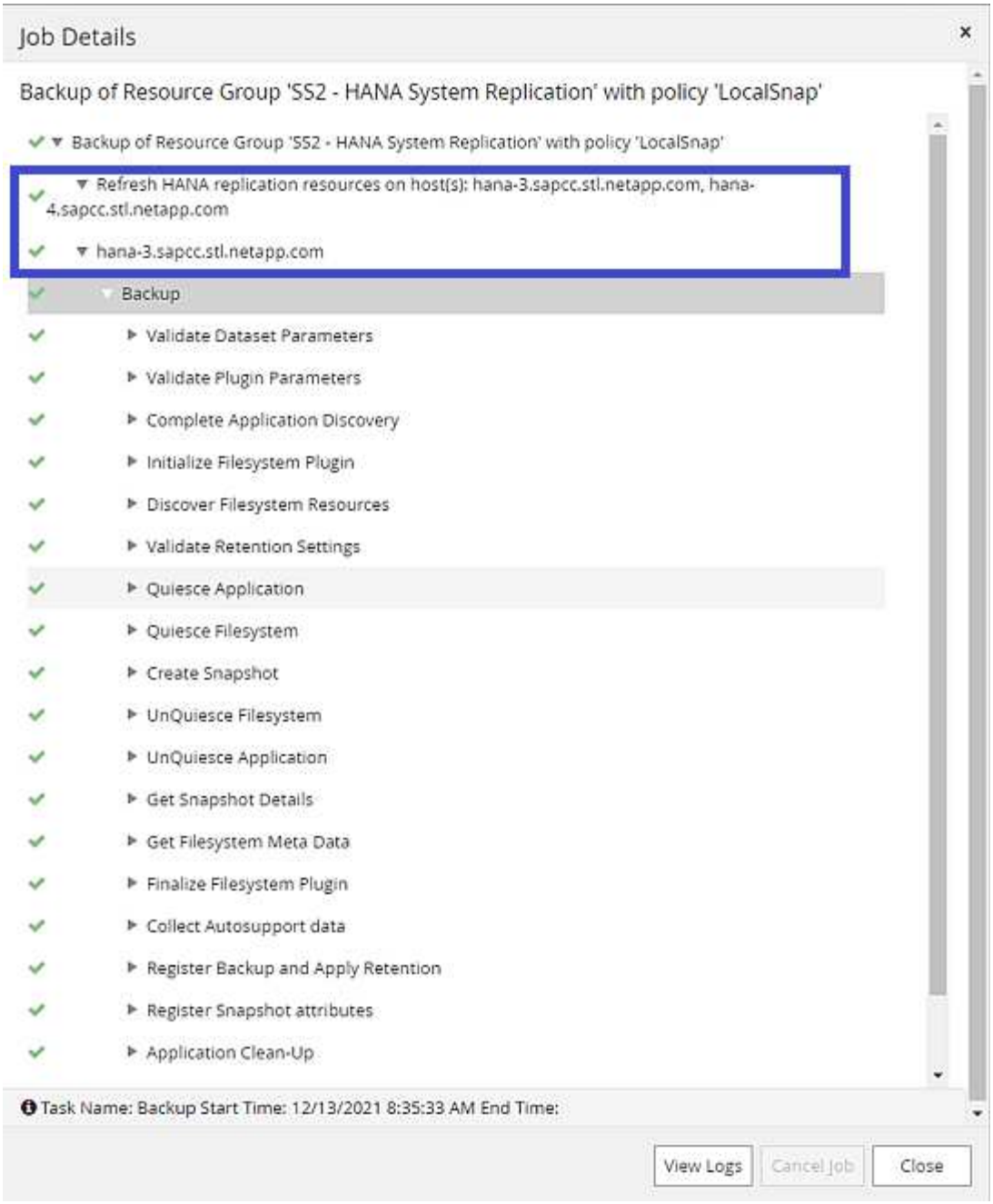


## Snapshot のバックアップ処理

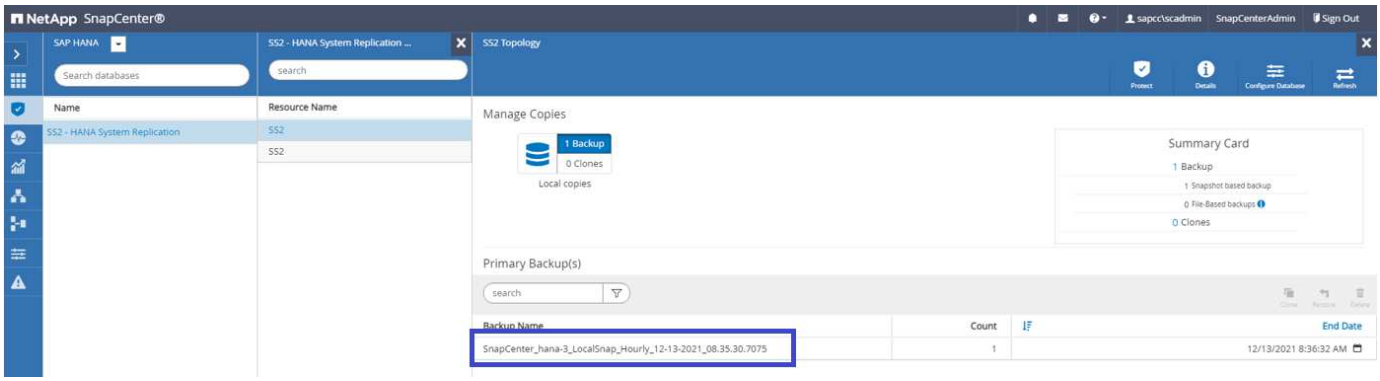
リソースグループのバックアップ処理が実行されると、 SnapCenter はどのホストがプライマリであるかを識別し、プライマリホストでのみバックアップをトリガーします。つまり、プライマリホストのデータボリュームのみが Snapshot されます。この例では、 HANA 3 が現在のプライマリホストであり、このホストでバックアップが実行されています。



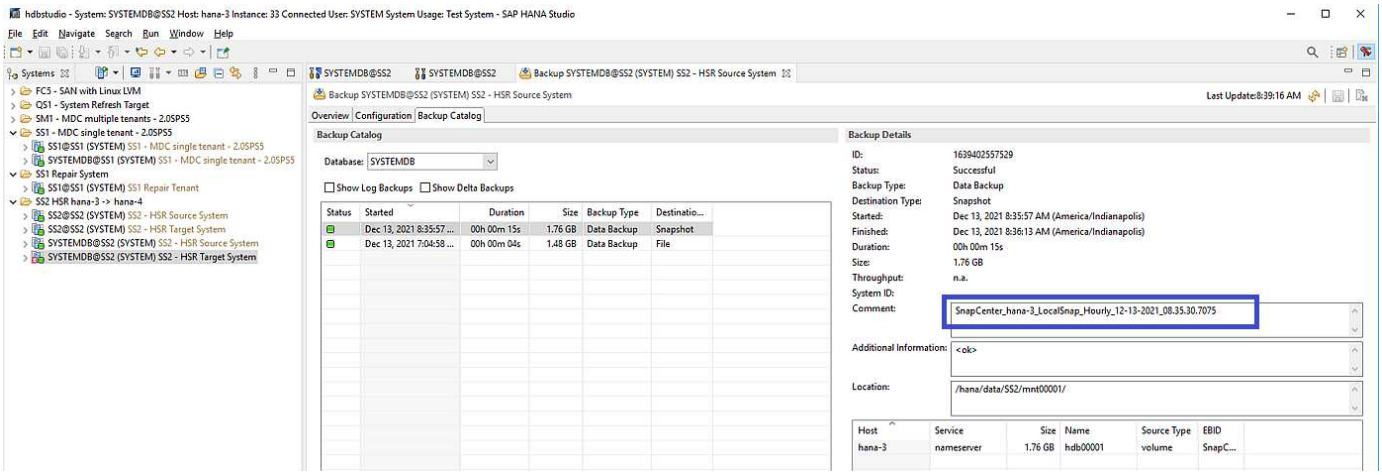

SnapCenter ジョブログには、識別処理と、現在のプライマリホスト HANA でのバックアップの実行が表示されます。




これで、プライマリ HANA リソースに Snapshot バックアップが作成されました。バックアップ名に含まれるホスト名は HANA - 3 と表示されます。

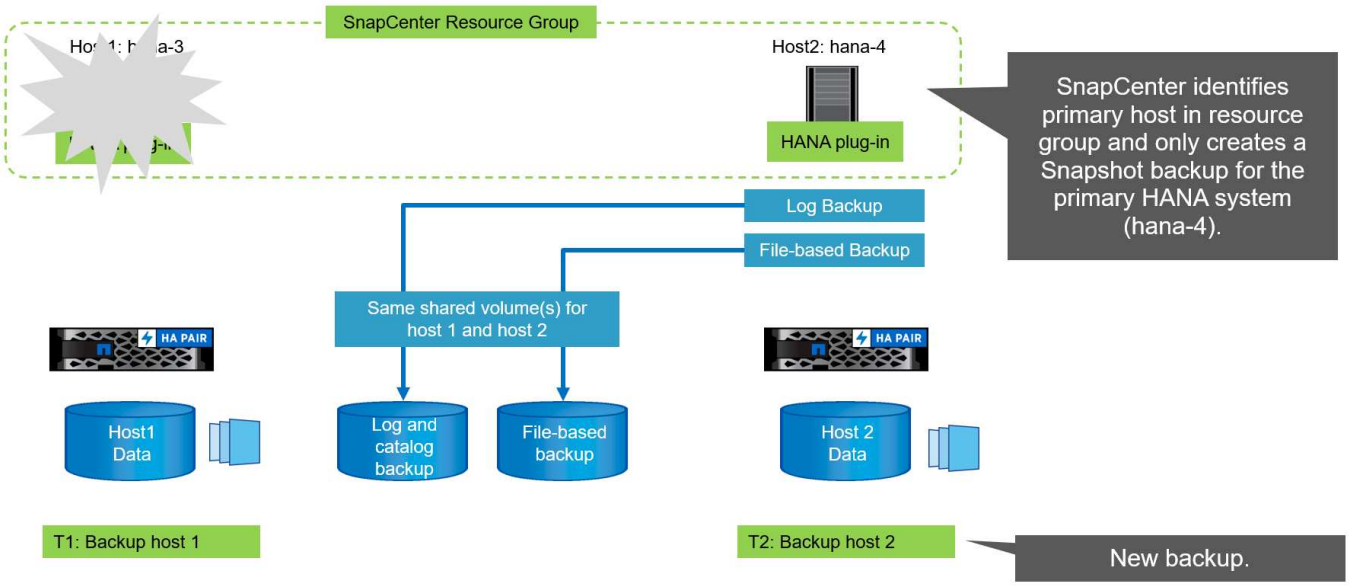


HANA のバックアップカタログにも同じ Snapshot バックアップが表示されます。

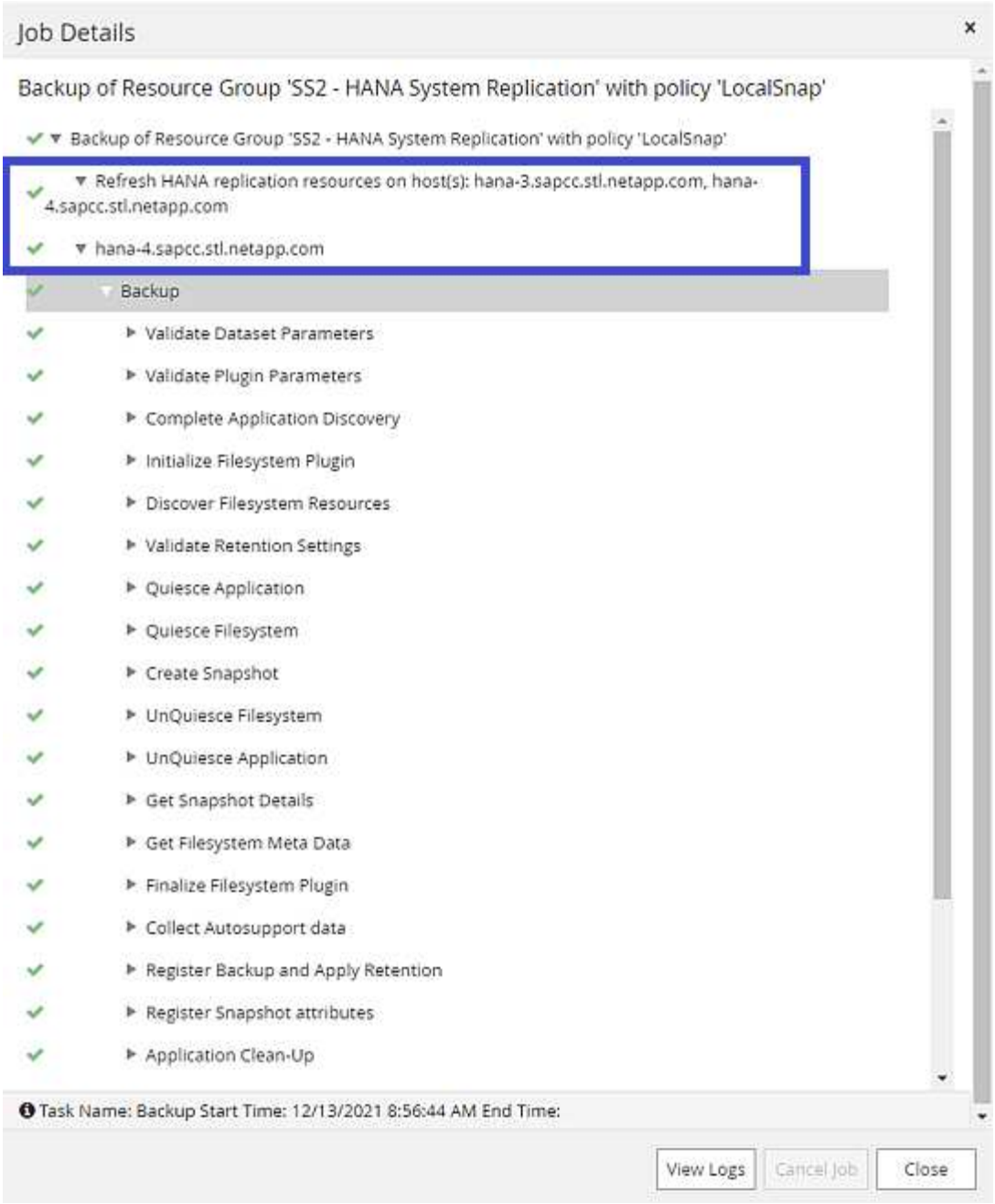



テイクオーバー処理が実行されると、それ以降の SnapCenter バックアップで元のセカンダリホスト（ Hana-4 ）がプライマリとして識別され、 Hana-4 でバックアップ処理が実行されるようになります。ここでも、新しいプライマリホスト（ HANA - 4 ）のデータボリュームのみが Snapshot されています。

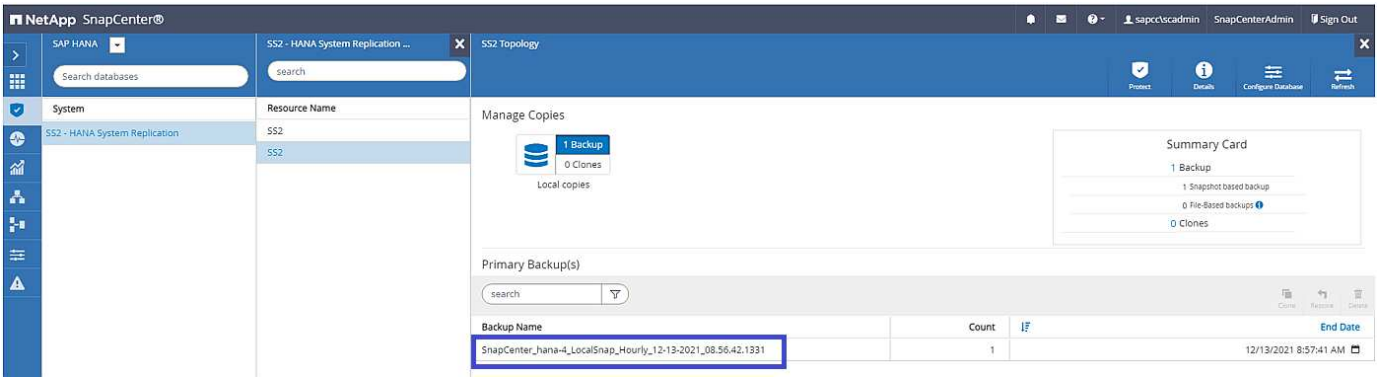
SnapCenter 識別ロジックで対応しているのは、 HANA ホストがプライマリとセカンダリの関係にあるシナリオと、 HANA ホストの 1 つがオフラインになっているシナリオだけです。



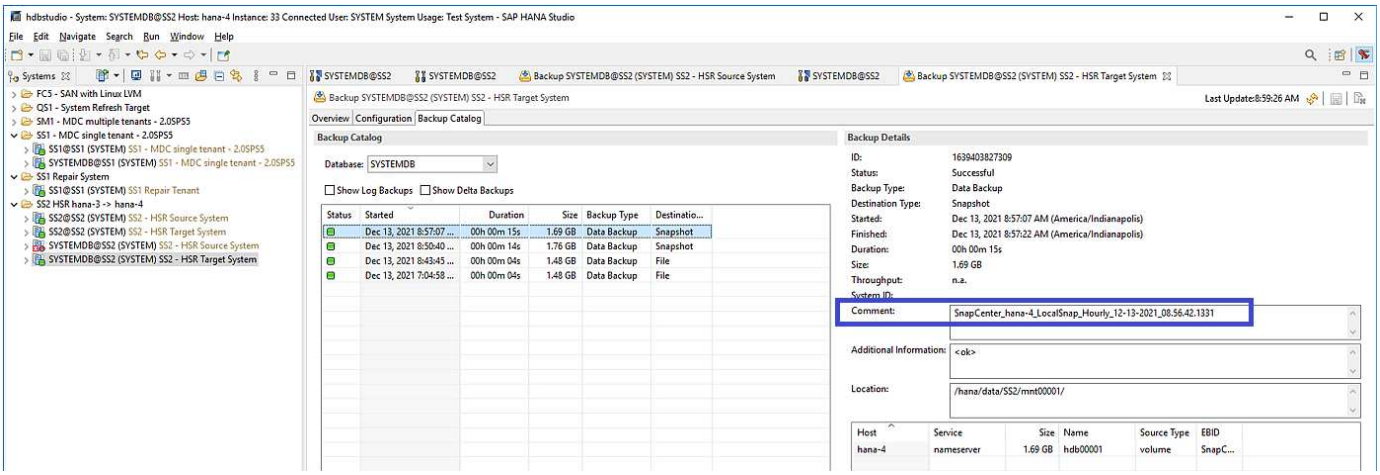

SnapCenter ジョブログには、識別処理と、現在のプライマリホスト HANA でのバックアップの実行が表示されます。




これで、プライマリ HANA リソースに Snapshot バックアップが作成されました。バックアップ名に含まれているホスト名は、 HANA のホスト名です。



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




ファイルベースのバックアップを使用したブロック整合性チェック処理

SnapCenter 4.6 では、ファイルベースのバックアップでブロック整合性チェック処理を実行する場合と同じロジックを使用します。SnapCenter は現在のプライマリ HANA ホストを識別し、このホストに対してファイルベースのバックアップを実行します。保持管理も両方のホスト間で実行されるため、現在プライマリになっているホストに関係なく、最も古いバックアップが削除されます。

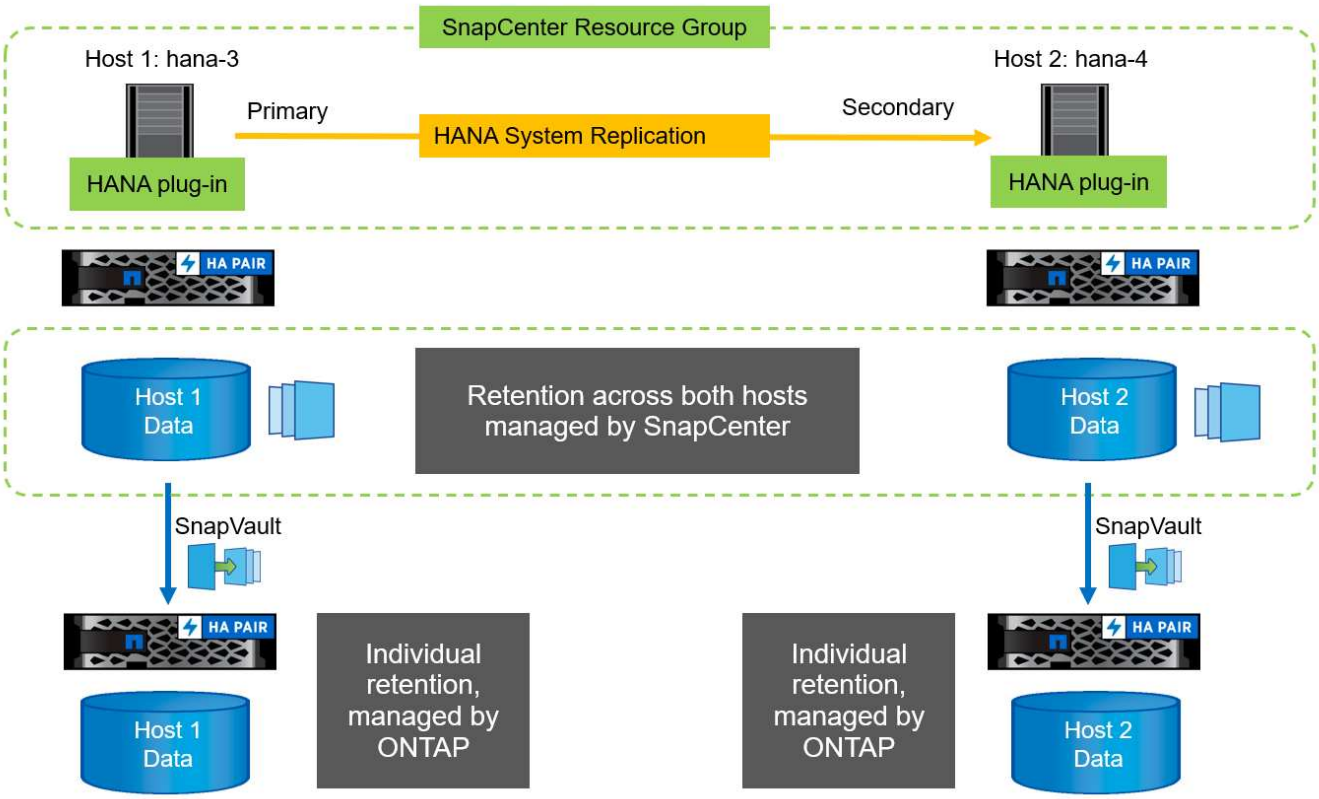
**SnapVault** レプリケーション

テイクオーバー時に透過的なバックアップ処理を可能にし、現在プライマリホストになっている HANA ホストに依存しないようにするには、両方のホストのデータボリュームに SnapVault 関係を設定する必要があります。SnapCenter は、バックアップの実行ごとに、現在のプライマリホストに対して SnapVault 更新処理を実行します。

セカンダリホストへのテイクオーバーが長時間実行されない場合、セカンダリホストでの最初の SnapVault 更新で変更されたブロック数は多くなります。

SnapVault ターゲットの保持管理は ONTAP by SnapCenter の外部で管理されるため、両方の HANA ホスト間で処理することはできません。そのため、テイクオーバー前に作成されたバックアップは、以前のセカンダリではバックアップ処理によって削除されません。これらのバックアップは、元のプライマリが再びプライマリになるまで保持されます。これらのバックアップによってログバックアップの保持管理がブロックされないように、 SnapVault ターゲットまたは HANA のバックアップカタログから手動で削除する必要があります。

1 つの SnapVault コピーが同期ポイントとしてブロックされるため、すべての Snapshot コピーのクリーンアップを実行できません。最新の Snapshot コピーも削除する必要がある場合は、 SnapVault レプリケーション関係を削除してください。この場合は、 HANA のバックアップカタログ内のバックアップを削除して、ログのバックアップ保持管理のブロックを解除することを推奨します。



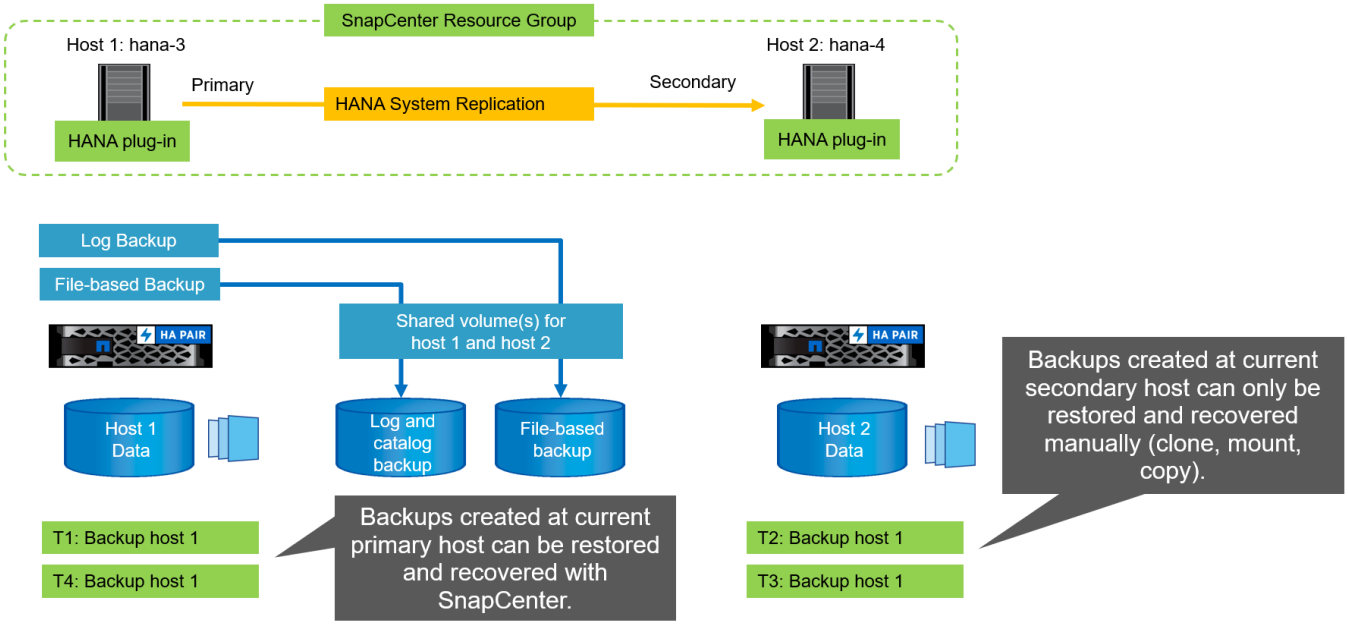

保持管理

SnapCenter 4.6 は、両方の HANA ホストで Snapshot バックアップ、ブロック整合性チェック処理、 HANA バックアップカタログのエントリ、ログバックアップ（無効になっていない場合）の保持を管理できるため、どちらのホストが現在プライマリであるかセカンダリであるかは関係ありません。削除処理が現在のプライマリホストとセカンダリホストのどちらで必要かに関係なく、定義された保持設定に基づいて HANA カタログのバックアップ（データとログ）とエントリが削除されます。つまり、テイクオーバー処理を実行した場合や、レプリケーションが反対方向に設定されている場合は、手動での操作は必要ありません。

SnapVaultレプリケーションがデータ保護戦略の一部である場合は、特定のシナリオについて手動での操作が必要です。詳細については、セクションを参照してください。"SnapVaultレプリケーション"

リストアとリカバリ

次の図は、複数のテイクオーバーが実行され、両方のサイトに Snapshot バックアップが作成された場合のシナリオを示しています。現在のステータスでは、ホスト HA-3 がプライマリホスト、最新のバックアップは T4 であり、これはホスト HA-3 で作成されています。リストアおよびリカバリ処理を実行する必要がある場合、バックアップ T1 および T4 は SnapCenter のリストアとリカバリに使用できます。ホスト HA-4 （ T2 、 T3 ）で作成されたバックアップは、 SnapCenter を使用してリストアできません。リカバリのために、これらのバックアップを HANA のデータボリュームに手動でコピーする必要があります。




SnapCenter 4.6 リソースグループ構成のリストアおよびリカバリ操作は ' 自動検出されたシステム以外のレプリケーション設定と同じですリストアと自動リカバリのすべてのオプションを使用できます。詳細については、テクニカルレポートを参照して"TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"ください。

もう一方のホストで作成されたバックアップからのリストア処理については、セクションで説明し"他のホストで作成されたバックアップからのリストアとリカバリ"ます。

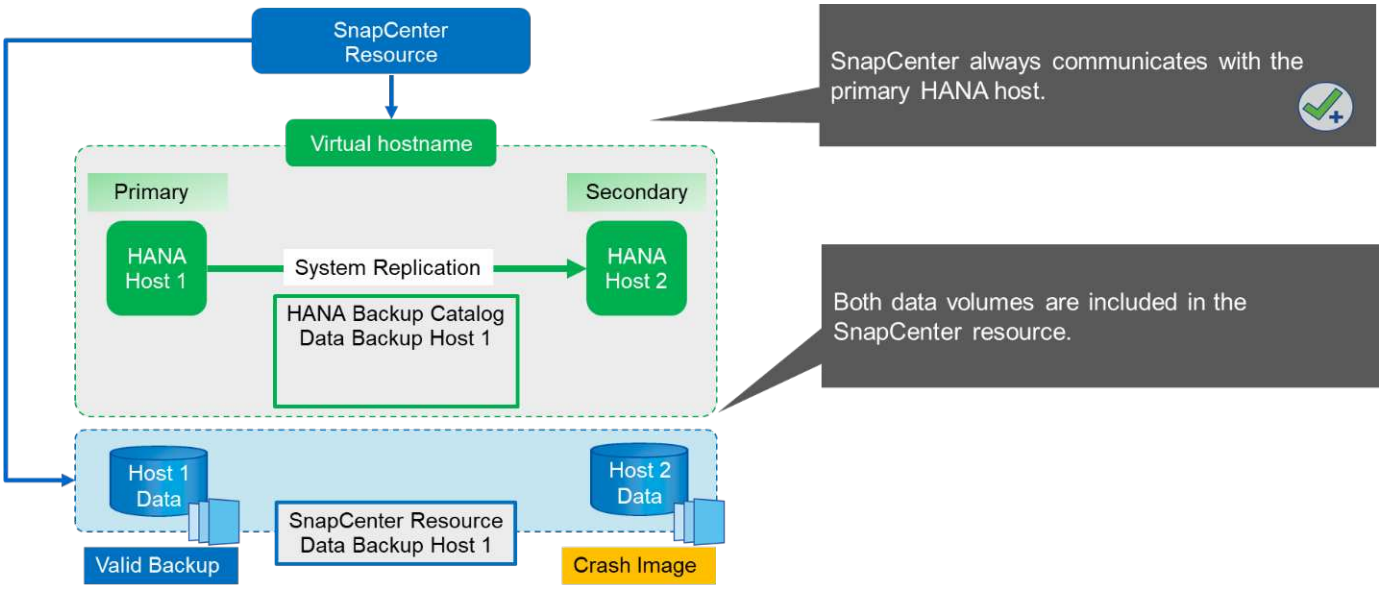
## 単一のリソースを使用する **SnapCenter** 構成

SnapCenter リソースは、 HANA システムレプリケーション環境の仮想 IP アドレス（ホスト名）で構成されます。このアプローチでは、ホスト 1 とホスト 2 のどちらがプライマリかに関係なく、 SnapCenter は常にプライマリホストと通信します。両方の SAP HANA ホストのデータボリュームは、 SnapCenter リソースに含まれています。

仮想 IP アドレスは常にプライマリ SAP HANA ホストにバインドされているものとします。仮想 IP アドレスのフェイルオーバーは、 HANA システムレプリケーションのフェイルオーバーワークフローの一環として、 SnapCenter の外部で実行されます。

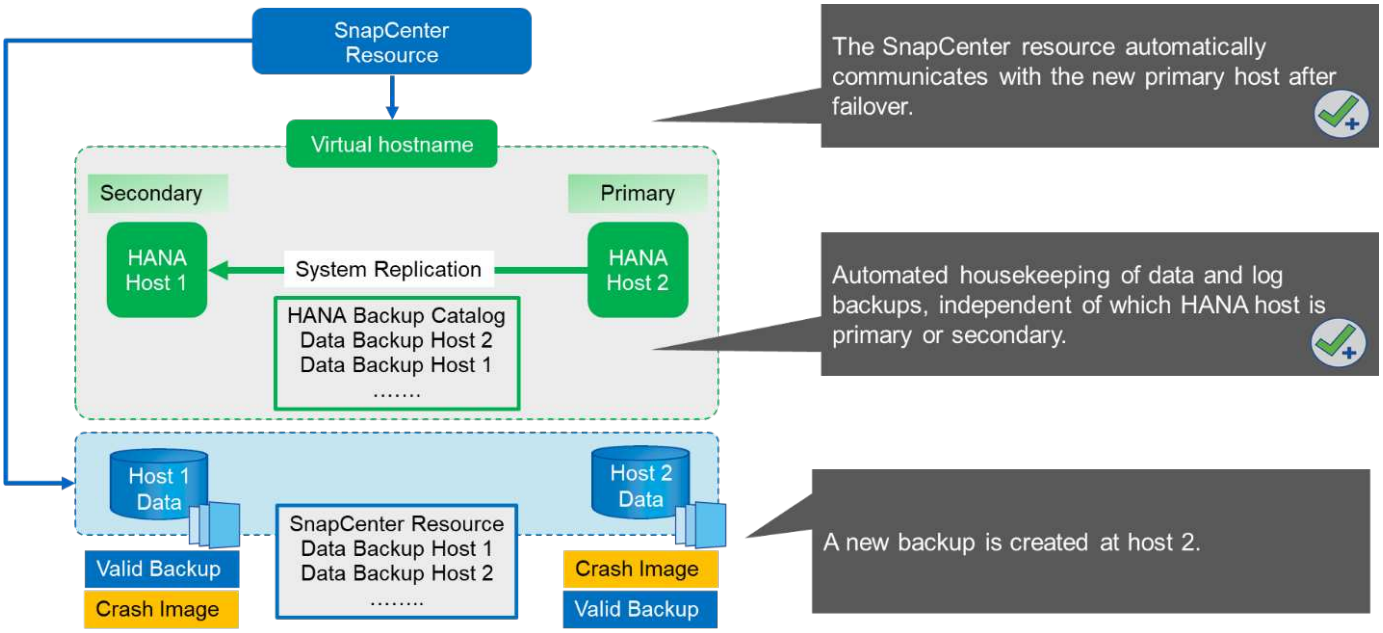
ホスト 1 をプライマリホストとするバックアップを実行すると、データベースと整合性のある Snapshot バックアップがホスト 1 のデータボリュームに作成されます。ホスト 2 のデータボリュームは SnapCenter リソースの一部であるため、このボリュームに対してもう 1 つの Snapshot コピーが作成されます。この Snapshot コピーはデータベースの整合性を維持するのではなく、セカンダリホストのクラッシュイメージにすぎません。

SAP HANA のバックアップカタログと SnapCenter リソースには、ホスト 1 で作成されたバックアップが含まれています。




次の図に、ホスト 2 へのフェイルオーバーおよびホスト 2 からホスト 1 へのレプリケーション後のバックアップ処理を示します。SnapCenter は、 SnapCenter リソースに設定されている仮想 IP アドレスを使用して、ホスト 2 と自動的に通信します。これで、ホスト 2 にバックアップが作成されます。SnapCenter によって 2 つの Snapshot コピーが作成されます。ホスト 2 のデータボリュームにあるデータベースと整合性のあるバックアップと、ホスト 1 のデータボリュームにあるクラッシュイメージの Snapshot コピーです。SAP HANA のバックアップカタログと SnapCenter リソースに、ホスト 1 で作成されたバックアップとホスト 2 で作成されたバックアップが含まれるようになりました。

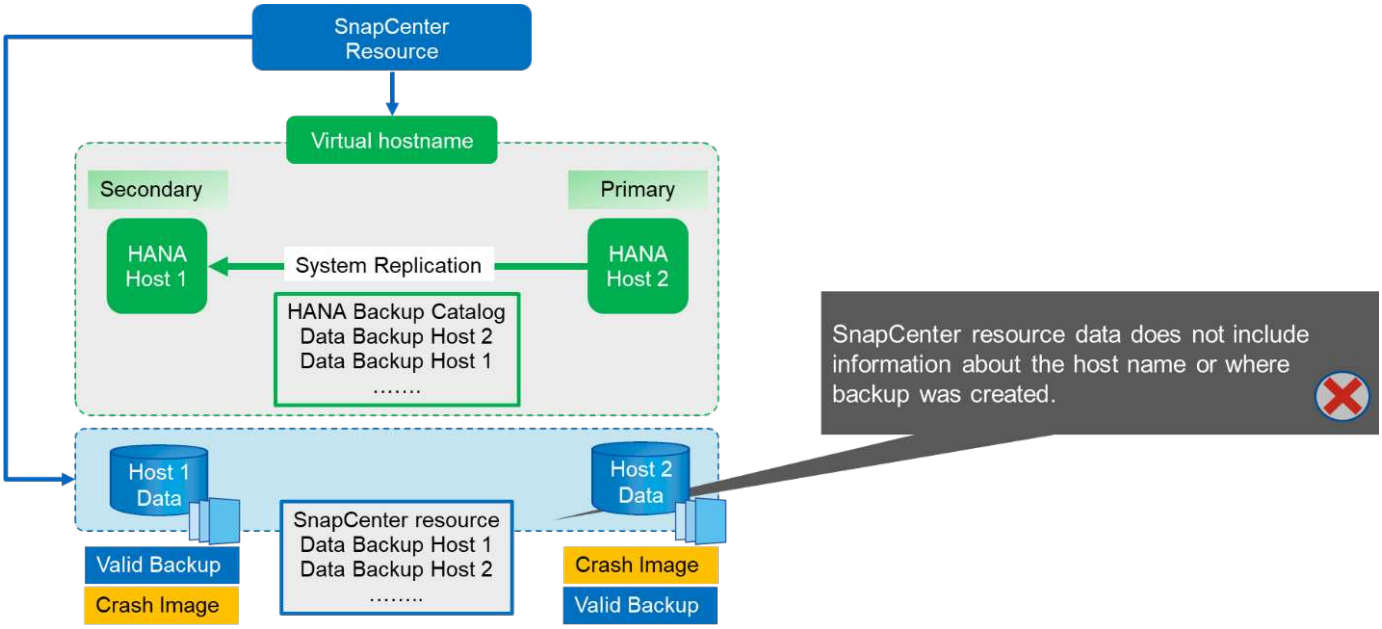
不要なデータバックアップやログバックアップは、定義された SnapCenter 保持ポリシーに基づいて削除され、プライマリまたはセカンダリのホストに関係なく、バックアップは削除されます。




セクションで説明したように、"ストレージ Snapshot バックアップと SAP システムレプリケーション"ストレージベースのSnapshotバックアップを使用したリストア処理は、リストアが必要なバックアップによって異なります。ローカル・ストレージ・ボリュームでリストアを実行できるかどうか、または他のホストのストレージ・ボリュームでリストアを実行する必要があるかどうかを判断するには、バックアップが作成されたホストを特定することが重要です。

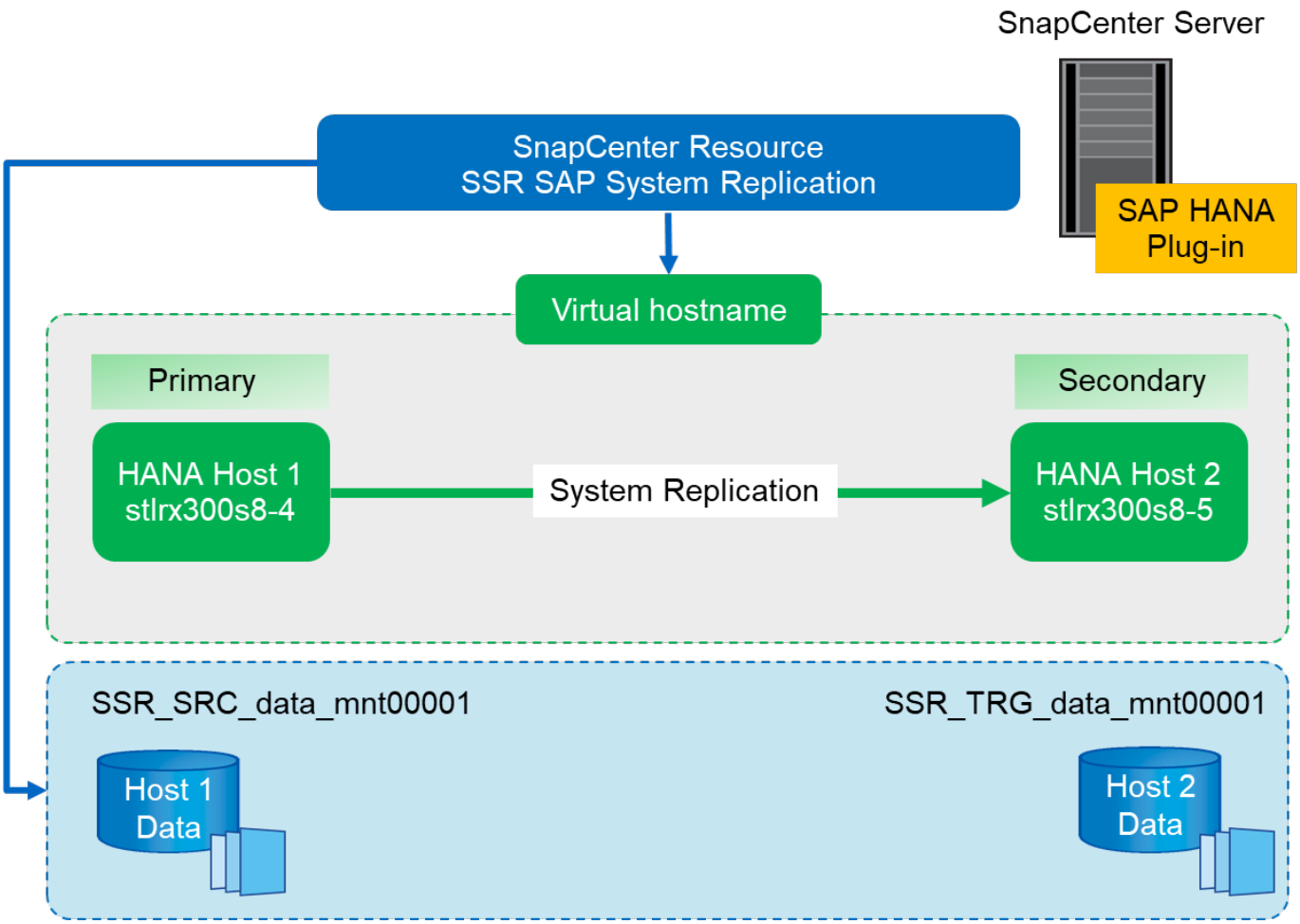
シングルリソースの SnapCenter 構成では、バックアップがどこに作成されたかが SnapCenter で認識されません。そのため、 SnapCenter のバックアップワークフローにバックアップ前のスクリプトを追加して、現在プライマリ SAP HANA ホストになっているホストを特定することを推奨します。

次の図は、バックアップホストの ID を示しています。




**SnapCenter** 構成

次の図は、ラボでのセットアップと必要な SnapCenter 構成の概要を示しています。



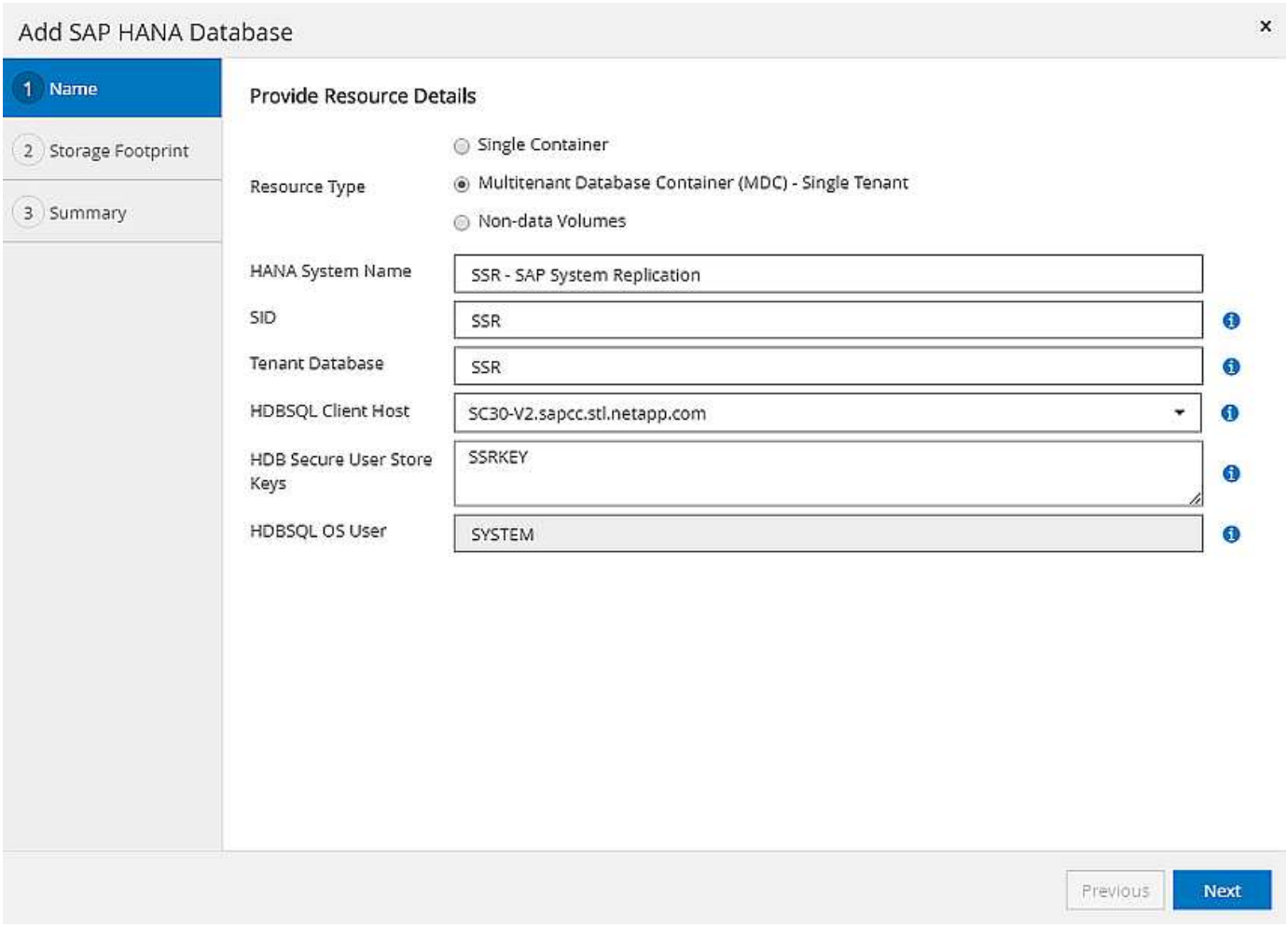

どの SAP HANA ホストがプライマリであっても、 1 つのホストがダウンしている場合でもバックアップ処理を実行するには、 SnapCenter SAP HANA プラグインを中央のプラグインホストに導入する必要があります。今回のラボ環境では、 SnapCenter サーバを中央プラグインホストとして使用し、 SnapCenter サーバに SAP HANA プラグインを導入しました。

HANA データベースに、バックアップ処理を実行するユーザを作成しました。SAP HANA プラグインがインストールされている SnapCenter サーバにユーザストアキーが設定されている。ユーザーストアキーには、SAP HANA システムレプリケーションホスト（ SSR-VIP ）の仮想 IP アドレスが含まれます。

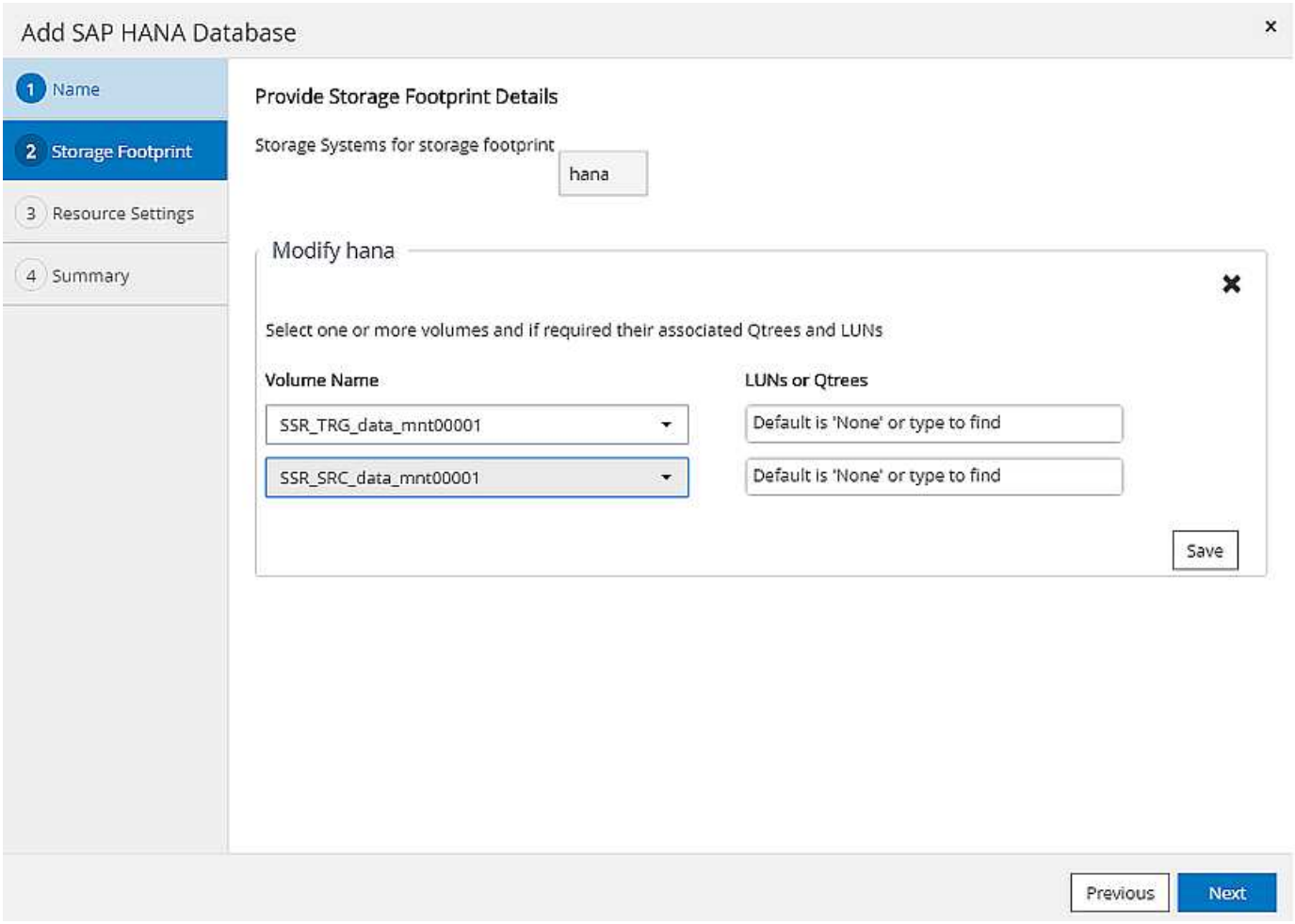
```
hdbuserstore.exe -u SYSTEM set SSRKEY ssr-vip:31013 SNAPCENTER <password>
```

SAP HANAプラグインの導入オプションとユーザストアの設定の詳細については、テクニカルレポートTR-4614：を参照"SnapCenter を使用した SAP HANA のバックアップとリカバリ"してください。

SnapCenter では ' 次の図に示すように ' リソースは ' 前に構成されたユーザー・ストア・キーと SnapCenter サーバを 'hdbsql' 通信ホストとして構成されます

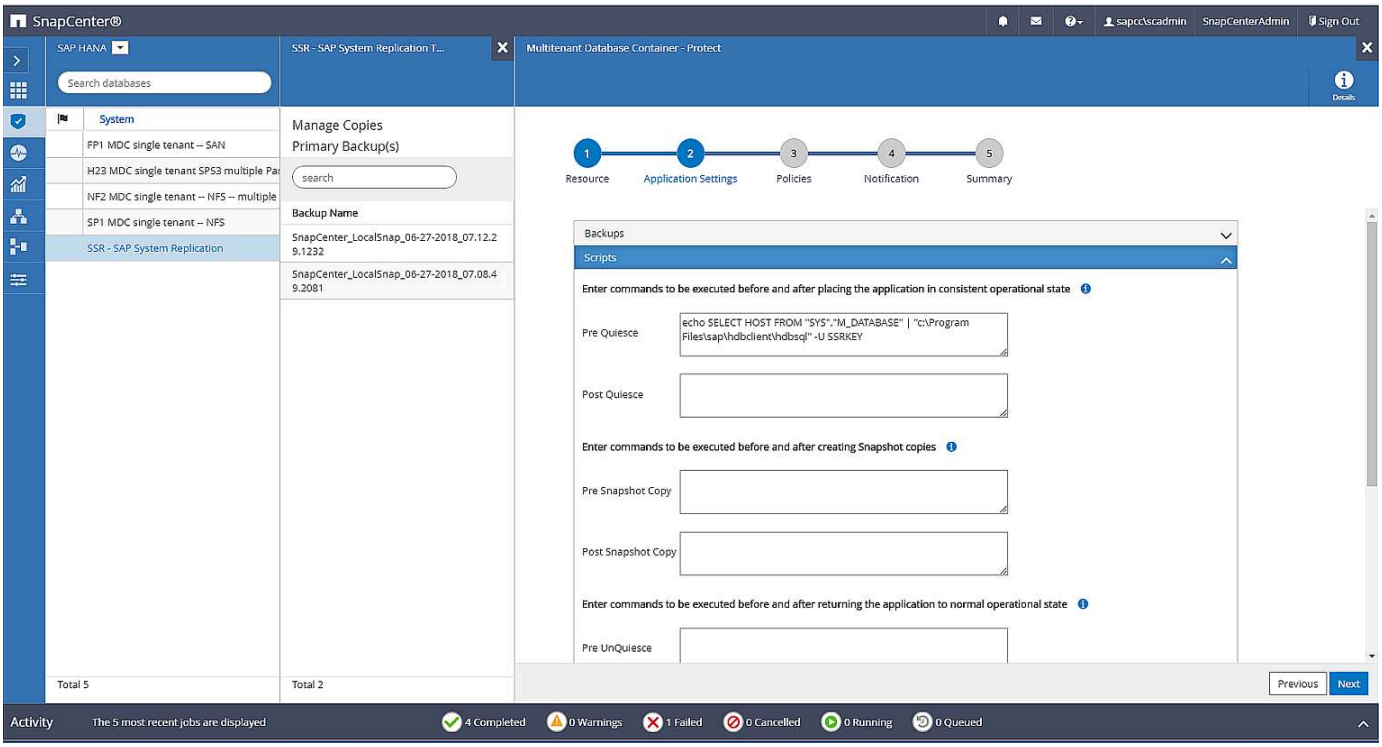



次の図に示すように、両方の SAP HANA ホストのデータボリュームがストレージ設置面積構成に含まれています。




前述したように、 SnapCenter はバックアップがどこで作成されたかを認識しません。したがって、 SnapCenter バックアップワークフローにバックアップ前のスクリプトを追加して、現在プライマリ SAP HANA ホストとなっているホストを特定することを推奨します。この識別は、次の図に示すように、バックアップワークフローに追加された SQL ステートメントを使用して実行できます。

```
Select host from “SYS”.M_DATABASE
```

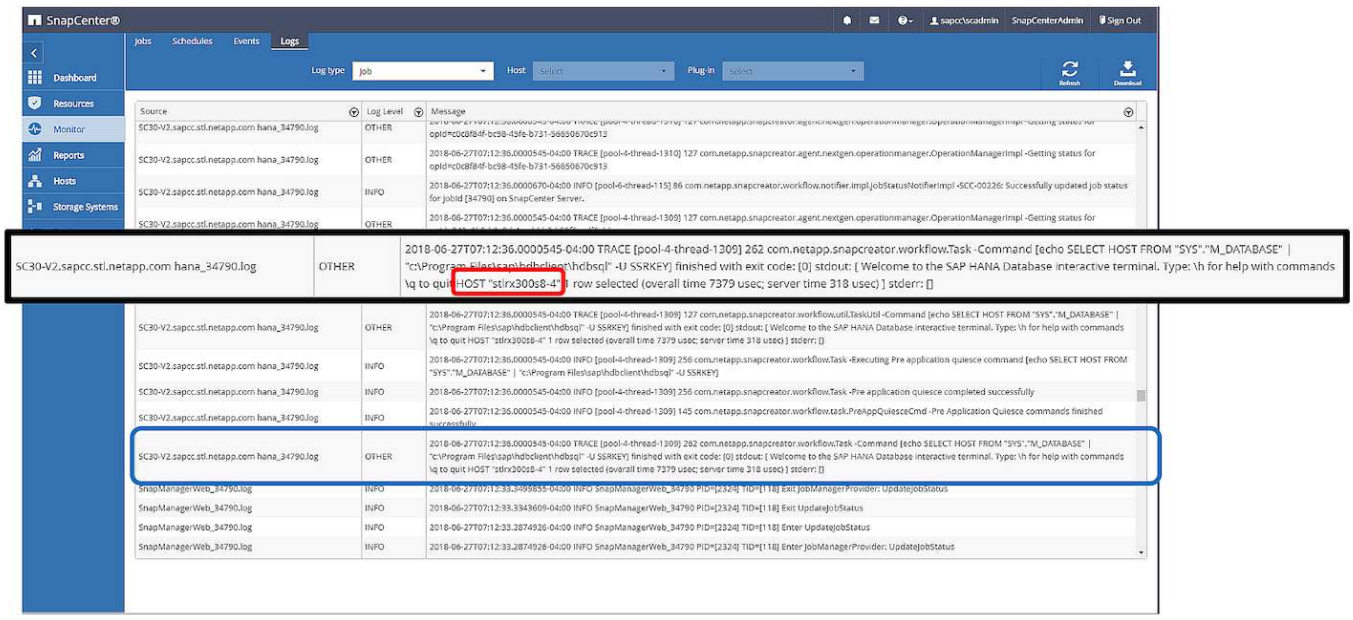



## SnapCenter バックアップ処理

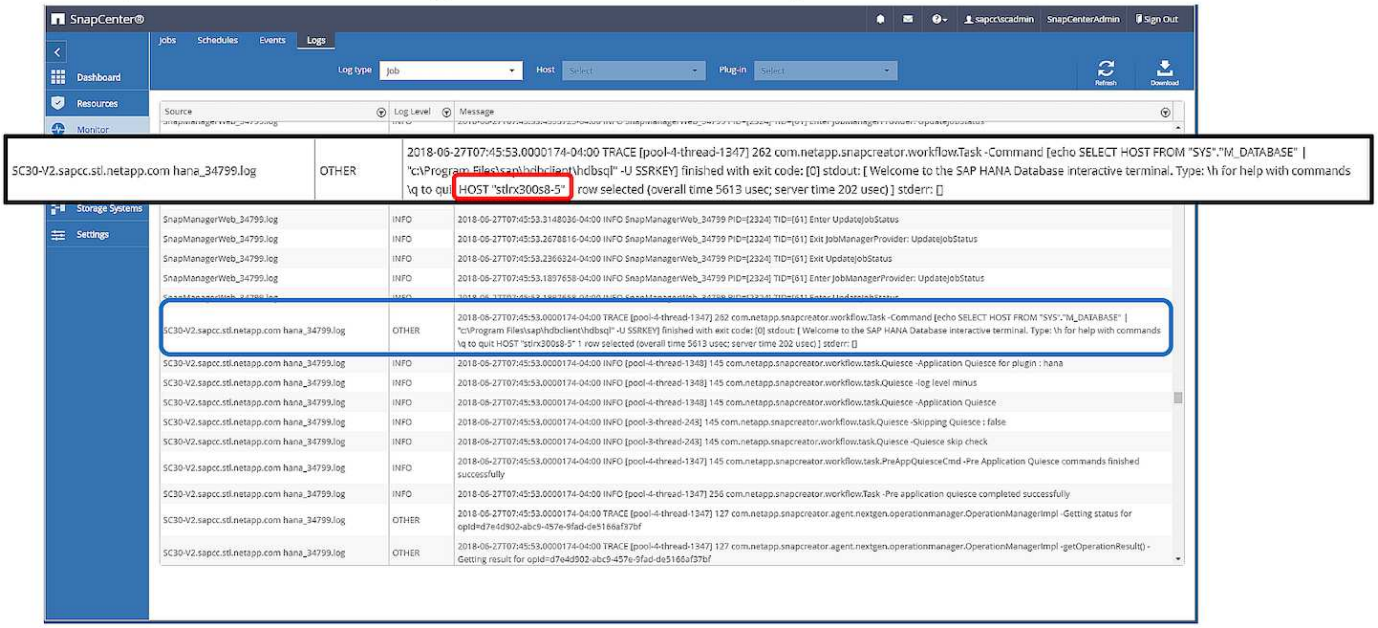
バックアップ処理が通常どおり実行されるようになりました。不要なデータバックアップとログバックアップの削除は、プライマリまたはセカンダリの SAP HANA ホストとは無関係に実行されます。

バックアップジョブログには SQL ステートメントの出力が含まれており、バックアップが作成された SAP HANA ホストを特定できます。

次の図に、ホスト 1 をプライマリホストとするバックアップジョブログを示します。

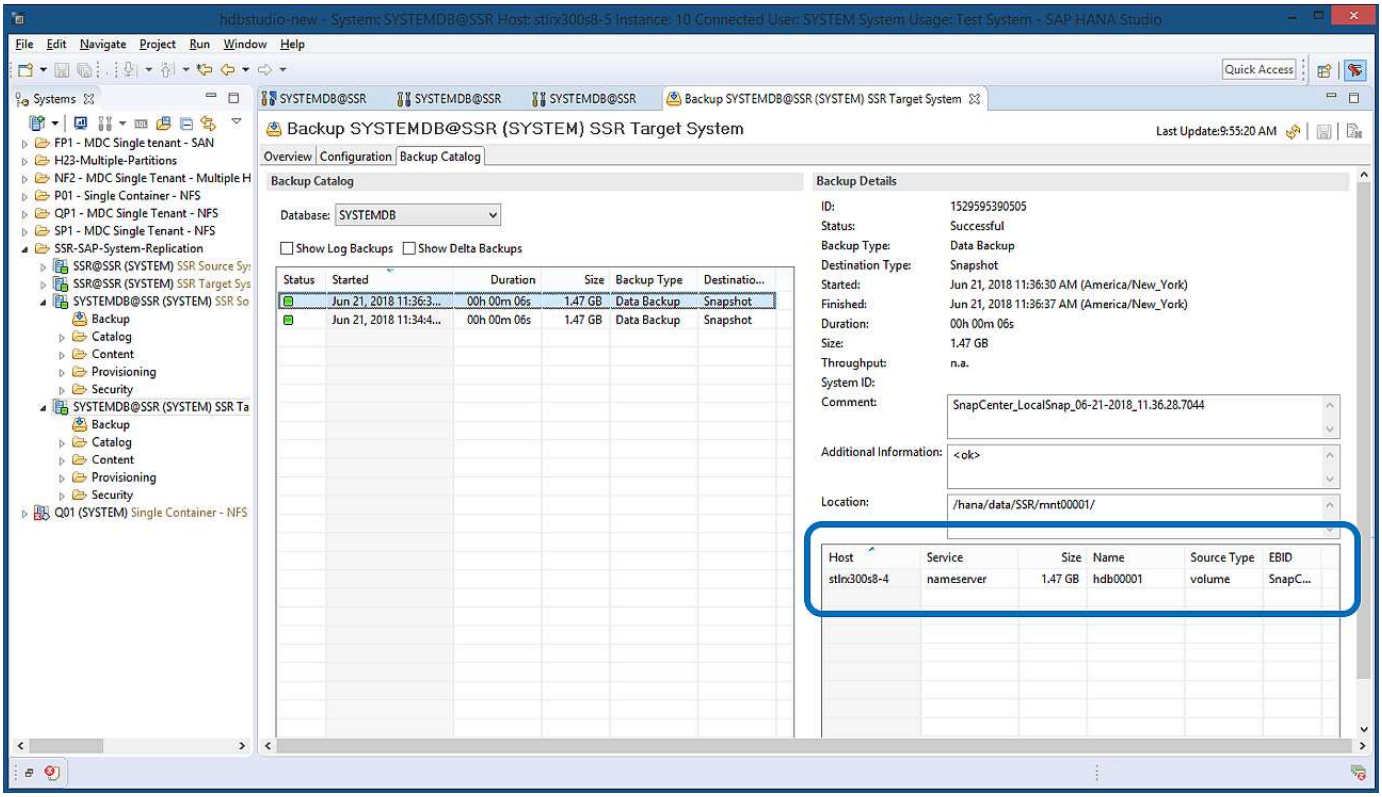



この図は、ホスト 2 がプライマリホストであるバックアップジョブログを示しています。




次の図は、 SAP HANA Studio の SAP HANA バックアップカタログを示しています。SAP HANA データベースがオンラインの場合、バックアップが作成された SAP HANA ホストが SAP HANA Studio に表示されます。

リストア処理とリカバリ処理で使用されるファイルシステム上の SAP HANA バックアップカタログに、バックアップが作成されたホスト名は含まれません。データベースがダウンしているときにホストを識別する唯一の方法は、バックアップカタログのエントリと、両方の SAP HANA ホストの「 backup.log 」ファイルを組み合わせることです。



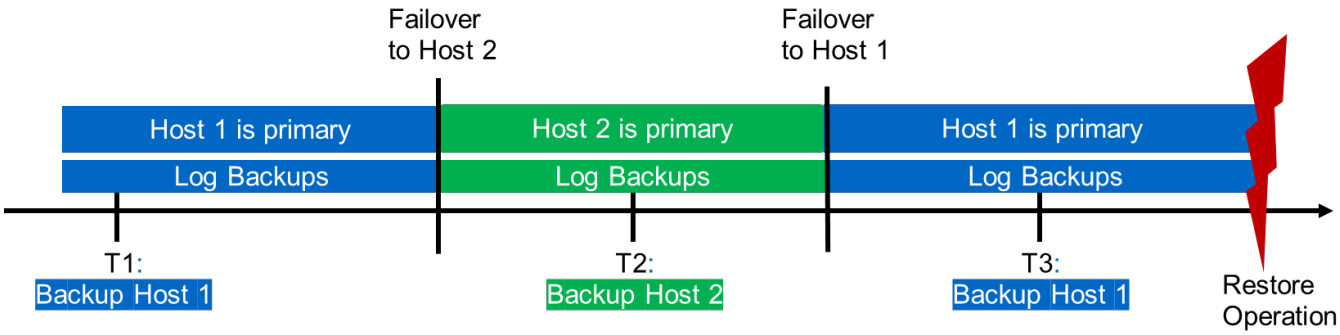
リストアとリカバリ

前述したように、必要なリストア処理を定義するために、選択したバックアップの作成先を特定できる必要があります。SAP HANA データベースがオンラインのままの場合は、 SAP HANA Studio を使用して、バックアップが作成されたホストを特定できます。データベースがオフラインの場合、情報は SnapCenter バックアップジョブログでのみ確認できます。

次の図に、選択したバックアップに応じたリストア処理を示します。

タイムスタンプ T3 の後にリストア処理を実行する必要があり、ホスト 1 がプライマリである場合は、SnapCenter を使用して T1 または T3 で作成されたバックアップをリストアできます。これらの Snapshot バックアップは、ホスト 1 に接続されているストレージボリュームで使用できます。

ホスト 2 （ T2 ）に作成されたバックアップを使用してリストアする必要がある場合は、ホスト 2 のストレージボリュームにある Snapshot コピーを使用する必要があります。このバックアップを利用するには、バックアップから NetApp FlexClone コピーを作成し、 FlexClone コピーをホスト 1 にマウントし、データを元の場所にコピーします。




| Restore Operation With | |
|---|---|
| Backup T1 | SnapCenter |
| Backup T2 | Create FlexClone from „Backup host 2“, mount and copy |
| Backup T3 | SnapCenter |

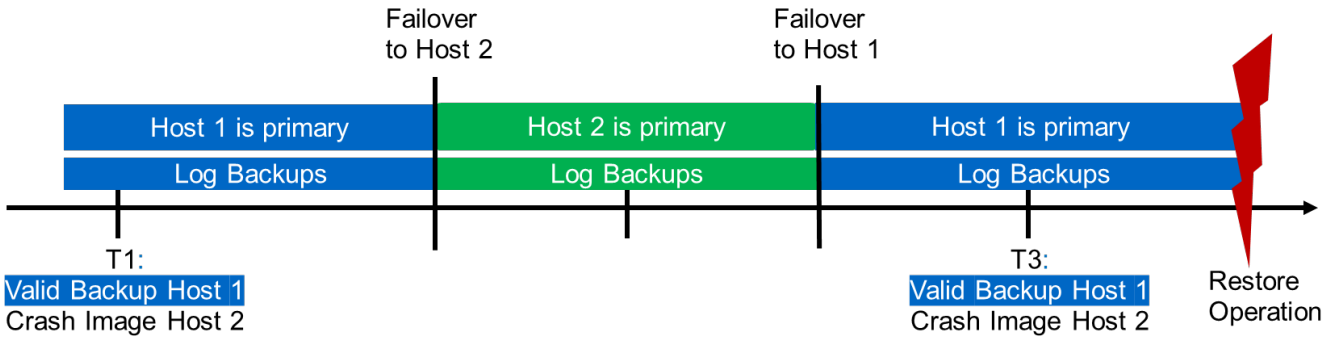
単一の SnapCenter リソース構成では、両方の SAP HANA システムレプリケーションホストの両方のストレージボリュームに Snapshot コピーが作成されます。フォワードリカバリに使用できるのは、プライマリ SAP HANA ホストのストレージボリュームに作成された Snapshot バックアップのみです。セカンダリ SAP HANA ホストのストレージボリュームに作成された Snapshot コピーは、フォワードリカバリに使用できないクラッシュイメージです。

SnapCenter でのリストア処理は、次の 2 つの方法で実行できます。

- 有効なバックアップのみをリストアしてください
- 有効なバックアップとクラッシュ・イメージを含む ' リソース全体をリストアする以下のセクションでは '2 つの異なるリストア・オペレーションについて詳細に説明します

もう一方のホストで作成されたバックアップからのリストア処理については、セクションで説明し"他のホストで作成されたバックアップからのリストアとリカバリ"ます。

次の図は、単一の SnapCenter リソース構成を使用したリストア処理を示しています。

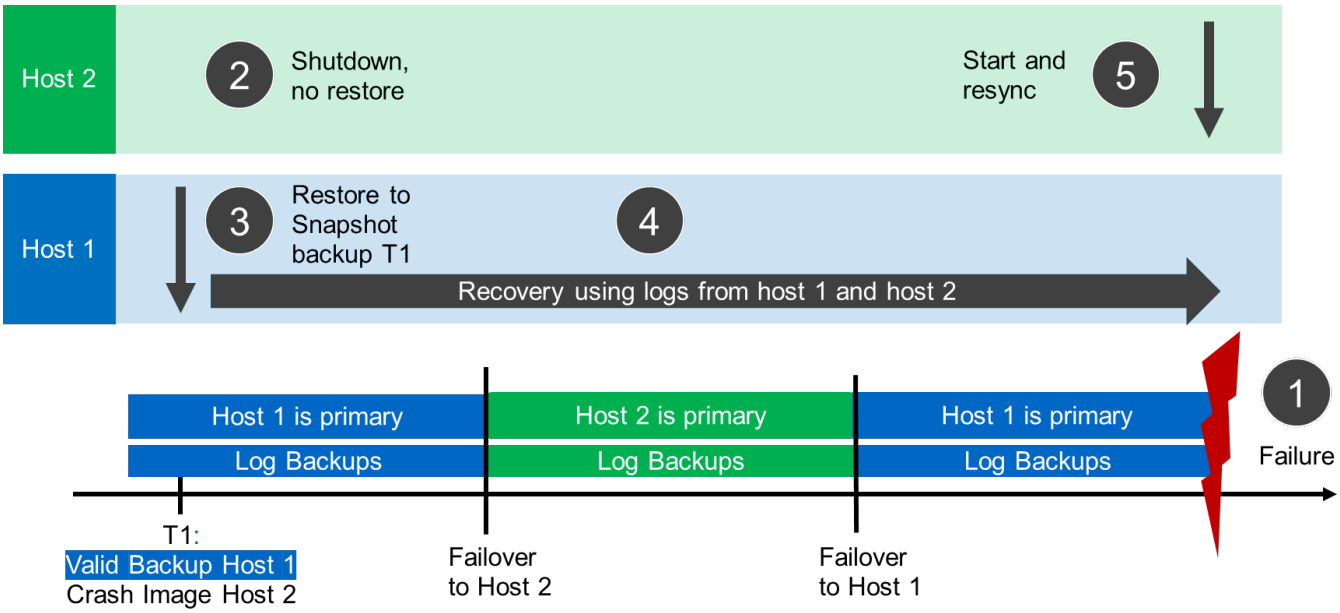



有効なバックアップの **SnapCenter** リストアのみを実行してください

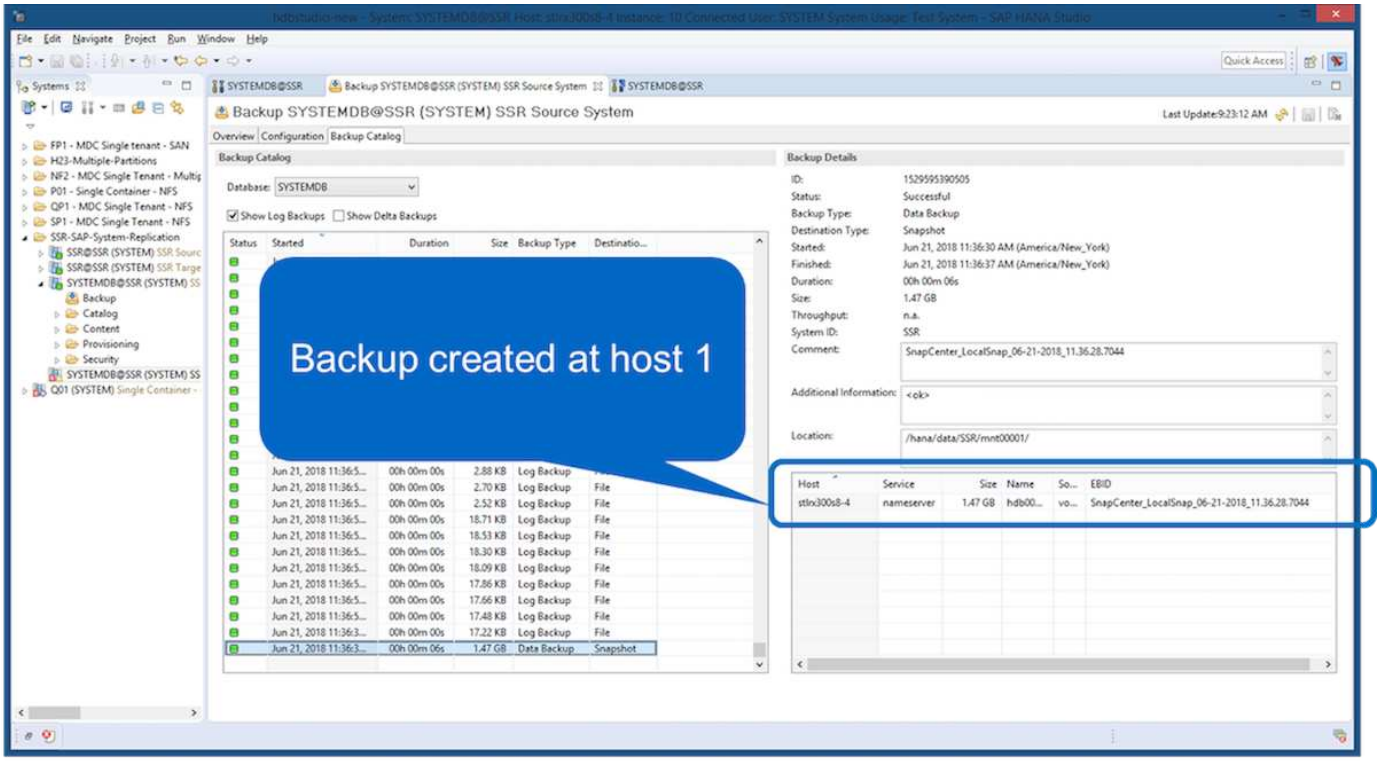
次の図に、このセクションで説明するリストアとリカバリのシナリオの概要を示します。

T1 のホスト 1 にバックアップが作成されました。ホスト 2 へのフェイルオーバーが実行されました。特定の時点で、ホスト 1 へのフェイルオーバーが再度実行されます。現在の時点では、ホスト 1 がプライマリホストになります。

1. 障害が発生したため、 T1 のホスト 1 で作成されたバックアップにリストアする必要があります。
2. セカンダリホスト（ホスト 2 ）はシャットダウンされますが、リストア処理は実行されません。
3. ホスト 1 のストレージボリュームは、 T1 で作成されたバックアップに復元されます。
4. フォワードリカバリは、ホスト 1 およびホスト 2 のログを使用して実行されます。
5. ホスト 2 が開始され、ホスト 2 のシステムレプリケーションの再同期が自動的に開始されます。



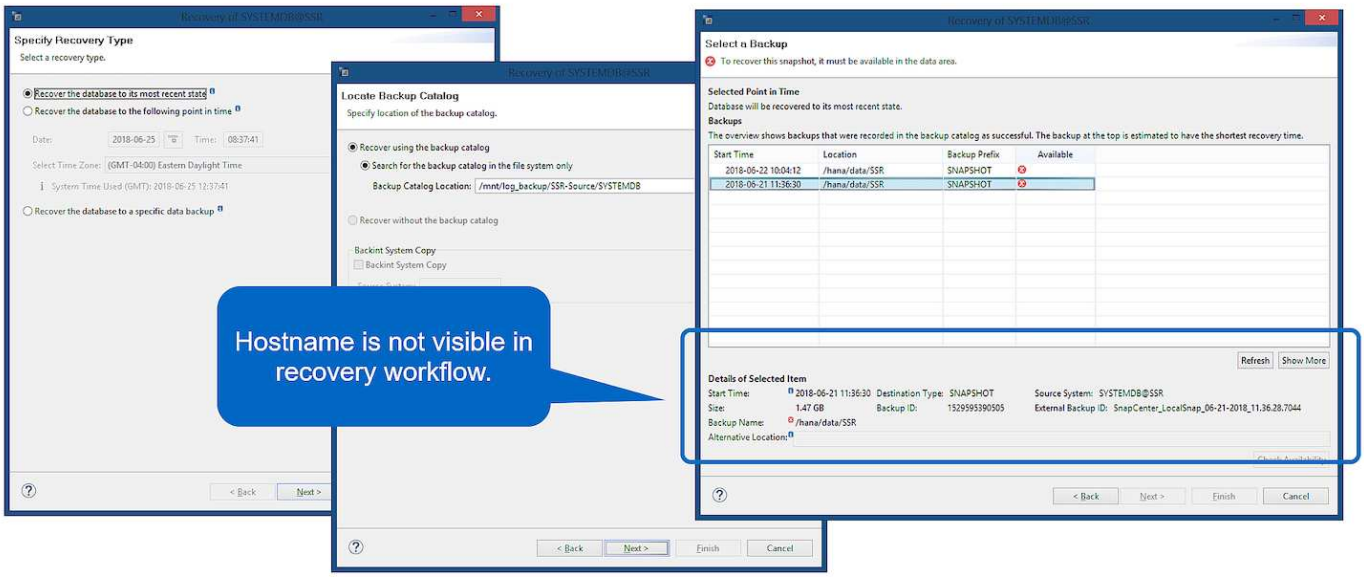

次の図は、 SAP HANA Studio の SAP HANA バックアップカタログを示しています。強調表示されたバックアップは、 T1 のホスト 1 で作成されたバックアップを示しています。




25

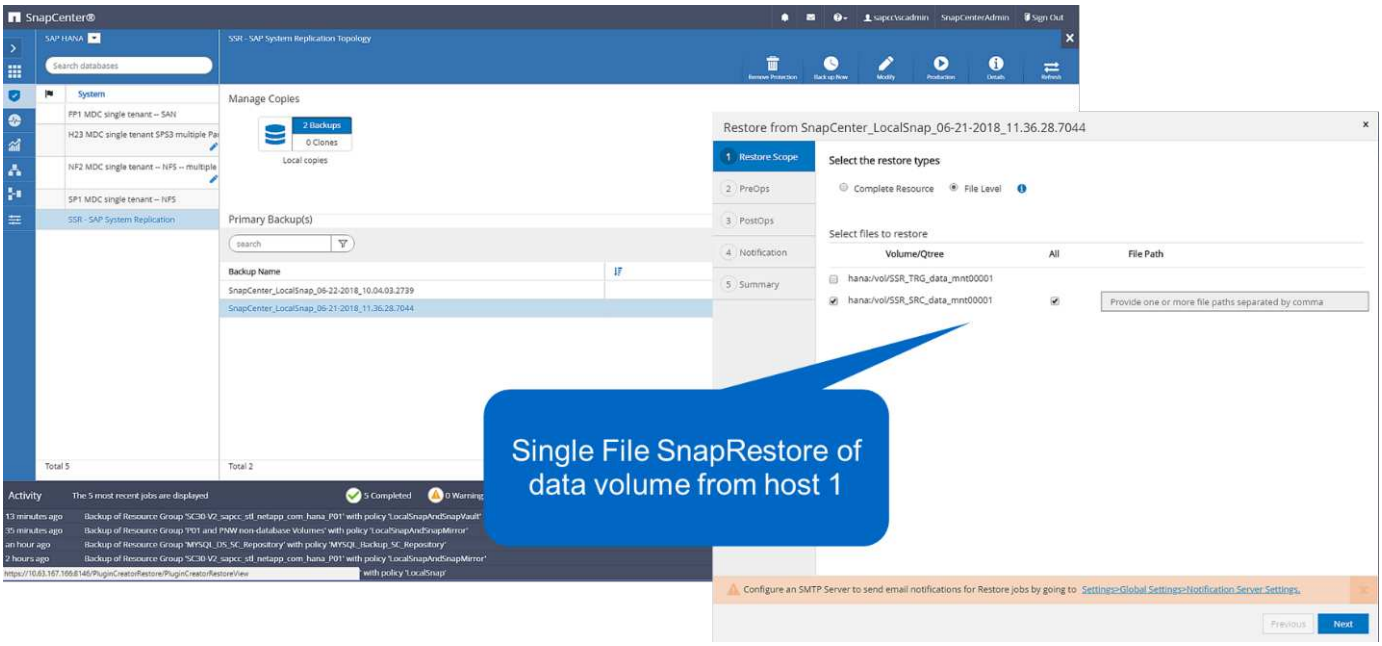
リストア処理とリカバリ処理は SAP HANA Studio で開始されます。次の図に示すように、バックアップが作成されたホストの名前はリストアとリカバリのワークフローには表示されません。

テストシナリオでは、データベースがオンラインのままの場合、 SAP HANA Studio で正しいバックアップ（ホスト 1 で作成されたバックアップ）を特定できました。データベースを使用できない場合は、 SnapCenter バックアップジョブログで適切なバックアップを特定する必要があります。

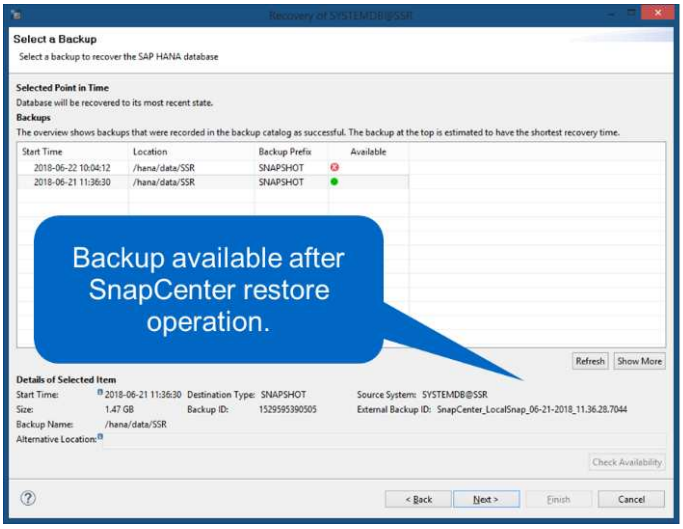


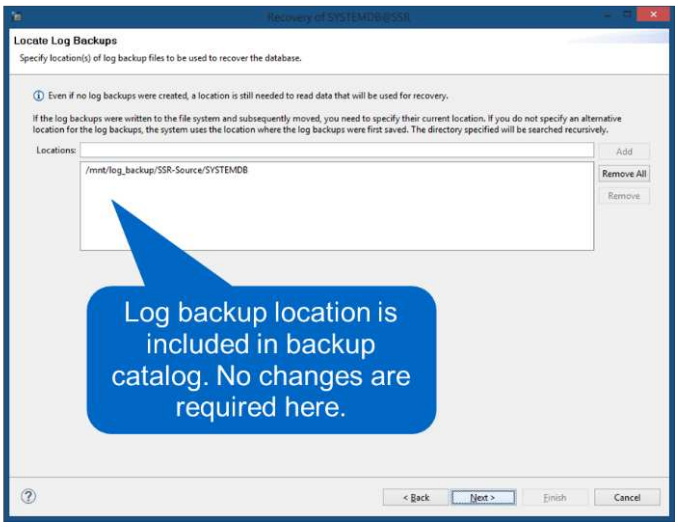

SnapCenter では、バックアップが選択され、ファイルレベルのリストア処理が実行されます。ファイルレベ

ルのリストア画面では、有効なバックアップのみがリストアされるように、ホスト 1 のボリュームのみが選択されます。



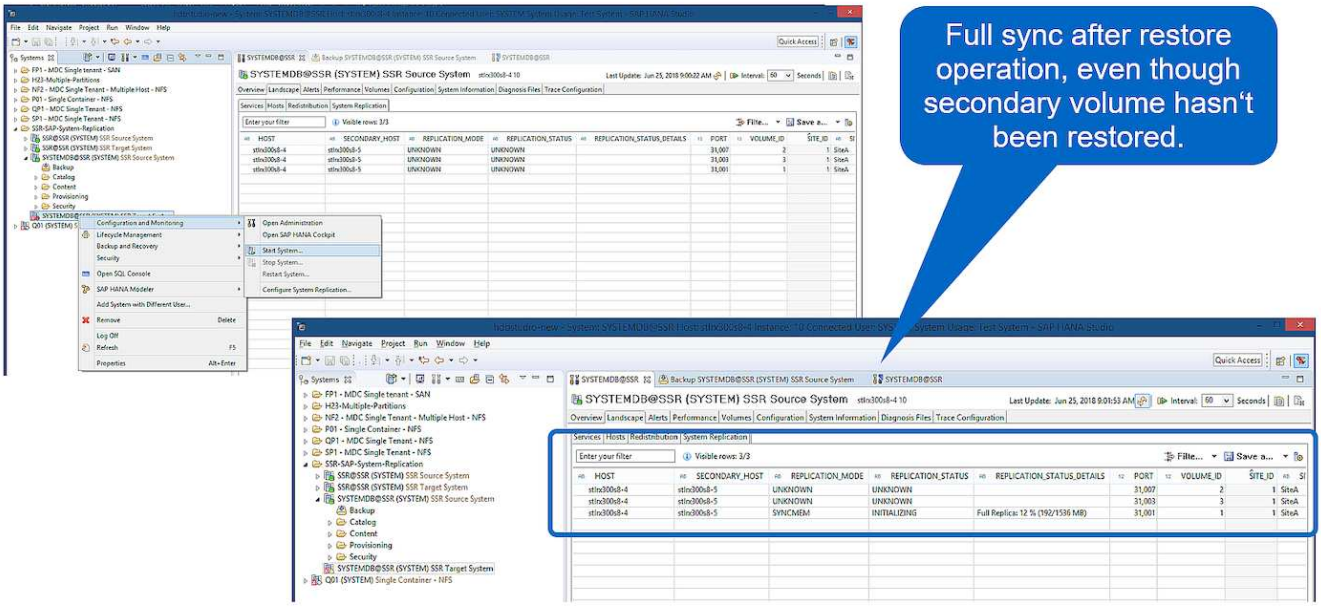

リストア処理が完了すると、 SAP HANA Studio でバックアップが緑色で強調表示されます。ホスト 1 とホスト 2 のログバックアップのファイルパスがバックアップカタログに含まれているため、追加のログバックアップの場所を入力する必要はありません。




フォワードリカバリが完了すると、セカンダリホスト（ホスト 2 ）が起動し、 SAP HANA システムレプリケーションの再同期が開始されます。

セカンダリホストが最新の状態である（ホスト 2 に対してリストア処理が実行されていない）場合でも、 SAP HANA はすべてのデータの完全なレプリケーションを実行します。この動作は、 SAP HANA システムレプリケーションを使用したリストア処理とリカバリ処理後に標準で実行されます。

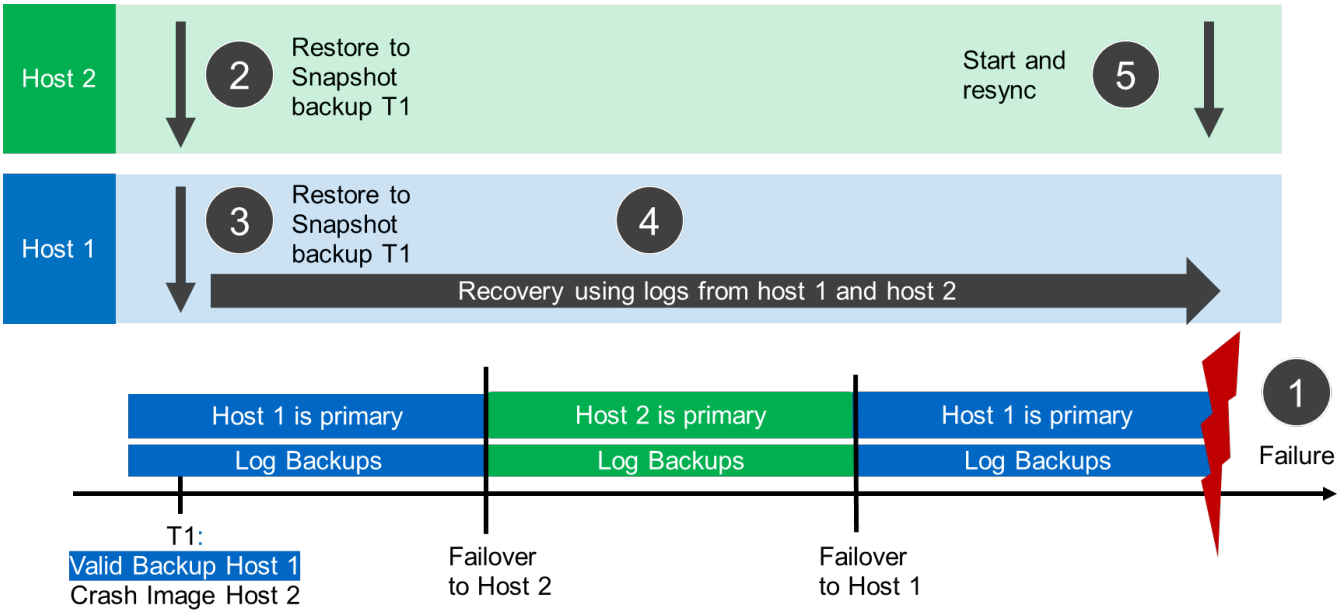



有効なバックアップとクラッシュイメージの **SnapCenter** リストア

次の図に、このセクションで説明するリストアとリカバリのシナリオの概要を示します。

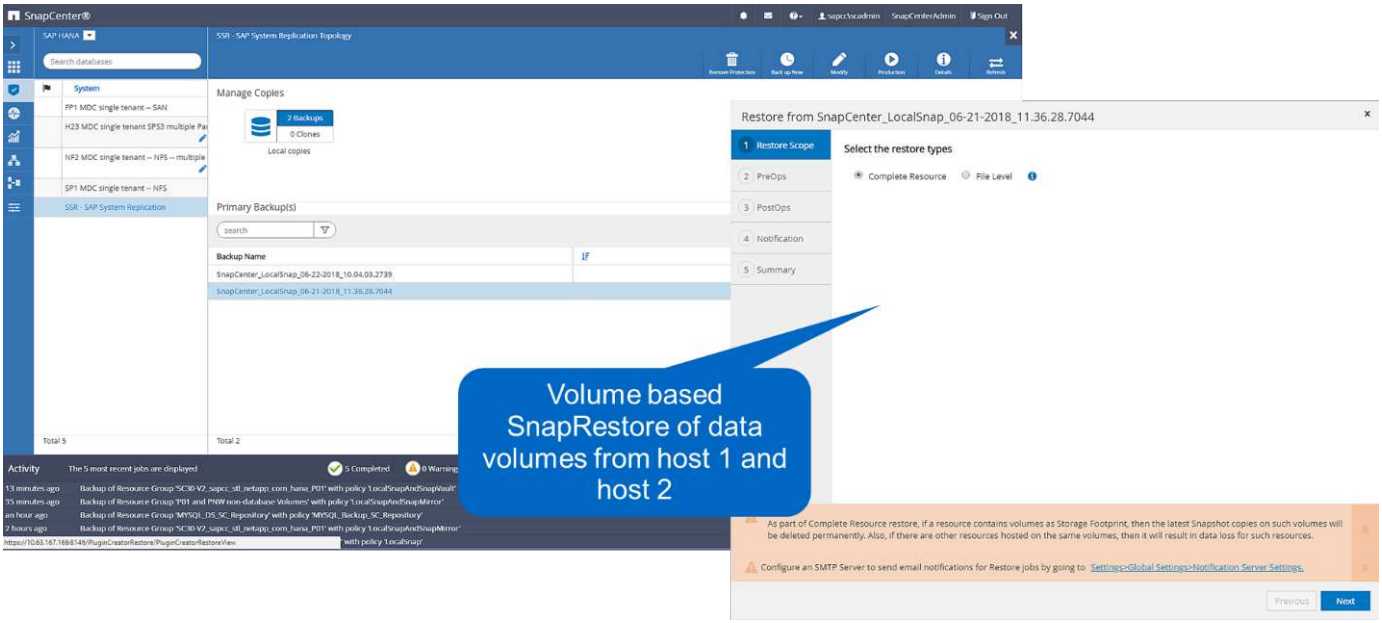
T1 のホスト 1 にバックアップが作成されました。ホスト 2 へのフェイルオーバーが実行されました。特定の時点で、ホスト 1 へのフェイルオーバーが再度実行されます。現在の時点では、ホスト 1 がプライマリホストになります。

1. 障害が発生したため、 T1 のホスト 1 で作成されたバックアップにリストアする必要があります。
2. セカンダリホスト（ホスト 2 ）がシャットダウンされ、 T1 クラッシュイメージが復元されます。
3. ホスト 1 のストレージボリュームは、 T1 で作成されたバックアップに復元されます。
4. フォワードリカバリは、ホスト 1 およびホスト 2 のログを使用して実行されます。
5. ホスト 2 が開始され、ホスト 2 のシステムレプリケーションの再同期が自動的に開始されます。

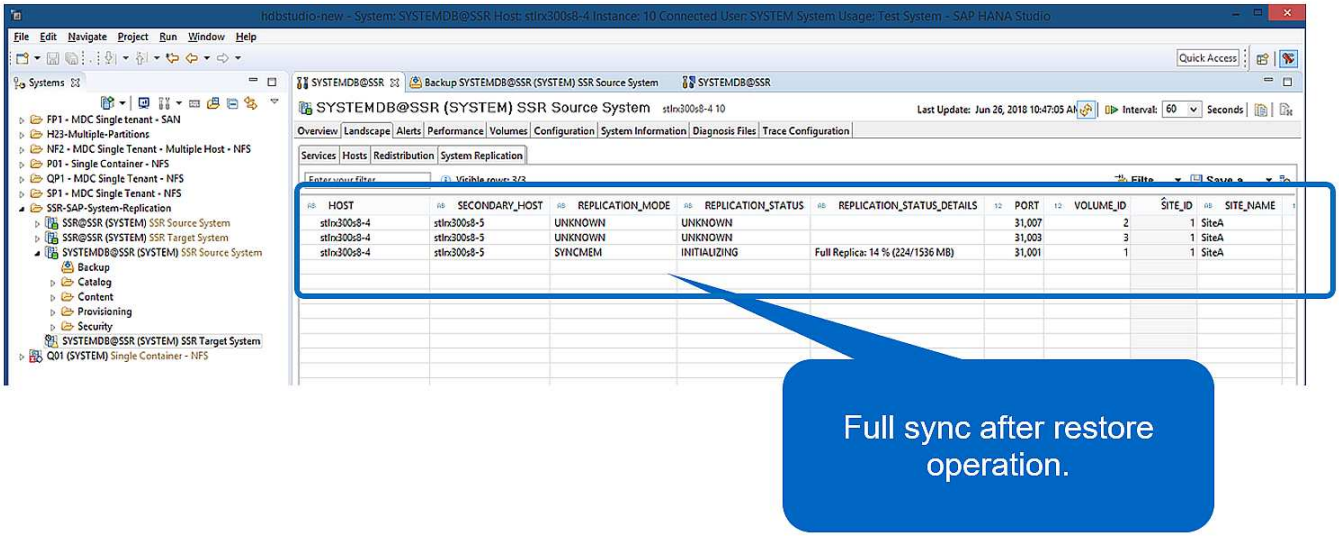


SAP HANA Studioを使用したリストアとリカバリの処理は、で説明した手順と同じ"有効なバックアップのSnapCenter リストアのみを実行してください"です。

リストア処理を実行するには、 SnapCenter でリソースを完全に選択してください。両方のホストのボリュームがリストアされます。




フォワードリカバリが完了すると、セカンダリホスト（ホスト 2 ）が起動し、 SAP HANA システムレプリケーションの再同期が開始されます。すべてのデータの完全なレプリケーションが実行されます。



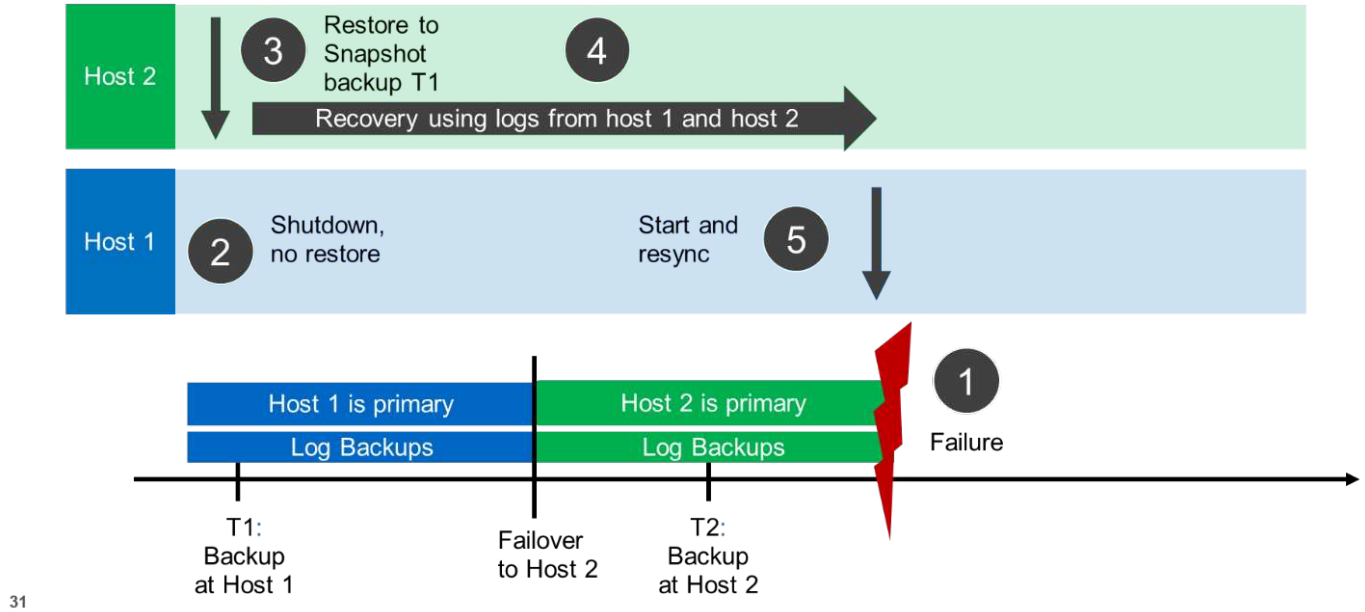

## もう一方のホストで作成されたバックアップからのリストアとリカバリ

他の SAP HANA ホストで作成されたバックアップからのリストア処理は、両方の SnapCenter 構成オプションで有効なシナリオです。

次の図に、このセクションで説明するリストアとリカバリのシナリオの概要を示します。

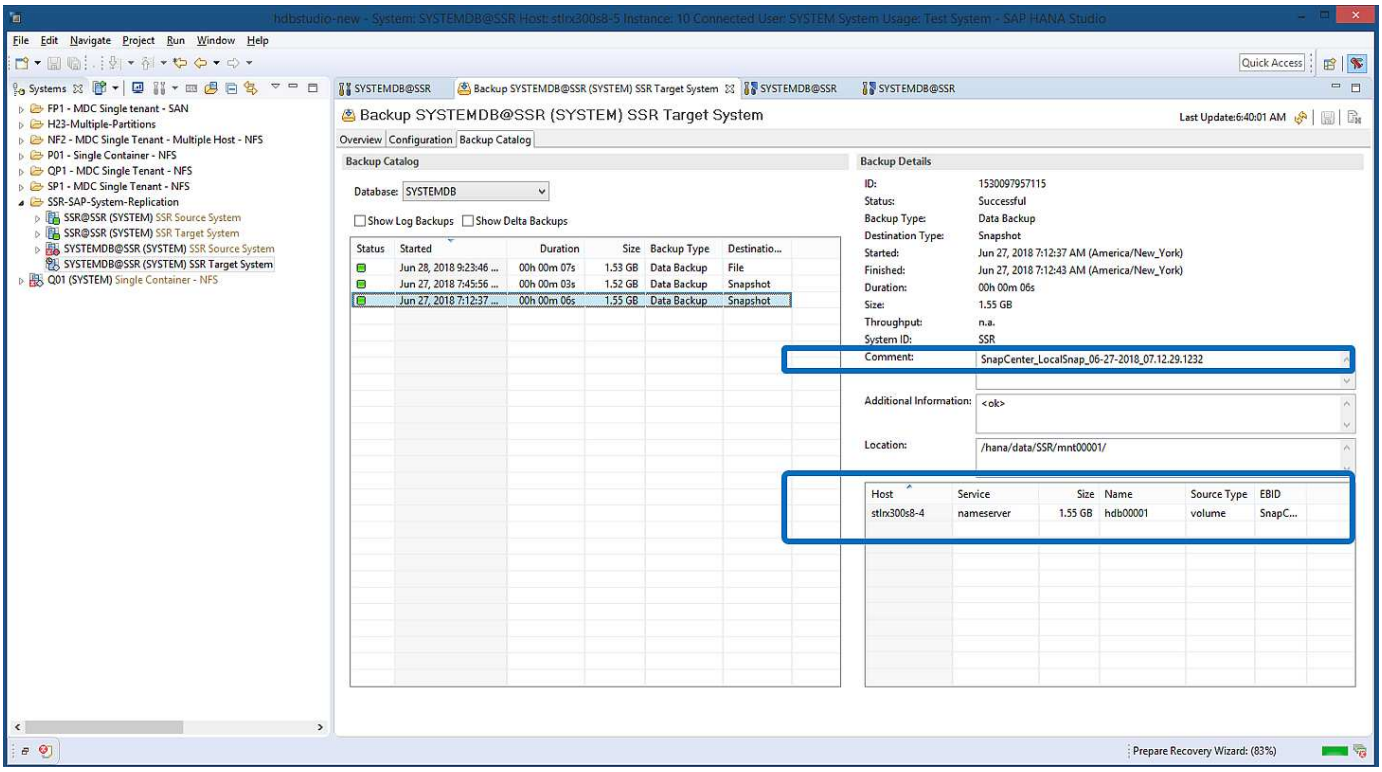
T1 のホスト 1 にバックアップが作成されました。ホスト 2 へのフェイルオーバーが実行されました。現在の時点では、ホスト 2 がプライマリホストになります。

1. 障害が発生したため、 T1 のホスト 1 で作成されたバックアップにリストアする必要があります。
2. プライマリホスト（ホスト 1 ）がシャットダウンされます。
3. ホスト 1 のバックアップデータ T1 は、ホスト 2 に復元されます。
4. フォワードリカバリは、ホスト 1 およびホスト 2 のログを使用して実行されます。
5. ホスト 1 が開始され、ホスト 1 のシステムレプリケーションの再同期が自動的に開始されます。




31

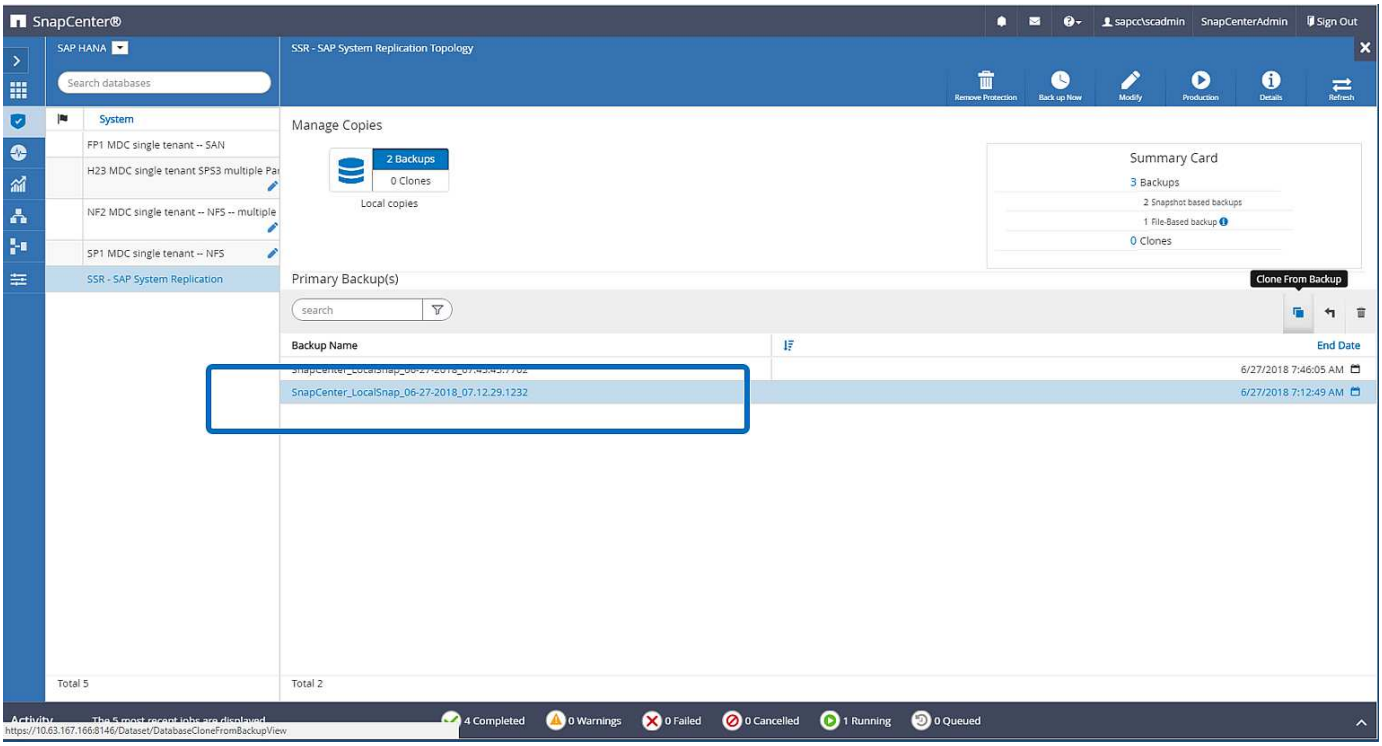
次の図は、 SAP HANA のバックアップカタログを示しており、リストア処理とリカバリ処理に使用した、ホスト 1 で作成されたバックアップを強調表示しています。




リストア処理には次の手順が含まれます。

1. ホスト 1 で作成したバックアップからクローンを作成します。
2. クローンボリュームをホスト 2 にマウントします。
3. クローンボリュームのデータを元の場所にコピーします。

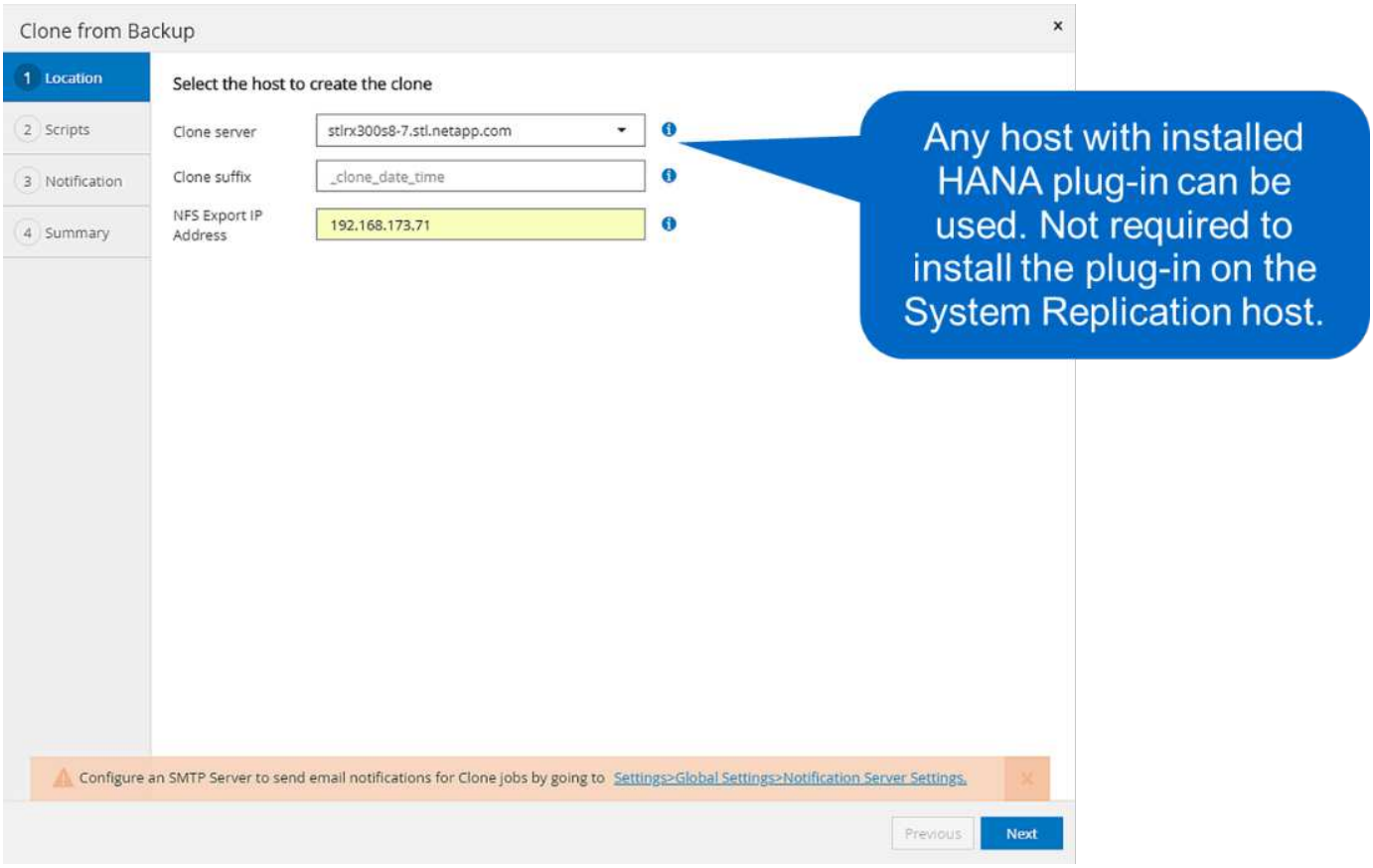
SnapCenter で、バックアップが選択され、クローニング処理が開始されます。



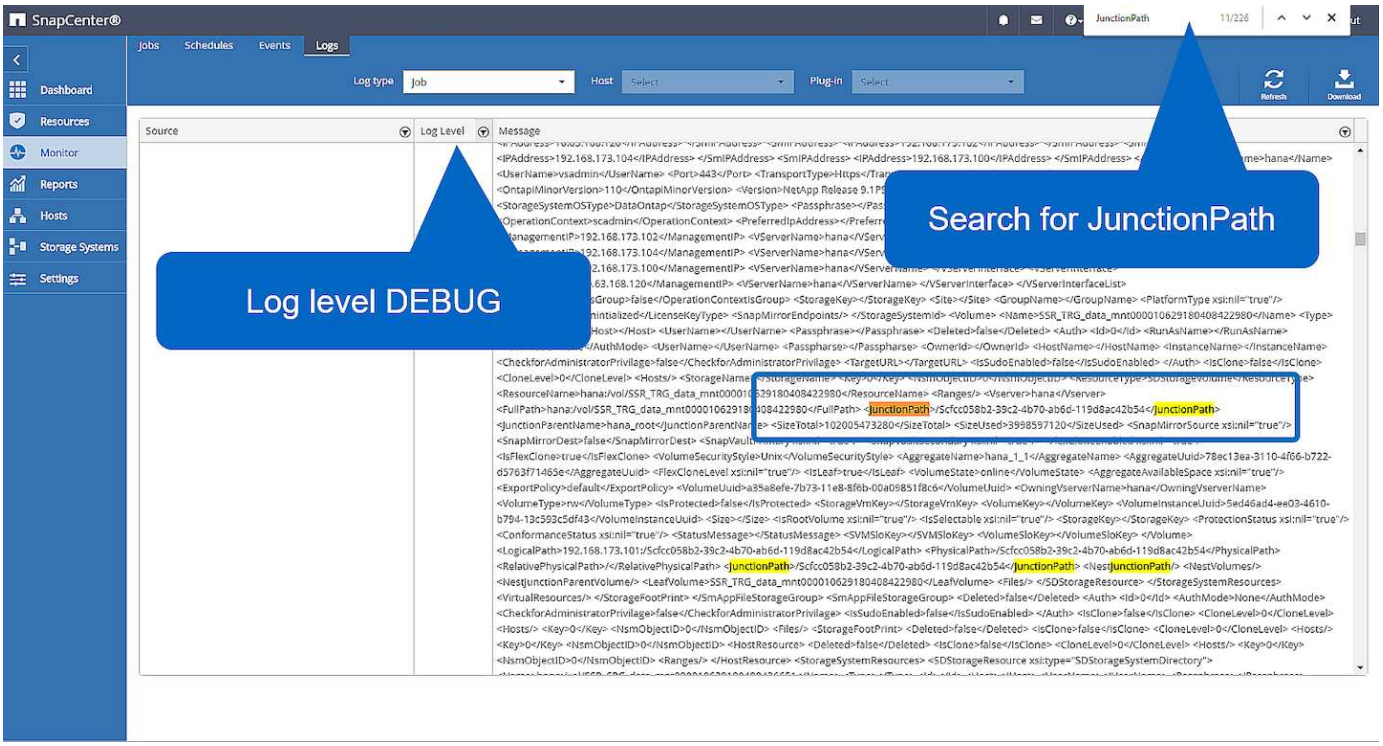
クローンサーバおよび NFS エクスポートの IP アドレスを指定する必要があります。

SnapCenter のシングルリソース構成では、 SAP HANA プラグインはデータベースホストにインストールされません。SnapCenter のクローニングワークフローを実行するには、 HANA プラグインがインストールされたすべてのホストをクローンサーバとして使用できます。

+ 別々のリソースを使用する SnapCenter 構成では、 HANA データベースホストがクローンサーバとして選択され、マウントスクリプトを使用してクローンがターゲットホストにマウントされます。




クローンボリュームのマウントに必要なジャンクションパスを特定するには、次の図に示すように、クローニングジョブのジョブログを確認します。




これで、クローンボリュームをマウントできるようになります。

```
stlrx300s8-5:/mnt/tmp # mount 192.168.173.101:/Scc373da37-00ff-4694-b1e1-
8153dbd46caf /mnt/tmp
```

クローンボリュームには、 HANA データベースのデータが含まれています。

```
stlrx300s8-5:/mnt/tmp/# ls -al
drwxr-x--x 2 ssradm sapsys 4096 Jun 27 11:12 hdb00001
drwx------ 2 ssradm sapsys 4096 Jun 21 09:38 hdb00002.00003
drwx------ 2 ssradm sapsys 4096 Jun 27 11:12 hdb00003.00003
-rw-r--r-- 1 ssradm sapsys   22 Jun 27 11:12 nameserver.lck
```

データが元の場所にコピーされます。

```
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00001 /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00002.00003/ /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00003.00003/ /hana/data/SSR/mnt00001/
```

SAP HANA Studioを使用したリカバリは、の説明に従って実行されます"有効なバックアップの SnapCenter リストアのみを実行してください"。

### 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、次のドキュメントを参照してください。

- "SnapCenter を使用した SAP HANA のバックアップとリカバリ"
- "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"
- SAP HANA Disaster Recovery with Storage Replication 』を参照してください

  "https://www.netapp.com/us/media/tr-4646.pdf"

### バージョン履歴

バージョン履歴：

| バージョン | 日付 | ドキュメントバージョン履歴 |
| --- | --- | --- |
| バージョン 1.0 以降 | 2018 年 10 月 | 初版 |
| バージョン 2.0 以降 | 2022 年 1 月 | SnapCenter 4.6 HANA システムレプリケーションのサポートに対応するように更新 |

# Azure NetApp Files を使用した SAP HANA ディザスタリカバリ

## TR-4891 ：『 SAP HANA disaster recovery with Azure NetApp Files 』

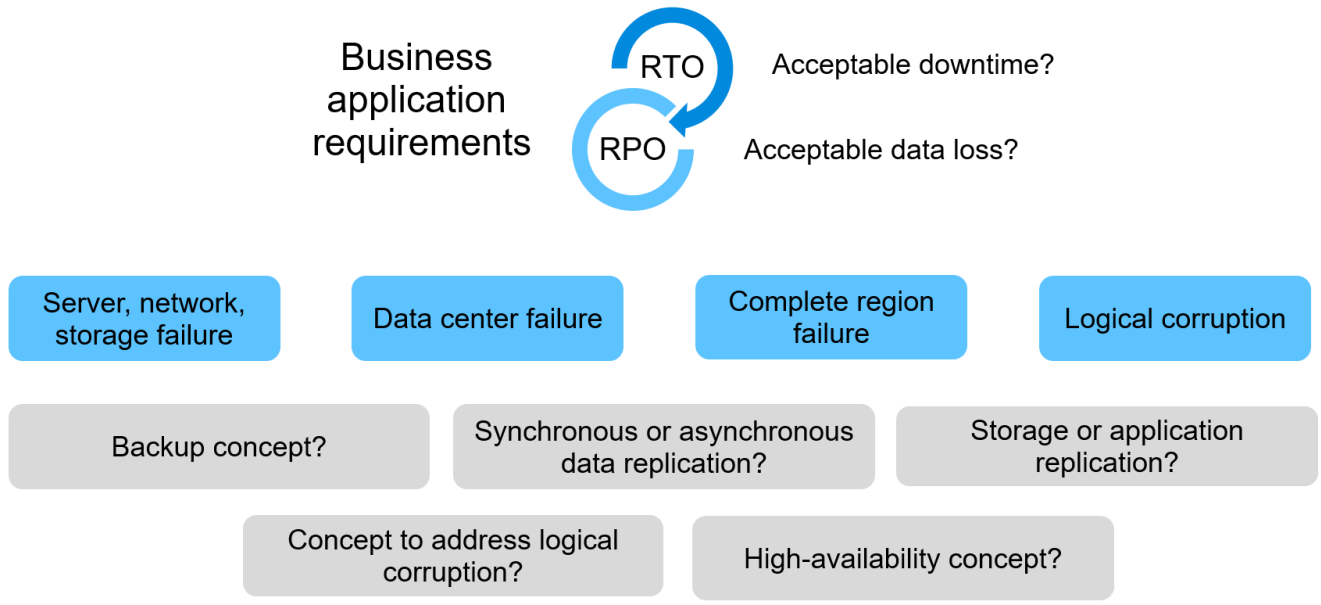
調査によると、ビジネスアプリケーションのダウンタイムは企業のビジネスに大きな悪影響を与えることがわかっています。

作成者：Nils Bauer、NetApp Ralf Klahr、Microsoft

財務面での影響に加えて、ダウンタイムは企業の評判、スタッフの士気、顧客ロイヤルティを損なう可能性もあります。驚くべきことに、すべての企業が包括的なディザスタリカバリポリシーを持っているわけではありません。

SAP HANA on Azure NetApp Files （ ANF ）を実行すると、 SAP HANA に組み込まれているデータ保護機能やディザスタリカバリ機能を拡張、向上させる追加機能を利用できます。この概要セクションでは、お客様がビジネスニーズをサポートするオプションを選択できるように、これらのオプションについて説明します。

包括的なディザスタリカバリポリシーを作成するには、データ保護とディザスタリカバリに必要なビジネスアプリケーションの要件と技術的な機能を理解する必要があります。次の図に、データ保護の概要を示します。




ビジネスアプリケーションの要件

ビジネスアプリケーションの主要な指標として、次の 2 つがあります。

- Recovery Point Objective （ RPO ；目標復旧時点）、またはデータ損失の許容量の上限
- Recovery Time Objective （ RTO ；目標復旧時間）、またはビジネスアプリケーションの最大許容ダウンタイム

これらの要件は、使用するアプリケーションの種類とビジネスデータの性質によって定義されます。1 つの Azure リージョンで障害から保護する場合は、 RPO と RTO が異なることがあります。また、 Azure リージョン全体の損失など、災害による災害に備える場合にも同じように、災害によって異なることがあります。RPO と RTO は、利用可能な技術的オプションに大きく影響するため、これらの要件によって定義されるビジネス要件を評価することが重要です。

高可用性

仮想マシン、ネットワーク、ストレージなど、 SAP HANA 用のインフラには、単一点障害がないように冗長コンポーネントが必要です。MS Azure は、さまざまなインフラコンポーネントに対して冗長性を提供します。

コンピューティング側とアプリケーション側で高可用性を実現するために、スタンバイの SAP HANA ホストは、 SAP HANA マルチホストシステムを使用して、組み込みの高可用性を実現するように構成できます。サーバまたは SAP HANA サービスに障害が発生すると、 SAP HANA サービスがスタンバイホストにフェイルオーバーするため、アプリケーションのダウンタイムが発生します。

サーバやアプリケーションの障害時にアプリケーションのダウンタイムが許容されない場合は、 SAP HANA システムのレプリケーションをハイアベイラビリティ解決策として使用して、非常に短時間でフェイルオーバーを実現することもできます。SAP のお客様は、 HANA システムレプリケーションを使用して、計画外障害に対する高可用性を実現できるだけでなく、 HANA ソフトウェアのアップグレードなどの計画的運用のダウンタイムを最小限に抑えることができます。

### 論理的破損

論理的破損は、ソフトウェアエラー、人為的エラー、破壊行為などが原因で発生する可能性があります。残念ながら、論理的破損は、標準的な高可用性ソリューションやディザスタリカバリソリューションでは対処できないことがよくあります。そのため、論理的破損が発生したレイヤ、アプリケーション、ファイルシステム、またはストレージによっては、 RTO と RPO の要件が満たされないことがあります。

最悪のケースは、 SAP アプリケーションが論理的に破損した場合です。SAP アプリケーションは多くの場合、異なるアプリケーションが相互に通信してデータを交換する環境で動作します。このため、論理的な破損が発生した SAP システムはリストアとリカバリを実行しないことを推奨します。システムを破損前の特定の時点にリストアするとデータが失われるため、 RPO はゼロより大きくなります。また、 SAP ランドスケープは同期されず、さらにポストプロセスが必要になります。

SAP システムをリストアする代わりに、別の修復システムで問題を分析して、システム内の論理エラーを修正する方法を推奨します。ルート原因分析には、ビジネスプロセスやアプリケーション所有者の関与が必要です。このシナリオでは、論理的破損が発生する前に格納されたデータに基づいて、修復システム（本番用システムのクローン）を作成します。リペアシステム内では、必要なデータをエクスポートし、本番システムにインポートできます。このアプローチでは、生産性の高いシステムを停止する必要はありません。また、最良のシナリオでは、データが失われたり、データの一部しか失われたりすることはありません。

> 修復システムのセットアップに必要な手順は、このドキュメントで説明するディザスタリカバリのテストシナリオと同じです。そのため、説明したディザスタリカバリ解決策を拡張して、論理的な破損にも簡単に対処できます。

### バックアップ

さまざまなポイントインタイムデータセットからリストアとリカバリを実行できるようにバックアップが作成されている。通常、これらのバックアップは数日から数週間保持されます。

破損の種類に応じて、データを損失するかどうかに関係なく、リストアとリカバリを実行できます。RPO をゼロにする必要がある場合は、プライマリストレージとバックアップストレージが失われた場合でも、バックアップを同期データレプリケーションと組み合わせる必要があります。

リストアとリカバリの RTO は、必要なリストア時間、リカバリ時間（データベースの起動を含む）、およびデータをメモリにロードすることによって定義されます。大規模なデータベースや従来のバックアップ方法では、 RTO が数時間に及ぶことがありますが、これは許容されない場合があります。RTO を大幅に短縮するには、バックアップを、データをメモリにプリロードすることを含むホットスタンバイ解決策と組み合わせる必要があります。

一方、バックアップ解決策は、データレプリケーションソリューションがあらゆる種類の論理的破損に対応できないため、論理的破損に対処する必要があります。

### 同期または非同期のデータレプリケーション

RPO は、主に、使用するデータレプリケーション方法を決定します。RPO をゼロにする必要がある場合は、プライマリストレージとバックアップストレージが失われた場合でも、データを同期的にレプリケートする必要があります。ただし、同期レプリケーションについては、 2 つの Azure リージョン間の距離などの技術的な制限があります。ほとんどの場合、同期レプリケーションは 100km を超えるレイテンシから受ける距離には適していないため、 Azure リージョン間でのデータレプリケーションには対応できません。

RPO を大きくすることが許容される場合は、長距離間で非同期レプリケーションを使用できます。この場合の RPO は、レプリケーションの頻度によって定義されます。

**HANA** システムのレプリケーションでデータプリロードを設定するかどうか

SAP HANA データベースの起動時間は、従来のデータベースよりもはるかに長くなります。これは、データベースが期待されるパフォーマンスを提供するためには、大量のデータをメモリにロードする必要があるためです。そのため、 RTO の大部分はデータベースの起動に必要な時間です。ストレージベースのレプリケーションに加えて、 HANA システムレプリケーションを事前ロードなしで実行する場合、ディザスタリカバリサイトにフェイルオーバーするためには、 SAP HANA データベースを起動する必要があります。

SAP HANA システムレプリケーションでは、データがプリロードされ、セカンダリホストで継続的に更新される動作モードが提供されます。このモードでは、 RTO の値が非常に低くなりますが、ソースシステムからのレプリケーションデータの受信にのみ使用される専用のサーバが必要になります。

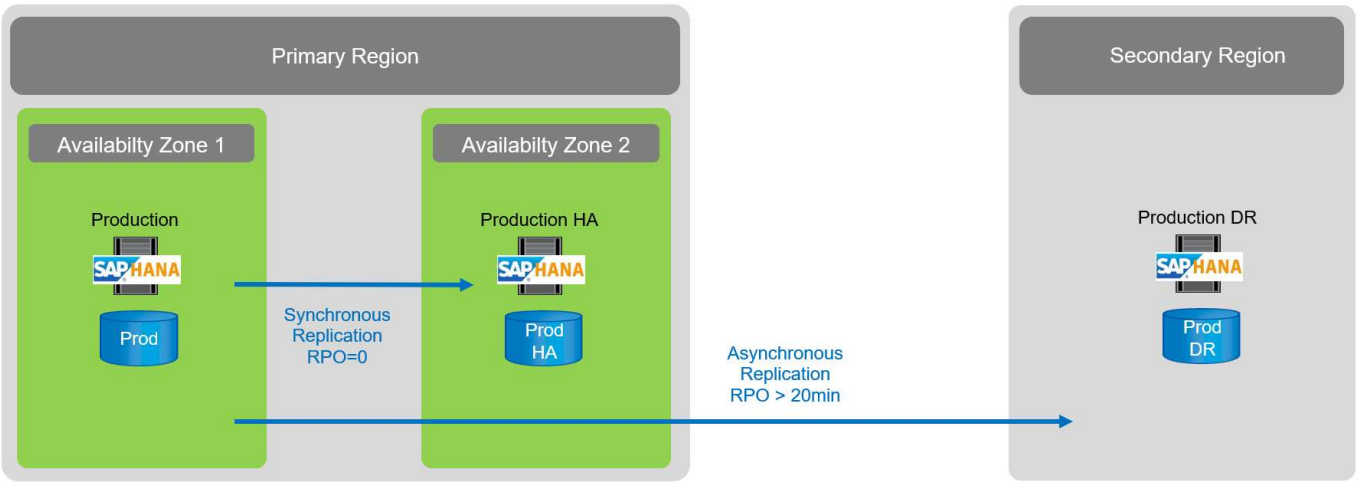
## ディザスタリカバリ解決策の比較

包括的なディザスタリカバリ解決策では、お客様がプライマリサイトの完全な障害からリカバリできるようにする必要があります。そのため、サイト障害が発生した場合に必要な本番用 SAP HANA システムを実行するには、データをセカンダリサイトに転送し、インフラ全体を構築する必要があります。アプリケーションの可用性の要件や保護する災害の種類に応じて、 2 サイトまたは 3 サイトのディザスタリカバリ解決策を検討する必要があります。

次の図は、データが同じ Azure リージョン内で同時に 2 つ目のアベイラビリティゾーンにレプリケートされる一般的な設定を示しています。短距離では、データを同期的にレプリケートして、 RPO をゼロにすることができます（一般に HA の提供に使用されます）。

また、プライマリリージョンに影響が生じた場合は、災害から保護するためにデータがセカンダリリージョンに非同期でレプリケートされます。達成可能な最小 RPO は、データレプリケーションの頻度によって異なります。この頻度は、プライマリリージョンとセカンダリリージョンの間で使用可能な帯域幅によって制限されます。一般的な最小 RPO は、 20 分から複数時間の範囲です。

このドキュメントでは、 2 リージョンのディザスタリカバリ解決策のさまざまな実装オプションについて説明します。




**SAP HANA** システムレプリケーション

SAP HANA システムレプリケーションはデータベースレイヤで機能します。解決策は、プライマリシステムから変更を受信するディザスタリカバリサイトにある追加の SAP HANA システムに基づいています。このセ

カンダリシステムは、プライマリシステムと同じである必要があります。

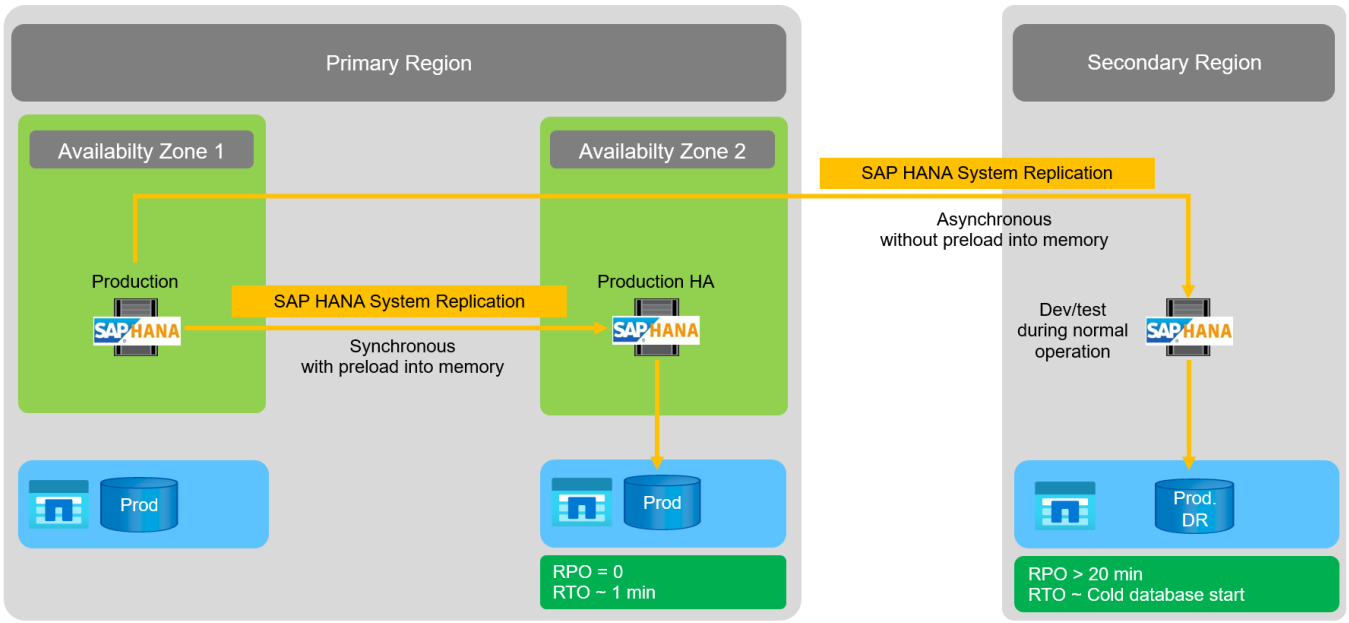
SAP HANA システムレプリケーションは、次のいずれかのモードで実行できます。

- データがメモリにプリロードされており、ディザスタリカバリサイトにある専用サーバにロードされている場合：
  - このサーバは、 SAP HANA システムレプリケーションセカンダリホストとしてのみ使用されます。
  - データはすでにメモリにロードされており、フェイルオーバー時にデータベースを起動する必要がないため、 RTO 値は非常に低くなります。
- メモリおよび災害復旧サイトの共有サーバにデータがプリロードされていない場合：
  - サーバは、 SAP HANA システムレプリケーションセカンダリシステムおよび開発 / テストシステムとして共有されます。
  - RTO は、主にデータベースの起動とメモリへのデータのロードに必要な時間に左右されます。

すべての設定オプションとレプリケーションシナリオの概要の詳細については、を参照してください "『 SAP HANA Administration Guide 』をご覧ください"。

次の図は、 SAP HANA システムレプリケーションを使用した 2 リージョンのディザスタリカバリ解決策のセットアップを示しています。メモリにプリロードされたデータを含む同期レプリケーションは、同じ Azure リージョン内のローカル HA には使用されますが、アベイラビリティゾーンによって異なります。リモートのディザスタリカバリリージョンには、データがプリロードされていない非同期レプリケーションが設定されています。

次の図は、 SAP HANA システムレプリケーションを示しています。




**SAP HANA** システムレプリケーションとメモリにデータがプリロードされています

SAP HANA の RTO 値が非常に低い場合は、メモリにデータがプリロードされた SAP HANA System Replication でのみ達成できます。ディザスタリカバリサイトにある専用のセカンダリサーバを使用して SAP HANA システムレプリケーションを運用すると、 RTO の値が約 1 分以下になります。複製されたデータは、セカンダリシステムのメモリにロードされて受信されます。フェイルオーバーにかかる時間が短く、 SAP HANA システムレプリケーションは、 HANA ソフトウェアのアップグレードなど、ダウンタイムがほぼゼロ

に近いメンテナンス処理にも使用されることがよくあります。

通常、 SAP HANA システムレプリケーションは、データプリロードが選択されたときに同期的にレプリケートされるように設定されます。同期レプリケーションでサポートされる最大距離は 100km です。

#### SAP システムレプリケーション：メモリにデータがプリロードされていません

RTO 要件が厳しくない場合は、データがプリロードされていなくても SAP HANA システムレプリケーションを使用できます。この運用モードでは、ディザスタリカバリ領域のデータはメモリにロードされません。DR リージョンのサーバは、必要なすべての SAP HANA プロセスを実行する SAP HANA システムレプリケーションの処理にも使用されます。ただし、サーバのメモリのほとんどは、 SAP HANA 開発 / テストシステムなどの他のサービスを実行するために使用できます。

障害が発生した場合は、開発 / テストシステムをシャットダウンし、フェイルオーバーを開始して、データをメモリにロードする必要があります。このコールドスタンバイアプローチの RTO は、データベースのサイズと、行ストアと列ストアの負荷時の読み取りスループットによって異なります。1000Mbps のスループットでデータが読み取られることを前提として、 1TB のデータをロードするには約 18 分かかります。

### ANF クロスリージョンレプリケーションを使用した SAP HANA ディザスタリカバリ

ANF には、非同期データレプリケーションを使用したディザスタリカバリ解決策として ANF に組み込まれています。ANF クロスリージョンレプリケーションは、プライマリリージョンとセカンダリ Azure リージョンの 2 つの ANF ボリューム間でデータ保護関係を介して設定されます。ANF のクロスリージョンレプリケーションでは、ブロックの差分レプリケーションを効率的に使用してセカンダリボリュームが更新されます。更新スケジュールはレプリケーション設定時に定義できます。

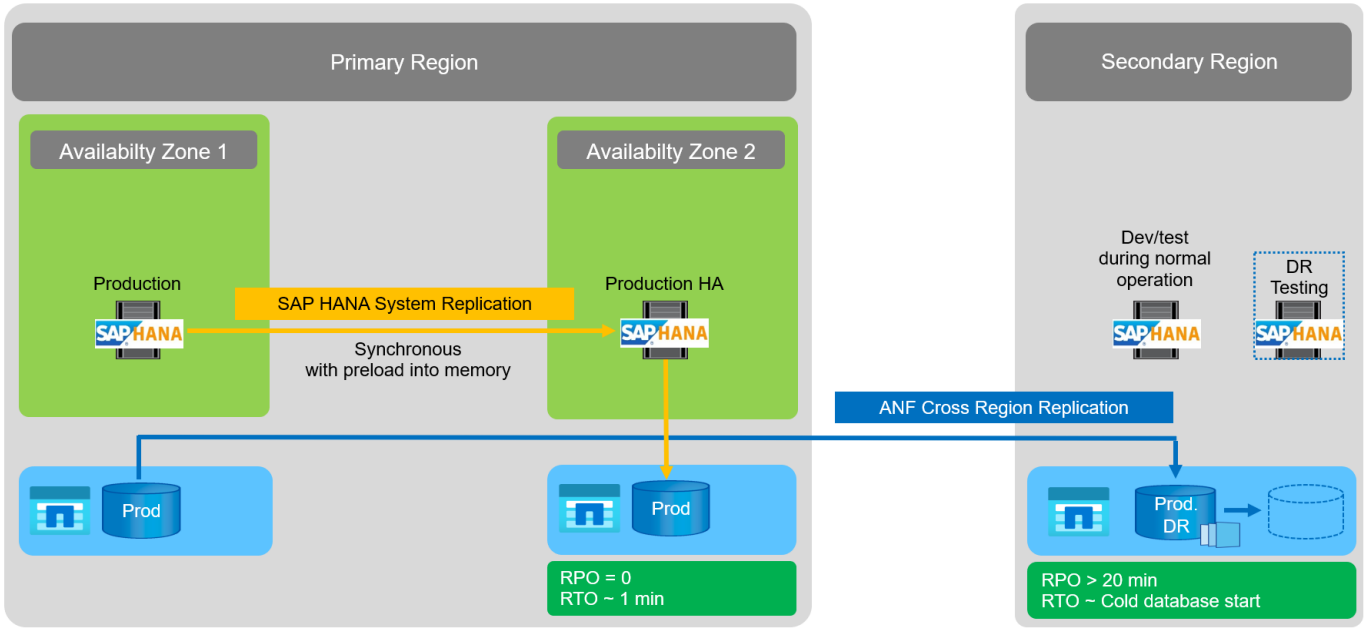
次の図は、 ANF クロスリージョンレプリケーションを使用した 2 リージョンのディザスタリカバリ解決策の例を示しています。この例では、前の章で説明したように、 HANA システムはプライマリリージョン内で HANA システムレプリケーションによって保護されています。セカンダリリージョンへのレプリケーションは、 ANF のクロスリージョンレプリケーションを使用して実行されます。RPO は、レプリケーションスケジュールとレプリケーションオプションによって定義されます。

RTO は、主に、ディザスタリカバリサイトで HANA データベースを起動してメモリにデータをロードするのに必要な時間に左右されます。データの読み取りスループットが 1000Mb/s の場合、 1TB のデータをロードするには約 18 分かかります。レプリケーション設定に応じて、フォワードリカバリが必要で、 RTO の合計値にも加算されます。

各種の設定オプションの詳細については、の章を参照して"SAP HANA を使用したリージョン間レプリケーションの構成オプション"ください。

通常の運用中は、ディザスタリカバリサイトのサーバを開発 / テストシステムとして使用できます。災害が発生した場合は、開発 / テスト用システムをシャットダウンし、 DR 本番用サーバとして起動する必要があります。

ANF クロスリージョンレプリケーションを使用すると、 RPO と RTO に影響を与えることなく DR ワークフローをテストできます。そのためには、ボリュームクローンを作成し、 DR テストサーバに接続します。




ディザスタリカバリソリューションの概要

次の表に、このセクションで説明したディザスタリカバリソリューションの比較を示し、最も重要な指標を示します。

主な調査結果は次のとおりです。

- RTO が非常に低い場合は、プリロードが設定された SAP HANA システムレプリケーションが唯一のオプションです。
  - DR サイトに専用のサーバが必要となります。これにより、レプリケートされたデータを受信してデータをメモリにロードできます。
- また、データベースの外部にあるデータ（共有ファイル、インターフェイスなど）にもストレージレプリケーションが必要です。
- RTO / RPO の要件が厳しい場合は、 ANF のクロスリージョンレプリケーションを使用して次のことを行うこともできます。
  - データベースと非データベースのデータレプリケーションを組み合わせます。
  - ディザスタリカバリのテストや開発 / テストの更新など、その他のユースケースについて説明します。
  - ストレージレプリケーションを行うことで、 DR サイトのサーバを QA またはテストシステムとして通常運用時に使用できます。
- RPO = 0 の HA 解決策として SAP HANA システムレプリケーションを組み合わせ、長距離のストレージレプリケーションを行う場合は、さまざまな要件に対応することが重要です。

次の表に、ディザスタリカバリソリューションの比較を示します。

| | ストレージレプリケーション | **SAP HANA** システムのレプリケーション | |
|---|---|---|---|
| | * リージョン間レプリケーション * | * データプリロードあり * | * データプリロードなし * |

| | ストレージレプリケーション | **SAP HANA** システムのレプリケーション | |
|---|---|---|---|
| RTO | データベースの起動時間およびフォワードリカバリに応じて、低 ～ 中 | とても低いです | データベースの起動時間に応じて、低から中に移動します |
| RPO | RPO > 20 分の非同期レプリケーション | RPO > 20 分の非同期レプリケーション RPO = 0 の同期レプリケーション | RPO > 20 分の非同期レプリケーション RPO = 0 の同期レプリケーション |
| DR サイトのサーバは、開発とテストに使用できます | はい。 | いいえ | はい。 |
| データベース以外のデータのレプリケーション | はい。 | いいえ | いいえ |
| DR データは、開発 / テストシステムの更新に使用できます | はい。 | いいえ | いいえ |
| RTO と RPO に影響を与えずに DR テストを実施 | はい。 | いいえ | いいえ |

## **SAP HANA** を使用した **ANF** のクロスリージョンレプリケーション

**SAP HANA** を使用した **ANF** のクロスリージョンレプリケーション

クロスリージョンレプリケーションに関するアプリケーションに依存しない情報は、次の場所にあります。

"Azure NetApp Files のドキュメント | Microsoft ドキュメント"を参照してください。

**SAP HANA** によるクロスリージョンレプリケーションの設定オプション

次の図は、 ANF クロスリージョンレプリケーションを使用した SAP HANA システムのボリュームレプリケーション関係を示しています。ANF クロスリージョンレプリケーションでは、 HANA データと HANA 共有ボリュームがレプリケートされている必要があります。HANA データボリュームのみがレプリケートされている場合、通常の RPO 値は 1 日の範囲になります。RPO の値を低くする必要がある場合は、 HANA のログバックアップもフォワードリカバリのためにレプリケートする必要があります。

このドキュメントで使用されている「ログバックアップ」という用語には、ログバックアップと HANA バックアップカタログバックアップが含まれています。フォワードリカバリ処理を実行するには、 HANA のバックアップカタログが必要です。

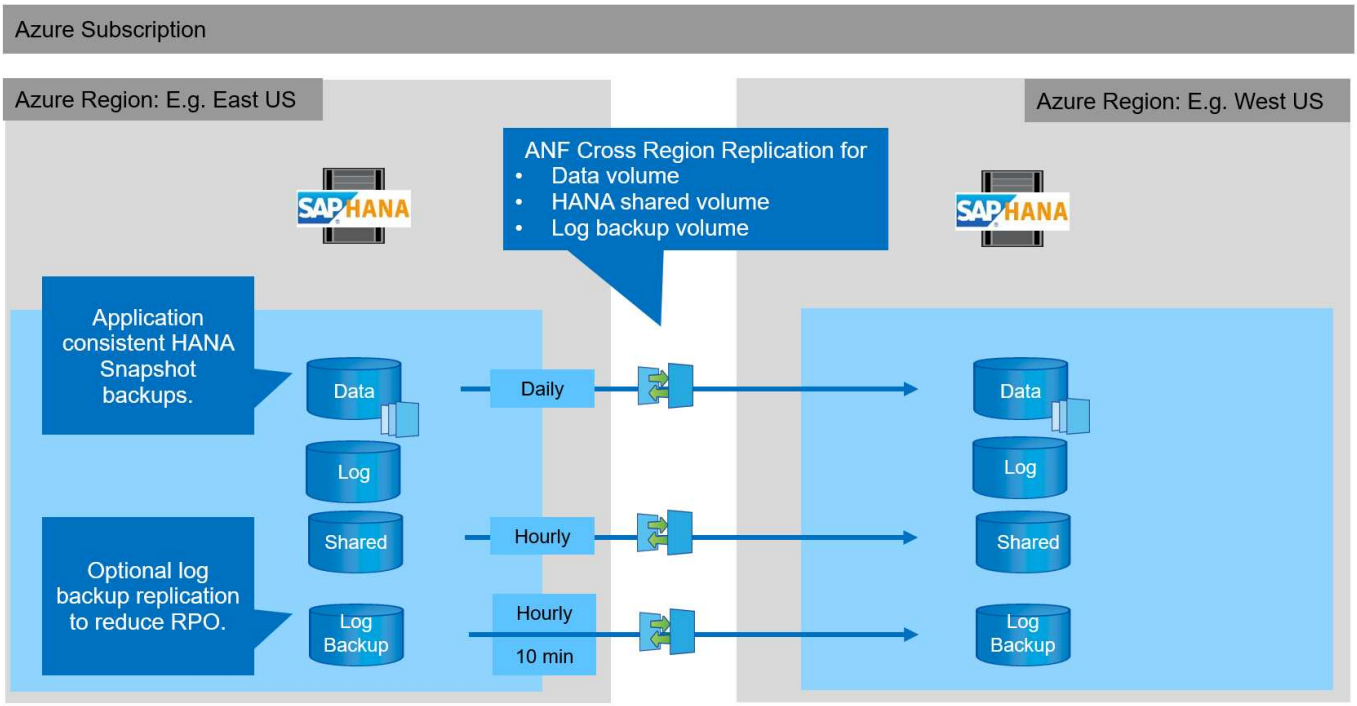
以下の概要とラボ環境は、 HANA データベースを対象としています。SAP 転送ディレクトリなどのその他の共有ファイルは、 HANA 共有ボリュームと同じように保護およびレプリケートされます。

ログバックアップを使用して HANA のセーブポイントリカバリまたはフォワードリカバリを有効にするに

は、アプリケーションと整合性のあるデータ Snapshot バックアップを、 HANA データボリュームのプライマリサイトに作成する必要があります。これは、 ANF バックアップツール AzAcSnap を使用した場合などに実行できます（も参照） "Azure NetApp Files | Microsoft Docs 用の Azure Application Consistent Snapshot ツールとは何ですか"）。プライマリサイトで作成された Snapshot バックアップが、 DR サイトにレプリケートされます。

災害時のフェイルオーバーの場合は、レプリケーション関係を解除し、ボリュームを DR 本番用サーバにマウントして、 HANA データベースを最後の HANA セーブポイントにリカバリするか、レプリケートされたログバックアップを使用してフォワードリカバリでリカバリする必要があります。の章"ディザスタリカバリフェイルオーバー"では、必要な手順について説明します。

次の図は、複数リージョンレプリケーション用の HANA 構成オプションを示しています。




現在のバージョンのクロスリージョンレプリケーションでは、固定のスケジュールのみを選択でき、実際のレプリケーション更新時間はユーザが定義することはできません。スケジュールは、毎日、毎時、および 10 分ごとに設定できます。これらのスケジュールオプションを使用すると、 RPO の要件に応じて、毎時または 10 分ごとの異なるスケジュールでのデータボリュームのレプリケーションとログバックアップのレプリケーションの 2 種類の設定が有効になります。達成可能な最小の RPO は約 20 分です。次の表に、設定オプションと、結果として得られる RPO と RTO の値を示します。

| | データボリュームのレプリケーション | データとログのバックアップ・ボリューム・リストア | データとログのバックアップ・ボリューム・リストア |
|---|---|---|---|
| CRR スケジュールのデータ・ボリューム | 毎日 | 毎日 | 毎日 |
| CRR のスケジュールログバックアップボリューム | 該当なし | 毎時 | 10 分 |
| 最大 RPO | +24 時間 + Snapshot スケジュール（ 6 時間など）+ | 1 時間 | 2 x 10 分 |

| | データボリュームのレプリケーション | データとログのバックアップ・ボリューム・リストア | データとログのバックアップ・ボリューム・リストア |
|---|---|---|---|
| 最大 RTO | 主に HANA の起動時間によって定義されます | + HANA の起動時間 + リカバリ時間 + | + HANA の起動時間 + リカバリ時間 + |
| フォワードリカバリ | 該当なし | + 過去 24 時間のログ + Snapshot スケジュール（ 6 時間など） + | + 過去 24 時間のログ + Snapshot スケジュール（ 6 時間など） + |

要件およびベストプラクティス

Microsoft Azure では、作成時や割り当て解除された VM の起動時に、特定の仮想マシン（ VM ）タイプの可用性が保証されません。具体的には、リージョンで障害が発生した場合、多くのクライアントでディザスタリカバリリージョンに追加の VM が必要になることがあります。そのため、ディザスタリカバリ領域でテストシステムまたは QA システムとして、必要なサイズの VM を、必要な VM タイプを割り当ててアクティブに使用することを推奨します。

コストを最適化するには、通常運用時にパフォーマンス階層を下げた ANF 容量プールを使用することを推奨します。データレプリケーションには高パフォーマンスは必要ないため、標準のパフォーマンス階層では大容量プールを使用する可能性があります。ディザスタリカバリのテストやディザスタフェイルオーバーが必要な場合は、高パフォーマンス階層を使用する大容量プールにボリュームを移動する必要があります。

2 つ目の容量プールがオプションでない場合は、通常運用時のパフォーマンス要件ではなく、容量要件に基づいてレプリケーションターゲットボリュームを設定する必要があります。クォータまたはスループット（手動 QoS の場合）は、ディザスタリカバリのテスト用にディザスタフェイルオーバーの際に適用できます。

詳細については、を参照してください "Azure NetApp Files ボリュームのリージョン間レプリケーションを使用する場合の要件と考慮事項 | Microsoft Docs"。

ラボのセットアップ

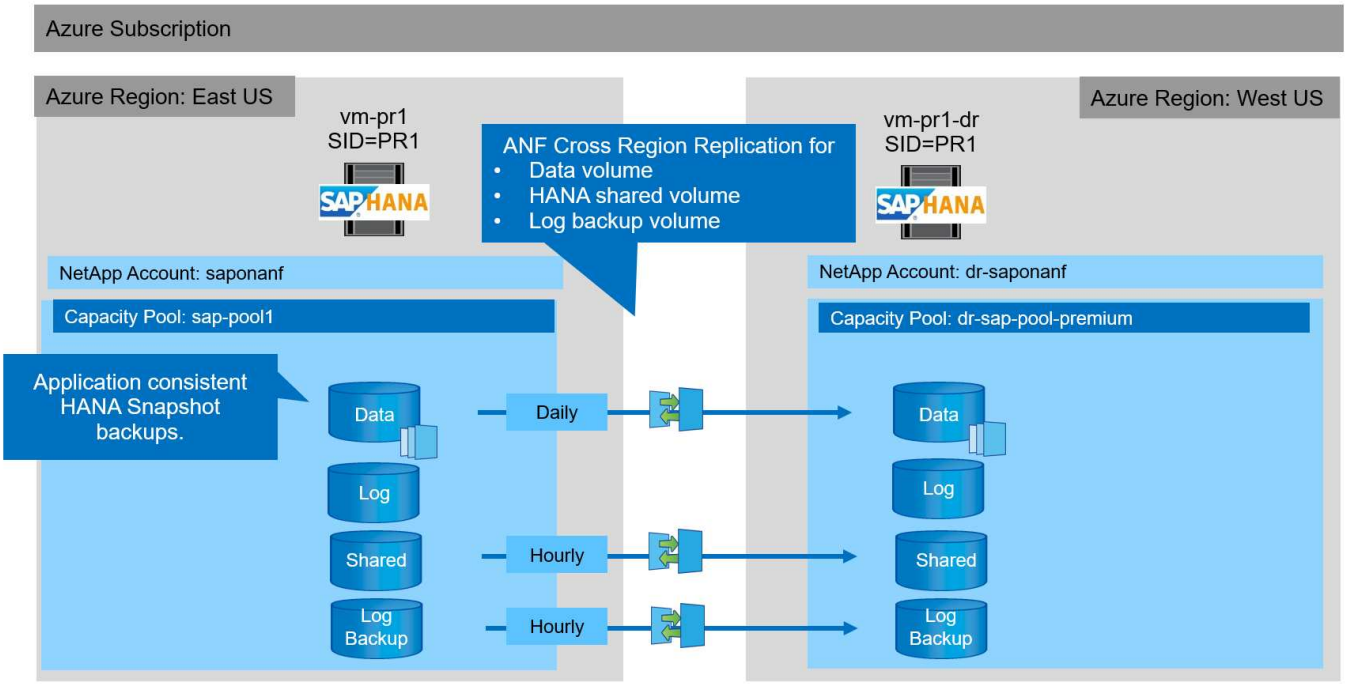
解決策の検証は、 SAP HANA シングルホストシステムで実行されています。ANF 用 Microsoft AzAcSnap Snapshot バックアップツールを使用して、 HANA アプリケーションと整合性のある Snapshot バックアップを設定しました。日次データボリューム、時間単位のログバックアップ、および共有ボリュームレプリケーションがすべて設定されました。ディザスタリカバリのテストとフェイルオーバーは、フォワードリカバリ処理と同様に、保存ポイントで検証済みです。

ラボ環境で使用しているソフトウェアのバージョンを次に示します。

- シングルホスト SAP HANA 2.0 SPS5 システムとシングルテナント
- SUSE SLES for SAP 15 SP1
- AzAcSnap 5.0

DR サイトに、手動 QoS を設定した単一の容量プールが設定されている。

次の図は、ラボのセットアップを示しています。

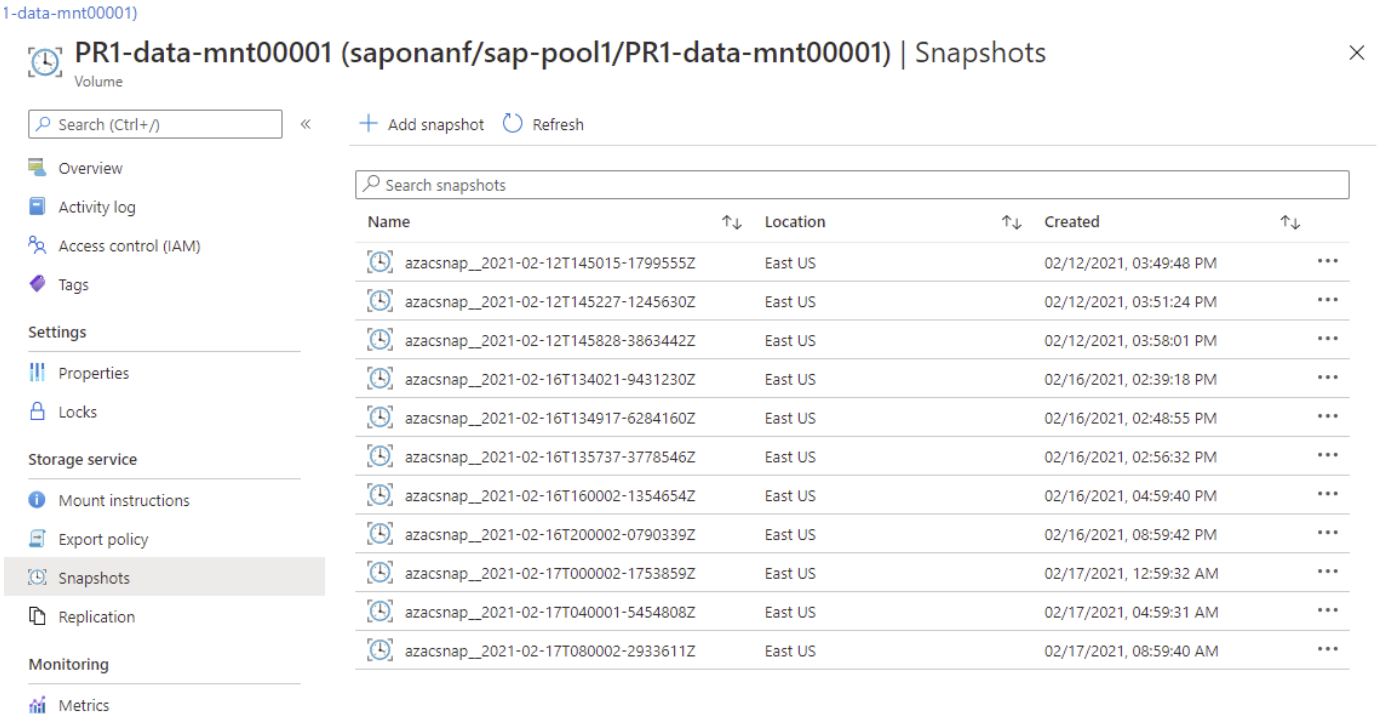



**AzAcSnap** を使用した **Snapshot** バックアップ設定

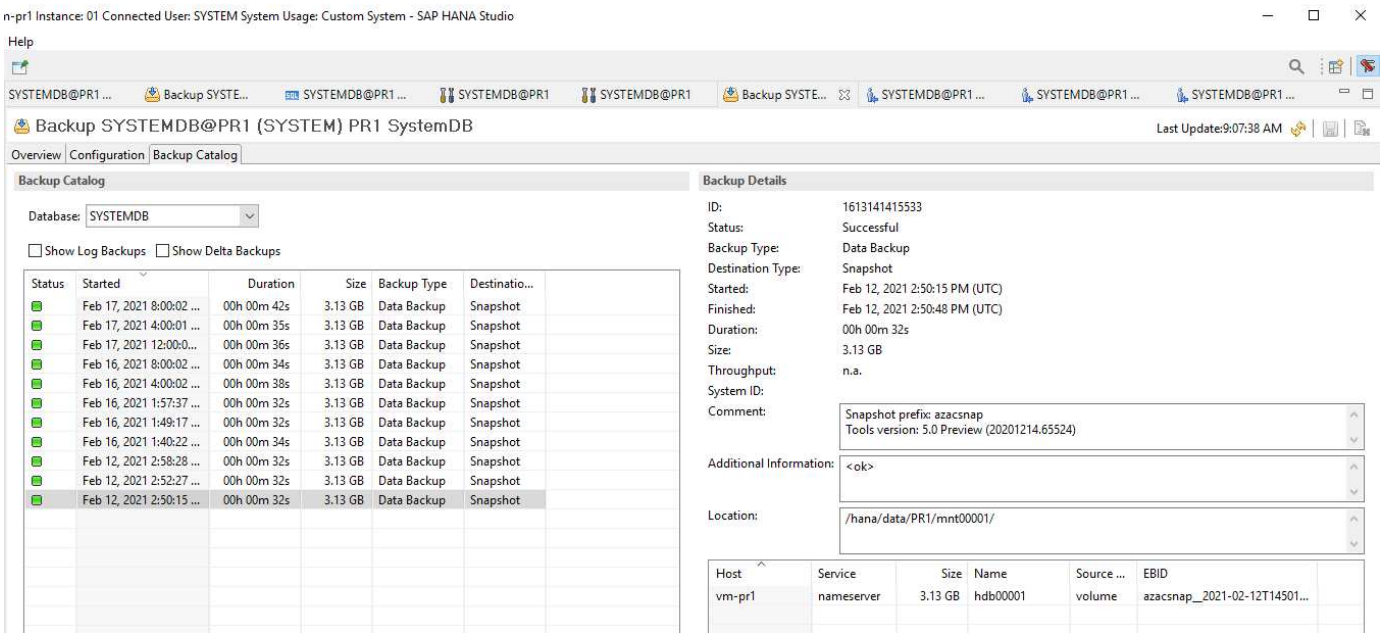
プライマリサイトでは、 HANA システム PR1 のアプリケーションと整合性のある Snapshot バックアップを作成するように AzAcSnap が設定されています。これらの Snapshot バックアップは、次の 2 つの図に示すように、 PR1 HANA システムの ANF データボリュームで利用でき、 SAP HANA バックアップカタログにも登録されています。Snapshot バックアップは 4 時間ごとにスケジュールされています。

ANF クロスリージョンレプリケーションを使用してデータボリュームをレプリケーションすると、これらの Snapshot バックアップがディザスタリカバリサイトにレプリケートされ、 HANA データベースのリカバリに使用できます。

次の図は、 HANA データボリュームの Snapshot バックアップを示しています。




次の図は、 SAP HANA のバックアップカタログを示しています。




**ANF** クロスリージョンレプリケーションの設定手順

ボリュームレプリケーションを設定する前に、ディザスタリカバリサイトでいくつかの準備手順を実行する必要があります。

- ネットアップアカウントが利用可能で、ソースと同じ Azure サブスクリプションで設定されている必要があります。
- 容量プールは、前述のネットアップアカウントを使用して使用および設定する必要があります。
- 仮想ネットワークが使用可能で、設定されている必要があります。

- 仮想ネットワーク内で ANF で使用するためには、委任サブネットが使用可能で構成されている必要があります。

HANA データ、 HANA 共有、 HANA ログバックアップボリュームの保護ボリュームを作成できるようになりました。このラボ環境でのデスティネーションボリュームの設定を次の表に示します。

最高のレイテンシを実現するには、災害時のフェイルオーバー時に SAP HANA を実行する VM の近くにボリュームを配置する必要があります。そのため、他の SAP HANA 本番システムと同じピン固定プロセスが DR ボリュームに必要です。

| **HANA** ボリューム | ソース | 宛先 | レプリケーションスケジュール |
|---|---|---|---|
| HANA データボリューム | pr1 -data-mnt00001 | pr1 -data-mnt00001 -sm -dest | 毎日 |
| HANA 共有ボリューム | PR1 - 共有 | pr1 -shared-sm-dest | 毎時 |
| HANA のログ / カタログのバックアップボリューム | ハンナバックアップ | hanabackup-sm -dest | 毎時 |

ボリュームごとに、次の手順を実行する必要があります。

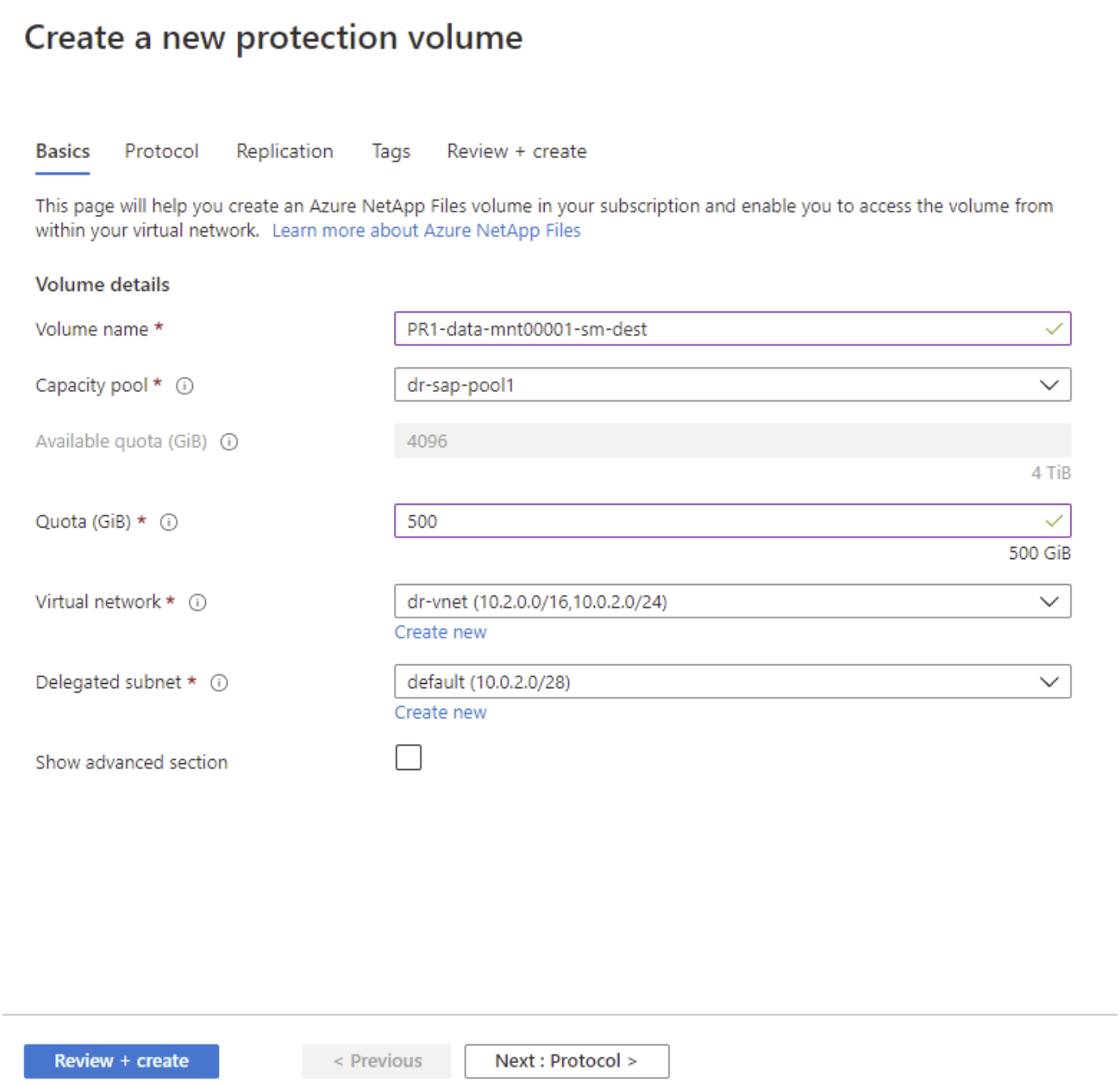
1. DR サイトに新しい保護ボリュームを作成します。
   a. ボリューム名、容量プール、クォータ、およびネットワークの情報を指定します。
   b. プロトコルとボリュームのアクセス情報を指定します。
   c. ソースボリュームの ID とレプリケーションスケジュールを指定します。
   d. ターゲットボリュームを作成します。
2. ソースボリュームでレプリケーションを許可します。
   - ターゲットボリュームの ID を指定します。

以下のスクリーンショットは、設定手順を詳しく示しています。

ディザスタリカバリサイトでは、ボリュームを選択して Add Data Replication （データレプリケーションの追加）をクリックすることで、新しい保護ボリュームが作成されます。[Basics] タブでは、ボリューム名、容量プール、およびネットワーク情報を入力する必要があります。

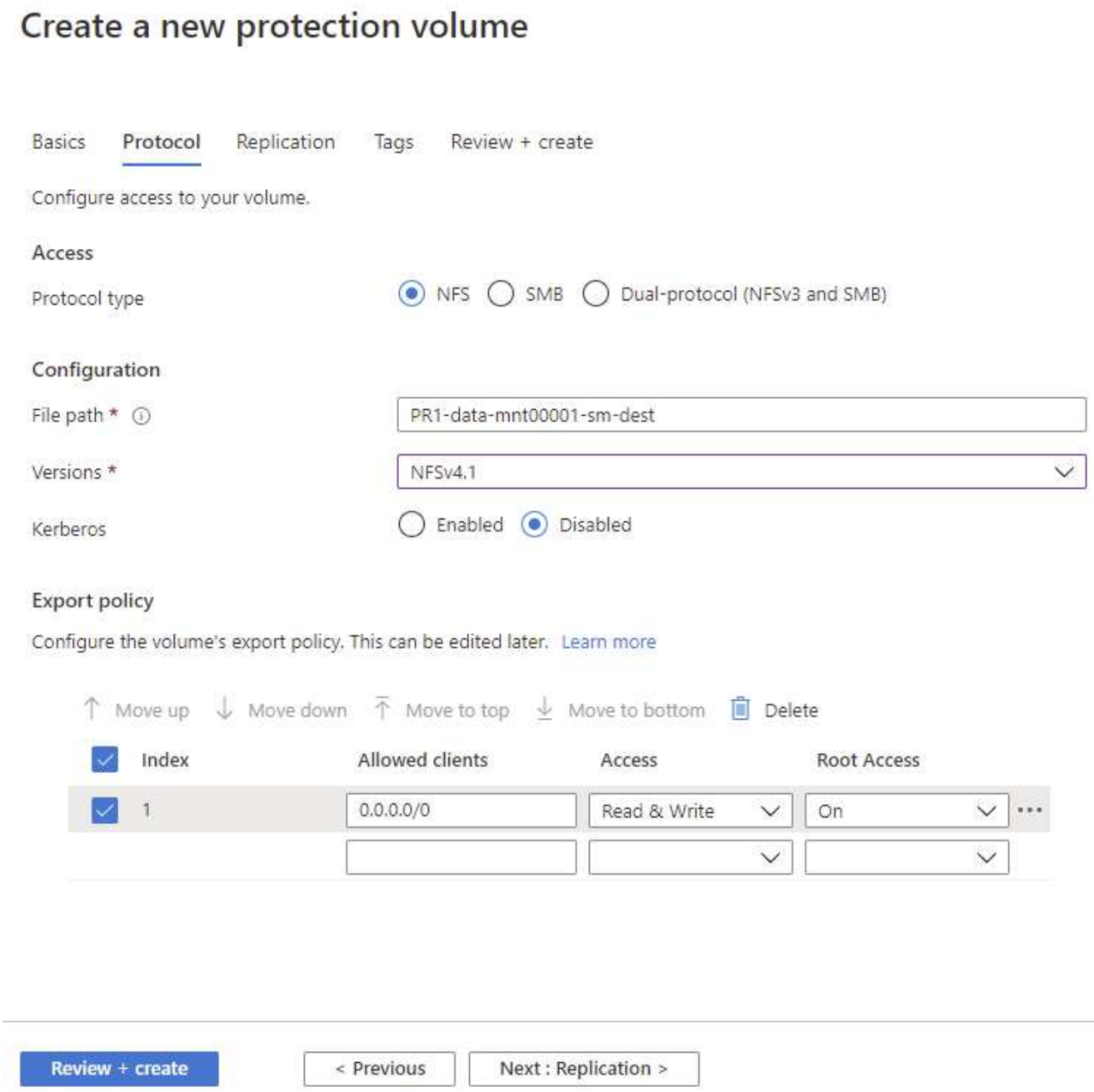
ボリュームのパフォーマンスはレプリケーションプロセスには影響しないため、ボリュームのクォータは容量要件に基づいて設定できます。ディザスタリカバリフェイルオーバーの場合は、実際のパフォーマンス要件を満たすようにクォータを調整する必要があります。

容量プールで QoS が手動で設定されている場合は、容量の要件に加えてスループットも設定できます。上記と同様に、通常運用時はスループットの値を低く設定して、ディザスタリカバリフェイルオーバー時に設定することができます。



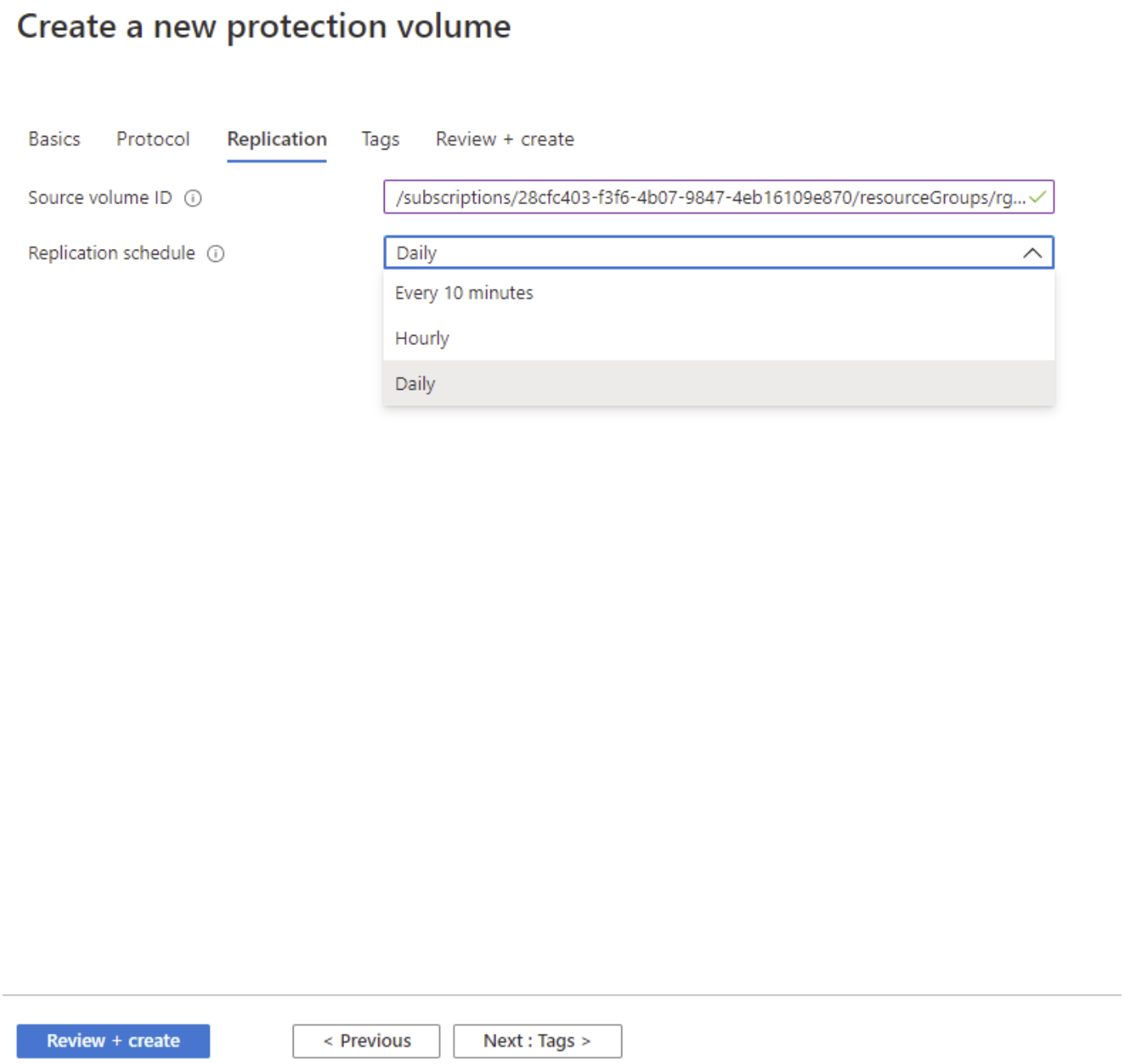

Protocol タブで、ネットワークプロトコル、ネットワークパス、およびエクスポートポリシーを指定する必要があります。

プロトコルは、ソースボリュームで使用されているプロトコルと同じである必要があります。



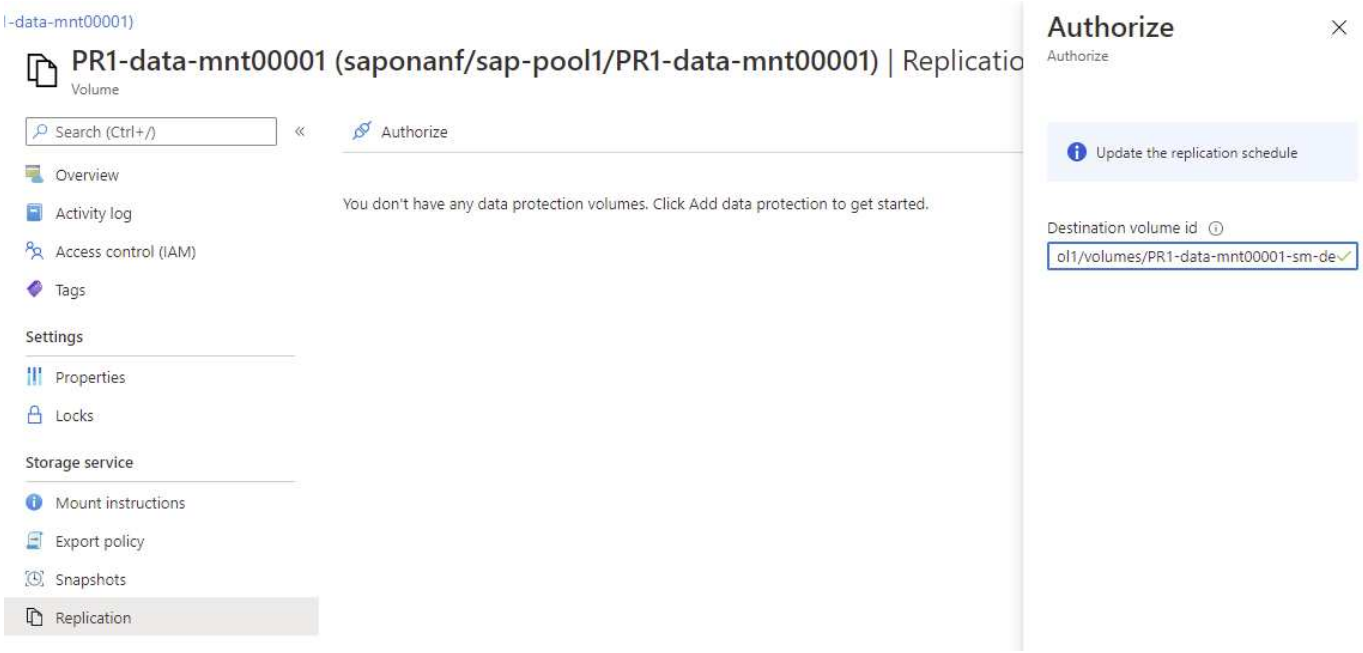

Replication （レプリケーション）タブで、ソースボリューム ID とレプリケーションスケジュールを設定する必要があります。データボリュームのレプリケーションについては、ラボのセットアップで日次レプリケーションスケジュールを設定しました。

ソースボリュームの ID は、ソースボリュームのプロパティ画面からコピーできます。




最後の手順として、ターゲットボリュームの ID を指定してソースボリュームでレプリケーションを許可する必要があります。

デスティネーションボリュームのプロパティ画面からデスティネーションボリューム ID をコピーできます。




HANA 共有ボリュームとログバックアップボリュームで同じ手順を実行する必要があります。

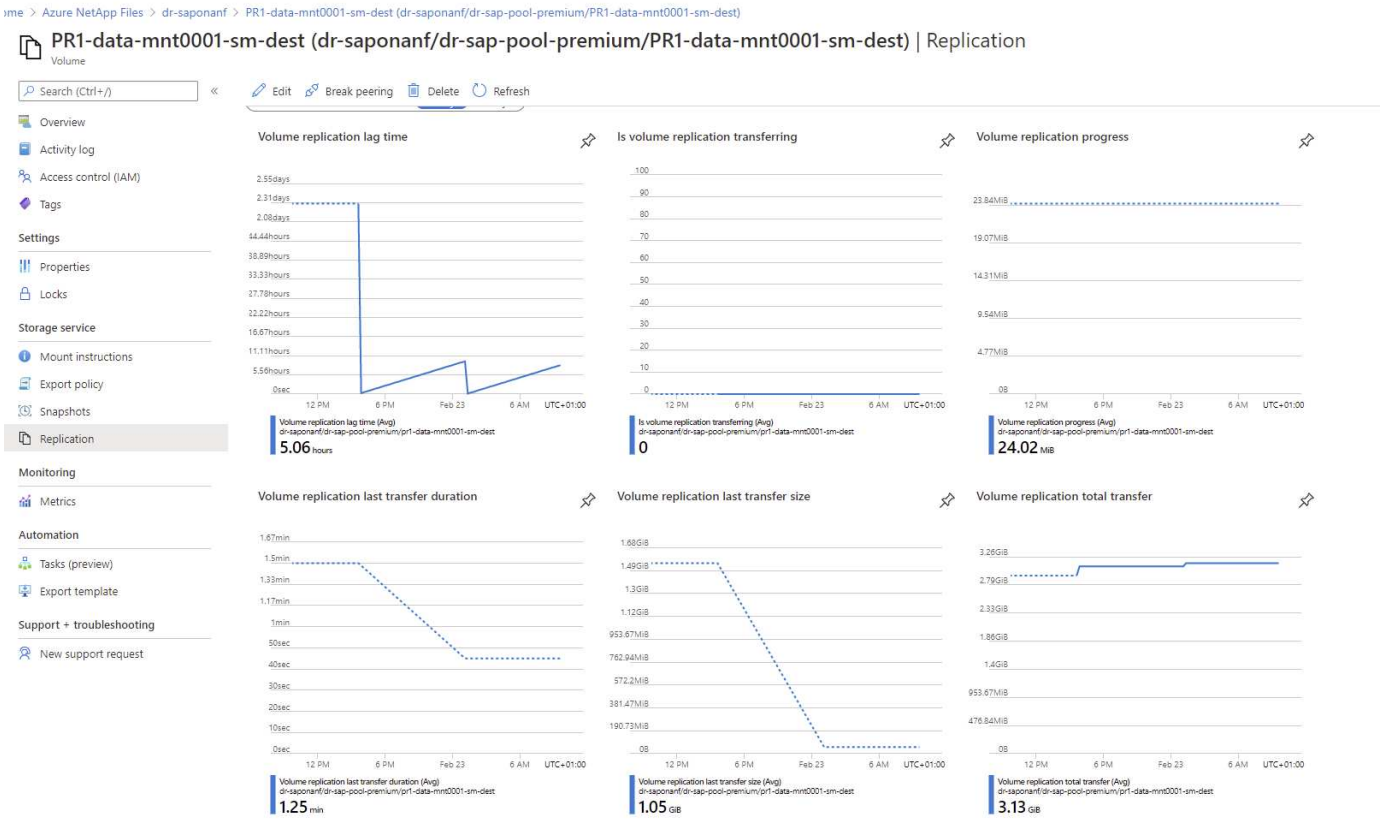
**ANF** のクロスリージョンレプリケーションを監視しています

次に示す 3 つのスクリーンショットは、データ、ログバックアップ、および共有ボリュームのレプリケーションステータスを示しています。

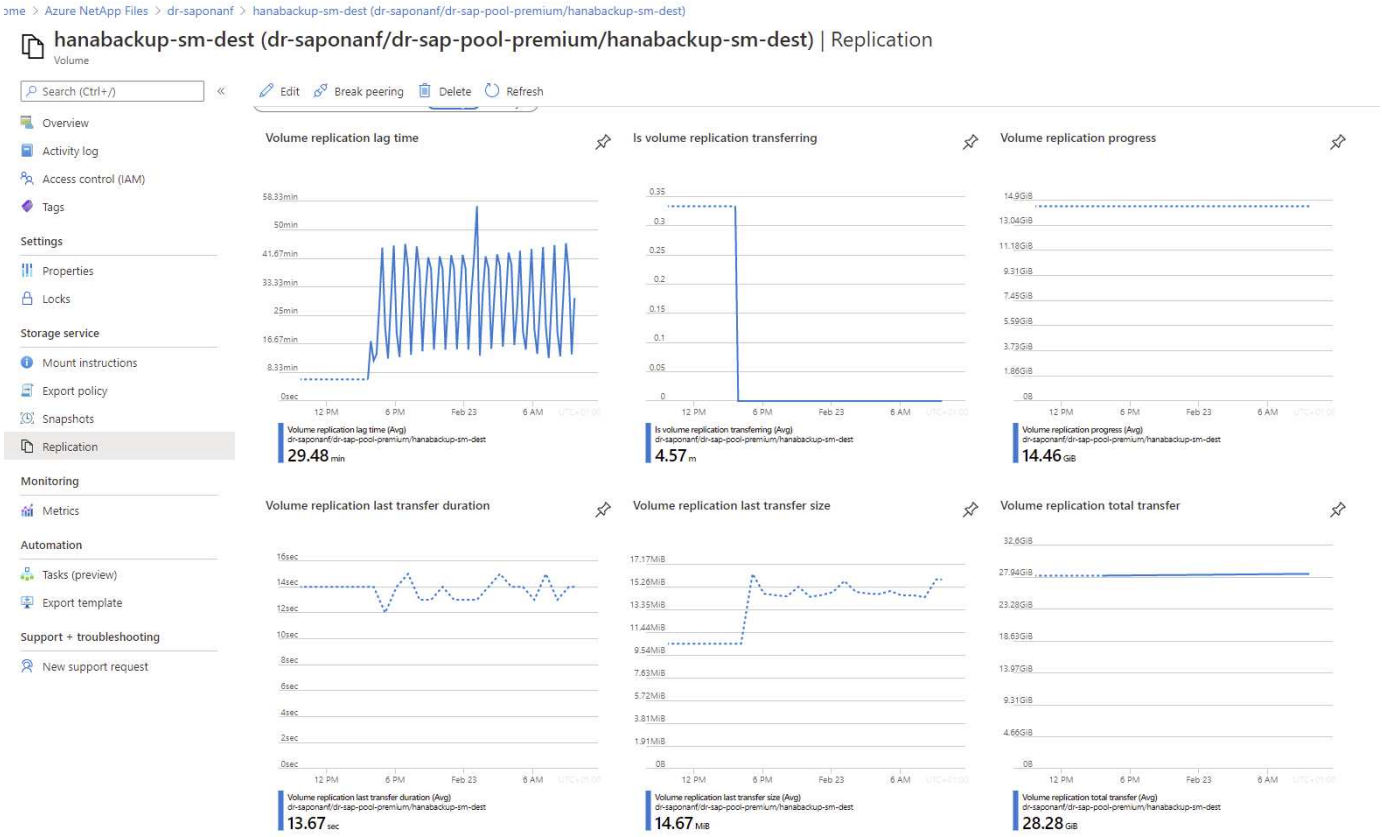
ボリュームレプリケーションの遅延時間は、 RPO の期待値を把握するのに役立ちます。たとえば、ログバックアップボリュームのレプリケーションで最大遅延時間が 58 分と表示されています。つまり、 RPO の最大値は同じです。

転送時間と転送サイズによって、必要な帯域幅とレプリケートされたボリュームの速度に関する有用な情報が提供されます。

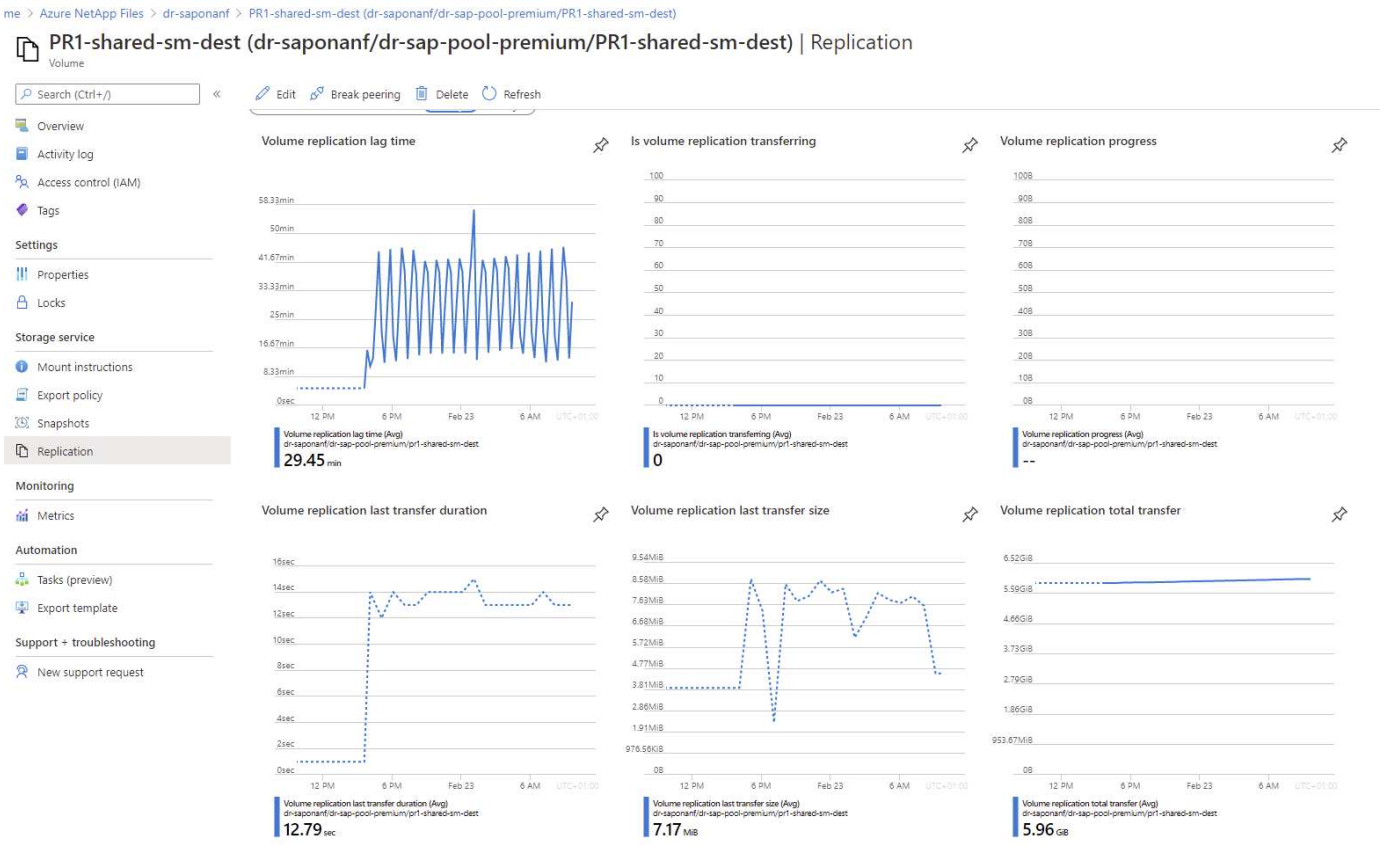
次のスクリーンショットは、 HANA データボリュームのレプリケーションステータスを示しています。




次のスクリーンショットは、 HANA のログバックアップボリュームのレプリケーションステータスを示しています。



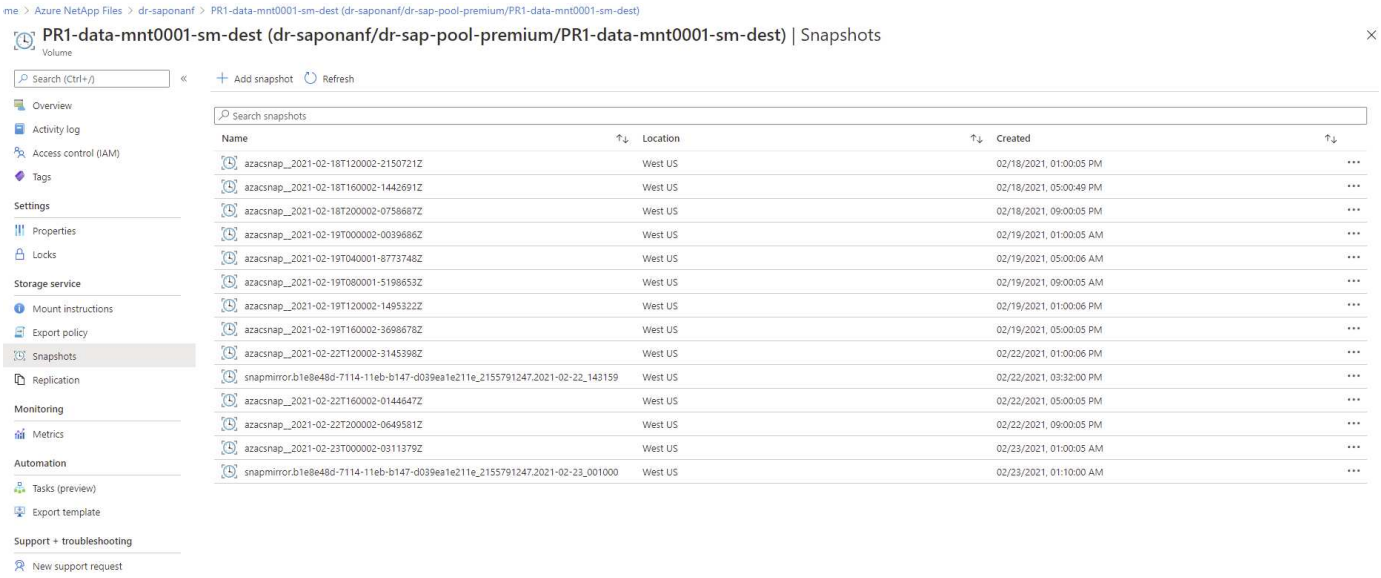
次のスクリーンショットは、 HANA 共有ボリュームのレプリケーションステータスを示しています。




レプリケートされた **Snapshot** バックアップ

ソースボリュームからターゲットボリュームへのレプリケーションの更新が行われるたびに、前回と現在の更新の間に行われたすべてのブロックの変更がターゲットボリュームにレプリケートされます。これには、ソースボリュームで作成された Snapshot も含まれます。次のスクリーンショットは、ターゲットボリュームで使用可能な Snapshot を示しています。すでに説明したように、 AzAcSnap ツールによって作成される各スナップショットは、アプリケーションと整合性のある HANA データベースのイメージであり、セーブポイントまたはフォワードリカバリのいずれかを実行するために使用できます。

ソースボリュームとターゲットボリュームに SnapMirror Snapshot コピーが作成され、再同期処理とレプリケーション更新処理にも使用されます。これらの Snapshot コピーは、 HANA データベースの観点からはアプリケーションと整合性がありません。 HANA のリカバリ処理には、 AzaCSsnap で作成されたアプリケーションと整合性のある Snapshot のみを使用できます。




# ディザスタリカバリのテスト

ディザスタリカバリのテスト

## 効果的なディザスタリカバリ戦略を実装するには、必要なワークフローをテストする必要があります。テストでは、戦略が機能するかどうか、および内部ドキュメントで十分かどうかを検証し、管理者が必要な手順についてトレーニングできるようにします。

ANF のクロスリージョンレプリケーションにより、 RTO と RPO をリスクにさらすことなくディザスタリカバリテストを実施できます。ディザスタリカバリのテストは、データレプリケーションを中断することなく実行できます。

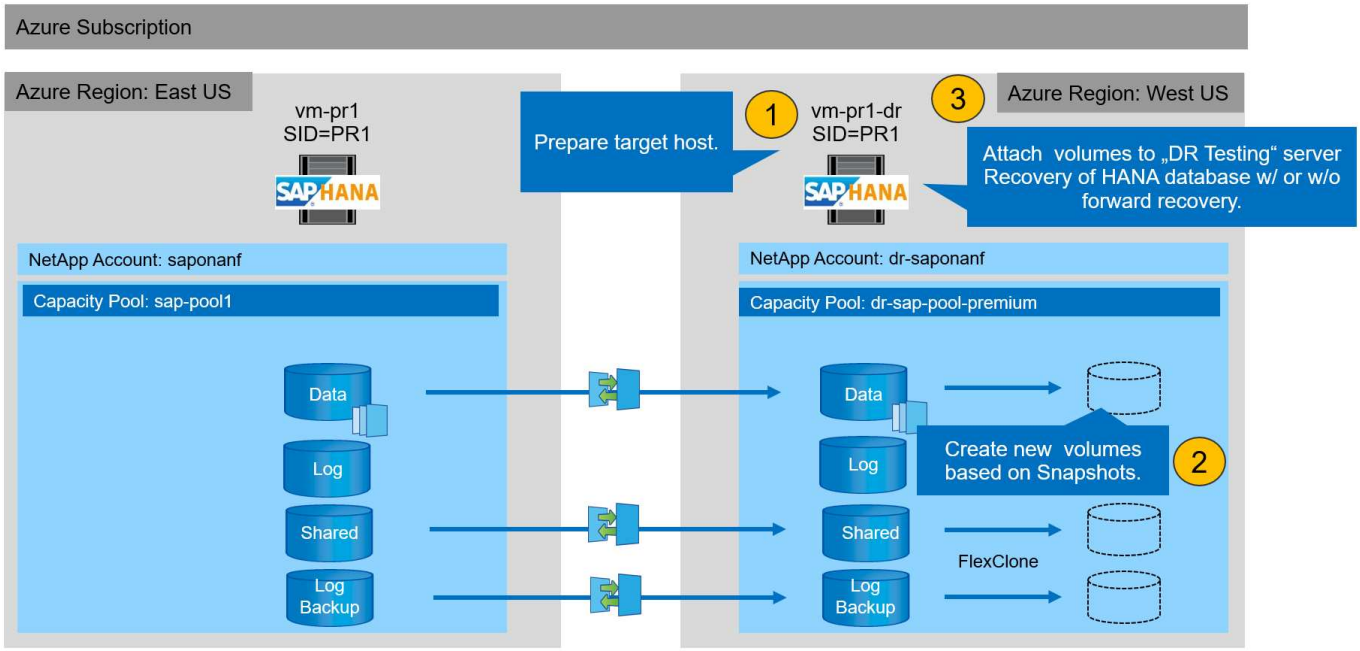
ディザスタリカバリテストのワークフローでは、 ANF 機能セットを利用して、ディザスタリカバリターゲットの既存の Snapshot バックアップに基づいて新しいボリュームを作成します。を参照してください "Azure NetApp Files スナップショットの仕組み | Microsoft Docs"。

ログバックアップレプリケーションがディザスタリカバリの設定に含まれているかどうかに応じて、ディザスタリカバリの手順は少し異なります。ここでは、データバックアップのみのレプリケーション、およびログバックアップボリュームのレプリケーションと組み合わせたデータボリュームのレプリケーションに対するディザスタリカバリのテストについて説明します。

ディザスタリカバリテストを実行するには、次の手順を実行します。

1. ターゲットホストを準備します。
2. ディザスタリカバリサイトでの Snapshot バックアップに基づいて新しいボリュームを作成します。
3. ターゲットホストに新しいボリュームをマウントします。
4. HANA データベースをリカバリします。
    - データボリュームのリカバリのみ
    - レプリケートされたログバックアップを使用してリカバリを転送する。

以降のサブセクションで、これらの手順について詳しく説明します。




ターゲットホストを準備します

## ここでは、ディザスタリカバリフェイルオーバーに使用するサーバで必要な準備手順について説明します。

通常運用時は、 HANA の QA やテスト用システムなど、通常はターゲットホストがその他の目的に使用されます。そのため、災害時のフェイルオーバーテストを実行する際には、ほとんどの手順を実行する必要があります。一方、関連する構成ファイルは、「 /etc/fstab 」や「 /usr/sap/sapservices 」のように準備し、構成ファイルをコピーするだけで運用に移すことができます。ディザスタリカバリフェイルオーバー手順は、準備された関連する構成ファイルが確実に正しく設定されるようにします。

ターゲット・ホストの準備には、 HANA の QA またはテスト・システムのシャットダウン、および「 systemctl stop sapinit 」を使用したすべてのサービスの停止も含まれます。

### ターゲットサーバのホスト名と **IP** アドレス

ターゲット・サーバのホスト名は ' ソース・システムのホスト名と同じである必要がありますIP アドレスは異なっていてもかまいません。

ターゲットサーバが他のシステムと通信できないように、ターゲットサーバの適切なフェンシングを確立する必要があります。適切なフェンシングが設定されていないと、クローニングされた本番用システムは、他の本番用システムとデータを交換し、論理的にデータが破損する可能性があります。

### 必要なソフトウェアをインストールします

SAP ホストエージェントソフトウェアをターゲットサーバにインストール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 "SAP ホストエージェント" SAP ヘルプポータルで、次の作業を行います。

ホストが HANA QA またはテストシステムとして使用されている場合は、 SAP ホストエージェントソフトウェアがすでにインストールされています。

ユーザ、ポート、および **SAP** サービスを設定する

ターゲットサーバに、 SAP HANA データベースに必要なユーザとグループが配置されている必要があります。通常は、ユーザの一元管理が使用されるため、ターゲットサーバで設定手順を行う必要はありません。HANA データベースに必要なポートは、ターゲットホストで設定する必要があります。構成は '/etc/services ファイルをターゲット・サーバにコピーすることによって ' ソース・システムからコピーできます

必要な SAP サービスのエントリがターゲットホストにあることが必要です。/usr/sap/sapservices' ファイルをターゲットサーバにコピーすることで ' ソースシステムから構成をコピーできます次の出力は、このラボ環境で使用する SAP HANA データベースの必須エントリを示しています。

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
limit.descriptors=1048576
```

**HANA** のログボリュームを準備

HANA のログボリュームはレプリケーションの一部ではないため、空のログボリュームがターゲットホストに存在している必要があります。ログボリュームには、ソース HANA システムと同じサブディレクトリを含める必要があります。

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root   root   4096 Feb 19 16:20 .
drwxr-xr-x 3 root   root     22 Feb 18 13:38 ..
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

ログバックアップボリュームを準備

ソースシステムは HANA ログバックアップ用の個別のボリュームで構成されているため、ターゲットホストにログバックアップボリュームも必要です。ログバックアップ用のボリュームを設定し、ターゲットホストにマウントする必要があります。

ディザスタリカバリの設定でログバックアップボリュームのレプリケーションを行う場合、複製されたログバックアップボリュームはターゲットホストにマウントされるため、追加のログバックアップボリュームを準備する必要はありません。

ファイルシステムのマウントを準備

次の表に、このラボ環境で使用する命名規則を示します。災害復旧サイトのボリューム名は '/etc/fstab に含まれています

| **HANA PR1** ボリューム | ディザスタリカバリサイトにあるボリュームとサブディレクトリ | ターゲットホストのマウントポイント |
|---|---|---|
| データボリューム | pr1 -data-mnt00001 -sm -dest | /hana/data /pr1/mnt00001 |
| 共有ボリューム | pr1 -shared-sm-dest/shared pr1 -shared-sm-dest/usr -sap-pr1 | /hana/shared /usr/sap/pr1 |
| ログバックアップボリューム | hanabackup-sm -dest | / はなんバックアップ |

このテーブルのマウントポイントは、ターゲットホストに作成する必要があります。

ここでは ' 必須の /etc/fstab エントリを示します

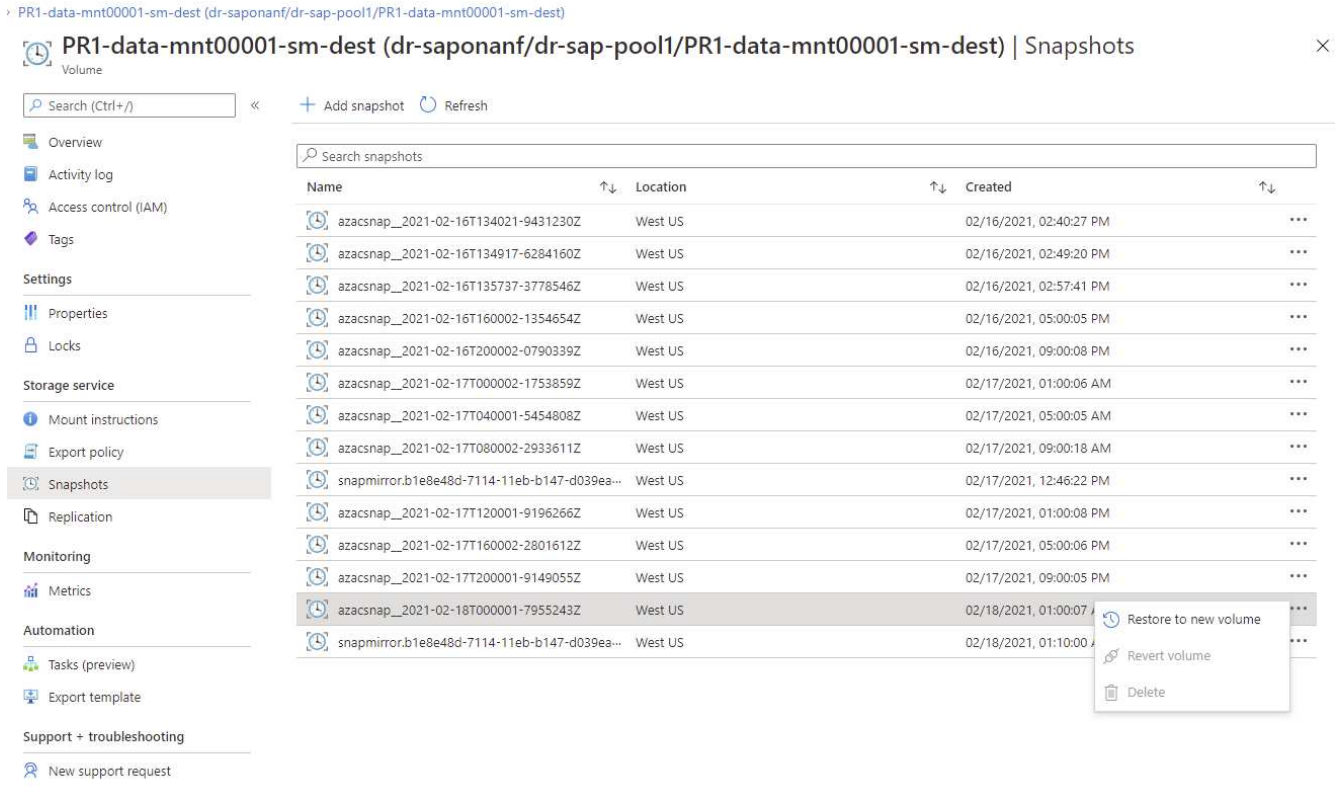
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest    /hanabackup nfs
rw,vers=3,hard,timeo=600,rsize=262144,wsize=262144,nconnect=8,bg,noatime,n
olock 0 0
```

ディザスタリカバリサイトでの **Snapshot** バックアップに基づいて新しいボリュームを作成します

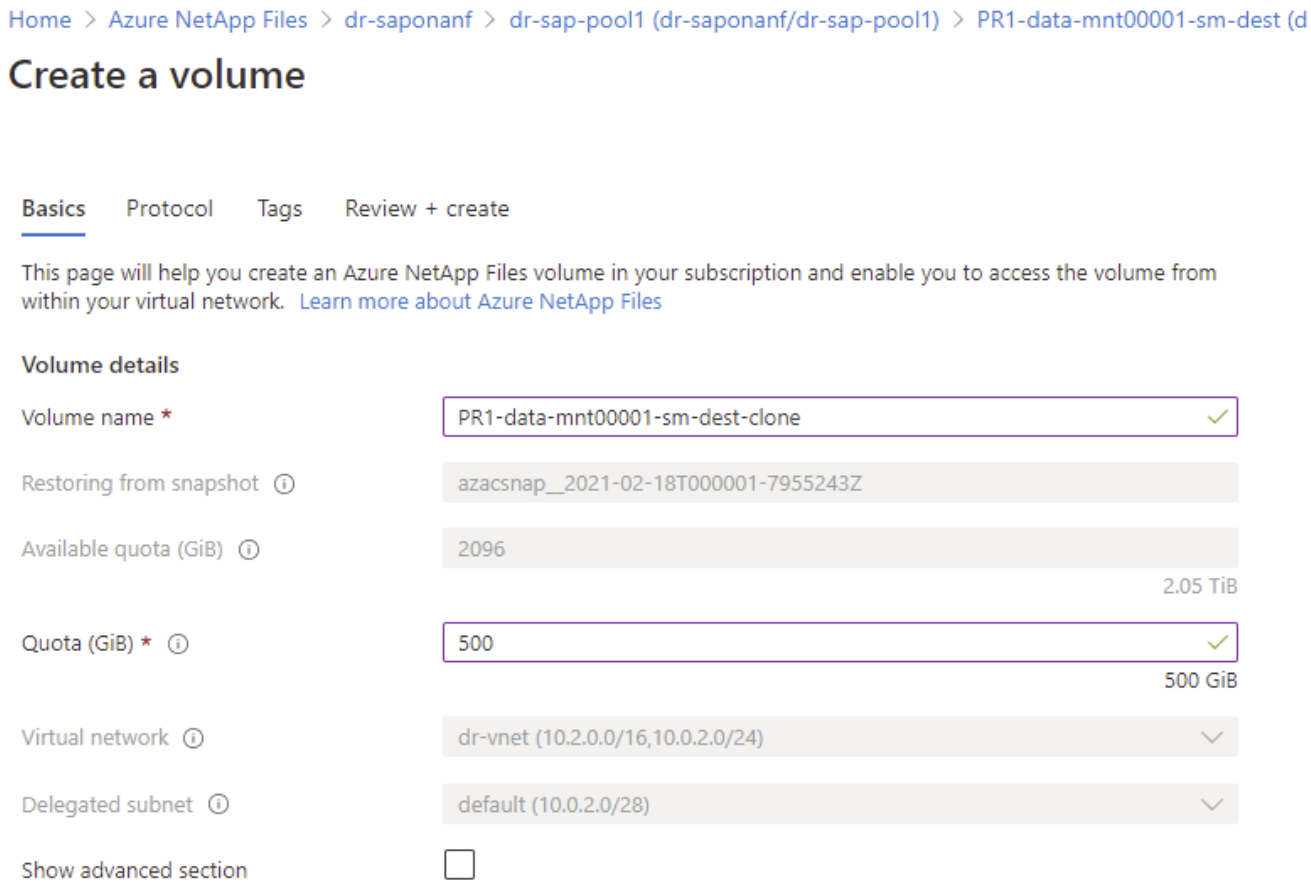
## ディザスタリカバリの設定によっては（ログバックアップレプリケーションを使用するかどうかに関係なく）、 Snapshot バックアップに基づいて 2 つまたは 3 つの新しいボリュームを作成する必要があります。どちらの場合も、データの新しいボリュームと HANA 共有ボリュームを作成する必要があります。

ログバックアップデータもレプリケートする場合は、ログバックアップボリュームの新しいボリュームを作成する必要があります。この例では、データとログバックアップボリュームがディザスタリカバリサイトにレプリケートされています。以下の手順では、 Azure Portal を使用します。

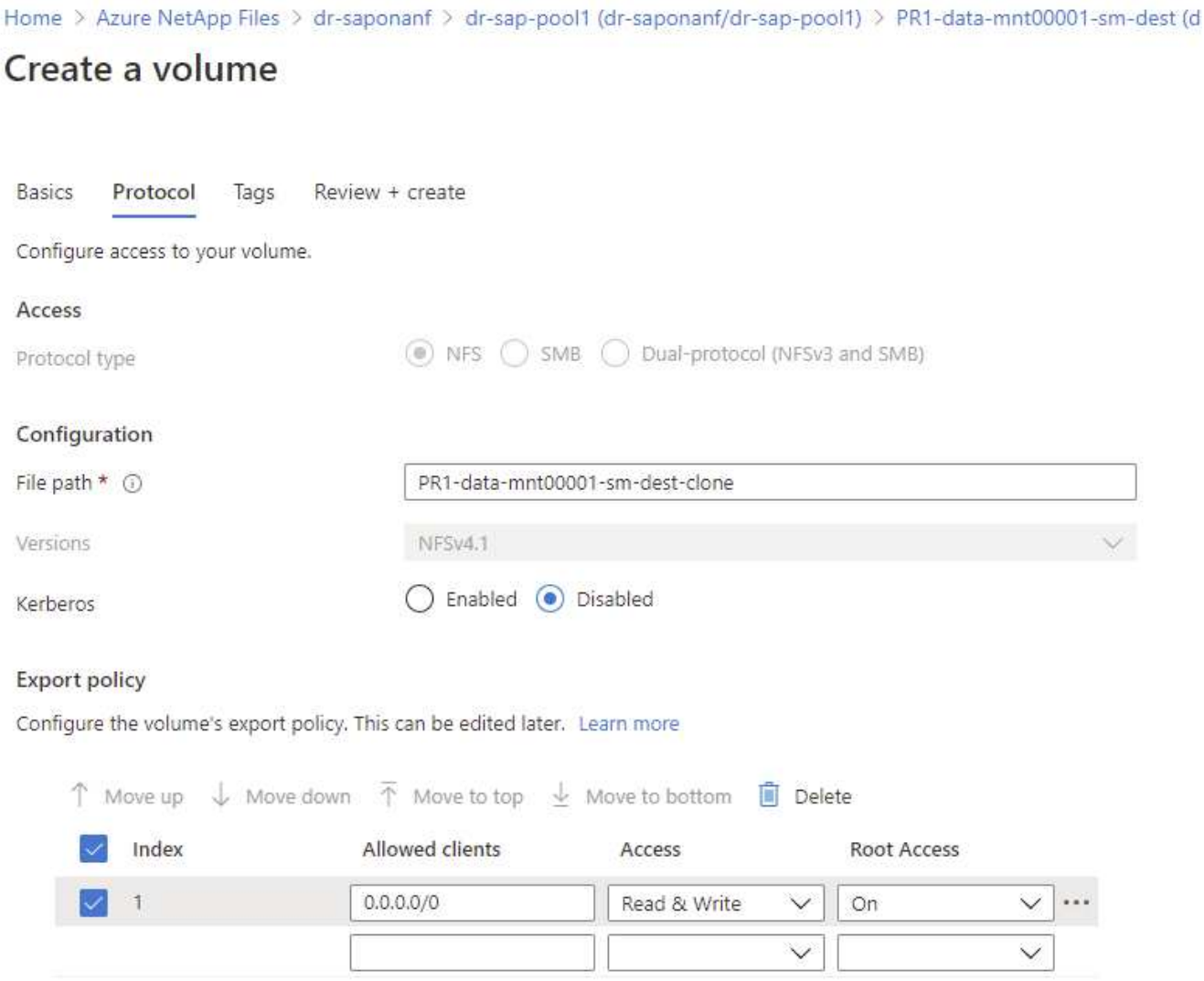
1. アプリケーションと整合性のある Snapshot バックアップの 1 つが、 HANA データボリュームの新しいボリュームのソースとして選択されています。新規ボリュームへのリストアは、 Snapshot バックアップに基づいて新しいボリュームを作成する場合に選択されます。



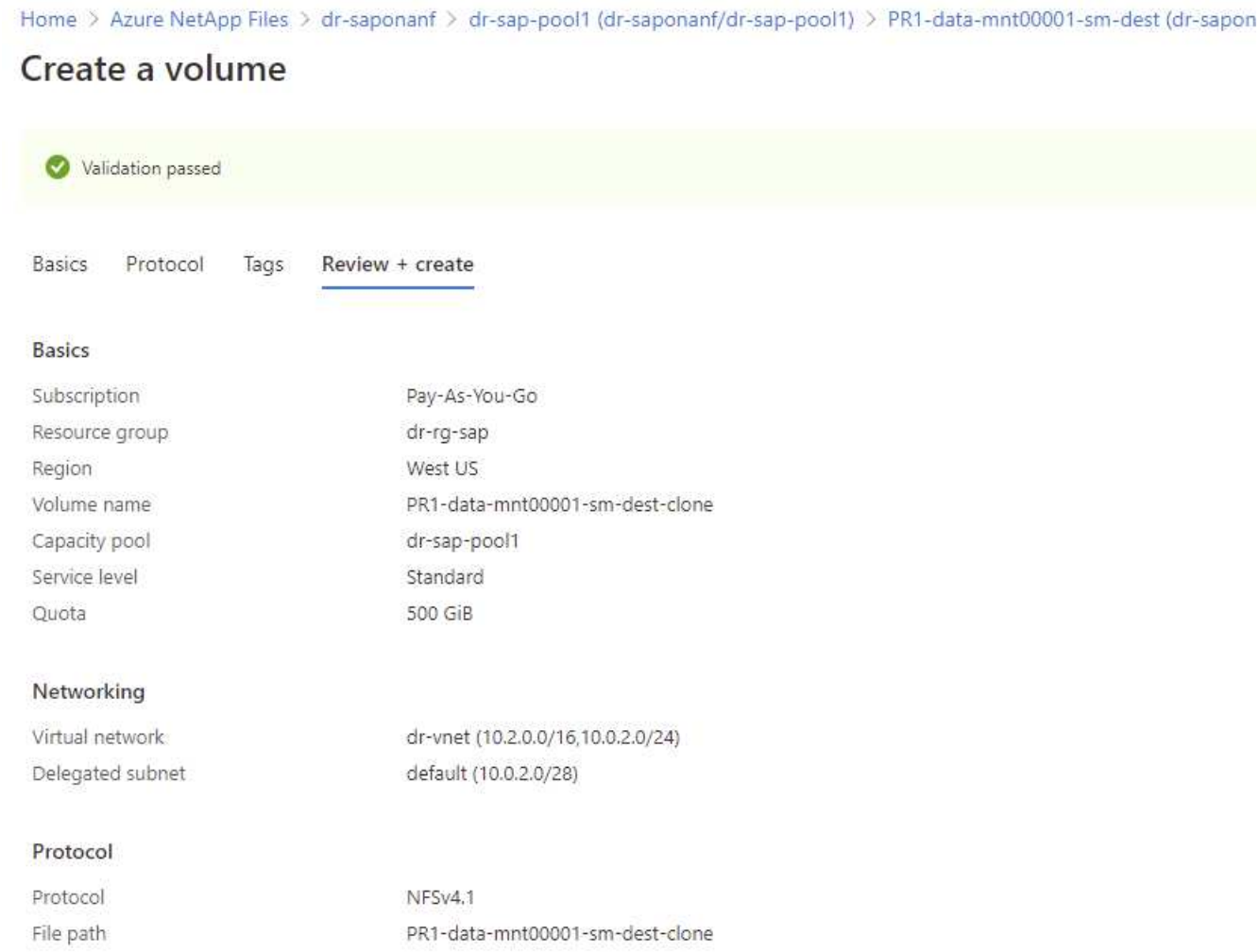

2. 新しいボリューム名とクォータをユーザインターフェイスに指定する必要があります。



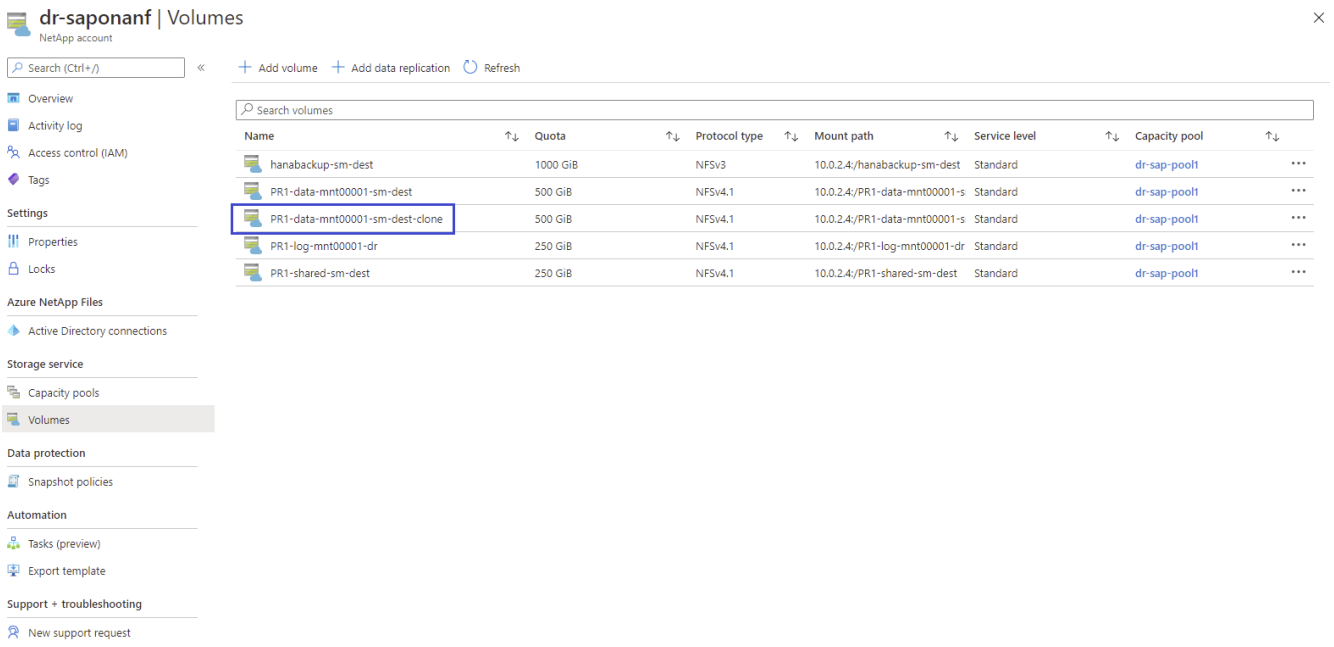
3. プロトコルタブでは、ファイルパスとエクスポートポリシーが設定されます。



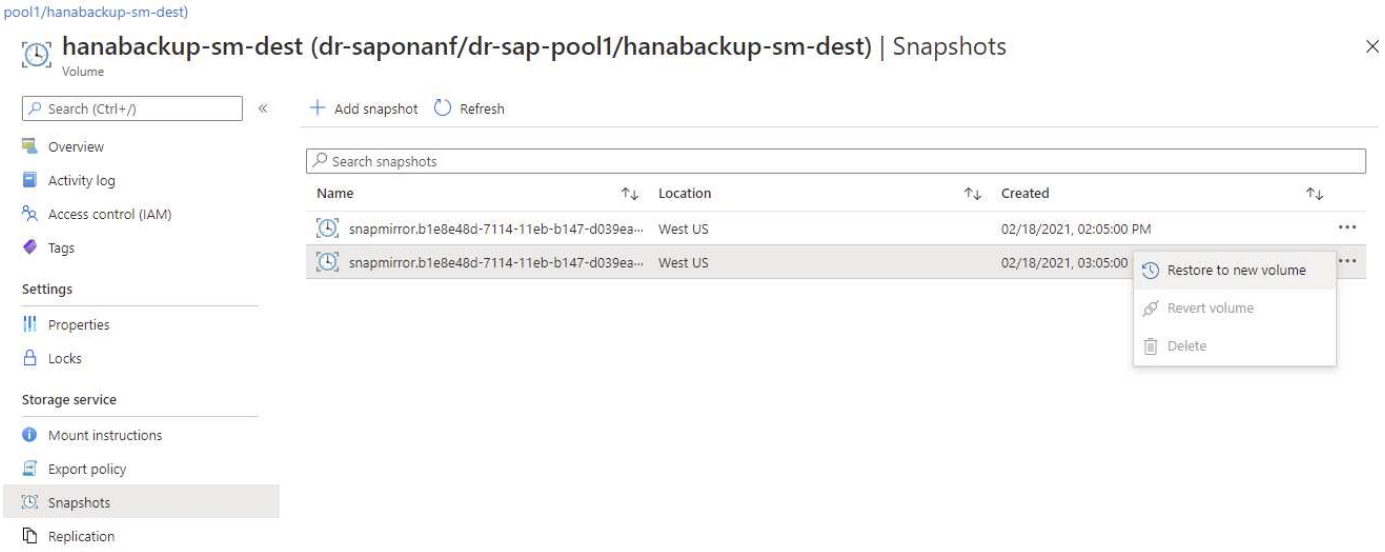

4. Create and Review （作成およびレビュー）画面に構成の概要が表示されます。



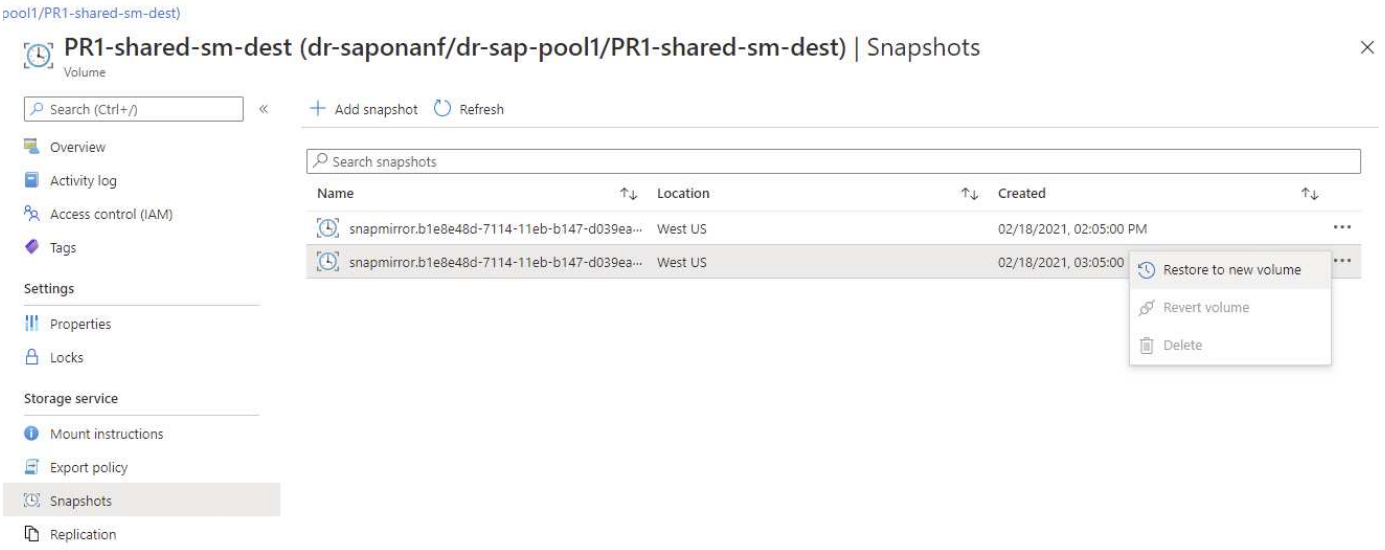

5. これで、 HANA の Snapshot バックアップに基づいて新しいボリュームが作成されました。



次の 2 つのスクリーンショットに示すように、 HANA 共有ボリュームとログバックアップボリュームで同じ手順を実行する必要があります。HANA の共有バックアップボリュームとログバックアップボリュームには Snapshot が追加で作成されていないため、新しいボリュームのソースとして最新の SnapMirror Snapshot コピーを選択する必要があります。これは非構造化データであり、 SnapMirror Snapshot コピーを使用してこのユースケースに対応できます。




次のスクリーンショットは、新しいボリュームにリストアされた HANA 共有ボリュームを示しています。






高パフォーマンス階層が低い大容量プールを使用している場合は、必要なパフォーマンスを提供する容量プールにボリュームを移動する必要があります。

これで 3 つの新しいボリュームがすべて使用できるようになり、ターゲットホストにマウントできるようになります。

ターゲットホストに新しいボリュームをマウントします

## これで ' 前に作成した /etc/fstab ファイルに基づいて ' 新しいボリュームをターゲット・ホストにマウントできるようになります

```
vm-pr1:~ # mount -a
```

次の出力は、必要なファイルシステムを示しています。

```
vm-pr1:/hana/data/PR1/mnt00001/hdb00001 # df
Filesystem                                          1K-blocks     Used
Available Use% Mounted on
devtmpfs                                             8190344        8
8190336   1% /dev
tmpfs                                               12313116        0
12313116   0% /dev/shm
tmpfs                                                8208744    17292
8191452   1% /run
tmpfs                                                8208744        0
8208744   0% /sys/fs/cgroup
/dev/sda4                                           29866736  2438052
27428684   9% /
/dev/sda3                                            1038336   101520
936816  10% /boot
/dev/sda2                                             524008     1072
522936   1% /boot/efi
/dev/sdb1                                           32894736    49176
31151560   1% /mnt
tmpfs                                                1641748        0
1641748   0% /run/user/0
10.0.2.4:/PR1-log-mnt00001-dr                    107374182400      256
107374182144   1% /hana/log/PR1/mnt00001
10.0.2.4:/PR1-data-mnt00001-sm-dest-clone      107377026560  6672640
107370353920   1% /hana/data/PR1/mnt00001
10.0.2.4:/PR1-shared-sm-dest-clone/hana-shared 107377048320 11204096
107365844224   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest-clone/usr-sap-PR1 107377048320 11204096
107365844224   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest-clone             107379429120 35293440
107344135680   1% /hanabackup
```

**HANA** データベースのリカバリ

## 以下は、 HANA データベースのリカバリ手順を示しています

必要な SAP サービスを開始します。

```
vm-pr1:~ # systemctl start sapinit
```

次の出力は、必要なプロセスを示しています。

```
vm-pr1:/ # ps -ef | grep sap
root     23101     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm   23191     1  3 11:29 ?        00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm   23202     1  5 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root     23292     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root     23359  2597  0 11:29 pts/1    00:00:00 grep --color=auto sap
```

以降のサブセクションでは、複製されたログ・バックアップを使用した、フォワード・リカバリを行う場合としない場合のリカバリ・プロセスについて説明しますリカバリは、システムデータベース用の HANA リカバリスクリプトおよびテナントデータベース用の hdbsql コマンドを使用して実行されます。

#### 最新の **HANA** データボリュームバックアップセーブポイントへのリカバリ

最新のバックアップセーブポイントへのリカバリは ' ユーザー pr1adm として次のコマンドを使用して実行されます

- システムデータベース

```
recoverSys.py --command "RECOVER DATA USING SNAPSHOT CLEAR LOG”
```

- テナントデータベース

```
Within hdbsql: RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
```

また、 HANA Studio または Cockpit を使用して、システムとテナントデータベースのリカバリを実行することもできます。

次のコマンド出力は、リカバリの実行を示しています。

システムデータベースのリカバリ

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py
--command="RECOVER DATA USING SNAPSHOT CLEAR LOG"
[139702869464896, 0.008] >> starting recoverSys (at Fri Feb 19 14:32:16
2021)
[139702869464896, 0.008] args: ()
[139702869464896, 0.009] keys: {'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 14:32:16 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 14:32:16
stopped system: 2021-02-19 14:32:16
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 14:32:21
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T14:32:56+00:00  P0027646      177bab4d610 INFO    RECOVERY
RECOVER DATA finished successfully
recoverSys finished successfully: 2021-02-19 14:32:58
[139702869464896, 42.017] 0
[139702869464896, 42.017] << ending recoverSys, rc = 0 (RC_TEST_OK), after
42.009 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>
```

テナントデータベースのリカバリ

ソースシステムで pr1adm ユーザー用のユーザーストアキーが作成されていない場合は ' ターゲットシステムでキーを作成する必要がありますキーで設定されたデータベースユーザには、テナントのリカバリ処理を実行する権限が必要です。

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>
```

これで、 hdbsql を使用してテナントのリカバリが実行されました。

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
0 rows affected (overall time 66.973089 sec; server time 66.970736 sec)
hdbsql SYSTEMDB=>
```

HANA データベースが起動して実行されるようになり、 HANA データベースのディザスタリカバリワークフローがテストされました。

#### ログ / カタログバックアップを使用したフォワードリカバリでのリカバリ

ログバックアップと HANA のバックアップカタログがソースシステムからレプリケートされている。

使用可能なすべてのログ・バックアップを使用したリカバリは ' ユーザー pr1adm として次のコマンドを使用して実行されます

- システムデータベース

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- テナントデータベース

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```

使用可能なすべてのログを使用してリカバリするには、リカバリステートメントのタイムスタンプとして将来の任意の時点を使用します。

また、 HANA Studio または Cockpit を使用して、システムとテナントデータベースのリカバリを実行することもできます。

次のコマンド出力は、リカバリの実行を示しています。

システムデータベースのリカバリ

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING
SNAPSHOT"
[140404915394368, 0.008] >> starting recoverSys (at Fri Feb 19 16:06:40
2021)
[140404915394368, 0.008] args: ()
[140404915394368, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 16:06:40 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 16:06:40
stopped system: 2021-02-19 16:06:41
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 16:06:46
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T16:07:19+00:00  P0009897      177bb0b4416 INFO    RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
19T15:17:33+00:00, reached log position 38272960
recoverSys finished successfully: 2021-02-19 16:07:20
[140404915394368, 39.757] 0
[140404915394368, 39.758] << ending recoverSys, rc = 0 (RC_TEST_OK), after
39.749 secs
```

テナントデータベースのリカバリ

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit

hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 63.791121 sec; server time 63.788754 sec)

hdbsql SYSTEMDB=>
```

HANA データベースが起動して実行されるようになり、 HANA データベースのディザスタリカバリワークフローがテストされました。

最新のログバックアップの整合性をチェックしてください

ログバックアップボリュームのレプリケーションは、 SAP HANA データベースによって実行されるログバックアッププロセスとは独立して実行されるため、ディザスタリカバリサイトには一貫性のないオープンなログバックアップファイルが存在する可能性があります。最新のログ・バックアップ・ファイルのみが整合性を保持していない可能性がありますこれらのファイルは 'hdbbackupcheck' ツールを使用して災害復旧サイトでフォワード・リカバリを実行する前にチェックする必要があります

「 hdbbackupcheck 」ツールが最新のログ・バックアップのエラーを報告する場合は、最新のログ・バックアップ・セットを削除するか、削除する必要があります。

```
pr1adm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

システムとテナントデータベースの最新のログバックアップファイルに対してチェックを実行する必要があります。

「 hdbbackupcheck 」ツールが最新のログ・バックアップのエラーを報告する場合は、最新のログ・バックアップ・セットを削除するか、削除する必要があります。

## ディザスタリカバリフェイルオーバー

ディザスタリカバリフェイルオーバー

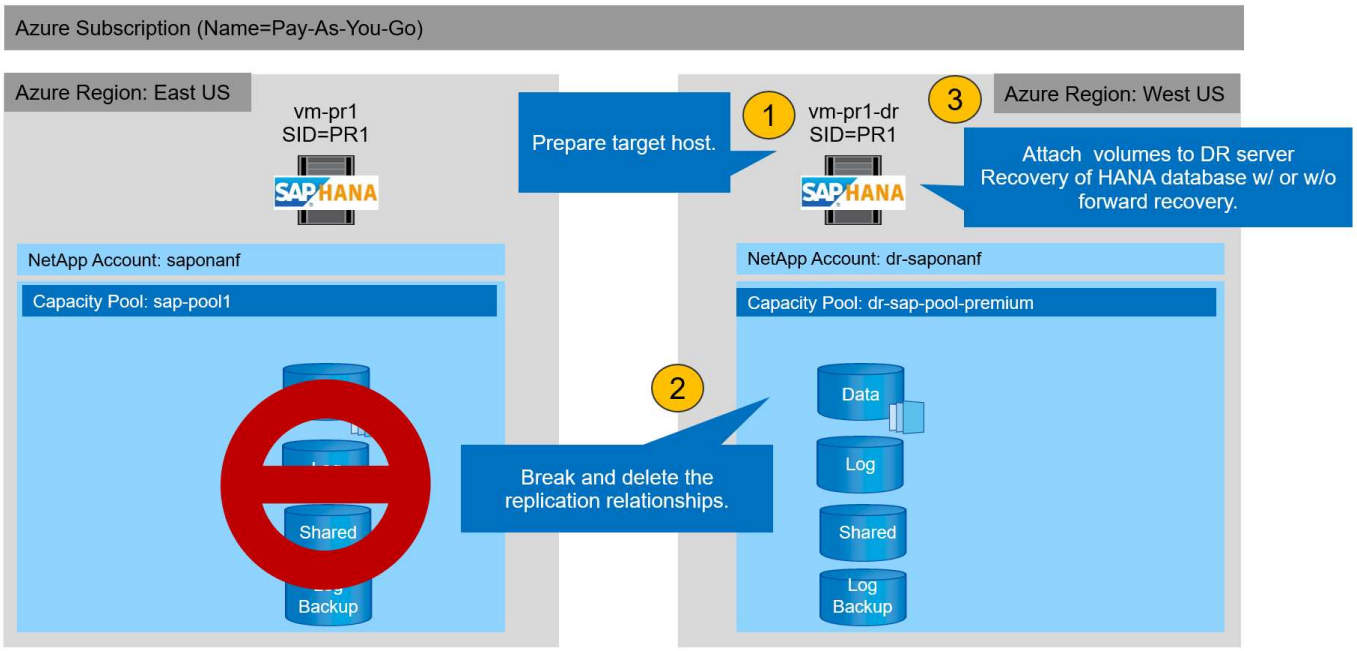
ログバックアップレプリケーションがディザスタリカバリの設定の一部かどうかによって、ディザスタリカバリの手順は少し異なります。ここでは、データバックアップのみのレプリケーション、およびログバックアップボリュームのレプリケーションと組み合わせたデータボリュームのレプリケーションのためのディザスタリカバリフェイルオーバーについて説明します。

ディザスタリカバリフェイルオーバーを実行するには、次の手順を実行します。

1. ターゲットホストを準備します。
2. レプリケーション関係を解除して削除します。
3. データボリュームを、アプリケーションと整合性のある最新の Snapshot バックアップにリストアします。
4. ターゲットホストにボリュームをマウントします。
5. HANA データベースをリカバリします。
    - データボリュームのリカバリのみ

◦ レプリケートされたログバックアップを使用してリカバリを転送する。

以降のサブセクションで、これらの手順について詳しく説明します。次の図は、ディザスタフェイルオーバーのテストを示しています。




ターゲットホストを準備します

## ここでは、ディザスタリカバリフェイルオーバーに使用するサーバで必要な準備手順について説明します。

通常運用時は、 HANA の QA やテスト用システムなど、通常はターゲットホストがその他の目的に使用されます。そのため、災害時のフェイルオーバーテストを実行する際には、ほとんどの手順を実行する必要があります。一方、関連する構成ファイルは、「 /etc/fstab 」や「 /usr/sap/sapservices 」のように準備し、構成ファイルをコピーするだけで運用に移すことができます。ディザスタリカバリフェイルオーバー手順は、準備された関連する構成ファイルが確実に正しく設定されるようにします。

ターゲット・ホストの準備には、 HANA の QA またはテスト・システムのシャットダウン、および「 systemctl stop sapinit 」を使用したすべてのサービスの停止も含まれます。

### ターゲットサーバのホスト名と **IP** アドレス

ターゲット・サーバのホスト名は ' ソース・システムのホスト名と同じである必要がありますIP アドレスは異なっていてもかまいません。

ターゲットサーバが他のシステムと通信できないように、ターゲットサーバの適切なフェンシングを確立する必要があります。適切なフェンシングが設定されていないと、クローニングされた本番用システムは、他の本番用システムとデータを交換し、論理的にデータが破損する可能性があります。

### 必要なソフトウェアをインストールします

SAP ホストエージェントソフトウェアをターゲットサーバにインストール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 "SAP ホストエージェント" SAP ヘルプポータルで、次の作業を行います。

ホストが HANA QA またはテストシステムとして使用されている場合は、 SAP ホストエージェントソフトウェアがすでにインストールされています。

#### ユーザ、ポート、および **SAP** サービスを設定する

ターゲットサーバに、 SAP HANA データベースに必要なユーザとグループが配置されている必要があります。通常は、ユーザの一元管理が使用されるため、ターゲットサーバで設定手順を行う必要はありません。HANA データベースに必要なポートは、ターゲットホストで設定する必要があります。構成は '/etc/services ファイルをターゲット・サーバにコピーすることによって ' ソース・システムからコピーできます

必要な SAP サービスのエントリがターゲットホストにあることが必要です。/usr/sap/sapservices' ファイルをターゲットサーバにコピーすることで ' ソースシステムから構成をコピーできます次の出力は、このラボ環境で使用する SAP HANA データベースの必須エントリを示しています。

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
limit.descriptors=1048576
```

#### **HANA** のログボリュームを準備

HANA のログボリュームはレプリケーションの一部ではないため、空のログボリュームがターゲットホストに存在している必要があります。ログボリュームには、ソース HANA システムと同じサブディレクトリを含める必要があります。

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root   root   4096 Feb 19 16:20 .
drwxr-xr-x 3 root   root     22 Feb 18 13:38 ..
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

#### ログバックアップボリュームを準備

ソースシステムは HANA ログバックアップ用の個別のボリュームで構成されているため、ターゲットホストにログバックアップボリュームも必要です。ログバックアップ用のボリュームを設定し、ターゲットホストにマウントする必要があります。

ディザスタリカバリの設定でログバックアップボリュームのレプリケーションを行う場合、複製されたログバックアップボリュームはターゲットホストにマウントされるため、追加のログバックアップボリュームを準備する必要はありません。

次の表に、このラボ環境で使用する命名規則を示します。災害復旧サイトのボリューム名は '/etc/fstab に含まれています

| **HANA PR1** ボリューム | ディザスタリカバリサイトにあるボリュームとサブディレクトリ | ターゲットホストのマウントポイント |
|---|---|---|
| データボリューム | pr1 -data-mnt00001 -sm -dest | /hana/data /pr1/mnt00001 |
| 共有ボリューム | pr1 -shared-sm-dest/shared pr1 -shared-sm-dest/usr -sap-pr1 | /hana/shared /usr/sap/pr1 |
| ログバックアップボリューム | hanabackup-sm -dest | / はなんバックアップ |



このテーブルのマウントポイントは、ターゲットホストに作成する必要があります。

ここでは ' 必須の /etc/fstab エントリを示します

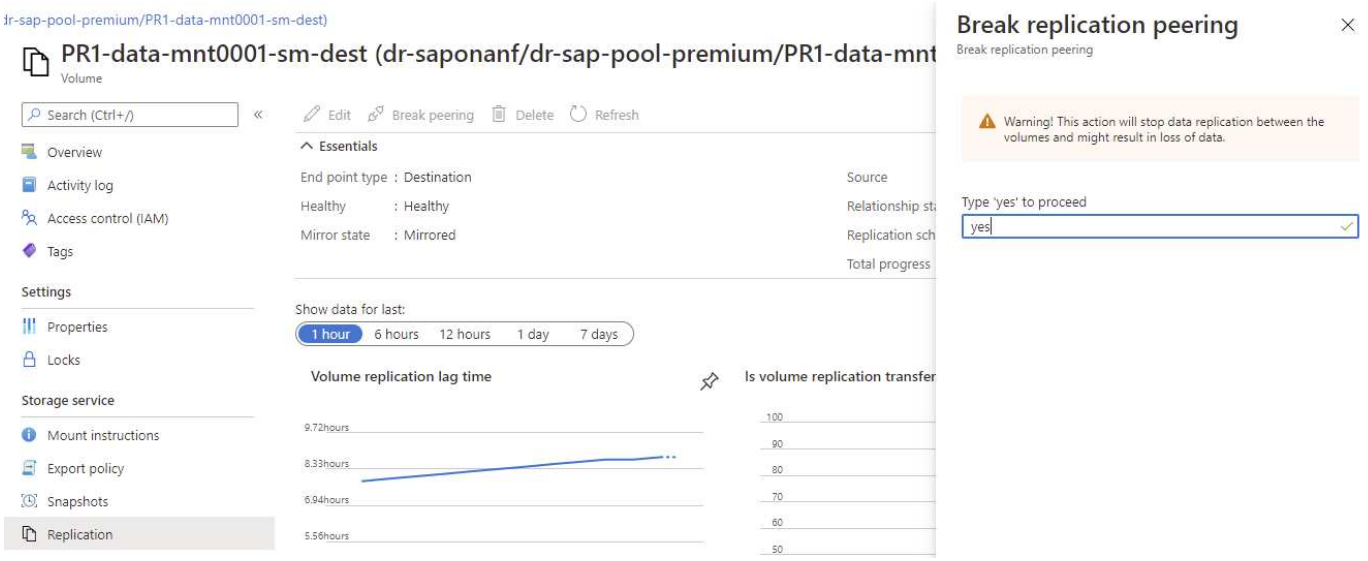
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest    /hanabackup nfs
rw,vers=3,hard,timeo=600,rsize=262144,wsize=262144,nconnect=8,bg,noatime,n
olock 0 0
```

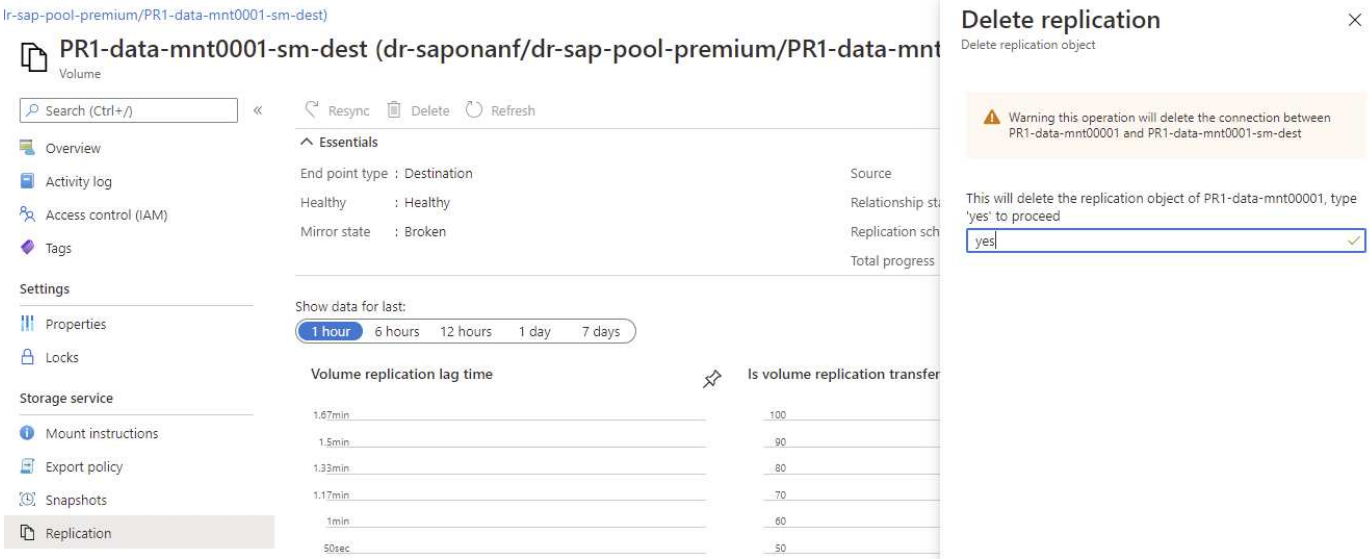
レプリケーションピアリングを解除して削除します

## 災害発生時にフェイルオーバーする場合は、ターゲットホストがボリュームをマウントして読み取りおよび書き込み処理を実行できるように、ターゲットボリュームを切断する必要があります。

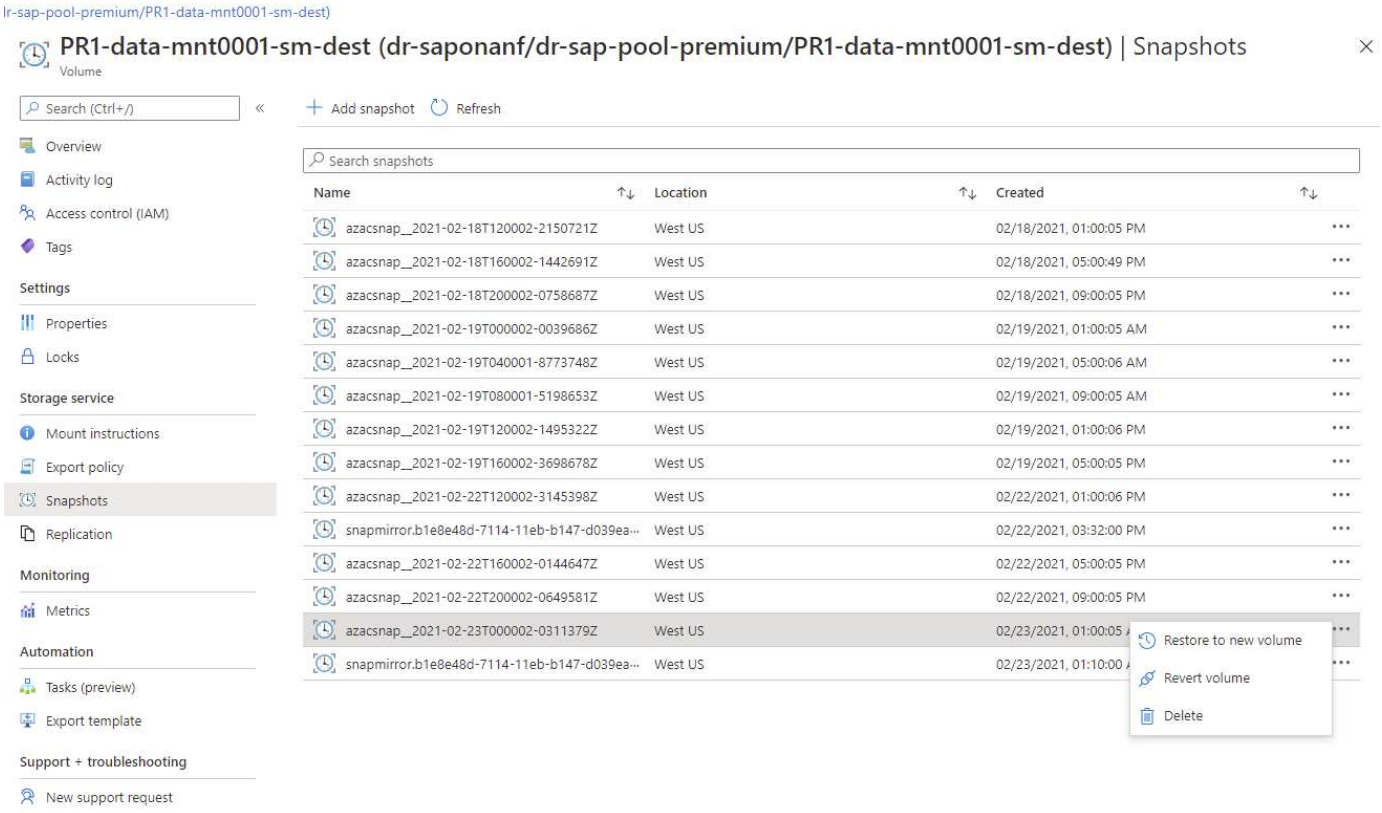
HANA データボリュームの場合は、 AzAcSnap で作成された最新の HANA Snapshot バックアップにボリュームをリストアする必要があります。レプリケーションピアリングが原因で最新のレプリケーション Snapshot がビジーとしてマークされている場合、このボリュームリバート処理は実行できません。そのため、レプリケーションピアリングも削除する必要があります。

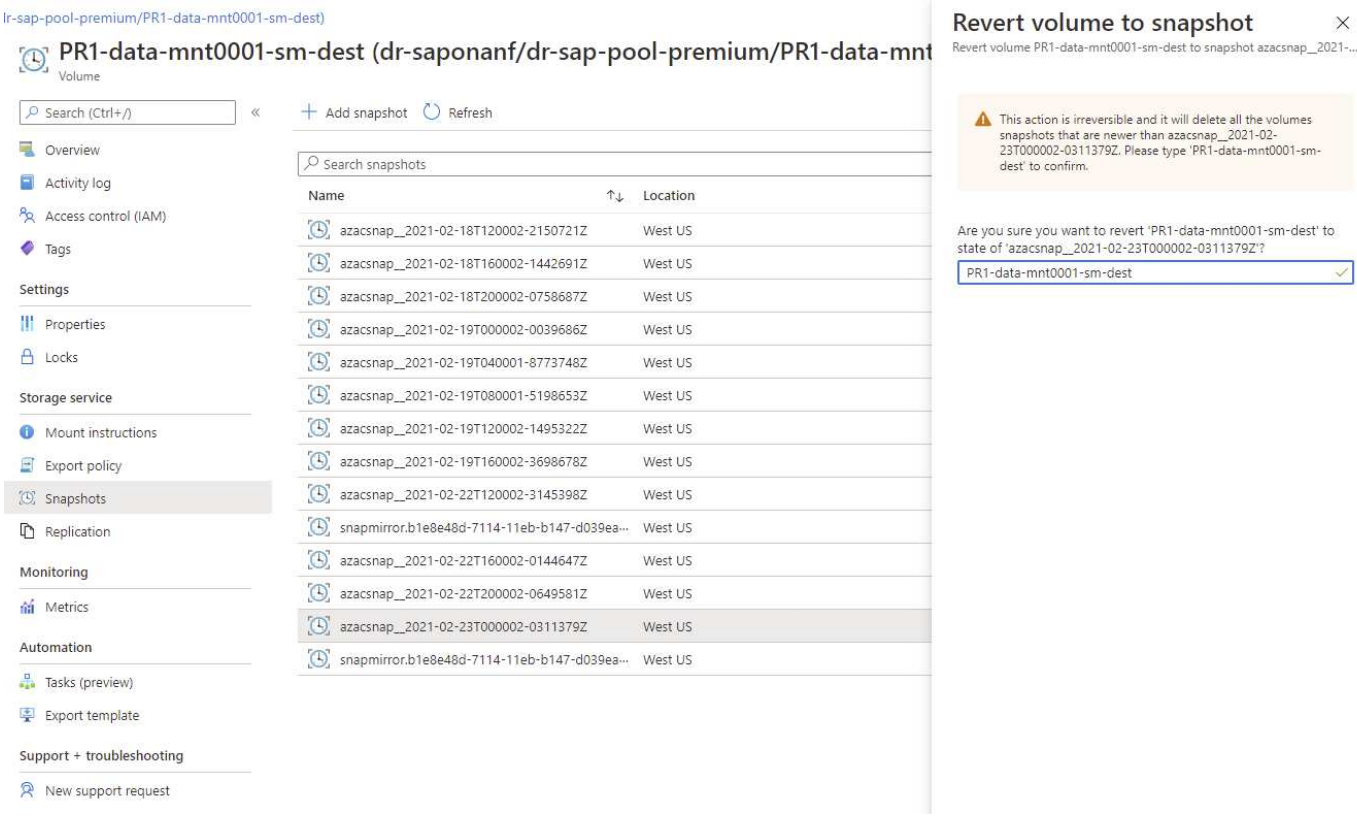
次の 2 つのスクリーンショットは、 HANA データボリュームのピアリング操作の解除と削除を示しています。ログバックアップと HANA 共有ボリュームについても、同じ処理を実行する必要があります。




レプリケーションピアリングが削除されたため、ボリュームを最新の HANA Snapshot バックアップにリバートできます。ピアリングが削除されない場合、リバートボリュームの選択はグレー表示になり、選択できなくなります。次に示す 2 つのスクリーンショットは、ボリュームのリバート処理を示しています。




ボリュームのリバート処理後、データボリュームは整合性のある HANA Snapshot バックアップに基づいており、フォワードリカバリ処理を実行するために使用できるようになりました。

高パフォーマンス階層が低い大容量プールを使用している場合は、必要なパフォーマンスを提供できる容量プールにボリュームを移動する必要があります。

ターゲットホストにボリュームをマウントします

## これで ' 以前に作成した /etc/fstab ファイルに基づいて ' ボリュームをターゲット・ホストにマウントできるようになります

```
vm-pr1:~ # mount -a
```

次の出力は、必要なファイルシステムを示しています。

```
vm-pr1:~ # df
Filesystem                                      1K-blocks     Used
Available Use% Mounted on
devtmpfs                                          8201112        0
8201112   0% /dev
tmpfs                                            12313116        0
12313116   0% /dev/shm
tmpfs                                             8208744     9096
8199648   1% /run
tmpfs                                             8208744        0
8208744   0% /sys/fs/cgroup
/dev/sda4                                        29866736  2543948
27322788   9% /
/dev/sda3                                         1038336    79984
958352   8% /boot
/dev/sda2                                          524008     1072
522936   1% /boot/efi
/dev/sdb1                                        32894736    49180
31151556   1% /mnt
10.0.2.4:/PR1-log-mnt00001-dr             107374182400     6400
107374176000   1% /hana/log/PR1/mnt00001
tmpfs                                             1641748        0
1641748   0% /run/user/0
10.0.2.4:/PR1-shared-sm-dest/hana-shared 107377178368 11317248
107365861120   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 107377178368 11317248
107365861120   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest              107379678976 35249408
107344429568   1% /hanabackup
10.0.2.4:/PR1-data-mnt0001-sm-dest        107376511232  6696960
107369814272   1% /hana/data/PR1/mnt00001
vm-pr1:~ #
```

## 以下は、 HANA データベースのリカバリ手順を示しています

必要な SAP サービスを開始します。

```
vm-pr1:~ # systemctl start sapinit
```

次の出力は、必要なプロセスを示しています。

```
vm-pr1:/ # ps -ef | grep sap
root     23101     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm   23191     1  3 11:29 ?        00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm   23202     1  5 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root     23292     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root     23359  2597  0 11:29 pts/1    00:00:00 grep --color=auto sap
```

以降のサブセクションでは、複製されたログ・バックアップを使用した、フォワード・リカバリを行う場合としない場合のリカバリ・プロセスについて説明しますリカバリは、システムデータベース用の HANA リカバリスクリプトおよびテナントデータベース用の hdbsql コマンドを使用して実行されます。

### 最新の HANA データボリュームバックアップセーブポイントへのリカバリ

最新のバックアップセーブポイントへのリカバリは ' ユーザー pr1adm として次のコマンドを使用して実行されます

- システムデータベース

```
recoverSys.py --command "RECOVER DATA USING SNAPSHOT CLEAR LOG”
```

- テナントデータベース

```
Within hdbsql: RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
```

また、 HANA Studio または Cockpit を使用して、システムとテナントデータベースのリカバリを実行することもできます。

次のコマンド出力は、リカバリの実行を示しています。

システムデータベースのリカバリ

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py
--command="RECOVER DATA USING SNAPSHOT CLEAR LOG"
[139702869464896, 0.008] >> starting recoverSys (at Fri Feb 19 14:32:16
2021)
[139702869464896, 0.008] args: ()
[139702869464896, 0.009] keys: {'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 14:32:16 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 14:32:16
stopped system: 2021-02-19 14:32:16
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 14:32:21
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T14:32:56+00:00  P0027646      177bab4d610 INFO    RECOVERY
RECOVER DATA finished successfully
recoverSys finished successfully: 2021-02-19 14:32:58
[139702869464896, 42.017] 0
[139702869464896, 42.017] << ending recoverSys, rc = 0 (RC_TEST_OK), after
42.009 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>
```

テナントデータベースのリカバリ

ソースシステムで pr1adm ユーザー用のユーザーストアキーが作成されていない場合は ' ターゲットシステムでキーを作成する必要がありますキーで設定されたデータベースユーザには、テナントのリカバリ処理を実行する権限が必要です。

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>
```

これで、 hdbsql を使用してテナントのリカバリが実行されました。

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
0 rows affected (overall time 66.973089 sec; server time 66.970736 sec)
hdbsql SYSTEMDB=>
```

HANA データベースが起動して実行されるようになり、 HANA データベースのディザスタリカバリワークフローがテストされました。

#### ログ / カタログバックアップを使用したフォワードリカバリでのリカバリ

ログバックアップと HANA のバックアップカタログがソースシステムからレプリケートされている。

使用可能なすべてのログ・バックアップを使用したリカバリは ' ユーザー pr1adm として次のコマンドを使用して実行されます

- システムデータベース

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- テナントデータベース

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```

使用可能なすべてのログを使用してリカバリするには、リカバリステートメントのタイムスタンプとして将来の任意の時点を使用します。

また、 HANA Studio または Cockpit を使用して、システムとテナントデータベースのリカバリを実行することもできます。

次のコマンド出力は、リカバリの実行を示しています。

システムデータベースのリカバリ

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING
SNAPSHOT"
[140404915394368, 0.008] >> starting recoverSys (at Fri Feb 19 16:06:40
2021)
[140404915394368, 0.008] args: ()
[140404915394368, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 16:06:40 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 16:06:40
stopped system: 2021-02-19 16:06:41
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 16:06:46
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T16:07:19+00:00  P0009897      177bb0b4416 INFO    RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
19T15:17:33+00:00, reached log position 38272960
recoverSys finished successfully: 2021-02-19 16:07:20
[140404915394368, 39.757] 0
[140404915394368, 39.758] << ending recoverSys, rc = 0 (RC_TEST_OK), after
39.749 secs
```

テナントデータベースのリカバリ

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit

hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 63.791121 sec; server time 63.788754 sec)

hdbsql SYSTEMDB=>
```

HANA データベースが起動して実行されるようになり、 HANA データベースのディザスタリカバリワークフローがテストされました。

最新のログバックアップの整合性をチェックしてください

ログバックアップボリュームのレプリケーションは、 SAP HANA データベースによって実行されるログバックアッププロセスとは独立して実行されるため、ディザスタリカバリサイトには一貫性のないオープンなログバックアップファイルが存在する可能性があります。最新のログ・バックアップ・ファイルのみが整合性を保持していない可能性がありますこれらのファイルは 'hdbbackupcheck' ツールを使用して災害復旧サイトでフォワード・リカバリを実行する前にチェックする必要があります

「 hdbbackupcheck 」ツールが最新のログ・バックアップのエラーを報告する場合は、最新のログ・バックアップ・セットを削除するか、削除する必要があります。

```
pr1adm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

システムとテナントデータベースの最新のログバックアップファイルに対してチェックを実行する必要があります。

「 hdbbackupcheck 」ツールが最新のログ・バックアップのエラーを報告する場合は、最新のログ・バックアップ・セットを削除するか、削除する必要があります。

## 履歴を更新します

この解決策の初版以降には、次の技術的な変更が加えられています。

| バージョン | 日付 | 概要を更新します |
| --- | --- | --- |
| バージョン 1.0 以降 | 2021年4月 | 初版 |

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

TR-4646 では、 SAP HANA 向けのディザスタリカバリ保護オプションの概要を説明しています。詳細なセットアップ情報、および同期および非同期の NetApp SnapMirror ストレージレプリケーションをベースとした 3 サイトディザスタリカバリ解決策のユースケース概要が含まれます。説明されている解決策では、データベースの整合性を管理するために、 NetApp SnapCenter と SAP HANA プラグインを使用します。

作成者：Nils Bauer、NetApp

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

# TR-4711 ：『 SAP HANA Backup and Recovery Using NetApp Storage Systems and Commvault Software 』

TR-4711 は、 Commvault IntelliSnap Snapshot 管理テクノロジとネットアップの Snapshot テクノロジを含む、ネットアップと Commvault 解決策 for SAP HANA の設計をまとめたものです。解決策は、ネットアップストレージと Commvault データ保護スイートを基盤としています。

執筆者：NetAppのMarco Schoen氏、Commvault SystemsのTristan Daude博士

https://www.netapp.com/pdf.html?item=/media/17050-tr4711pdf.pdf

# SnapCenterとSAP ASEデータベースの統合

このドキュメントでは、SAP環境で使用されるSAP ASEデータベースのSnapCenter統合の詳細について説明します。

## はじめに

このドキュメントは、環境全体のセットアップ方法を段階的に説明することを目的としたものではありませんが、以下に関連する概念と関連する詳細について説明します。

- セツテイノカイヨウレイ
- サンプルレイアウト
- SAP ASEインスタンスの保護
- SAP ASEインスタンスのリストアとリカバリ

作成者：Michael Schlosser、NetApp

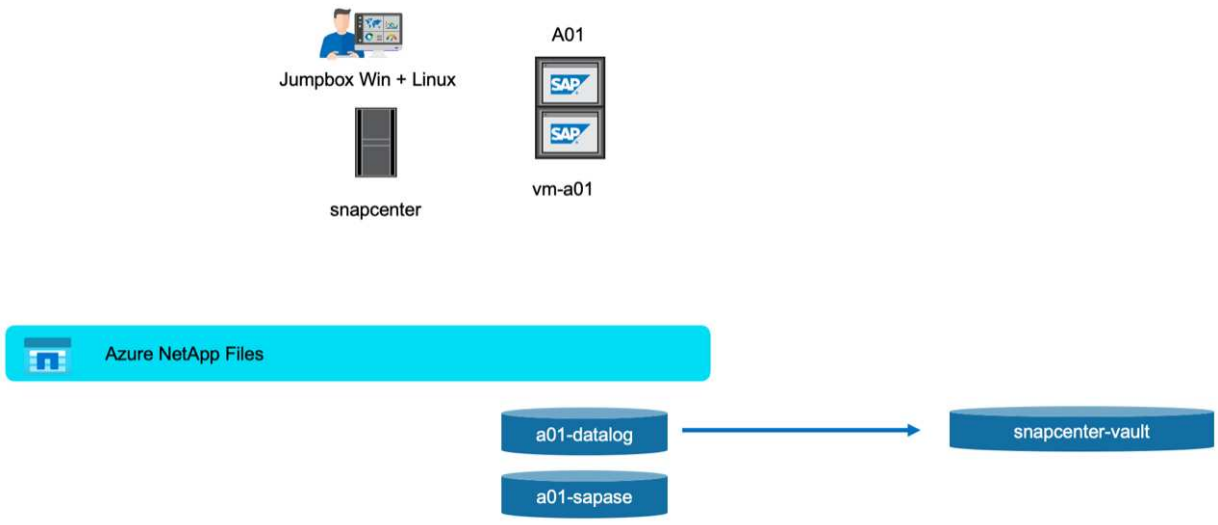
### セツテイノカイヨウレイ

Azureプラットフォームで実行されているSAPシステム用のSnapCenter ASEプラグインの実装例。

> この実装では、最小限必要なボリューム構成について説明します。データ・ダンプ・バックアップとログ・ダンプ・バックアップは、SAP Note 1588316に従って設定します。

または、これに記載されている体積構造を"MSテクニカルコミュニティブログ"使用することもできます。

### デモ環境




ソフトウェアバージョン

| ソフトウェア | * バージョン * |
| --- | --- |
| Linux OS | SLES for SAP 15 SP5 |
| SAP | SAP NetWeaver 7.5 |
| SAP ASE | 16.0 SP04 PL06 HF1 |
| SnapCenter | 6.1 |

**ASE**ボリューム設計

SAP ASEデータベースのバックアップ/リカバリとクローニングのユースケースには、次の最小ボリュームレイアウトを使用する必要があります。この設定例では、<SID>：A01を使用しています。

| ボリューム名 | ボリューム上のディレクトリ（**qtree**） | サーバ上のマウントポイント | * コメント * |
| --- | --- | --- | --- |
| <SID>サパス | Sybase の場合 | /Sybase | ASE関連ファイルの親ディレクトリ |
| | | /Sybase /<SID>//バックアップ | データダンプのバックアップ（別のボリュームに配置されている場合がある） |
| | | /Sybase /<SID>/ log_archives | ログダンプのバックアップ（別のボリュームに配置されている可能性あり） |
| | <sid> adm | <sid> adm | ユーザ<sid> admのホームディレクトリ |
| | usrsaptrans | /usr/sap/trans | 転送ディレクトリ |
| | Usrsap <SID> | /usr/sap/<SID> | ユーザSAP |
| | sapmnt <SID> | /sapmnt/<SID> | SAP GlobalHostディレクトリ |

| ボリューム名 | ボリューム上のディレクトリ（**qtree**） | サーバ上のマウントポイント | * コメント * |
|---|---|---|---|
| <SID>-データログ | SAPDATA_1 | /Sybase/Sybase/Sapdata_1 <SID> | DBデータ（SID） |
| | saplog_1 | /sybase/saplog_1 <SID> | DBログ（SID） |
| | saptemp | /Sybase/Sybase/Saptemp <SID> | PSAPTEMP |
| | Sybsecurity | /Sybase/Sybase/Sybsecurity <SID> | SybaseセキュリティDB |
| | Sybsystem | /Sybase/Sybase/Sybsystem <SID> | SybaseシステムDB |
| | sybtemp | /Sybase/Sybase/Sybtemp <SID> | SybaseシステムDB-Temp |
| | sapdiag | /Sybase/Sybase/Sapdiag <SID> | 'saptools’データベース |

データベース**A01**を保護する手順

- サンプルレイアウトに従ってファイルの配布をチェックします。
- ホストの前提条件の確認（VM-A01）
- データベースの前提条件の確認(A01)
- ホストへのSnapCenterエージェントの導入/インストール（VM-A01）
- SnapCenterインスタンスリソース構成の作成

ホストの前提条件

より最新の情報が得られる可能性があり"ここをクリック"ます。

ホストを追加してLinux用のプラグインパッケージをインストールする前に、すべての要件を満たしておく必要があります。

- iSCSIを使用している場合は、iSCSIサービスが実行されている必要があります。
- パスワードベースの認証またはSSHキーベースの認証を使用できます。パスワードベースの認証はrootユーザとroot以外のユーザが使用できます。
- SnapCenter Plug-in for UNIX File Systemsは、root以外のユーザもインストールできます。ただし、プラグイン プロセスをインストールして開始できるよう、root以外のユーザにsudo権限を設定する必要があります。プラグインのインストール後、プロセスは有効なroot以外のユーザとして実行されます。
- インストール ユーザのクレデンシャルを、認証モードをLinuxに設定して作成します。
- Java 11をLinuxホストにインストールしておく必要があります。
- LinuxホストにJava 11の認定エディションのみがインストールされていることを確認します。
- Javaのダウンロードについては、「Java Downloads for All Operating Systems」を参照してください。
- プラグインのインストールには、デフォルトのシェルとしてbashを使用する必要があります。

データベースの前提条件–ログとバックアップの有効化

- バックアップとLOG_ARCHIVESのディレクトリを作成（/sybase/a01/backups、/sybase/a01/log_archives）
- データベースA01に接続（OS-user syba01として）
  - isql -S A01 -U sapsa -X -w 1024
- SAP Note 1588316に従って、データ（A01DB）のダンプ構成を作成します。
  - マスターを使用
  - 移動
  - exec exec SP _config_dump@config_name ='A01DB'、@stripe_dir='/sybase/A01/backups'、@compression='101'、@verify='header'
  - 移動
- SAP Note 1588316に従って、ログ（A01LOG）のダンプ構成を作成します。
  - マスターを使用
  - 移動
  - sybase_config_dump@config_name ='A01LOG'、@stripe_dir='/sybase/A01/log_archives'、@compression='101'、@verify='header' SP
  - 移動
- データベースA01のフルロギングを有効にする
  - dboption a01、'trunc log on chkpt'、false SP
  - 移動
  - vlan_dboption A01、'full logging for all'、'true' SP
  - 移動
  - dboption a01、'Enforce dump tran sequence'、'true' SP
  - 移動
- ログダンプバックアップを有効にするデータベースダンプバックアップ
  - config='A01DB’を使用してデータベースA01をダンプする
  - 移動
  - ログダンプ
  - config='A01LOG’を使用してトランザクションA01をダンプします
  - 移動
- SAP Note 1588316に従って、定期的なログバックアップが設定されていることを確認します。

オプション–専用のデータベースユーザを作成する

SAP環境では、ユーザsapsaを使用できます。

- データベースA01に接続（OS-user syba01として）

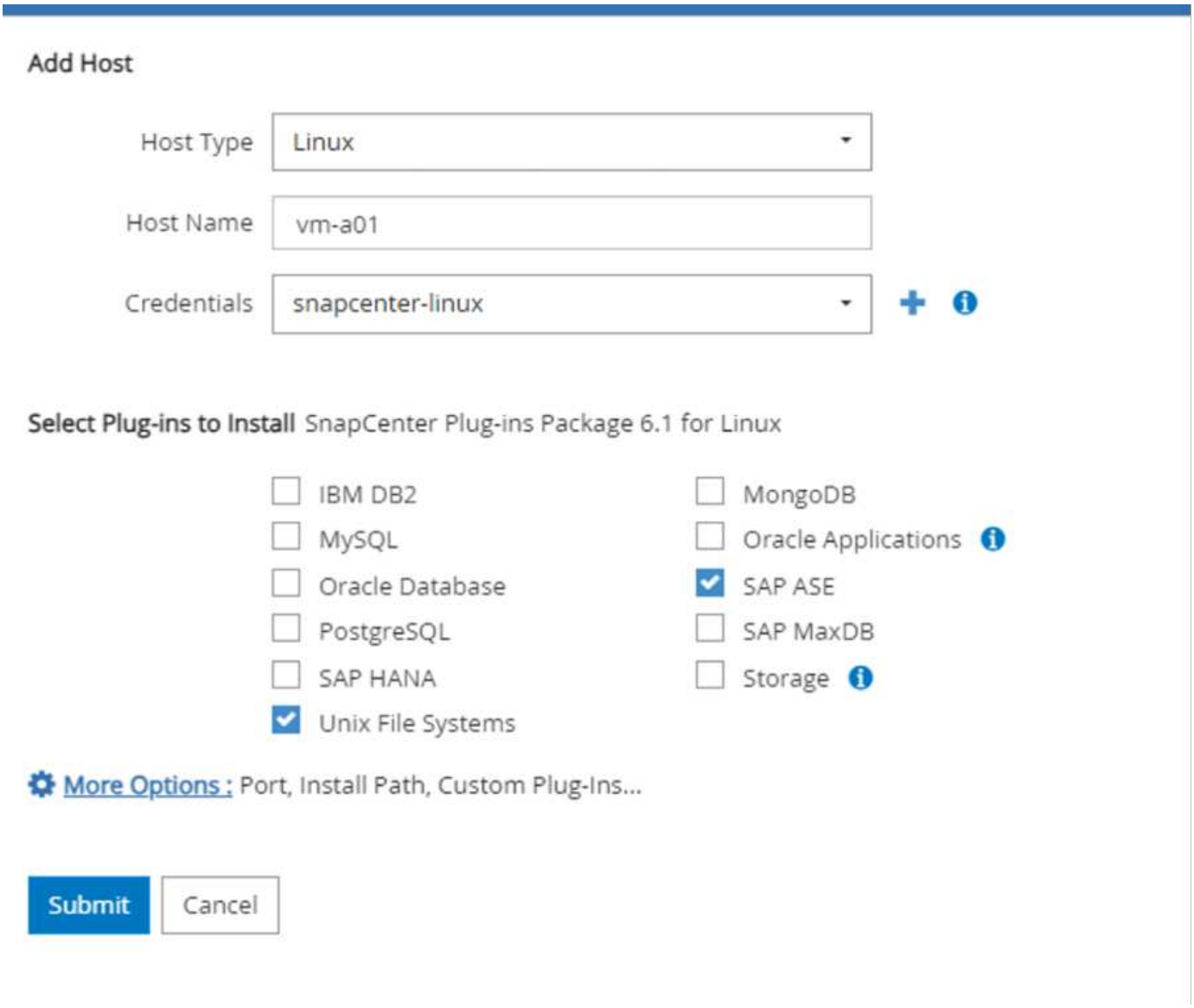
- isql -S A01 -U sapsa -X -w 1024

- ユーザの作成
  - パスワード「<password>」でログインのバックアップを作成します。
  - 移動
- ユーザーへの権限/役割の割り当て
  - ロールsa_role、sso_role、oper_role、sybase_ts_roleをバックアップに付与
  - 移動

**SnapCenter**エージェントをホスト**VM-A01**に展開する

詳細については、を参照して"SnapCenter のドキュメント"ください。

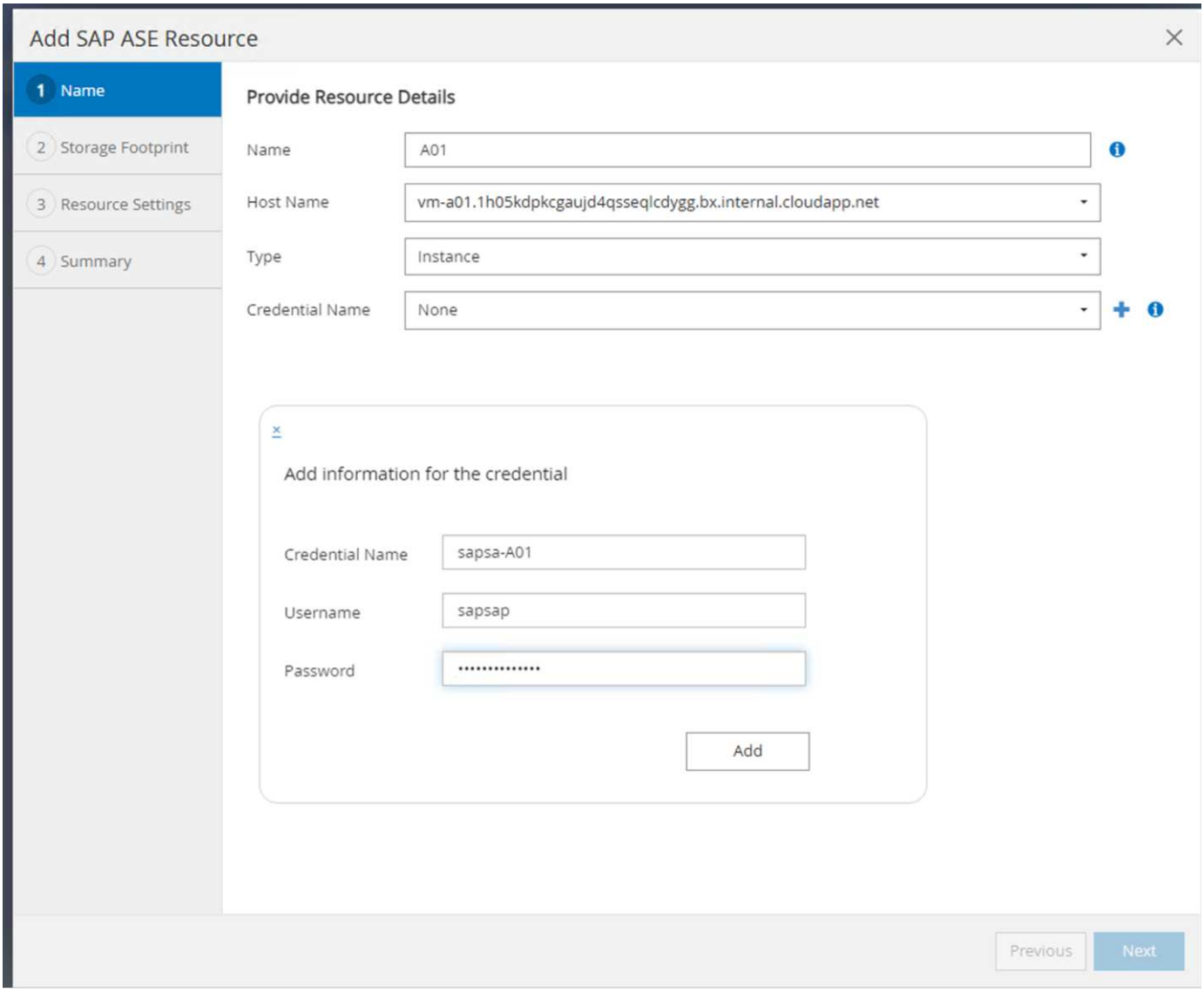
[SAP ASE and Unix File Systems Plugins]を選択します。




ダイアログのスクリーンショット"]

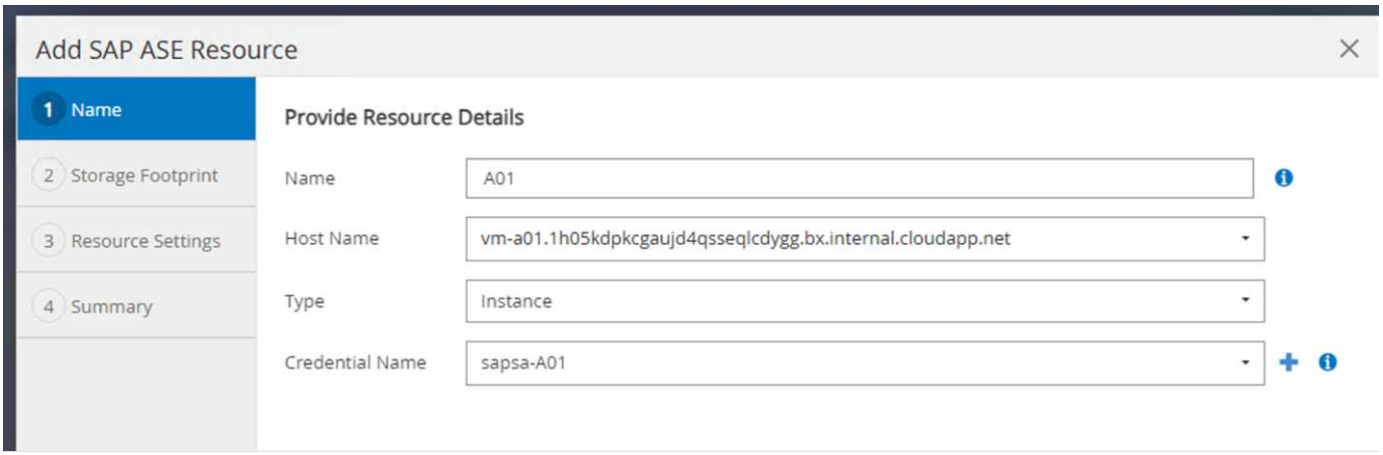
データベース**A01**の**SnapCenter**インスタンスリソース構成の作成

リソース→ SAP ASE →リソースの追加

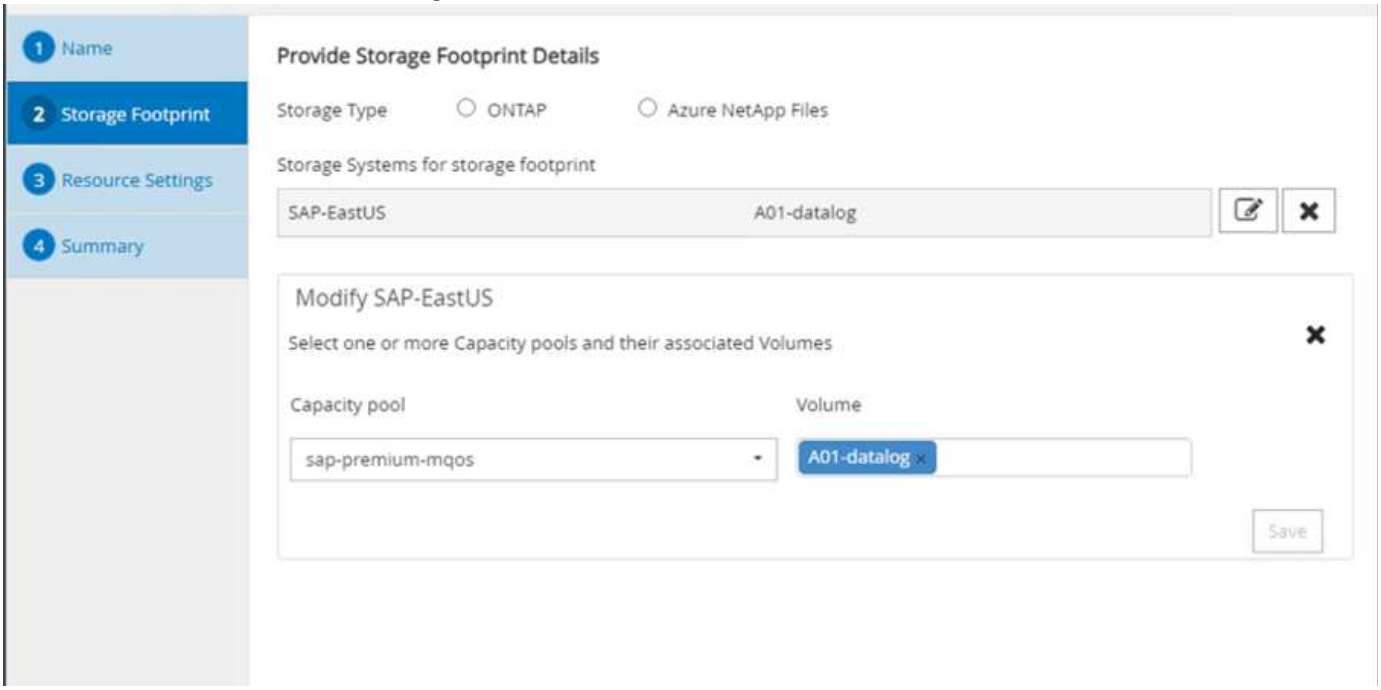


ダイアログのスクリーンショット"]

パスワードに特殊文字が含まれている場合は、バックスラッシュでマスクする必要があります。例：Test！123! →テスト\!123\!



ダイアログのスクリーンショット"]

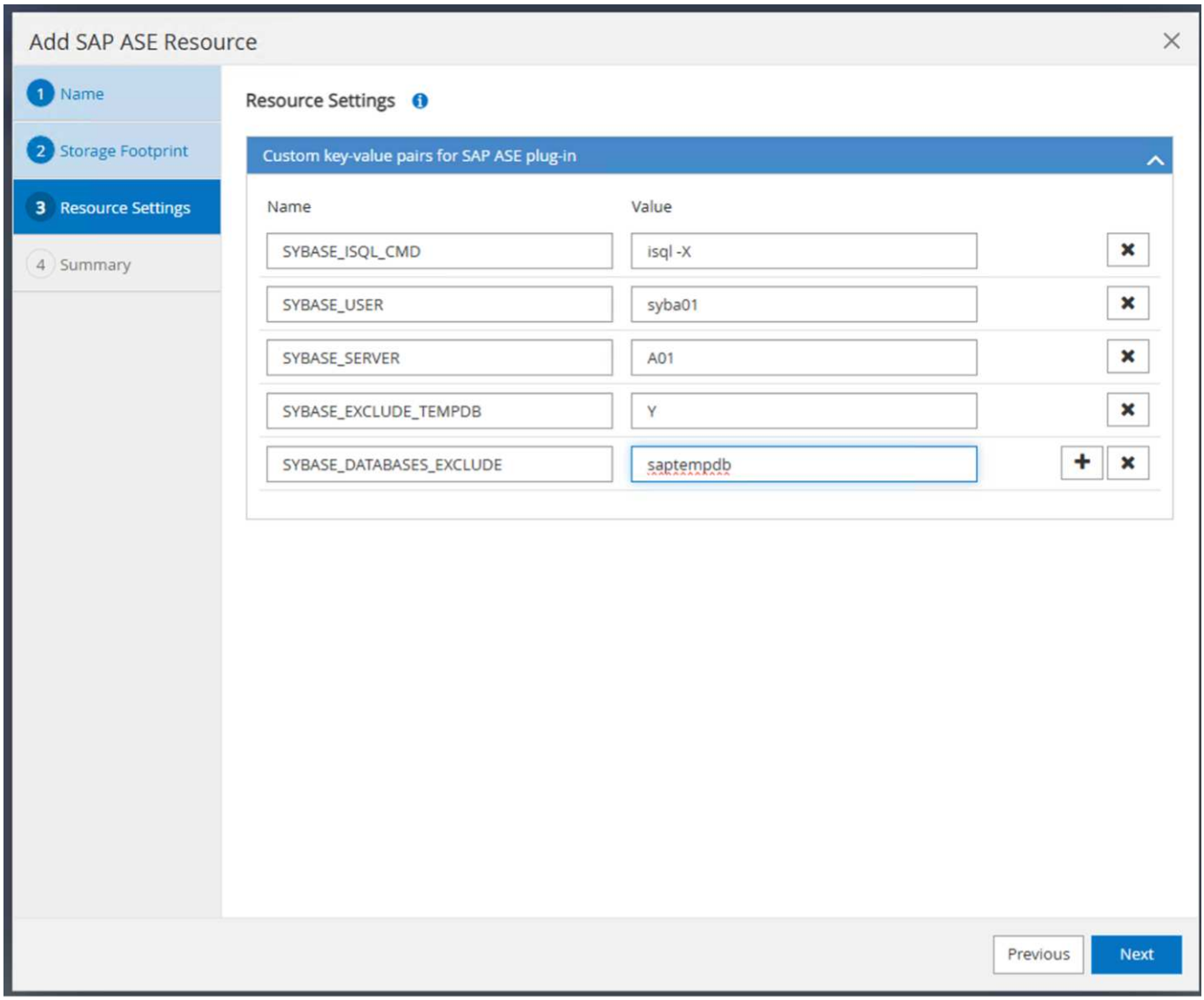


ダイアログのスクリーンショット"]

からボリュームデザインを使用している場合"MSテクニカルコミュニティブログ"。

ボリューム/vol/<SID> Sybase、/vol/<SID> data、/vol/<SID> logをストレージフットプリントとして設定する必要がある

次のリソース設定カスタムのキーと値のペアを作成する必要があります(少なくとも)。



[Custom key-value pairs]ダイアログのスクリーンショット"]

次の表に、 Sybase プラグインのパラメータの一覧、設定、説明を示します。

| * パラメータ * | 設定 | * 概要 * |
| --- | --- | --- |
| SYBASE_ISQL_CMD のようになります | 例：/opt/sybase/ocs-15__0/bin/isql -X | isql コマンドへのパスを定義します。使用可能なオプション： https://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.dc34237.1500/html/mvsinst/CIHHFDGC.htm |
| SYBASE_USER | user_name （ユーザー名 | isql コマンドを実行できるオペレーティングシステムユーザを指定します。このパラメータは UNIX では必須です。このパラメータは、 Snap Creator の Agentstart コマンドおよび stop コマンド（通常は root ユーザ）を実行しているユーザと、 isql コマンドを実行しているユーザが異なる場合に必要です。 |
| SYBASE_SERVER のことです | data_sserver_name を選択します | Sybaseデータサーバ名を指定します（isqlコマンドの-Sオプション）。例：A01 |

| * パラメータ * | 設定 | * 概要 * |
| --- | --- | --- |
| SYBASE_DATABASES | db_name ： user_name password | バックアップするインスタンス内のデータベースのリストを表示します。たとえば、DBAtest2:sa/53616c7404351eのようにマスターデータベースが追加されます。+allという名前のデータベースを使用すると、データベースの自動検出が使用され、sybsyntax、sybsystemdb、sybsystemprocs、tempdbデータベースは除外されます。例：+all：sa/53616c71a6351e NTAP_PWD_PROTECTIONパラメータが設定されている場合、暗号化されたパスワードがサポートされます。 |
| SYBASE_DATABASE_EXCLUDE | データベース名 | ALL construct を使用する場合にデータベースを除外できるようにします。複数のデータベースを指定するには、セミコロンで区切ったリストを使用します。例：pubs2；test_db1 |
| Sybase_Tran ダンプ | db_name ： direction_path | Snapshotコピーを作成したあとにSybaseトランザクションダンプを実行できます。例：pubs2 ：/sybasedumps/pubs2トランザクションダンプが必要な各データベースを指定する必要があります。 |
| SYBASE_TRAN_DUMP_FORMAT | %S_%D_%T.cmn | ダンプの命名規則を指定できます。次のキーを指定できます。%S = SYBASE_SERVERのインスタンス名%D = SYBASE_DATABASESのデータベース%T = UNIQUE TIMESTAMP例を次に示します。%S_%D_% T.log |
| SYBASE_TRAN_DUMP_COMPRESSE_COMPRESS | （Y/N） | 標準の Sybase トランザクションダンプの圧縮を有効または無効にします。 |
| Sybase の場合 | 例：/Sybase | Sybase をインストールする場所を指定します。 |
| SYBASE_MANIMANIEST | 例：a01 ：/sybase/a01/sapdiag | マニフェストファイルを作成する必要のあるデータベースと、マニフェストファイルを配置する必要のある場所を指定します。 |
| SYBASE_MANIMANIT_FORMAT の場合 | %S__%D_.manifest例 ：%S_%D_.manifest | マニフェストファイルの命名規則を指定できます。次のキーを指定できます。%S = Sybase_serverのインスタンス名%D = Sybase_databasesのデータベース |
| SYBASE_MANIMANIT_DELETE | （Y/N） | Snapshot コピーの作成後にマニフェストを削除できます。Snapshot コピー内でマニフェストファイルをキャプチャし、常にバックアップで利用できるようにする必要があります。 |
| SYBASE_EXCLUDE tempdb の場合 | （Y/N） | ユーザが作成した一時データベースの自動除外を有効にします。 |

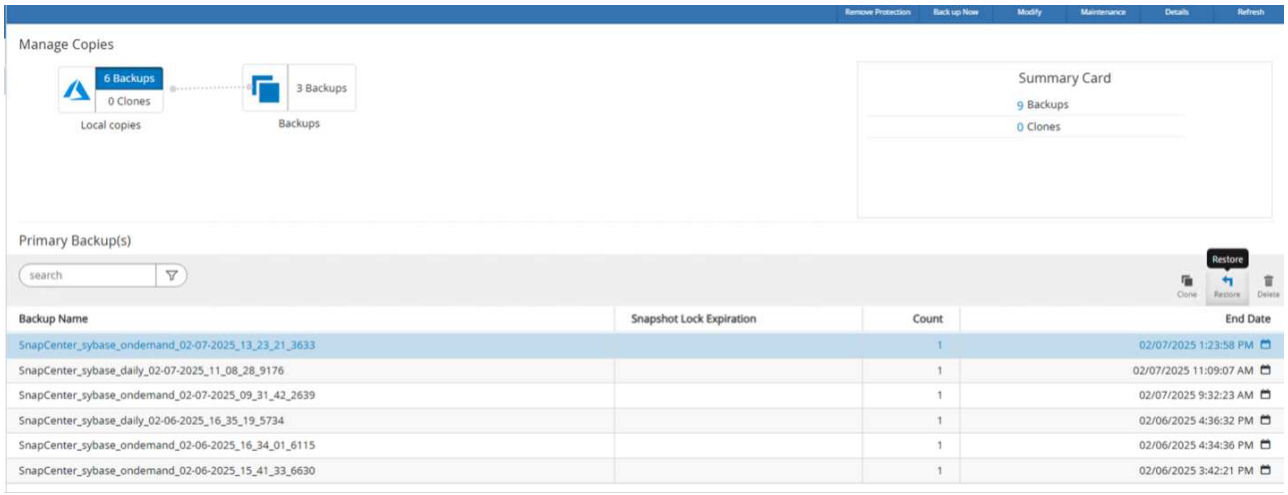
システム**A01**をリカバリする手順

1. SAPシステムA01（データベースを含む）の停止、sapinitの停止
2. ファイルシステムのアンマウント

3. リストアボリュームA01-datalog（SnapCenterを使用）
4. ファイルシステムのマウント
5. データベースA01を起動します（SAP Note 1887068に準拠して、自動オンラインを回避し、データベースのフォワードリカバリを可能にするために–qオプションを指定）。
6. BackupServer A01の起動
7. オンラインデータベースsaptools、sybsecurity、sybmgmtdb
8. データベースA01のリカバリ（isqlを使用）
9. オンラインデータベースA01
10. sapinit、SAPシステムA01の起動

インスタンス**A01**のリカバリ

- ホストVM-A01でSAPシステム+ DB A01を停止
  - ユーザーa01adm：停止
  - ユーザroot：/etc/init.d/sapinit stop
  - ユーザroot：umount -a -t nfs
- リストア バックアップ
  - SnapCenter GUI：リストアに必要なバックアップを選択



ダイアログのスクリーンショット"]

  - ANF導入の場合–完全なリソースのみ提供



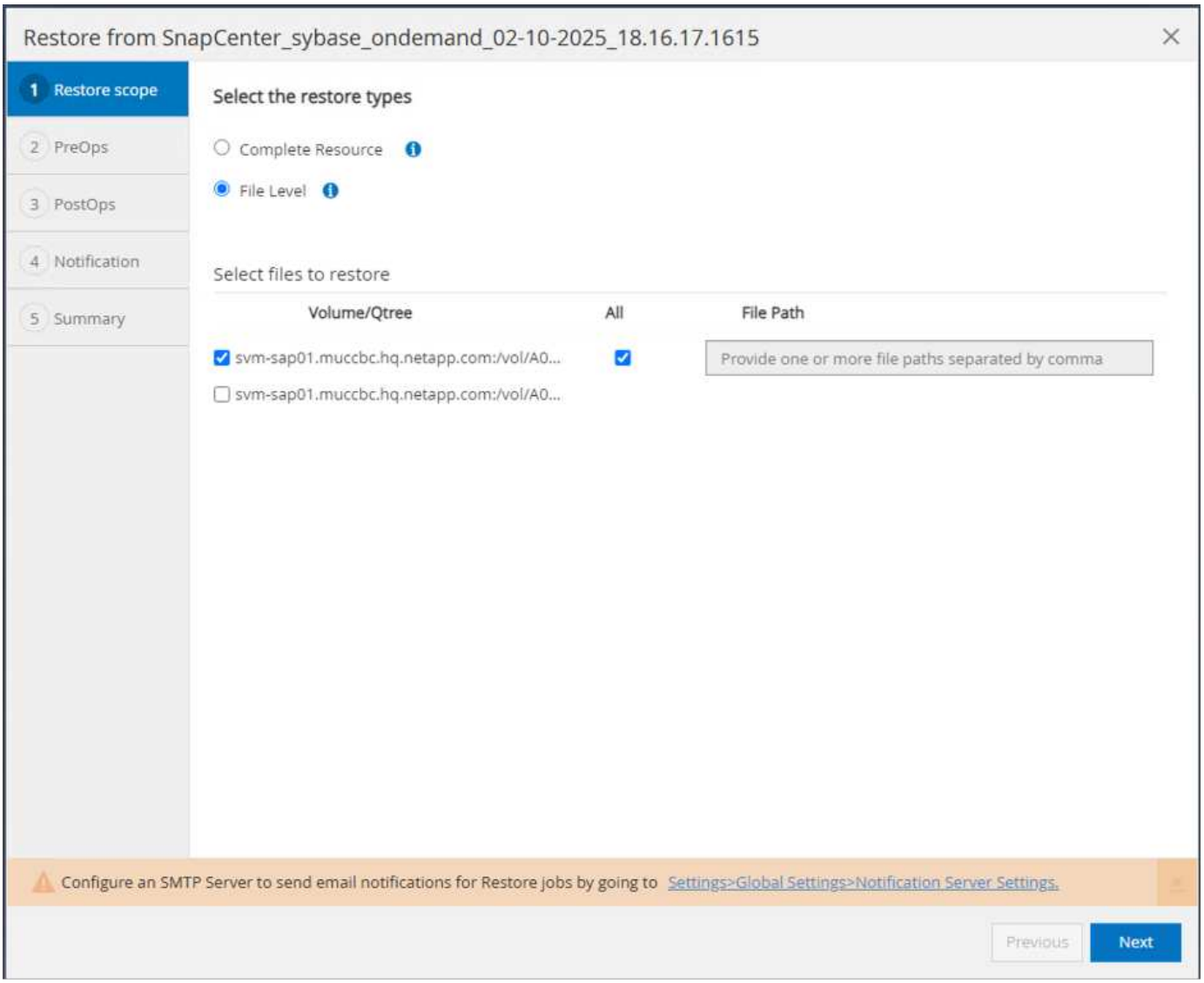
ダイアログのスクリーンショット"]

[Complete Resource]を選択すると、Volume Based Snap Restore（VBSR）が実行されます。Azure内ではと呼ばれます"ボリュームのリバート"。

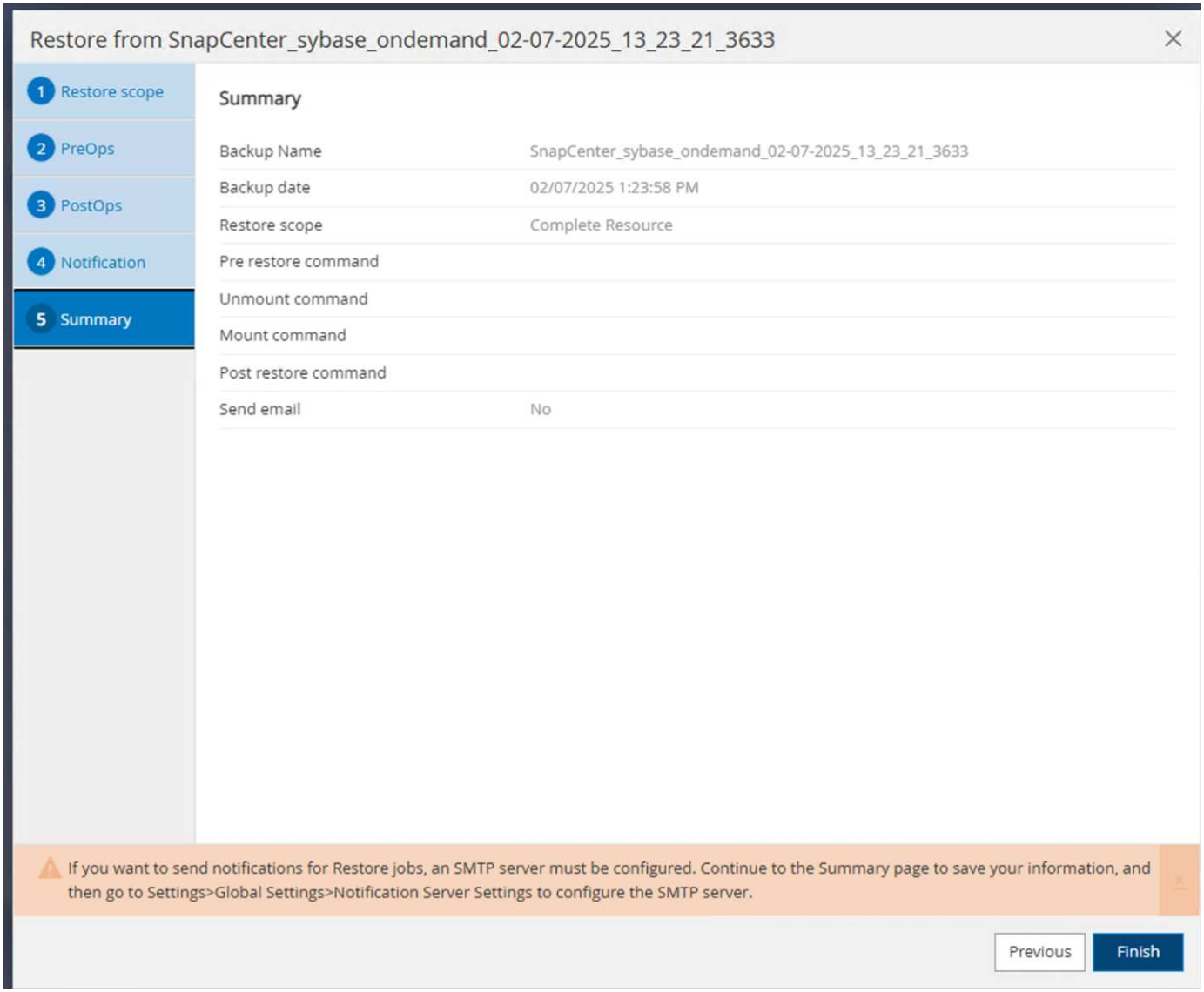
**Important**

Active filesystem data and snapshots that were taken after the selected snapshot will be lost. The snapshot revert operation will replace *all* the data in the targeted volume with the data in the selected snapshot. You should pay attention to the snapshot contents and creation date when you select a snapshot. You cannot undo the snapshot revert operation.

その他のタイプの導入（オンプレミスANFなど）では、Single File Snap Restore（SFSR）処理をオーケストレーションできます。[File Level]と[According Volume]を選択し、[All]にチェックマークを付けます。次のスクリーンショットを参照してください。




概要が表示され、[Finish]をクリックすると、実際のリストアが開始されます。




- ファイルシステムのマウント（VM-A01）
  - ユーザroot：mount -a -t nfs
- データベースA01+ BackupServerの起動
  - run_a01を変更し、-q\を追加します（SAP Note 1887068に準拠）。
  - ユーザsyba01：run_A01 &
  - ユーザsyba01：run_A01_BS&
- オンラインデータベースsaptools、sybsecurity、sybmgmtdb
  - ユーザsyba01：isql -S A01 -U sapsa -X -w 1024
  - オンラインデータベースのsaptools
  - 移動
  - オンラインデータベースsybsecurity
  - 移動
  - オンラインデータベースsybmgmtdb

- 移動

- データベースA01のリカバリ
  - SP dump_history（トランザクション・ログ・ダンプを表示）
  - 移動
  - 必要に応じてトランザクションログダンプをロードします。詳細については、次のドキュメントを参照してください。 https://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.dc36272.1572/html/commands/X75212.htm
  - 例：'/sybase/a01/log_archives/a01.Tran.20250207.140248.6.000'からTran A01をロードします
  - 移動
  - オンラインデータベースA01
  - 移動
- run_A01から-qを削除
- SAPシステムの起動
  - ユーザroot：/etc/init.d/sapinit start
  - ユーザa01adm：startsap

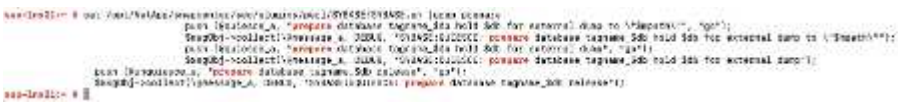
## 追加情報とバージョン履歴

休止と準備

リンク
：https://help.sap.com/docs/SAP_ASE/4e870f06a15b4bbeb237cca890000421/d9d3ce996bdd415693cdb17663bfc0e3.html?locale=en-US&version=16.0.2.0[SAPヘルプページ]のドキュメントを参照してください。




SnapCenter SAP ASEプラグインはquiesce databaseコマンドを使用しますが、prepareコマンドに置き換えることもできます。必要に応じて、473、475、479、481、673、675のSybase.pmで変更する必要があります。



デモの録画

ドキュメントをサポートするために、次の記録済みデモを利用できます。

インストールと設定ASEプラグイン、ASEデータベースのバックアップ

ASEデータベースのリストアとリカバリ

外部ドキュメント

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。

- "ANFでのAzureのSAPインストール"
- "SnapCenterプラグインの前提条件"
- "SnapCenterインストールプラグイン"
- "Sybase Infocenter - isql"
- "Sybase Infocenter -トランザクションログダンプをロード"
- SAP Notes（ログインが必要）
  - 1887068-SYB：SAP ASEでの外部バックアップとリストアの使用： https://me.sap.com/notes/1887068/E
  - 1618817- SYB: SAP ASEデータベース・サーバのリストア方法(UNIX): https://me.sap.com/notes/1618817/E
  - 1585981-SYB：SAP ASEのリカバリ性の確保： https://me.sap.com/notes/1585981/E
  - 1588316-SYB：データベースとログの自動バックアップを設定します。 https://me.sap.com/notes/1588316/E
  - NetApp製品ドキュメント： https://www.netapp.com/support-and-training/documentation/
  - "NetApp SAPソリューション–ユースケース、ベストプラクティス、メリットに関する情報"

バージョン履歴

| * バージョン * | * 日付 * | ドキュメントバージョン履歴 |
| --- | --- | --- |
| バージョン 1.0 以降 | 2025年4月 | 初期バージョン：ASEデータベースのバックアップ/リカバリ |

# IBM DB2データベース用のSnapCenter統合

## このドキュメントでは’SAP環境で使用されるIBM DB2データベースのSnapCenter統合の詳細について説明します

## はじめに

このドキュメントは、環境全体のセットアップ方法を段階的に説明することを目的としたものではありませんが、以下に関連する概念と関連する詳細について説明します。

- セツテイノカイヨウレイ
- サンプルレイアウト
- DB2データベースの保護
- DB2データベースのリストアとリカバリ

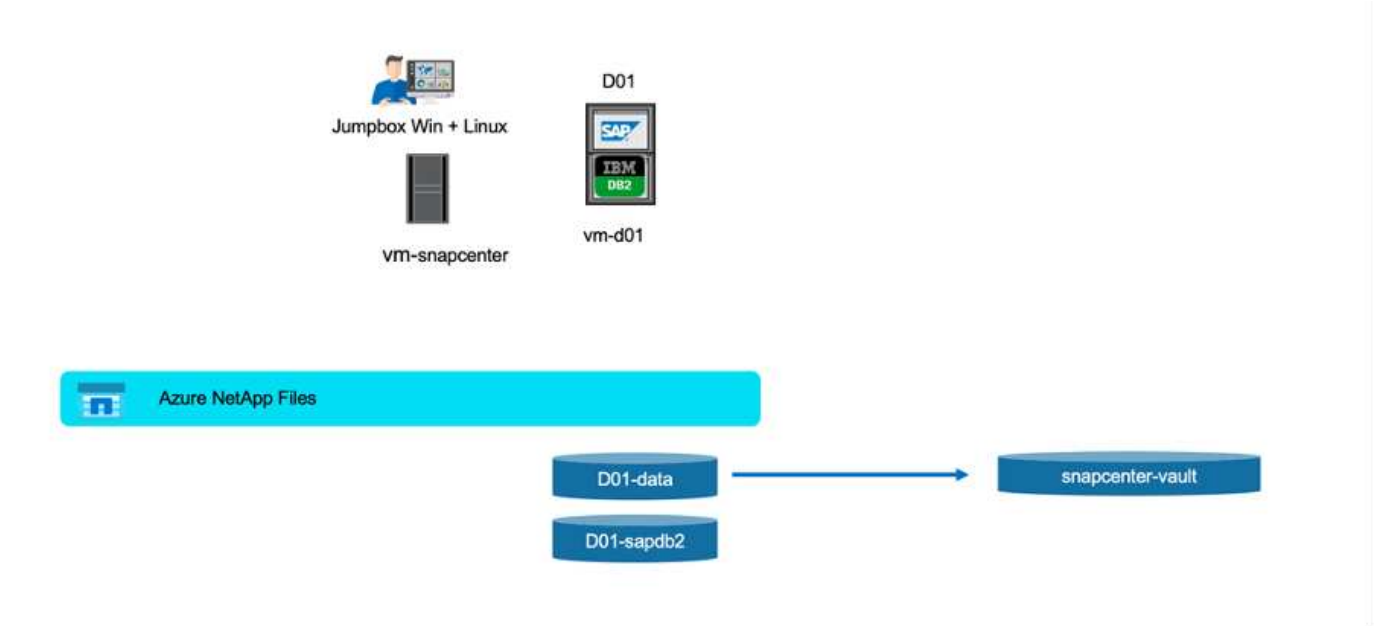
作成者：Michael Schlosser、NetApp

## セツテイノカイヨウレイ

AzureプラットフォームでSAPシステム向けSnapCenter DB2プラグインの実装例

この実装では、最小限必要なボリューム構成について説明します。

または、これに記載されている体積構造を"MSテクニカルコミュニティブログ"使用することもできます。




## デモ環境

ソフトウェアバージョン

| ソフトウェア | * バージョン * |
| --- | --- |
| Linux OS | SLES for SAP 15 SP5 |
| SAP | SAP NetWeaver 7.5 |
| DB2 | 10.5.0.7 |
| SnapCenter | 6.1 |

**DB2**ボリューム設計

DB2データベースのバックアップ/リカバリとクローンのユースケースには、次の最小ボリュームレイアウト

を使用する必要があります。この設定例では、<SID>：D01を使用しています。

| ボリューム名 | ボリューム上のディレクトリ（**qtree**） | サーバ上のマウントポイント | * コメント * |
|---|---|---|---|
| <SID>- sapdb2 | DB2 | /db2 | |
| | | /DB2/<SID> | DB2関連ファイルの親ディレクトリ |
| | | /DB2/DB2 <sid> | ユーザDB2 <sid>およびDB2ソフトウェアのホームディレクトリ |
| | | /db2/<SID>/db2dump | DB2診断ログおよびダンプファイル |
| | | /DB2 /<SID>/バックアップ | バックアップの場所（別のボリュームに配置される場合がある） |
| | | /db2/<SID>/log_arch | オフラインREDOログ（別のボリュームに配置される可能性があります。Snapshotがトリガーされます） |
| | | /db2/<SID>/log_dir | オンラインREDOログ（別のボリュームに配置されている可能性があります。Snapshotがトリガーされます） |
| | <sid> adm | <sid> adm | ユーザ<sid> admのホームディレクトリ |
| | SAP <sid> | /home/SAP <sid> | ユーザsap <sid>のホームディレクトリ |
| | usrsaptrans | /usr/sap/trans | 転送ディレクトリ |
| | Usrsap <SID> | /usr/sap/<SID> | ユーザSAP |
| | sapmnt <SID> | /sapmnt/<SID> | SAP GlobalHostディレクトリ |
| <SID>データ | sapdata1 | /db2 /<SID>/ sapdata1 | DBデータ |
| | sapdata2 | /db2 /<SID>/ sapdata2 | DBデータ |
| | sapdata3 | /db2 /<SID>/ sapdata3 | DBデータ |
| | sapdata4 | /db2 /<SID>/ sapdata4 | DBデータ |
| | saptmp1 | /db2/<SID>/saptmp1 | DB一時ファイル |
| | saptmp2 | /db2/<SID>/saptmp2 | DB一時ファイル |
| | saptmp3 | <SID>/saptmp3 | DB一時ファイル |
| | saptmp4 | <SID>/saptmp4 | DB一時ファイル |
| | DB2 <sid> | /DB2/<SID>/ DB2 <sid> | インスタンスファイル |

DB2プラグインでは自動検出がデフォルトで有効になっているため、次のファイルパスに一致するボリュームに対してSnapshotが作成されます。

| | |
|---|---|
| Database StoragePath | /db2/D01/saptmp4/, /db2/D01/saptmp3/, /db2/D01/saptmp2/, /db2/D01/saptmp1/, /db2/D01/sapdata4/, /db2/D01/sapdata3/, /db2/D01/sapdata2/, /db2/D01/sapdata1/ |
| Database LogPath | /db2/D01/log_dir/NODE0000/LOGSTREAM0000/ |
| Database Archive Path (Primary) | DISK:/db2/D01/log_arch/ |

データベース**D01**を保護する手順

- サンプルレイアウトに従ってファイルの配布をチェックします。
- ホストの前提条件の確認（vm-d01）
- データベースの前提条件の確認（D01）
- ホストへのSnapCenterエージェントの導入/インストール（vm-d01）
- SnapCenterインスタンスリソース構成の作成

ホストの前提条件

詳細については、次のサイトを参照してください。

- https://docs.netapp.com/us-en/snapcenter/protect-scu/reference_prerequisites_for_adding_hosts_and_installing_snapcenter_plug_ins_package_for_linux.html
- https://docs.netapp.com/us-en/snapcenter/protect-db2/prerequisites-for-using-snapcenter-plug-in-for-ibm-db2.html

ホストを追加してLinux用のプラグインパッケージをインストールする前に、すべての要件を満たしておく必要があります。

- iSCSIを使用している場合は、iSCSIサービスが実行されている必要があります。
- パスワードベースの認証またはSSHキーベースの認証を使用できます。パスワードベースの認証はrootユーザとroot以外のユーザが使用できます。
- SnapCenter Plug-in for UNIX File Systemsは、root以外のユーザもインストールできます。ただし、プラグイン プロセスをインストールして開始できるよう、root以外のユーザにsudo権限を設定する必要があります。プラグインのインストール後、プロセスは有効なroot以外のユーザとして実行されます。
- インストール ユーザのクレデンシャルを、認証モードをLinuxに設定して作成します。
- Java 11をLinuxホストにインストールしておく必要があります。
- LinuxホストにJava 11の認定エディションのみがインストールされていることを確認します。
- Javaのダウンロードについては、「Java Downloads for All Operating Systems」を参照してください。
- プラグインのインストールには、デフォルトのシェルとしてbashを使用する必要があります。

データベースの前提条件–ログとバックアップの有効化

> オフラインログを有効にするには、データベースのオフラインフルバックアップが必要です。通常、生産性の高いシステムではすでに有効になっています。

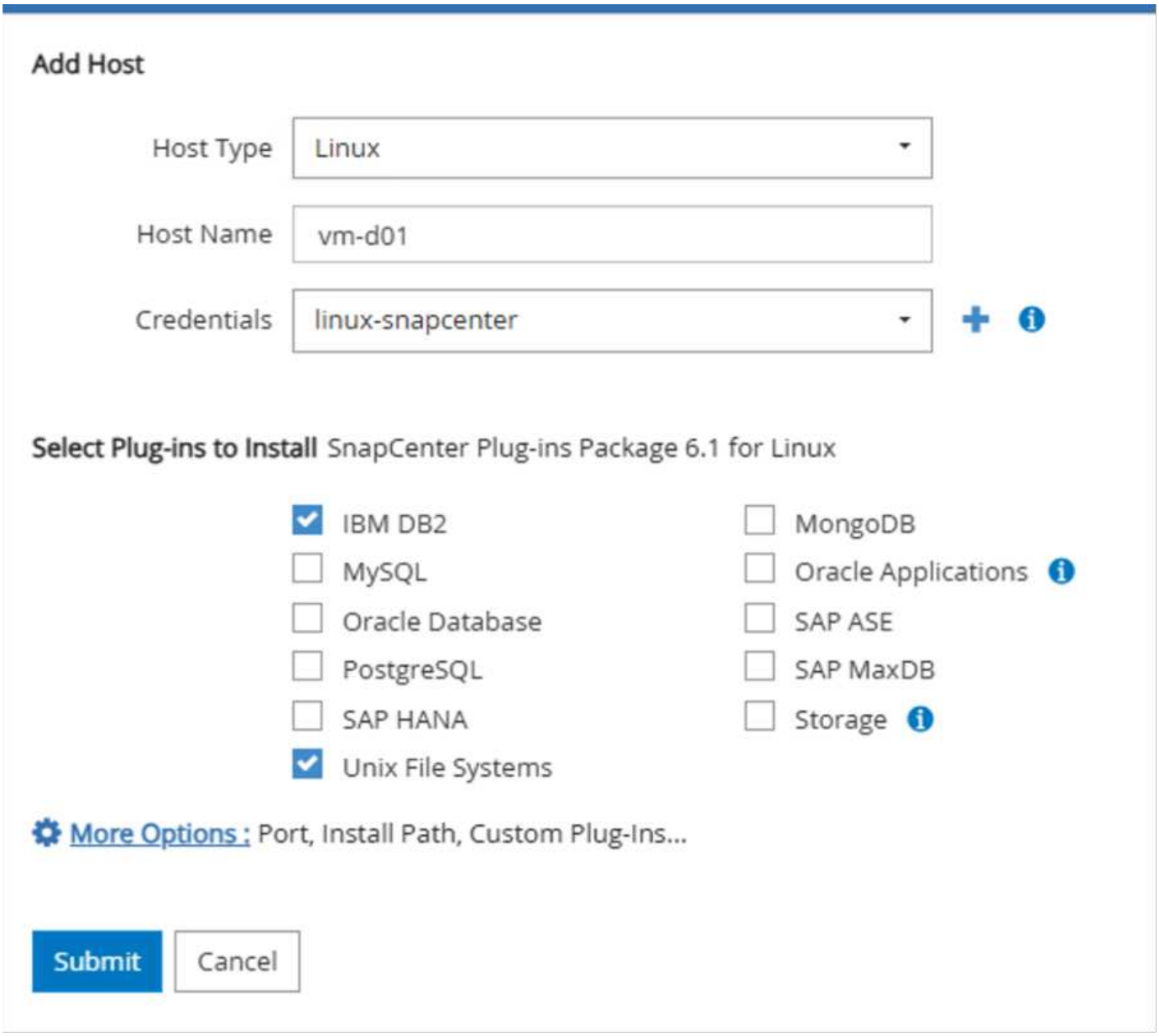
- バックアップおよびLOG_ARCHのディレクトリの作成（/db2/d01/backup、/sybase/d01/log_arch）

- logarchmeth1を有効にする（os-user db2d01として）
  - db2は、logarchmeth1 disk：/db2/d01/log_arch/を使用してD01のdb cfgを更新します。
- オフラインバックアップの作成（os-user db2d01として）
  - db2ストップフォース
  - db2start adminモード制限付きアクセス
  - DB2バックアップDB D01から/DB2/D01/backup
  - db2 activate db D01

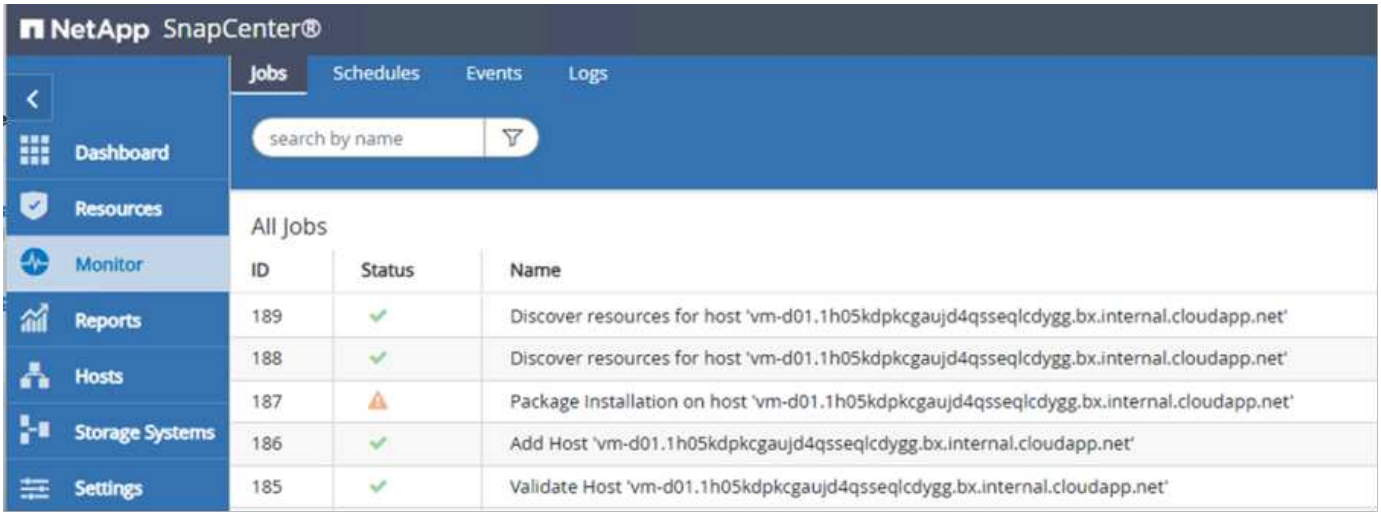
**SnapCenter**エージェントをホスト**VM-d01**にデプロイする

詳細については、を参照して"SnapCenter のドキュメント"ください。

[IBM DB2 and Unix File Systems Plugins]を選択します。



インストール後、ホスト上のデータベースの検出が開始されます。

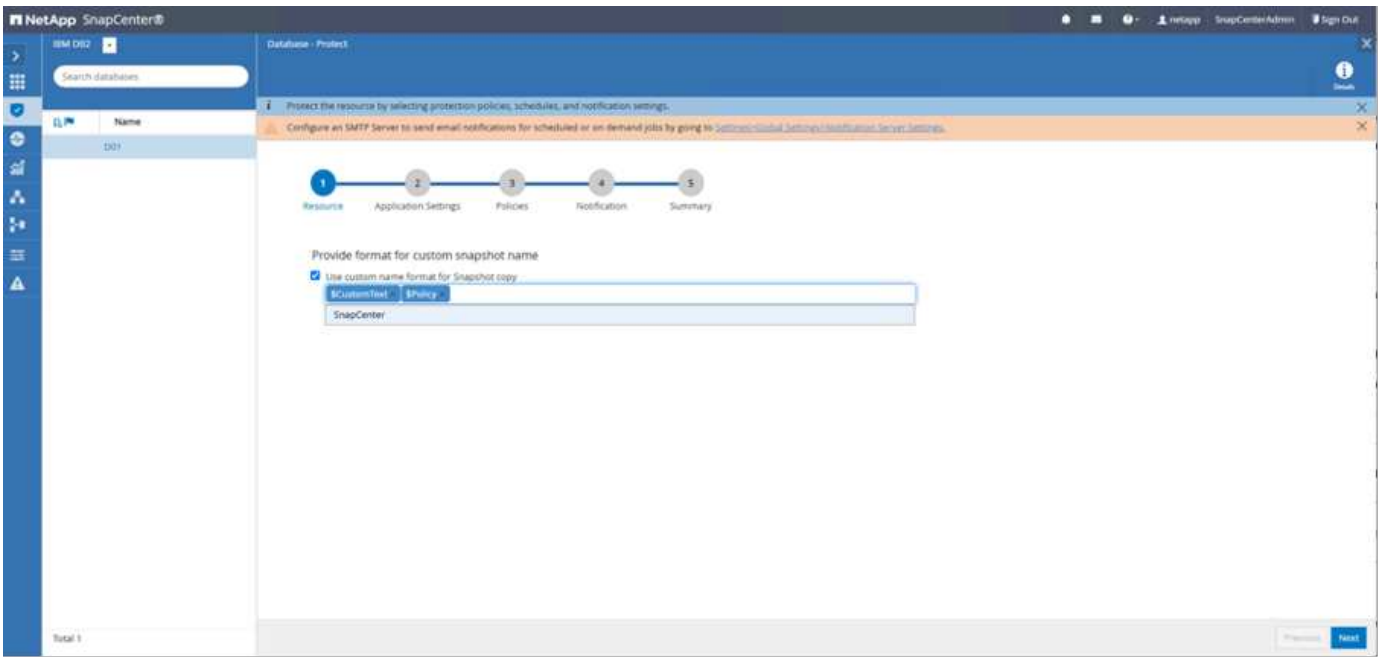



データベース**D01**のリソース構成の作成

検出されたリソースD01を選択

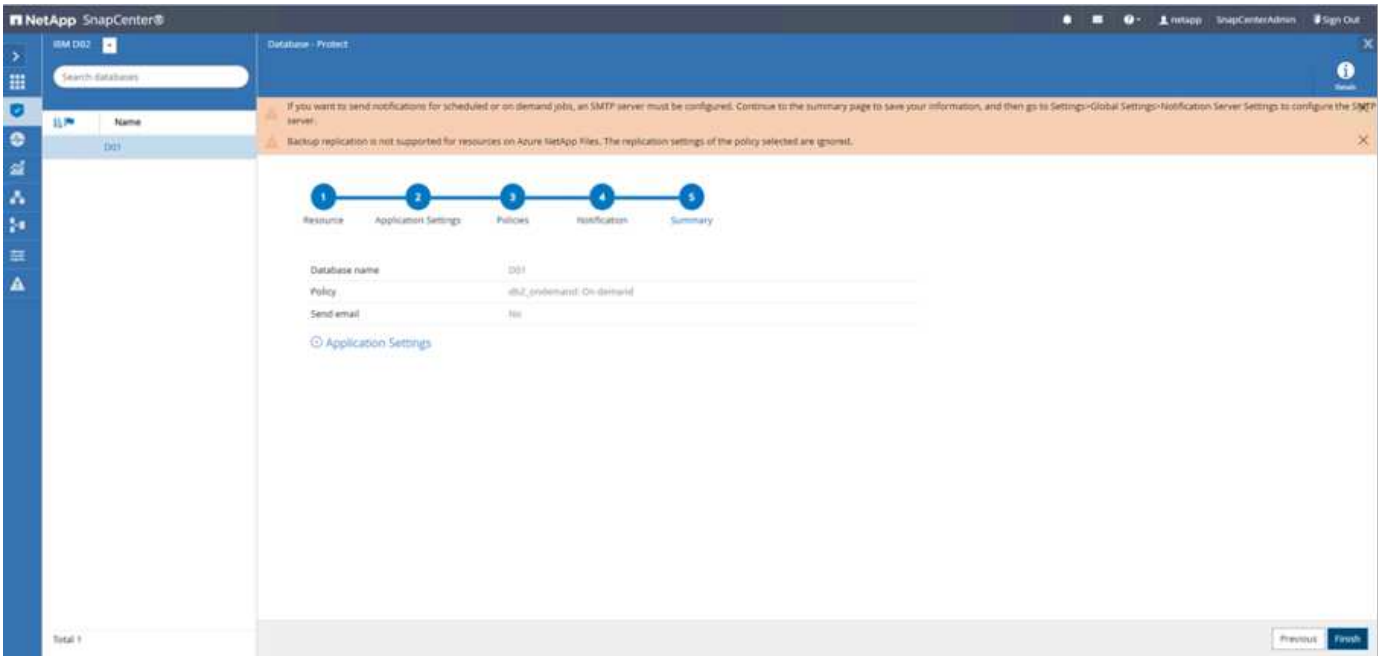



Snapshot名の設定




ダイアログのスクリーンショット"]

特定のアプリケーション設定は必要ありません。必要に応じてポリシーと通知を設定します。




設定を完了します。

システム**D01**を回復する手順

1. SAPシステムD01の停止（データベースを含む）
2. SnapCenterバックアップのリストア（ボリュームD01-data）
   a. ファイルシステムのアンマウント
   b. ボリュームのリストア
   c. ファイルシステムのマウント
   d. データベースをミラーDBとして初期化
3. データベースD01のリカバリ（DB2ロールフォワードを使用）
4. SAPシステムD01の起動

データベース**D01**のリカバリ

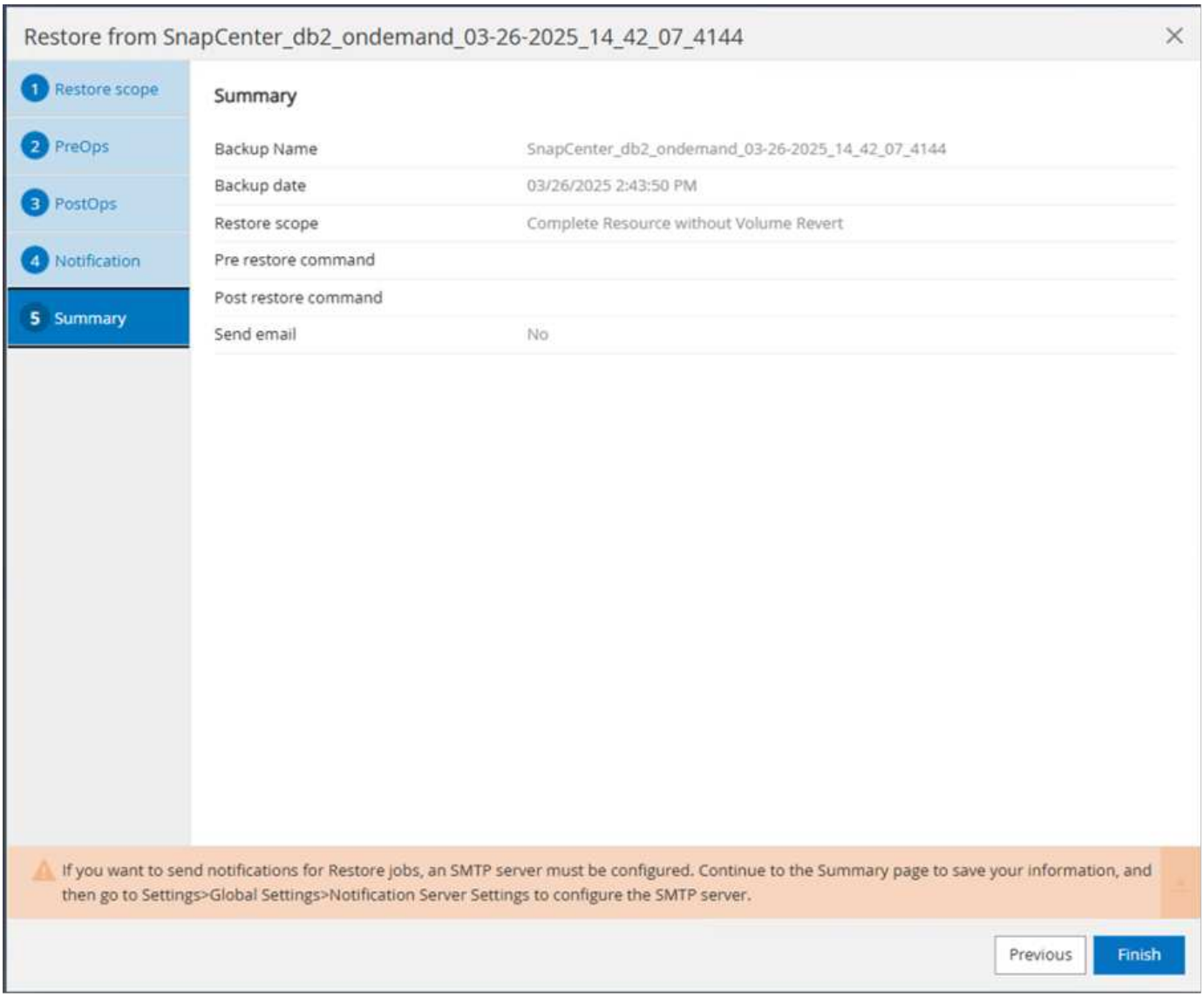
- ホストVM上でSAPシステム+ DB D01を停止- d01
  - ユーザーd01adm:停止
- リストア バックアップ
  - SnapCenter GUI：リストアに必要なバックアップを選択




- ANF導入の場合–完全なリソースのみ提供




概要が表示され、[Finish]をクリックすると、実際のリストアが開始されます。




「db2inidb D01 as mirror」は、SnapCenterリストアワークフローの一部として実行されます。

- リカバリステータスデータベースD01（ユーザdb2d01として）を確認します
  - DB2 rollforward db D01クエリステータス
- 必要に応じてデータベースをリカバリします。ここではロスレスリカバリが開始されます（ユーザdb2d01として実行）。
  - db2 rollforward db d01からログの末尾へ
- データベースリカバリの停止とオンラインデータベースD01（ユーザdb2d01として）
  - DB2ロールフォワードDB D01ストップ
- SAPシステムの起動(ユーザd01admとして)
  - スタートサップ

## 追加情報とバージョン履歴

ドキュメントをサポートするために、次の記録済みデモを利用できます。

インストールおよび設定DB2プラグイン、DB2データベースのバックアップ

DB2データベースのリストアとリカバリ

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。

- "SAP on DB2インストールAzure on ANF"
- "SnapCenterプラグインの前提条件"
- "SnapCenterインストールプラグイン"
- "SnapCenter DB2プラグインのドキュメント"
- SAP Notes（ログインが必要）
  - 83000- DB2/390:バックアップとリカバリのオプション: https://me.sap.com/notes/83000
  - 594301-db6:管理ツールとスプリットミラー: https://me.sap.com/notes/594301
- NetApp製品ドキュメント： https://www.netapp.com/support-and-training/documentation/
- "NetApp SAPソリューション–ユースケース、ベストプラクティス、メリットに関する情報"

バージョン履歴

| * バージョン * | * 日付 * | ドキュメントバージョン履歴 |
| --- | --- | --- |
| バージョン 1.0 以降 | 2025年4月 | 初期バージョン：バックアップ/リカバリDB2データベース |

# SAP MaxDBデータベースのSnapCenter統合

このドキュメントでは、SAP環境で使用されるSAP MaxDBデータベースの SnapCenter 統合について説明します。

## はじめに

このドキュメントは、環境全体のセットアップ方法を段階的に説明することを目的としたものではありませんが、以下に関連する概念と関連する詳細について説明します。

- セツテイノカイヨウレイ
- サンプルレイアウト
- SAP MaxDBインスタンスの保護
- SAP MaxDBインスタンスのリストアとリカバリ

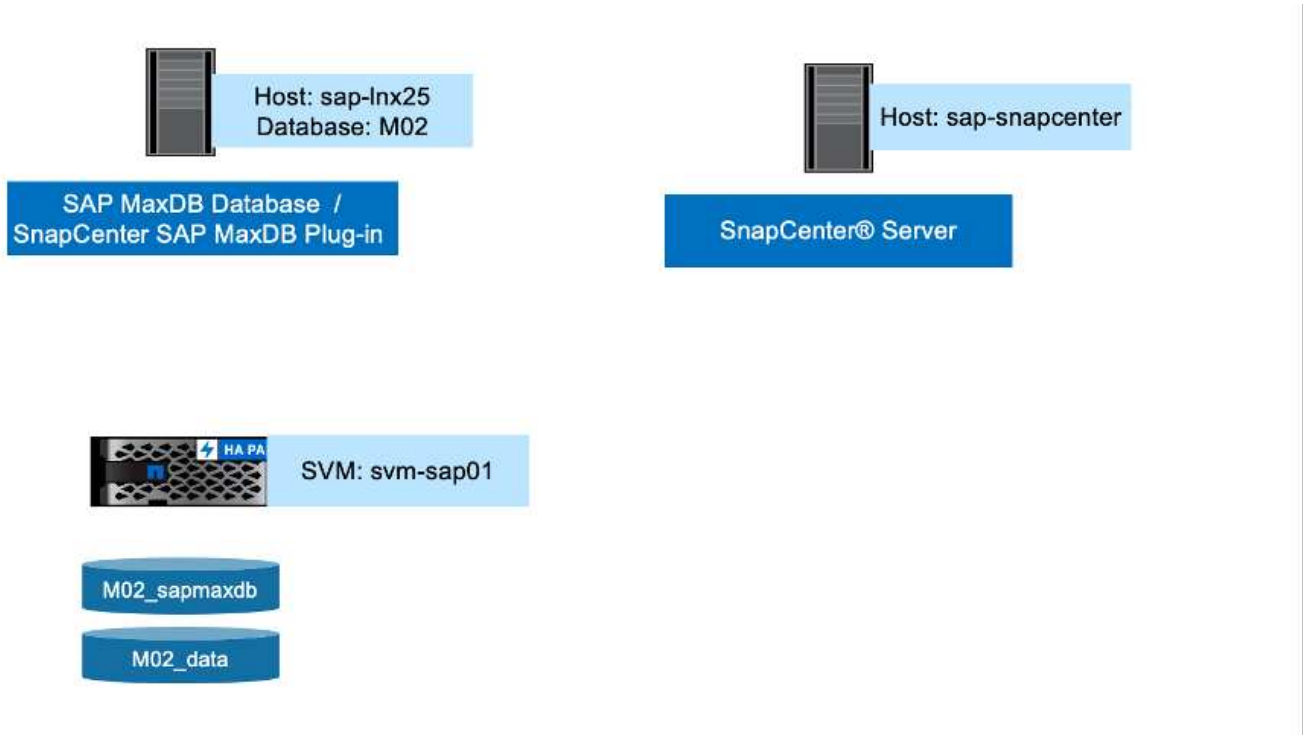
## セツテイノカイヨウレイ

デモセンターで実行されているSAPシステム用のSnapCenter MaxDBプラグインの実装例。

この実装では、最小限必要なボリューム構成について説明します。Data Dump Backups and Log Dump Backups、Backup Templateなどは、SAP Note「1928060 - Data backup and recovery with file system backup」およびそこから参照されている注意事項に従って設定します。

または、に記載されているボリューム構造を"MS Techcommunityブログ"使用することもできます。

## デモ環境




## ソフトウェアバージョン

| ソフトウェア | * バージョン * |
|---|---|
| Linux OS | SLES for SAP 15 SP5 |
| SAP | SAP NetWeaver 7.5 |
| SAP MaxDB | DBMServer 7.9.10ビルド004-123-265-969 |
| SnapCenter | 6.1 |

## MaxDBボリューム設計

SAP MaxDBデータベースのバックアップ/リカバリとクローンのユースケースを有効にするには、以下の最小ボリュームレイアウトを使用する必要があります。この設定例では、<SID>：M02を使用しています。

| ボリューム名 | ボリューム上のディレクトリ（**qtree**） | サーバ上のマウントポイント | * コメント * |
|---|---|---|---|
| <SID>_ sapmaxdb | SAPDB | /SAPDB | MaxDB関連ファイルの親ディレクトリ |

| ボリューム名 | ボリューム上のディレクトリ（**qtree**） | サーバ上のマウントポイント | * コメント * |
|---|---|---|---|
| | | /SAPDB/SAPDB/SAPLOG <SID> | REDOログ（別のボリュームに配置される可能性あり） |
| | | /SAPDB /<SID>/バックアップ | ダンプバックアップ（データ+ログ）（別のボリュームに配置可能） |
| | <sid> adm | <sid> adm | ユーザ<sid> admのホームディレクトリ |
| | sdb | /home/sdb | ユーザsdbのホームディレクトリ |
| | SQD <sid> | /home/sqd <sid> | ユーザsqd <sid>のホームディレクトリ |
| | usrsaptrans | /usr/sap/trans | 転送ディレクトリ |
| | Usrsap <SID> | /usr/sap/<SID> | ユーザSAP |
| | sapmnt <SID> | /sapmnt/<SID> | SAP GlobalHostディレクトリ |
| <SID>データ | SAPDATA | /SAPDB/SAPDB/sapdata <SID> | DBデータファイル（SID） |

## データベース**M02**を保護する手順

- サンプルレイアウトに従ってファイルの配布をチェックします。
- ホストの前提条件の確認（sap-lnx25）
- データベースの前提条件の確認(M02)
- ホストへのSnapCenterエージェントの導入/インストール（sap-lnx25）
- SnapCenterインスタンスリソース構成の作成

## ホストの前提条件

より最新の情報が得られる可能性があり"ここをクリック"ます。

ホストを追加してLinux用のプラグインパッケージをインストールする前に、すべての要件を満たしておく必要があります。

- iSCSIを使用している場合は、iSCSIサービスが実行されている必要があります。
- パスワードベースの認証またはSSHキーベースの認証を使用できます。パスワードベースの認証はrootユーザとroot以外のユーザが使用できます。
- SnapCenter Plug-in for UNIX File Systemsは、root以外のユーザもインストールできます。ただし、プラグイン プロセスをインストールして開始できるよう、root以外のユーザにsudo権限を設定する必要があります。プラグインのインストール後、プロセスは有効なroot以外のユーザとして実行されます。
- インストール ユーザのクレデンシャルを、認証モードをLinuxに設定して作成します。
- Java 11をLinuxホストにインストールしておく必要があります。
- LinuxホストにJava 11の認定エディションのみがインストールされていることを確認します。
- Javaのダウンロードについては、「Java Downloads for All Operating Systems」を参照してください。
- プラグインのインストールには、デフォルトのシェルとしてbashを使用する必要があります。

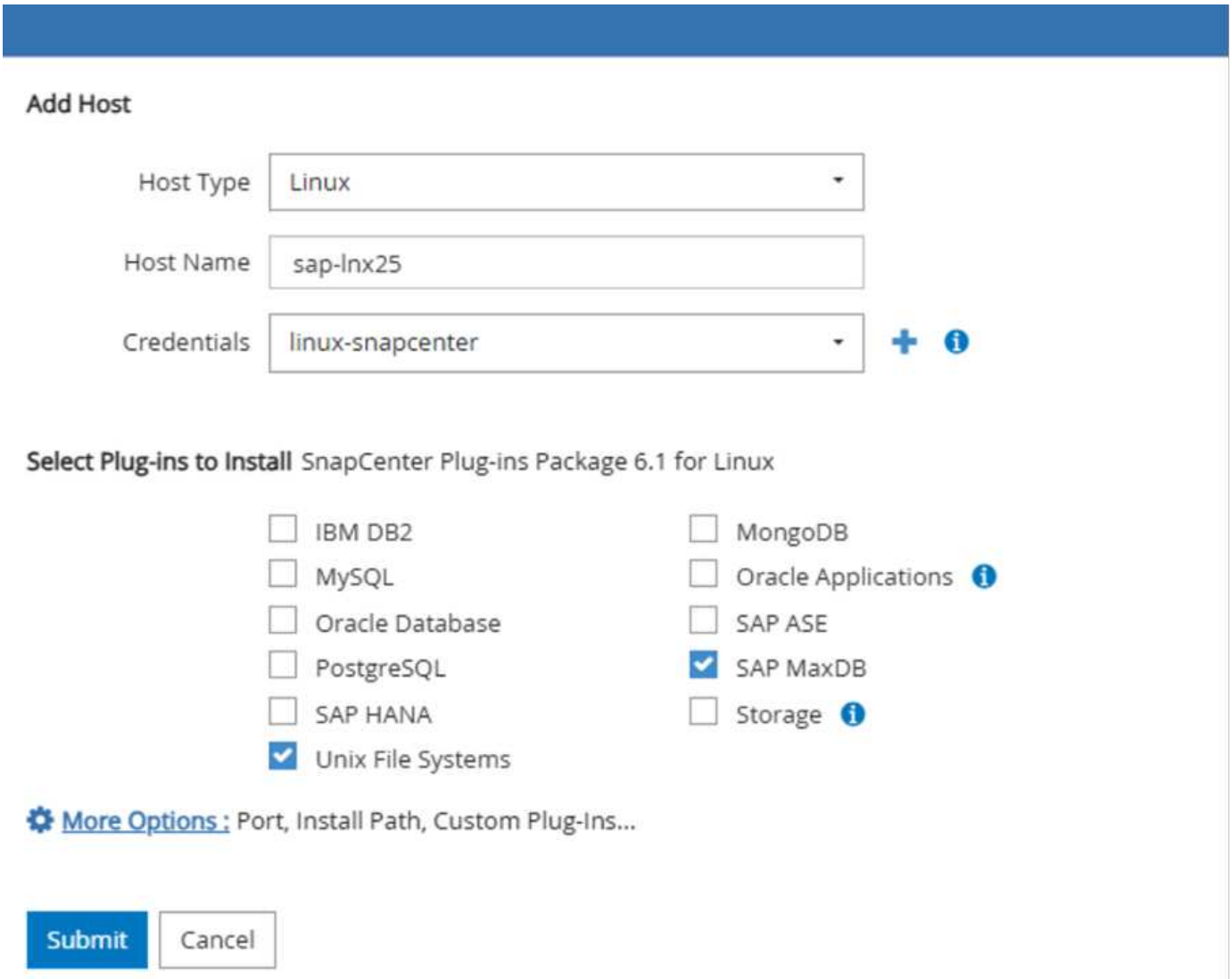
## データベースの前提条件–バックアップテンプレートの作成、ログバックアップの有効化

- データおよびログのバックアップ用ディレクトリの作成（/sapdb/m02/backup/data 、/sapdb/m02/backup/log–owner sdb：sdba–Permissions 755）
- データベースM02に接続（OS-user sqdm02として）
  - dbmcli -d M02 -uコントロール、<password>
- SAP Note 1928060に従って、データファイルバックアップテンプレート（M02_DATA）を作成します。
  - backup_template_create M02_data to file /SAPDB/M02/backup/data/M02_data content data
- SAP Note 1928060に従って、データバックアップテンプレート（M02_log）を作成します。
  - backup_template_create M02_logをファイル/SAPDB/M02/backup/log/m02_logコンテンツログに保存
- SAP Note 1928060に従って、データSnapshotバックアップテンプレート（M02_snap）を作成
  - 外部スナップショットへのbackup_template_create M02_snap
- ログバックアップを有効にするには偽装バックアップを作成してください
  - util_connect
  - バックアップ開始M02_SNAP
  - backup_finish M02_snap ExternalBackupID first_full_fake_backup
- データベースロギングモードの切り替え
  - 自動ログオフ
  - AutoLog_on M02_log間隔300
  - AutoLog_show

## **sap-lnx25**をホストするための**SnapCenter**エージェントの配備

詳細については、を参照して"SnapCenter のドキュメント"ください。

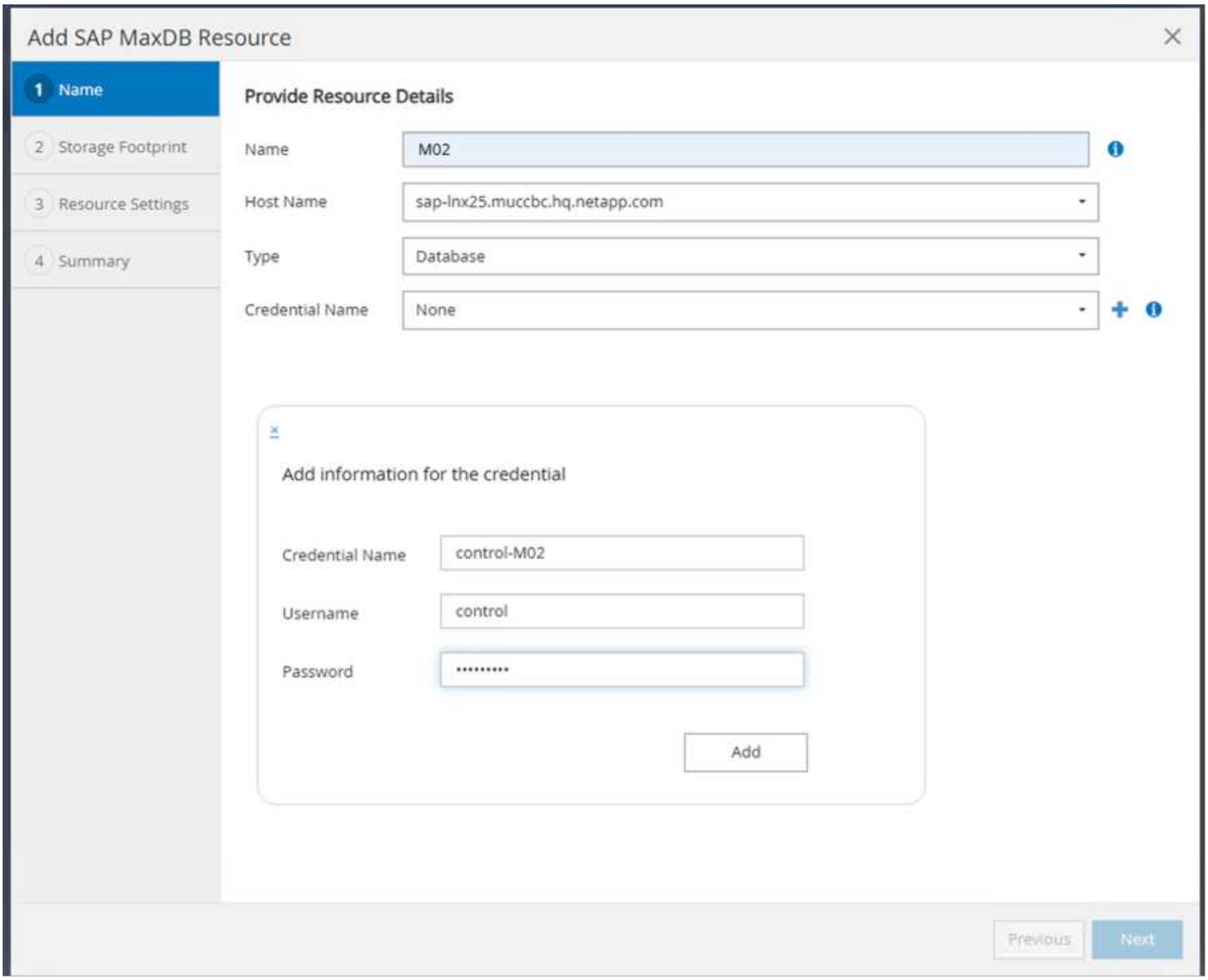
[SAP MaxDB and Unix File Systems Plugins]を選択します。




ユーザインターフェイスのスクリーンショット"]

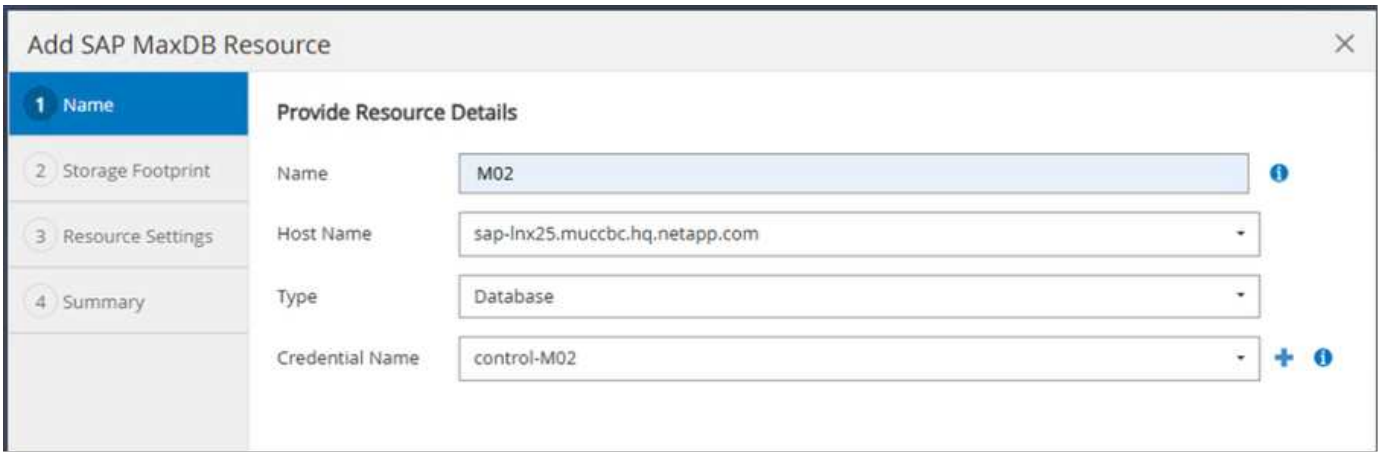
## データベース**M02**の**SnapCenter**リソース構成の作成

リソース→ SAP MaxDB →リソースの追加

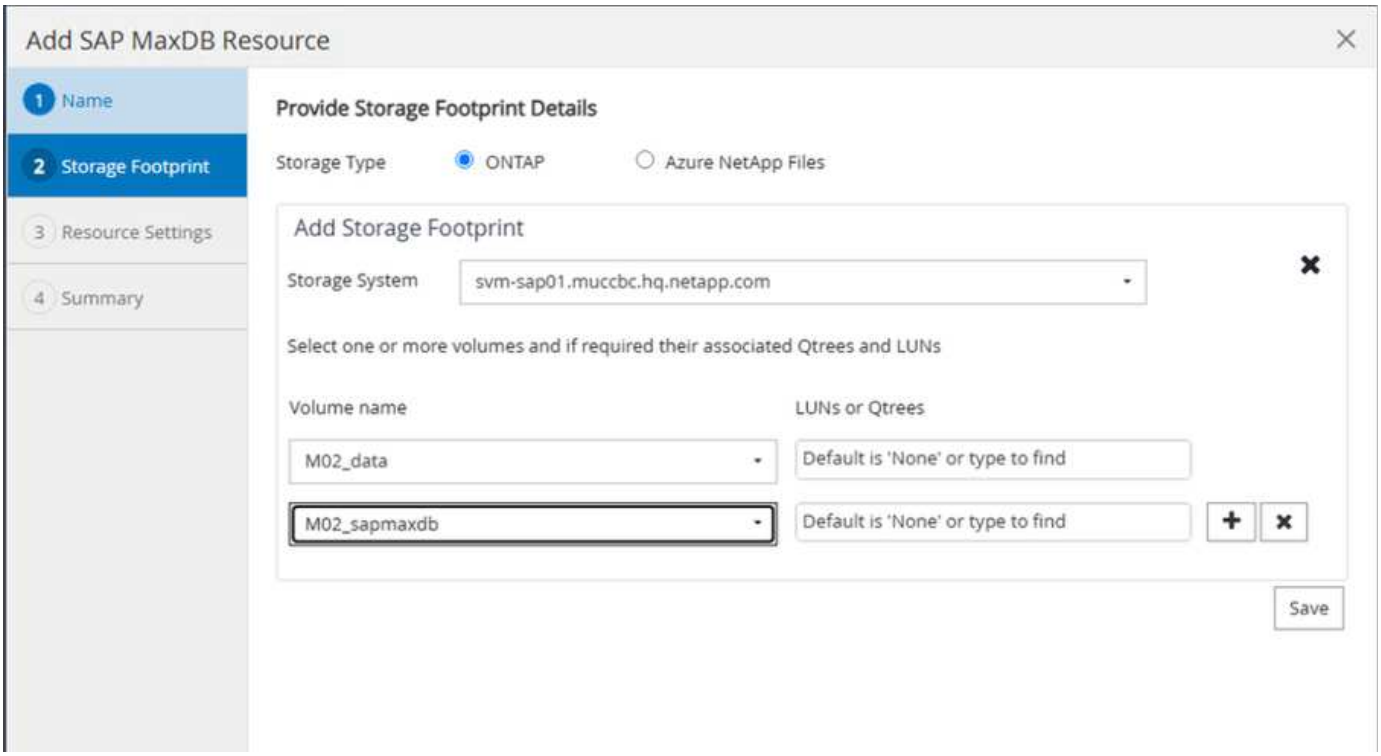


ユーザインターフェイスのスクリーンショット"]

パスワードに特殊文字が含まれている場合は、バックスラッシュでマスクする必要があります（例：Test!123! →テスト\!123\!）。

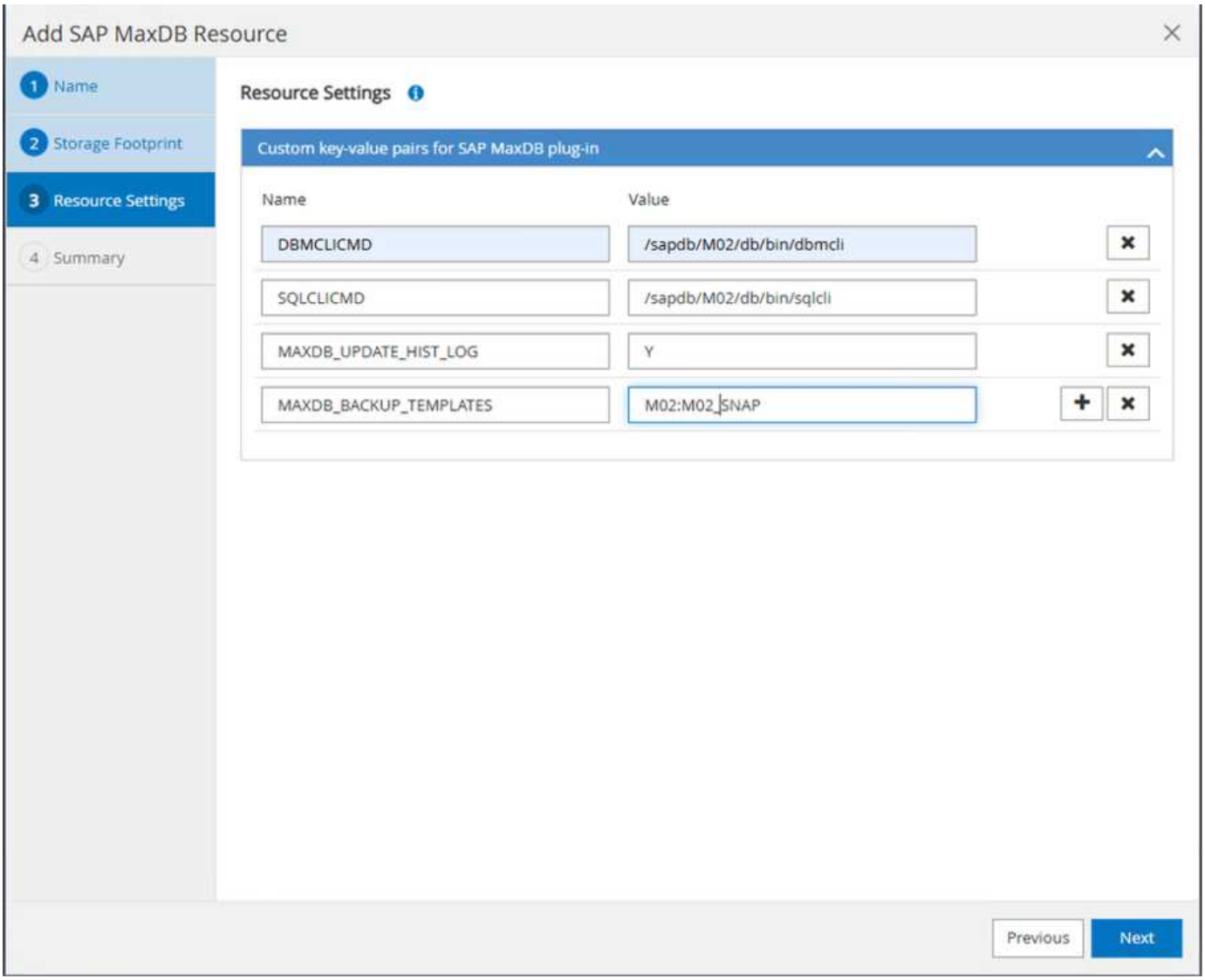


ユーザインターフェイスのスクリーンショット"]



ユーザインターフェイスのスクリーンショット"]

次のリソース設定カスタムのキーと値のペアを作成する必要があります(少なくとも)。

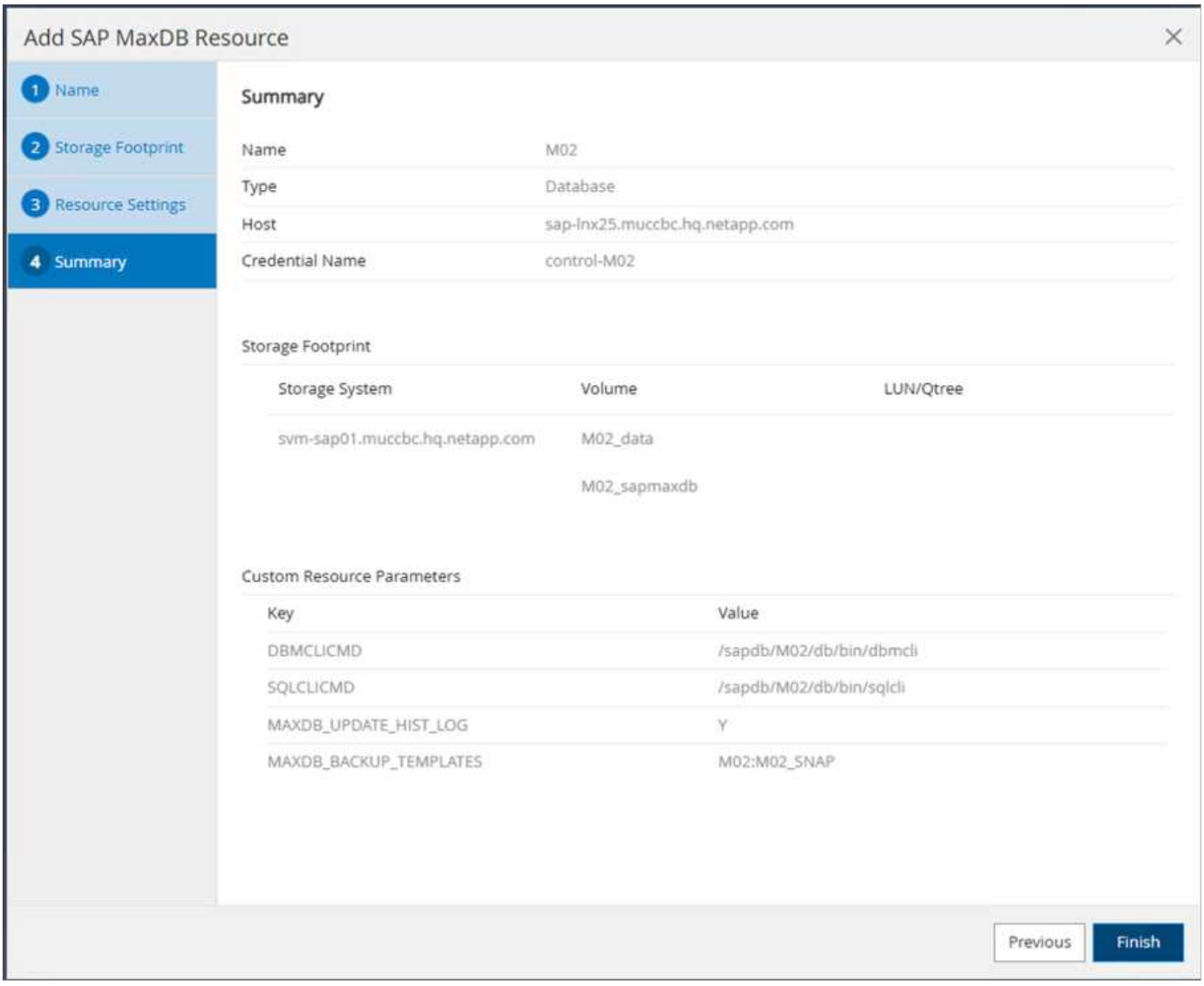


ユーザインターフェイスのスクリーンショット"]

次の表に、 MaxDB プラグインのパラメータを示します。このパラメータの設定と説明が表示されます。

| * パラメータ * | 設定 | * 概要 * |
| --- | --- | --- |
| handle_logWRITER | （Y/N） | suspend logwriter （ N ） または resume logwriter （ Y ）操作を実行します。 |
| DBMCLICMD | path_to dbmcli_cmd | MaxDB の dbmcli コマンドへのパスを指定します。設定しない場合、検索パス上の dbmcli が使用されます。 |
| SQLCLICMD | path_to _sqlcli_cmd | MaxDB の sqlcli コマンドのパスを指定します。設定しない場合、 sqlcli は検索パスで使用されます。 |
| MaxDB の更新 _HIST_LOG | （Y/N） | MaxDB バックアッププログラムに MaxDB 履歴ログを更新するかどうかを指示します。 |

| * パラメータ * | 設定 | * 概要 * |
| --- | --- | --- |
| MaxDB のバックアップテンプレート | template_name（例： M02_SNAP） | 各データベースのバックアップテンプレートを指定します。テンプレートはすでに存在している必要があり、外部タイプのバックアップテンプレートである必要があります。MaxDB 7.8 以降の Snapshot コピー統合を有効にするには、 MaxDB のバックグラウンドサーバ機能を持っていて、 MaxDB バックアップテンプレートをすでに設定している必要があります。 |
| MaxDB の BG_server_prefix | BG_SERVER_PREFIX（例： na_bg） | バックグラウンドサーバ名のプレフィックスを指定します。MaxDB_backup_templatesパラメータが設定されている場合は、MaxDB_BG_SERVER_PREFIXパラメータも設定する必要があります。プレフィックスを設定しない場合は、デフォルト値na_bg_databaseが使用されます。 |

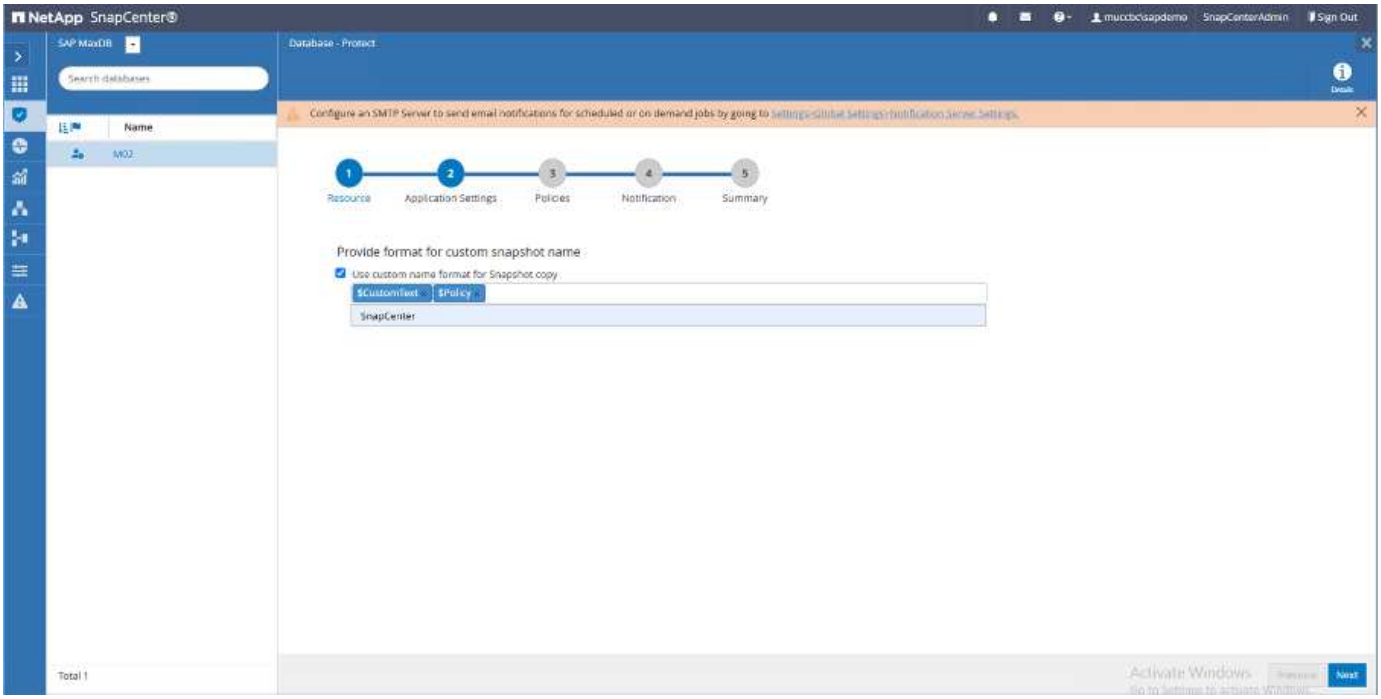


ユーザインターフェイスのスクリーンショット"]

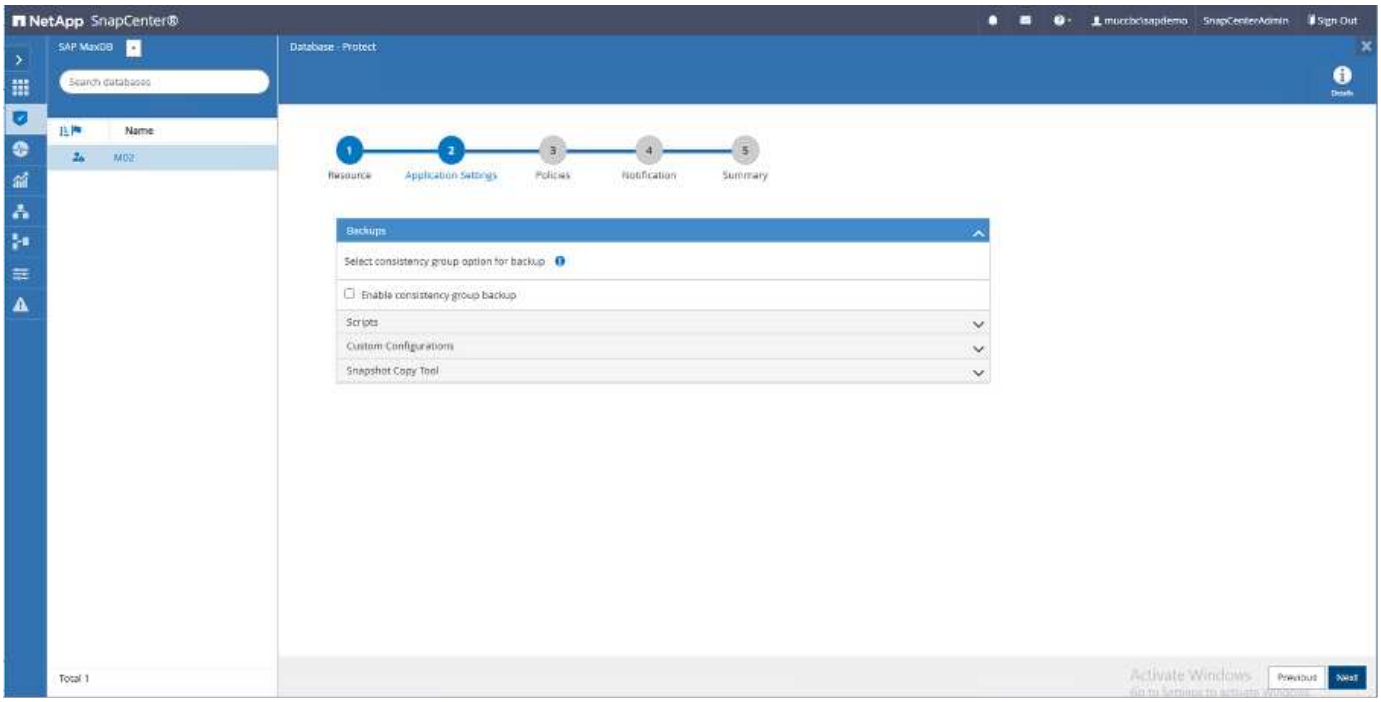
これで、全体的な保護コンセプトに従って設定を終了し、バックアップをスケジュールできます。



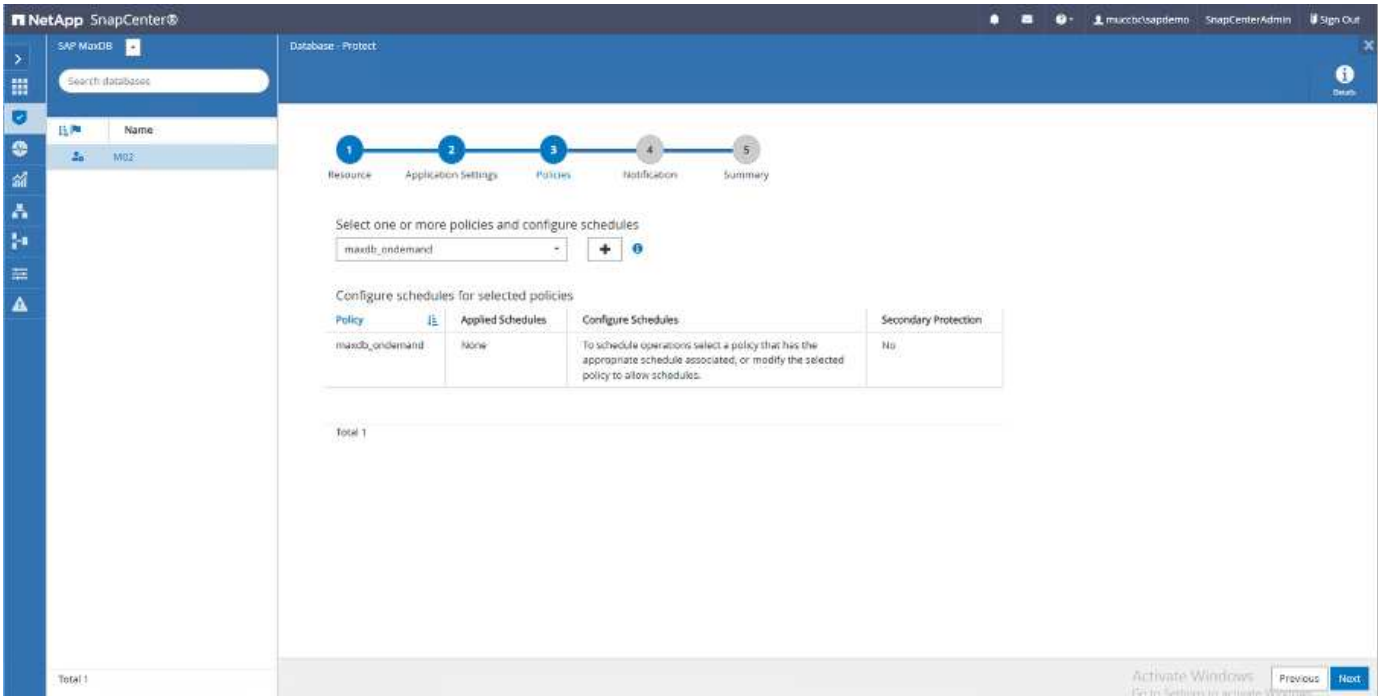
ユーザインターフェイスのスクリーンショット"]



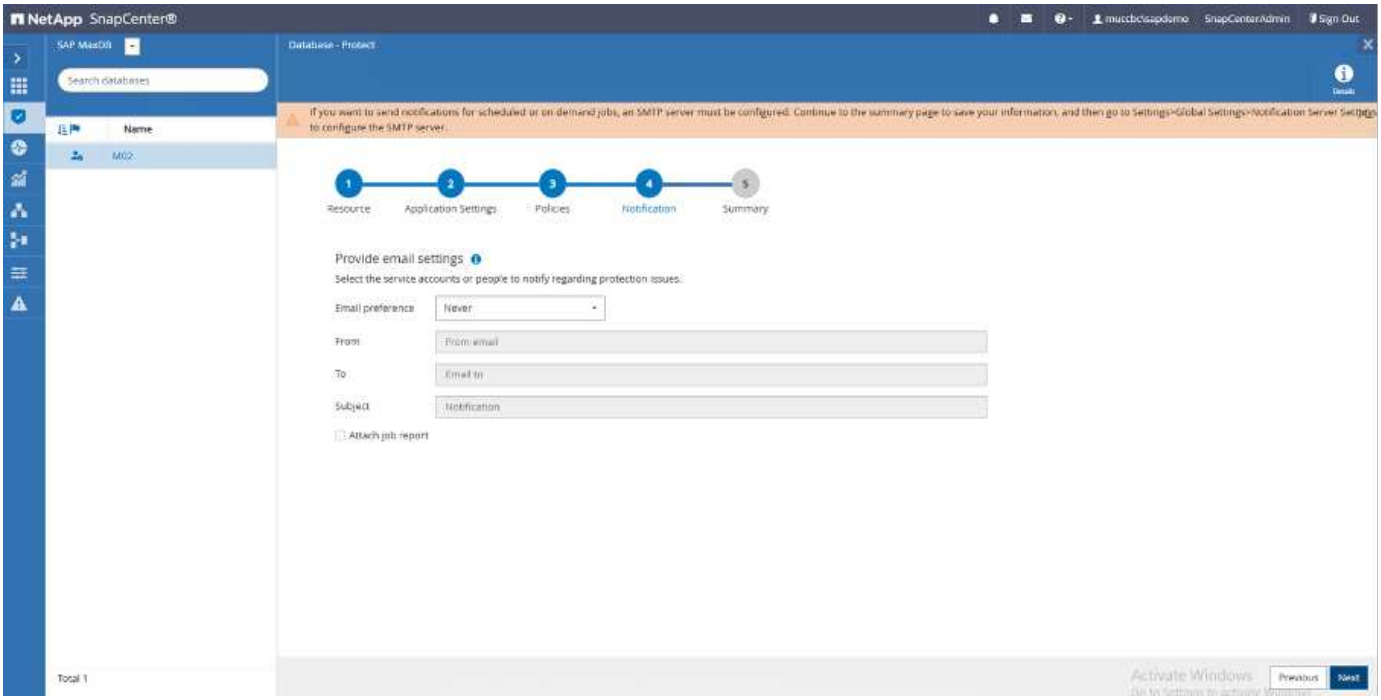
ユーザインターフェイスのスクリーンショット"]



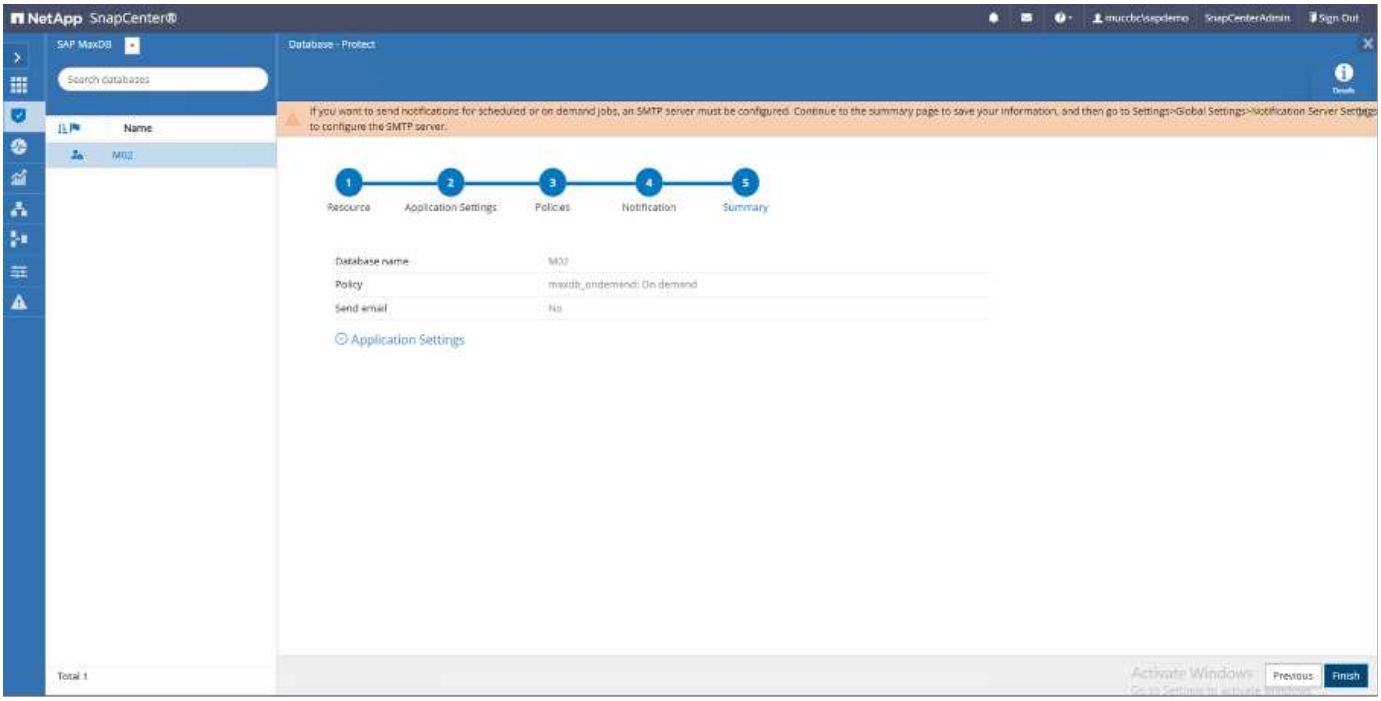
ユーザインターフェイスのスクリーンショット"]




ユーザインターフェイスのスクリーンショット"]




ユーザインターフェイスのスクリーンショット"]



ユーザインターフェイスのスクリーンショット"]

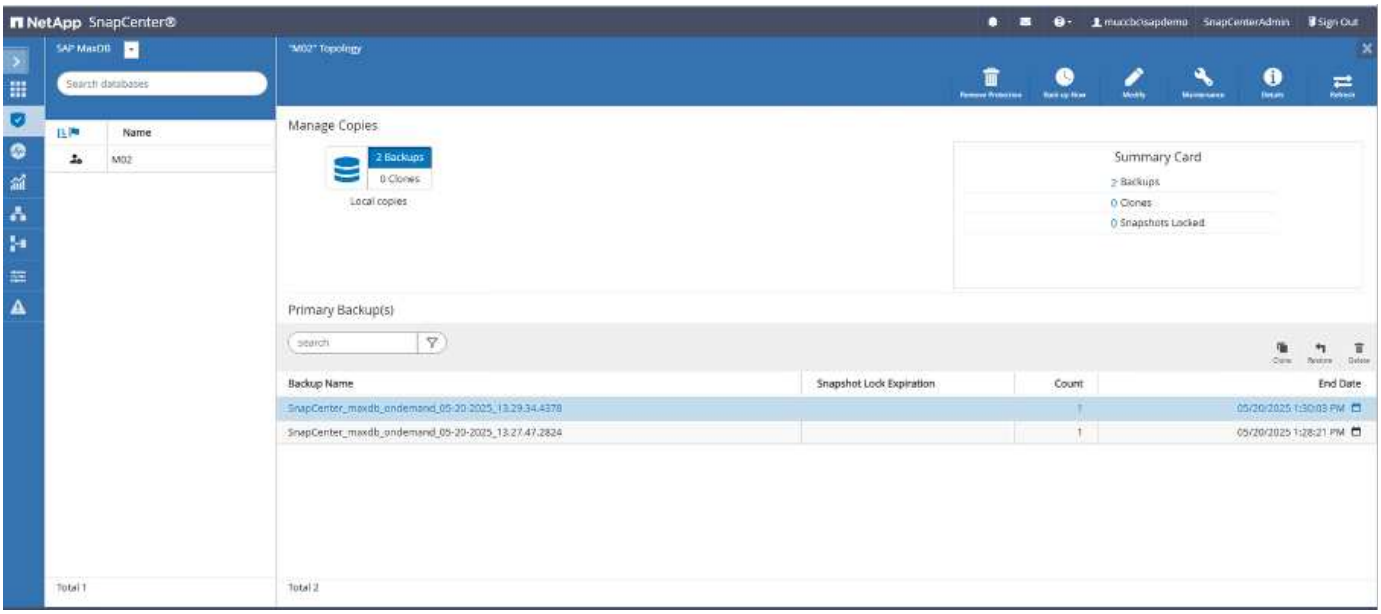
## システム**M02**をリカバリする手順

1. SAPシステムM02（データベースを含む）の停止、sapinitの停止
2. ファイルシステム/SAPDB/M02/sapdataのアンマウント
3. ボリュームM02_dataのリストア（SnapCenterを使用）
4. ファイルシステム/SAPDB/M02/sapdataをマウント
5. データベースM02の起動と接続（管理者モード）
6. バックアップ情報の収集
7. データベースデータバックアップのリカバリ
8. データベースログバックアップをリカバリします。
9. データベースの停止
10. sapinit、SAPシステムM02の起動

## インスタンス**M02**のリカバリ

- ホストsap-lnx25でSAPシステム+ DB M02を停止
  - ユーザーm02adm：停止
  - オプション–データベースが正常に停止していない場合–ユーザ：sqdm02
  - dbmcli -d M02 -uコントロール、<password>
    - DB_OFFLINE
  - ユーザroot：/etc/init.d/sapinit stop
  - ユーザroot：umount /sapdb/m02/sapdata

- リストア バックアップ
  - SnapCenter GUI：リストアに必要なバックアップを選択



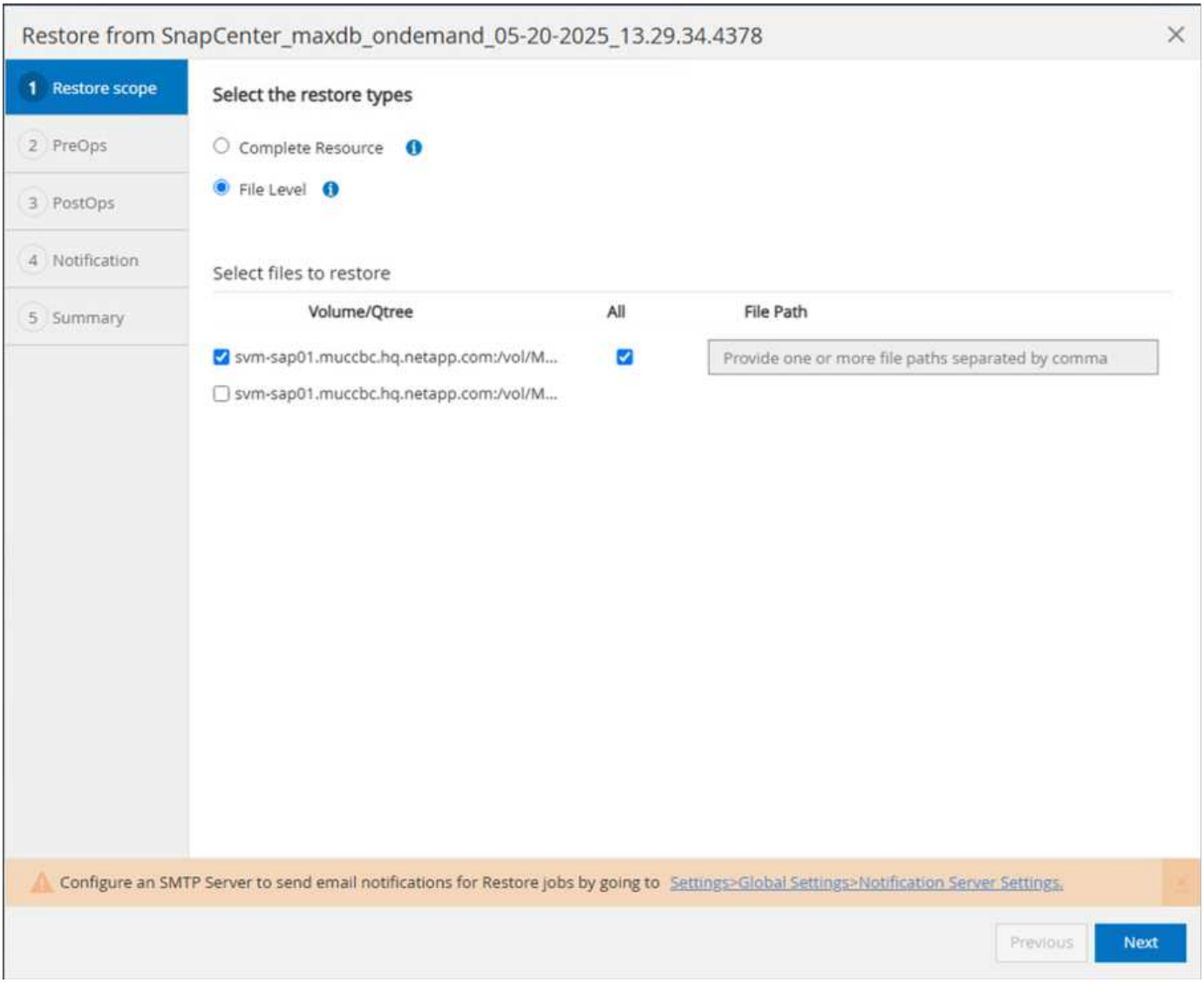
ユーザインターフェイスのスクリーンショット"]

[Complete Resource]を選択すると、Volume Based Snap Restore（VBSR）が実行されます。Azure内ではと呼ばれます"ボリュームのリバート"。ANF導入の場合*完全なリソースのみが提供されます*。

**Important**

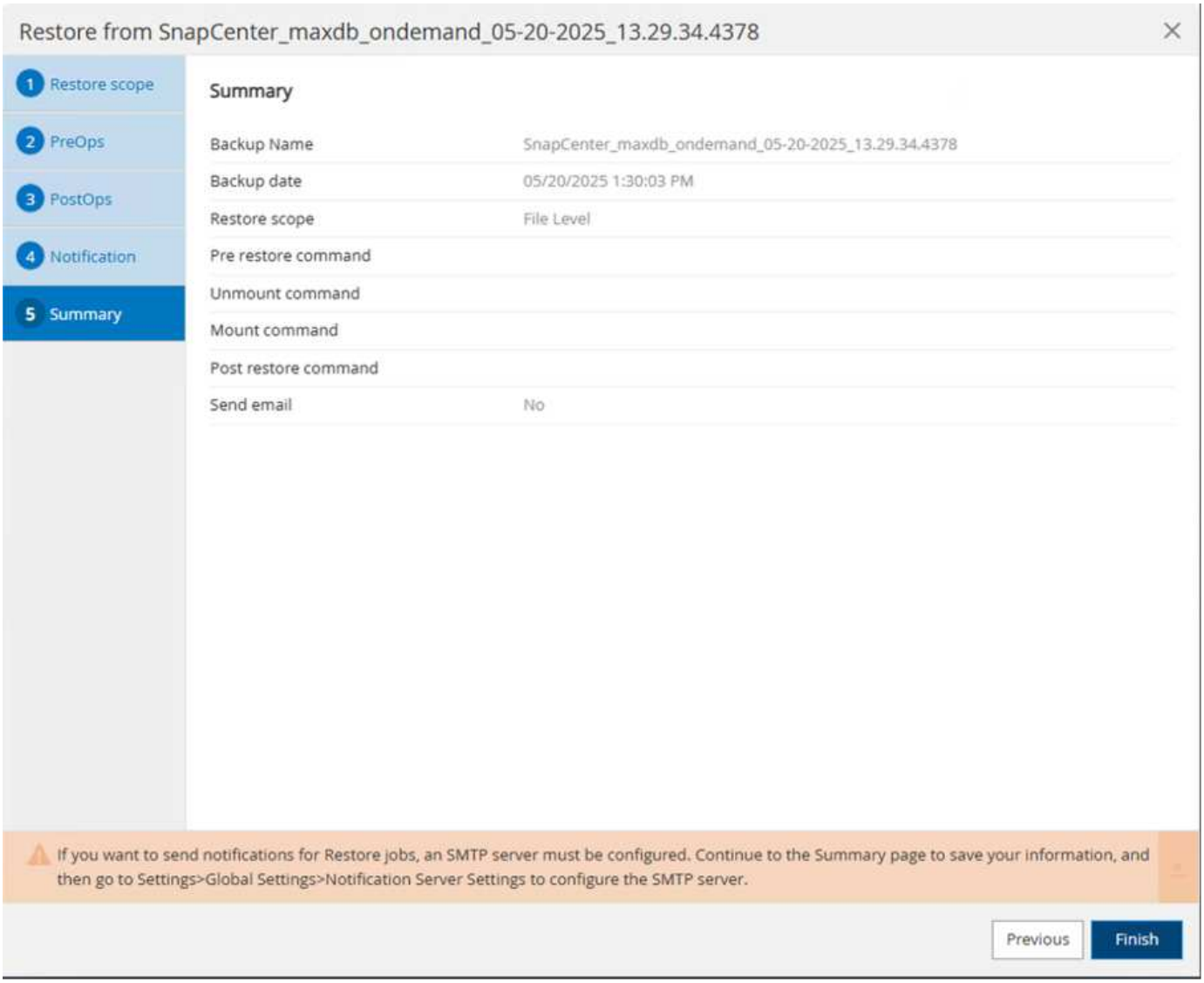
Active filesystem data and snapshots that were taken after the selected snapshot will be lost. The snapshot revert operation will replace *all* the data in the targeted volume with the data in the selected snapshot. You should pay attention to the snapshot contents and creation date when you select a snapshot. You cannot undo the snapshot revert operation.

その他のタイプの導入（オンプレミスANFなど）では、Single File Snap Restore（SFSR）処理をオーケストレーションできます。[File Level]と[According Volume]を選択し、[All]にチェックマークを付けます。次のスクリーンショットを参照してください。



ユーザインターフェイスのスクリーンショット"]

概要が表示され、[Finish]をクリックすると、実際のリストアが開始されます。



ユーザインターフェイスのスクリーンショット"]

- ファイルシステムのマウント（sap-lnx25）
  - ユーザルート：mount /sapdb/m02/sapdata
- データベースM02を管理者モードで起動し、接続します。
  - ユーザ：sqdm02：dbmcli -d m02 -uコントロール、<password>
    - db_admin
    - DB_CONNECT
- バックアップ情報の収集
  - backup_history_open
  - backup_history_list -cラベル、アクション、ページ、停止、メディア-r last

```
dbmcli on M02>backup_history_list -c label,action,pages,stop,media -r last
OK
END
DAT_000000008|SAVE WARM|         0|2025-05-20 13:29:50|M02_SNAP

---
```

- データベースをリカバリ
  - データバックアップのリカバリ
    - RECOVER_START M02_SNAP DATA ExternalBackupID DAT_000000008

```
dbmcli on M02>recover_start M02_SNAP data ExternalBackupID DAT_000000008
OK
Returncode              0
Date                    20250520
Time                    00151550
Server                  sap-lnx25
Database                M02
Kernel Version          Kernel    7.9.10   Build 004-123-265-969
Pages Transferred       0
Pages Left
Volumes
Medianame               M02_SNAP
Location
Errortext
Label                   DAT_000000008
Is Consistent           true
First LOG Page          512226
Last LOG Page
DB Stamp 1 Date         20250520
DB Stamp 1 Time         00132933
DB Stamp 2 Date
DB Stamp 2 Time
Page Count
Devices Used            0
Database ID             sap-lnx25:M02_20241203_104036
Max Used Data Page      3187892
Converter Page Count

---
```

  - 必要に応じてログバックアップをリカバリ
    - 例：RECOVER_START M02_LOG LOG 147

```
dbmcli on M02>recover_start M02_LOG LOG 147
OK
Returncode              0
Date                    20250521
Time                    00112001
Server                  sap-lnx25
Database                M02
Kernel Version          Kernel    7.9.10   Build 004-123-265-969
Pages Transferred       24
Pages Left              0
Volumes                 1
Medianame               M02_LOG
Location                /sapdb/M02/backup/log/M02_LOG.147
Errortext
Label                   LOG_000000147
Is Consistent
First LOG Page          514072
Last LOG Page           514075
DB Stamp 1 Date         20250520
DB Stamp 1 Time         00180238
DB Stamp 2 Date         20250520
DB Stamp 2 Time         00180539
Page Count              4
Devices Used            1
Database ID             sap-lnx25:M02_20241203_104036
Max Used Data Page
Converter Page Count
```

- オプション情報–特定のタイムスタンプに自動リカバリします（専用のデータ/ログバックを指定する必要はありません）。
  - 例：20250520 200000までの自動リカバリ

```
---
dbmcli on M02>autorecover until 20250520 200000
OK
Returncode              0
Date                    20250521
Time                    00131559
Server                  sap-lnx25
Database                M02
Kernel Version          Kernel    7.9.10   Build 004-123-265-969
Pages Transferred       10096
Pages Left              0
Volumes                 1
Medianame               M02_LOG
Location                /sapdb/M02/backup/log/M02_LOG.102
Errortext
Label                   LOG_000000102
Is Consistent
First LOG Page          256227
Last LOG Page           341559
DB Stamp 1 Date         20241203
DB Stamp 1 Time         00190348
DB Stamp 2 Date         20241226
DB Stamp 2 Time         00193615
Page Count              85333
Devices Used            1
Database ID             sap-lnx25:M02_20241203_104036
Max Used Data Page
Converter Page Count

---
```

- リカバリを終了してデータベースを停止

- DB_OFFLINE

  リカバリの詳細については、"MaxDBのマニュアル"

- SAPシステムの起動
  - ユーザroot：/etc/init.d/sapinit start
  - ユーザm02adm：startsap

## 追加情報とバージョン履歴

### デモの録画

ドキュメントをサポートするために、次の記録済みデモを利用できます。

MaxDBプラグインのインストール、MaxDBプラグインの設定、MaxDBデータベースのバックアップ

MaxDBデータベースのリストアとリカバリ

### 外部ドキュメント

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。

- "ANFでのAzureのSAPインストール"
- "SnapCenterプラグインの前提条件"
- "SnapCenterインストールプラグイン"
- "MaxDBリカバリのマニュアル"
- SAP Notes（ログインが必要）
  - "1928060 -ファイルシステムのバックアップを使用したデータのバックアップとリカバリ"
  - "2282054 -バックグラウンドDBMサーバ"
  - "616814 -スプリット・ミラーまたはスナップショットのログ・ライターを中断します"
- "HOWTO - Database Manager CLIによるSAP MaxDBバックアップ"
- "HOWTO - Database Manager CLIを使用したSAP MaxDBリカバリ"
- "ネットアップの製品マニュアル"
- "NetApp SAPソリューション–ユースケース、ベストプラクティス、メリットに関する情報"

### バージョン履歴

| * バージョン * | * 日付 * | ドキュメントバージョン履歴 |
| --- | --- | --- |
| バージョン 1.0 以降 | 2025年5月 | 初期バージョン–バックアップ/リカバリMaxDBデータベース |

# ライフサイクル管理

## Ansibleを使用したNetApp SAP Landscape Managementの統合

### TR-4953：『NetApp SAP Landscape Management Integration using Ansible』

SAP Landscape Management（LaMa）を使用すると、SAPシステム管理者は、SAPシステムのエンドツーエンドのクローニング、コピー、更新などのSAPシステム運用を自動化できます。

著者：Michael Schlosser、Nils Bauer、NetApp

ネットアップは、SAP LaMa対応の各種Ansibleモジュールを搭載しており、SAP LaMaのAutomation Studioを通じて、NetApp SnapshotやFlexCloneなどのテクノロジにアクセスできます。これらのテクノロジを使用することで、SAPシステムのクローニング、コピー、更新の処理を簡易化、高速化できます。

この統合は、ネットアップのストレージソリューションをオンプレミスで運用しているお客様や、Amazon Web Services、Microsoft Azure、Google Cloud Platformなどのパブリッククラウドプロバイダでネットアップのストレージサービスを使用しているお客様が利用できます。

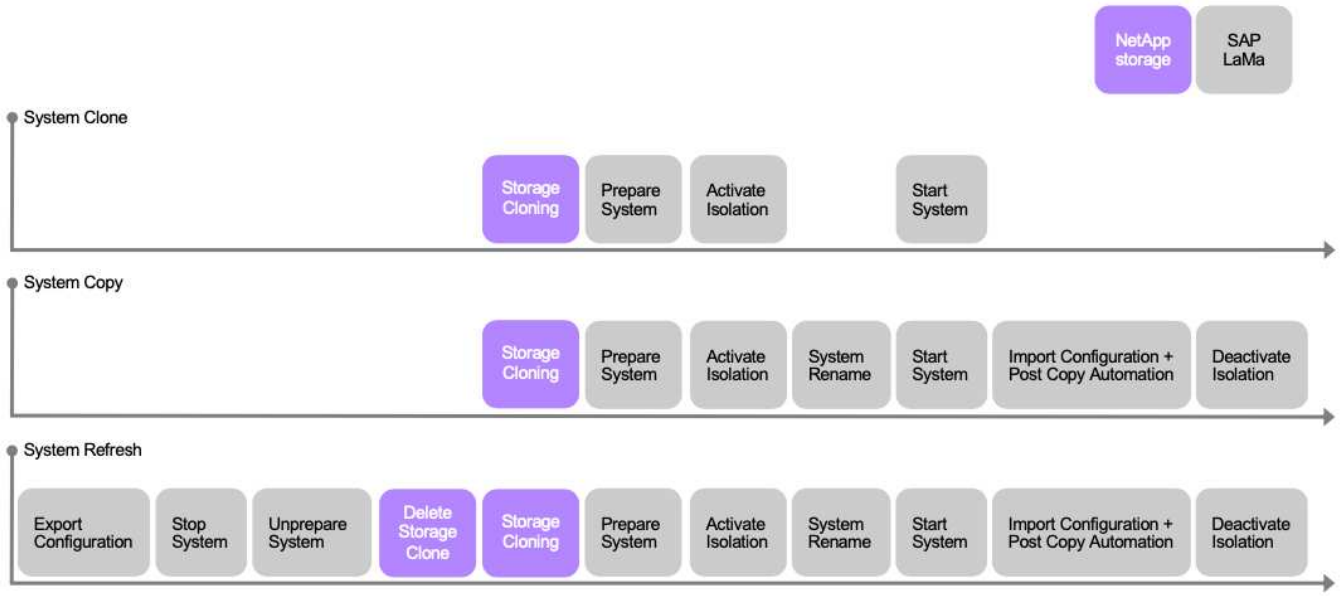
このドキュメントでは、Ansibleによる自動化を使用して、SAPシステムのコピー、クローニング、更新の処理に対応するネットアップのストレージ機能を利用したSAP LaMaの設定について説明します。

### SAPシステムのクローニング、コピー、更新のシナリオ

SAPシステムのコピーという用語は、SAPシステムのクローニング、SAPシステムのコピー、SAPシステムの更新の3つのプロセスを表す同義語としてよく使用されます。ワークフローとユースケースはそれぞれ異なるため、異なる処理を区別することが重要です。

- * SAPシステムのクローン。* SAPシステムのクローンは、ソースSAPシステムの同一クローンです。SAPシステムクローンは、一般に論理的な破損に対処したり、ディザスタリカバリのシナリオをテストしたりするのに使用されます。システムのクローニング処理では、ホスト名、インスタンス番号、およびSIDの値は変更されません。そのため、本番環境と通信できないように、ターゲットシステムの適切なネットワークフェンシングを設定することが重要です。
- * SAPシステムのコピー。* SAPシステムのコピーとは、ソースSAPシステムのデータを含む新しいターゲットSAPシステムのセットアップを指します。たとえば、本番用システムのデータを含む追加のテストシステムを新しいターゲットシステムとして使用できます。ソース・システムとターゲット・システムでは、ホスト名、インスタンス番号、およびSIDが異なります。
- * SAPシステムの更新。* SAPシステムの更新は、ソースSAPシステムのデータを使用した既存のターゲットSAPシステムの更新です。ターゲットシステムは、通常、品質管理システムなどのSAP転送環境の一部であり、本番用システムのデータで更新されます。ソース・システムとターゲット・システムでは、ホスト名、インスタンス番号、およびSIDが異なります。

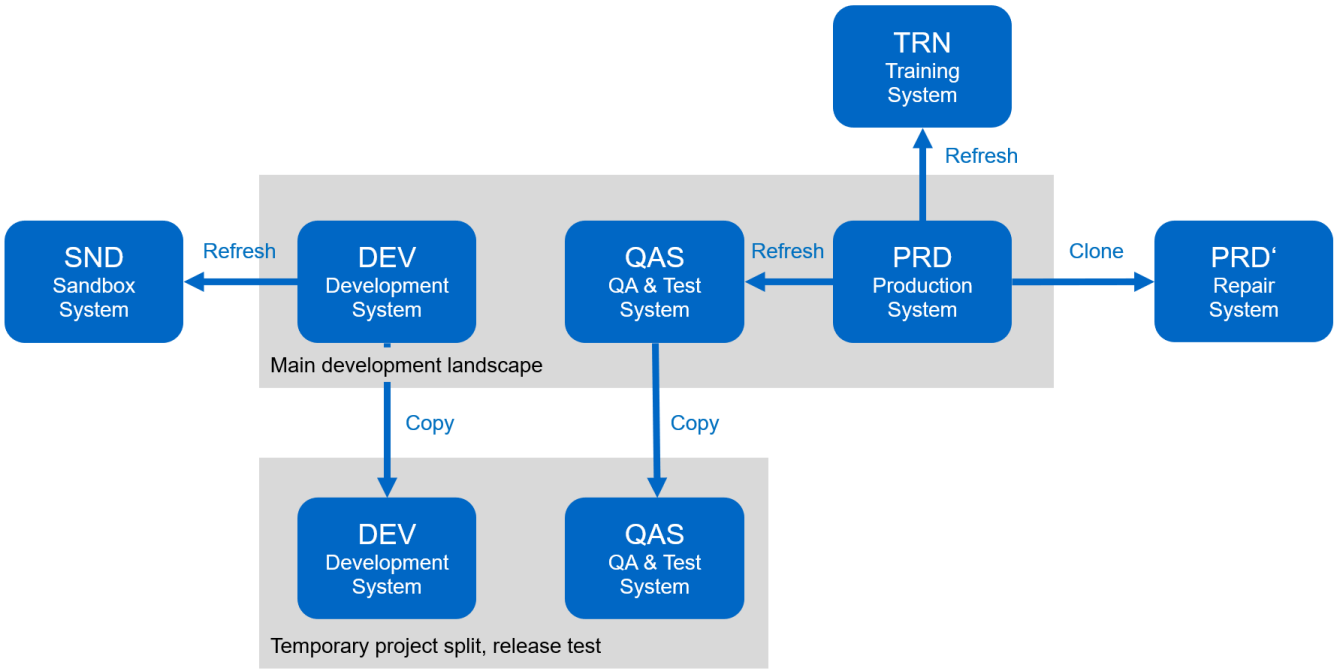
次の図に、システムのクローン、システムのコピー、またはシステムの更新の各処理で実行する必要がある主な手順を示します。紫のボックスは、ネットアップストレージ機能を統合できる手順を示しています。3つの運用はすべて、SAP LaMaを使って完全に自動化できます。




## システムの更新、コピー、クローニングのユースケース

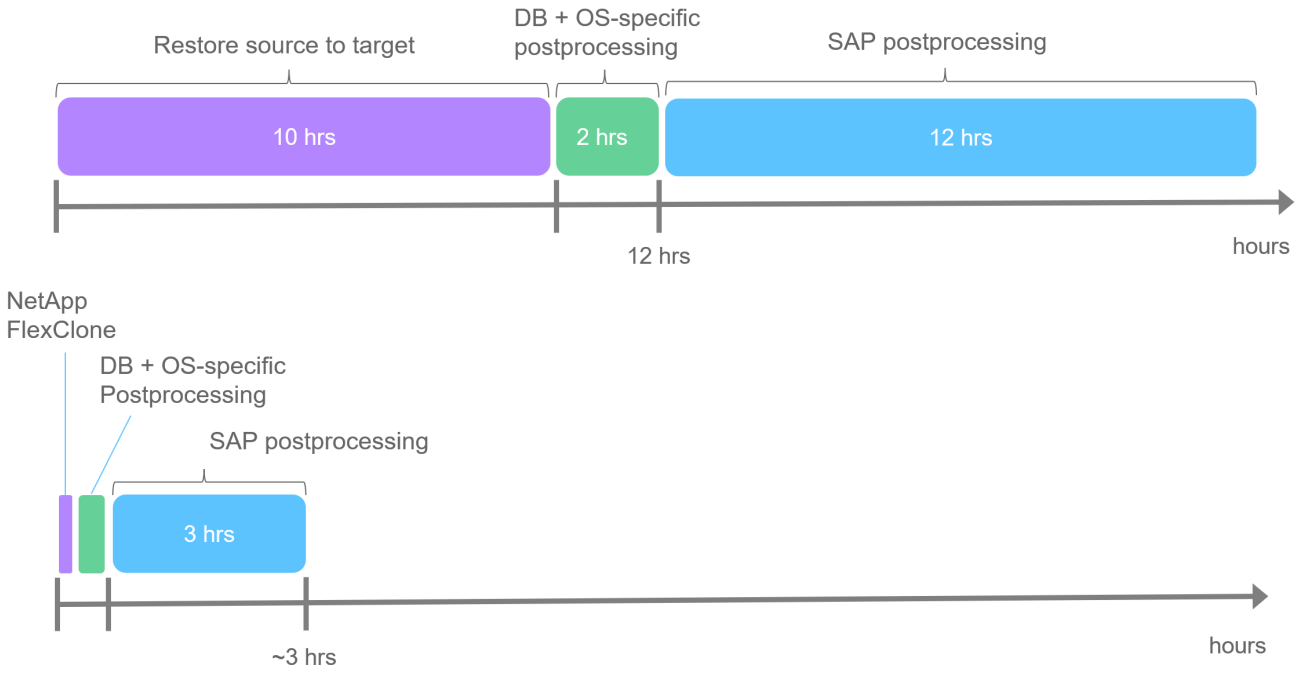
テストやトレーニングの目的で、ソースシステムのデータをターゲットシステムで使用できるようにする必要があるシナリオは複数あります。テストおよびトレーニング用のシステムは、ソースシステムのデータで定期的に更新し、現在のデータセットでテストとトレーニングが実行されていることを確認する必要があります。

このシステム更新処理は、インフラ、データベース、アプリケーションの各レイヤ上で実行される複数のタスクで構成されます。自動化のレベルによっては、数日かかる場合があります。




SAP LaMaとネットアップのクローニングワークフローを使って、インフラレイヤとデータベースレイヤで必

要なタスクを高速化し、自動化できます。SAP LaMaは、バックアップをソースシステムからターゲットシステムにリストアする代わりに、NetApp SnapshotコピーとNetApp FlexCloneテクノロジを使用して、起動したHANAデータベースまでの必要なタスクを、次の図に示すように数時間ではなく数分で実行します。クローニングプロセスに要する時間はデータベースのサイズに左右されないため、非常に大規模なシステムでも数分で作成できます。また、オペレーティングシステムとデータベースレイヤ、およびSAPの後処理側でタスクを自動化することにより、ランタイムをさらに削減できます。




論理的破損に対処する

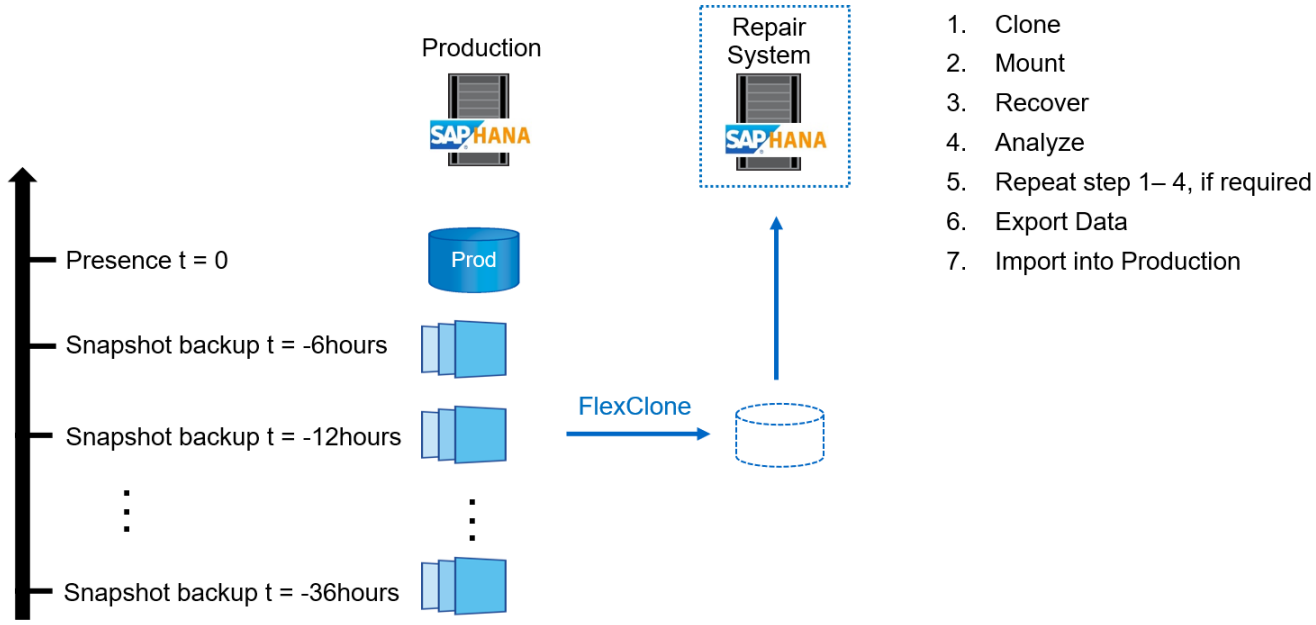
論理的破損は、ソフトウェアエラー、人為的エラー、破壊行為などが原因で発生する可能性があります。残念ながら、論理的破損は、標準的な高可用性ソリューションやディザスタリカバリソリューションでは対処できないことがよくあります。その結果、論理的な破損が発生したレイヤ、アプリケーション、ファイルシステム、またはストレージによっては、ダウンタイムを最小限に抑え、データ損失要件を許容できる範囲で満たすことができない場合があります。

最悪のケースは、SAPアプリケーションが論理的に破損した場合です。SAP アプリケーションは多くの場合、異なるアプリケーションが相互に通信してデータを交換する環境で動作します。このため、論理的な破損が発生した SAP システムはリストアとリカバリを実行しないことを推奨します。破損が発生する前の時点にシステムをリストアすると、データが失われます。また、 SAP ランドスケープは同期されず、さらにポストプロセスが必要になります。

SAPシステムをリストアする代わりに、別の修復システムで問題を分析して、システム内の論理エラーを修正する方法を推奨します。ルート原因分析には、ビジネスプロセスやアプリケーション所有者の関与が必要です。このシナリオでは、論理的破損が発生する前に格納されたデータに基づいて、修復システム（本番用システムのクローン）を作成します。リペアシステム内では、必要なデータをエクスポートし、本番システムにインポートできます。このアプローチでは、本番用システムを停止する必要はなく、最良のシナリオでは、データの損失だけでなく、ごくわずかなデータの損失も発生します。

リペアシステムを設定する際には、柔軟性とスピードが不可欠です。ネットアップのストレージベースのSnapshotバックアップでは、複数の整合性のあるデータベースイメージを使用し、NetApp FlexCloneテクノロジを使用して本番用システムのクローンを作成できます。ファイルベースのバックアップからリダイレク

トされたリストアを使用して修復システムを設定する場合、FlexCloneボリュームは数時間ではなく数秒で作成できます。

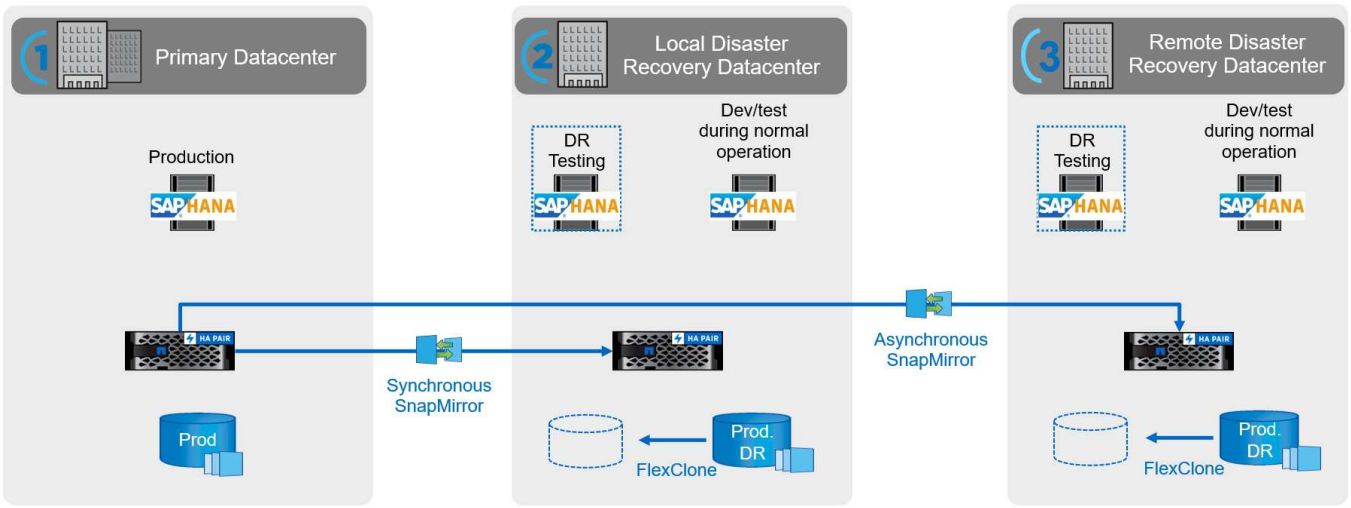



ディザスタリカバリのテスト

効果的なディザスタリカバリ戦略を策定するには、必要なワークフローをテストする必要がテストでは、戦略が機能するかどうか、および内部ドキュメントで十分かどうかを検証します。また、管理者は必要な手順をトレーニングできます。

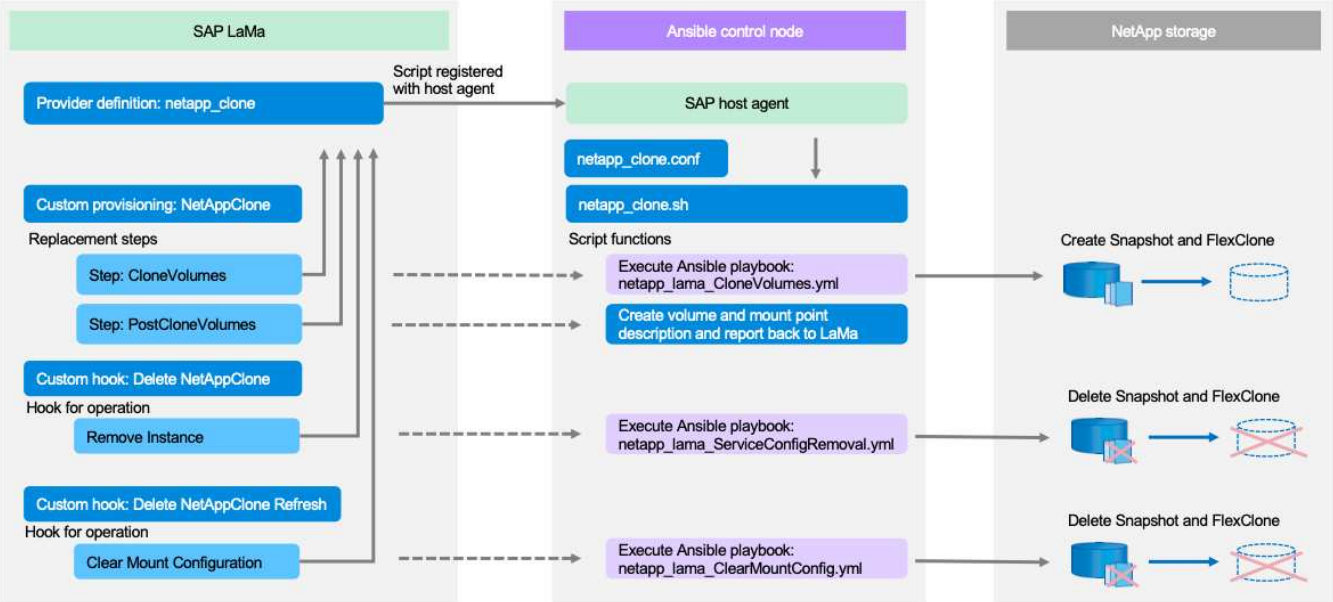
SnapMirrorを使用したストレージレプリケーションでは、RTOとRPOをリスクにさらすことなく、ディザスタリカバリのテストを実行できます。ディザスタリカバリテストは、データレプリケーションを中断することなく実行できます。非同期SnapMirrorと同期SnapMirrorのディザスタリカバリテストでは、ディザスタリカバリターゲットでSnapshotバックアップとFlexCloneボリュームを使用します。

SAP LaMaは、テスト手順 全体のオーケストレーションに使用でき、ネットワークの遮断やホストのメンテナンスなどにも対応します。



## Ansibleを使用して、NetApp SAP LaMaを統合

この統合アプローチでは、SAP LaMaのカスタムプロビジョニングと運用のフックを、ネットアップストレージ管理のAnsibleプレイブックと組み合わせて使用します。次の図は、LaMa側の設定の概要と、実装例の対応するコンポーネントを示しています。




Ansible制御ノードとして機能する中央ホストは、SAP LaMaからの要求を実行し、Ansibleプレイブックを使用してネットアップストレージの運用を開始するために使用されます。ホストをSAP LaMaへの通信ゲートウェイとして使用できるように、SAPホストエージェントコンポーネントをこのホストにインストールする必要があります。

LaMa Automation Studioでは、AnsibleホストのSAPホストエージェントに登録されたプロバイダが定義されます。ホストエージェント構成ファイルは、要求された処理に応じて、一連のコマンドラインパラメータを使用してSAP LaMaによって呼び出されるシェルスクリプトを指します。

LaMa Automation Studioでは、カスタムプロビジョニングとカスタムフックを定義して、プロビジョニング時にストレージのクローニング処理を実行し、システムがプロビジョニング解除されたときにクリーンアップ処理を実行します。その後、Ansible制御ノード上のシェルスクリプトによって、対応するAnsibleプレイブックが実行されます。これにより、SnapshotとFlexCloneの処理およびプロビジョニング解除ワークフローを使用したクローンの削除がトリガーされます。

NetApp AnsibleモジュールとLaMaプロバイダの定義の詳細については、以下をご覧ください。

- "NetApp Ansibleモジュール"
- "SAP LaMaのドキュメント-プロバイダ定義"

## 実装例

システムとストレージのセットアップでは多数のオプションを使用できるため、システムの個 々 のセットアップと設定の要件をテンプレートとして使用する必要があります。

このサンプルスクリプトは現状のまま提供されており、ネットアップではサポートしていません。スクリプトの最新バージョンは、mailto：ng-sapcc@netapp.com [ng-sapcc@netapp.com ^]にEメールでリクエストできます。

検証済みの構成と制限事項

以下の原則はサンプル導入に適用されており、お客様のニーズに合わせて調整する必要がある場合があります。

- マネージドSAPシステムは、NFSを使用してネットアップストレージボリュームにアクセスし、アダプティブデザインの原則に基づいてセットアップしました。
- NetApp Ansibleモジュール（ZAPIとREST API）でサポートされているすべてのONTAP リリースを使用できます。
- 1つのネットアップクラスタとSVMのクレデンシャルが、プロバイダスクリプトの変数としてハードコードされました。
- ストレージクローニングは、ソースSAPシステムで使用されていたのと同じストレージシステムで実行しました。
- ターゲットのSAPシステムのストレージボリュームの名前は、付録のソースと同じです。
- セカンダリストレージ（SV / SM）でのクローニングは実装されていません。
- FlexCloneスプリットを実装できませんでした。
- インスタンス番号は、ソースとターゲットのSAPシステムで同じです。

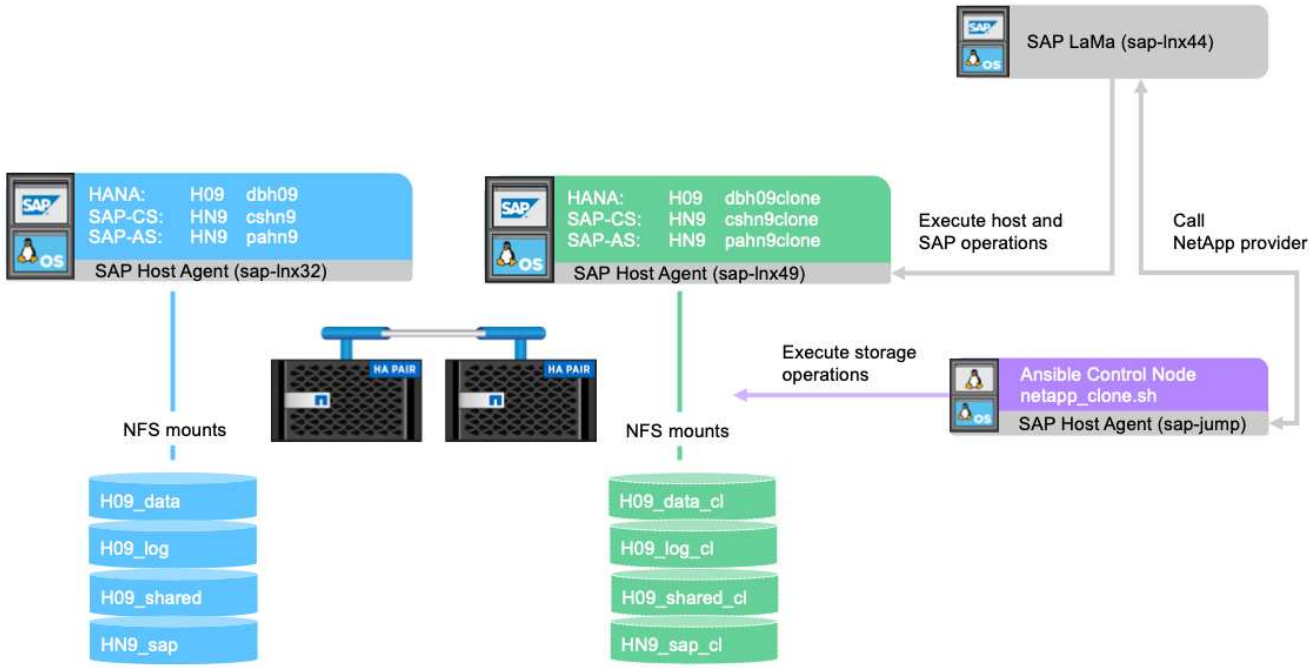
ラボのセットアップ

次の図は、ラボのセットアップを示しています。システムのクローニングに使用されるソースのSAPシステムHN9では、データベースH09、SAP CS、およびSAP ASサービスが、がインストールされた同じホスト（sap-lnx32）で実行されています "アダプティブデザイン" 有効。に従ってAnsibleコントロールノードが準備されました "NetApp ONTAP 向けのAnsibleプレイブック" ドキュメント

SAPホストエージェントもこのホストにインストールされています。NetAppプロバイダスクリプトとAnsibleプレイブックは、Ansibleコントロールノードで設定しました（を参照）。"「付録：プロバイダスクリプトの設定」"

ホスト `sap-lnx49` SAP LaMaクローニング運用のターゲットとして使用し、隔離に対応した機能を設定しました。

システムのコピーおよび更新には、さまざまなSAPシステム（ソースとしてHNA、ターゲットとしてHN2）が使用されました。これは、Post Copy Automation（PCA）が有効になっているためです。



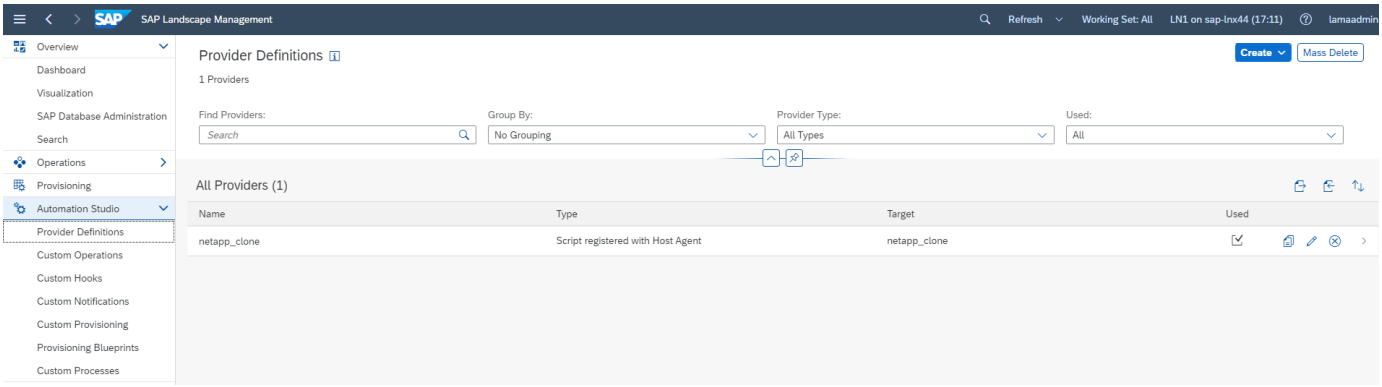

ラボ環境では、次のソフトウェアリリースを使用しました。

- SAP LaMa Enterprise Edition 3.00 SP23_2
- SAP HANA 2.00.052.00.1599235305
- SAP 7.77パッチ27（S/4 HANA 1909）
- SAPホストエージェント7.22パッチ56
- SAPACEXT 7.22パッチ69
- Linux SLES 15 SP2
- Ansible 2.13.7.
- NetApp ONTAP 9.8P8

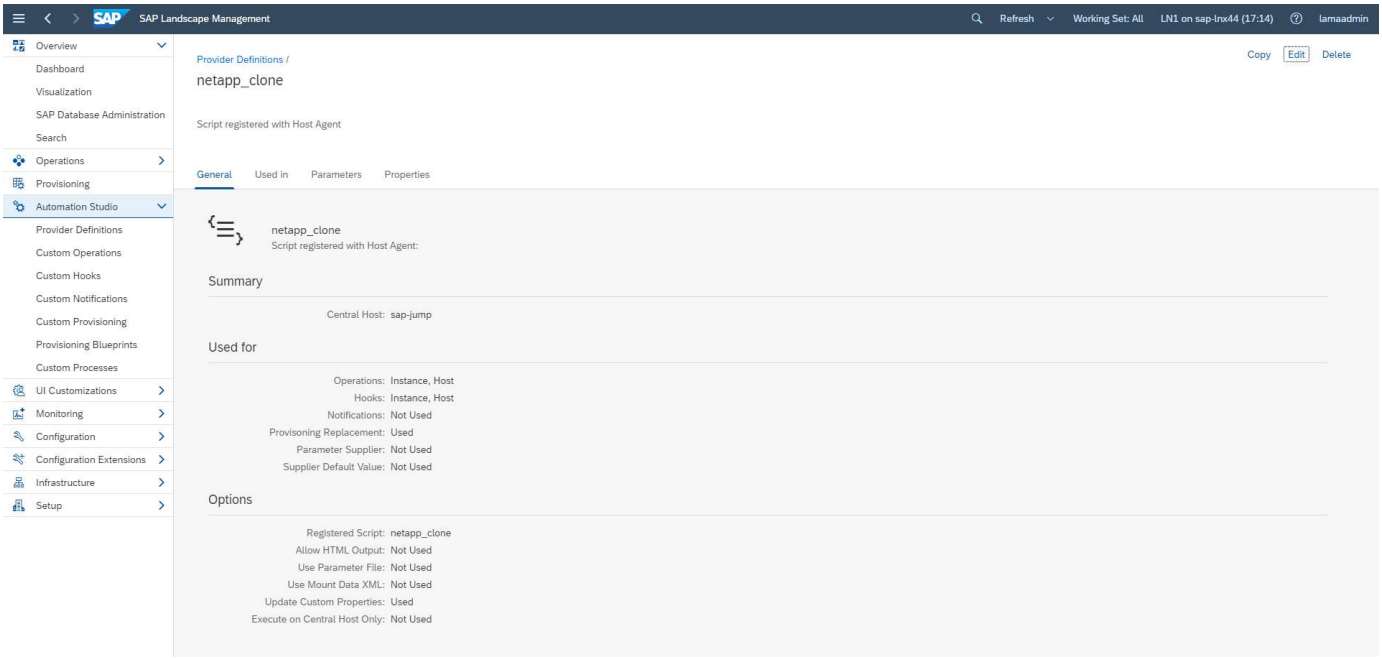
## SAP LaMa設定

#### SAP LaMaプロバイダによる定義

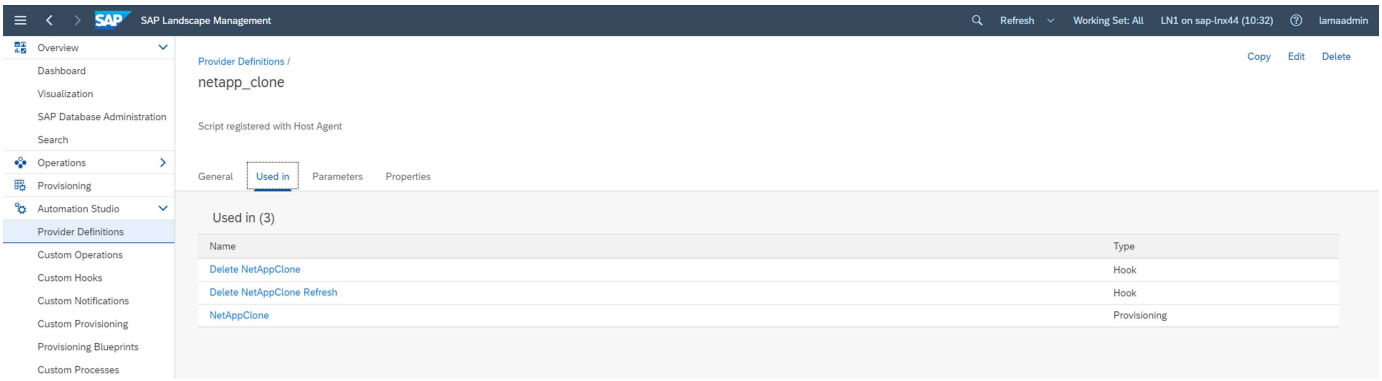
プロバイダの定義は、次のスクリーンショットに示すように、SAP LaMaのAutomation Studio内で実行されます。この例の実装では、前に説明したように、異なるカスタムプロビジョニングステップと操作フックに使用される単一のプロバイダ定義を使用します。



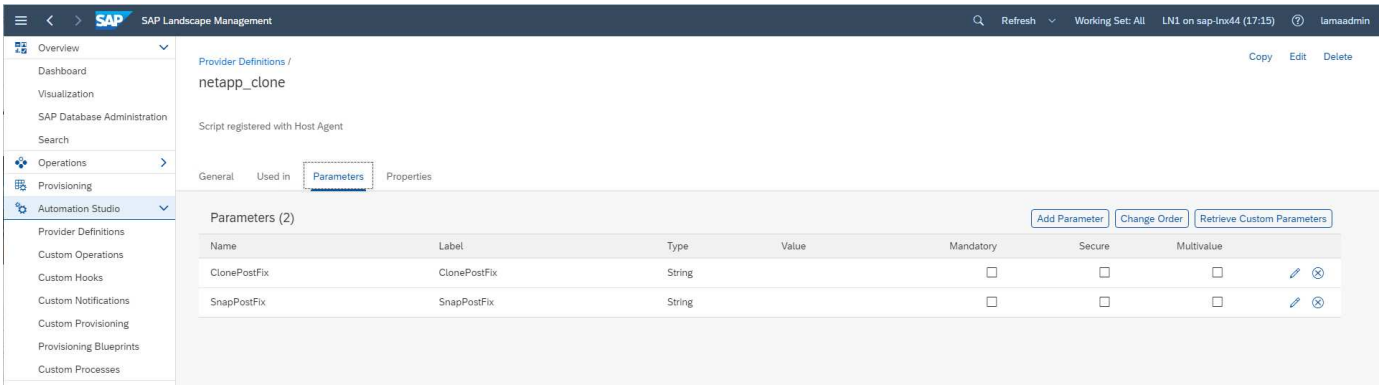

プロバイダ `netapp_clone` スクリプトとして定義されます `netapp_clone.sh` SAPホストエージェントに登録されている。SAPホストエージェントは、中央のホストで実行されます `sap-jump`Ansibleコントロールノードとしても機能します。




[で使用（ Used in ）]タブには、プロバイダーが使用されるカスタムオペレーションが表示されます。カスタムプロビジョニング NetAppClone およびカスタムフック Delete NetAppClone および Delete NetAppClone Refresh *の構成は、次の章で説明します。

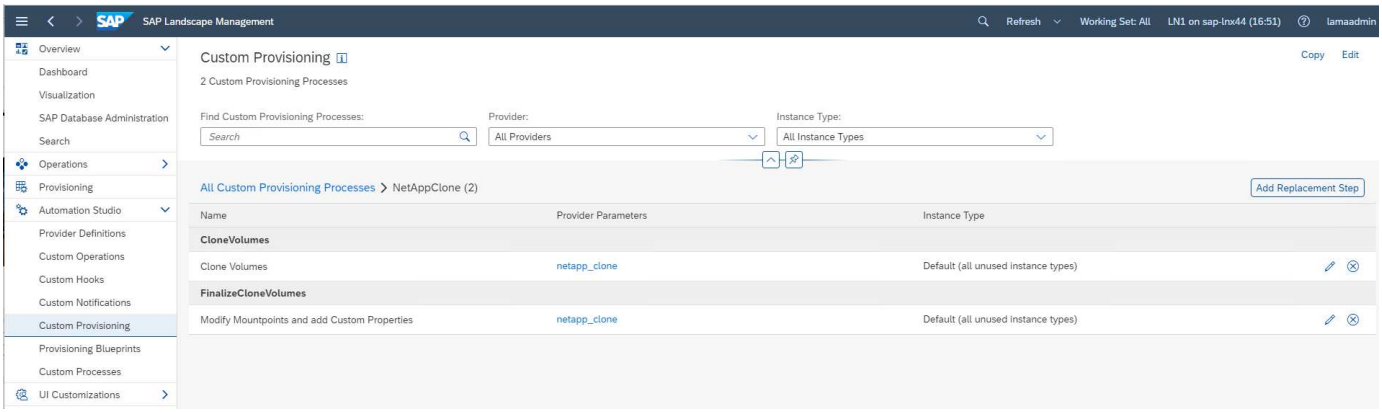



プロビジョニングワークフローの実行中にパラメータ* ClonePostFix および SnapPostFix *が要求され、SnapshotとFlexCloneボリュームの名前に使用されます。



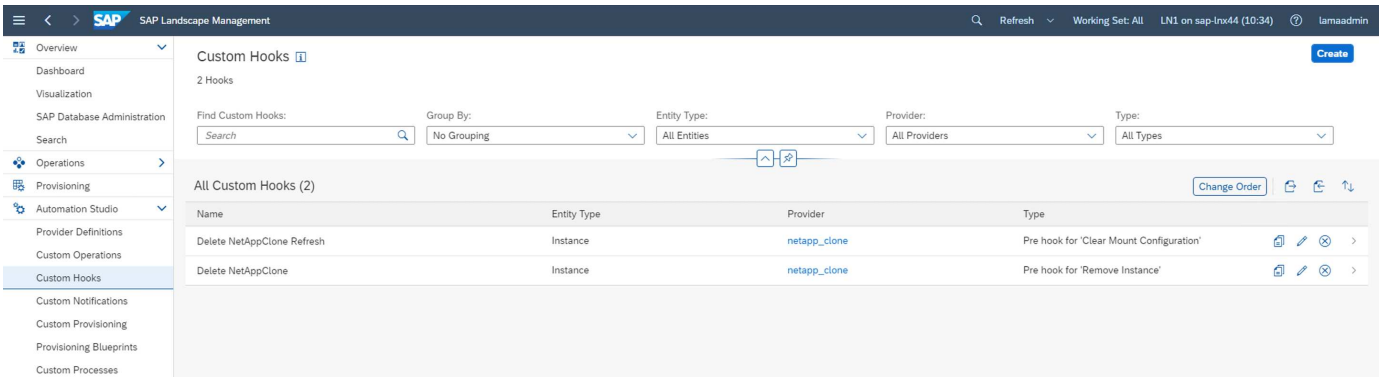

**SAP LaMa**カスタムプロビジョニング

SAP LaMaのカスタムプロビジョニング設定で、前述したお客様のプロバイダを使用して、プロビジョニングワークフローの手順* Clone Volumes と PostCloneVolumes *を置き換えます。

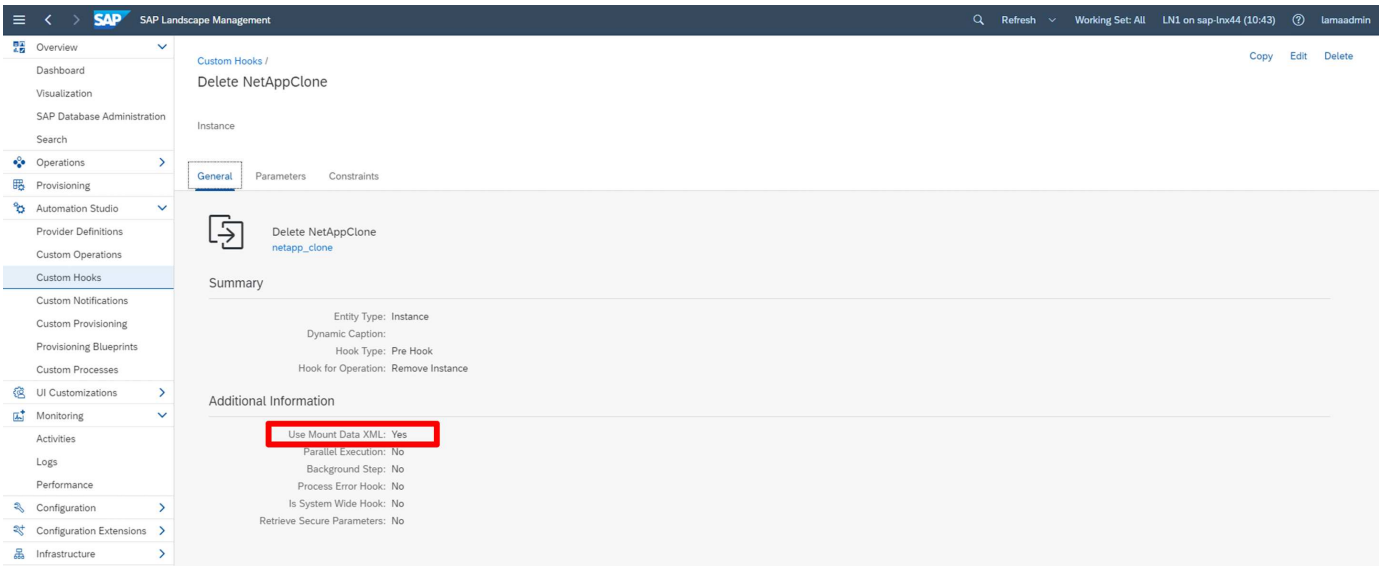



**SAP LaMa**カスタムフック

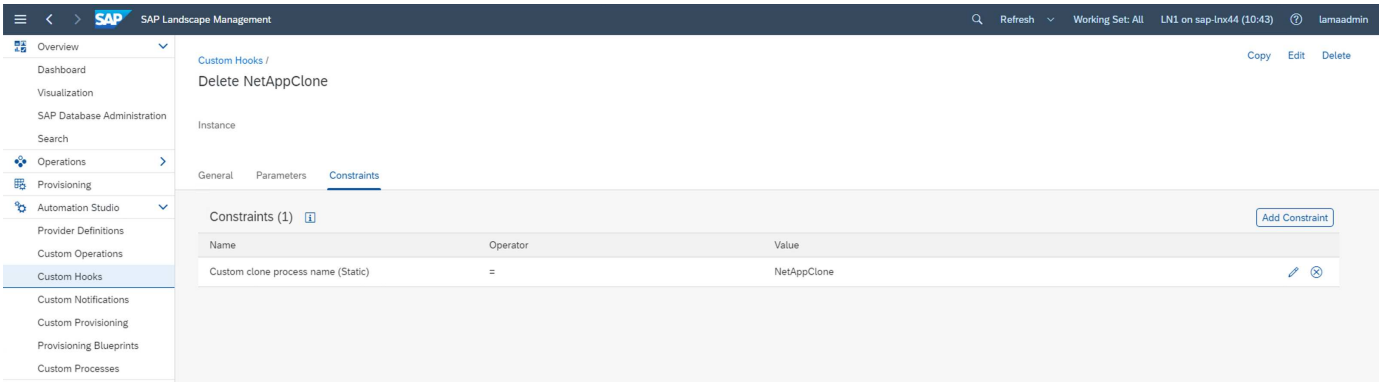
システムの削除ワークフロー時にシステムを削除した場合は、フック* Delete NetAppClone を使用してプロバイダ定義が呼び出されます **`netapp_clone`**。インスタンスは実行中も保持されるため、システムの更新ワークフロー中は Delete NetApp Clone Refresh *フックが使用されます。




SAP LaMaがマウントポイント設定の情報をプロバイダに提供できるように、カスタムフックに「データマウントXML *を使用」を設定することが重要です。



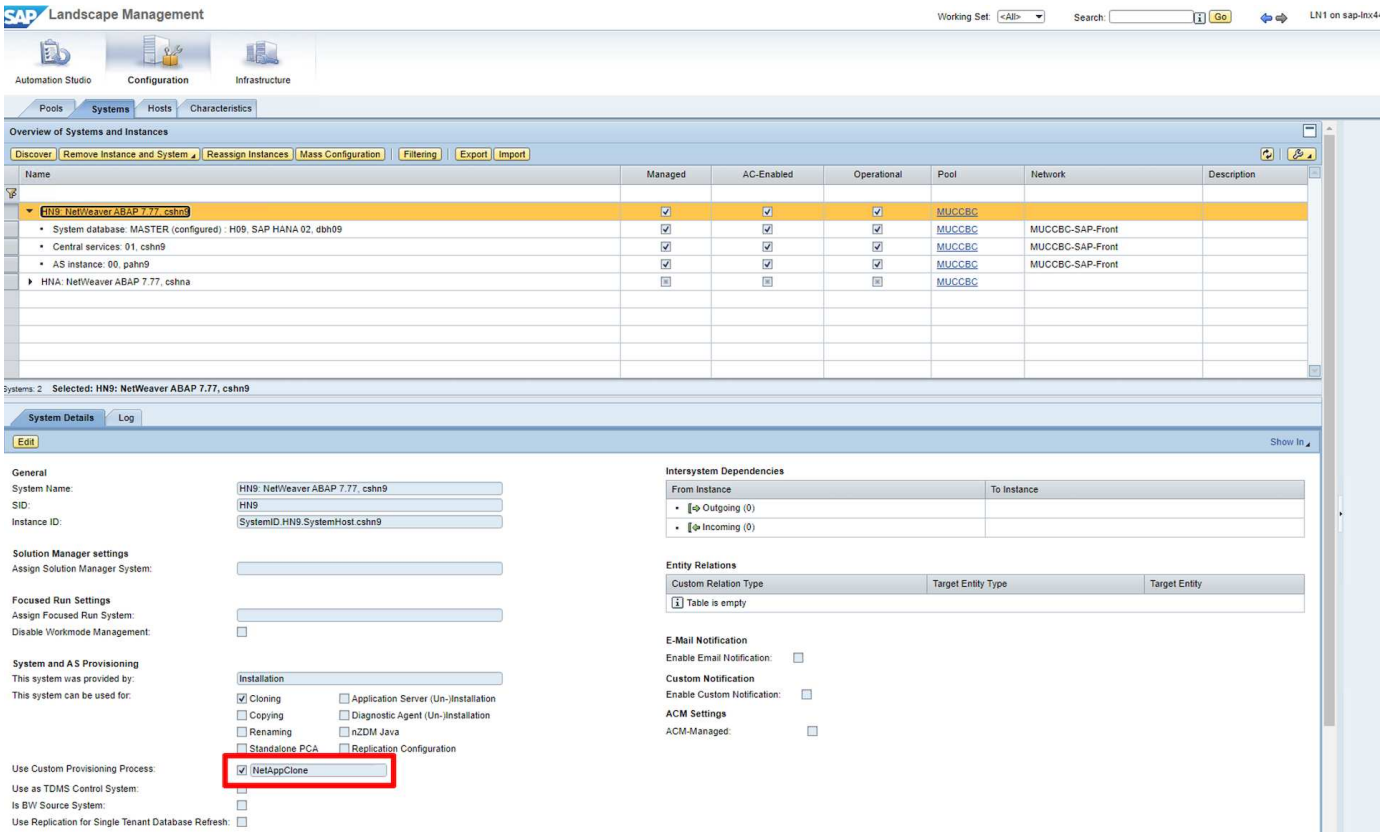

カスタムプロビジョニングワークフローを使用してシステムを作成したときにのみカスタムフックが使用および実行されるようにするために、次の制約がそのフックに追加されます。




カスタムフックの使用方法の詳細については、を参照してください "SAP LaMaのドキュメント"。

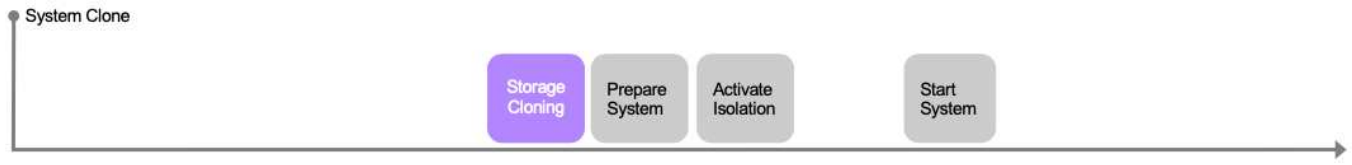
**SAP**ソースシステムでカスタムのプロビジョニングワークフローを有効にします

ソースシステムのカスタムプロビジョニングワークフローを有効にするには、その設定を該当するものにする必要があります。[カスタムプロビジョニングプロセスを使用する*]チェックボックスをオンにして、対応するカスタムプロビジョニング定義を選択する必要があります。

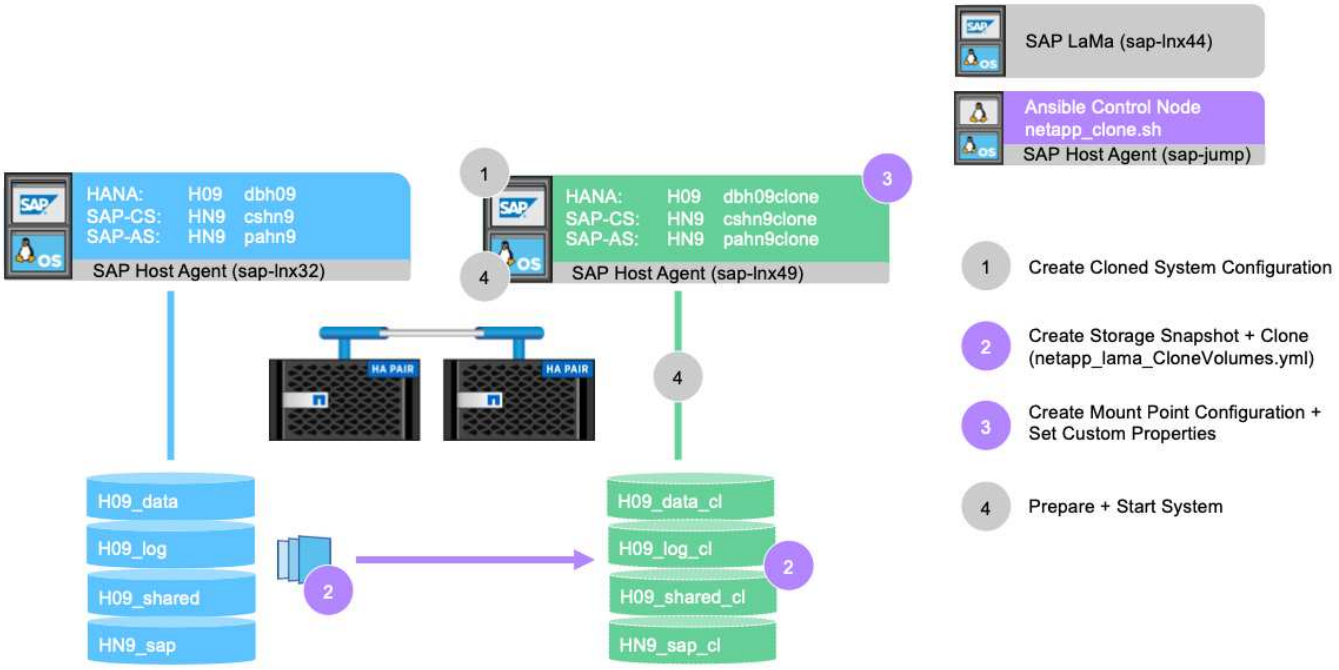



## SAP LaMaプロビジョニングワークフロー-クローンシステム

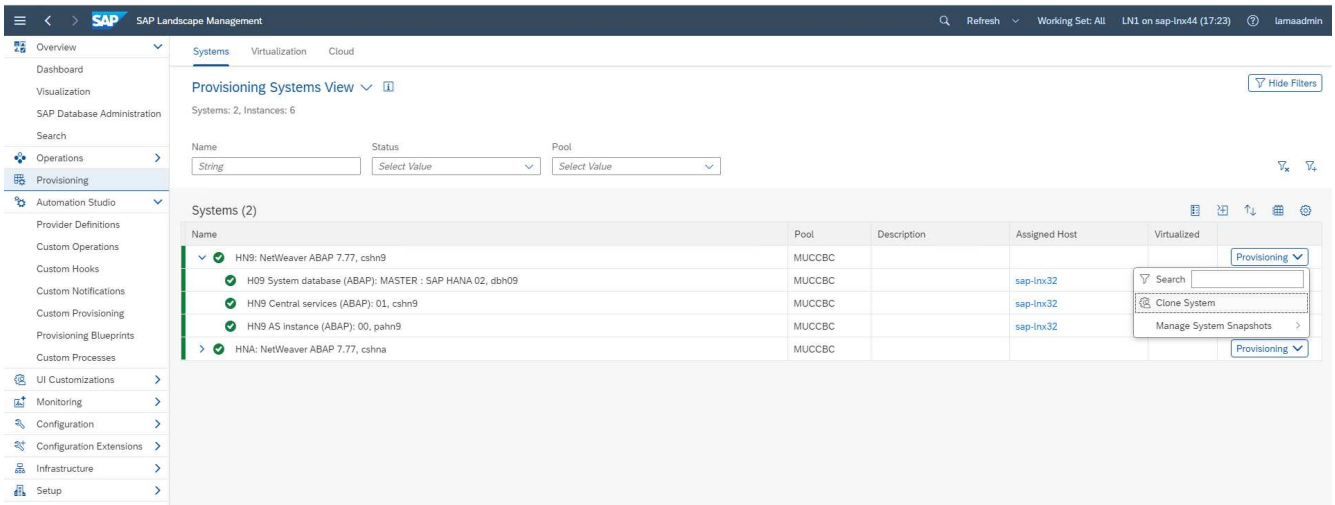
次の図は、システムのクローニングワークフローで実行する主な手順を示しています。



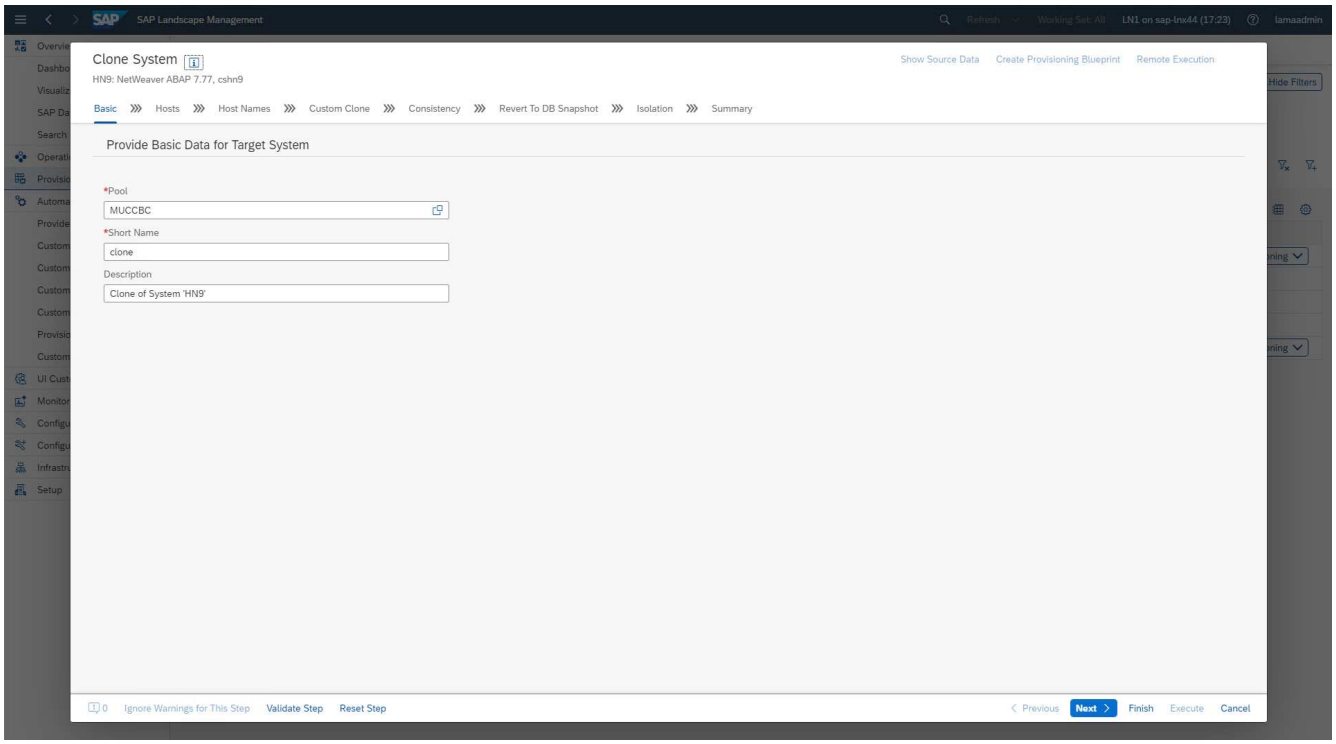

このセクションでは、HANAデータベースH09を使用するソースのSAPシステムHN9に基づく、SAP LaMaシステムの完全なクローニングワークフローを紹介します。次の図は、ワークフロー中に実行される手順の概要を示しています。



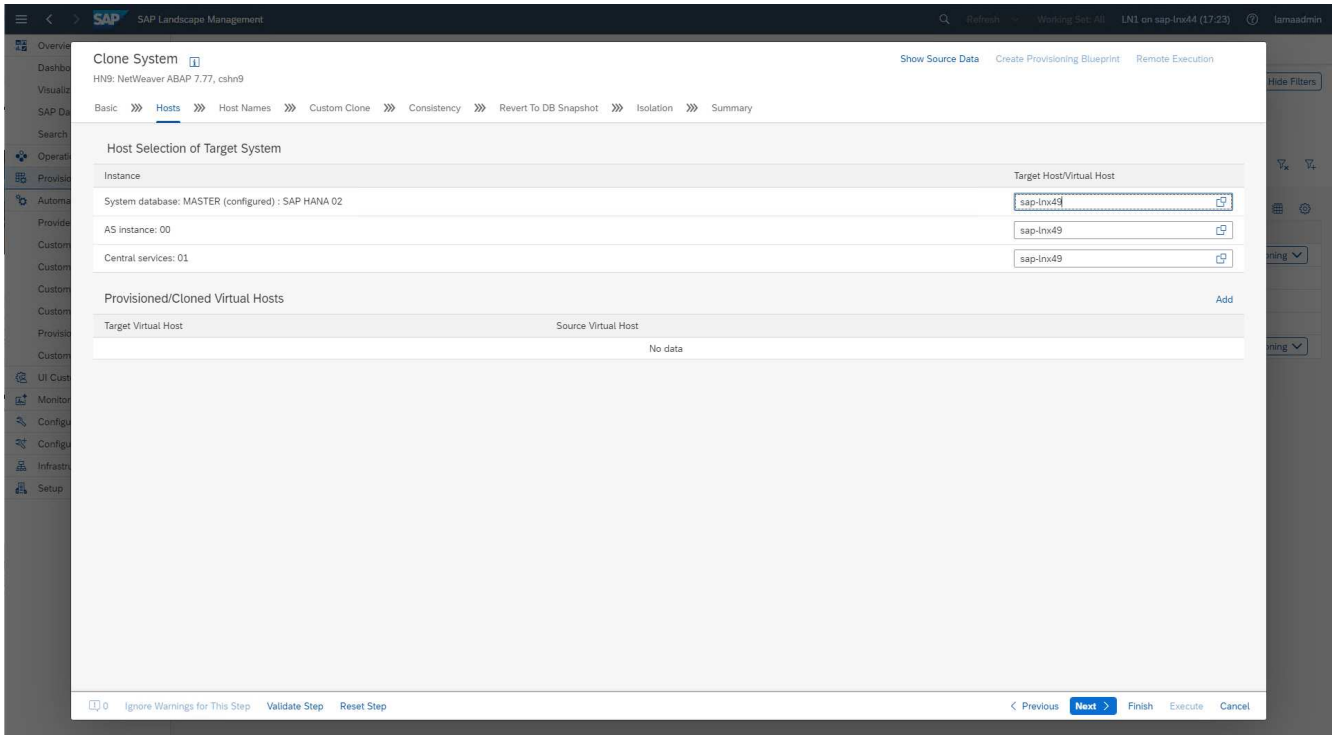

1. クローニングワークフローを開始するには、メニューツリーで* Provisioning を開き、ソースシステム（この例では**HN9**）を選択します。次に、 Clone System *ウィザードを起動します。



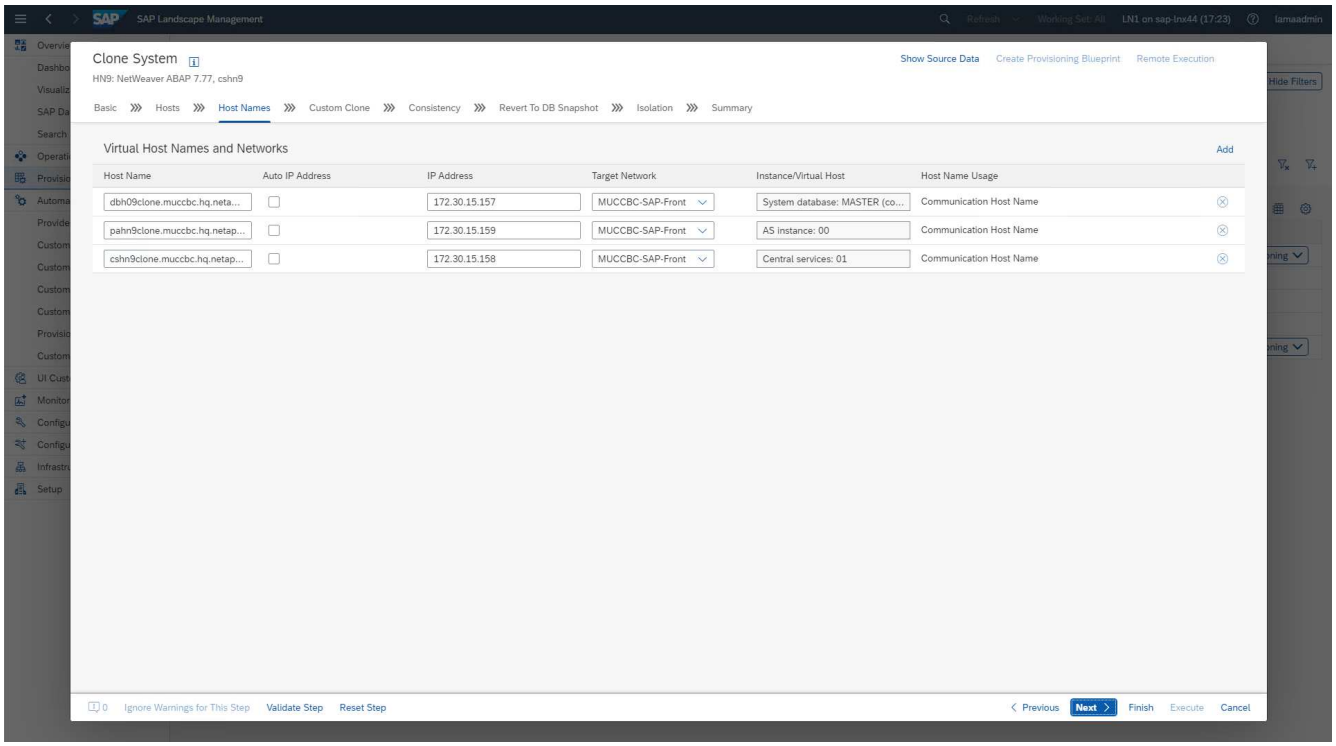

2. 必要な値を入力します。ウィザードの画面1で、クローニングしたシステムのプール名を入力するように求められます。このステップでは、クローニングされたシステムを起動するインスタンス（仮想または物理）を指定します。デフォルトでは、システムはターゲットシステムと同じプールにクローニングされます。



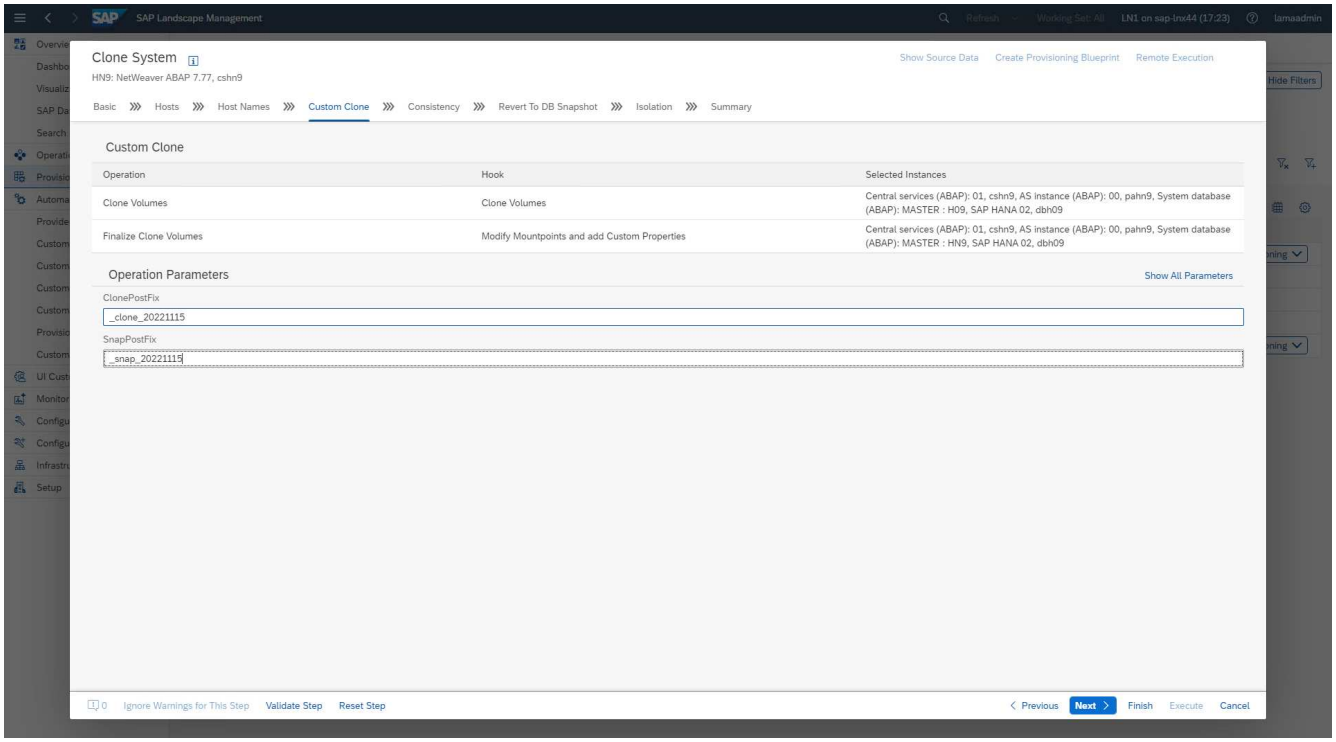

3. ウィザードの画面2で、新しいSAPインスタンスを起動するターゲットホストを指定するよう求められます。このインスタンスのターゲットホストは、前の画面で指定したホストプールから選択できます。各インスタンスまたはサービスは、別 々 のホストで開始できます。この例では、3つのサービスがすべて同じホスト上で実行されています。



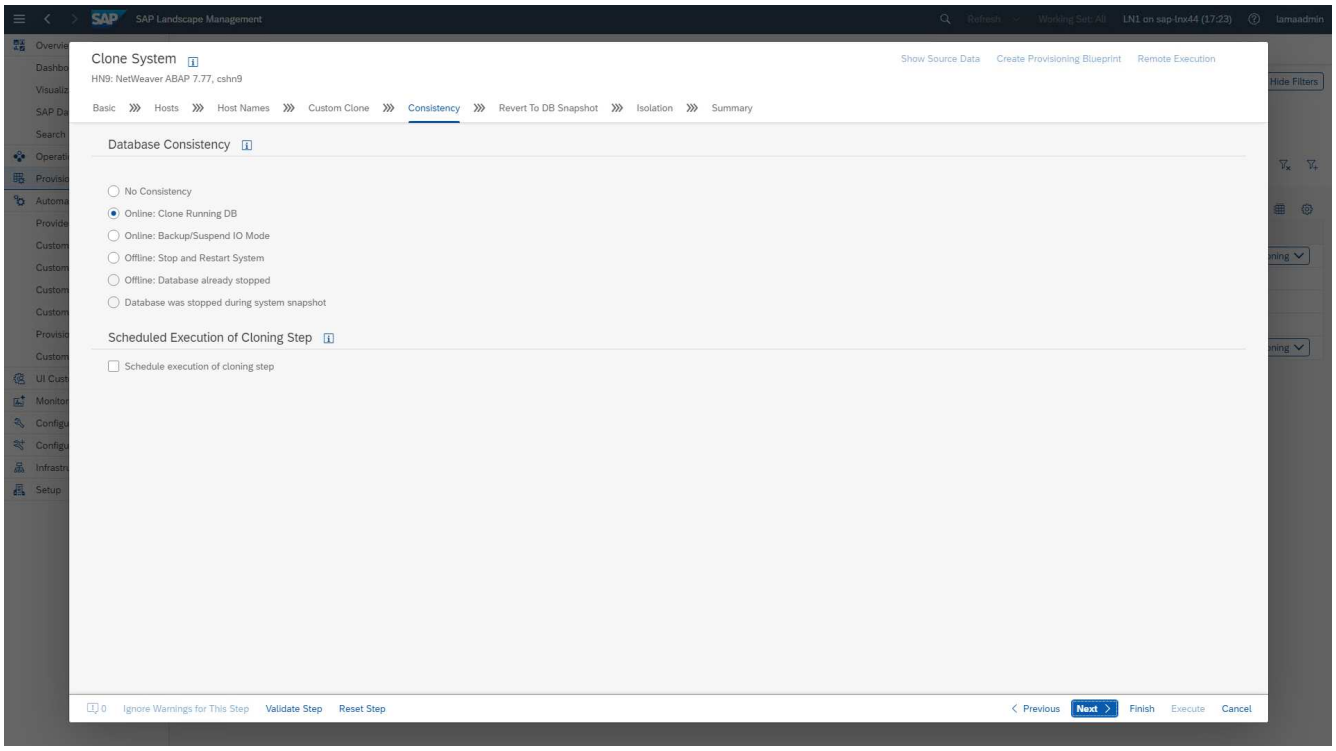

4. 画面3で要求された情報を入力します。この情報は、仮想ホスト名とネットワークを要求します。通常、ホスト名はDNSで管理されるため、IPアドレスもそれに応じて事前に入力されます。



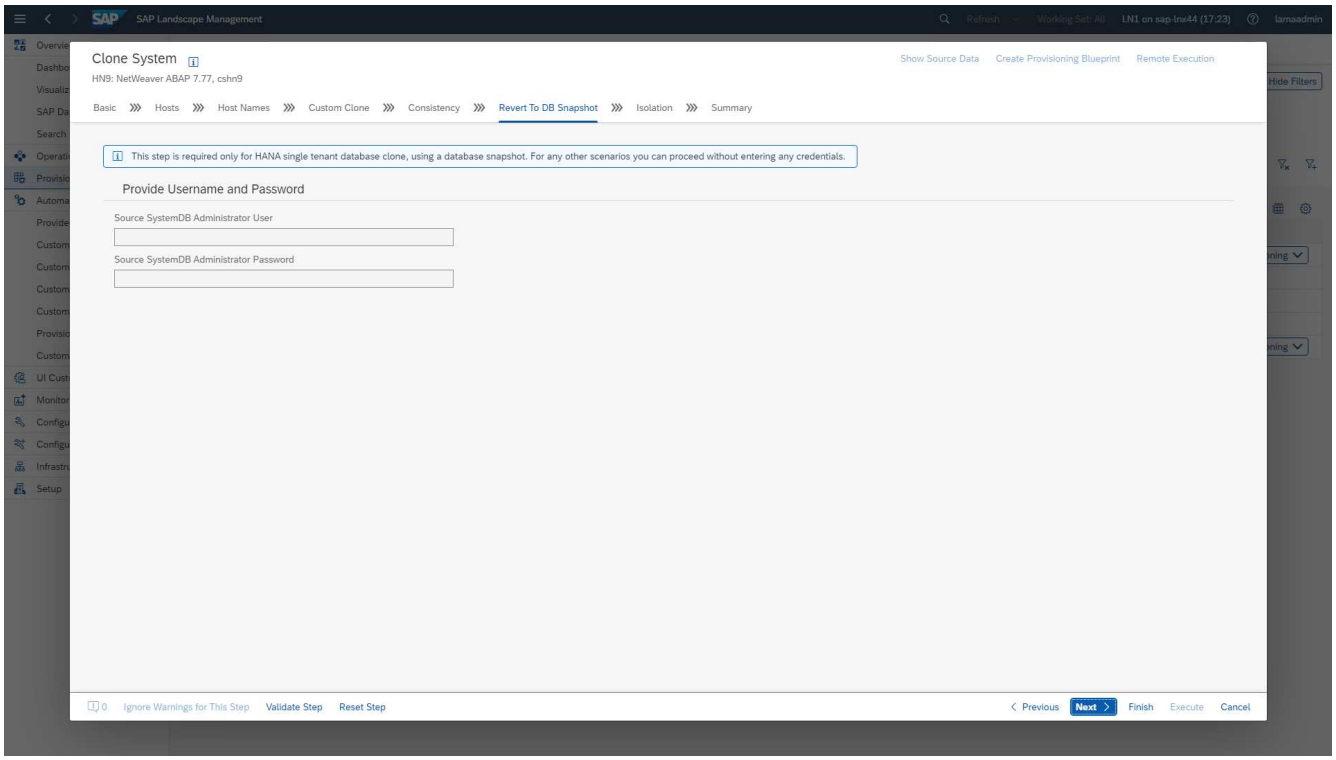

5. 画面4に、カスタムのクローン処理が表示されます。クローン名と* SnapPostfix *名を指定した場合、この名前は、FlexCloneボリュームとSnapshot名に対するストレージのクローン処理でそれぞれ使用されます。これらのフィールドを空のままにしておくと、プロバイダスクリプトの変数セクションで設定されたデフォルト値になります `netapp_clone.sh` を使用します。



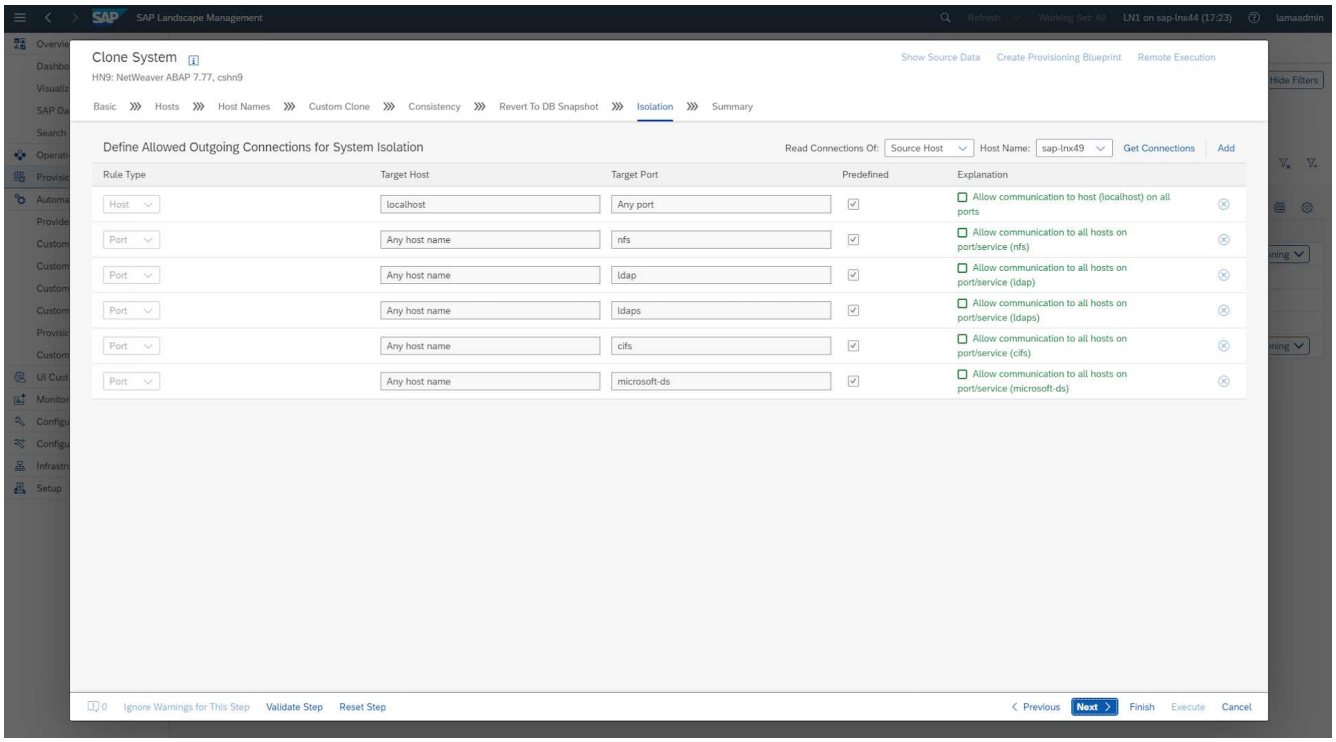

6. 画面5では、データベース整合性オプションが選択されています。この例では、「* Online：Clone running DB *」を選択しました。



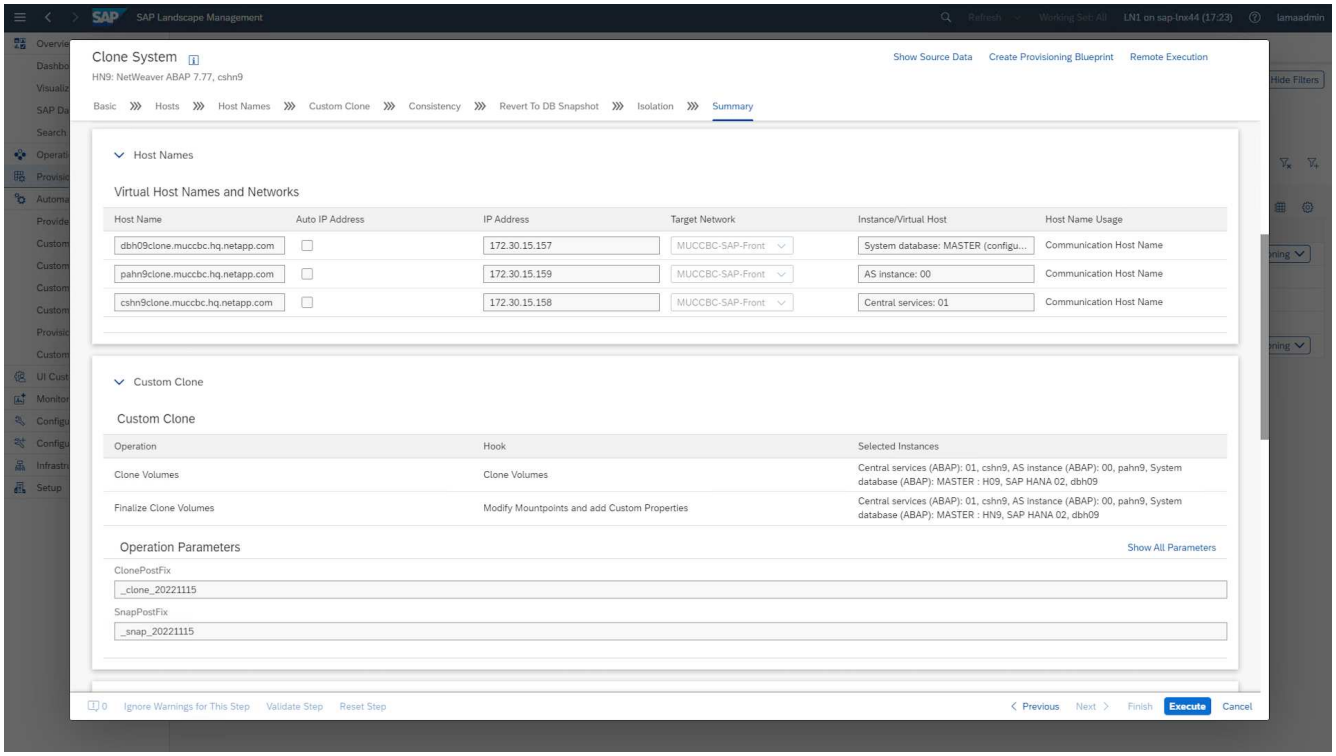

7. 画面6では、テナントのクローンを実行する場合にのみ入力する必要があります。




8. 画面7では、システムの隔離を構成できます。

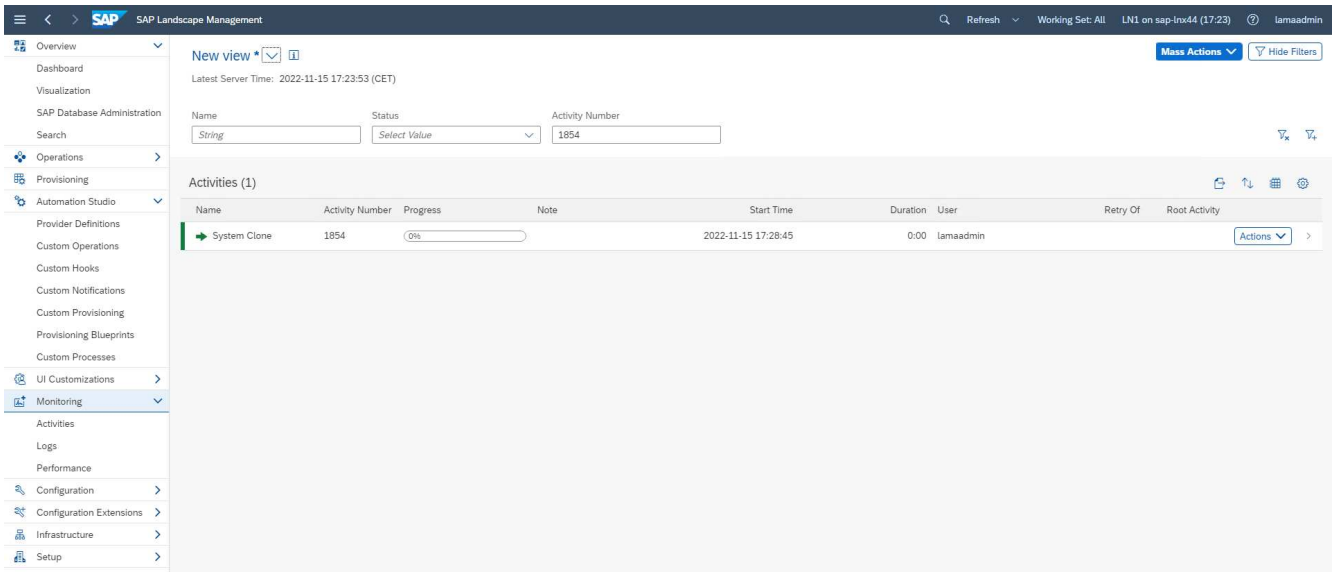



9. 画面8では、ワークフローを開始する前の最終確認のためのすべての設定が概要ページに表示されます。[**Execute**]をクリックして'ワークフローを開始します

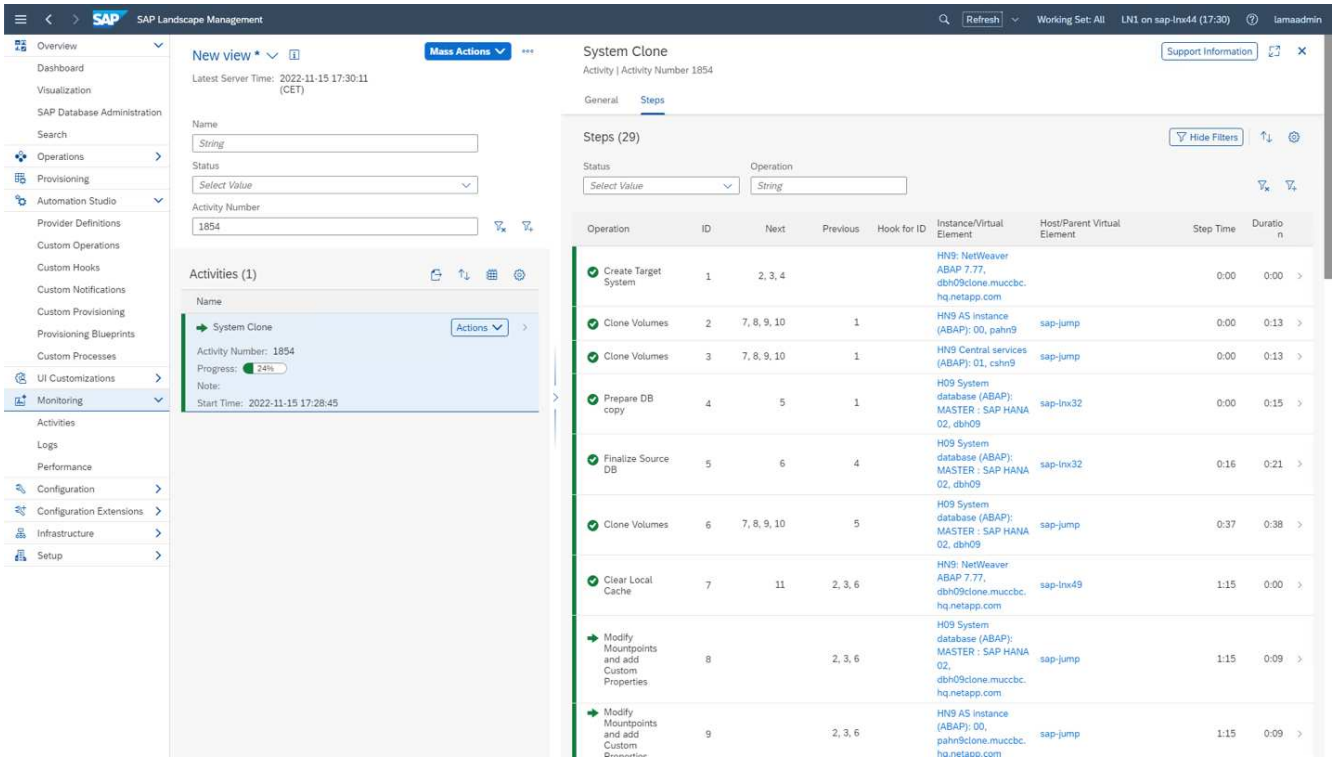



SAP LaMaが、設定に記載されたすべてのアクションを実行します。具体的には、ストレージボリュームのクローンとエクスポートの作成、ターゲットホストへのマウント、分離のためのファイアウォールルールの追加、HANAデータベースとSAPサービスの開始です。

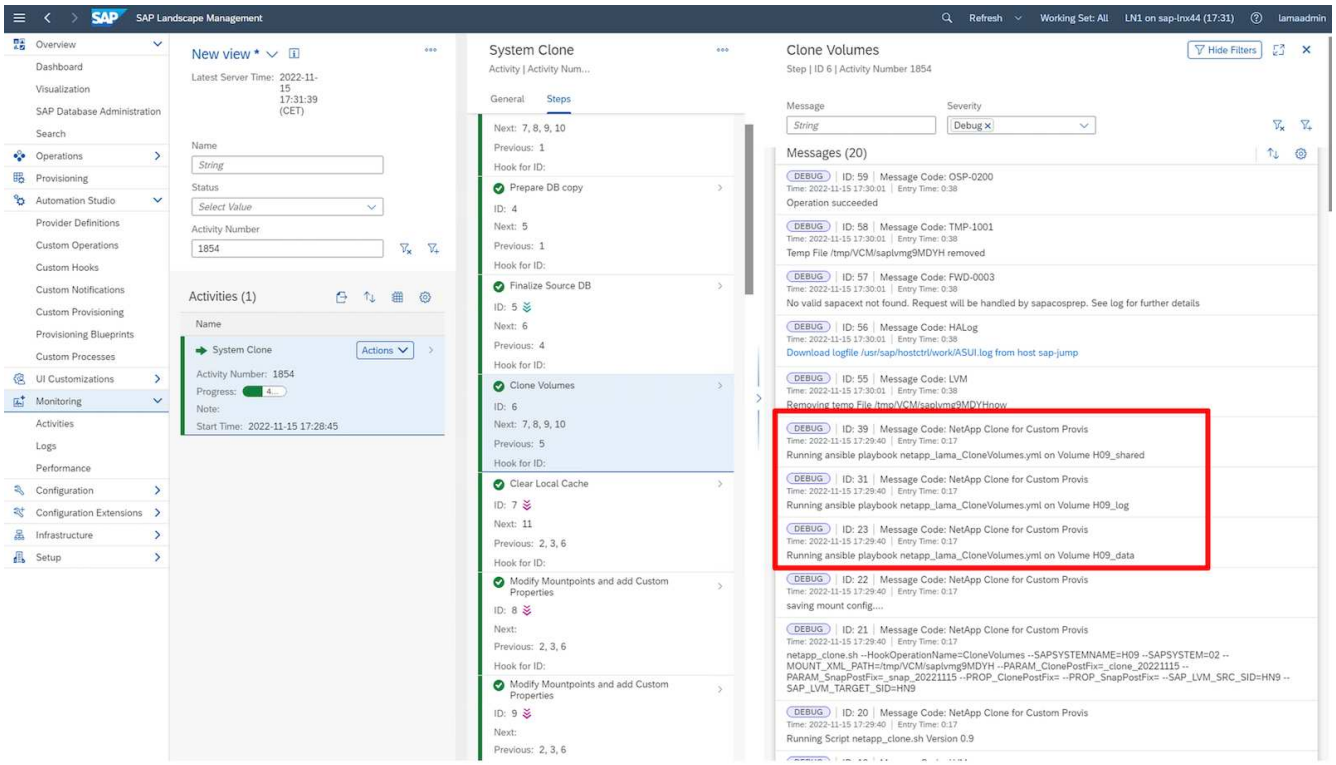
10. クローンワークフローの進行状況は、* Monitoring *メニューで監視できます。



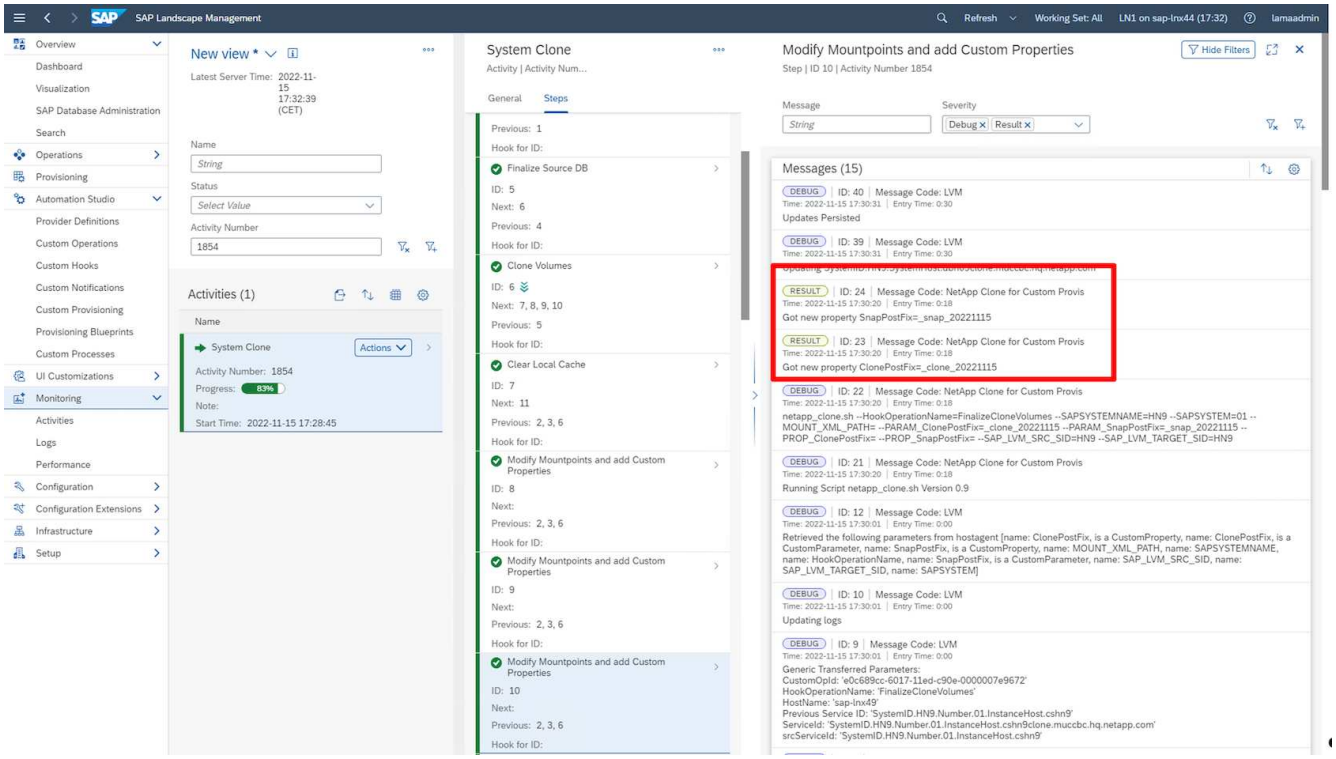

詳細ログには、* Clone Volume および Modifyマウントポイントと Add Custom Properties *の処理がAnsibleノード、で実行されます `sap-jump` ホスト：以下の手順は、各サービス、HANAデータベース、SAP中央サービス、およびSAPサービスに対して実行します。




11. Clone Volumes *タスクを選択すると、そのステップの詳細ログが表示され、Ansible Playbookの実行状況が表示されます。Ansibleプレイブックも確認できます `netapp_lama_CloneVolumes.yml` は、HANAデータベースのボリューム、データ、ログ、および共有ごとに実行されます。




12. マウントポイントの変更とカスタムプロパティの追加の手順*マウントポイントの詳細ビューには、マウントポイントと、実行スクリプトによって渡されたカスタムプロパティに関する情報が表示されます。



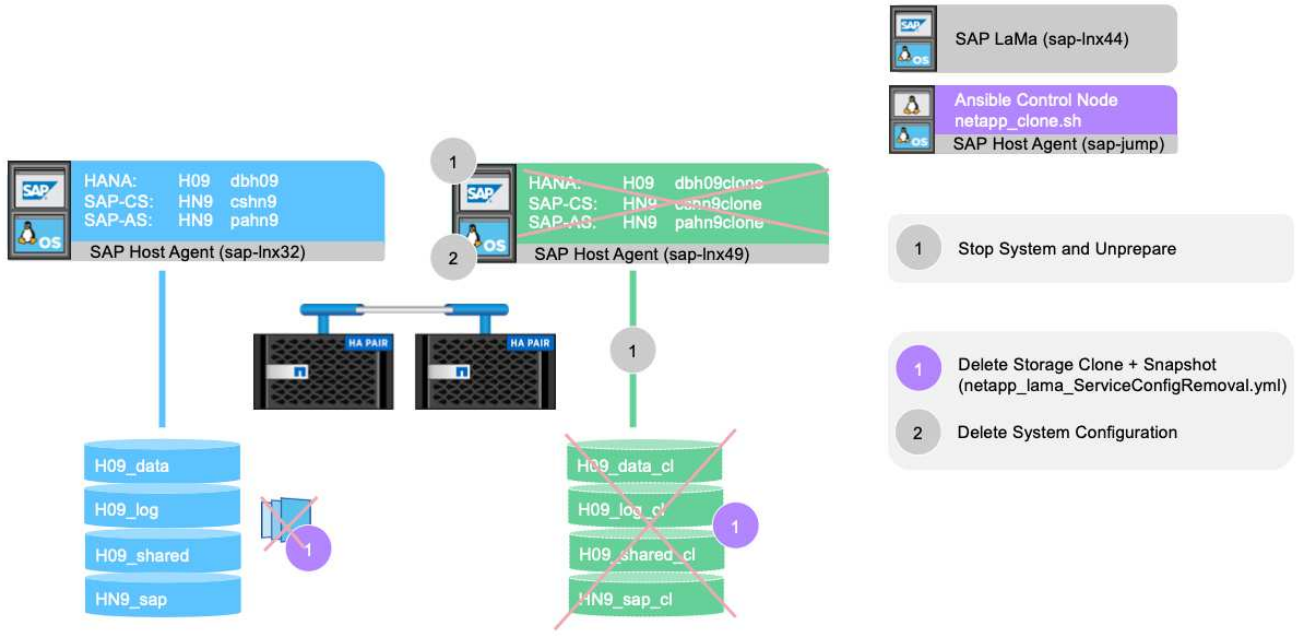

ワークフローが完了すると、クローニングしたSAPシステムの準備が完了し、使用できる状態になります。

## SAP LaMaによるワークフローのプロビジョニング解除-システムの破壊

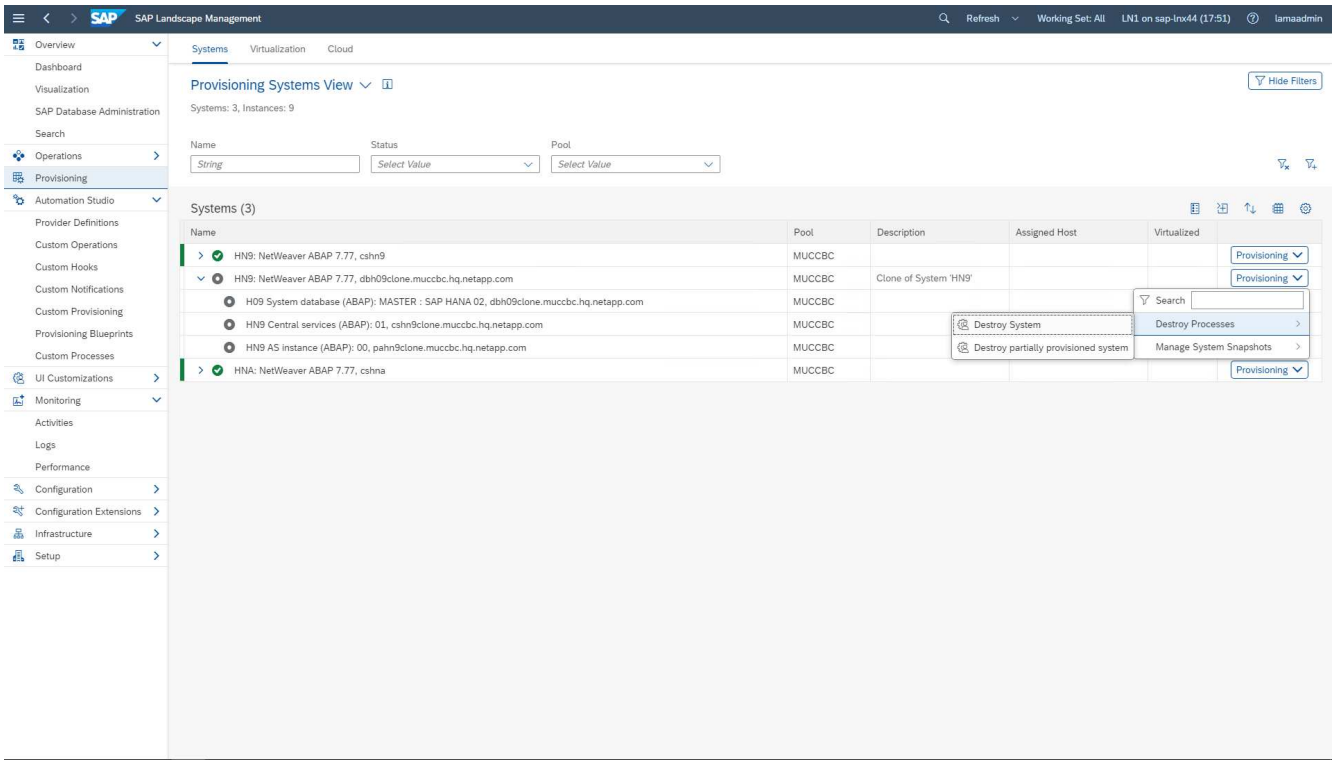
次の図は、system destroyワークフローで実行する主な手順を示しています。



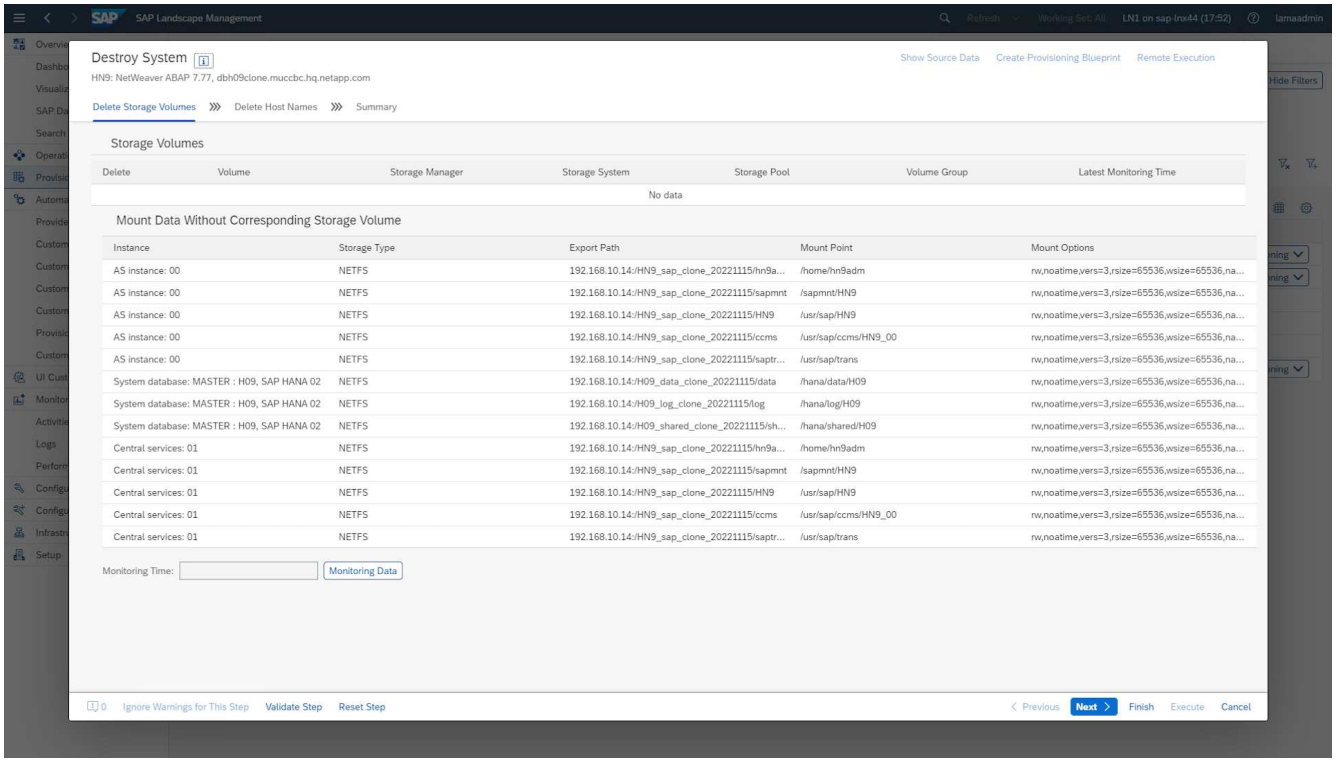

1. クローンシステムの運用を停止するには、運用を停止し、準備を事前に完了しておく必要があります。その後、システムの破棄ワークフローを開始できます。



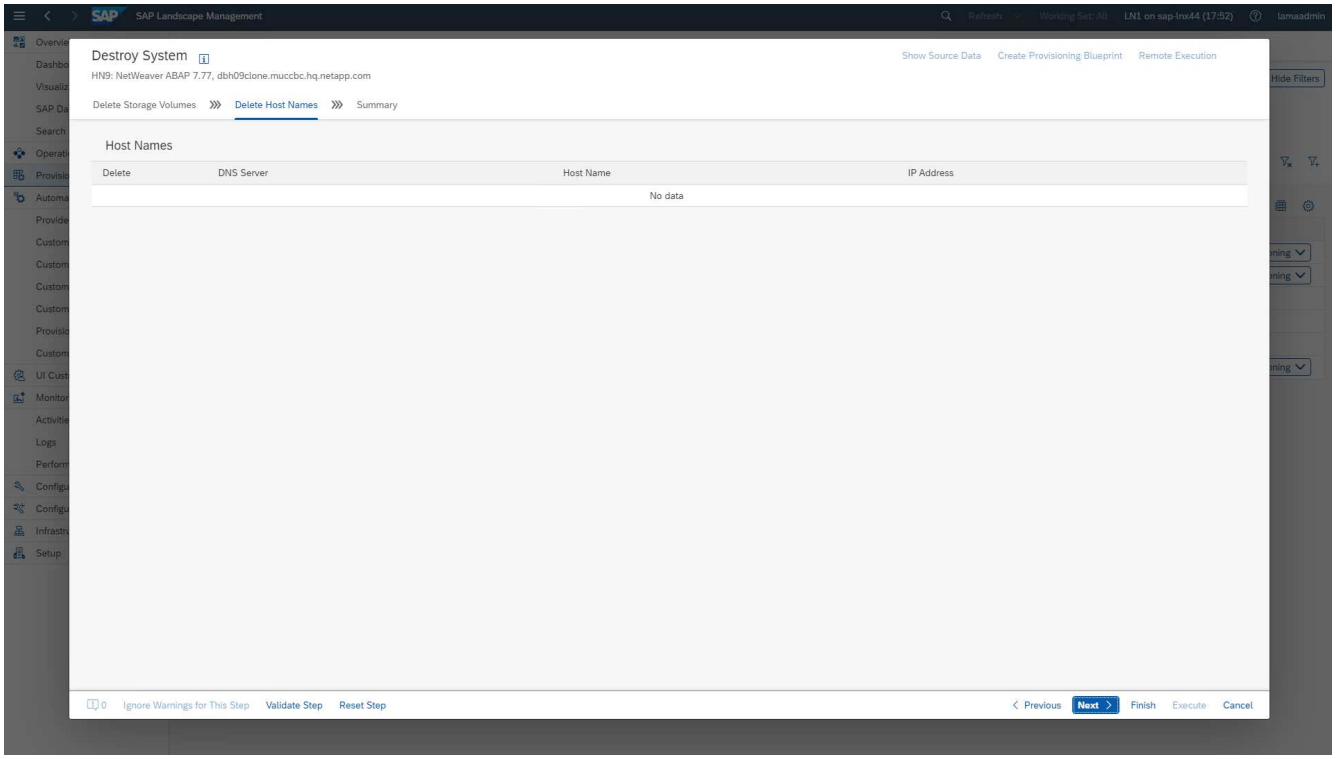

2. この例では、前に作成したシステムに対してsystem destroyワークフローを実行します。システムビュー*画面でシステムを選択し、*破棄プロセス*でシステム破棄ワークフローを開始します。



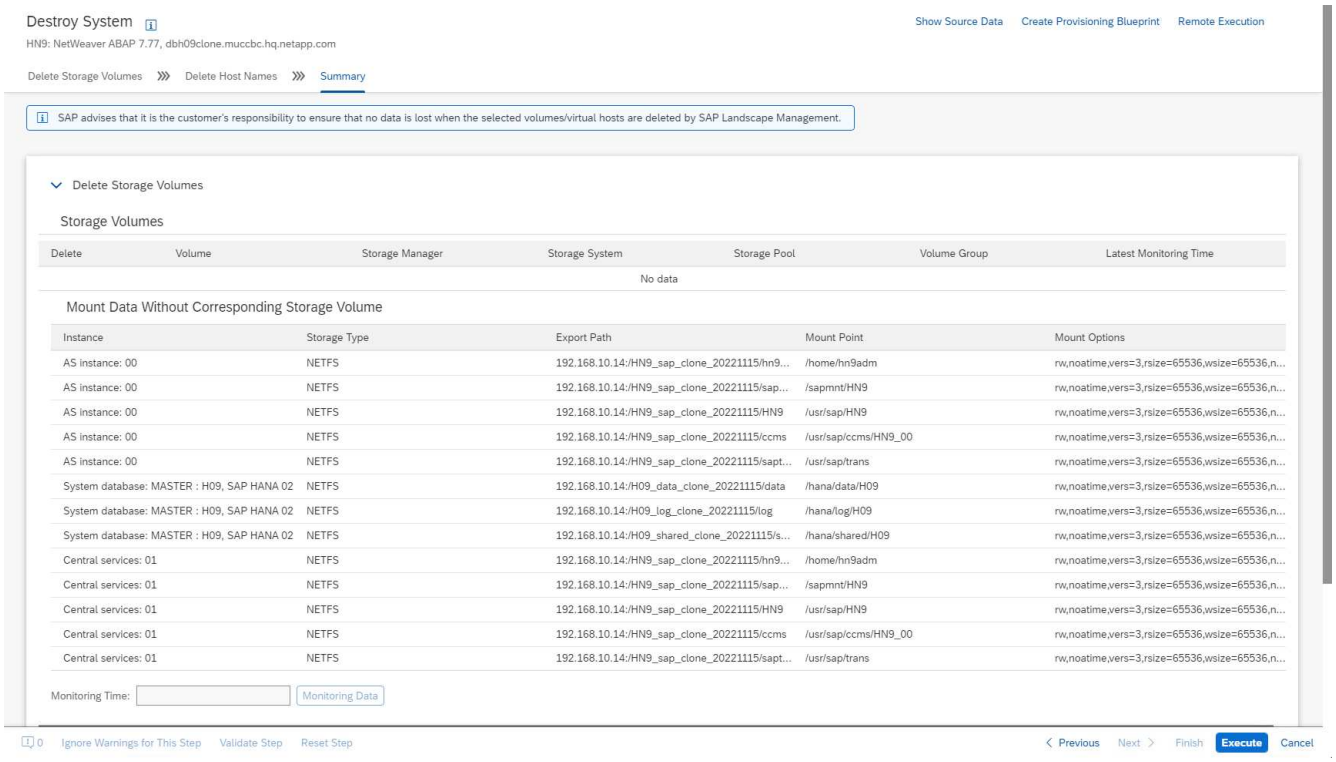

3. プロビジョニングフェーズで維持されたすべてのマウントポイントが表示され、システムの削除ワークフロープロセス中に削除されます。




仮想ホスト名はDNSを通じて管理され、自動的に割り当てられているため、削除されません。

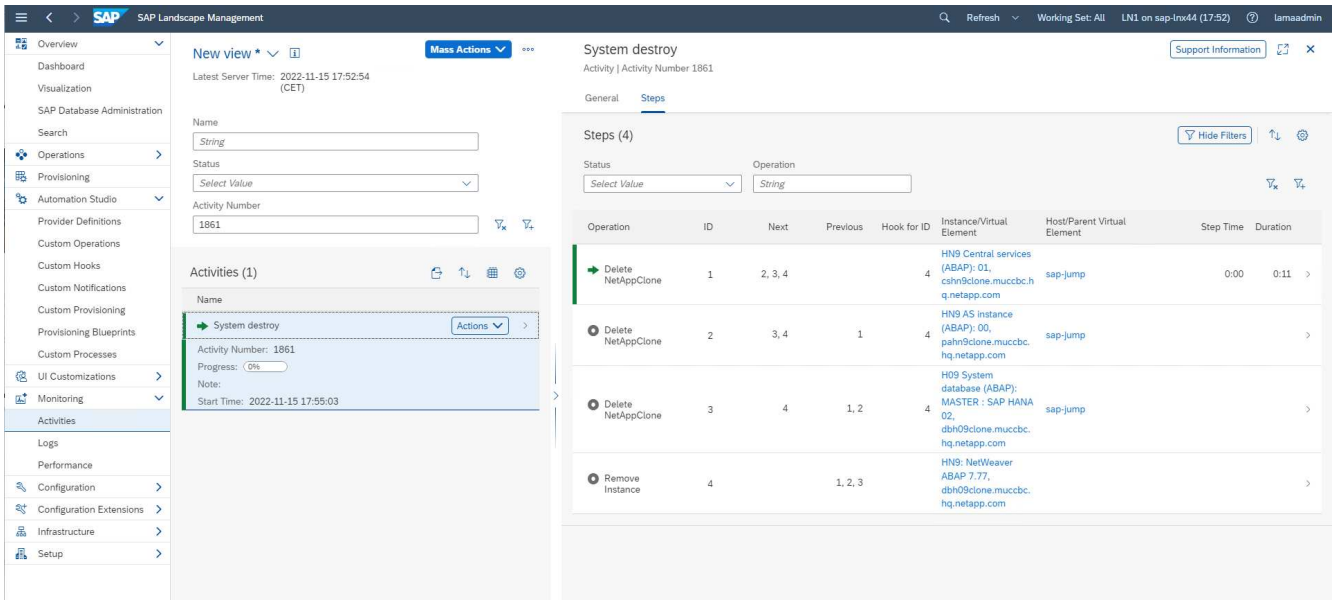



4. 実行ボタンをクリックすると、処理が開始されます。

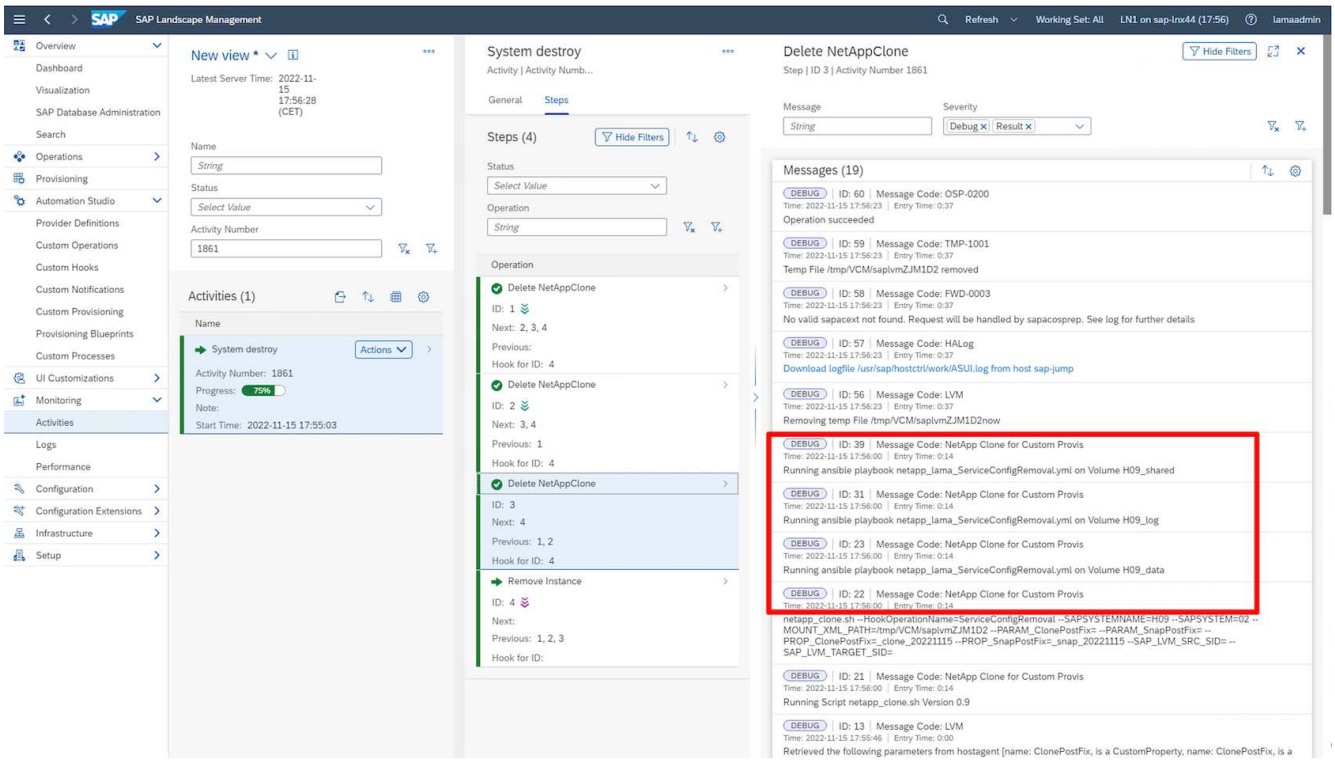



ボリュームクローンを削除し、そのクローンシステムの設定を削除する処理がSAP LaMaから実行されます。

5. クローンワークフローの進行状況は、* Monitoring *メニューで監視できます。

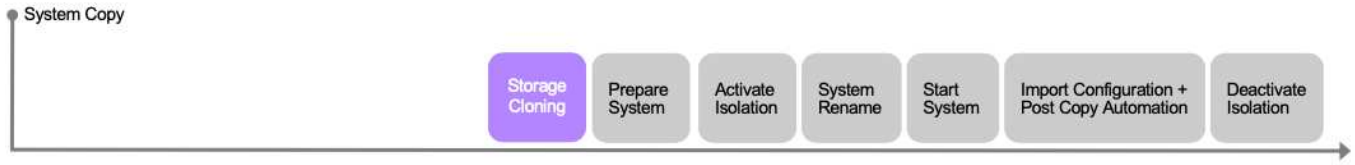



6. 「* Delete NetAppClone *」タスクを選択すると、その手順の詳細ログが表示されます。Ansibleプレイブックの実行方法を以下に示します。ご覧のように、Ansibleプレイブックもご覧いただけます `netapp_lama_ServiceConfigRemoval.yml` は、HANAデータベースのボリューム、データ、ログ、および共有ごとに実行されます。

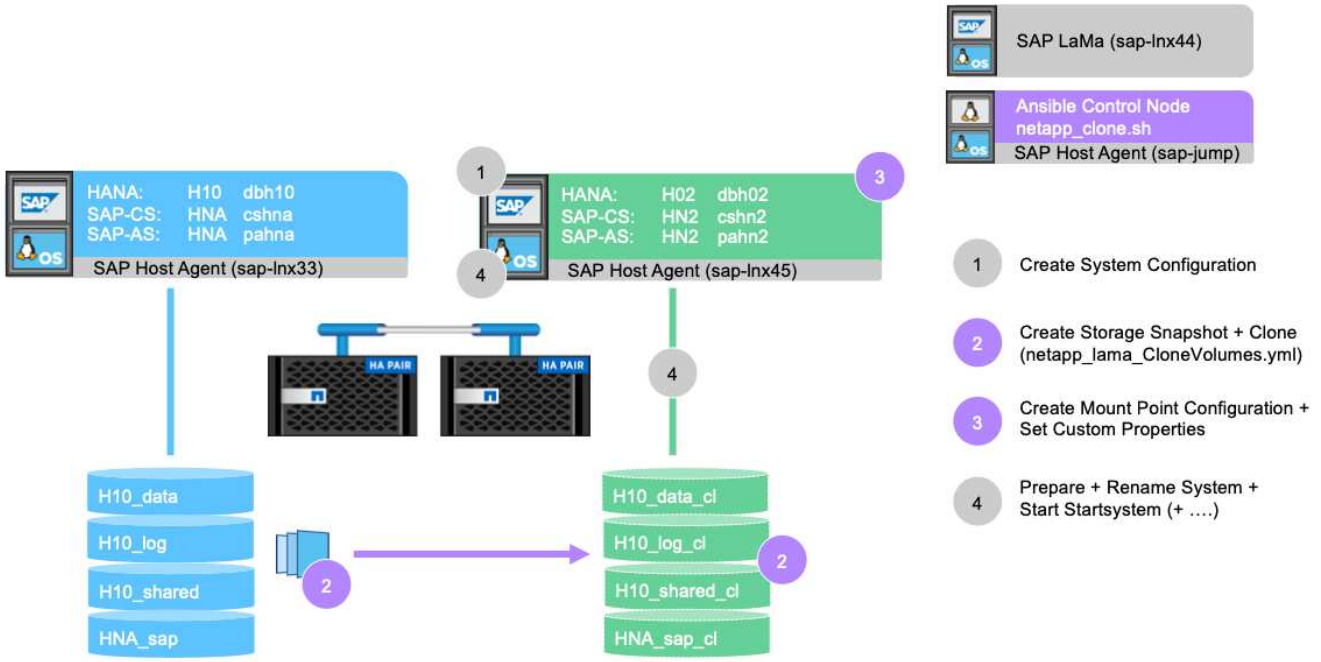



## SAP LaMaプロビジョニングワークフロー-コピーシステム

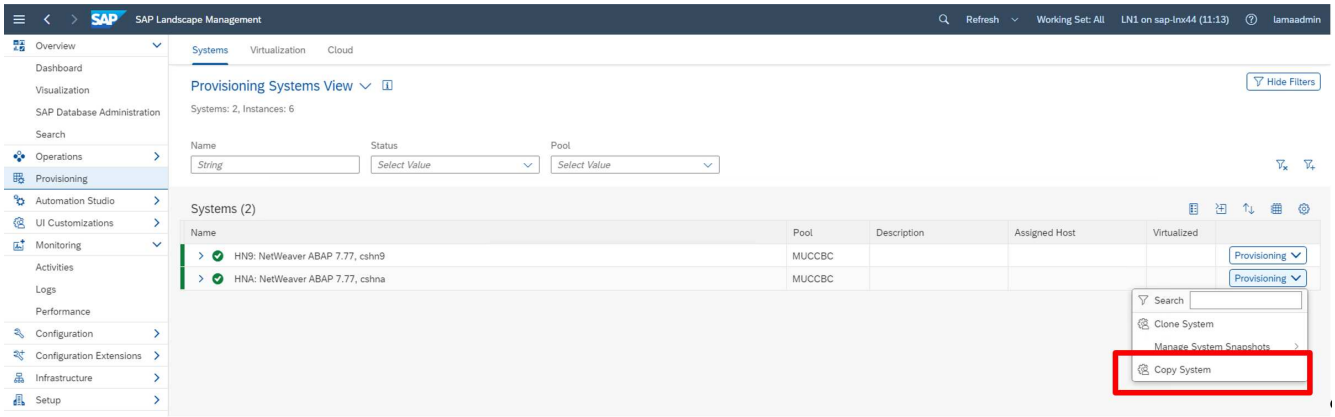
次の図は、システムコピーワークフローで実行する主な手順を示しています。




この章では、システムクローンのワークフローと入力画面の違いについて簡単に説明します。次の図に示すように、ストレージワークフローは変更されていません。

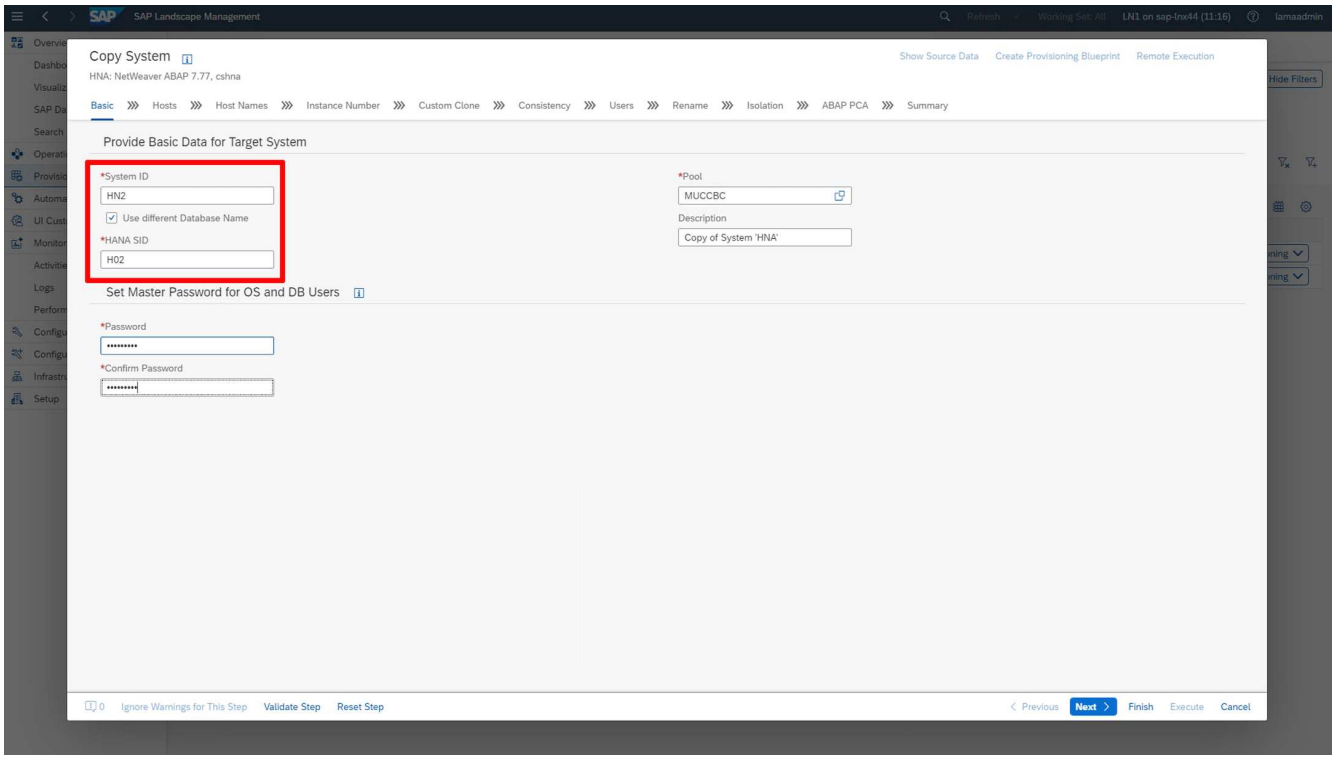



1. システムの準備が整ったら、システムコピーワークフローを開始できます。これは、この設定に関する特定のタスクではなく、詳細な説明も行いません。詳細については、SAP LaMaのドキュメントをご覧ください。

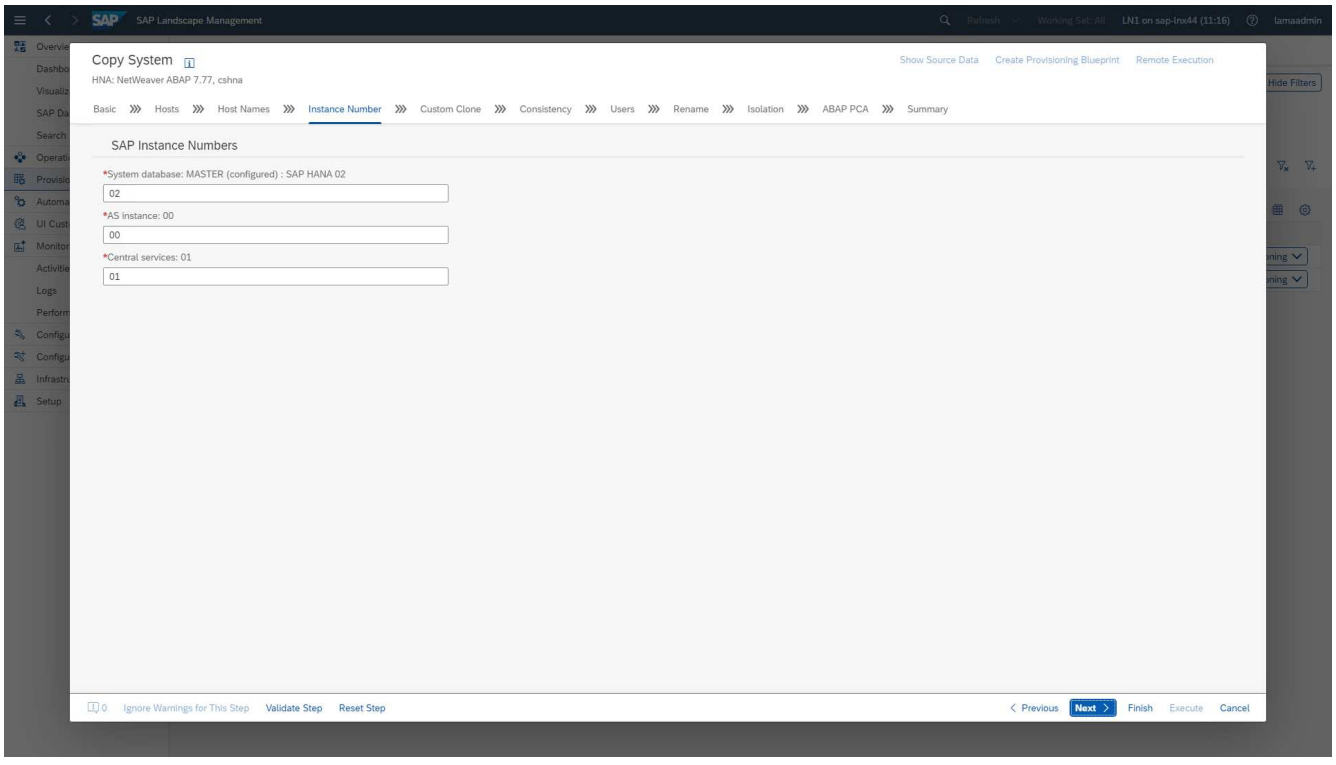



ドロップダウンが強調表示されます。"]

2. コピーワークフローの実行中、最初の画面で指定する必要があるのと同様に、システムの名前が変更されます。

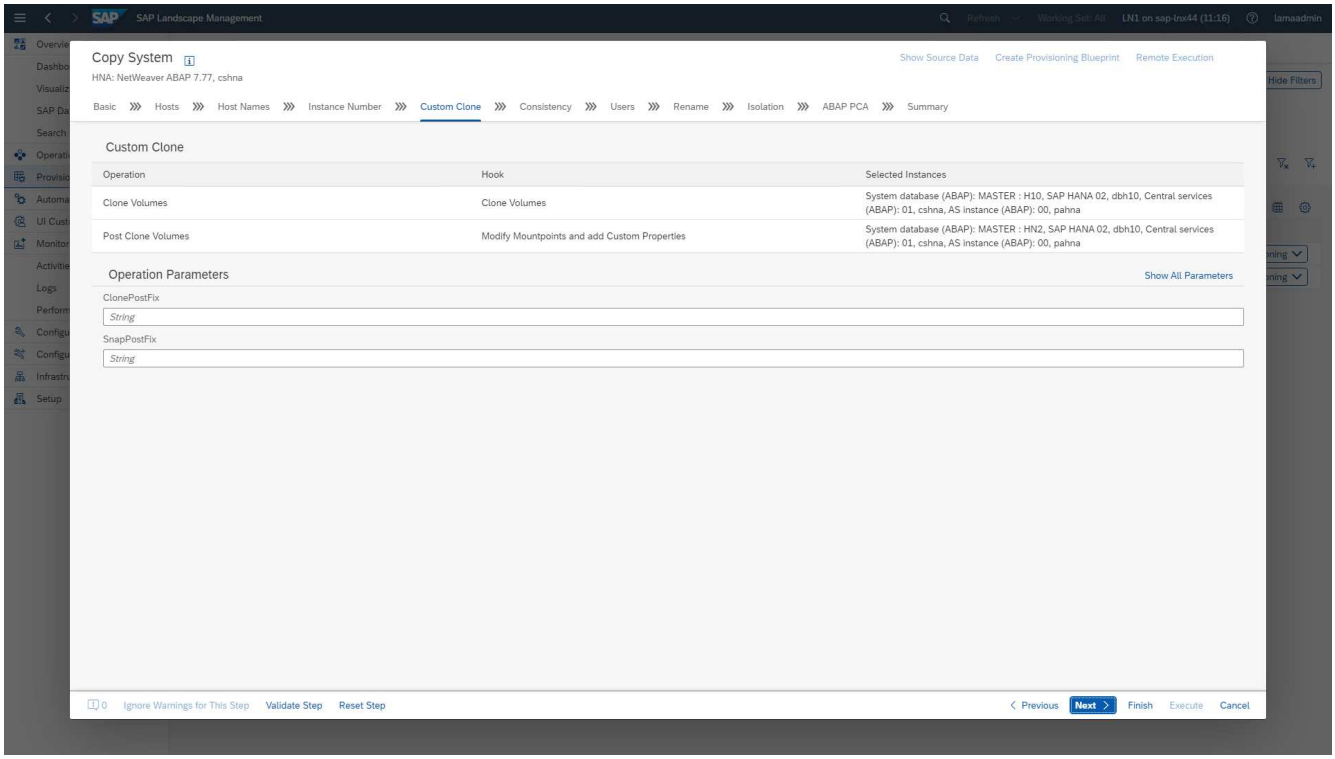



3. ワークフロー中にインスタンス番号を変更することができます。

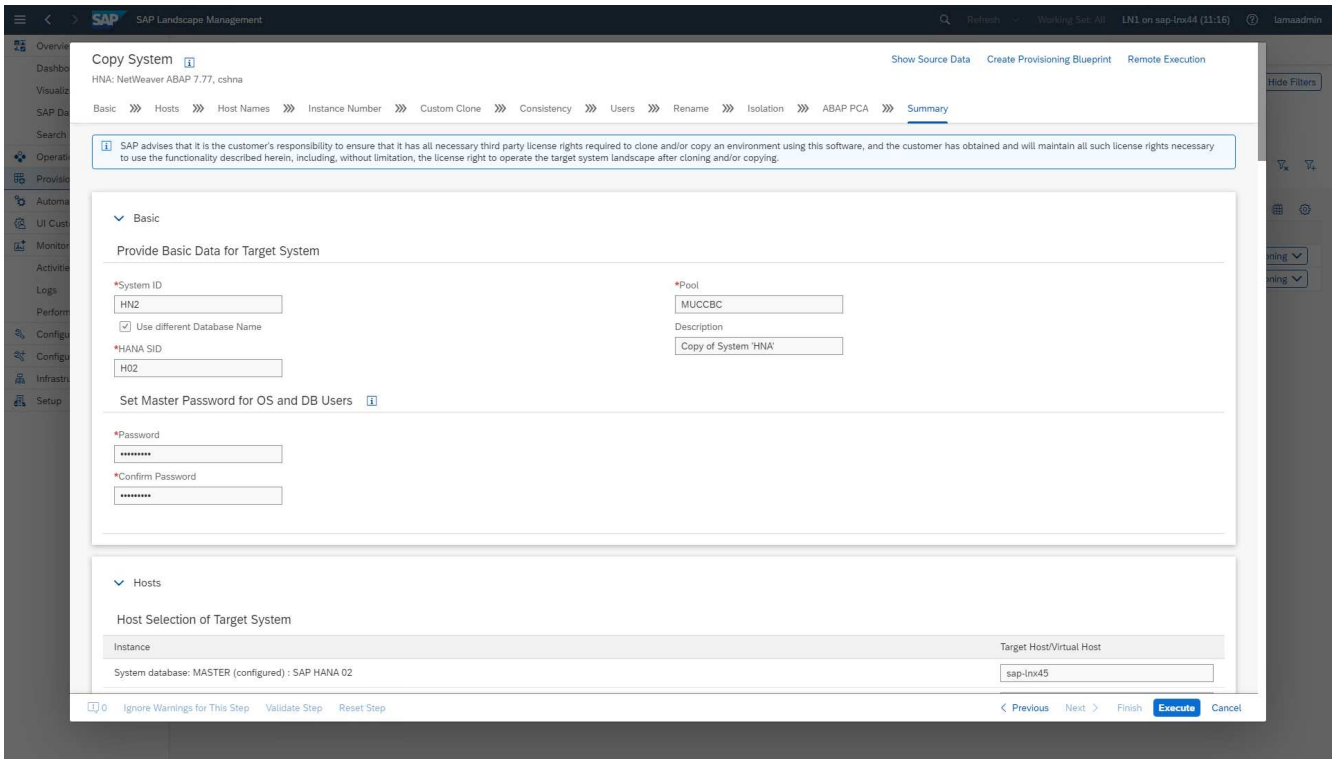



インスタンス番号の変更はテストされていないため、プロバイダスクリプトの変更が必要になる場合があります。

4. 前述のように、* Custom Clone *画面はクローニングワークフローとは異なりません。

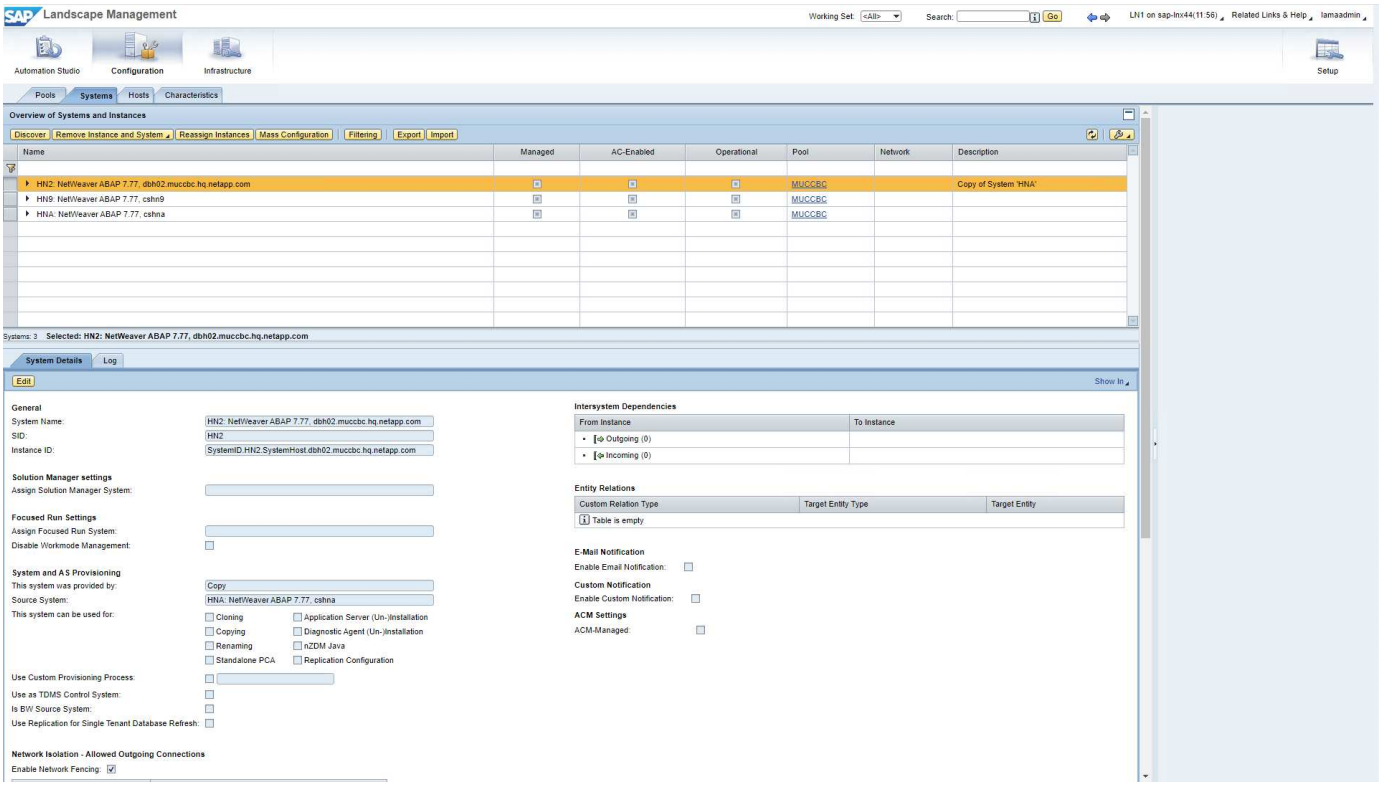



5. すでに説明したように、残りの入力マスクは標準とは異なるので、ここではそれ以上のマスクには入りません。最後の画面に概要が表示され、実行を開始できます。

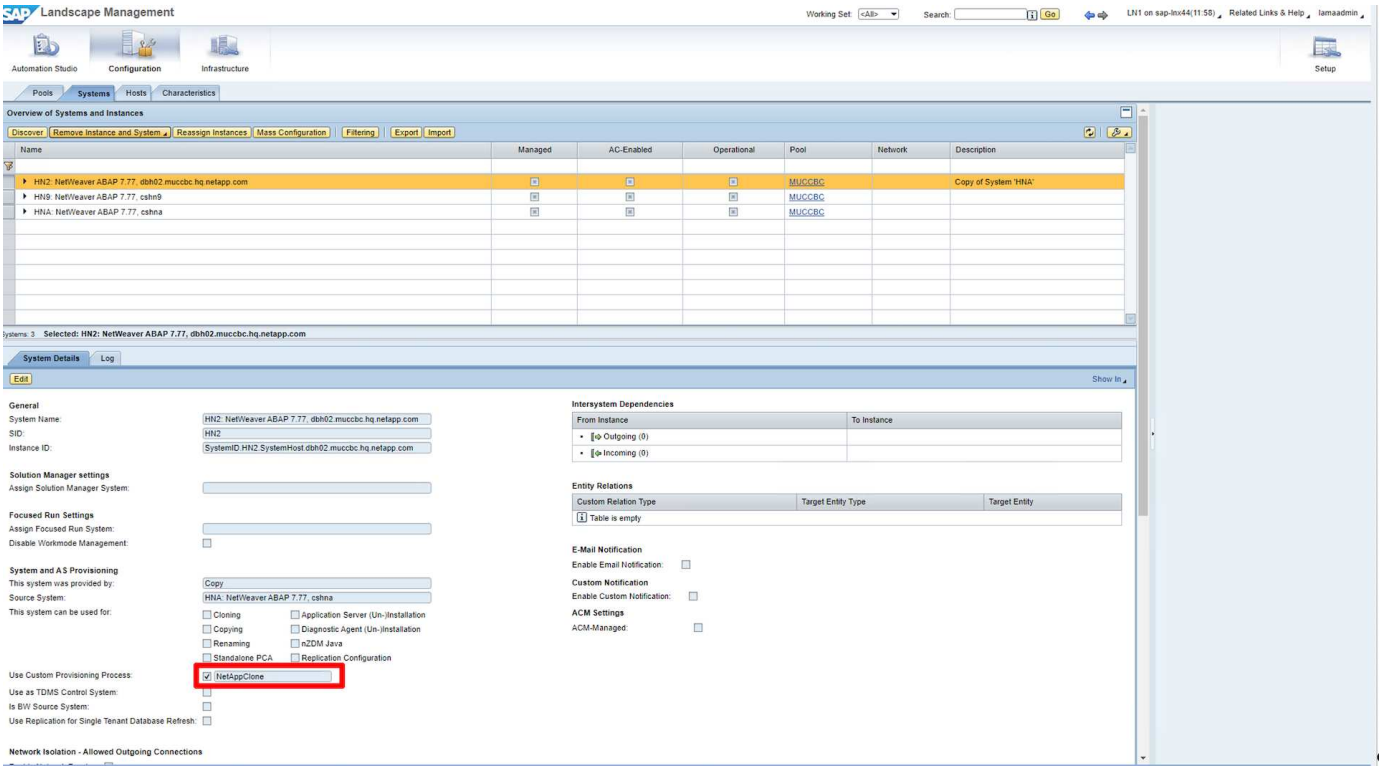



ボタンをクリックします。"]

コピープロセスの完了後、カスタムのクローニングプロセスでターゲットインスタンスが有効になりません。

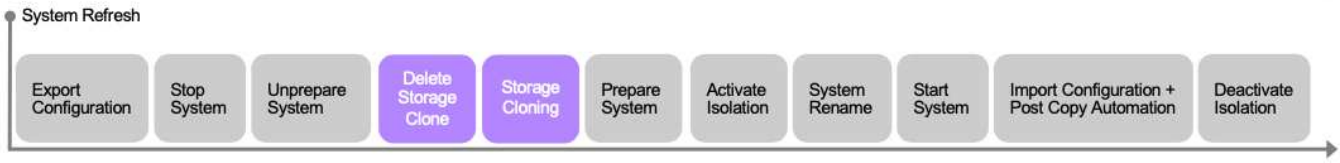



拘束が設定されて実行を妨げるため'システム破壊プロセス中にプフックステップを実行するには'手動で採用する必要があります

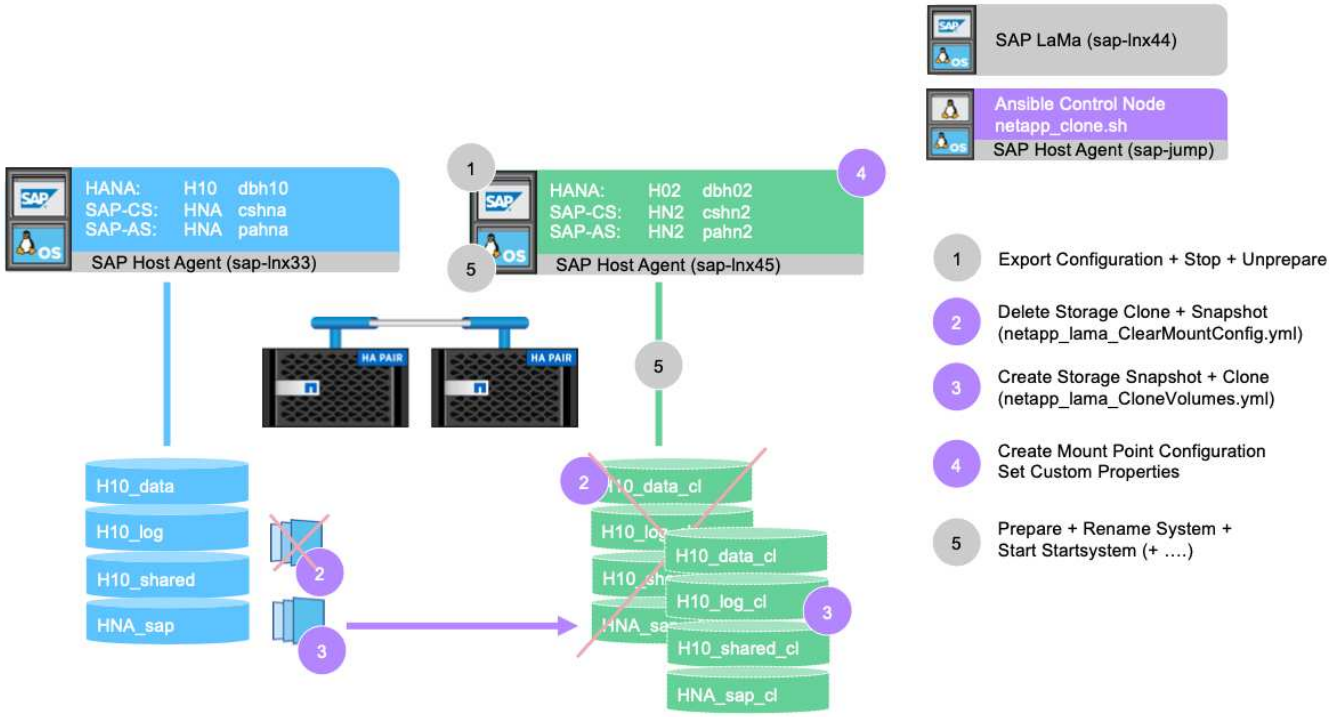



## SAP LaMaプロビジョニングワークフロー-システムの更新

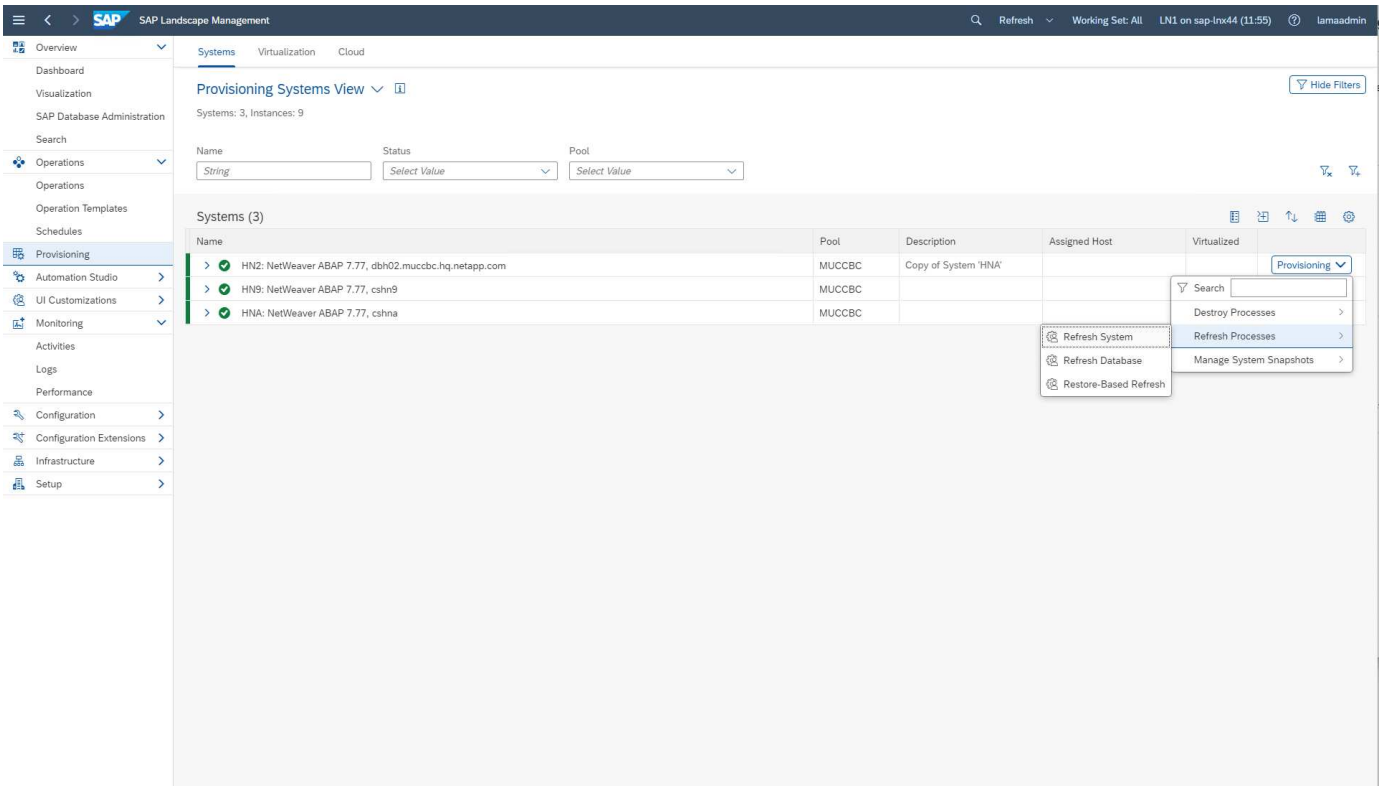
次の図は、システムの更新ワークフローで実行する主な手順を示しています。



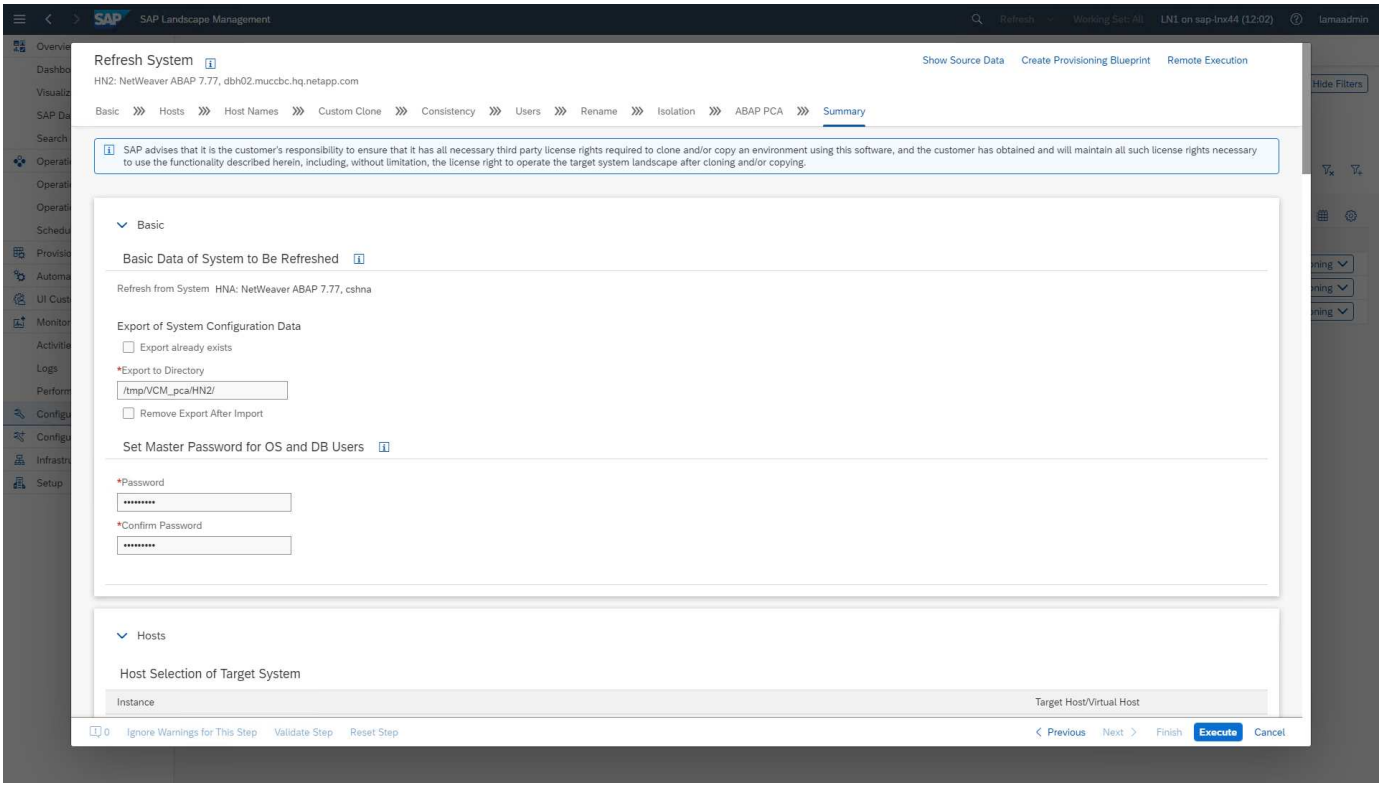

更新ワークフロー中に、ストレージクローンを削除する必要があります。システム破棄ワークフローにも同じAnsibleプレイブックを使用できます。ただし、カスタムフックは別の手順に定義されるため、プレイブックの名前も適宜変更されます。クローンのプロセス手順に違いはありません。




更新ワークフローは、コピーしたシステムのプロビジョニング画面から開始できます。




繰り返しますが、入力画面と標準画面では何も異なりません。ワークフローの実行は概要画面から開始できます。




## プロバイダスクリプトの設定と**Ansible**のプレイブック

このドキュメントの導入例とワークフローの実行時には、次のプロバイダ構成ファイ

ル、実行スクリプト、およびAnsibleプレイブックを使用します。

> このサンプルスクリプトは現状のまま提供されており、ネットアップではサポートしていません。スクリプトの最新バージョンは、mailto：ng-sapcc@netapp.com [ng-sapcc@netapp.com ^]にEメールでリクエストできます。

プロバイダ構成ファイル**NetApp_clone.conf**

構成ファイルは、の説明に従って作成されます "SAP LaMaドキュメント-「Configuring SAP Host Agent Registered Scripts"。この構成ファイルは、SAPホストエージェントがインストールされているAnsibleコントロールノードに配置する必要があります。

設定されているos-user `sapuser` スクリプトおよび呼び出されたAnsibleプレイブックを実行するための適切な権限が必要です。このスクリプトは共通のスクリプトディレクトリに配置できます。SAP LaMaは、スクリプトを呼び出す際に複数のパラメータを提供します。

カスタムパラメータに加えて、 `PARAM_ClonePostFix`、 `PROP_ClonePostFix`、 `PARAM_ClonePostFix` および `PROP_ClonePostFix`に示されているように、他の多くは手渡されることができる "SAP LaMaのドキュメント"。

```
root@sap-jump:~# cat /usr/sap/hostctrl/exe/operations.d/netapp_clone.conf
Name: netapp_clone
Username: sapuser
Description: NetApp Clone for Custom Provisioning
Command: /usr/sap/scripts/netapp_clone.sh
--HookOperationName=$[HookOperationName] --SAPSYSTEMNAME=$[SAPSYSTEMNAME]
--SAPSYSTEM=$[SAPSYSTEM] --MOUNT_XML_PATH=$[MOUNT_XML_PATH]
--PARAM_ClonePostFix=$[PARAM-ClonePostFix] --PARAM_SnapPostFix=$[PARAM
-SnapPostFix] --PROP_ClonePostFix=$[PROP-ClonePostFix]
--PROP_SnapPostFix=$[PROP-SnapPostFix]
--SAP_LVM_SRC_SID=$[SAP_LVM_SRC_SID]
--SAP_LVM_TARGET_SID=$[SAP_LVM_TARGET_SID]
ResulConverter: hook
Platform: Unix
```

プロバイダスクリプト**netapp_clone.sh**

プロバイダスクリプトはに保存する必要があります `/usr/sap/scripts` プロバイダの構成ファイルで設定されているとおりです。

変数（ **variables** ）

次の変数はスクリプトでハードコードされており、適宜変更する必要があります。

- `PRIMARY_CLUSTER=`<hostname of netapp cluster>
- `PRIMARY_SVM=`<SVM name where source system volumes are stored>

証明書ファイル `PRIMARY_KEYFILE=/usr/sap/scripts/ansible/certs/ontap.key` および

PRIMARY_CERTFILE=/usr/sap/scripts/ansible/certs/ontap.pem の説明に従って指定する必要があります "NetApp Ansibleモジュール- ONTAP を準備"。

> それぞれのSAPシステムで異なるクラスタやSVMが必要な場合は、SAP LaMaプロバイダ定義のパラメータとして追加できます。

機能：インベントリファイルを作成する

Ansibleプレイブックをより動的に実行するために、を使用します inventory. yml その場でファイルが作成されます。一部の静的値は変数セクションで設定され、一部は実行中に動的に作成されます。

関数：**Ansible**プレイブックを実行する

この関数は、Ansibleプレイブックと動的に作成されるを実行するために使用します inventory.yml ファイル。プレイブックの命名規則はです netapp_lama_${HookOperationName}.yml。の値 ${HookOperationName} LaMaの運用に依存し、LaMaをコマンドラインパラメータとして引き継ぎます。

セクション**Main**

ここでは、主な実行計画について説明します。変数 ${HookOperationName} LaMaの代替手順の名前が含まれ、スクリプトが呼び出されるとLaMaによって提供されます。

- システムクローンとシステムコピーのプロビジョニングワークフローを使用した値：
  - CloneVolumes
  - CloneVolumes
- system destroyワークフローを使用した値：
  - ServiceConfigRemovalサービス構成の削除
- システムの更新ワークフローによる値：
  - ClearMountConfigの場合

**HookOperationName=CloneVolumes**

この手順では、Ansibleプレイブックが実行され、Snapshotコピーとクローニングの処理が開始されます。ボリューム名とマウント設定は、変数で定義されたXMLファイルを使用してSAP LaMaによって引き継がれます $MOUNT_XML_PATH。このファイルは、あとで手順で使用するために保存されます FinalizeCloneVolumes 新しいマウントポイント設定を作成します。ボリューム名がXMLファイルから抽出され、各ボリュームに対してAnsibleのクローニングプレイブックが実行されます。

> この例では、ASインスタンスと中央サービスは同じボリュームを共有します。したがって、ボリュームクローニングはSAPインスタンス番号でのみ実行されます ($SAPSYSTEM）はではありません 01。これは他の環境とは異なる場合があるため、変更する必要があります。

**HookOperationName=PostCloneVolumes**

このステップでは、ユーザー定義プロパティを指定します ClonePostFix および SnapPostFix また、ターゲットシステムのマウントポイント設定が保持されます。

カスタムプロパティは、あとでででの運用停止時に入力として使用されます ServiceConfigRemoval または ClearMountConfig フェーズ：システムのプロビジョニングワークフローで指定されたカスタムパラメ

ータの設定を保持するように設計されています。

この例で使用されている値はです `ClonePostFix=_clone_20221115` および `SnapPostFix=_snap_20221115`。

ボリューム `HN9_sap`は、動的に作成されるAnsibleファイルに次の値が含まれています。 `datavolumename： HN9_sap、 snapshotpostfix: _snap_20221115`および `clonepostfix: _clone_20221115`。

これにより、ボリュームHN9_SAP上のSnapshot名に変換されます `HN9_sap_snap_20221115` 作成されたボリュームクローンの名前も表示されます `HN9_sap_clone_20221115`。

> ⓘ カスタムプロパティを使用すると、プロビジョニングプロセスで使用されるパラメータを保持できます。

マウントポイントの設定は、でLaMaに引き継がれたXMLファイルから抽出されます `CloneVolume` ステップ。。 `ClonePostFix` がボリューム名に追加され、デフォルトのスクリプト出力でLaMaに返信されます。機能については、を参照してください "SAPノート1889590"。

> ⓘ この例では、ストレージシステム上のqtreeを、単一のボリュームに異なるデータを配置する一般的な方法として使用します。例： `HN9_sap` のマウントポイントを保持します `/usr/sap/HN9`、 `/sapmnt/HN9`および `/home/hn9adm`。サブディレクトリも同様に機能します。これは他の環境とは異なる場合があるため、変更する必要があります。

**HookOperationName = ServiceConfigRemoval**

この手順では、ボリュームクローンの削除を実行するAnsibleプレイブックを使用します。

ボリューム名は、マウント構成ファイルとカスタムプロパティを通じてSAP LaMaから引き継がれます `ClonePostFix` および `SnapPostFix` は、システムプロビジョニングワークフローで最初に指定されたパラメータの値を渡すために使用します（の注を参照） `HookOperationName = PostCloneVolumes`）。

ボリューム名がXMLファイルから抽出され、各ボリュームに対してAnsibleのクローニングプレイブックが実行されます。

> ⓘ この例では、ASインスタンスと中央サービスは同じボリュームを共有します。そのため、ボリュームの削除はSAPインスタンス番号がの場合にのみ実行されます (`$SAPSYSTEM`）はではありません `01`。これは他の環境とは異なる場合があるため、変更する必要があります。

**HookOperationName=ClearMountConfig**

この手順では、システムの更新ワークフロー中にボリュームクローンを削除するAnsibleプレイブックを実行します。

ボリューム名は、マウント構成ファイルとカスタムプロパティを通じてSAP LaMaから引き継がれます `ClonePostFix` および `SnapPostFix` は、システムプロビジョニングワークフローで最初に指定されたパラメータの値を渡すために使用します。

ボリューム名がXMLファイルから抽出され、各ボリュームに対してAnsibleのクローニングプレイブックが実行されます。

この例では、ASインスタンスと中央サービスは同じボリュームを共有します。そのため、ボリュームの削除はSAPインスタンス番号がの場合にのみ実行されます ($SAPSYSTEM）はではありません 01。これは他の環境とは異なる場合があるため、変更する必要があります。

```
root@sap-jump:~# cat /usr/sap/scripts/netapp_clone.sh
#!/bin/bash
#Section - Variables
########################################
VERSION="Version 0.9"
#Path for ansible play-books
ANSIBLE_PATH=/usr/sap/scripts/ansible
#Values for Ansible Inventory File
PRIMARY_CLUSTER=grenada
PRIMARY_SVM=svm-sap01
PRIMARY_KEYFILE=/usr/sap/scripts/ansible/certs/ontap.key
PRIMARY_CERTFILE=/usr/sap/scripts/ansible/certs/ontap.pem
#Default Variable if PARAM ClonePostFix / SnapPostFix is not maintained in
LaMa
DefaultPostFix=_clone_1
#TMP Files - used during execution
YAML_TMP=/tmp/inventory_ansible_clone_tmp_$$.yml
TMPFILE=/tmp/tmpfile.$$
MY_NAME="`basename $0`"
BASE_SCRIPT_DIR="`dirname $0`"
#Sendig Script Version and run options to LaMa Log
echo "[DEBUG]: Running Script $MY_NAME $VERSION"
echo "[DEBUG]: $MY_NAME $@"
#Command declared in the netapp_clone.conf Provider definition
#Command: /usr/sap/scripts/netapp_clone.sh
--HookOperationName=$[HookOperationName] --SAPSYSTEMNAME=$[SAPSYSTEMNAME]
--SAPSYSTEM=$[SAPSYSTEM] --MOUNT_XML_PATH=$[MOUNT_XML_PATH]
--PARAM_ClonePostFix=$[PARAM-ClonePostFix] --PARAM_SnapPostFix=$[PARAM
-SnapPostFix] --PROP_ClonePostFix=$[PROP-ClonePostFix]
--PROP_SnapPostFix=$[PROP-SnapPostFix]
--SAP_LVM_SRC_SID=$[SAP_LVM_SRC_SID]
--SAP_LVM_TARGET_SID=$[SAP_LVM_TARGET_SID]
#Reading Input Variables hand over by LaMa
for i in "$@"
do
case $i in
--HookOperationName=*)
HookOperationName="${i#*=}";shift;;
--SAPSYSTEMNAME=*)
SAPSYSTEMNAME="${i#*=}";shift;;
--SAPSYSTEM=*)
```

```
SAPSYSTEM="${i#*=}";shift;;
--MOUNT_XML_PATH=*)
MOUNT_XML_PATH="${i#*=}";shift;;
--PARAM_ClonePostFix=*)
PARAM_ClonePostFix="${i#*=}";shift;;
--PARAM_SnapPostFix=*)
PARAM_SnapPostFix="${i#*=}";shift;;
--PROP_ClonePostFix=*)
PROP_ClonePostFix="${i#*=}";shift;;
--PROP_SnapPostFix=*)
PROP_SnapPostFix="${i#*=}";shift;;
--SAP_LVM_SRC_SID=*)
SAP_LVM_SRC_SID="${i#*=}";shift;;
--SAP_LVM_TARGET_SID=*)
SAP_LVM_TARGET_SID="${i#*=}";shift;;
*)
# unknown option
;;
esac
done
#If Parameters not provided by the User - defaulting to DefaultPostFix
if [ -z $PARAM_ClonePostFix ]; then PARAM_ClonePostFix=$DefaultPostFix;fi
if [ -z $PARAM_SnapPostFix ]; then PARAM_SnapPostFix=$DefaultPostFix;fi
#Section - Functions
########################################
#Function Create (Inventory) YML File
########################################
create_yml_file()
{
echo "ontapservers:">$YAML_TMP
echo " hosts:">>$YAML_TMP
echo "  ${PRIMARY_CLUSTER}:">>$YAML_TMP
echo "   ansible_host: "'"'$PRIMARY_CLUSTER'"'">>$YAML_TMP
echo "   keyfile: "'"'$PRIMARY_KEYFILE'"'">>$YAML_TMP
echo "   certfile: "'"'$PRIMARY_CERTFILE'"'">>$YAML_TMP
echo "   svmname: "'"'$PRIMARY_SVM'"'">>$YAML_TMP
echo "   datavolumename: "'"'$datavolumename'"'">>$YAML_TMP
echo "   snapshotpostfix: "'"'$snapshotpostfix'"'">>$YAML_TMP
echo "   clonepostfix: "'"'$clonepostfix'"'">>$YAML_TMP
}
#Function run ansible-playbook
########################################
run_ansible_playbook()
{
echo "[DEBUG]: Running ansible playbook
netapp_lama_${HookOperationName}.yml on Volume $datavolumename"
```

```
ansible-playbook -i $YAML_TMP
$ANSIBLE_PATH/netapp_lama_${HookOperationName}.yml
}
#Section - Main
########################################
#HookOperationName - CloneVolumes
########################################
if [ $HookOperationName = CloneVolumes ] ;then
#save mount xml for later usage - used in Section FinalizeCloneVolues to
generate the mountpoints
echo "[DEBUG]: saving mount config...."
cp $MOUNT_XML_PATH /tmp/mount_config_${SAPSYSTEMNAME}_${SAPSYSTEM}.xml
#Instance 00 + 01 share the same volumes - clone needs to be done once
if [ $SAPSYSTEM != 01 ]; then
#generating Volume List - assuming usage of qtrees - "IP-
Adress:/VolumeName/qtree"
xmlFile=/tmp/mount_config_${SAPSYSTEMNAME}_${SAPSYSTEM}.xml
if [ -e $TMPFILE ];then rm $TMPFILE;fi
numMounts=`xml_grep --count "/mountconfig/mount" $xmlFile | grep "total: "
| awk '{ print $2 }'`
i=1
while [ $i -le $numMounts ]; do
     xmllint --xpath "/mountconfig/mount[$i]/exportpath/text()" $xmlFile
|awk -F"/" '{print $2}' >>$TMPFILE
i=$((i + 1))
done
DATAVOLUMES=`cat  $TMPFILE |sort -u`
#Create yml file and rund playbook for each volume
for I in $DATAVOLUMES; do
datavolumename="$I"
snapshotpostfix="$PARAM_SnapPostFix"
clonepostfix="$PARAM_ClonePostFix"
create_yml_file
run_ansible_playbook
done
else
echo "[DEBUG]: Doing nothing .... Volume cloned in different Task"
fi
fi
#HookOperationName - PostCloneVolumes
########################################
if [ $HookOperationName = PostCloneVolumes] ;then
#Reporting Properties back to LaMa Config for Cloned System
echo "[RESULT]:Property:ClonePostFix=$PARAM_ClonePostFix"
echo "[RESULT]:Property:SnapPostFix=$PARAM_SnapPostFix"
#Create MountPoint Config for Cloned Instances and report back to LaMa
```

```
according to SAP Note: https://launchpad.support.sap.com/#/notes/1889590
echo "MountDataBegin"
echo '<?xml version="1.0" encoding="UTF-8"?>'
echo "<mountconfig>"
xmlFile=/tmp/mount_config_${SAPSYSTEMNAME}_${SAPSYSTEM}.xml
numMounts=`xml_grep --count "/mountconfig/mount" $xmlFile | grep "total: "
| awk '{ print $2 }'`
i=1
while [ $i -le $numMounts ]; do
MOUNTPOINT=`xmllint --xpath "/mountconfig/mount[$i]/mountpoint/text()"
$xmlFile`;
        EXPORTPATH=`xmllint --xpath
"/mountconfig/mount[$i]/exportpath/text()" $xmlFile`;
        OPTIONS=`xmllint --xpath "/mountconfig/mount[$i]/options/text()"
$xmlFile`;
#Adopt Exportpath and add Clonepostfix - assuming usage of qtrees - "IP-
Adress:/VolumeName/qtree"
TMPFIELD1=`echo $EXPORTPATH|awk -F":/" '{print $1}'`
TMPFIELD2=`echo $EXPORTPATH|awk -F"/" '{print $2}'`
TMPFIELD3=`echo $EXPORTPATH|awk -F"/" '{print $3}'`
EXPORTPATH=$TMPFIELD1":/"${TMPFIELD2}$PARAM_ClonePostFix"/"$TMPFIELD3
echo -e '\t<mount fstype="nfs" storagetype="NETFS">'
echo -e "\t\t<mountpoint>${MOUNTPOINT}</mountpoint>"
echo -e "\t\t<exportpath>${EXPORTPATH}</exportpath>"
echo -e "\t\t<options>${OPTIONS}</options>"
echo -e "\t</mount>"
i=$((i + 1))
done
echo "</mountconfig>"
echo "MountDataEnd"
#Finished MountPoint Config
#Cleanup Temporary Files
rm $xmlFile
fi
#HookOperationName – ServiceConfigRemoval
########################################
if [ $HookOperationName = ServiceConfigRemoval ] ;then
#Assure that Properties ClonePostFix and SnapPostfix has been configured
through the provisioning process
if [ -z $PROP_ClonePostFix ]; then echo "[ERROR]: Propertiy ClonePostFix
is not handed over - please investigate";exit 5;fi
if [ -z $PROP_SnapPostFix ]; then echo "[ERROR]: Propertiy SnapPostFix is
not handed over - please investigate";exit 5;fi
#Instance 00 + 01 share the same volumes - clone delete needs to be done
once
if [ $SAPSYSTEM != 01 ]; then
```

```
#generating Volume List - assuming usage of qtrees - "IP-
Adress:/VolumeName/qtree"
xmlFile=$MOUNT_XML_PATH
if [ -e $TMPFILE ];then rm $TMPFILE;fi
numMounts=`xml_grep --count "/mountconfig/mount" $xmlFile | grep "total: "
| awk '{ print $2 }'`
i=1
while [ $i -le $numMounts ]; do
     xmllint --xpath "/mountconfig/mount[$i]/exportpath/text()" $xmlFile
|awk -F"/" '{print $2}' >>$TMPFILE
i=$((i + 1))
done
DATAVOLUMES=`cat  $TMPFILE |sort -u| awk -F $PROP_ClonePostFix '{ print $1
}'`
#Create yml file and rund playbook for each volume
for I in $DATAVOLUMES; do
datavolumename="$I"
snapshotpostfix="$PROP_SnapPostFix"
clonepostfix="$PROP_ClonePostFix"
create_yml_file
run_ansible_playbook
done
else
echo "[DEBUG]: Doing nothing .... Volume deleted in different Task"
fi
#Cleanup Temporary Files
rm $xmlFile
fi
#HookOperationName - ClearMountConfig
########################################
if [ $HookOperationName = ClearMountConfig ] ;then
        #Assure that Properties ClonePostFix and SnapPostfix has been
configured through the provisioning process
        if [ -z $PROP_ClonePostFix ]; then echo "[ERROR]: Propertiy
ClonePostFix is not handed over - please investigate";exit 5;fi
        if [ -z $PROP_SnapPostFix ]; then echo "[ERROR]: Propertiy
SnapPostFix is not handed over - please investigate";exit 5;fi
        #Instance 00 + 01 share the same volumes - clone delete needs to
be done once
        if [ $SAPSYSTEM != 01 ]; then
                #generating Volume List - assuming usage of qtrees - "IP-
Adress:/VolumeName/qtree"
                xmlFile=$MOUNT_XML_PATH
                if [ -e $TMPFILE ];then rm $TMPFILE;fi
                numMounts=`xml_grep --count "/mountconfig/mount" $xmlFile
| grep "total: " | awk '{ print $2 }'`
```

```
                i=1
                while [ $i -le $numMounts ]; do
                        xmllint --xpath
"/mountconfig/mount[$i]/exportpath/text()" $xmlFile |awk -F"/" '{print
$2}' >>$TMPFILE
                        i=$((i + 1))
                done
                DATAVOLUMES=`cat  $TMPFILE |sort -u| awk -F
$PROP_ClonePostFix '{ print $1 }'`
                #Create yml file and rund playbook for each volume
                for I in $DATAVOLUMES; do
                        datavolumename="$I"
                        snapshotpostfix="$PROP_SnapPostFix"
                        clonepostfix="$PROP_ClonePostFix"
                        create_yml_file
                        run_ansible_playbook
                done
        else
                echo "[DEBUG]: Doing nothing .... Volume deleted in
different Task"
        fi
        #Cleanup Temporary Files
        rm $xmlFile
fi
#Cleanup
########################################
#Cleanup Temporary Files
if [ -e $TMPFILE ];then rm $TMPFILE;fi
if [ -e $YAML_TMP ];then rm $YAML_TMP;fi
exit 0
```

**Ansible Playbook：NetApp_LaMa _CloneVolume.yml**

LaMaシステムのクローニングワークフローのCloneVolumesの手順で実行されるPlaybookは、を組み合わせたものです `create_snapshot.yml` および `create_clone.yml` （を参照） "NetApp Ansibleモジュール-YAMLファイル"）。このプレイブックは、セカンダリからのクローニング処理やクローンスプリット処理など、他のユースケースにも簡単に対応できます。

```
root@sap-jump:~# cat /usr/sap/scripts/ansible/netapp_lama_CloneVolumes.yml
---
- hosts: ontapservers
  connection: local
  collections:
    - netapp.ontap
  gather_facts: false
  name: netapp_lama_CloneVolumes
  tasks:
  - name: Create SnapShot
    na_ontap_snapshot:
      state: present
      snapshot: "{{ datavolumename }}{{ snapshotpostfix }}"
      use_rest: always
      volume: "{{ datavolumename }}"
      vserver: "{{ svmname }}"
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
  - name: Clone Volume
    na_ontap_volume_clone:
      state: present
      name: "{{ datavolumename }}{{ clonepostfix }}"
      use_rest: always
      vserver: "{{ svmname }}"
      junction_path: '/{{ datavolumename }}{{ clonepostfix }}'
      parent_volume: "{{ datavolumename }}"
      parent_snapshot: "{{ datavolumename }}{{ snapshotpostfix }}"
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
```

**Ansible Playbook：NetApp_LaMa _ServiceConfigRemoval.yml**

実行されるプレイブック `ServiceConfigRemoval` LaMaシステムの破棄ワークフローのフェーズは、のフェーズです `delete_clone.yml` および `delete_snapshot.yml` （を参照） "NetApp Ansibleモジュール-YAMLファイル"）。の実行ステップに合わせて調整する必要があります `netapp_lama_CloneVolumes` Playbook：

```
root@sap-jump:~# cat
/usr/sap/scripts/ansible/netapp_lama_ServiceConfigRemoval.yml
---
- hosts: ontapservers
  connection: local
  collections:
    - netapp.ontap
  gather_facts: false
  name: netapp_lama_ServiceConfigRemoval
  tasks:
  - name: Delete Clone
    na_ontap_volume:
      state: absent
      name: "{{ datavolumename }}{{ clonepostfix }}"
      use_rest: always
      vserver: "{{ svmname }}"
      wait_for_completion: True
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
  - name: Delete SnapShot
    na_ontap_snapshot:
      state: absent
      snapshot: "{{ datavolumename }}{{ snapshotpostfix }}"
      use_rest: always
      volume: "{{ datavolumename }}"
      vserver: "{{ svmname }}"
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
root@sap-jump:~#
```

**Ansible Playbook：NetApp_LaMa _ClearMountConfig.yml**

プレイブックは、の実行時に指定します `netapp_lama_ClearMountConfig` LaMaシステムの更新ワークフローのフェーズは、のフェーズです `delete_clone.yml` および `delete_snapshot.yml` （を参照）"NetApp Ansibleモジュール- YAMLファイル"）。の実行ステップに合わせて調整する必要があります `netapp_lama_CloneVolumes` Playbook：

```
root@sap-jump:~# cat
/usr/sap/scripts/ansible/netapp_lama_ServiceConfigRemoval.yml
---
- hosts: ontapservers
  connection: local
  collections:
    - netapp.ontap
  gather_facts: false
  name: netapp_lama_ServiceConfigRemoval
  tasks:
  - name: Delete Clone
    na_ontap_volume:
      state: absent
      name: "{{ datavolumename }}{{ clonepostfix }}"
      use_rest: always
      vserver: "{{ svmname }}"
      wait_for_completion: True
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
  - name: Delete SnapShot
    na_ontap_snapshot:
      state: absent
      snapshot: "{{ datavolumename }}{{ snapshotpostfix }}"
      use_rest: always
      volume: "{{ datavolumename }}"
      vserver: "{{ svmname }}"
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
root@sap-jump:~#
```

**Ansibleのinventory.ymlの例**

このインベントリファイルは、ワークフローの実行時に動的に作成されます。このファイルは、説明のためにのみここに表示されています。

```
ontapservers:
 hosts:
  grenada:
   ansible_host: "grenada"
   keyfile: "/usr/sap/scripts/ansible/certs/ontap.key"
   certfile: "/usr/sap/scripts/ansible/certs/ontap.pem"
   svmname: "svm-sap01"
   datavolumename: "HN9_sap"
   snapshotpostfix: " _snap_20221115"
   clonepostfix: "_clone_20221115"
```

## まとめ

Ansibleなどの最新の自動化フレームワークがSAP LaMaプロビジョニングワークフローに統合されているため、柔軟な解決策 を利用して、標準的なインフラや複雑なインフラ要件に対応できます。

### 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。

- NetAppネームスペース内のコレクション

  "https://docs.ansible.com/ansible/latest/collections/netapp/index.html"

- AnsibleとAnsibleのPlaybookのサンプルに関するドキュメント

  "https://github.com/sap-linuxlab/demo.netapp_ontap"

- Ansibleとネットアップの統合

  "https://www.ansible.com/integrations/infrastructure/netapp"

- SAP LaMaとAnsibleの統合に関するブログ

  "https://blogs.sap.com/2020/06/08/outgoing-api-calls-from-sap-landscape-management-lama-with-automation-studio/"

- SAP Landscape Management 3.0, Enterprise Edition Documentation

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/4df88a8f418c5059e10000000a42189c.html#loio4df88a8f418c5059e10000000a42189c"

- SAP LaMaのドキュメント–プロバイダの定義

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/bf6b3e43340a4cbcb0c0f3089715c068.html"

- SAP LaMaドキュメント-カスタムフック

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/139eca2f925e48738a20dbf0b56674c5.html"

- SAP LaMaドキュメント-「Configuring SAP Host Agent Registered Scripts

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/250dfc5eef4047a38bab466c295d3a49.html"

- SAP LaMaドキュメント-カスタム運用とカスタムフックのパラメータ

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/0148e495174943de8c1c3ee1b7c9cc65.html"

- SAP LaMaドキュメント-アダプティブデザイン

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/737a99e86f8743bdb8d1f6cf4b862c79.html"

- ネットアップの製品マニュアル

  "https://www.netapp.com/support-and-training/documentation/"

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 | 2023年1月 | 初版リリース |

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

今日のダイナミックなビジネス環境では、企業は継続的なイノベーションを提供し、変化する市場に迅速に対応する必要があります。このような競争の激しい状況下で、業務プロセスの柔軟性を高める企業は、市場の需要に効果的に対応できます。

作成者：Nils Bauer、NetApp

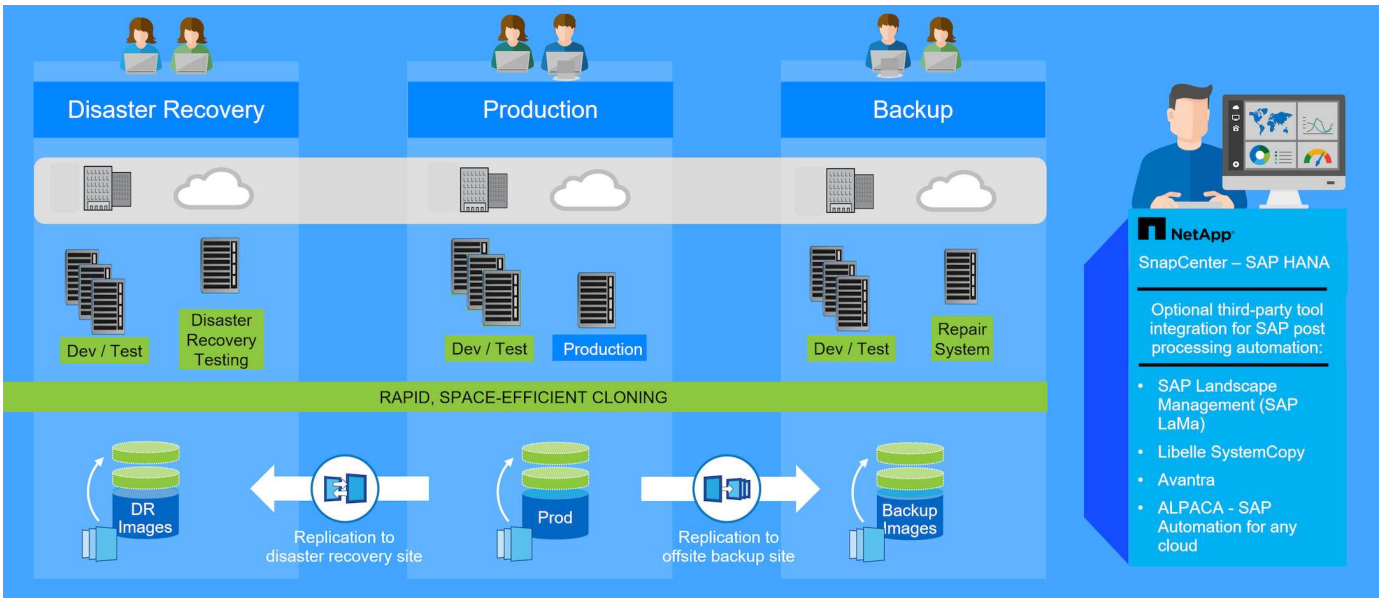
はじめに

市場ニーズの変化は、企業のSAP環境にも影響を及ぼし、定期的な統合、変更、更新が必要になります。IT部門は、これらの変更を、より少ないリソースでより短い期間で実装する必要があります。変更を導入する際のリスクを最小限に抑えるには、本番環境の実際のデータを使用するSAPシステムを追加で必要とする、テストとトレーニングを徹底的に実施する必要があります。

従来のSAPライフサイクル管理アプローチでは、このようなシステムは主に手動プロセスに基づいてプロビジョニングされます。このような手動プロセスは、ミスを避けられず、時間もかかることが多く、イノベーショ

ンの遅れやビジネス要件への対応の遅れにつながります。

次の図に示すように、SAP HANAデータベースとライフサイクル管理ツールにSAPのライフサイクル管理を最適化するネットアップのソリューションが統合されています。効率的なアプリケーション統合データプロテクションに、SAPのテストシステムを柔軟にプロビジョニングすることができます。これらのソリューションは、オンプレミスのSAP HANAにも、Azure NetApp Files（ANF）やAmazon FSx for NetApp ONTAP（FSx for ONTAP）のクラウドで実行されているSAP HANAにも対応しています。




アプリケーションと統合された**Snapshot**バックアップ処理

アプリケーションと整合性のあるSnapshotバックアップをストレージレイヤで作成する機能は、本ドキュメントで説明するシステムコピー処理とシステムクローニング処理の基盤となります。ストレージベースのSnapshotバックアップは、SAP HANA用のNetApp SnapCenter プラグインと、SAP HANAデータベースが提供するインターフェイスを使用して作成します。SnapCenter は、SnapshotバックアップをSAP HANAバックアップカタログに登録して、リストアやリカバリ、クローニング処理に使用できるようにします。

オフサイトのバックアップおよび/または災害復旧データのレプリケーション

アプリケーションと整合性のあるSnapshotバックアップを、ストレージレイヤから、SnapCenter の制御下にあるオフサイトのバックアップサイトやディザスタリカバリサイトにレプリケートします。レプリケーションは変更されたブロックと新しいブロックに基づいて行われるため、スペースと帯域幅の効率が向上します。

任意の**Snapshot**バックアップを**SAP**システムのコピーやクローン処理に使用

ネットアップのテクノロジとソフトウェアの統合により、ソースシステムのSnapshotバックアップを利用してSAPシステムのコピーやクローニングを実行することができます。このSnapshotバックアップは、SAP本番用システムと同じストレージ、オフサイトのバックアップ用ストレージ、またはディザスタリカバリサイトのストレージから選択できます。この柔軟性により、必要に応じて開発用システムとテスト用システムを本番用システムと分離し、ディザスタリカバリサイトでのディザスタリカバリのテストなど、さまざまなシナリオに対応することができます。

オフサイトのバックアップストレージやディザスタリカバリストレージからのクローニングは、オンプレミスのNetAppシステムとAmazon FSx for NetApp ONTAPでサポートされます。Azure NetApp Filesを使用する場合、クローンはソースボリュームにのみ作成できます。

SAPテストシステムのプロビジョニングにはさまざまなシナリオとユースケースがあり、自動化のレベルに関してもさまざまな要件が存在する場合があります。ネットアップのSAP向けソフトウェア製品は、SAPのデータベースやライフサイクル管理製品と統合されているため、さまざまなシナリオや自動化のレベルに対応できます。

NetApp SnapCenter とSAP HANA向けプラグインを使用して、アプリケーションと整合性のあるSnapshotバックアップに基づいて必要なストレージボリュームをプロビジョニングし、開始されたSAP HANAデータベースまで、必要なホストおよびデータベースのすべての処理を実行します。SAPシステムのコピー、システムクローン、システムの更新、SAPのポストプロセスなどの追加の手動手順が必要になる場合があります。詳細については、次のセクションで説明します。

SAPテストシステムのプロビジョニングは、サードパーティのツールを使用してNetAppの機能を統合することで、完全に自動化されたエンドツーエンドで実行できます。詳細については、次のサイトを参照してください。

"TR-4953：『NetApp SAP Landscape Management Integration using Ansible』"

"TR-4929：『Automating SAP system copy operations with Libelle SystemCopy』（netapp.com）"

"AlpacaとNetApp SnapCenterを使用したSAPシステムのコピーとクローンワークフローの自動化"

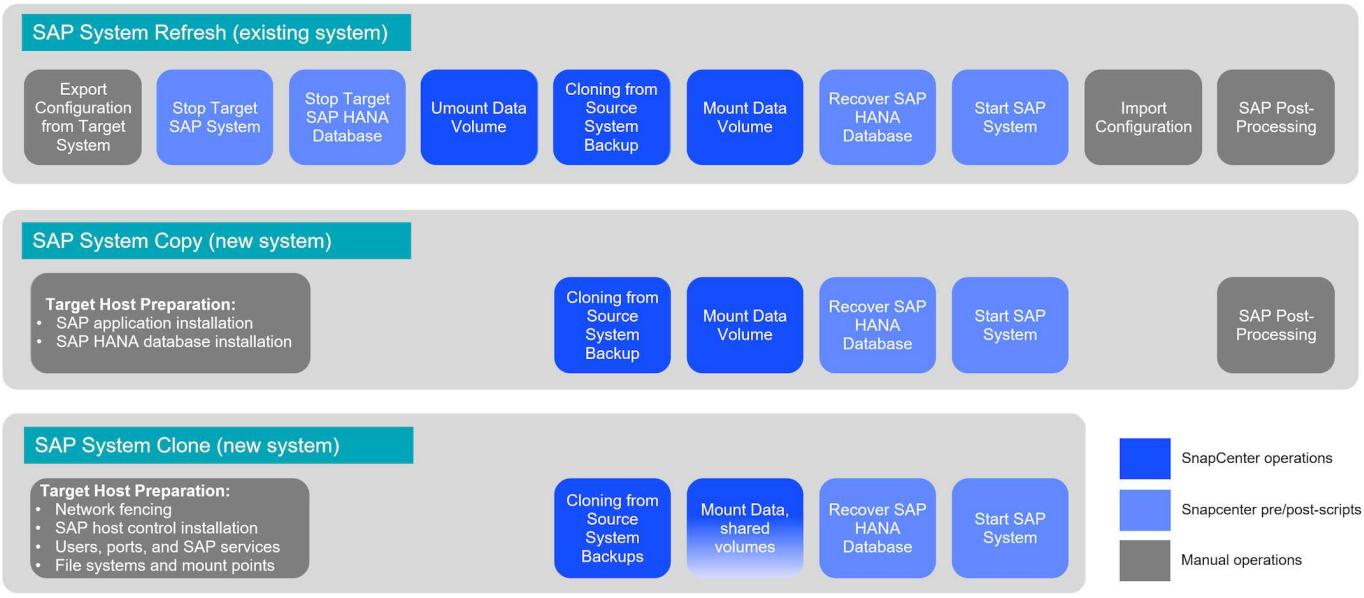
"AvantraとNetApp SnapCenterを使用したSAPシステムのコピーとクローンワークフローの自動化"

## SAPシステムのコピー、更新、クローニングのシナリオ

SAPシステムの更新、SAPシステムのコピー、SAPシステムのクローニングの3つのプロセスの同義語としてよく使用されます。ワークフローとユースケースはそれぞれ異なるため、異なる処理を区別することが重要です。

- * SAPシステムの更新。* SAPシステムの更新は、ソースSAPシステムのデータを使用した既存のターゲットSAPシステムの更新です。ターゲットシステムは、通常、品質管理システムなどのSAP転送環境の一部であり、本番用システムのデータで更新されます。ソース・システムとターゲット・システムでは、ホスト名、インスタンス番号、およびSIDが異なります。
- * SAPシステムのコピー。* SAPシステムのコピーとは、ソースSAPシステムのデータを含む新しいターゲットSAPシステムのセットアップを指します。たとえば、本番用システムのデータを含む追加のテストシステムを新しいターゲットシステムとして使用できます。ソース・システムとターゲット・システムでは、ホスト名、インスタンス番号、およびSIDが異なります。
- * SAPシステムのクローン。* SAPシステムのクローンは、ソースSAPシステムの同一クローンです。SAPシステムクローンは、一般に論理的な破損に対処したり、ディザスタリカバリのシナリオをテストしたりするのに使用されます。システムのクローニング処理では、ホスト名、インスタンス番号、およびSIDの値は変更されません。そのため、本番環境と通信できないように、ターゲットシステムの適切なネットワークフェンシングを設定することが重要です。

次の図は、システム更新、システムコピー、またはシステムクローンの処理中に実行する必要がある主な手順を示しています。青のボックスはSnapCenterで自動化できる手順を示し、グレーのボックスは手動またはサードパーティのツールを使用してSnapCenter以外で実行する必要がある手順を示します。

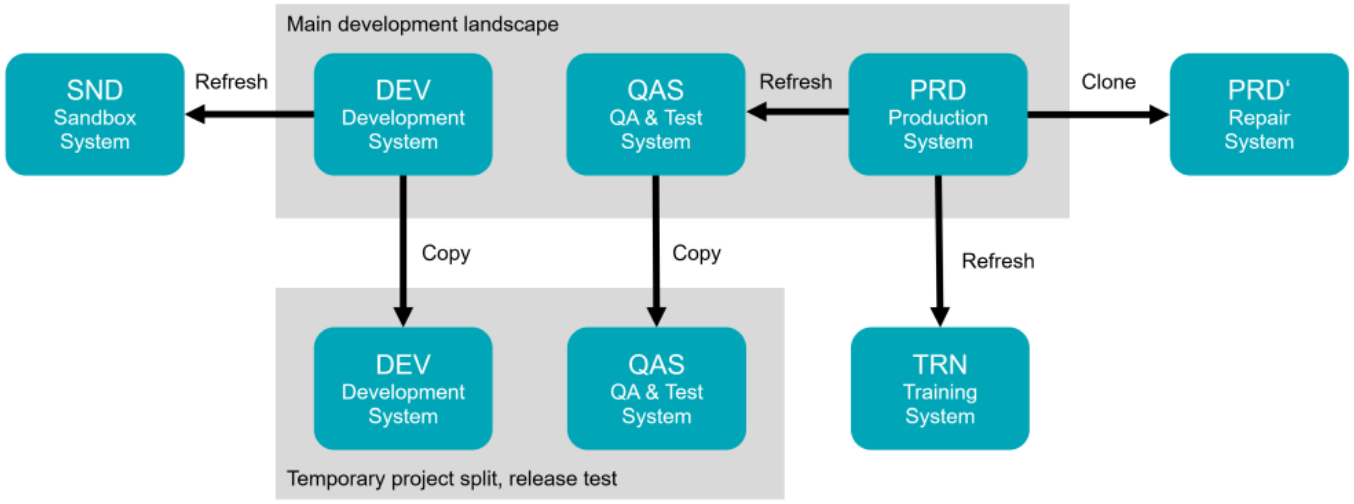



## システムの更新とクローニングのユースケース

SAPのライフサイクル管理を最適化するNetAppソリューションは、SAP HANAデータベースとライフサイクル管理ツールに統合されており、効率的なアプリケーション統合データプロテクションと、SAPテストシステムの柔軟なプロビジョニングが組み合わされています。

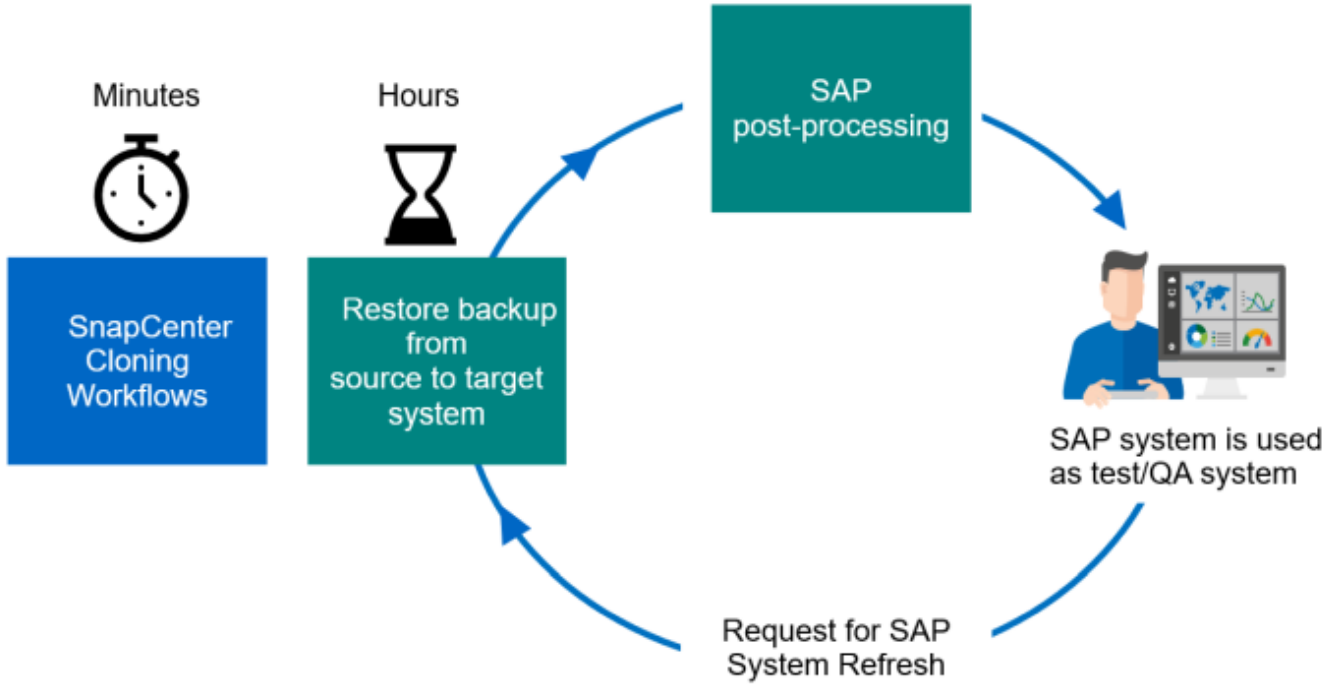
### QA、テスト、サンドボックス、トレーニングシステムのデータ更新

テストやトレーニングの目的で、ソースシステムのデータをターゲットシステムで使用できるようにする必要があるシナリオは複数あります。テストおよびトレーニング用のシステムは、ソースシステムのデータで定期的に更新し、現在のデータセットでテストとトレーニングが実行されていることを確認する必要があります。このシステム更新処理は、インフラ、データベース、アプリケーションの各レイヤ上で実行される複数のタスクで構成されます。自動化のレベルによっては、数日かかる場合があります。




SnapCenterクローニングのワークフローを使用すると、インフラレイヤとデータベースレイヤで必要なタスクを高速化、自動化できます。SnapCenterでは、ソースシステムからターゲットシステムにバックアップをリストアする代わりに、NetApp SnapshotコピーとNetApp FlexCloneテクノロジを使用しているため、起動し

たSAP HANAデータベースに必要なタスクを数時間ではなく数分で実行できます。クローニングプロセスに要する時間はデータベースのサイズに左右されないため、非常に大規模なシステムでも数分で作成できます。起動時間は、データベースのサイズ、およびデータベースサーバとストレージシステム間の接続によって異なります。




システム更新処理のワークフローについては、を参照してください。"「SnapCenter でSAP HANAシステムを更新」"

論理的破損に対処する

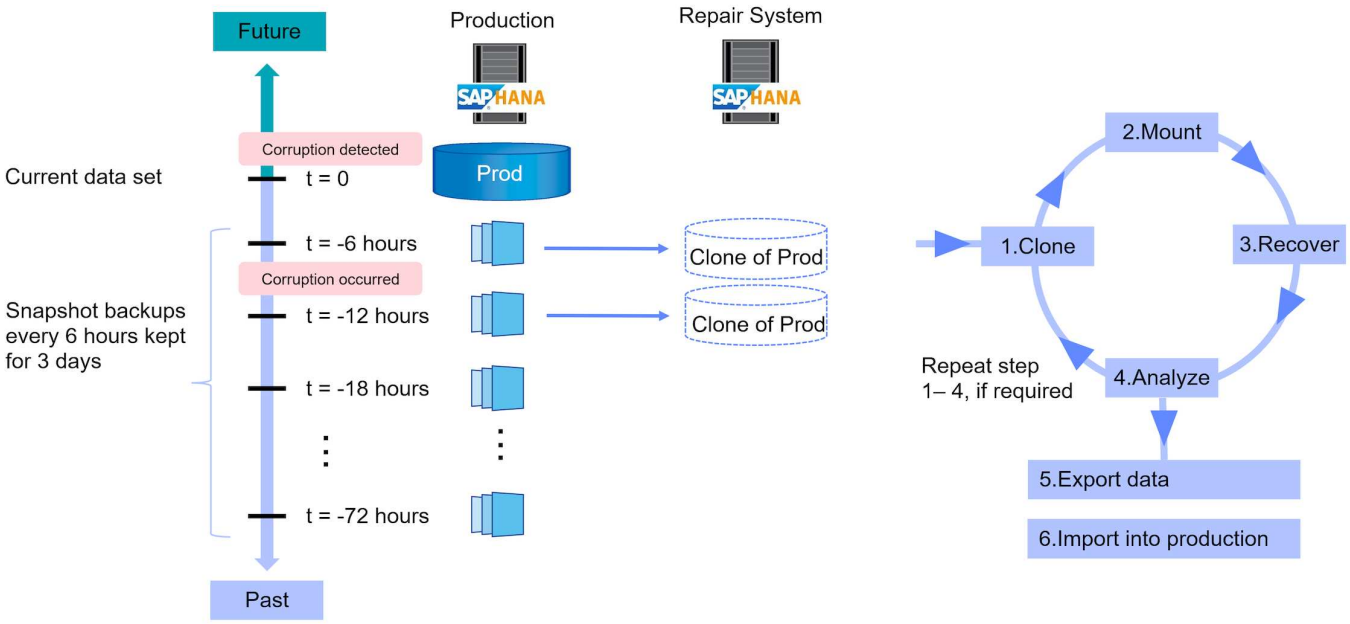
論理的破損は、ソフトウェアエラー、人為的エラー、破壊行為などが原因で発生する可能性があります。残念ながら、論理的破損は、標準的な高可用性ソリューションやディザスタリカバリソリューションでは対処できないことがよくあります。その結果、論理的な破損が発生したレイヤ、アプリケーション、ファイルシステム、またはストレージによっては、ダウンタイムを最小限に抑え、データ損失を最大化するための要件を満たすことができない場合があります。

最悪のケースは、SAPアプリケーションが論理的に破損した場合です。SAP アプリケーションは多くの場合、異なるアプリケーションが相互に通信してデータを交換する環境で動作します。このため、論理的な破損が発生した SAP システムはリストアとリカバリを実行しないことを推奨します。破損が発生する前の時点にシステムをリストアすると、データが失われます。また、 SAP ランドスケープは同期されず、さらにポストプロセスが必要になります。

SAPシステムをリストアする代わりに、別の修復システムで問題を分析して、システム内の論理エラーを修正する方法を推奨します。ルート原因分析には、ビジネスプロセスやアプリケーション所有者の関与が必要です。このシナリオでは、論理的破損が発生する前に格納されたデータに基づいて、修復システム（本番用システムのクローン）を作成します。リペアシステム内では、必要なデータをエクスポートし、本番システムにインポートできます。このアプローチでは、本番用システムを停止する必要はなく、最良のシナリオでは、データの損失だけでなく、ごくわずかなデータの損失も発生します。

リペアシステムを設定する際には、柔軟性と俊敏性が重要です。NetAppのストレージベースのSnapshotバッ

クアップを使用すると、NetApp FlexCloneテクノロジを使用して、複数の整合性のあるデータベースイメージを使用して本番用システムのクローンを作成できます。ファイルベースのバックアップからリダイレクトされたリストアを使用して修復システムを設定する場合、FlexCloneボリュームは数時間ではなく数秒で作成できます。



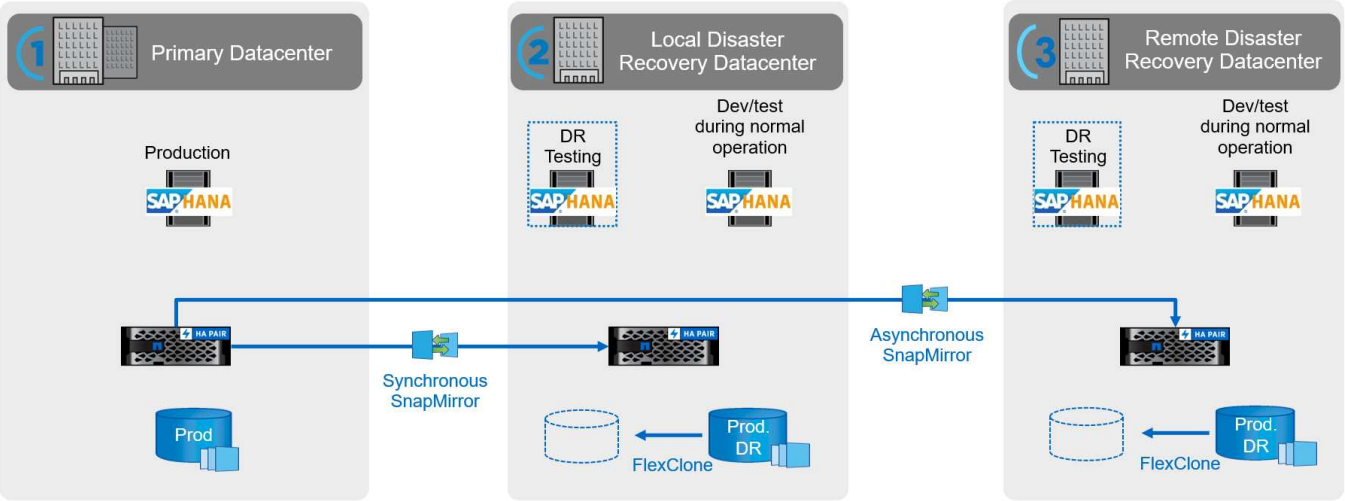

リペアシステムの作成ワークフローについては、のセクションを参照してください。"「SnapCenter を使用したSAPシステムのクローン作成」"

ディザスタリカバリのテスト

効果的なディザスタリカバリ戦略では、必要なワークフローをテストする必要があります。テストでは、戦略が機能するかどうか、および内部ドキュメントで十分かどうかを検証します。また、管理者は必要な手順をトレーニングすることもできます。

SnapMirrorを使用したストレージレプリケーションでは、RTOとRPOをリスクにさらすことなく、ディザスタリカバリのテストを実行できます。ディザスタリカバリテストは、データレプリケーションを中断することなく実行できます。

非同期SnapMirrorと同期SnapMirrorのディザスタリカバリテストでは、ディザスタリカバリターゲットでSnapshotバックアップとFlexCloneボリュームを使用します。




詳細な手順については、テクニカルレポートを参照してください。

"TR-4646：『SAP HANA Disaster Recovery with Storage Replication』（netapp.com）"

"TR-4891 ：『 SAP HANA disaster recovery with Azure NetApp Files 』"

## サポートされるインフラとシナリオ

このドキュメントでは、オンプレミスのNetAppシステム、Amazon FSx for NetApp ONTAPシステム、およびAzure NetApp Filesで実行されるSAP HANAシステムの更新とクローニングのシナリオについて説明します。ただし、すべてのストレージプラットフォームですべての機能とシナリオを使用できるわけではありません。次の表は、サポートされる構成をまとめたものです。

このドキュメントでは、オンプレミスのNetAppシステムで実行されるSAP HANAランドスケープを使用し、NFSをストレージプロトコルとして使用しています。ワークフローの手順のほとんどは、プラットフォームごとに同じです。違いがある場合は、このドキュメントで説明します。

| | オンプレミスの**NetApp**システム | *** AWS FSx for NetApp ONTAP *** | *** Azure NetApp Files *** |
|---|---|---|---|
| ストレージプロトコル | NFS、ファイバチャネル | NFS | NFS |
| シンクローン（FlexClone） | はい。 | はい。 | いいえ。現在のANFバージョンでは、クローンボリュームは常にスプリットされます。 |
| クローンスプリット処理 | はい。 | はい。 | N/A |
| フライマリカラノクロニンク | はい。 | はい。 | はい。 |
| オフサイトバックアップからのクローニング | はい。 | はい。 | いいえ |
| DRサイトでのクローニング | はい。 | はい。 | はい。ただしSnapCenterには統合されていません。 |

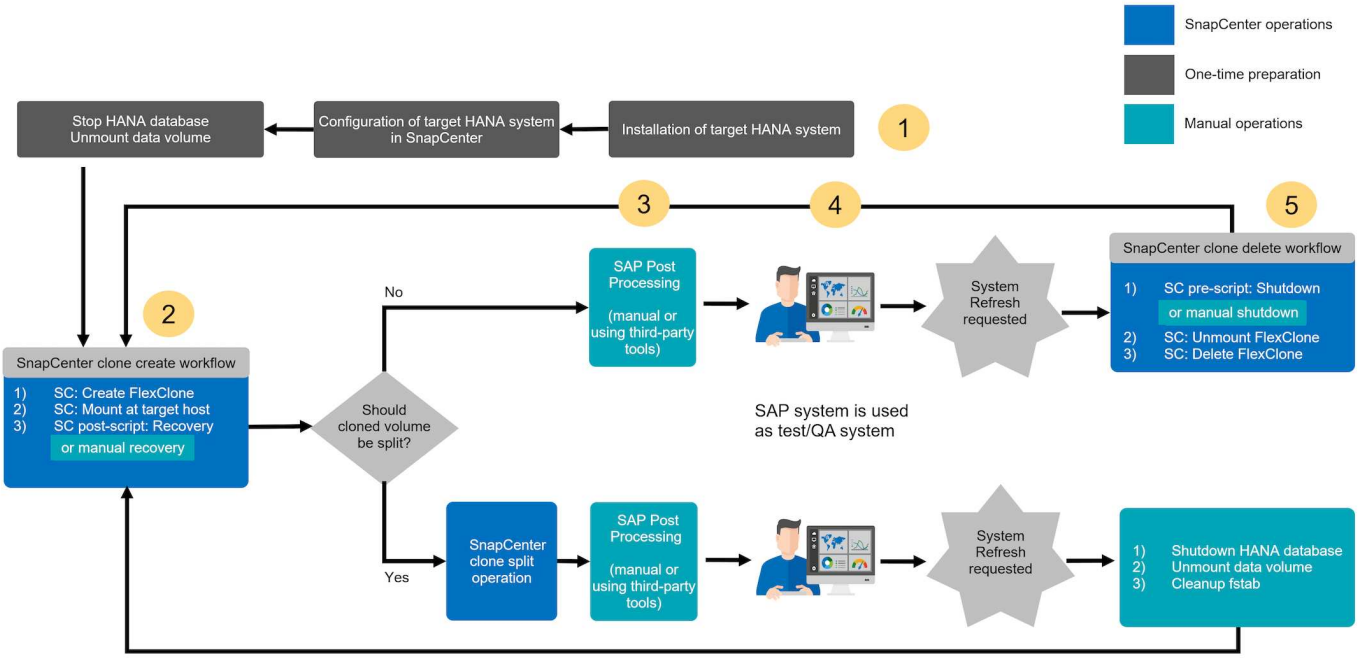
# SnapCenter を使用したSAPシステムの更新ワークフローの概要

SnapCenterには、既存のSnapshotバックアップからデータセットのクローンを管理するワークフローが用意されています。このクローンデータセットはFlexCloneボリュームで、ソースシステムからHANAデータボリュームを迅速にプロビジョニングしてターゲットシステムに接続するために使用できます。したがって、QA、テスト、サンドボックス、またはトレーニングシステムのシステム更新処理を実行する場合に最適です。

SnapCenter クローニングワークフローは、ストレージレイヤで必要なすべての処理を処理します。また、スクリプトを使用して拡張し、ホスト固有の処理とHANAデータベース固有の処理を実行することもできます。本ドキュメントでは、スクリプトを使用して、HANAデータベースのリカバリ処理とシャットダウン処理を実行します。SnapCenter ワークフローにスクリプトを使用してさらに自動化を進めることで、必要なHANAデータベースの処理はすべて処理されますが、SAPの後処理の手順については説明しません。SAPの後処理は、手動またはサードパーティのツールを使用して実行する必要があります。

SnapCenterを使用したSAPシステムの更新ワークフローは、次の図に示すように、主に5つの手順で構成されます。

1. ターゲットシステムの初回インストールと準備
    a. 新しいターゲットシステムにSnapCenter HANAプラグインをインストールし、SnapCenterでHANAシステムを設定する必要があります。
    b. ターゲットシステムを停止し、HANAデータボリュームをアンマウントする必要があります。
2. SnapCenterクローン作成ワークフロー
    a. SnapCenterがソースシステムの選択したSnapshotのFlexCloneボリュームを作成
    b. SnapCenterがターゲットシステムにFlexCloneボリュームをマウントする
    c. ターゲットのHANAデータベースのリカバリは、スクリプトをポストスクリプトとして使用して自動化することも、手動で実行することもできます `sc-system-refresh` 。
3. SAPの後処理（手動またはサードパーティのツールを使用）
4. これで、システムをテスト/QAシステムとして使用できるようになります。
5. 新しいシステム更新が要求されると、SnapCenterクローン削除ワークフローを使用してFlexCloneボリュームが削除されます。
    a. ターゲットのHANAシステムがSnapCenterで保護されている場合は、クローン削除ワークフローを開始する前に保護を削除する必要があります。
    b. HANAシステムは手動で停止するか、SnapCenterのプリスクリプトとしてスクリプトを使用して自動的に停止する必要があります。 `sc-system-refresh`
    c. SnapCenterがHANAデータボリュームをアンマウントする
    d. SnapCenterがFlexCloneボリュームを削除
    e. ステップ2でリフレッシュが再開されます。




ほとんどの場合、ターゲットテスト/QAシステムは少なくとも数週間使用されます。FlexCloneボリュームがソースシステムボリュームのSnapshotをブロックしているため、このSnapshotには、ソースシステムボリュームでのブロック変更率に基づいて追加の容量が必要になります。本番ソースシステムで1日あたりの平均変更率が20%の場合、ブロックされたSnapshotは5日後に100%に達します。そのため、NetAppでは、クローンが本番用のソースシステムに基づいている場合は、FlexCloneボリュームをすぐにスプリットするか、数日後にスプリットすることを推奨しています。クローンスプリット処理ではクローンボリュームの使用はブロックされないため、HANAデータベースの使用中にいつでも実行できます。

FlexCloneボリュームをスプリットすると、SnapCenter はターゲットシステムに作成されたすべてのバックアップを削除します。

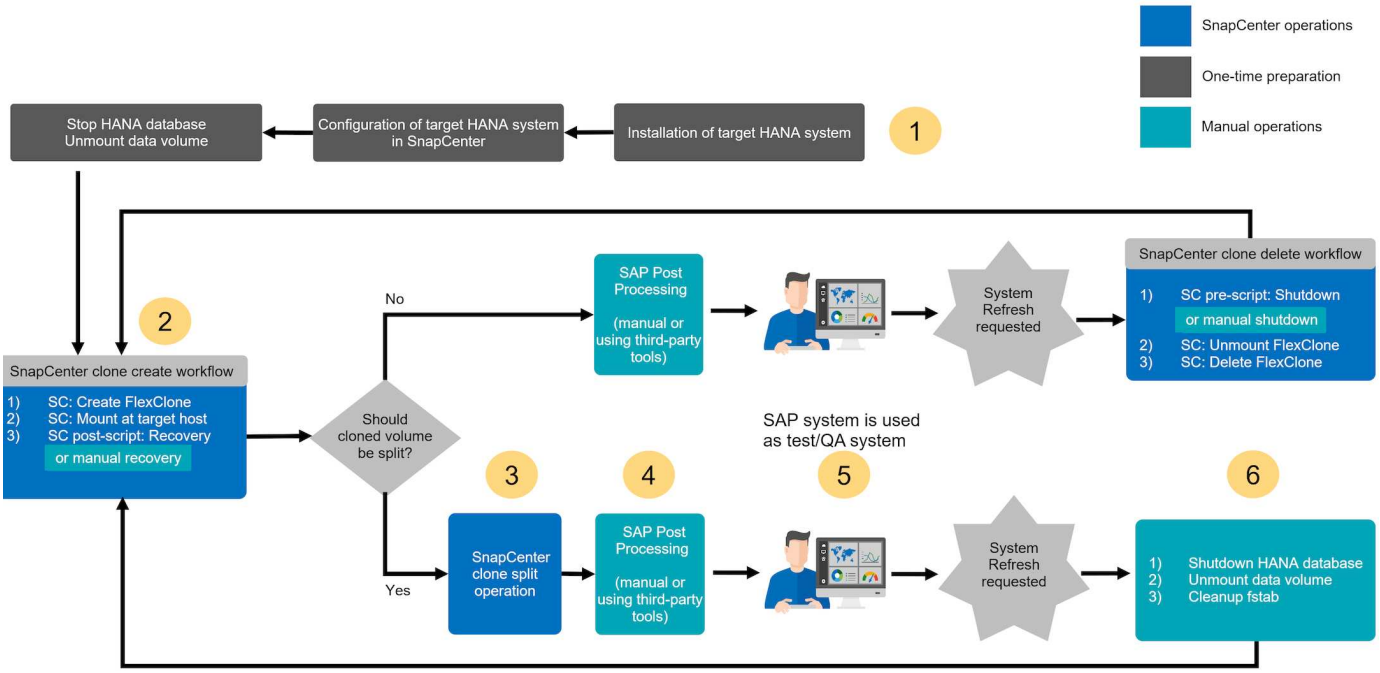
SnapCenterおよびAzure NetApp FilesでAzure NetApp Filesは、作成後に常にクローンがスプリットされるため、クローンスプリット処理は実行できません。

クローンスプリットを含む更新処理は、次の手順で構成されます。

1. ターゲットシステムの初回インストールと準備
   a. 新しいターゲットシステムにSnapCenter HANAプラグインをインストールし、SnapCenterでHANAシステムを設定する必要があります。
   b. ターゲットシステムを停止し、HANAデータボリュームをアンマウントする必要があります。
2. SnapCenterクローン作成ワークフロー
   a. SnapCenterがソースシステムの選択したSnapshotのFlexCloneボリュームを作成
   b. SnapCenterがターゲットシステムにFlexCloneボリュームをマウントする
   c. ターゲットのHANAデータベースのリカバリは、スクリプトをポストスクリプトとして使用して自動化することも、手動で実行することもできます `sc-system-refresh` 。
3. SnapCenterクローンスプリットワークフローを使用してFlexCloneボリュームをスプリットします。
4. SAPの後処理（手動またはサードパーティのツールを使用）

5. これで、システムをテスト/QAシステムとして使用できるようになります。
6. 新しいシステムの更新が要求されると、クリーンアップは次の手動手順で実行されます。
    a. ターゲットのHANAシステムがSnapCenterで保護されている場合は、保護を削除する必要があります。
    b. HANAシステムを手動で停止する必要がある
    c. HANAデータボリュームをアンマウントし、SnapCenterからfstabエントリを削除する（手動タスク）
    d. ステップ2でリフレッシュが再開されます。

> 以前にスプリットされていた古いデータボリュームは、ストレージシステムで手動で削除する必要があります。




このセクションでは"「SnapCenter でSAP HANAシステムを更新」"、両方のシステム更新ワークフローについて、詳細なステップバイステップで説明します。

## SnapCenter を使用したSAPシステムのクローニングワークフローの概要

前のセクションで説明したように、SnapCenter は、任意の既存のSnapshotバックアップからデータセットのクローンを管理し、これらのデータセットを任意のターゲットシステムに迅速にプロビジョニングできます。論理的な破損に対処するために本番データをリペアシステムに柔軟かつ迅速にプロビジョニングすることは、リペアシステムをリセットして別の本番データセットを選択する必要があることが多いため、非常に重要です。FlexCloneテクノロジを使用すると、修復システムは通常短時間しか使用されないため、高速なプロビジョニングプロセスが可能になり、容量を大幅に削減できます。

次の図は、SnapCenterを使用したSAPシステムのクローニング処理に必要な手順をまとめたものです。

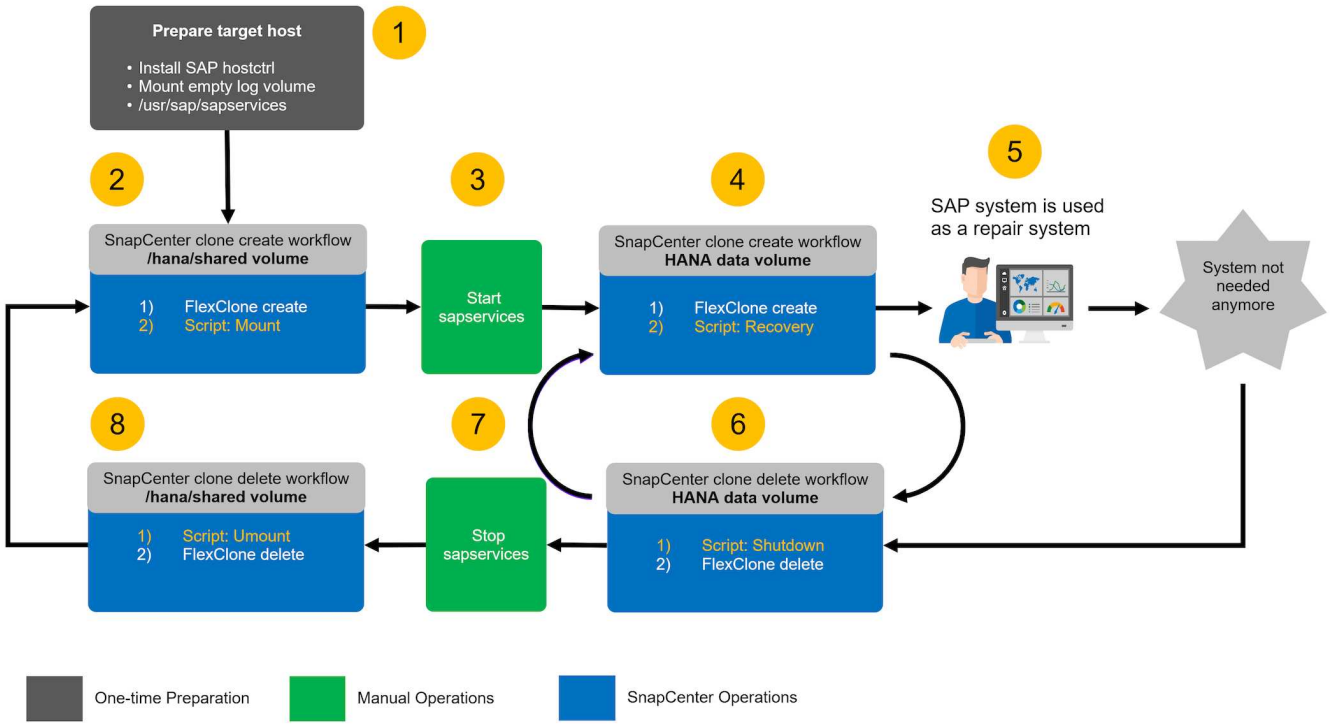
1. ターゲットホストを準備します。

2. SAP HANA共有ボリューム用のSnapCenterクローン作成ワークフロー
3. SAP HANAサービスを開始します。
4. SnapCenterクローンは、SAP HANAデータボリュームのデータベースリカバリを含むワークフローを作成します。
5. SAP HANAシステムを修復システムとして使用できるようになりました。

システムが不要になった場合は、次の手順でクリーンアッププロセスを実行します。

1. データベースのシャットダウンを含む、SAP HANAデータボリュームのSnapCenterクローン削除ワークフロー（自動スクリプト使用時）。
2. SAP HANAサービスを停止します。
3. SAP HANA共有ボリュームのSnapCenterクローン削除ワークフロー

システムを別のSnapshotバックアップにリセットする必要がある場合は、手順6と手順4で十分です。SAP HANA共有ボリュームの更新は必要ありません。




「」セクションでは"「SnapCenter を使用したSAPシステムのクローン作成」"、システムクローニングワークフローの詳細な手順を説明します。

## ストレージ**Snapshot**バックアップを使用した**SAP HANA**システムの更新処理に関する考慮事項

SAPのライフサイクル管理を最適化するNetAppソリューションは、SAP HANAデータベースとライフサイクル管理ツールに統合されており、効率的なアプリケーション統合データプロテクションと、SAPテストシステムの柔軟なプロビジョニングが組み合わされています。

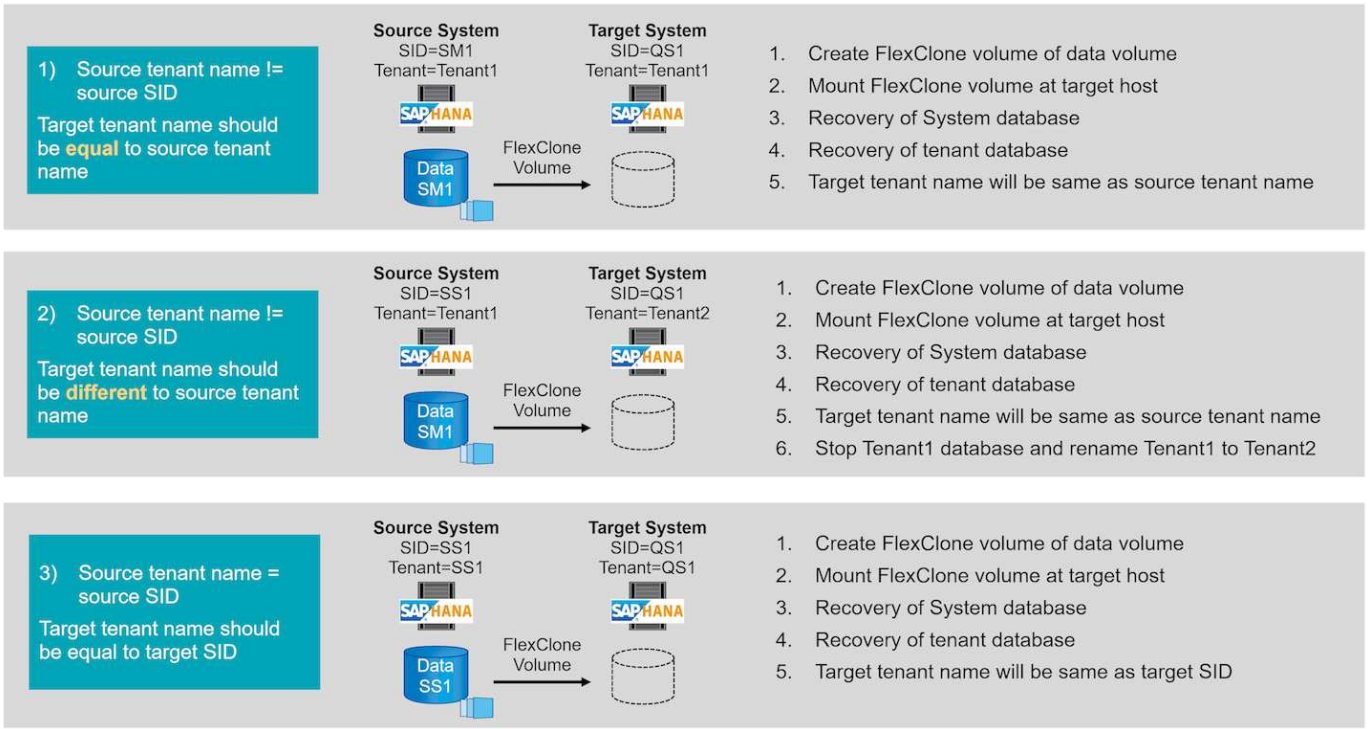
ターゲットシステムのテナント名

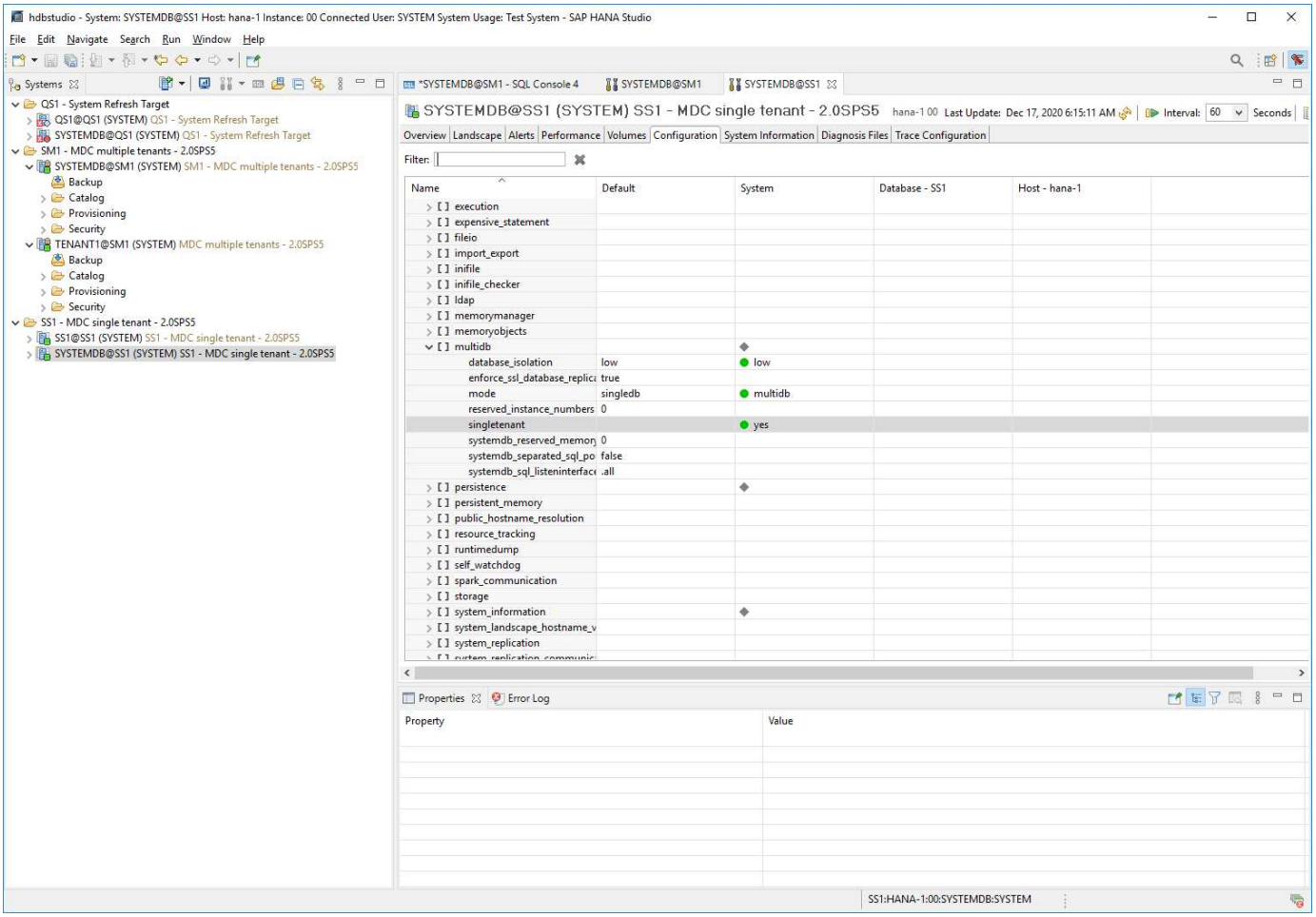
SAP HANAシステムの更新を実行する手順は、次の図に示すように、ソースシステムのテナント構成とターゲットシステムで必要なテナント名によって異なります。

システムデータベースにはテナント名が設定されているため、システムデータベースのリカバリ後にターゲットシステムでもソースシステムのテナント名を使用できます。そのため、ターゲットシステムのテナントは、オプション1に示すように、ソーステナントと同じ名前でしかリカバリできません。ターゲットシステムでテナント名を異なる名前にする必要がある場合は、最初にソーステナントと同じ名前でテナントをリカバリし、必要なターゲットテナント名に変更する必要があります。これはオプション2です。

ただし、テナント名がシステムのSIDと同じであるシングルテナントのSAP HANAシステムは例外です。これは、SAP HANAの初回インストール後のデフォルトの設定です。この特定の構成は、SAP HANAデータベースによってフラグ付けされます。この場合、ターゲットシステムでのテナントリカバリは、ターゲットシステムのテナント名を使用して実行できます。この名前は、ターゲットシステムのシステムSIDと同じである必要もあります。このワークフローをオプション3に示します。

> この設定フラグは、テナントの作成、名前変更、削除処理がソースシステムで実行されるとすぐにSAP HANAデータベースによって削除されます。したがって、構成をTenant = SIDの状態に戻しても、フラグは使用できなくなり、ワークフロー3でのテナントのリカバリに関する例外は実行できなくなります。この場合、必要なワークフローはオプション2です。






**SAP HANA**の暗号化を有効にしたシステム更新ワークフロー

SAP HANAの永続性暗号化を有効にしている場合は、ターゲットシステムでSAP HANAデータベースをリカバリする前に追加の手順が必要です。

ソースシステムで、システムデータベースおよびすべてのテナントデータベースの暗号化ルートキーのバックアップを作成する必要があります。リカバリ処理を実行する前に、バックアップファイルをターゲットシステムにコピーし、ルートキーをバックアップからインポートする必要があります。

も参照してください "『 SAP HANA Administration Guide 』をご覧ください"。

ルートキーのバックアップ

ルートキーに変更があった場合は、常にルートキーのバックアップが必要です。backupコマンドでは、CLIパラメータとしてDBIDを指定する必要があります。DBIDは、次のSQLステートメントを使用して識別できます。




SQLステートメントおよびその他のドキュメントについては、『SAP HANA Admin Guide』を参照してください。 "ルートキーのバックアップ| SAPヘルプポータル" 以下の手順は、シングルテナントSS1を使用するHANAシステムに必要な処理を示しており、ソースシステムで実行されます。

1. システムおよびテナント（SS1）データベースのバックアップパスワードを設定します（まだ設定していない場合）。

```
hdbsql SYSTEMDB=> ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD
Netapp123;
0 rows affected (overall time 3658.128 msec; server time 3657.967 msec)
hdbsql SYSTEMDB=>
hdbsql SS1=> ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD
Netapp123;
0 rows affected (overall time 2424.236 msec; server time 2424.010 msec)
hdbsql SS1=>
```

1. システムおよびテナント（SS1）データベースのルートキーのバックアップを作成します。

```
ss1adm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-backupRootKeys root-key-backup-SS1-SYSTEMDB.rkb --dbid=1 --type='ALL'
Exporting root key backup for database SYSTEMDB (DBID: 1) to
/usr/sap/SS1/home/root-key-backup-SS1-SYSTEMDB.rkb
done.
ss1adm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-backupRootKeys root-key-backup-SS1-SS1.rkb --dbid=3 --type='ALL'
Exporting root key backup for database SS1 (DBID: 3) to
/usr/sap/SS1/home/root-key-backup-SS1-SS1.rkb
done.
```

1. ルートキーのバックアップの検証（オプション）

```
ss1adm@hana-1:/usr/sap/SS1/home> ls -al root*
-rw-r----- 1 ss1adm sapsys 1440 Apr 24 07:00 root-key-backup-SS1-SS1.rkb
-rw-r----- 1 ss1adm sapsys 1440 Apr 24 06:54 root-key-backup-SS1-
SYSTEMDB.rkb
ss1adm@hana-1:/usr/sap/SS1/home>

ss1adm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-validateRootKeysBackup root-key-backup-SS1-SS1.rkb
Please Enter the password:
Successfully validated SSFS backup file /usr/sap/SS1/home/root-key-backup-
SS1-SS1.rkb
done.

ss1adm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-validateRootKeysBackup root-key-backup-SS1-SYSTEMDB.rkb
Please Enter the password:
Successfully validated SSFS backup file /usr/sap/SS1/home/root-key-backup-
SS1-SYSTEMDB.rkb
done.
```

ターゲットシステムでのルートキーのインポート

最初のシステム更新処理では、最初にルートキーをインポートする必要があります。ソースシステムでルートキーが変更されていない場合は、追加のインポートは必要ありません。importコマンドでは、CLIパラメータとしてDBIDを指定する必要があります。DBIDは、ルートキーのバックアップと同じ方法で識別できます。

1. このセットアップでは、ルートキーがソースシステムからNFS共有にコピーされます。

```
hana-1:~ # cp /usr/sap/SS1/home/root-key-backup-SS1-SS1.rkb /mnt/sapcc-
share/SAP-System-Refresh/
hana-1:~ # cp /usr/sap/SS1/home/root-key-backup-SS1-SYSTEMDB.rkb
/mnt/sapcc-share/SAP-System-Refresh/
```

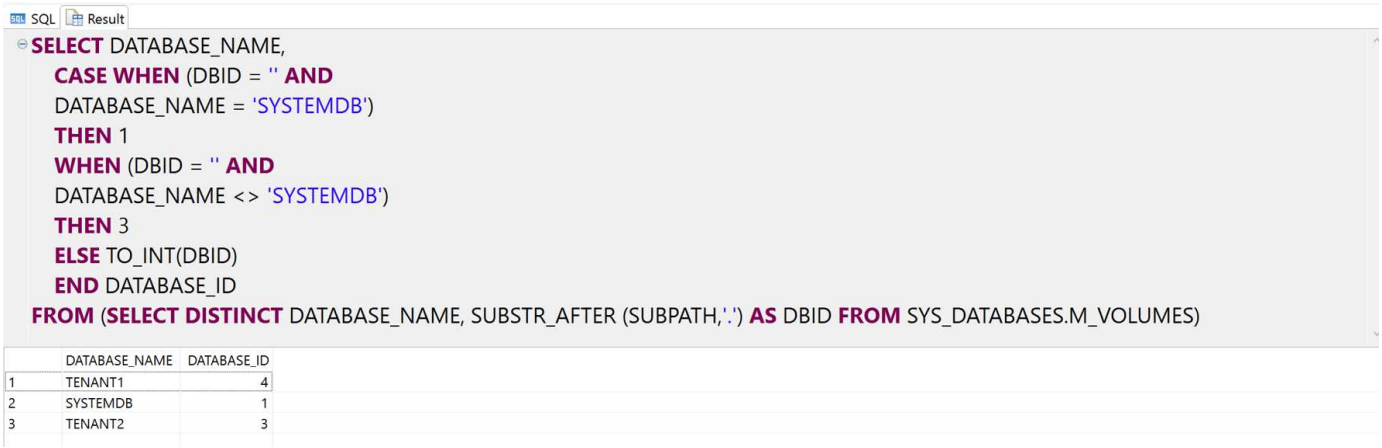
1. これで、hdbnsutilを使用してルートキーをインポートできるようになりました。コマンドでは、システムおよびテナントデータベースのDBIDを指定する必要があります。バックアップパスワードも必要です。

```
qs1adm@hana-7:/usr/sap/QS1/HDB11> ./exe/hdbnsutil -recoverRootKeys
/mnt/sapcc-share/SAP-System-Refresh/root-key-backup-SS1-SYSTEMDB.rkb
--dbid=1 --type=ALL
Please Enter the password:
Importing root keys for DBID: 1 from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SYSTEMDB.rkb
Successfully imported root keys from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SYSTEMDB.rkb
done.

qs1adm@hana-7:/usr/sap/QS1/HDB11> ./exe/hdbnsutil -recoverRootKeys
/mnt/sapcc-share/SAP-System-Refresh/root-key-backup-SS1-SS1.rkb --dbid=3
--type=ALL Please Enter the password:
Importing root keys for DBID: 3 from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SS1.rkb
Successfully imported root keys from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SS1.rkb
done.
qs1adm@hana-7:/usr/sap/QS1/HDB11>
```

ルートキーのインポート（ターゲットに**DBID**が存在しない場合）

前の章で説明したように、DBIDは、システムおよびすべてのテナントデータベースのルートキーをインポートするために必要です。システムデータベースでは常にDBID=0ですが、テナントデータベースでは異なるDBIDを使用できます。




上の出力は、DBID=3、DBID=4の2つのテナントを示しています。ターゲットシステムがDBID=4のテナントをまだホストしていない場合、ルートキーのインポートは失敗します。その場合は、まずシステムデータベースをリカバリしてから、DBID=4のテナントのキーをインポートする必要があります。

## 自動化スクリプトの例

本ドキュメントでは、SnapCenter クローンの作成処理とクローンの削除処理をさらに自動化するために、2つのスクリプトを使用しています。

- script.shは `sc-system-refresh`、システム更新とシステムクローニングのワークフローでSAP HANAデータベースのリカバリ処理とシャットダウン処理を実行するために使用します。
- このスクリプトは `sc-mount-volume.sh` 、システムクローンワークフローでSAP HANA共有ボリュームのマウントとアンマウントの処理を実行するために使用します。

> このサンプルスクリプトは現状のまま提供されており、ネットアップではサポートしていません。スクリプトは、ng-sapcc@netapp.com宛てにEメールでリクエストできます。

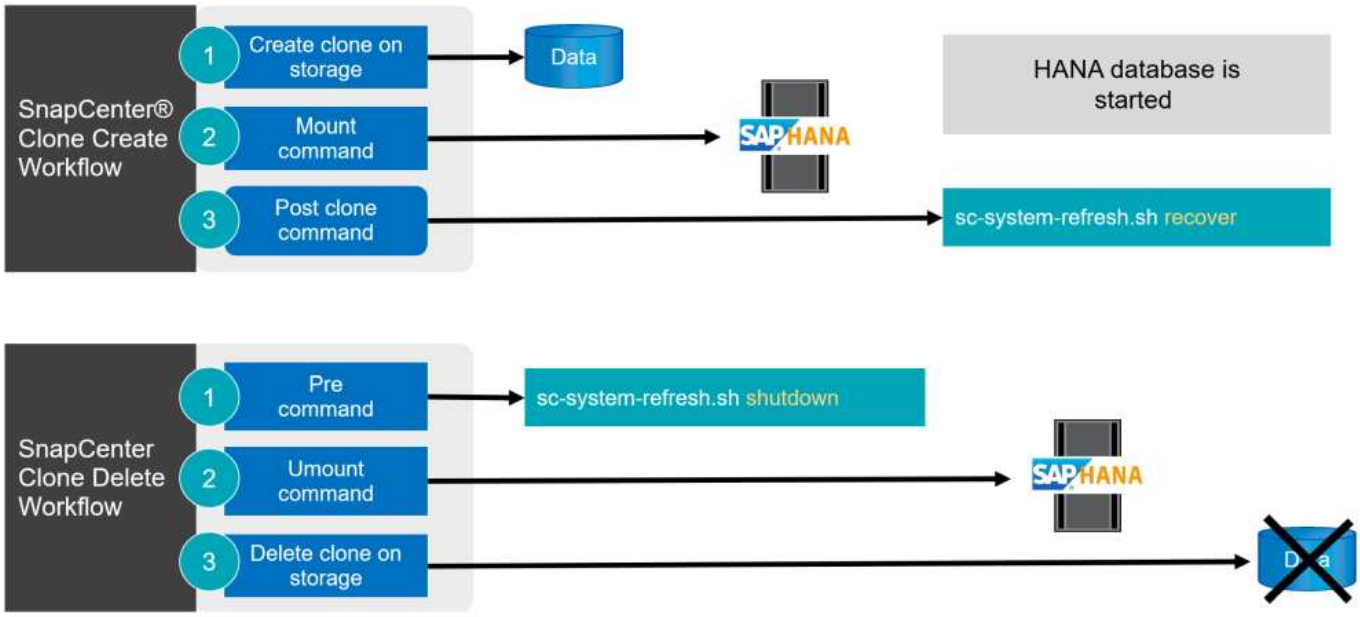
スクリプト**sc-system-refresh.sh**

このスクリプト例は `sc-system-refresh.sh` 、リカバリ処理とシャットダウン処理を実行するために使用します。このスクリプトは、次の図に示すように、SnapCenterワークフローのclone createおよびclone deleteで特定のコマンドラインオプションを指定して呼び出されます。

このスクリプトは汎用的で、SIDなどの必要なすべてのパラメータをターゲットシステムから読み取ります。このスクリプトは、システム更新処理のターゲットホストで使用できる必要があります。ターゲットシステムのユーザ<SID> admに対してhdbユーザストアキーが設定されている必要があります。このキーには、SAP HANAシステムデータベースへのアクセスを許可し、リカバリ処理の権限を付与する必要があります。キーには<TARGET-SID>キーという名前が必要です。

スクリプトは、実行されるディレクトリと同じディレクトリにログファイルを書き込み `sc-system-refresh-SID.log``ます。

> 現在のバージョンのスクリプトは、シングルホストシステムMDCのシングルテナント構成、またはMDCのマルチテナント構成をサポートしています。SAP HANAマルチホストシステムはサポートされていません。




サポートされているテナントリカバリ処理

セクション「ストレージSnapshotを使用したSAP HANAシステムの更新処理のワークフロー」で説明したように、ターゲットシステムで想定されるテナントリカバリ処理は、ソースシステムのテナント構成によって異なります。このスクリプト `sc-system-refresh.sh` では、次の表に示すように、すべてのテナントリカバ

リ処理がサポートされます。これらの処理はソースシステムの構成によって可能です。

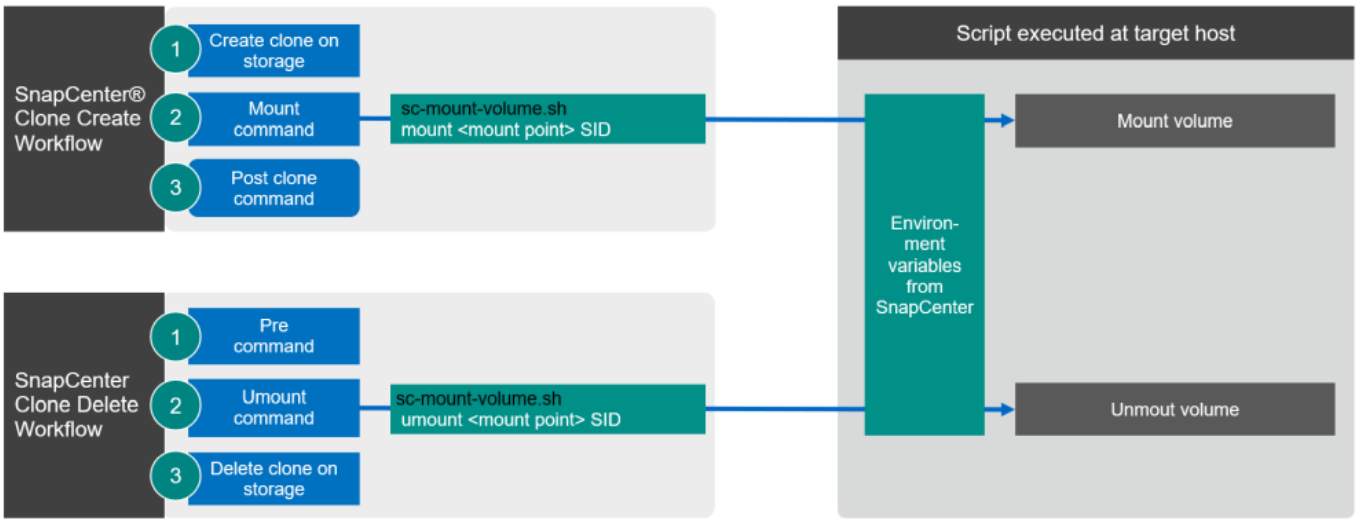
ターゲットシステムで別のテナント名が必要な場合は、リカバリ処理後にテナントの名前を手動で変更する必要があります。

| **SAP HANA**システム | テナント構成+ソースシステム | 変更後のテナント構成+をターゲットシステムに配置 |
|---|---|---|
| MDCのシングルテナント | ソースのテナント名がソースのSIDと同じです | ターゲットテナント名はターゲットSIDと同じです |
| MDCのシングルテナント | ソーステナント名がソースSIDと同じではありません | ターゲットテナント名はソーステナント名と同じです |
| MDCの複数のテナント | 任意のテナント名 | すべてのテナントがリカバリされ、ソーステナントと同じ名前になります。 |

### スクリプト**sc-mount-volume.sh**

このスクリプト例で `sc-mount-volume.sh` は、任意のボリュームのマウントとアンマウントを実行しています。このスクリプトは、SAP HANAシステムのクローニング処理でSAP HANA共有ボリュームをマウントするために使用されます。このスクリプトは、次の図に示すように、SnapCenterワークフローのclone createおよびclone deleteで特定のコマンドラインオプションを指定して呼び出されます。

このスクリプトは、NFSをストレージプロトコルとして使用するSAP HANAシステムをサポートします。




#### **SnapCenter** 環境変数

SnapCenter には、ターゲットホストで実行されるスクリプト内で使用可能な一連の環境変数が用意されています。スクリプトはこれらの変数を使用して、関連する構成設定を決定します。

- スクリプト変数 `STORAGE`, `JUNCTION_PATH` はマウント処理に使用されます。
- 「cloned_volume_mount_path」環境変数から派生したものです。
- `CLONED_VOLUMES_MOUNT_PATH=${STORAGE}:/${JUNCTION_PATH}`

- 例：
  CLONED_VOLUMES_MOUNT_PATH=192.168.175.117:/SS1_shared_Clone_05112206115489411

**SnapCenter** 環境変数を取得するスクリプト

自動化スクリプトを使用せず、手順を手動で実行する必要がある場合は、FlexCloneボリュームのストレージシステムのジャンクションパスを把握しておく必要があります。ジャンクションパスはSnapCenter 内では表示されないため、ストレージシステムで直接ジャンクションパスを検索するか、ターゲットホストにSnapCenter 環境変数を提供する単純なスクリプトを使用する必要があります。このスクリプトは、SnapCenter のクローン作成処理にマウント処理スクリプトとして追加する必要があります。

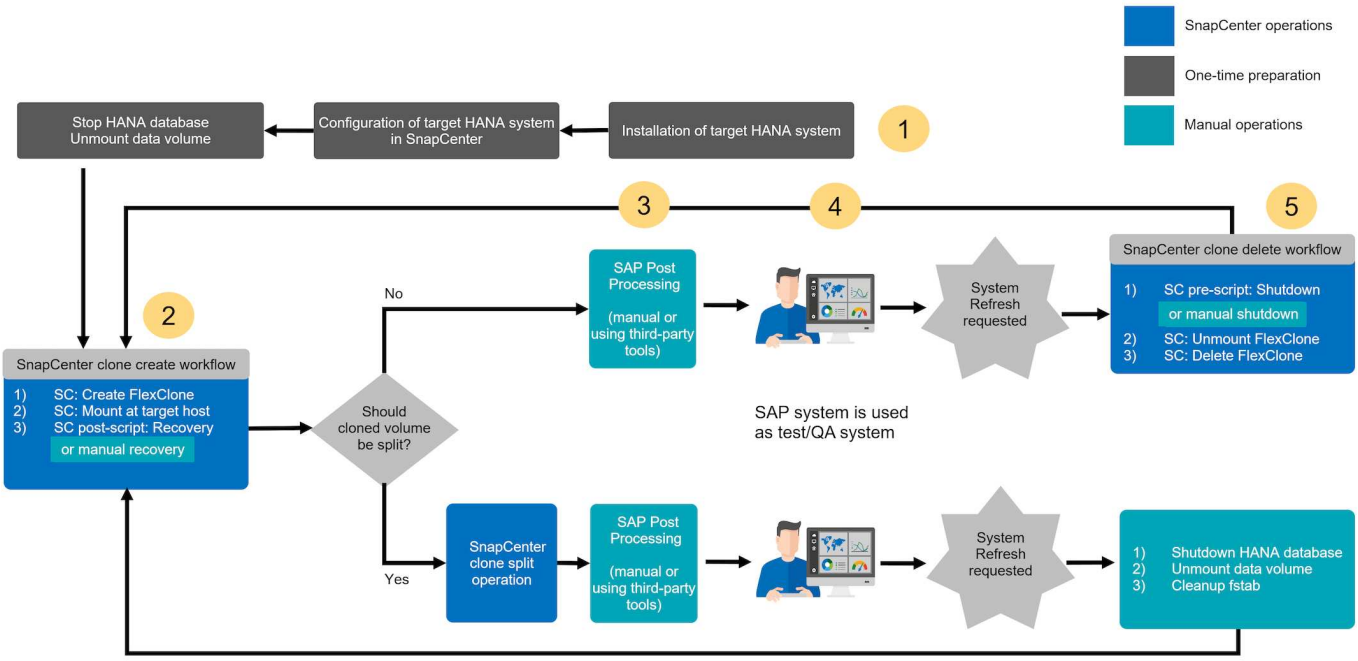
```
ss1adm@hana-1:/mnt/sapcc-share/SAP-System-Refresh> cat get-env.sh
#!/bin/bash
env > /tmp/env-from-sc.txt
ss1adm@hana-1:/mnt/sapcc-share/SAP-System-Refresh>
```

「env-from-ssc.txt」ファイル内で、変数「cloned_volume_mount_path」を検索して、FlexCloneボリュームのストレージシステムのIPアドレスとジャンクションパスを取得します。

例：
CLONED_VOLUMES_MOUNT_PATH=192.168.175.117:/SS1_data_mnt00001_Clone_05112206115489411

## SAP HANAシステムを**SnapCenter** で更新

次のセクションでは、SAP HANAデータベースのさまざまなシステム更新処理オプションについて、ステップバイステップの概要 を示します。




SAP HANAデータベースの設定に応じて、追加の手順を実行するか、準備が必要です。次の表に概要を示しま

す。

| ソースシステム | ソースシステムの構成 | **SnapCenter**と**SAP HANA**の運用 |
| --- | --- | --- |
| MDCシングルテナント+ SID =テナント名 | 標準構成 | SnapCenterクローン処理とリカバリスクリプトの実行（オプション）。 |
| | SAP HANAの永続性暗号化 | 最初に、またはソースシステムでルートキーが変更された場合は、リカバリを実行する前に、ルートキーのバックアップをターゲットシステムにインポートする必要があります。 |
| | SAP HANAシステムレプリケーションのソース | 追加の手順は必要ありません。ターゲットシステムにHSRが設定されていない場合は、スタンドアロンシステムのままになります。 |
| | SAP HANAマルチパーティション | 追加の手順は必要ありませんが、ターゲットシステムに同じ命名規則（SIDのみが異なります）を使用してSAP HANAボリュームパーティションのマウントポイントを使用できる必要があります。 |
| MDCの複数のテナント<br><br>またはMDCシングルテナント+（SID <>テナント名） | 標準構成 | SnapCenterクローン処理とリカバリスクリプトの実行（オプション）。スクリプトによってすべてのテナントがリカバリされます。ターゲットシステム名にテナント名またはテナント名が存在しない場合は、SAP HANAのリカバリ処理中に必要なディレクトリが自動的に作成されます。テナント名はソースと同じであり、必要に応じてリカバリ後に名前を変更する必要があります。 |
| | SAP HANAの永続性暗号化 | ターゲットシステムに以前にソースシステムのDBIDが存在しない場合は、このテナントのルートキーバックアップをインポートする前に、システムデータベースをリカバリする必要があります。 |
| | HANAシステムレプリケーションのソース | 追加の手順は必要ありません。ターゲットシステムにHSRが設定されていない場合は、スタンドアロンシステムのままになります。 |
| | HANAマルチパーティション | 追加の手順は必要ありませんが、ターゲットシステムに同じ命名規則（SIDのみが異なります）を使用してSAP HANAボリュームパーティションのマウントポイントを使用できる必要があります。 |

このセクションでは、次のシナリオについて説明します。

- クローンスプリット処理を実行せずにSAP HANAシステムが更新されます。
- テナント名がSIDと同じであるプライマリストレージからのクローニング
- オフサイトのバックアップストレージからのクローニング
- 複数テナントのプライマリストレージからのクローニング
- クローンの削除処理

- SAP HANAシステムがクローンスプリット処理で更新されます
- テナント名がSIDと同じであるプライマリストレージからのクローニング
- クローンスプリット処理

前提条件および制限事項

以降のセクションで説明するワークフローには、SAP HANAシステムのアーキテクチャとSnapCenterの設定に関する前提条件と制限事項がいくつかあります。

- ここで説明するワークフローは、SnapCenter 5.0リリース以降でのみ有効です。
- ここで説明するワークフローは、シングルテナントまたは複数テナントのシングルホストSAP HANA MDCシステムに対して有効です。SAP HANAマルチホストシステムは対象外です。
- SnapCenterの自動検出と自動スクリプトの実行を有効にするには、SnapCenter SAP HANAプラグインをターゲットホストに導入する必要があります。
- ワークフローは、物理ホストでNFSまたはFCPを使用するSAP HANAシステム、またはゲスト内NFSマウントを使用する仮想ホストに有効です。

ラボのセットアップ

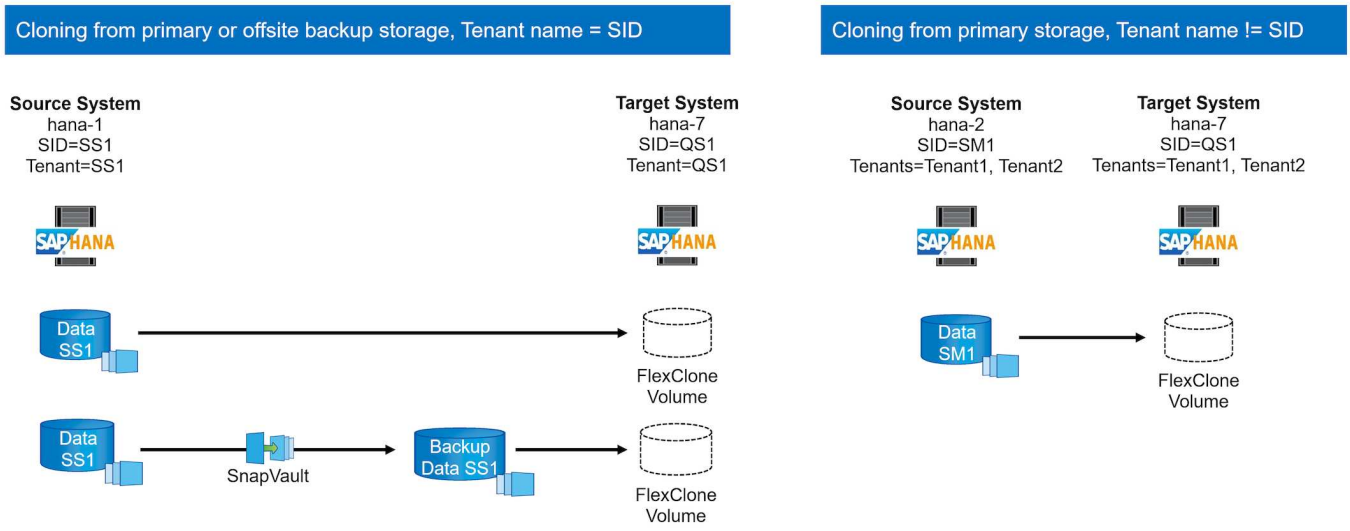
次の図は、さまざまなシステム更新操作オプションに使用したラボのセットアップを示しています。

- プライマリストレージまたはオフサイトバックアップストレージからのクローニング。テナント名はSIDと同じです。
  - ソースSAP HANAシステム：SS1とテナントSS1
  - ターゲットのSAP HANAシステム：QS1とテナントQS1
- プライマリストレージからのクローニング（複数テナント）。
  - ソースSAP HANAシステム：SM1とTenant1およびTenant2
  - ターゲットのSAP HANAシステム：QS1とTenant1およびTenant2

使用したソフトウェアバージョンは次のとおりです。

- SnapCenter 5.0
- SAP HANAシステム：HANA 2.0 SPS7 rev.73
- SLES 15
- ONTAP 9.14P1

すべてのSAP HANAシステムは、構成ガイドに基づいて設定する必要があります"NFSを使用したNetApp AFFシステムでのSAP HANA"。SnapCenterとSAP HANAのリソースは、ベストプラクティスガイドに基づいて設定されました"SnapCenter を使用した SAP HANA のバックアップとリカバリ"。




最初の**1**回限りの準備手順

最初のステップとして、ターゲットのSAP HANAシステムがSnapCenter内で設定されている必要があります。

1. SAP HANAターゲットシステムのインストール
2. SnapCenterでのSAP HANAシステムの構成（を参照）"TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"
   a. SnapCenterバックアップ処理用のSAP HANAデータベースユーザの設定このユーザは、ソースシステムとターゲットシステムで同一である必要があります。
   b. 上記のバックアップユーザを使用した<sid> admのhdbuserstoreキーの設定。リカバリに自動スクリプトを使用する場合は、キー名を<SID>キーにする必要があります。
   c. SnapCenter SAP HANAプラグインをターゲットホストに導入SAP HANAシステムは、SnapCenterによって自動検出されます。
   d. SAP HANAリソース保護の設定（オプション）

初期インストールの準備が完了してから、次の手順で最初のSAPシステムの更新処理を実行します。

1. ターゲットのSAP HANAシステムをシャットダウン
2. SAP HANAデータボリュームをアンマウントします。

ターゲットシステムで実行するスクリプトを、SnapCenter allowed commands configファイルに追加する必要があります。

```
hana-7:/opt/NetApp/snapcenter/scc/etc # cat
/opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh
hana-7:/opt/NetApp/snapcenter/scc/etc #
```

テナント名を**SID**と同じにしてプライマリストレージからクローニングする

ここでは、SAP HANAシステムの更新ワークフローについて説明します。このワークフローでは、ソースシステムとターゲットシステムのテナント名がSIDと同じになります。ストレージのクローニングはプライマリストレージで実行され、スクリプトによってリカバリが自動化され `sc-system-refresh.sh`ます。




このワークフローは、次の手順で構成されます。

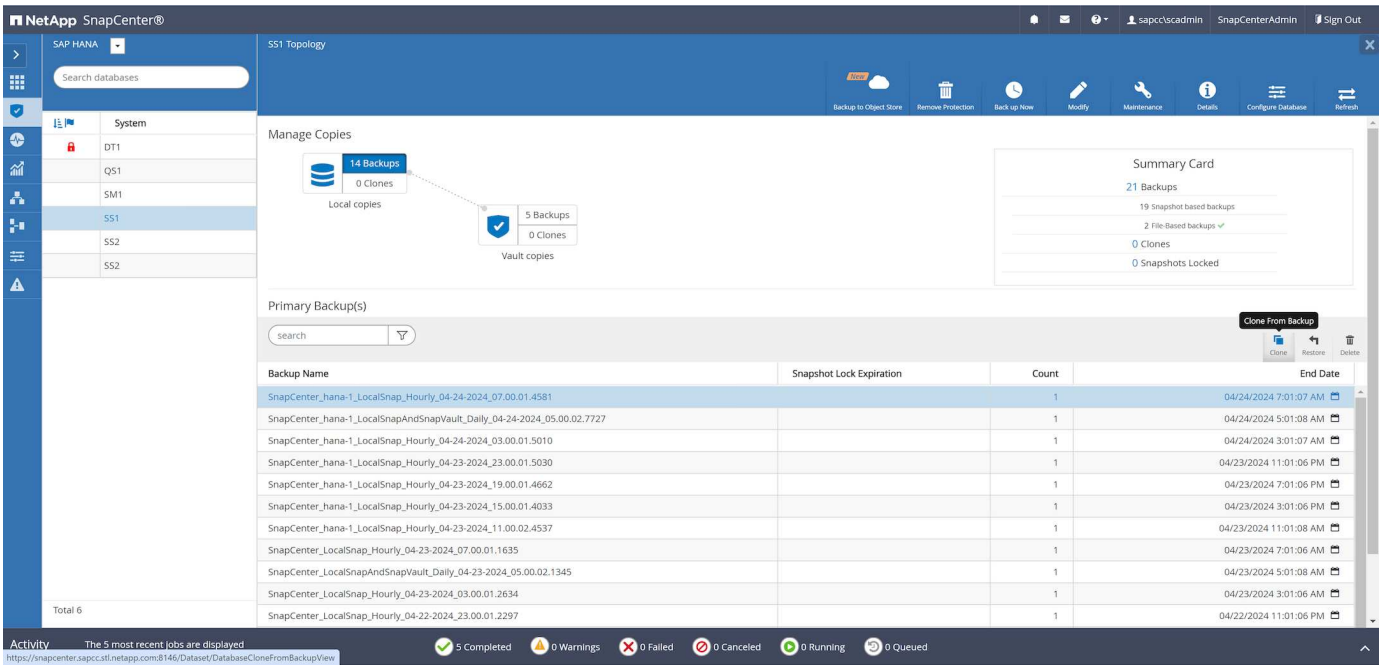
1. ソースシステムでSAP HANA永続性暗号化が有効になっている場合は、暗号化ルートキーを1回インポートする必要があります。ソースシステムでキーが変更されている場合もインポートが必要です。章を参照 "「ストレージSnapshotバックアップを使用したSAP HANAシステムの更新処理に関する考慮事項」"
2. ターゲットのSAP HANAシステムがSnapCenterで保護されている場合は、まず保護を削除する必要があります。
3. SnapCenter クローンの作成ワークフロー
   a. ソースSAP HANAシステムSS1から[Snapshot backup]を選択します。
   b. ターゲットホストを選択し、ターゲットホストのストレージネットワークインターフェイスを指定してください。
   c. ターゲットシステムのSIDを指定します（この例ではQS1）。
   d. 必要に応じて、クローン後の処理としてリカバリ用のスクリプトを指定します。
4. SnapCenter クローニング処理。
   a. ソースSAP HANAシステムの選択したSnapshotバックアップに基づいてFlexCloneボリュームを作成します。
   b. FlexCloneボリュームをターゲットホストストレージのネットワークインターフェイスまたはigroupにエクスポートします。
   c. のマウント処理を実行します。FlexCloneボリュームをターゲットホストにマウントします。
   d. クローニング後処理のリカバリスクリプトを実行します（前に設定した場合）。それ以外の場合は、SnapCenterワークフローが終了したときにリカバリを手動で実行する必要があります。
      - システムデータベースのリカバリ。

- テナント名= QS1でのテナントデータベースのリカバリ

5. 必要に応じて、ターゲットのSAP HANAリソースをSnapCenterで保護します。

以下のスクリーンショットは、必要な手順を示しています。

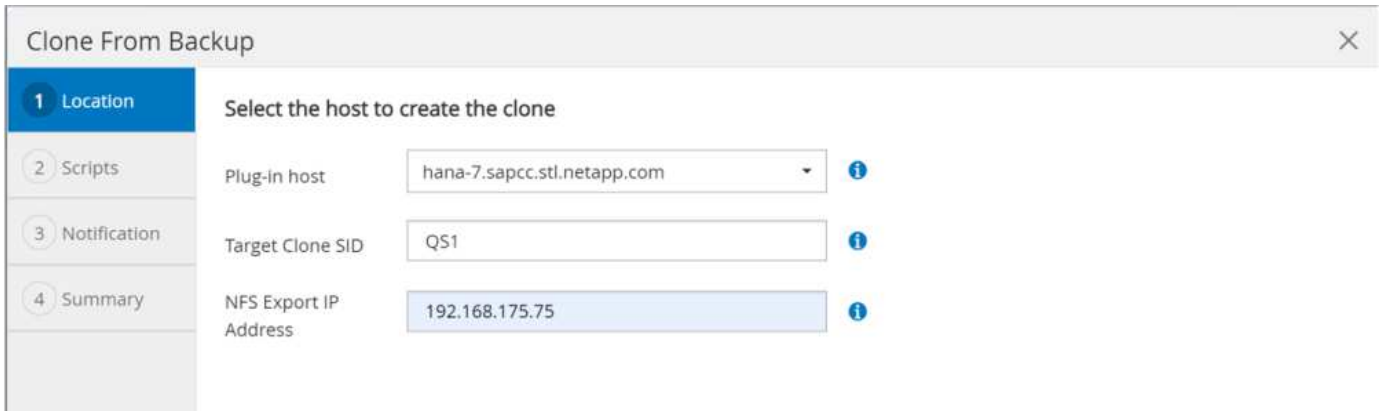
1. ソースシステムSS1からSnapshotバックアップを選択し、[Clone]をクリックします。




1. ターゲットシステムQS1がインストールされているホストを選択します。ターゲットSIDとして「QS1」と入力します。NFSエクスポートのIPアドレスは、ターゲットホストのストレージネットワークインターフェイスである必要があります。

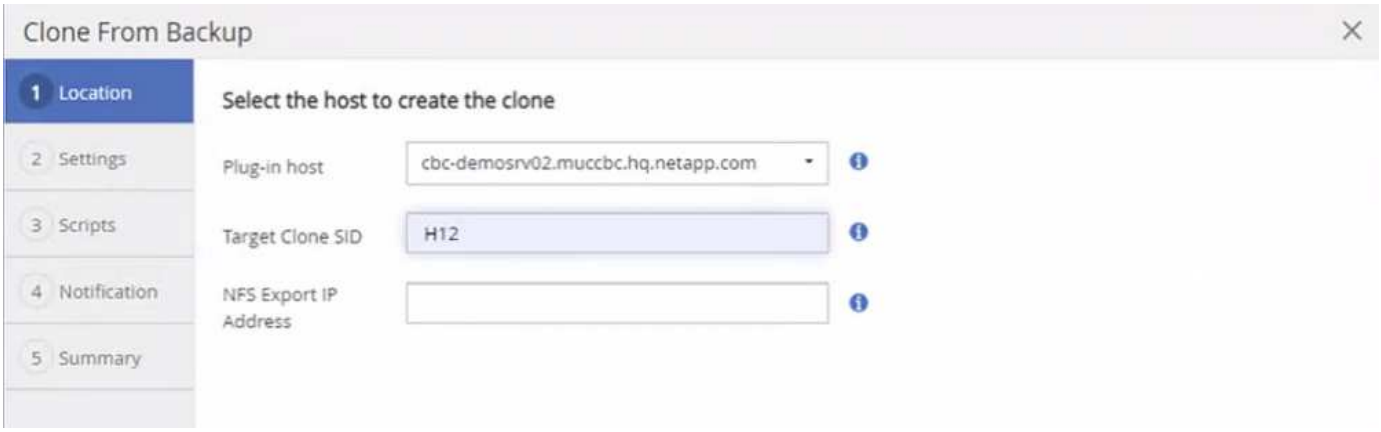
入力するターゲットSIDによって、SnapCenterによるクローンリソースの管理方法が制御されます。ターゲットSIDのリソースがすでにSnapCenterで設定されており、プラグインホストと一致する場合、SnapCenterはクローンをこのリソースに割り当てます。ターゲットホストでSIDが設定されていない場合、SnapCenter は新しいリソースを作成します。

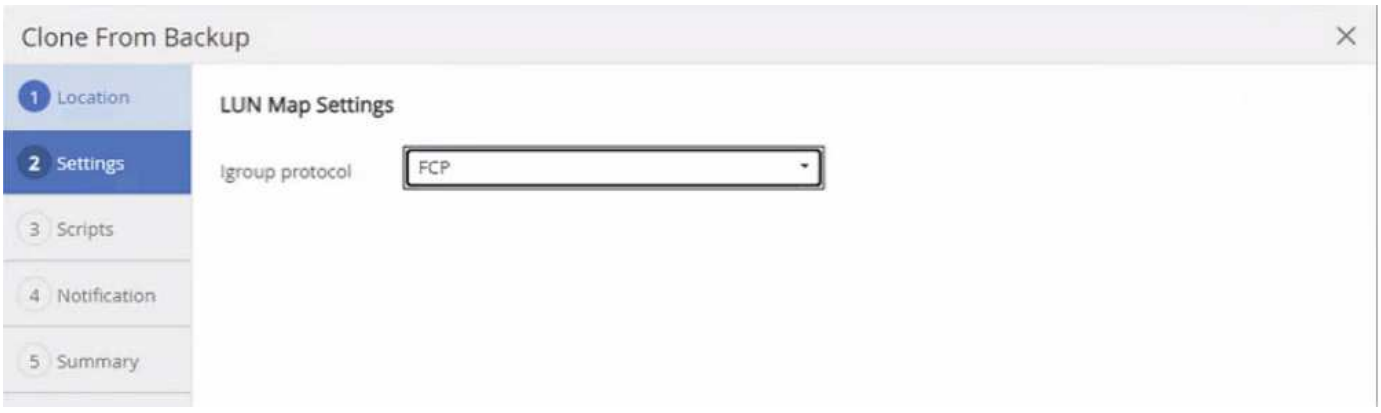
クローニングのワークフローを開始する前に、ターゲットシステムのリソースとホストをSnapCenterで設定しておくことが重要です。そうしないと、SnapCenterで作成された新しいリソースでは自動検出がサポートされず、説明されているワークフローは機能しません。




ファイバチャネルSANのセットアップでは、エクスポートIPアドレスは必要ありませんが、次の画面で使用するプロトコルを指定する必要があります。

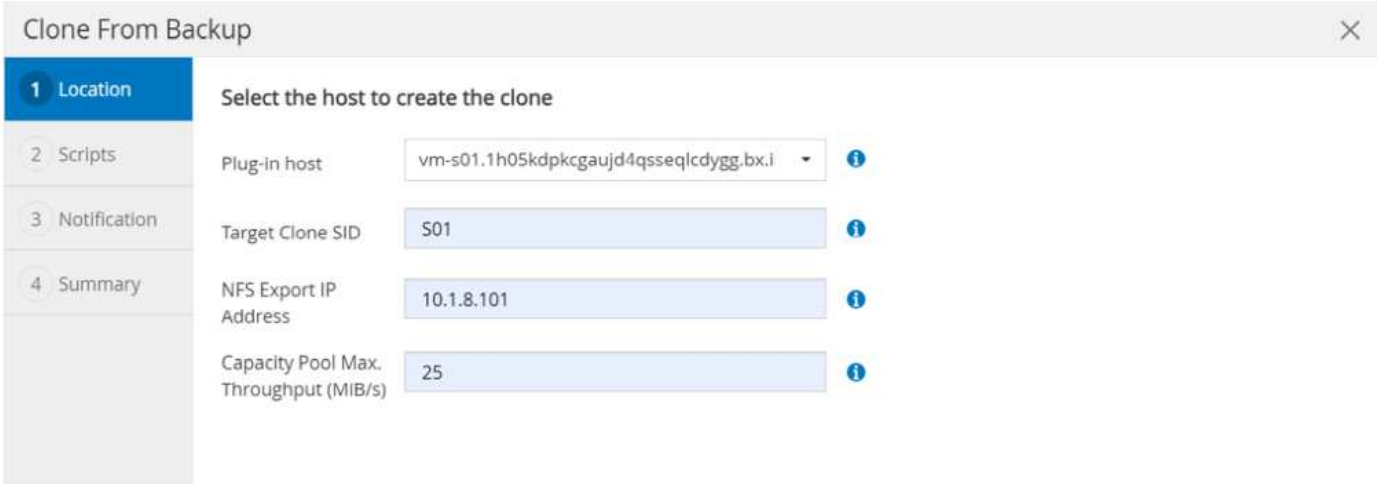
スクリーンショットは、ファイバチャネル接続を使用した別のラボセットアップを示しています。



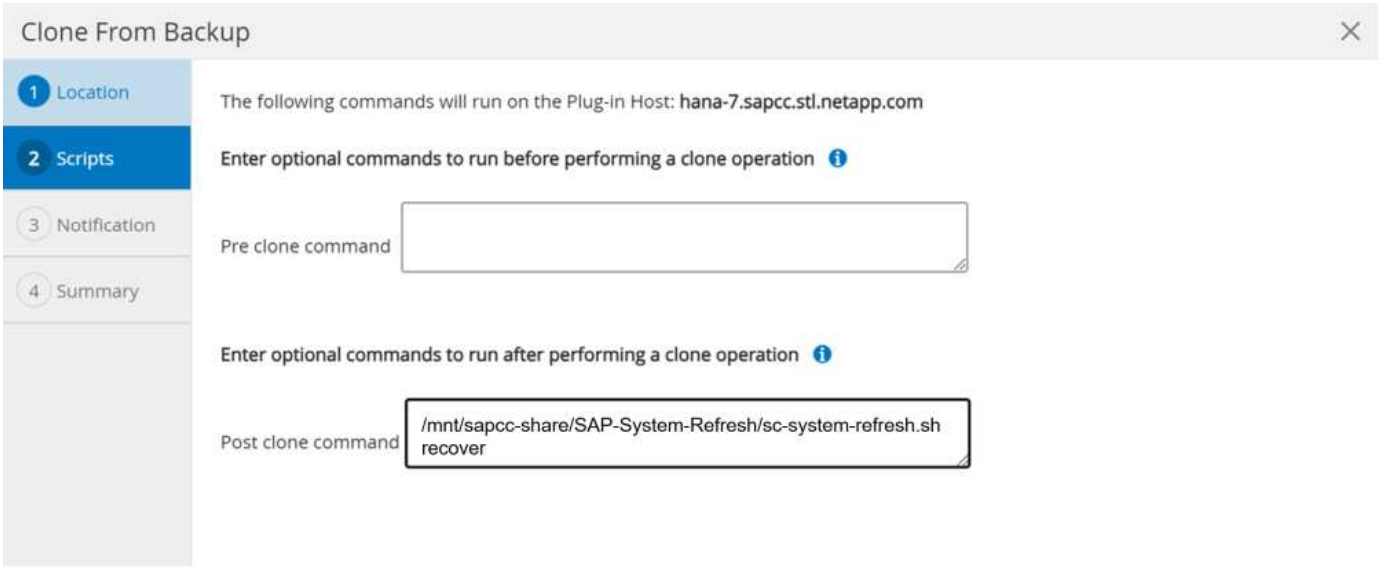




Azure NetApp Filesと手動のQoS容量プールを使用している場合は、新しいボリュームのスループットを最大化する必要があります。容量プールに十分なヘッドルームがあることを確認してください。そうしないと、クローニングワークフローが失敗します。

スクリーンショットは、Azure NetApp Filesを使用したMicrosoft Azureで実行される別のラボセットアップを示しています。



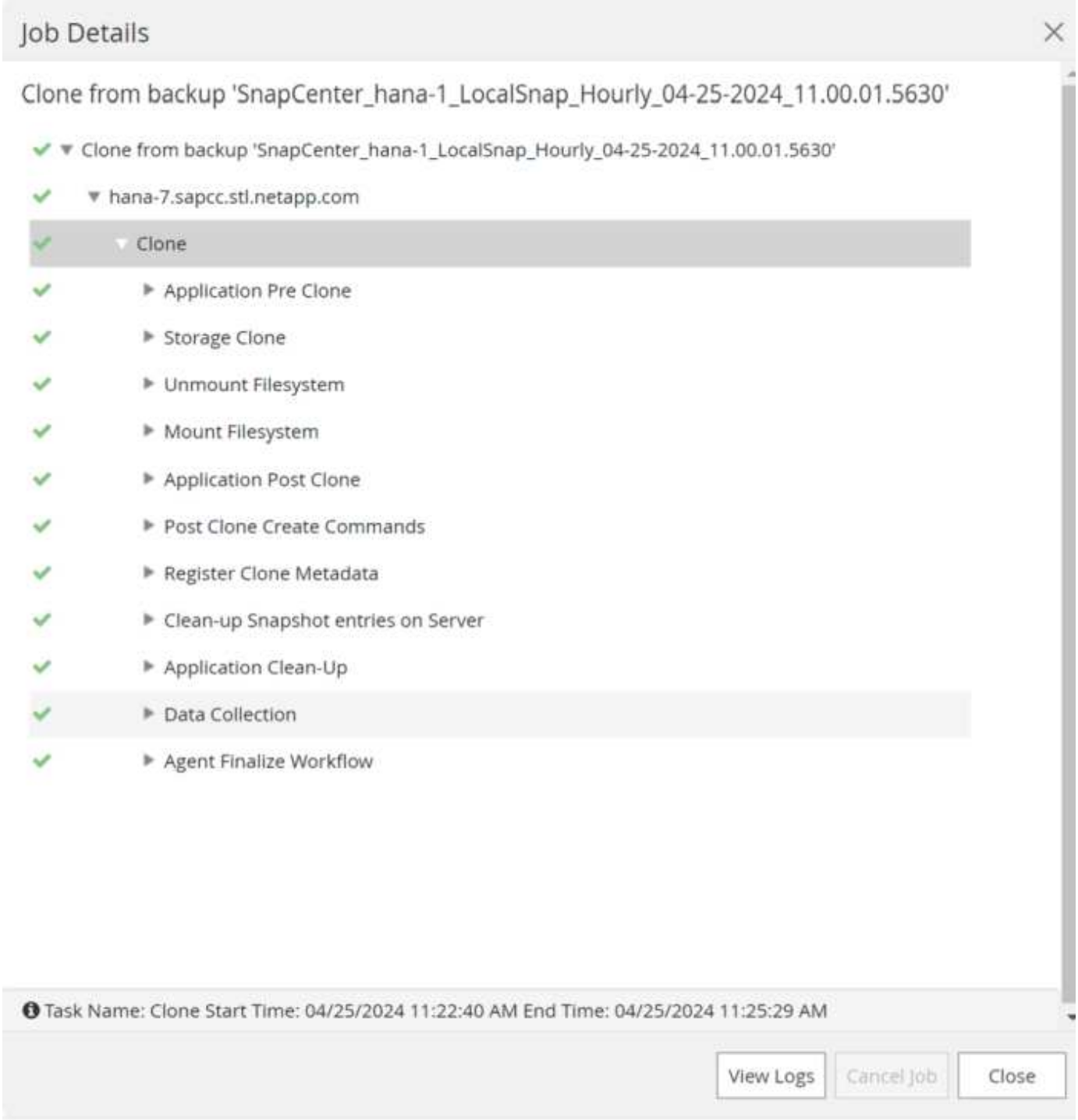

1. 必要なコマンドラインオプションを指定して、オプションのクローニング後スクリプトを入力します。この例では、クローニング後のスクリプトを使用してSAP HANAデータベースのリカバリを実行します。




前述したように、リカバリスクリプトの使用はオプションです。SnapCenterクローニングのワークフローが終了したあとに、手動でリカバリを実行することもできます。

リカバリ処理用スクリプトは、ログのクリア処理を使用してSAP HANAデータベースをSnapshotのポイントインタイムにリカバリし、フォワードリカバリは実行しません。特定の時点までのフォワードリカバリが必要な場合は、リカバリを手動で実行する必要があります。手動フォワードリカバリでは、ソースシステムのログバックアップをターゲットホストで利用できることも必要です。

1. SnapCenter の[ジョブの詳細]画面に、処理の進捗状況が表示されます。ジョブの詳細には、データベースリカバリを含めた全体的な実行時間が3分未満であることも示されています。

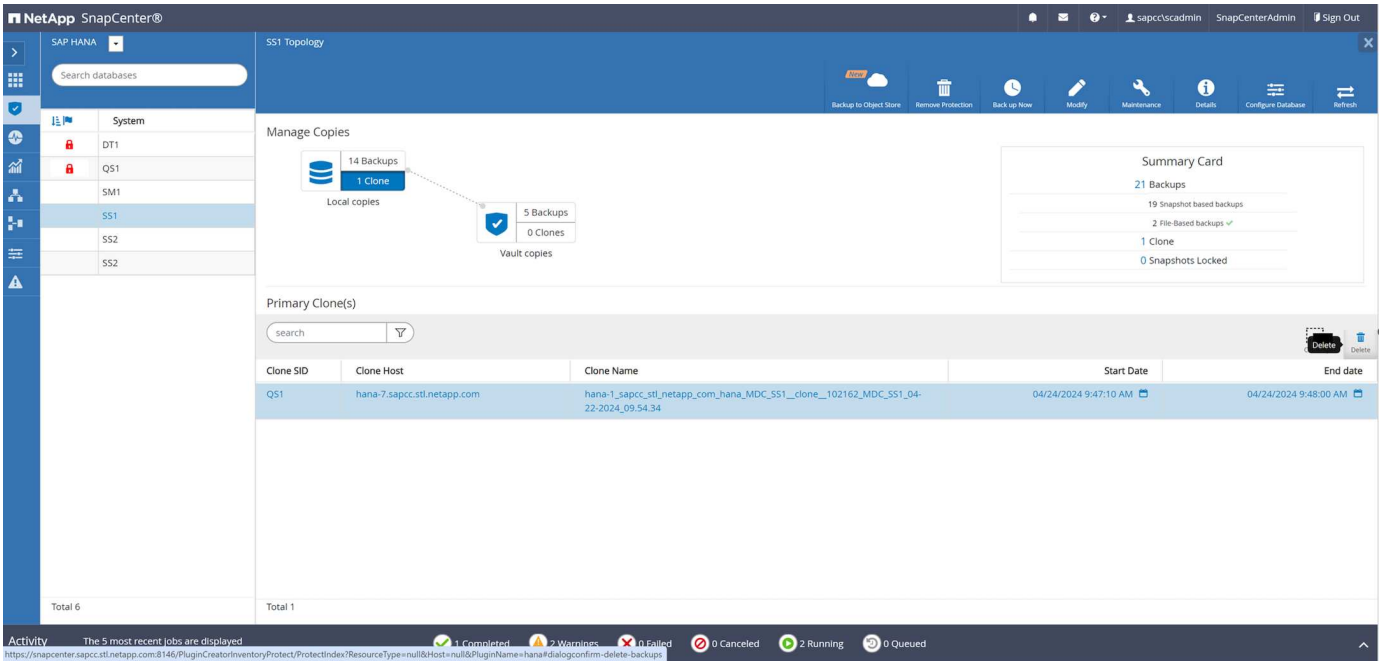



1. スクリプトのログファイル `sc-system-refresh` には、リカバリ処理で実行されたさまざまなステップが表示されます。このスクリプトは、システムデータベースからテナントのリストを読み取り、既存のすべてのテナントのリカバリを実行します。

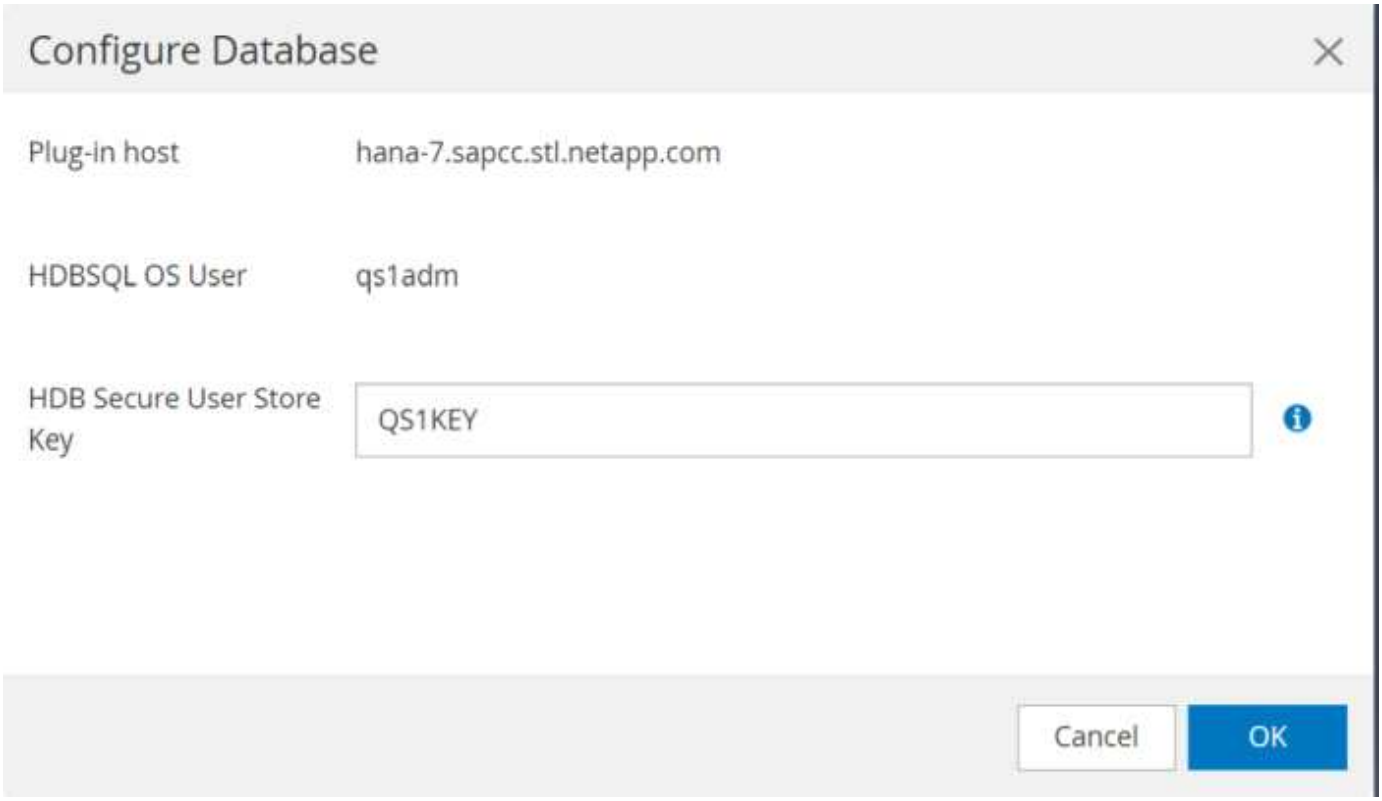
```
20240425112328###hana-7###sc-system-refresh.sh: Script version: 3.0
hana-7:/mnt/sapcc-share/SAP-System-Refresh # cat sap-system-refresh-
QS1.log
20240425112328###hana-7###sc-system-refresh.sh: ******************
Starting script: recovery operation ************************
20240425112328###hana-7###sc-system-refresh.sh: Recover system database.
```

```
20240425112328###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/HDB11/exe/Python/bin/python
/usr/sap/QS1/HDB11/exe/python_support/recoverSys.py --command "RECOVER
DATA USING SNAPSHOT CLEAR LOG"
20240425112346###hana-7###sc-system-refresh.sh: Wait until SAP HANA
database is started ....
20240425112347###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112357###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112407###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112417###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112428###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112438###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112448###hana-7###sc-system-refresh.sh: Status: GREEN
20240425112448###hana-7###sc-system-refresh.sh: HANA system database
started.
20240425112448###hana-7###sc-system-refresh.sh: Checking connection to
system database.
20240425112448###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY 'select * from sys.m_databases;'
DATABASE_NAME,DESCRIPTION,ACTIVE_STATUS,ACTIVE_STATUS_DETAILS,OS_USER,OS_G
ROUP,RESTART_MODE,FALLBACK_SNAPSHOT_CREATE_TIME
"SYSTEMDB","SystemDB-QS1-11","YES","","","","DEFAULT",?
"QS1","QS1-11","NO","ACTIVE","","","DEFAULT",?
2 rows selected (overall time 16.225 msec; server time 860 usec)
20240425112448###hana-7###sc-system-refresh.sh: Succesfully connected to
system database.
20240425112449###hana-7###sc-system-refresh.sh: Tenant databases to
recover: QS1
20240425112449###hana-7###sc-system-refresh.sh: Found inactive
tenants(QS1) and starting recovery
20240425112449###hana-7###sc-system-refresh.sh: Recover tenant database
QS1.
20240425112449###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY RECOVER DATA FOR QS1 USING
SNAPSHOT CLEAR LOG
0 rows affected (overall time 22.138599 sec; server time 22.136268 sec)
20240425112511###hana-7###sc-system-refresh.sh: Checking availability of
Indexserver for tenant QS1.
20240425112511###hana-7###sc-system-refresh.sh: Recovery of tenant
database QS1 succesfully finished.
20240425112511###hana-7###sc-system-refresh.sh: Status: GREEN
20240425112511###hana-7###sc-system-refresh.sh: ******************
Finished script: recovery operation *************************
hana-7:/mnt/sapcc-share/SAP-System-Refresh
```

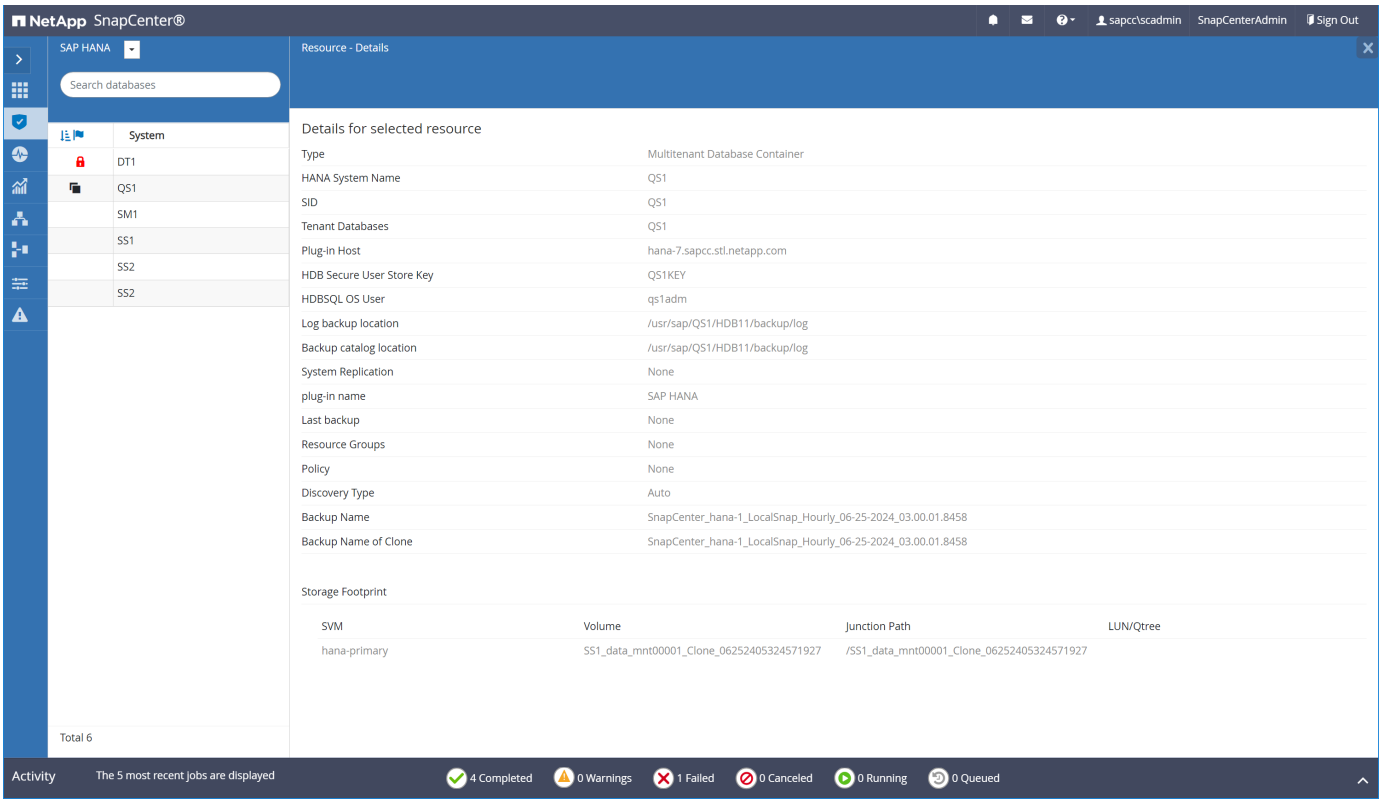
1. SnapCenter ジョブが完了すると、ソースシステムのトポロジビューにクローンが表示されます。



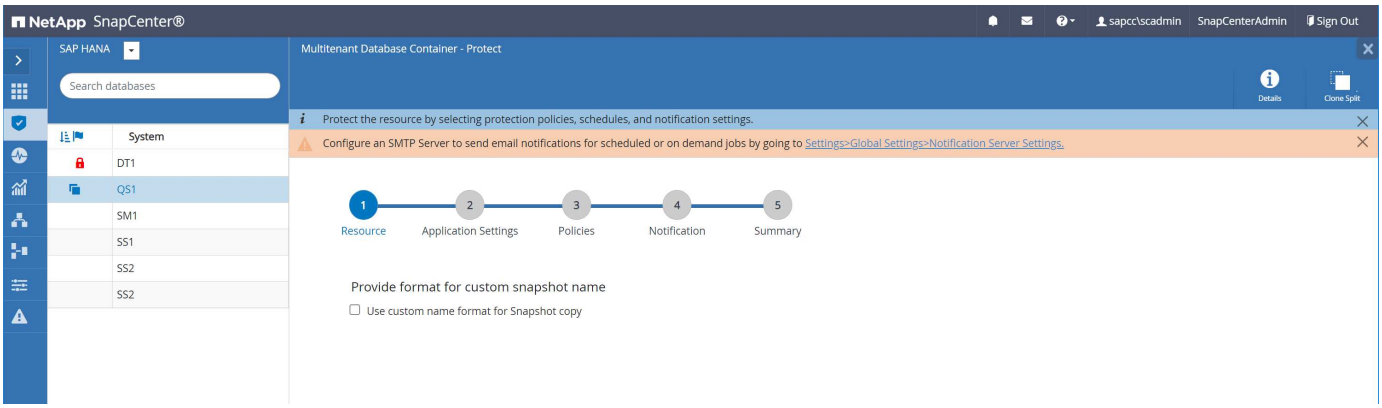

1. SAP HANAデータベースが実行されます。
2. ターゲットのSAP HANAシステムを保護する場合は、ターゲットシステムのリソースをクリックして自動検出を実行する必要があります。




自動検出プロセスが完了すると、新しいクローンボリュームがストレージフットプリントセクションに表示されます。

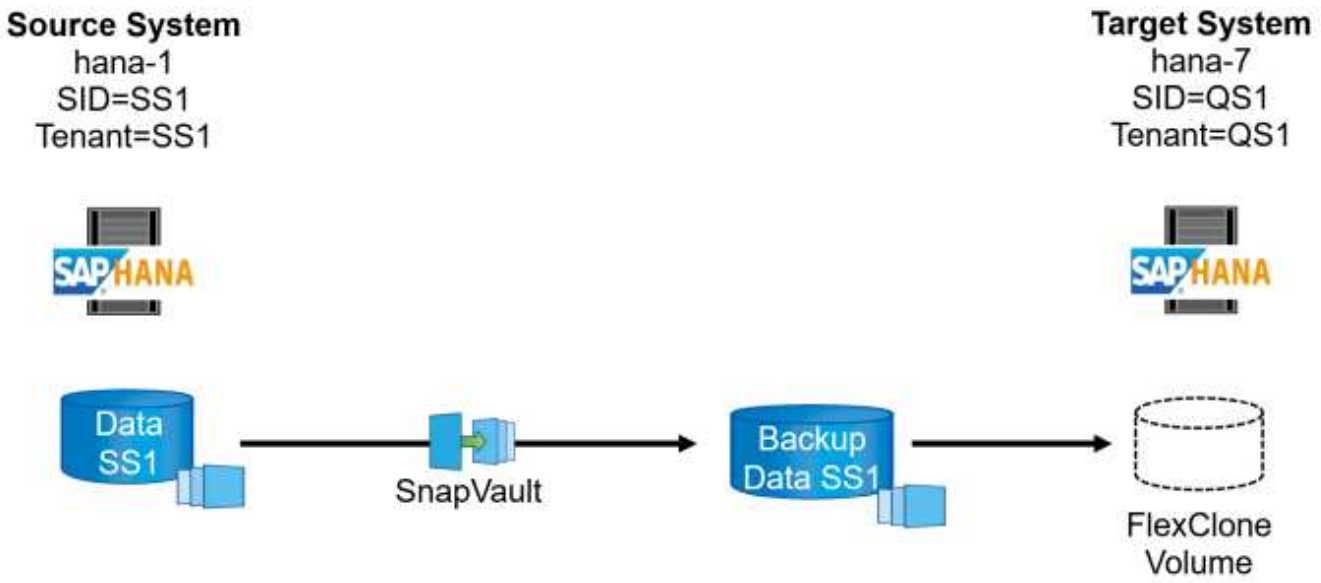



リソースを再度クリックすると、更新したQS1システムのデータ保護を設定できます。

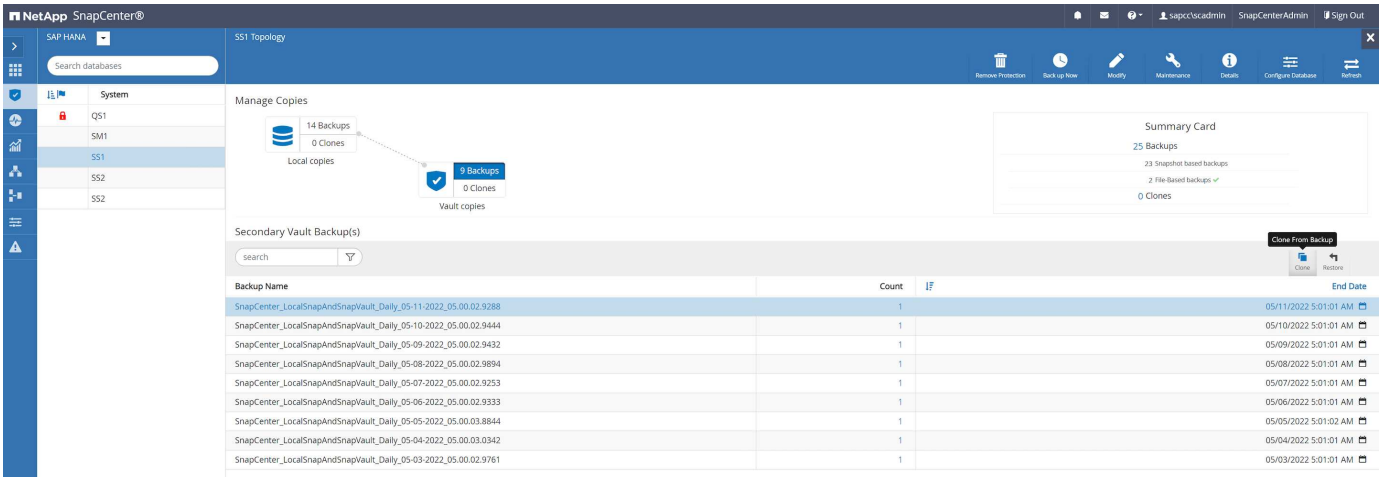



オフサイトのバックアップストレージからのクローニング

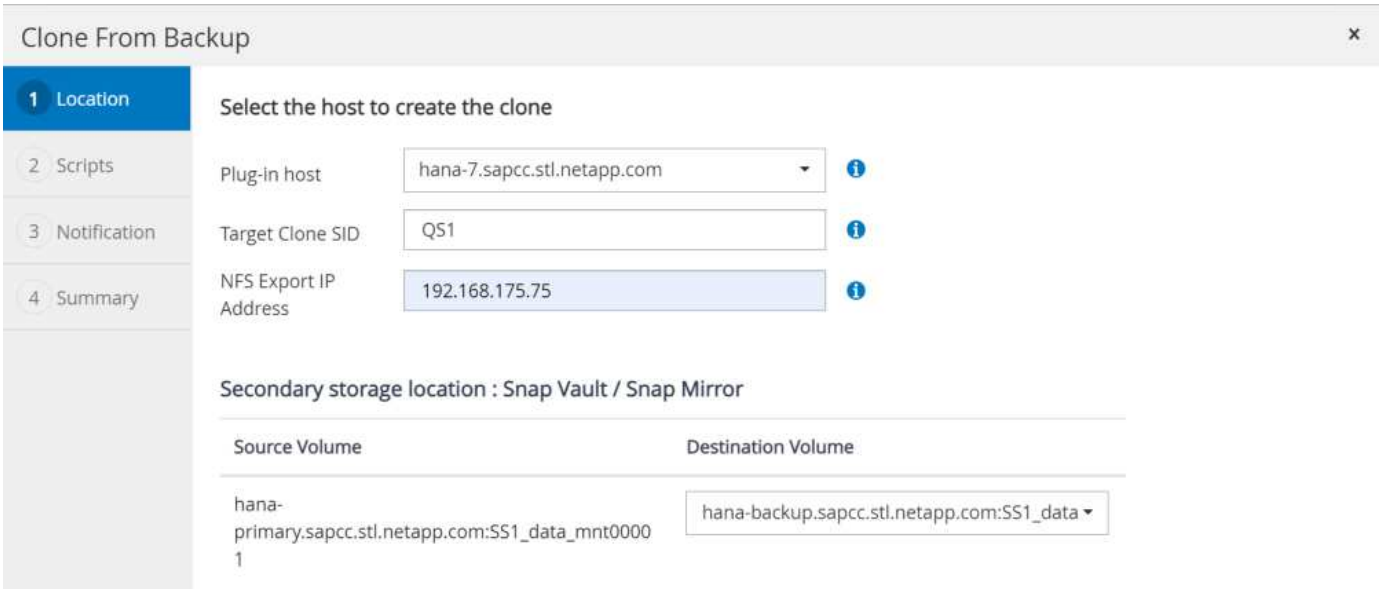
ここでは、ソースシステムとターゲットシステムのテナント名がSIDと同じであるSAP HANAシステムの更新ワークフローについて説明します。ストレージのクローニングはオフサイトのバックアップストレージで実行され、スクリプトsc-system-refresh.shを使用してさらに自動化されます。




プライマリとオフサイトのバックアップストレージのクローニングでSAP HANAシステムの更新ワークフローが異なるのは、SnapCenterでSnapshotバックアップを選択することだけです。オフサイトのバックアップストレージのクローニングでは、まずセカンダリバックアップを選択し、次にSnapshotバックアップを選択する必要があります。



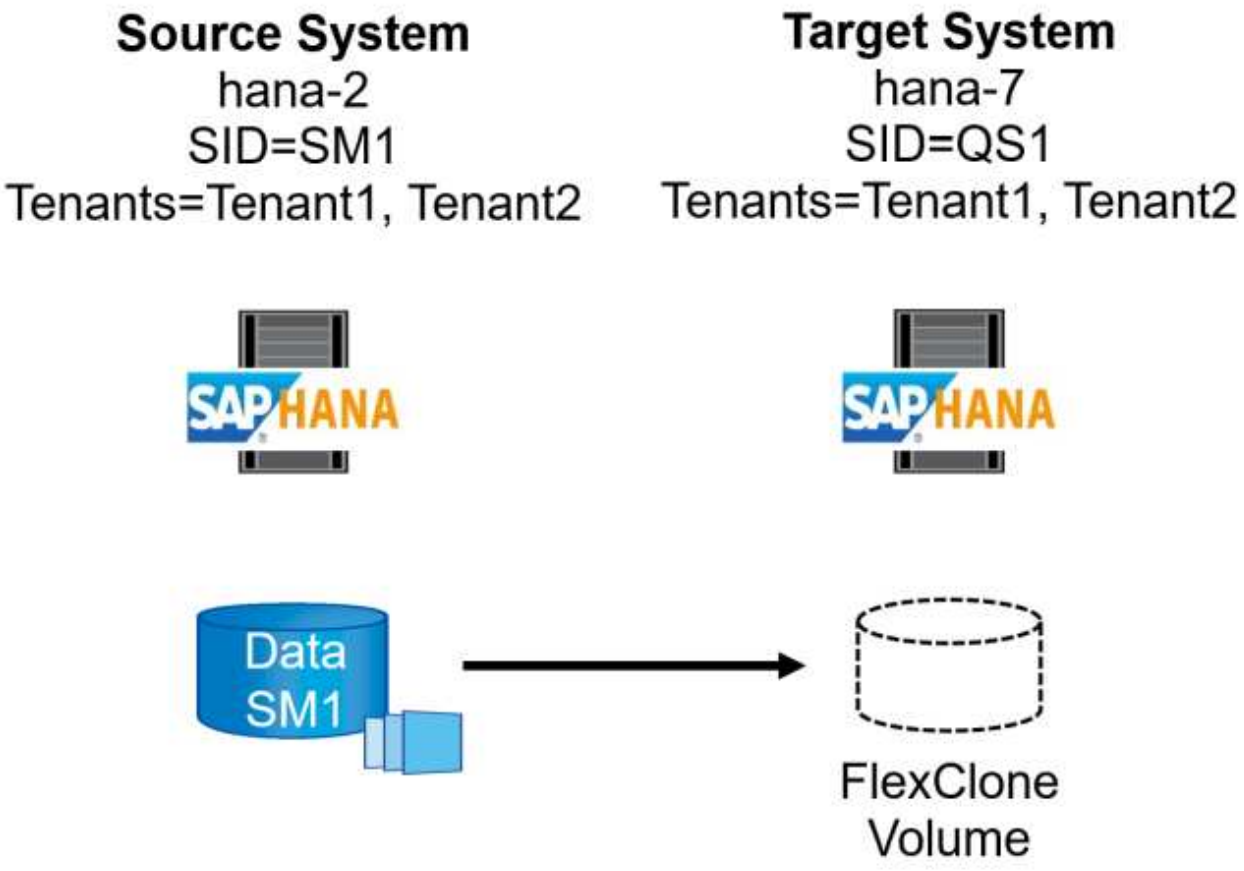

選択したバックアップにセカンダリストレージの場所が複数ある場合は、必要なデスティネーションボリュームを選択する必要があります。




以降の手順は、プライマリストレージからのクローニングのワークフローと同じです。

## 複数テナントのSAP HANAシステムのクローニング

このセクションでは、複数のテナントを使用したSAP HANAシステムの更新ワークフローについて説明します。ストレージのクローニングはプライマリストレージで実行され、スクリプトを使用してさらに自動化され`sc-system-refresh.sh`ます。



SnapCenterで必要な手順は、「テナント名がSIDと等しいプライマリストレージからのクローニング」セクションで説明した手順と同じです。唯一の違いは、スクリプト内でのテナントリカバリ処理で、すべてのテナントがリカバリされる点です `sc-system-refresh.sh`。

```
20240430070214###hana-7###sc-system-refresh.sh:
**********************************************************************
********
20240430070214###hana-7###sc-system-refresh.sh: Script version: 3.0
20240430070214###hana-7###sc-system-refresh.sh: ******************
Starting script: recovery operation *************************
20240430070214###hana-7###sc-system-refresh.sh: Recover system database.
20240430070214###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/HDB11/exe/Python/bin/python
/usr/sap/QS1/HDB11/exe/python_support/recoverSys.py --command "RECOVER
DATA USING SNAPSHOT CLEAR LOG"
[140310725887808, 0.008] >> starting recoverSys (at Tue Apr 30 07:02:15
2024)
[140310725887808, 0.008] args: ()
[140310725887808, 0.008] keys: \{'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/QS1/HDB11/hana-7/trace/backup.log
recoverSys started: ============2024-04-30 07:02:15 ============
testing master: hana-7
hana-7 is master
shutdown database, timeout is 120
stop system
stop system on: hana-7
stopping system: 2024-04-30 07:02:15
stopped system: 2024-04-30 07:02:15
creating file recoverInstance.sql
restart database
restart master nameserver: 2024-04-30 07:02:20
start system: hana-7
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2024-04-30T07:02:32-04:00 P0023828 18f2eab9331 INFO RECOVERY RECOVER DATA
finished successfully
recoverSys finished successfully: 2024-04-30 07:02:33
[140310725887808, 17.548] 0
[140310725887808, 17.548] << ending recoverSys, rc = 0 (RC_TEST_OK), after
17.540 secs
20240430070233###hana-7###sc-system-refresh.sh: Wait until SAP HANA
database is started ....
20240430070233###hana-7###sc-system-refresh.sh: Status: GRAY
20240430070243###hana-7###sc-system-refresh.sh: Status: GRAY
20240430070253###hana-7###sc-system-refresh.sh: Status: GRAY
```

```
20240430070304###hana-7###sc-system-refresh.sh: Status: GRAY
20240430070314###hana-7###sc-system-refresh.sh: Status: GREEN
20240430070314###hana-7###sc-system-refresh.sh: HANA system database
started.
20240430070314###hana-7###sc-system-refresh.sh: Checking connection to
system database.
20240430070314###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY 'select * from sys.m_databases;'
20240430070314###hana-7###sc-system-refresh.sh: Succesfully connected to
system database.
20240430070314###hana-7###sc-system-refresh.sh: Tenant databases to
recover: TENANT2
TENANT1
20240430070314###hana-7###sc-system-refresh.sh: Found inactive
tenants(TENANT2
TENANT1) and starting recovery
20240430070314###hana-7###sc-system-refresh.sh: Recover tenant database
TENANT2.
20240430070314###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY RECOVER DATA FOR TENANT2 USING
SNAPSHOT CLEAR LOG
20240430070335###hana-7###sc-system-refresh.sh: Checking availability of
Indexserver for tenant TENANT2.
20240430070335###hana-7###sc-system-refresh.sh: Recovery of tenant
database TENANT2 succesfully finished.
20240430070335###hana-7###sc-system-refresh.sh: Status: GREEN
20240430070335###hana-7###sc-system-refresh.sh: Recover tenant database
TENANT1.
20240430070335###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY RECOVER DATA FOR TENANT1 USING
SNAPSHOT CLEAR LOG
20240430070349###hana-7###sc-system-refresh.sh: Checking availability of
Indexserver for tenant TENANT1.
20240430070350###hana-7###sc-system-refresh.sh: Recovery of tenant
database TENANT1 succesfully finished.
20240430070350###hana-7###sc-system-refresh.sh: Status: GREEN
20240430070350###hana-7###sc-system-refresh.sh: ********************
Finished script: recovery operation *************************
```

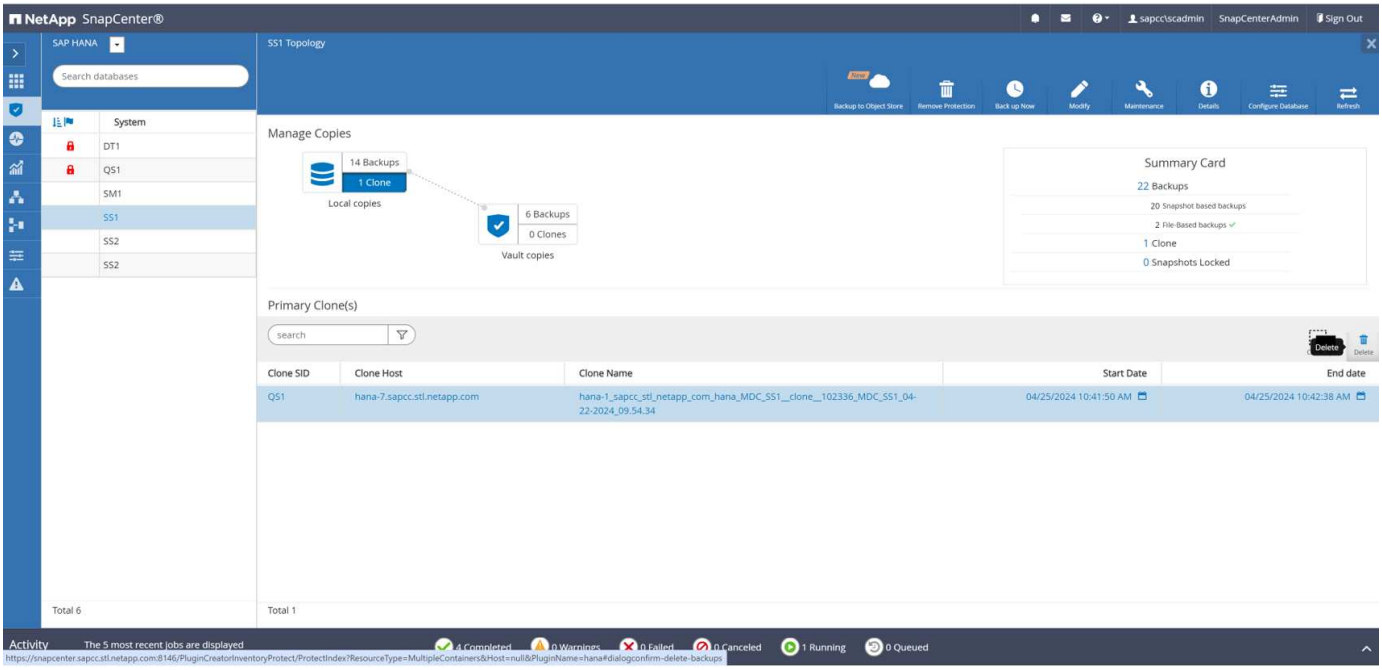
クローンの削除処理

新しいSAP HANAシステムの更新処理を開始するには、SnapCenter のクローンの削除処理を使用してターゲットシステムをクリーンアップします。

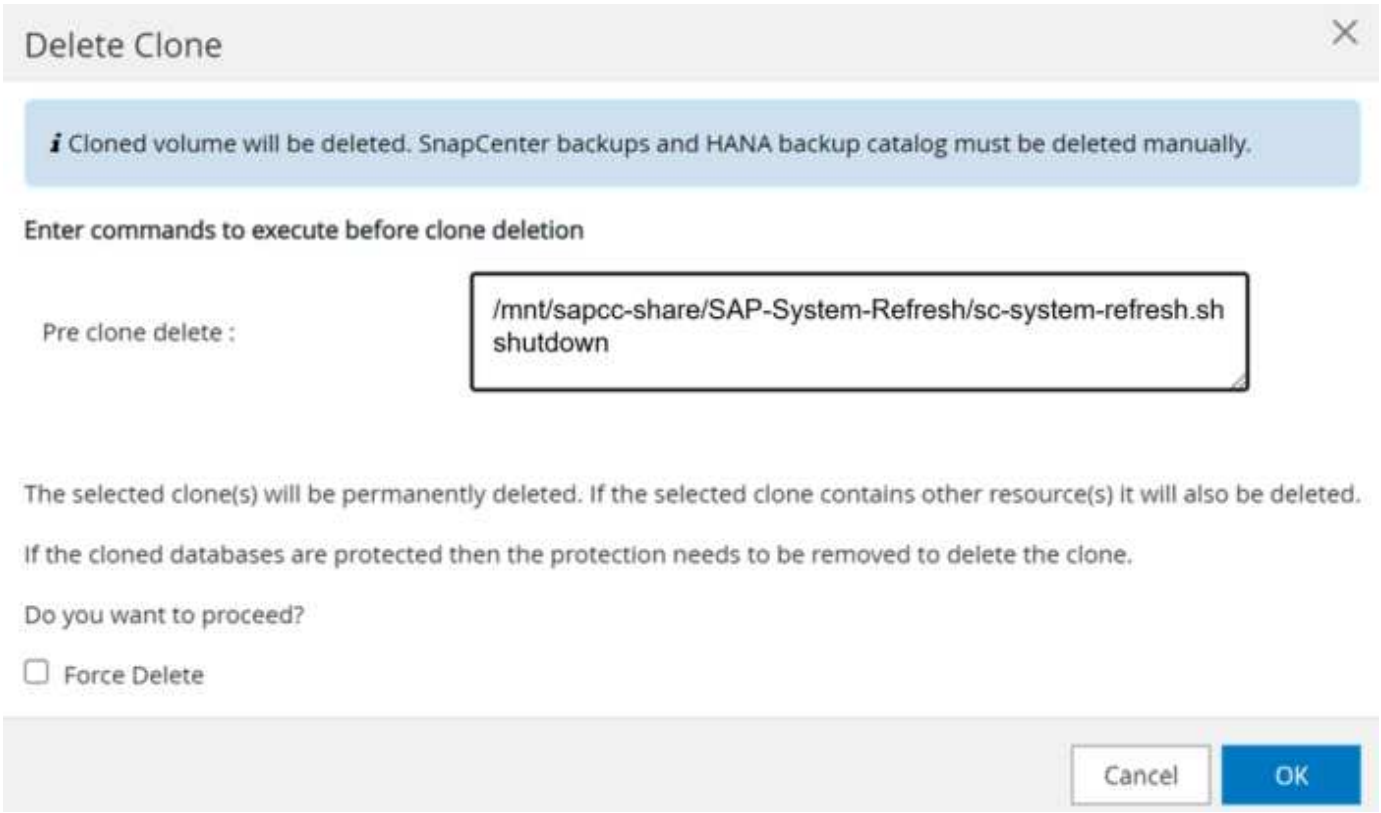
ターゲットのSAP HANAシステムがSnapCenterで保護されている場合は、まず保護を削除する必要があります。ターゲットシステムのトポロジビューで、Remove Protection（保護の削除）をクリックします。

クローン削除ワークフローを次の手順で実行します。

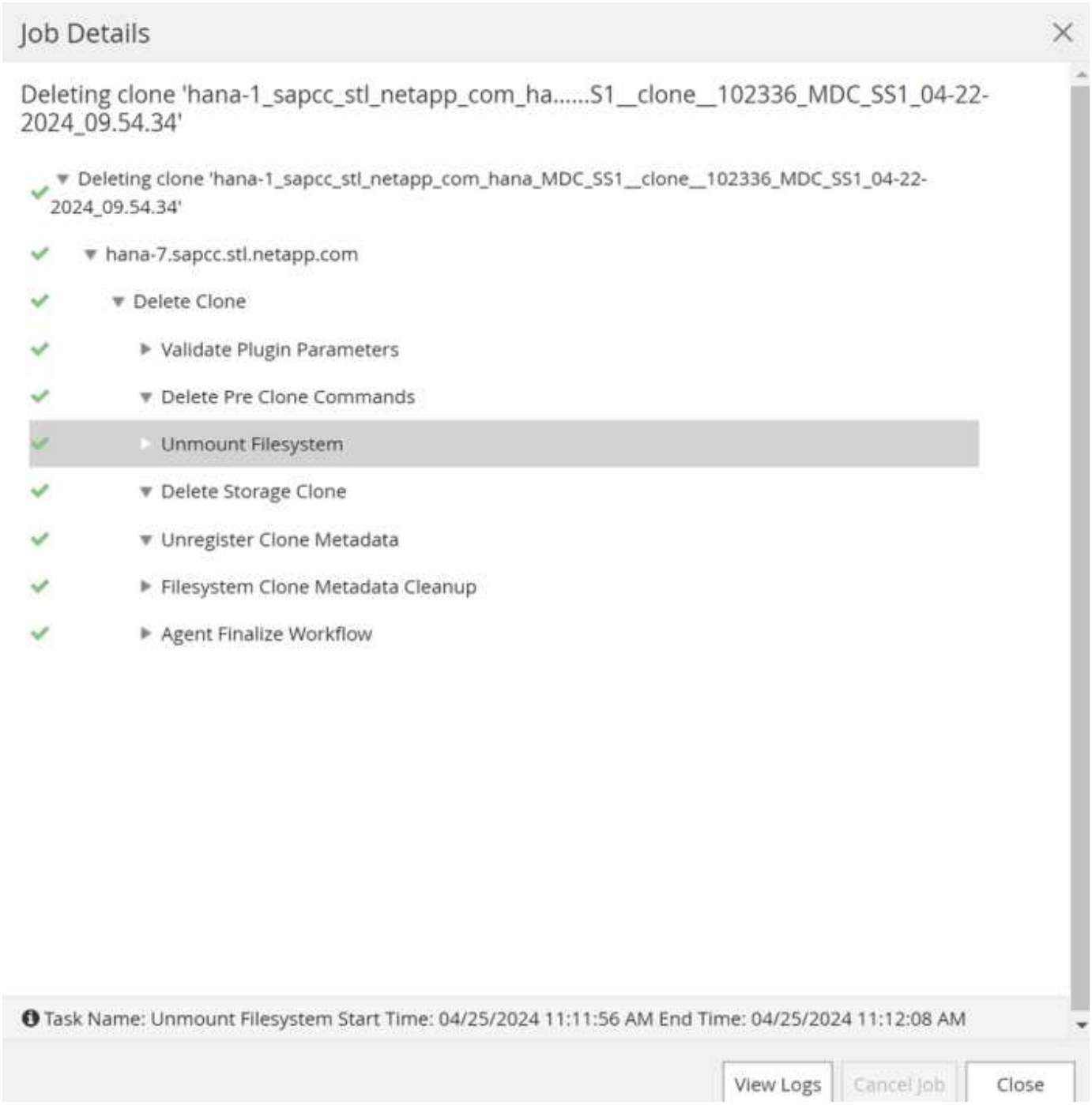
1. ソースシステムのトポロジビューでクローンを選択し、[Delete]をクリックします。




1. 必要なコマンドラインオプションを使用して、クローニング前スクリプトとアンマウント後スクリプトを入力します。




1. SnapCenter のジョブ詳細画面に処理の進捗状況が表示されます。




1. スクリプトのログファイルに `sc-system-refresh` は、シャットダウンとアンマウントの処理手順が表示されます。

```
20240425111042###hana-7###sc-system-refresh.sh:
**********************************************************************
********
20240425111042###hana-7###sc-system-refresh.sh: Script version: 3.0
20240425111042###hana-7###sc-system-refresh.sh: ******************
Starting script: shutdown operation *************************
20240425111042###hana-7###sc-system-refresh.sh: Stopping HANA database.
20240425111042###hana-7###sc-system-refresh.sh: sapcontrol -nr 11
-function StopSystem HDB
25.04.2024 11:10:42
StopSystem
OK
20240425111042###hana-7###sc-system-refresh.sh: Wait until SAP HANA
database is stopped ....
20240425111042###hana-7###sc-system-refresh.sh: Status: GREEN
20240425111052###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111103###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111113###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111123###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111133###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111144###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111154###hana-7###sc-system-refresh.sh: Status: GRAY
20240425111154###hana-7###sc-system-refresh.sh: SAP HANA database is
stopped.
20240425111154###hana-7###sc-system-refresh.sh: ******************
Finished script: shutdown operation *************************
```

1. SnapCenter のクローン作成処理を使用して、SAP HANAの更新処理を再開できるようになりました。

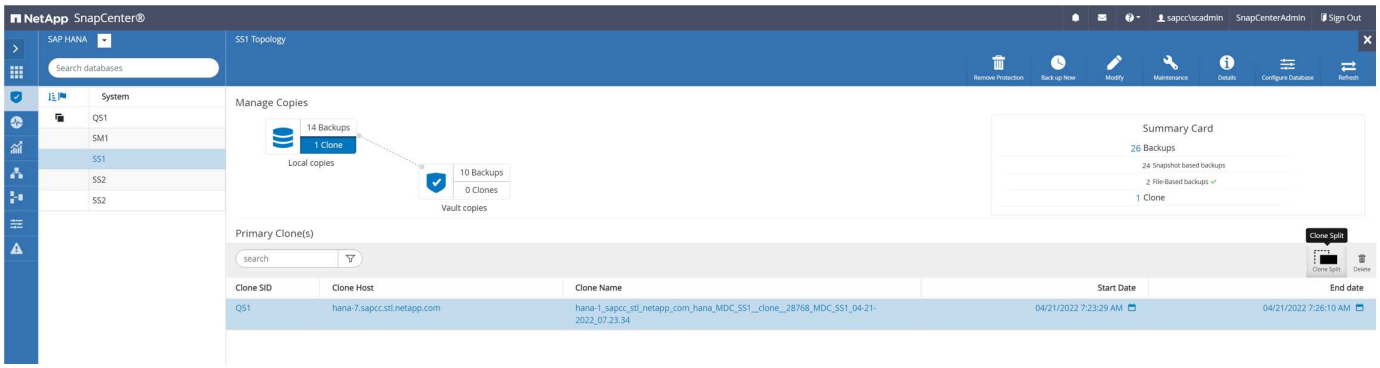
クローンスプリット処理を使用した**SAP HANA**システムの更新

システム更新処理のターゲットシステムを長期間使用する予定がある場合は、システム更新処理の一環としてFlexCloneボリュームをスプリットすることを推奨します。

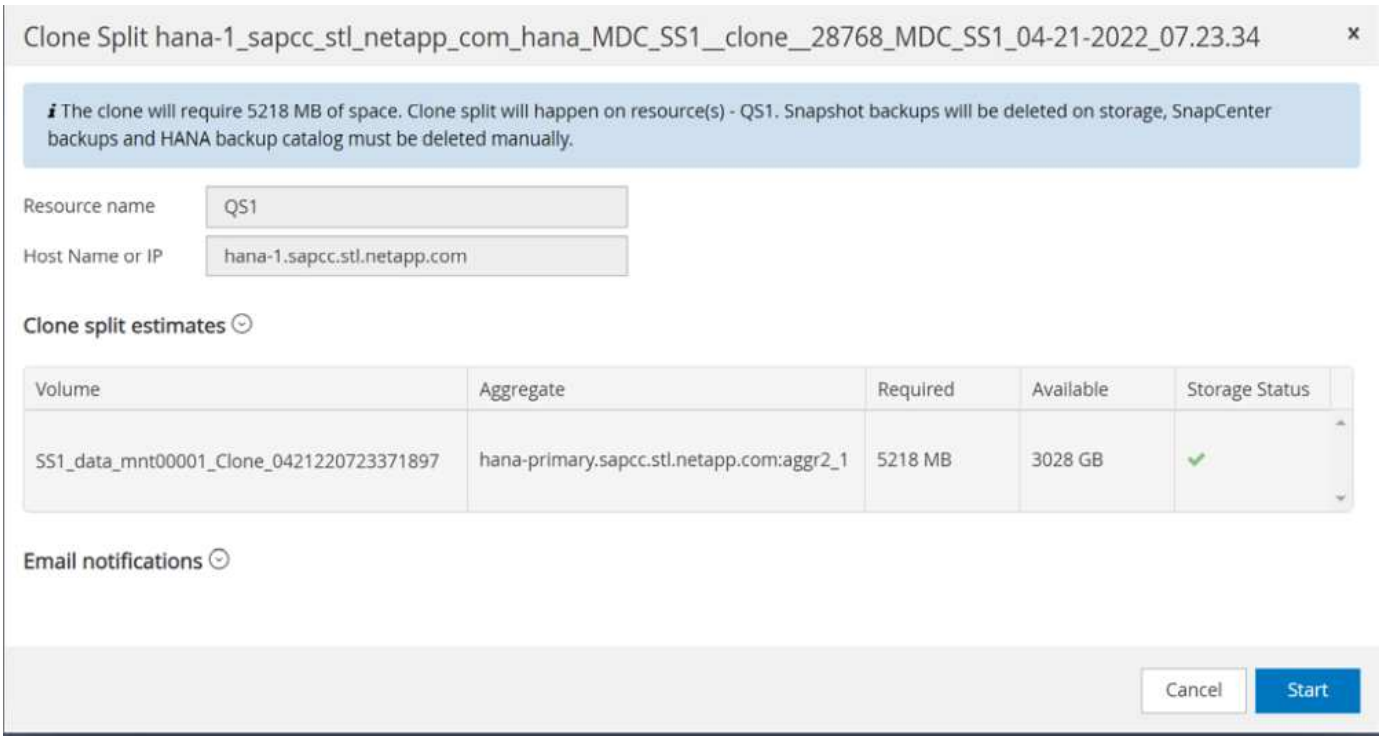
> クローンスプリット処理でクローンボリュームの使用がブロックされることはないため、SAP HANAデータベースの使用中にいつでも実行できます。

> Azure NetApp FilesではAzure NetApp Files、作成後に常にクローンがスプリットされるため、クローンスプリット処理は実行できません。

SnapCenter のクローンスプリットのワークフローは、クローンを選択してクローンスプリットをクリックすることで、ソースシステムのトポロジビューで開始されます。



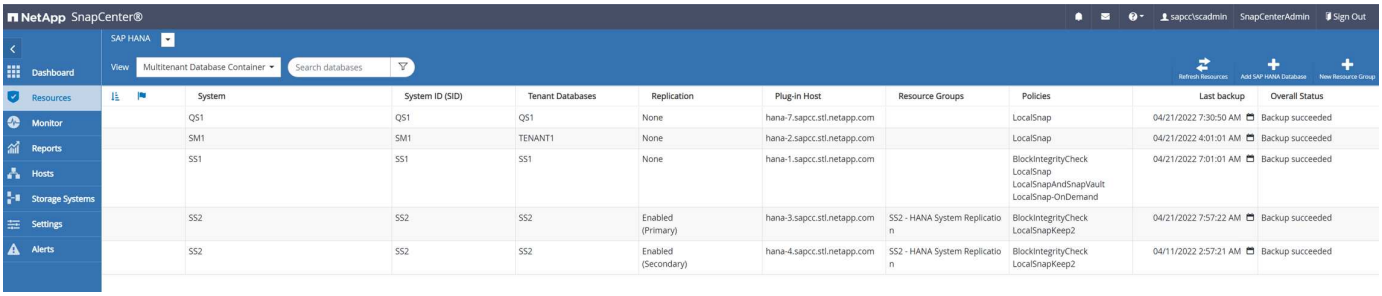

次の画面には、スプリットボリュームに必要な容量に関する情報がプレビューで表示されます。

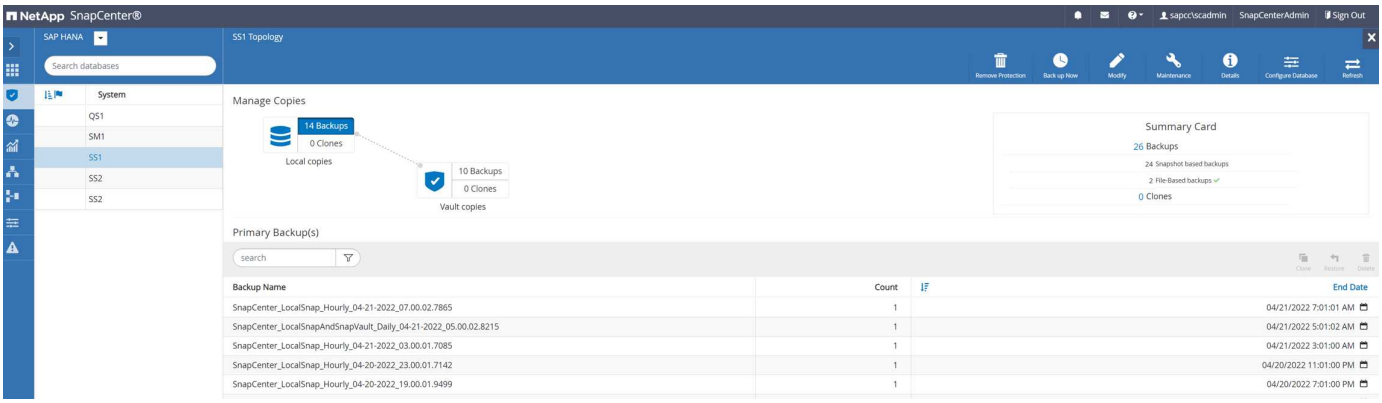



SnapCenter ジョブログには、クローンスプリット処理の進捗状況が表示されます。




SnapCenterのリソースビューで、ターゲットシステムQS1がクローニングされたリソースとしてマークされなくなりました。ソースシステムのトポロジビューに戻ると、クローンは表示されなくなります。スプリットボリュームは、ソースシステムのSnapshotバックアップとは独立しています。




クローンスプリット処理後の更新ワークフローは、クローンスプリットを使用しない処理と少し異なります。クローンスプリット処理後は、ターゲットデータボリュームがFlexCloneボリュームでなくなるため、クローン削除処理は必要ありません。

このワークフローは、次の手順で構成されます。

1. ターゲットのSAP HANAシステムがSnapCenterで保護されている場合は、まず保護を削除する必要があります。
2. SAP HANAデータベースをシャットダウンし、データボリュームをアンマウントして、SnapCenterで作成されたfstabエントリを削除する必要があります。これらの手順は手動で実行する必要があります。
3. これで、前のセクションで説明したように、SnapCenterクローン作成ワークフローを実行できるようになりました。
4. 更新処理後も古いターゲットデータボリュームは引き続き存在するため、ONTAP System Managerなどを使用して手動で削除する必要があります。

### PowerShellスクリプトによるSnapCenter ワークフロー自動化

前のセクションでは、SnapCenter UIを使用してさまざまなワークフローを実行し、PowerShellスクリプトまたはREST API呼び出しを使用してすべてのワークフローを実行することもできるため、さらなる自動化が可能です。以降のセクションでは、以降のワークフローの基本的なPowerShellスクリプトの例について説明します。

- クローンを作成します
- クローンを削除します

> このサンプルスクリプトは現状のまま提供されており、ネットアップではサポートしていません。

すべてのスクリプトはPowerShellコマンドウィンドウで実行する必要があります。スクリプトを実行する前に'Open-SmConnection'コマンドを使用してSnapCenter サーバへの接続を確立する必要があります

クローンを作成します

以下の簡単なスクリプトは、PowerShellコマンドを使用してSnapCenter クローン作成処理を実行する方法を示しています。SnapCenter の「New-SmClone」コマンドは、ラボ環境に必要なコマンドライン・オプションと、前述した自動化スクリプトを使用して実行します。

```
$BackupName='SnapCenter_hana-1_LocalSnap_Hourly_06-25-2024_03.00.01.8458'
$JobInfo=New-SmClone -AppPluginCode hana -BackupName $BackupName
-Resources @\{"Host"="hana-1.sapcc.stl.netapp.com";"UID"="MDC\SS1"}
-CloneToInstance hana-7.sapcc.stl.netapp.com -postclonecreatecommands
'/mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh recover'
-NFSExportIPs 192.168.175.75 -CloneUid 'MDC\QS1'
# Get JobID of clone create job
$Job=Get-SmJobSummaryReport | ?\{$_.JobType -eq "Clone" } | ?\{$_.JobName
-Match $BackupName} | ?\{$_.Status -eq "Running"}
$JobId=$Job.SmJobId
Get-SmJobSummaryReport -JobId $JobId
# Wait until job is finished
do \{ $Job=Get-SmJobSummaryReport -JobId $JobId; write-host $Job.Status;
sleep 20 } while ( $Job.Status -Match "Running" )
Write-Host " "
Get-SmJobSummaryReport -JobId $JobId
Write-Host "Clone create job has been finshed."
```

画面出力には、クローン作成PowerShellスクリプトの実行状況が表示されます。

```
PS C:\Windows\system32> C:\NetApp\clone-create.ps1
SmJobId : 110382
JobCreatedDateTime :
JobStartDateTime : 6/26/2024 9:55:34 AM
JobEndDateTime :
JobDuration :
JobName : Clone from backup 'SnapCenter_hana-1_LocalSnap_Hourly_06-25-
2024_03.00.01.8458'
JobDescription :
Status : Running
IsScheduled : False
JobError :
JobType : Clone
PolicyName :
JobResultData :
Running
Running
Running
Running
Running
Running
Running
Running
Running
Running
Completed
SmJobId : 110382
JobCreatedDateTime :
JobStartDateTime : 6/26/2024 9:55:34 AM
JobEndDateTime : 6/26/2024 9:58:50 AM
JobDuration : 00:03:16.6889170
JobName : Clone from backup 'SnapCenter_hana-1_LocalSnap_Hourly_06-25-
2024_03.00.01.8458'
JobDescription :
Status : Completed
IsScheduled : False
JobError :
JobType : Clone
PolicyName :
JobResultData :
Clone create job has been finshed.
```

クローンを削除します

以下の簡単なスクリプトは、PowerShellコマンドを使用してSnapCenter クローンの削除処理を実行する方法

を示しています。SnapCenter のRemove-SmCloneコマンドは'実習環境に必要なコマンド・ライン・オプションと'前に説明した自動化スクリプトを使用して実行します

```
$CloneInfo=Get-SmClone |?\{$_.CloneName -Match "hana-
1_sapcc_stl_netapp_com_hana_MDC_SS1" }
$JobInfo=Remove-SmClone -CloneName $CloneInfo.CloneName -PluginCode hana
-PreCloneDeleteCommands '/mnt/sapcc-share/SAP-System-Refresh/sc-system-
refresh.sh shutdown QS1' -UnmountCommands '/mnt/sapcc-share/SAP-System-
Refresh/sc-system-refresh.sh umount QS1' -Confirm: $False
Get-SmJobSummaryReport -JobId $JobInfo.Id
# Wait until job is finished
do \{ $Job=Get-SmJobSummaryReport -JobId $JobInfo.Id; write-host
$Job.Status; sleep 20 } while ( $Job.Status -Match "Running" )
Write-Host " "
Get-SmJobSummaryReport -JobId $JobInfo.Id
Write-Host "Clone delete job has been finshed."
PS C:\NetApp>
```

画面出力には、PowerShellスクリプトclone–delete.ps1が実行されたことが示されています。

```
PS C:\Windows\system32> C:\NetApp\clone-delete.ps1
SmJobId : 110386
JobCreatedDateTime :
JobStartDateTime : 6/26/2024 10:01:33 AM
JobEndDateTime :
JobDuration :
JobName : Deleting clone 'hana-
1_sapcc_stl_netapp_com_hana_MDC_SS1__clone__110382_MDC_SS1_04-22-
2024_09.54.34'
JobDescription :
Status : Running
IsScheduled : False
JobError :
JobType : DeleteClone
PolicyName :
JobResultData :
Running
Running
Running
Running
Completed
SmJobId : 110386
JobCreatedDateTime :
JobStartDateTime : 6/26/2024 10:01:33 AM
JobEndDateTime : 6/26/2024 10:02:38 AM
JobDuration : 00:01:05.5658860
JobName : Deleting clone 'hana-
1_sapcc_stl_netapp_com_hana_MDC_SS1__clone__110382_MDC_SS1_04-22-
2024_09.54.34'
JobDescription :
Status : Completed
IsScheduled : False
JobError :
JobType : DeleteClone
PolicyName :
JobResultData :
Clone delete job has been finshed.
PS C:\Windows\system32>
```

## SnapCenter によるSAPシステムのクローニング

このセクションでは、SAPシステムのクローニング処理の手順ごとの概要 を示します。このを使用して、論理的な破損に対処するための修復システムをセットアップできます。

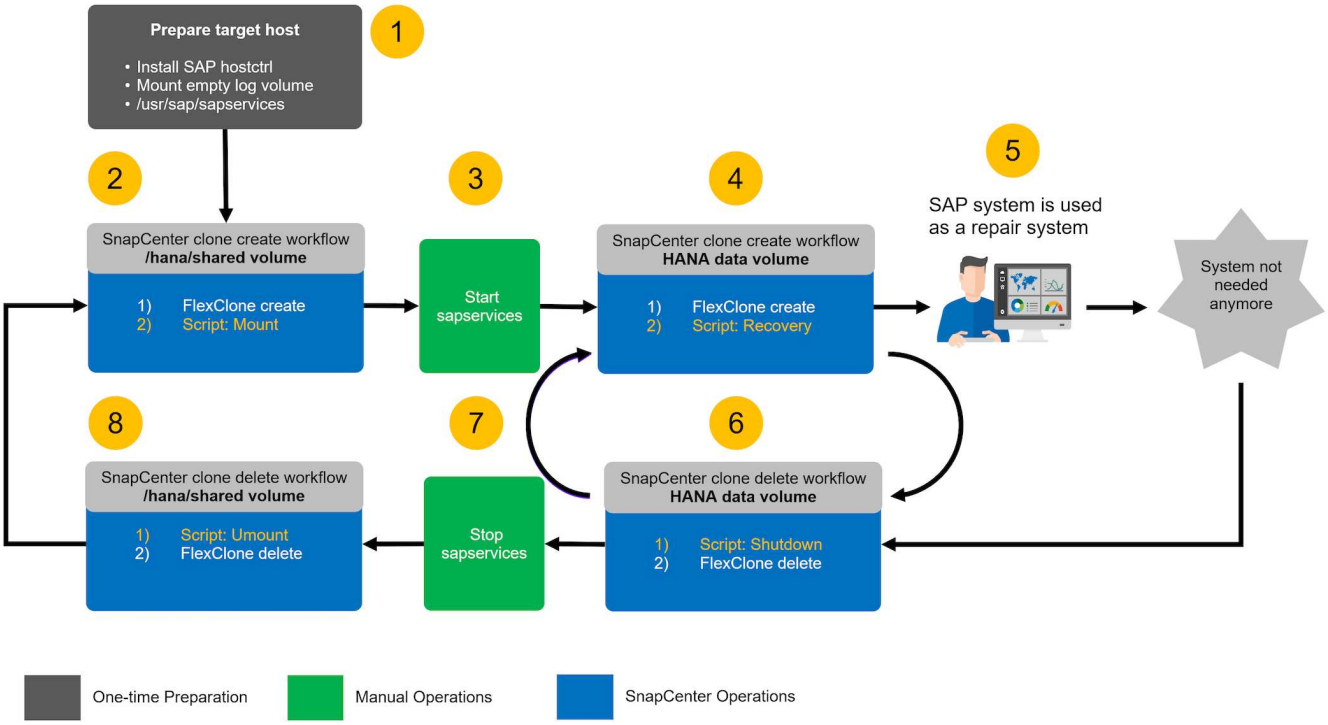
次の図は、SnapCenterを使用したSAPシステムのクローニング処理に必要な手順をまとめたものです。

1. ターゲットホストを準備します。
2. SAP HANA共有ボリューム用のSnapCenterクローン作成ワークフロー
3. SAP HANAサービスを開始します。
4. SnapCenterクローンは、SAP HANAデータボリュームのデータベースリカバリを含むワークフローを作成します。
5. SAP HANAシステムを修復システムとして使用できるようになりました。

> システムを別のSnapshotバックアップにリセットする必要がある場合は、手順6と手順4で十分です。SAP HANA共有ボリュームは引き続きマウントできます。

システムが不要になった場合は、次の手順でクリーンアッププロセスを実行します。

6. SAP HANAデータボリュームのSnapCenterクローン削除ワークフロー（データベースのシャットダウンを含む）。
7. SAP HANAサービスを停止します。
8. SAP HANA共有ボリュームのSnapCenterクローン削除ワークフロー




## 前提条件および制限事項

以降のセクションで説明するワークフローには、SAP HANAシステムのアーキテクチャとSnapCenterの設定に関する前提条件と制限事項がいくつかあります。

- ここで説明するワークフローは、シングルホストのSAP HANA MDCシステムに対して有効です。複数のホストシステムはサポートされません。

- 自動スクリプトを実行するには、SnapCenter SAP HANAプラグインをターゲットホストに導入する必要があります。
- NFSのワークフローが検証されました。SAP HANA共有ボリュームのマウントに使用される自動化で`script sc-mount-volume.sh`は、FCPはサポートされません。この手順は、手動で実行するか、スクリプトを拡張して実行する必要があります。
- ここで説明するワークフローは、SnapCenter 5.0リリース以降でのみ有効です。

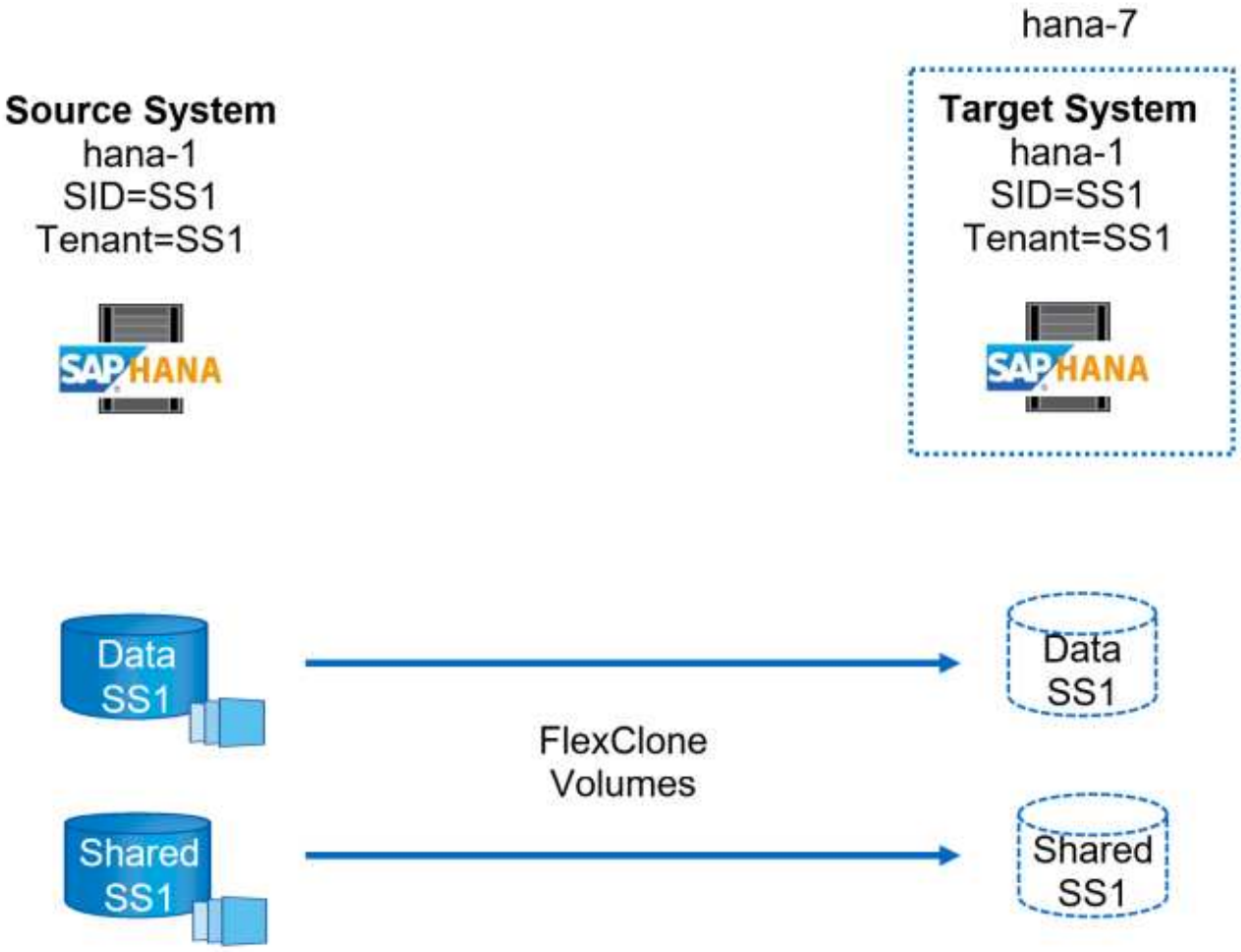
ラボのセットアップ

次の図は、システムのクローン作成に使用するラボのセットアップを示しています。

使用したソフトウェアバージョンは次のとおりです。

- SnapCenter 5.0
- SAP HANAシステム：HANA 2.0 SPS6 rev.61
- SLES 15
- ONTAP 9.7P7.

すべてのSAP HANAシステムは、構成ガイドに基づいて設定する必要があります"NFSを使用したNetApp AFFシステムでのSAP HANA"。SnapCenterとSAP HANAのリソースは、ベストプラクティスガイドに基づいて設定されました"SnapCenter を使用した SAP HANA のバックアップとリカバリ"。



## ターゲットホストの準備

ここでは、システムクローンターゲットとして使用するサーバで必要な準備手順について説明します。

通常運用時は、SAP HANA QAやテストシステムなど、他の目的にターゲットホストを使用できます。したがって、前述のほとんどの手順は、システムクローン処理が要求されたときに実行する必要があります。一方、やなどの関連する設定ファイルは `/etc/fstab` 、 `/usr/sap/sapservices`設定ファイルをコピーするだけで準備し、本番環境に置くことができます。

ターゲットホストの準備には、SAP HANA QAまたはテストシステムのシャットダウンも含まれます。

### ターゲットサーバーのホスト名とIPアドレス

ターゲット・サーバのホスト名は ' ソース・システムのホスト名と同じである必要がありますIP アドレスは異なっていてもかまいません。

ターゲットサーバが他のシステムと通信できないように、ターゲットサーバの適切なフェンシングを確立する必要があります。適切なフェンシングが設定されていないと、クローニングされた本番用システムは他の本番用システムとデータを交換する可能性があります。

このラボ環境では、ターゲットシステム側から見て、ターゲットシステムのホスト名を内部的にのみ変更しました。ホストの外部からは、ホスト名として「HANA -7」を使用してアクセスできました。ホストにログインすると、ホスト自体がHANAです。

### 必要なソフトウェアのインストール

SAP ホストエージェントソフトウェアをターゲットサーバにインストールする必要があります。詳細については、SAPヘルプポータルのを参照して "SAP ホストエージェント" ください。

SnapCenterでのホストの追加処理を使用して、SnapCenter SAP HANAプラグインをターゲットホストに導入する必要があります。

### ユーザー'ポート'およびSAPサービスの構成

ターゲットサーバに、 SAP HANA データベースに必要なユーザとグループが配置されている必要があります。通常は、ユーザの一元管理が使用されるため、ターゲットサーバで設定手順を行う必要はありません。SAP HANAデータベースに必要なポートがターゲットホストに設定されている必要があります。/etc/servicesファイルをターゲット・サーバにコピーすることにより'ソース・システムから構成をコピーできます

必要な SAP サービスのエントリがターゲットホストにあることが必要です。/usr/sap/sapservices' ファイルをターゲットサーバにコピーすることで ' ソースシステムから構成をコピーできます次の出力は、このラボ環境で使用する SAP HANA データベースの必須エントリを示しています。

```
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/SS1/HDB00/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/SS1/HDB00/exe/sapstartsrv
pf=/usr/sap/SS1/SYS/profile/SS1_HDB00_hana-1 -D -u ss1adm
limit.descriptors=1048576
```

ログとログのバックアップボリュームを準備

ログボリュームをソースシステムからクローニングする必要はなく、clear logオプションを使用してリカバリを実行するため、空のログボリュームをターゲットホストで準備しておく必要があります。

ソースシステムには独立したログバックアップボリュームが設定されているため、空のログバックアップボリュームを準備し、ソースシステムと同じマウントポイントにマウントする必要があります。

```
hana-1:/# cat /etc/fstab
192.168.175.117:/SS1_repair_log_mnt00001 /hana/log/SS1/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
192.168.175.117:/SS1_repair_log_backup /mnt/log-backup nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
```

ログボリュームhdb*内では、ソース・システムと同じ方法でサブディレクトリを作成する必要があります。

```
hana-1:/ # ls -al /hana/log/SS1/mnt00001/
total 16
drwxrwxrwx 5 root root 4096 Dec 1 06:15 .
drwxrwxrwx 1 root root 16 Nov 30 08:56 ..
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:14 hdb00001
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:15 hdb00002.00003
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:15 hdb00003.00003
```

ログバックアップボリュームには、システムとテナントデータベースのサブディレクトリを作成する必要があります。

```
hana-1:/ # ls -al /mnt/log-backup/
total 12
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 04:48 .
drwxr-xr-- 2 ss1adm sapsys 4896 Dec 1 03:42 ..
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:15 DB_SS1
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:14 SYSTEMDB
```

ファイル・システム・マウントの準備

データおよび共有ボリュームのマウントポイントを準備しておく必要があります。

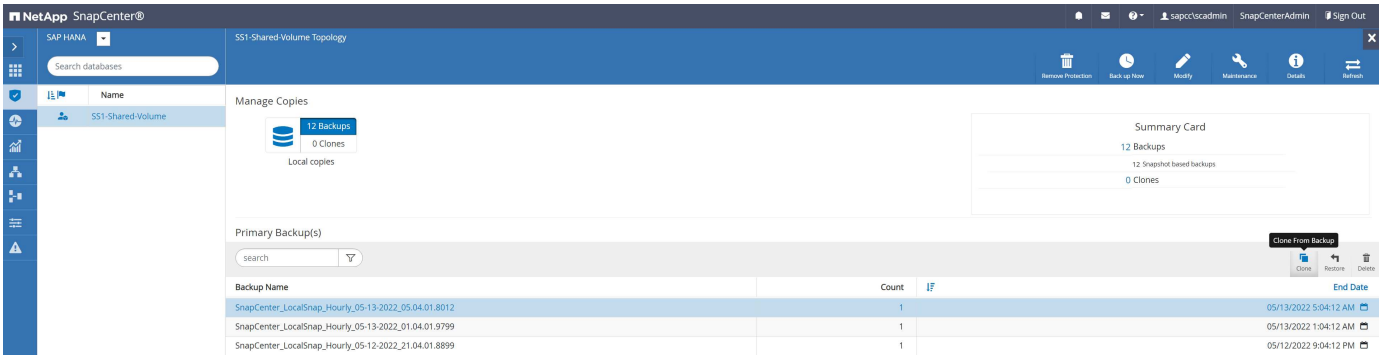
この例では、ディレクトリ `/hana/data/SS1/mnt00001`、 `/hana/shared` および `usr/sap/SS1` を作成する必要があります。

ターゲットシステムで実行するスクリプトを、SnapCenter allowed commands configファイルに追加する必要があります。

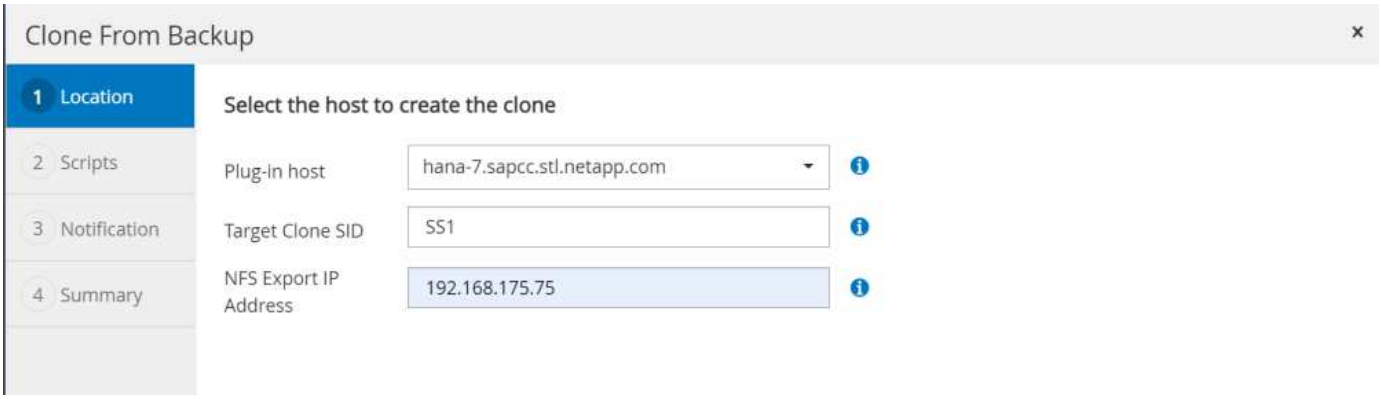
```
hana-7:/opt/NetApp/snapcenter/scc/etc # cat
/opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh
command: /mnt/sapcc-share/SAP-System-Refresh/sc-mount-volume.sh
hana-7:/opt/NetApp/snapcenter/scc/etc #
```

## HANA共有ボリュームのクローニング

1. ソースシステムのSS1共有ボリュームからSnapshotバックアップを選択し、[Clone]をクリックします。

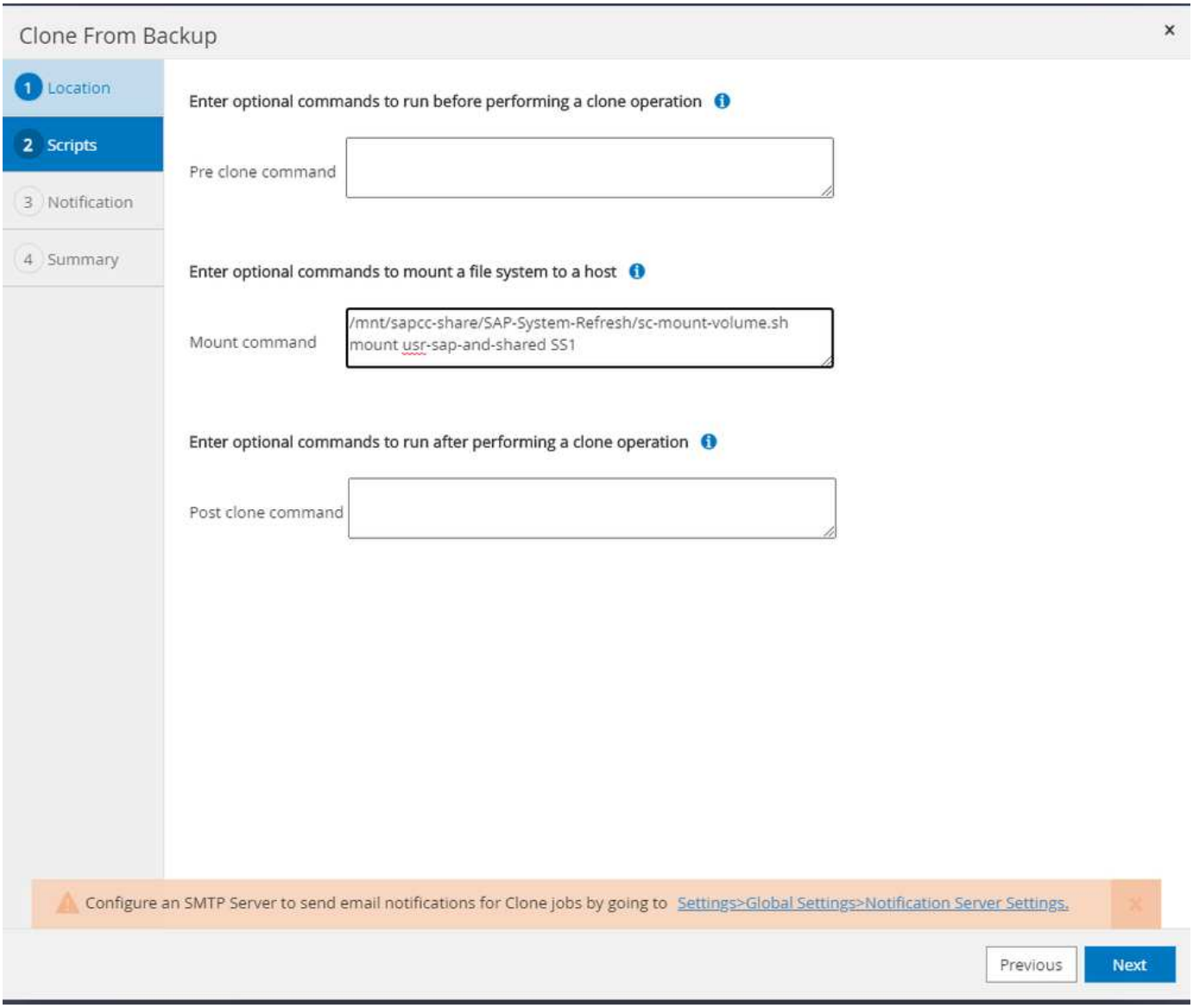



1. ターゲット修復システムの準備が完了したホストを選択します。NFSエクスポートのIPアドレスは、ターゲットホストのストレージネットワークインターフェイスである必要があります。ターゲットSIDとして、ソースシステムと同じSIDを保持します。この例では、SS1。

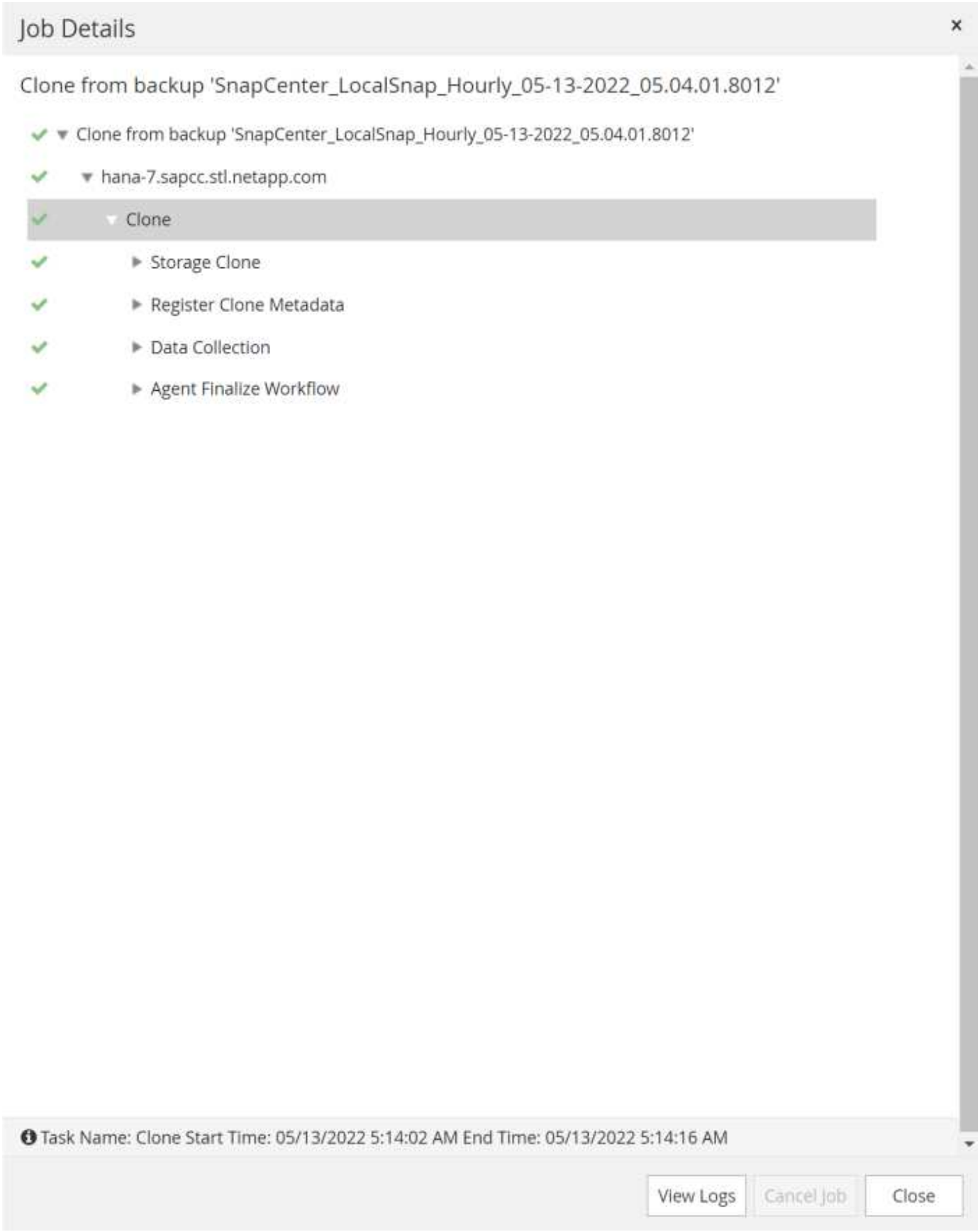



1. 必要なコマンドラインオプションを指定して、マウントスクリプトを入力します。

SAP HANAシステムでは、構成ガイドで推奨されているように、および`/usr/sap/SS1`単一のボリュームをサブディレクトリに分けて使用します`/hana/shared`"NFSを使用したNetApp AFF システムでのSAP HANA"。スクリプト`sc-mount-volume.sh`では、マウントパスに特別なコマンドラインオプションを使用してこの設定をサポートしています。mount pathコマンドラインオプションをusr-sap-and-sharedと指定すると、sharedおよびusr-sapのサブディレクトリがボリューム内に適宜マウントされます。




1. SnapCenter の[ジョブの詳細]画面に、処理の進捗状況が表示されます。



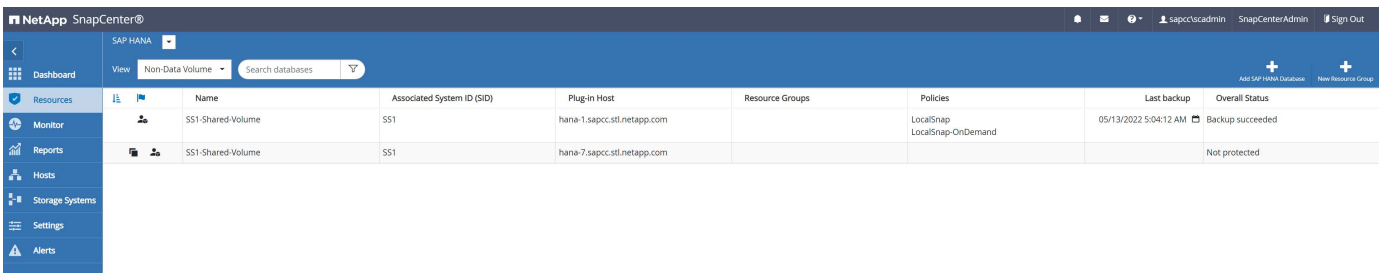

1. sc-mount-volume.shスクリプトのログファイルには、マウント処理で実行されたさまざまな手順が表示されます。

```
20201201041441###hana-1###sc-mount-volume.sh: Adding entry in /etc/fstab.
20201201041441###hana-1###sc-mount-volume.sh:
192.168.175.117://SS1_shared_Clone_05132205140448713/usr-sap /usr/sap/SS1
nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
20201201041441###hana-1###sc-mount-volume.sh: Mounting volume: mount
/usr/sap/SS1.
20201201041441###hana-1###sc-mount-volume.sh:
192.168.175.117:/SS1_shared_Clone_05132205140448713/shared /hana/shared
nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
20201201041441###hana-1###sc-mount-volume.sh: Mounting volume: mount
/hana/shared.
20201201041441###hana-1###sc-mount-volume.sh: usr-sap-and-shared mounted
successfully.
20201201041441###hana-1###sc-mount-volume.sh: Change ownership to ss1adm.
```

1. SnapCenterワークフローが完了すると、/usr/sap/ss1と/hana/sharedファイルシステムがターゲットホストにマウントされます。

```
hana-1:~ # df
Filesystem 1K-blocks Used Available Use% Mounted on
192.168.175.117:/SS1_repair_log_mnt00001 262144000 320 262143680 1%
/hana/log/SS1/mnt00001
192.168.175.100:/sapcc_share 1020055552 53485568 966569984 6% /mnt/sapcc-
share
192.168.175.117:/SS1_repair_log_backup 104857600 256 104857344 1%
/mnt/log-backup
192.168.175.117:/SS1_shared_Clone_05132205140448713/usr-sap 262144064
10084608 252059456 4% /usr/sap/SS1
192.168.175.117:/SS1_shared_Clone_05132205140448713/shared 262144064
10084608 252059456 4% /hana/shared
```

1. SnapCenter では、クローニングされたボリュームの新しいリソースが表示されます。



1. /hana/sharedボリュームが使用可能になったので、SAP HANAサービスを開始できます。

```
hana-1:/mnt/sapcc-share/SAP-System-Refresh # systemctl start sapinit
```

1. これで'SAPホスト・エージェントとsapstartsrvのプロセスが開始されました

```
hana-1:/mnt/sapcc-share/SAP-System-Refresh # ps -ef |grep sap
root 12377 1 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saphostexec
pf=/usr/sap/hostctrl/exe/host_profile
sapadm 12403 1 0 04:34 ? 00:00:00 /usr/lib/systemd/systemd --user
sapadm 12404 12403 0 04:34 ? 00:00:00 (sd-pam)
sapadm 12434 1 1 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/sapstartsrv
pf=/usr/sap/hostctrl/exe/host_profile -D
root 12485 12377 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saphostexec
pf=/usr/sap/hostctrl/exe/host_profile
root 12486 12485 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
ss1adm 12504 1 0 04:34 ? 00:00:00 /usr/sap/SS1/HDB00/exe/sapstartsrv
pf=/usr/sap/SS1/SYS/profile/SS1_HDB00_hana-1 -D -u ss1adm
root 12582 12486 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root 12585 7613 0 04:34 pts/0 00:00:00 grep --color=auto sap
hana-1:/mnt/sapcc-share/SAP-System-Refresh #
```

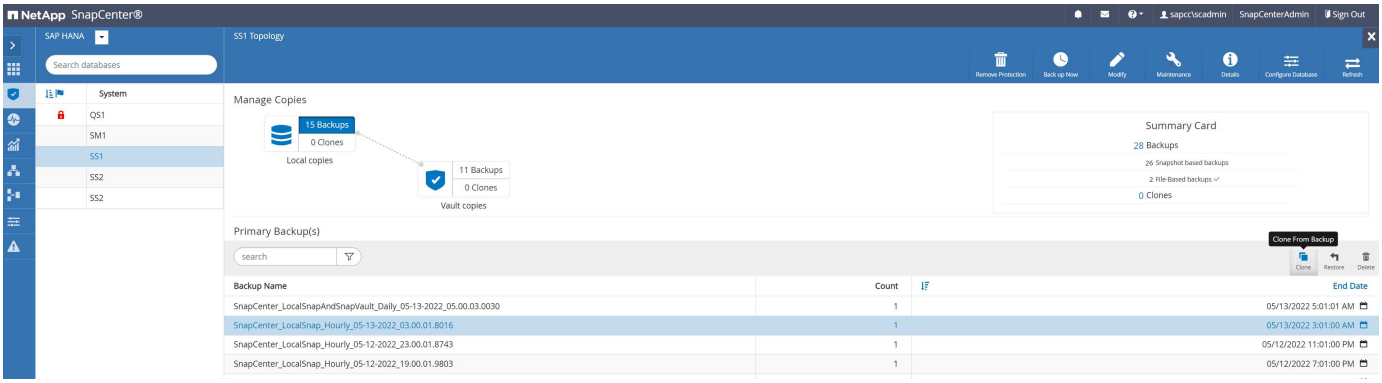
追加の**SAP**アプリケーションサービスのクローニング

その他のSAPアプリケーションサービスのクローニングは、セクション「SAP HANA共有ボリュームのクローニング」で説明したSAP HANA共有ボリュームと同じ方法で行います。もちろん、SAPアプリケーションサーバに必要なストレージボリュームもSnapCenterで保護する必要があります。

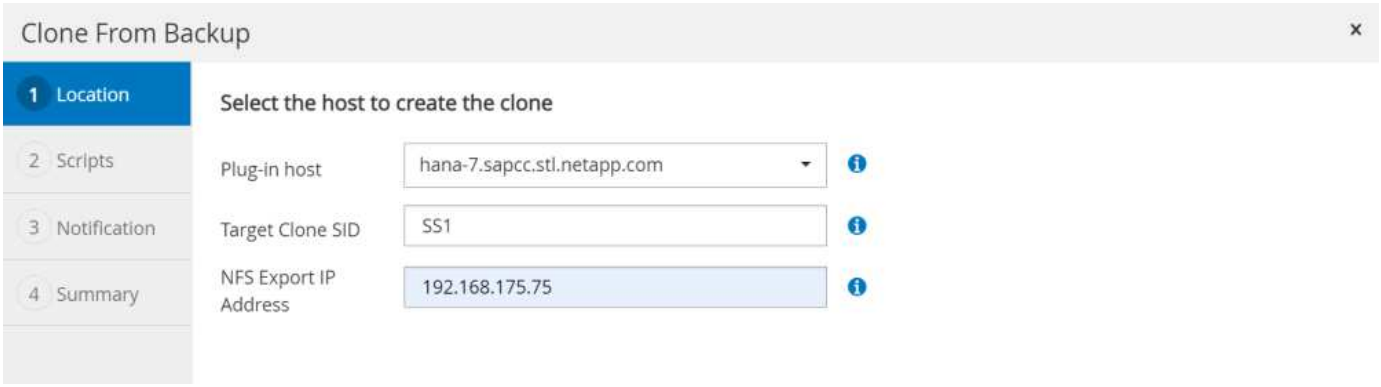
必要なサービスエントリを/usr/sap/sapservicesに追加し、ポート、ユーザ、およびファイルシステムのマウントポイント（/usr/sap/SIDなど）を準備しておく必要があります。

データボリュームのクローニングと**HANA**データベースのリカバリ

1. ソースシステムSS1からSAP HANA Snapshotバックアップを選択します。

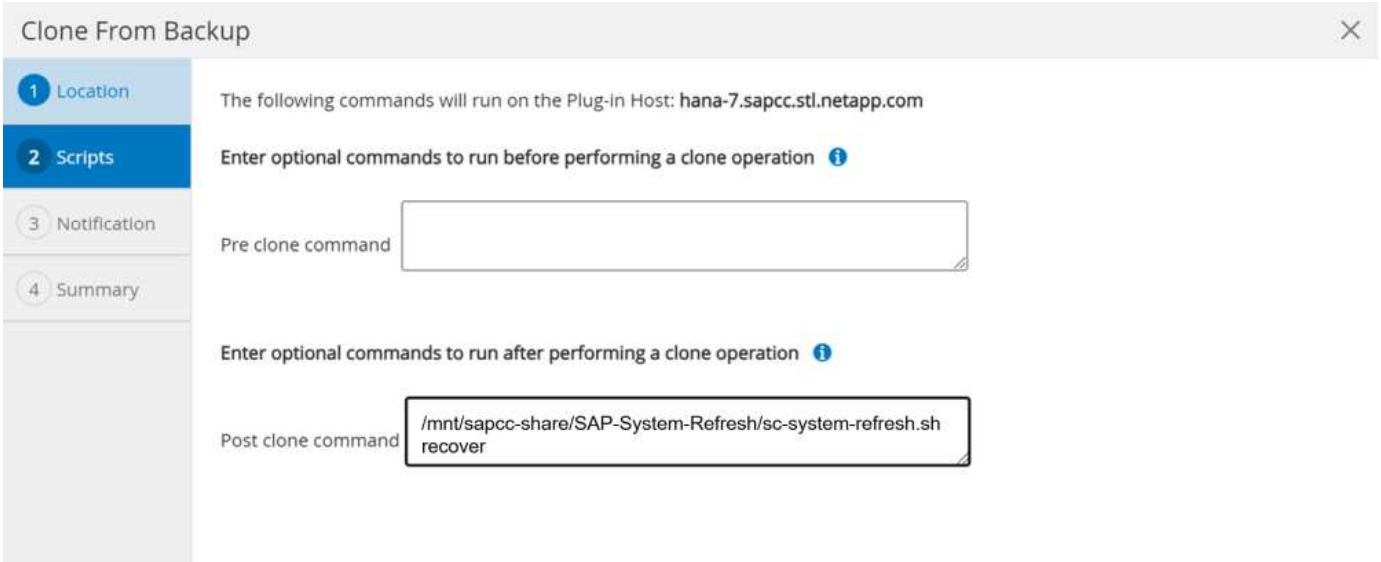



1. ターゲット修復システムの準備が完了したホストを選択します。NFSエクスポートのIPアドレスは、ターゲットホストのストレージネットワークインターフェイスである必要があります。ターゲットSIDとして、ソースシステムと同じSIDを保持します。この例では、SS1

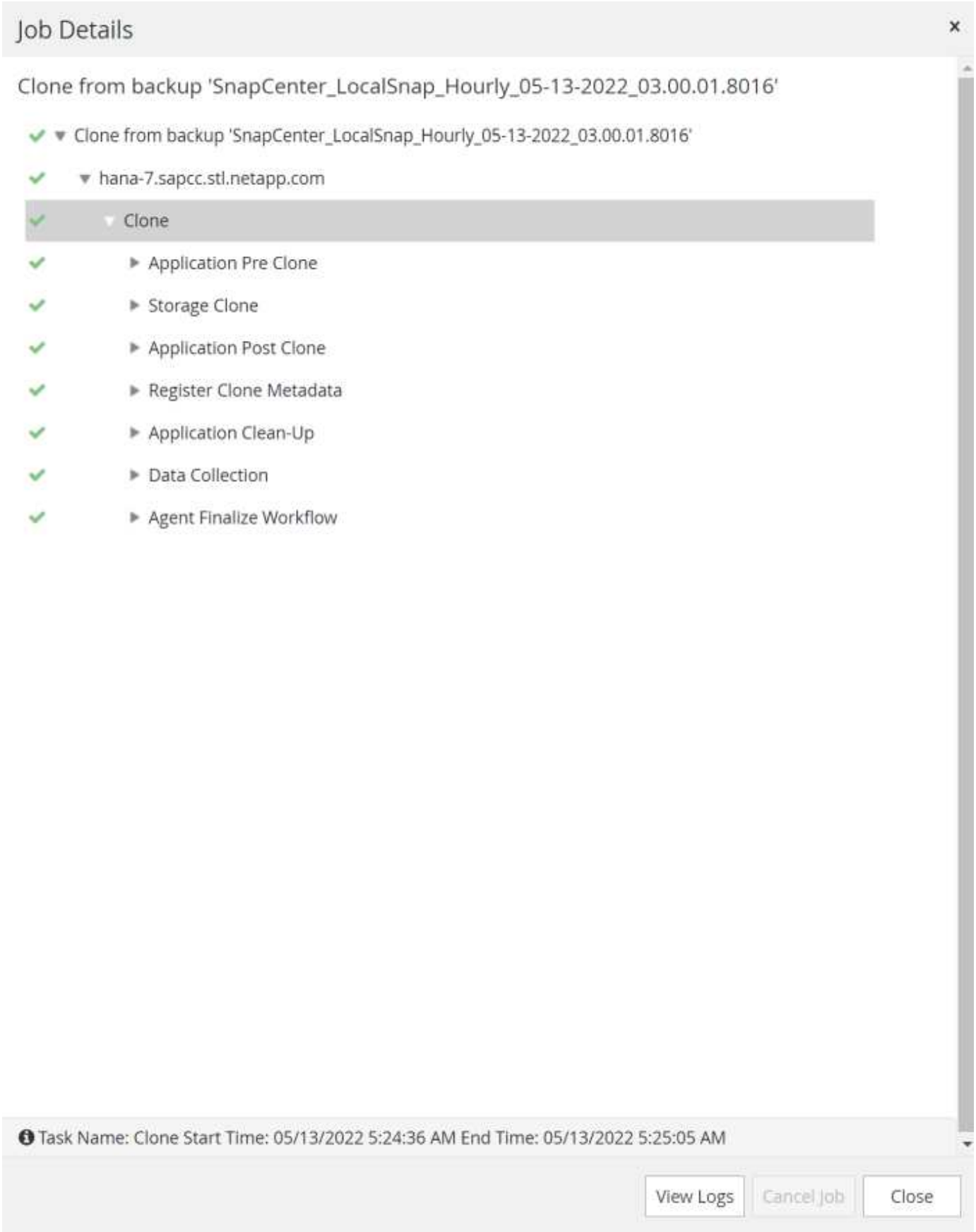



1. 必要なコマンドラインオプションを指定して、クローニング後のスクリプトを入力します。

リカバリ処理用スクリプトは、Snapshot処理の時点までSAP HANAデータベースをリカバリし、フォワードリカバリを実行しません。特定の時点までのフォワードリカバリが必要な場合は、リカバリを手動で実行する必要があります。手動フォワードリカバリでは、ソースシステムのログバックアップをターゲットホストで利用できることも必要です。



SnapCenter のジョブ詳細画面に処理の進捗状況が表示されます。



スクリプトのログファイル sc-system-refresh には、マウント処理とリカバリ処理に対して実行されるさまざまな手順が表示されます。

```
20201201052124###hana-1###sc-system-refresh.sh: Recover system database.
20201201052124###hana-1###sc-system-refresh.sh:
/usr/sap/SS1/HDB00/exe/Python/bin/python
/usr/sap/SS1/HDB00/exe/python_support/recoverSys.py --command "RECOVER
DATA USING SNAPSHOT CLEAR LOG"
20201201052156###hana-1###sc-system-refresh.sh: Wait until SAP HANA
database is started ....
20201201052156###hana-1###sc-system-refresh.sh: Status: GRAY
20201201052206###hana-1###sc-system-refresh.sh: Status: GREEN
20201201052206###hana-1###sc-system-refresh.sh: SAP HANA database is
started.
20201201052206###hana-1###sc-system-refresh.sh: Source system has a single
tenant and tenant name is identical to source SID: SS1
20201201052206###hana-1###sc-system-refresh.sh: Target tenant will have
the same name as target SID: SS1.
20201201052206###hana-1###sc-system-refresh.sh: Recover tenant database
SS1.
20201201052206###hana-1###sc-system-refresh.sh:
/usr/sap/SS1/SYS/exe/hdb/hdbsql -U SS1KEY RECOVER DATA FOR SS1 USING
SNAPSHOT CLEAR LOG
0 rows affected (overall time 34.773885 sec; server time 34.772398 sec)
20201201052241###hana-1###sc-system-refresh.sh: Checking availability of
Indexserver for tenant SS1.
20201201052241###hana-1###sc-system-refresh.sh: Recovery of tenant
database SS1 succesfully finished.
20201201052241###hana-1###sc-system-refresh.sh: Status: GREEN
After the recovery operation, the HANA database is running and the data
volume is mounted at the target host.
hana-1:/mnt/log-backup # df
Filesystem 1K-blocks Used Available Use% Mounted on
192.168.175.117:/SS1_repair_log_mnt00001 262144000 760320 261383680 1%
/hana/log/SS1/mnt00001
192.168.175.100:/sapcc_share 1020055552 53486592 966568960 6% /mnt/sapcc-
share
192.168.175.117:/SS1_repair_log_backup 104857600 512 104857088 1%
/mnt/log-backup
192.168.175.117:/SS1_shared_Clone_05132205140448713/usr-sap 262144064
10090496 252053568 4% /usr/sap/SS1
192.168.175.117:/SS1_shared_Clone_05132205140448713/shared 262144064
10090496 252053568 4% /hana/shared
192.168.175.117:/SS1_data_mnt00001_Clone_0421220520054605 262144064
3732864 258411200 2% /hana/data/SS1/mnt00001
```

これでSAP HANAシステムが利用可能になり、リペアシステムなどとして使用できます。

### 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。

- "SAP Business Application and SAP HANA Database Solutions（netapp.com）"
- "TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"
- "TR-4436：『SAP HANA on NetApp All Flash FAS Systems with Fibre Channel Protocol』"
- "TR-4435：『SAP HANA on NetApp All Flash FAS Systems with NFS』"
- "TR-4926：『SAP HANA on Amazon FSX for NetApp ONTAP - Backup and Recovery with SnapCenter 』"
- "TR-4953：『NetApp SAP Landscape Management Integration using Ansible』"
- "TR-4929：『Automating SAP system copy operations with Libelle SystemCopy』（netapp.com）"
- "AlpacaとNetApp SnapCenterによるSAPシステムのコピー、更新、クローニングのワークフローの自動化"
- "AvantraとNetApp SnapCenterを使用したSAPシステムのコピー、更新、クローニングのワークフローの自動化"

| バージョン | 日付 | ドキュメントバージョン履歴 |
|---|---|---|
| バージョン 1.0 以降 | 2018 年 2 月 | 初版リリース |
| バージョン 2.0 以降 | 2021年2月 | SnapCenter 4.3および改良された自動化スクリプトを対象とした完全な書き換え+システム更新処理とシステムクローン処理のワークフローの説明が新しくなりました。 |
| バージョン 3.0 以降 | 2022年5月 | SnapCenter 4.6 P1で変更されたワークフローに対応 |
| バージョン 4.0 以降 | 2024年7月 | このドキュメントはオンプレミスのNetAppシステムを対象としています。 FSx for ONTAPとAzure NetApp Files 新しいSnapCenter 5.0の操作クローンの作成と削除のワークフローでのマウントとアンマウント+ファイバチャネルSANの具体的な手順の追加 Azure NetApp Filesの具体的な手順の追加+対応したシンプルなスクリプト+有効なSAP HANAに必要な手順の追加 `sc-system-refresh` |

# Libelle SystemCopyによるSAPシステムのコピー処理の自動化

## TR-4929：Libelle SystemCopyによるSAPシステムのコピー処理の自動化

SAPのライフサイクル管理を最適化するネットアップのソリューションは、SAP AnyDBとSAP HANAデータベースに統合されています。さらに、ネットアップは、アプリケーションと統合された効率的なデータ保護と、SAPテストシステムの柔軟なプロビジョニ

ングを組み合わせた、SAPのライフサイクル管理ツールに統合しています。

著者：

Holger Zecha、Tobias Brandl、ネットアップFranz Diegruber、Libelle

今日のダイナミックなビジネス環境では、企業は継続的なイノベーションを提供し、変化する市場に迅速に対応する必要があります。このような競争の激しい状況下で、業務プロセスの柔軟性を高める企業は、市場の需要に効果的に対応できます。

市場ニーズの変化は、企業のSAP環境にも影響を及ぼし、定期的な統合、変更、更新が必要になります。IT部門は、これらの変更を、より少ないリソースでより短い期間で実装する必要があります。変更を導入する際のリスクを最小限に抑えるには、本番環境の実際のデータを使用するSAPシステムを追加で必要とする、テストとトレーニングを徹底的に実施する必要があります。

従来のSAPライフサイクル管理アプローチでは、このようなシステムは主に手動プロセスに基づいてプロビジョニングされます。このような手動プロセスは、ミスを避けられず、時間もかかることが多く、イノベーションの遅れやビジネス要件への対応の遅れにつながります。

SAPのライフサイクル管理を最適化するネットアップのソリューションは、SAP AnyDBとSAP HANAデータベースに統合されています。さらに、ネットアップは、アプリケーションと統合された効率的なデータ保護と、SAPテストシステムの柔軟なプロビジョニングを組み合わせた、SAPのライフサイクル管理ツールに統合しています。

このようなネットアップのソリューションは、大規模なデータベースでも膨大なデータを効率的に管理するという問題 を解決しますが、SAPシステムの完全なエンドツーエンドのコピーおよび更新処理には、ソースSAPシステムのIDをターゲットシステムに完全に変更するためのコピー前処理とコピー後処理が含まれている必要があります。SAPでは、で必要なアクティビティについて説明します "SAP同種システムのコピーガイド"。ネットアップのパートナー様は、手動プロセスの回数をさらに減らし、SAPシステムのコピープロセスの品質と安定性を高めるために "Libelle" を開発しました "Libelle SystemCopy (LSC)" ツール。Libelleと共同で、SAPシステムコピー用のネットアップソリューションをLSCに統合して提供しています "完全なエンドツーエンドの自動システムコピーを、記録的な時間で作成します"。

アプリケーションに統合された**Snapshot**コピー処理

アプリケーションと整合性のあるNetApp Snapshotコピーをストレージレイヤに作成する機能は、本ドキュメントで説明するシステムコピー処理とシステムクローン処理の基盤となります。ストレージベースのSnapshotコピーは、ネットアップのSnapCenter Plug-in for SAP HANAまたはSAPのネイティブONTAP システム上の任意のDBを使用して作成されます "Microsoft Azure Application Consistent Snapshotツール"（AzAcSnap）、およびMicrosoft Azureで実行されるSAP HANAとOracleデータベースによって提供されるインターフェイス。SAP HANAを使用している場合は、SnapCenter とAzAcSnapがSnapshotコピーをSAP HANAバックアップカタログに登録することで、リストアとリカバリ、およびクローニング処理に使用できます。

オフサイトバックアップやディザスタリカバリのデータレプリケーションを実行できます

アプリケーションと整合性のあるSnapshotコピーは、ストレージレイヤから、オンプレミスのSnapCenter で制御されるオフサイトのバックアップサイトやディザスタリカバリサイトにレプリケートできます。レプリケーションはブロック変更に基づいているため、スペースと帯域幅を効率的に使用できます。クロスリージョンレプリケーション（CRR）機能を使用してAzureリージョン間でAzure NetApp Files ボリュームを効率的にレプリケートすることで、AzureでAzure NetApp Files 実行されているSAP HANAシステムとOracleシステムにも同じテクノロジが使用されます。

**SAP**システムのコピー処理やクローニング処理には、任意の**Snapshot**コピーを使用できます

ネットアップのテクノロジとソフトウェアの統合により、ソースシステムの任意のSnapshotコピーを使用してSAPシステムのコピーやクローニングを実行できます。このSnapshotコピーは、SAP本番用システムと同じストレージ、オフサイトのバックアップに使用するストレージ（AzureのAzure NetApp Files バックアップなど）、またはディザスタリカバリサイトのストレージ（Azure NetApp Files CRRターゲットボリューム）のいずれかから選択できます。この柔軟性により、必要に応じて開発用システムとテスト用システムを本番用システムと分離し、ディザスタリカバリサイトでのディザスタリカバリのテストなど、さまざまなシナリオに対応することができます。

統合による自動化

SAPテストシステムのプロビジョニングにはさまざまなシナリオとユースケースがあり、自動化のレベルに関してもさまざまな要件が存在する場合があります。ネットアップのSAP向けソフトウェア製品は、SAPなどのサードパーティベンダーが提供するデータベースやライフサイクル管理製品（Libelleなど）と統合されており、さまざまなシナリオや自動化のレベルをサポートします。

SAP HANAとSAP AnyDBまたはAzure上のAzAcSnap向けのプラグインを備えたNetApp SnapCenter を使用して、アプリケーションと整合性のあるSnapshotコピーに基づいて必要なストレージボリュームのクローンをプロビジョニングし、開始されたSAPデータベースまで、必要なホストとデータベースのすべての処理を実行できます。SAPシステムのコピー、システムクローン、システムの更新、SAPのポストプロセスなどの追加の手動手順が必要になる場合があります。詳細については、次のセクションで説明します。

完全に自動化されたエンドツーエンドのSAPテストシステムのプロビジョニングまたは更新は、Libelle SystemCopy（LSC）自動化を使用して実行できます。SnapCenter またはAzAcSnapのLSCへの統合については、このドキュメントで詳しく説明します。

**Libelle SystemCopy**

Libelle SystemCopyは、完全に自動化されたシステムコピーとランドスケープコピーを作成するフレームワークベースのソフトウェア解決策 です。ボタンを口頭で操作することで、QAおよびテストシステムを新しい本番データで更新できます。Libelle SystemCopyは、従来のすべてのデータベースとオペレーティングシステムをサポートし、すべてのプラットフォームに独自のコピーメカニズムを提供しますが、同時にバックアップ/リストア手順や、NetApp SnapshotコピーやNetApp FlexCloneボリュームなどのストレージツールを統合します。システムのコピー中に必要なアクティビティは、SAP ABAPスタックの外部から制御されます。そのため、SAPアプリケーションでは転送などの変更は必要ありません。一般に、システムコピー手順 を正常に完了するために必要な手順は、次の4つに分類できます。

- *確認フェーズ。*関係するシステム環境を確認してください。
- *プリフェーズ*システムコピーのターゲット・システムを準備します。
- *コピーフェーズ*ソースからターゲット・システムに実際の本番データベースのコピーを提供します
- ポスト・フェーズ：コピー後のすべてのタスクで同機種システムのコピー手順 を完了し'ターゲット・システムを更新します

コピーフェーズでは、NetApp SnapshotとFlexCloneの機能を使用して、最大のデータベースであっても、必要な時間を数分に短縮できます。

チェックフェーズ、プリフェーズ、およびポストフェーズの場合、LSCには、一般的な更新操作の95%をカバーする450以上の事前設定されたタスクが付属しています。その結果、LSCはSAP標準に従って自動化を推進します。LSCはソフトウェアで定義されるため、システム更新プロセスを簡単に調整および拡張して、お客様のSAP環境固有のニーズに対応できます。

### SAPシステムの更新とクローニングのユースケース

ソースシステムのデータをターゲットシステムで使用できるようにする必要があるシナリオは複数あります。

- 品質保証およびテストおよびトレーニングシステムの定期的な更新
- 論理的な破損に対処するために、システム環境の障害修復または修復を行う
- ディザスタリカバリのテストシナリオ

修復システムと災害復旧テストシステムは、通常、更新されたテストおよびトレーニングシステムのためにSAPシステムクローン（広範囲な後処理操作は不要）を使用して提供されますが、これらの後処理手順を適用してソースシステムと共存させる必要があります。そのため、本ドキュメントでは、SAPシステムの更新シナリオに焦点を当てて説明します。さまざまなユースケースの詳細については、テクニカルレポートを参照し"TR-4667：『Automating SAP HANA System Copy and Clone Operations with SnapCenter 』"てください。

このドキュメントの残りの部分は、2つの部分に分かれています。最初のパートでは、オンプレミスのNetApp ONTAP システムで実行されているSAP HANAシステムとSAP AnyDBシステム向けのNetApp SnapCenterとLibelle SystemCopyの統合について説明します。2番目のパートでは、Microsoft Azureで実行されているSAP HANAシステム用のLSCと、提供されているAzure NetApp Files とのAzAcSnapの統合について説明します。ONTAP テクノロジの基盤は同じですが、Azure NetApp Files は、ネイティブONTAP インストールとは異なるインターフェイスとツールの統合（AzAcSnapなど）を提供します。

## LSCおよびSnapCenter でSAP HANAシステムが更新されます

このセクションでは、LSCをNetApp SnapCenter に統合する方法について説明します。LSCとSnapCenter の統合では、SAPでサポートされるすべてのデータベースがサポートされます。ただし、SAP HANAはSAP AnyDBでは使用できない中央通信ホストを提供するため、SAP AnyDBとSAP HANAを区別する必要があります。

SAP AnyDB用のデフォルトのSnapCenter エージェントとデータベースプラグインのインストールは、データベースサーバ用の対応するデータベースプラグインに加えて、SnapCenter エージェントからのローカルインストールです。

このセクションでは、例として、LSCとSnapCenter の統合についてSAP HANAデータベースを使用して説明します。前述したSAP HANAの場合、SnapCenter エージェントとSAP HANAデータベースプラグインのインストール方法は2つあります。

- *標準のSnapCenter エージェントとSAP HANA Plug-inのインストール。*標準のインストールでは、SnapCenter エージェントとSAP HANAプラグインはSAP HANAデータベースサーバにローカルでインストールされます。
- *中央通信ホストを使用するSnapCenter のインストール。*中央通信ホストは、SnapCenter エージェント、SAP HANAプラグイン、および複数のSAP HANAシステムのSAP HANAデータベースのバックアップとリストアに必要なすべてのデータベース関連操作を処理するHANAデータベースクライアントとともにインストールされます。したがって、中央通信ホストに完全なSAP HANAデータベースシステムをインストールする必要はありません。

これらのさまざまなSnapCenterエージェントとSAP HANAデータベースプラグインのインストールオプションの詳細については、テクニカルレポートを参照して"TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"ください。

次の項では、標準インストールまたは中央通信ホストを使用したLSCとSnapCenter の統合の違いについて説

明します。特に、インストールオプションと使用するデータベースに関係なく、強調表示されない設定手順はすべて同じです。

では、ソースデータベースからSnapshotコピーベースの自動バックアップを実行し、新しいターゲットデータベースのクローンを作成するために、LSCとSnapCenterの統合について説明しています"TR-4667：『Automating SAP HANA System Copy and Clone Operations with SnapCenter 』"。では、に記載されている設定オプションとスクリプトを使用しています。

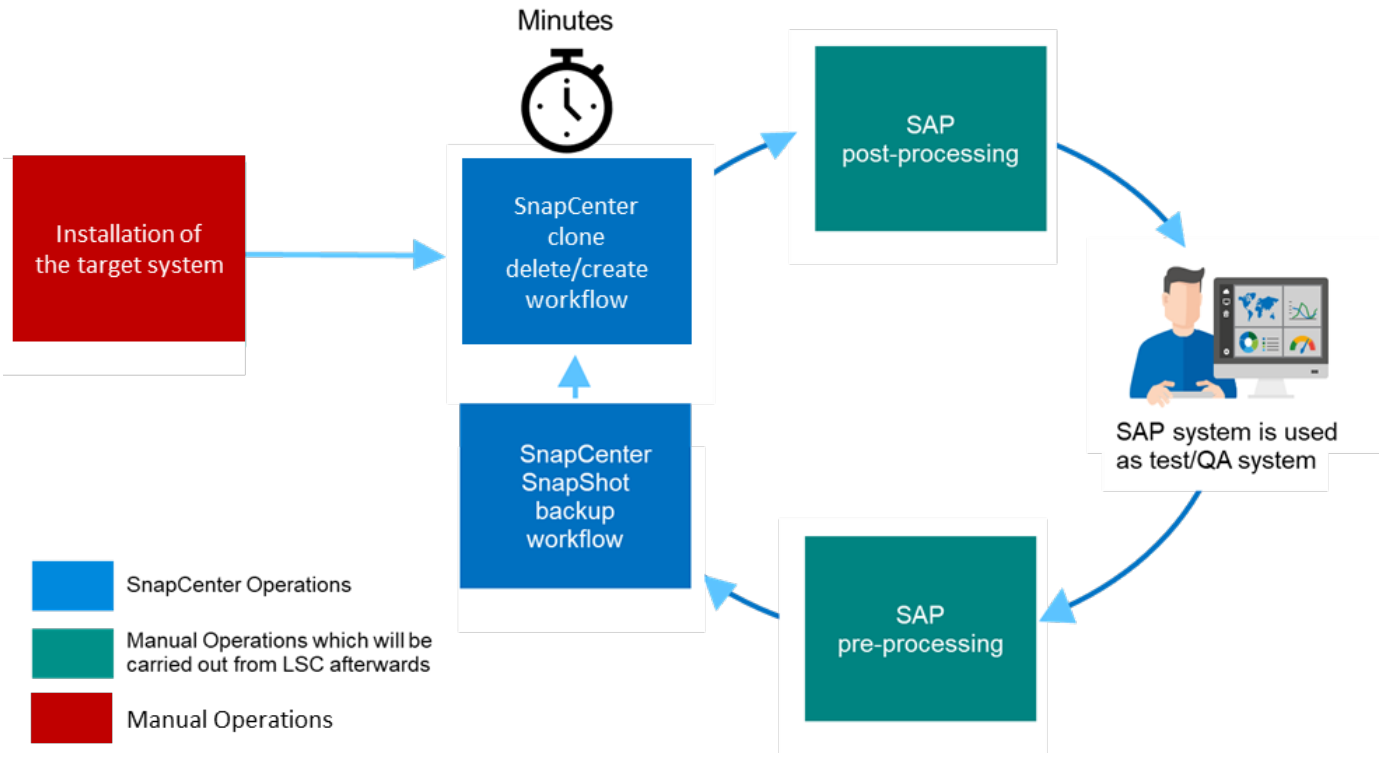
## 概要

次の図に、LSCを使用しないSnapCenter によるSAPシステムの更新ライフサイクルの一般的なワークフローを示します。

1. ターゲットシステムの初期インストールと準備を1回だけ行います。
2. 手動前処理（ライセンス、ユーザー、プリンターなどのエクスポート）。
3. 必要に応じて、ターゲットシステム上の既存のクローンを削除します。
4. ソースシステムの既存のSnapshotコピーを、SnapCenter によって実行されるターゲットシステムにクローニングすること。
5. SAP後処理の手動操作（ライセンスのインポート、ユーザー、プリンタ、バッチジョブの無効化など）。
6. その後、システムをテストシステムまたはQAシステムとして使用できます。
7. 新しいシステムの更新が要求されると、手順2でワークフローが再開されます。

SAPをご利用のお客様は、次の図に示す手動の手順が緑で表示されているため、時間がかかり、ミスが発生しやすくなっています。LSCとSnapCenter の統合を使用する場合、これらの手動手順は、信頼性の高い反復可能な方法でLSCを使用して実行されます。この方法では、内部および外部の監査に必要なすべてのログが使用されます。

次の図は、SnapCenterベースのSAPシステム更新手順 の概要を示しています。




前提条件および制限事項

次の前提条件を満たしている必要があります。

- SnapCenter をインストールする必要があります。ソースシステムとターゲットシステムは、標準インストールまたは中央通信ホストを使用して、SnapCenter で設定する必要があります。Snapshotコピーはソースシステム上に作成できます。
- 次の図に示すように、SnapCenter でストレージバックエンドが正しく設定されている必要があります。

Storage Connections

| Name | IP | Cluster Name | User Name | Controller License |
|---|---|---|---|---|
| svm-trident | | grenada.muccbc.hq.netapp.com | | ✔ |
| svm-sap02 | 10.65.58.253 | grenada.muccbc.hq.netapp.com | | ✔ |
| svm-sap01 | 10.65.58.252 | grenada.muccbc.hq.netapp.com | | ✔ |

次の2つの図は、SnapCenter エージェントとSAP HANAプラグインが各データベースサーバでローカルにインストールされる標準インストールを示しています。

SnapCenter エージェントと適切なデータベースプラグインをソースデータベースにインストールする必要があります。

| Name | Type | System | Plug-in | Version | Overall Status |
|---|---|---|---|---|---|
| sap-lnx35.muccbc.hq.netapp.com | Linux | Stand-alone | UNIX, SAP HANA | 4.3.1 | Running |

SnapCenter エージェントと適切なデータベースプラグインをターゲット・データベースにインストールする必要があります。

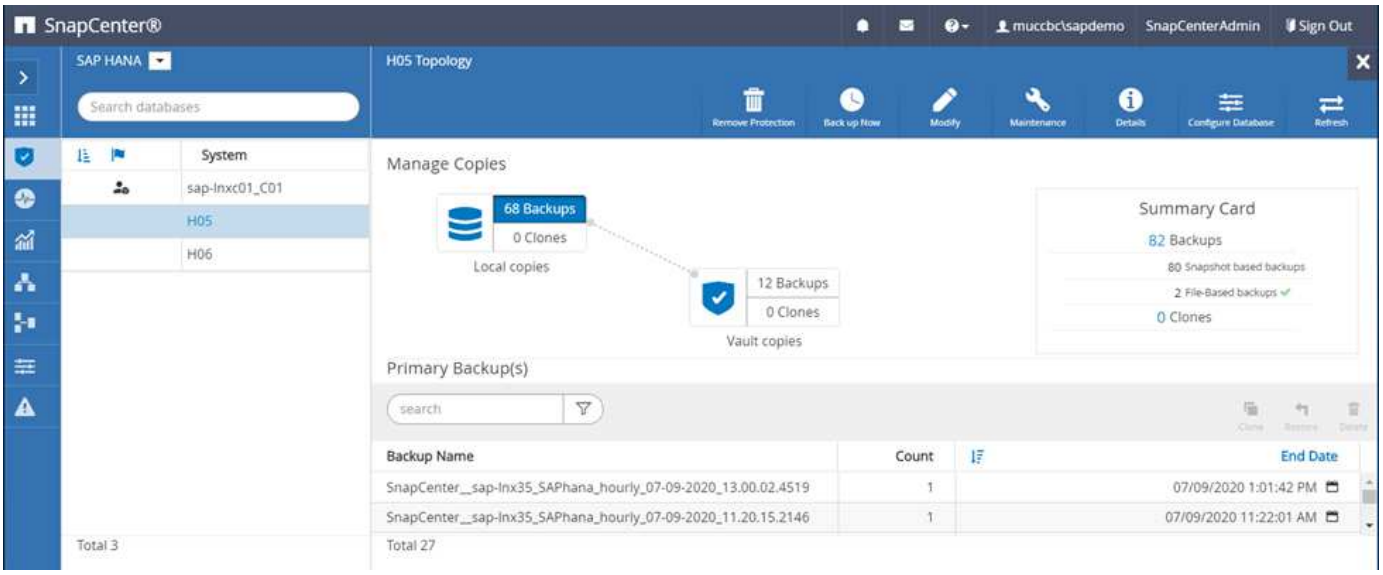
| | | | | | |
|---|---|---|---|---|---|
| sap-lnx36.muccbc.hq.netapp.com | Linux | Stand-alone | UNIX, SAP HANA | 4.3.1 | Running |

次の図は、SnapCenter エージェント、SAP HANAプラグイン、およびSAP HANAデータベースクライアントが一元化されたサーバ（SnapCenter サーバなど）にインストールされ、ランドスケープ内の複数のSAP HANAシステムを管理する、中央通信ホスト環境を示しています。

SnapCenter エージェント、SAP HANAデータベースプラグイン、およびHANAデータベースクライアントが、中央の通信ホストにインストールされている必要があります。




Snapshotコピーを正常に作成できるように、SnapCenter でソースデータベースのバックアップが適切に設定されている必要があります。




LSCマスターおよびLSCワーカーがSAP環境にインストールされている必要があります。この展開では、SnapCenter サーバにLSCマスターをインストールし、ターゲットのSAPデータベースサーバにLSCワーカーをインストールします。このサーバは更新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[ラボのセットアップ]」

ドキュメント：

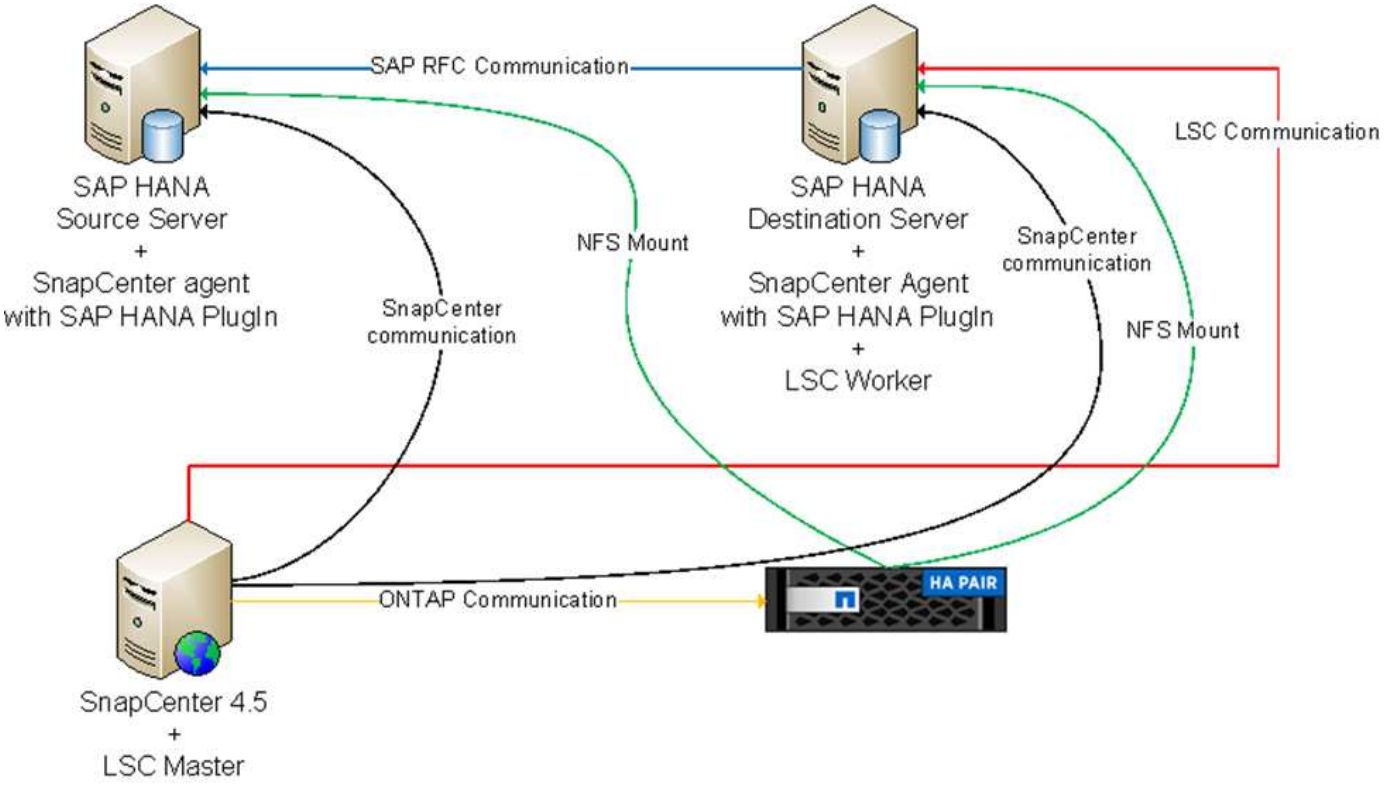
- "SnapCenter ドキュメントセンター"
- "TR-4700 ：『 SnapCenter Plug-in for Oracle Database 』"
- "TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』"
- "TR-4667：『Automating SAP HANA System Copy and Clone Operations with SnapCenter 』"
- "TR-4769：『SnapCenter Best Practices and Sizing Guidelines』"
- "SnapCenter 4.6コマンドレットリファレンスガイド"

## ラボのセットアップ

このセクションでは、デモデータセンターでセットアップされたアーキテクチャの例について説明します。セットアップは、標準的なインストールと、中央の通信ホストを使用したインストールに分かれています。

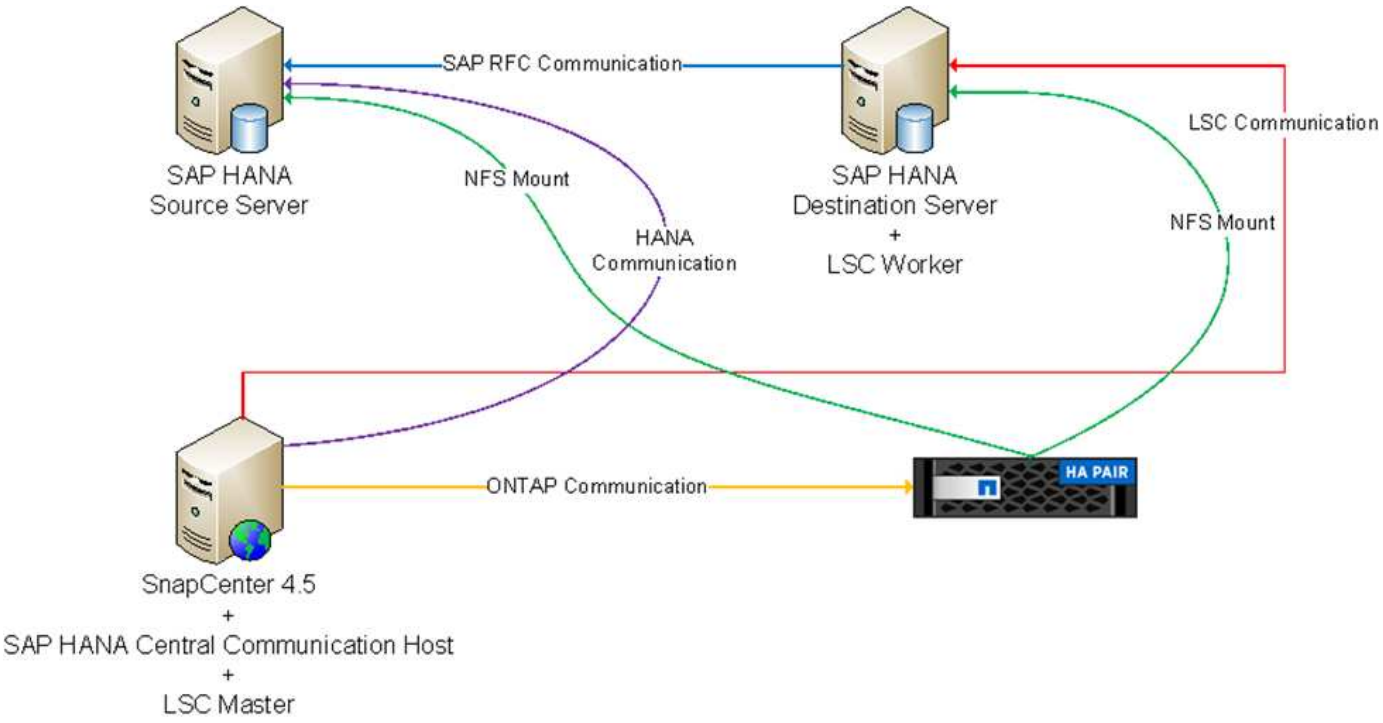
### 標準インストール

次の図に、SnapCenter エージェントとデータベースプラグインが、ソースおよびターゲットのデータベースサーバ上にローカルにインストールされた標準インストールを示します。このラボ環境では、SAP HANA Plug-inをインストールしました。また、ターゲットサーバにLSCワーカーもインストールされています。簡素化と仮想サーバ数の削減のために、SnapCenter サーバにLSCマスターをインストールしました。次の図は、各種コンポーネント間の通信を示しています。




### セントラルコミュニケーションホスト

次の図に、中央通信ホストを使用した設定を示します。この構成では、SnapCenter エージェントとSAP HANA Plug-inおよびHANAデータベースクライアントを専用サーバにインストールしました。このセットアップでは、SnapCenter サーバを使用して中央通信ホストをインストールしました。さらに、LSCワーカーが再びターゲットサーバにインストールされました。簡素化と仮想サーバ数の削減のため、SnapCenter サーバにLSCマスターもインストールすることにしました。次の図に、異なるコンポーネント間の通信を示します。




**Libelle SystemCopy**の初期**1**回限りの準備手順

LSCインストールには、次の3つの主要コンポーネントがあります。

- *LSC master.*という名前が示すように、Libelleベースのシステムコピーの自動ワークフローを制御するマスターコンポーネントです。デモ環境では、LSCマスターがSnapCenter サーバにインストールされています。
- * LSCワーカー。* LSCワーカーは、通常はターゲットSAPシステムで実行されるLibelleソフトウェアの一部であり、自動システムコピーに必要なスクリプトを実行します。デモ環境では、ターゲットのSAP HANAアプリケーションサーバにLSCワーカーがインストールされています。
- * LSC衛星。* LSC衛星は、それ以降のスクリプトを実行する必要があるサードパーティシステム上で実行されるLibelleソフトウェアの一部です。LSCマスターは、LSCサテライトシステムの役割も同時に果たすことができます。

次の図に示すように、最初にLSC内のすべての関連システムを定義しました。

- * 172.30.15.35.* SAPソースシステムとSAP HANAソースシステムのIPアドレス。
- *172.30.15.3.*この構成のLSCマスターおよびLSCサテライトシステムのIPアドレス。SnapCenter サーバにLSCマスターをインストールしたため、SnapCenter サーバのインストール時にインストールされたSnapCenter 4.x PowerShellコマンドレットは、このWindowsホストですでに使用できます。そのため、このシステムに対してLSCサテライトロールを有効にし、このホストですべてのSnapCenter PowerShellコマンドレットを実行することにしました。別のシステムを使用する場合は、SnapCenter のマニュアルに従って、このホストにSnapCenter PowerShellコマンドレットをインストールしてください。
- **172.30.15.36** SAPデスティネーションシステム、SAP HANAデスティネーションシステム、およびLSCワーカーのIPアドレス。

IPアドレス、ホスト名、完全修飾ドメイン名の代わりに使用することもできます。

次の図は、マスタ、ワーカー、サテライト、SAPソース、SAPターゲットのLSC構成を示しています。 ソースデータベースおよびターゲットデータベース。

| System Identifier | Worker | Source SAP | Source Database | Target SAP | Target Database | Satellite System |
|---|---|---|---|---|---|---|
| 172.30.15.35 | | ☑ | ☑ | ☐ | ☐ | ☐ |
| 172.30.15.3 | 172.30.15.3:9000 | ☐ | ☐ | ☐ | ☐ | ☑ |
| 172.30.15.36 | 172.30.15.36:9000 | ☐ | ☐ | ☑ | ☑ | ☐ |

メイン統合のためには、設定手順を標準インストールと中央通信ホストを使用したインストールに再度分ける必要があります。

標準インストール

このセクションでは、SnapCenter エージェントと必要なデータベースプラグインがソースシステムとターゲットシステムにインストールされている標準インストールを使用する場合に必要な設定手順について説明します。標準インストールを使用する場合は、クローンボリュームのマウントおよびターゲットシステムのリストアとリカバリに必要なすべてのタスクが、サーバ自体のターゲットデータベースシステムで実行されているSnapCenter エージェントから実行されます。これにより、SnapCenter エージェントの環境変数を使用して、クローン関連の詳細情報にアクセスできるようになります。したがって、LSCコピーフェーズでは、追加のタスクを1つだけ作成する必要があります。このタスクでは、ソース・データベース・システムでSnapshotコピーの処理を実行し、ターゲット・データベース・システムでクローンおよびリストアおよびリカバリの処理を実行します。SnapCenter に関連するすべてのタスクは、LSCタスク「NTAP_SYSTEM_CLONE」に入力されたPowerShellスクリプトを使用してトリガーされます。

次の図は、コピーフェーズのLSCタスクの設定を示しています。

| | copy | Copy Phase | | phase |
|---|---|---|---|---|
| | copy 1 | NTAP_SYSTEM_CLONE | NetApp SnapShot and Clone | psh |
| | *copy 2* | *NTAP_SYSTEM_CLONE_CP* | *NetApp SnapShot and Clone* | *psh* |
| | *copy 3* | *NTAP_MNT_RECOVER_CP* | *Mount Volume and Recover HANA Database* | *cmd* |
| | *copy 4* | *LPDBBCKP* | *Backup Source DB in Filesystem* | *lsh* |
| | *copy 5* | *LPDBCPYFLS* | *Copy DB Backup Files From Source to Target System* | *lsh* |
| | *copy 6* | *LTDBRESTORE* | *Restore DB Files* | *lsh* |
| | *copy 7* | *LTDBRESTORE_TENANT* | *Restore DB Files for Tenant Database* | *lsh* |
| | **post** | **Post Phase** | | **phase** |

次の図は'NTAP_SYSTEM_CLONEプロセスの構成を示していますPowerShellスクリプトを実行するため、このWindows PowerShellスクリプトはサテライトシステム上で実行されます。この場合、これは、サテライトシステムとしても機能する、インストールされたLSCマスターを持つSnapCenter サーバです。

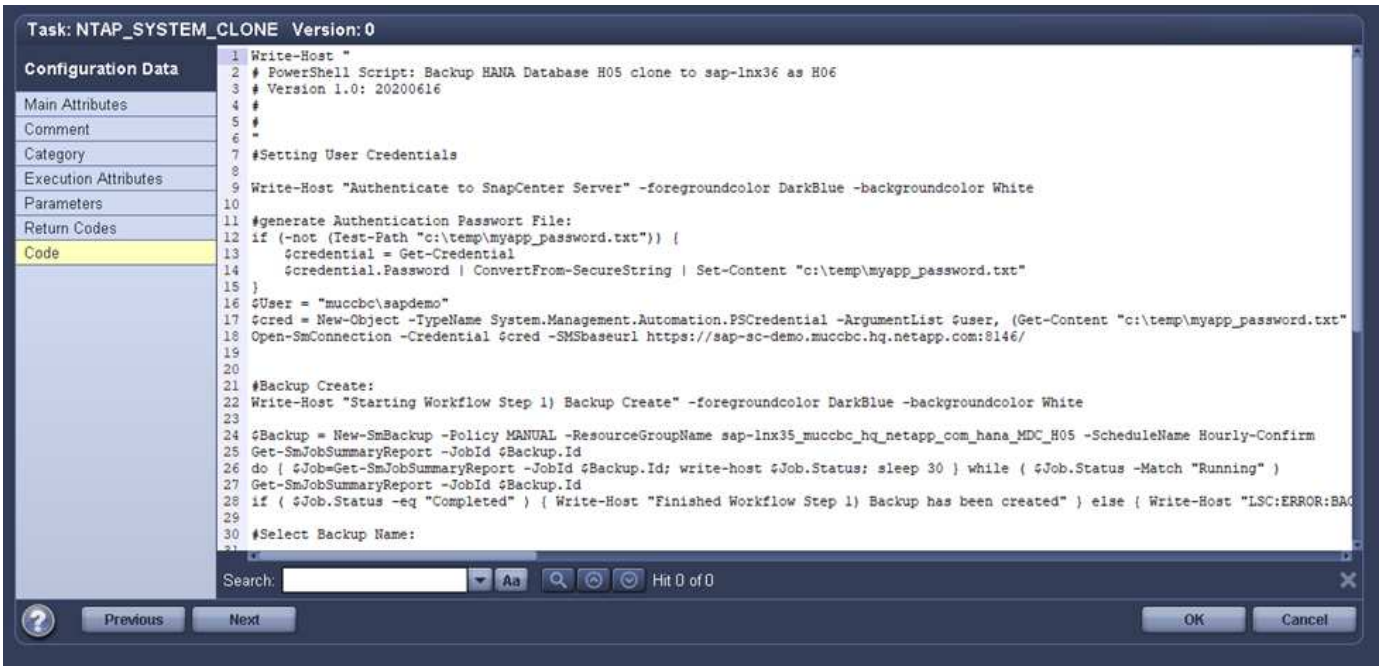



LSCは、Snapshotコピー、クローニング、およびリカバリ処理が成功したかどうかを認識する必要があるため、少なくとも2つの戻りコードタイプを定義する必要があります。次の図に示すように、1つのコードはスクリプトを正常に実行するためのもので、もう1つのコードはスクリプトの実行に失敗するためのものです。

- 実行が成功した場合は、スクリプトから標準出力に「LSC：OK」を書き込む必要があります。
- 実行に失敗した場合は、スクリプトから標準出力に「LSC：error」を書き込む必要があります。




次の図は、ソースデータベースシステムでSnapshotベースのバックアップを実行し、ターゲットデータベースシステムでクローンを実行する、PowerShellスクリプトの一部です。このスクリプトは、完全なものではありません。このスクリプトでは、LSCとSnapCenter の統合がどのように表示されるか、および設定がどの程度簡単かを示します。




スクリプトはLSCマスター（サテライトシステムでもある）上で実行されるため、SnapCenter サーバ上のLSCマスターは、SnapCenter でバックアップおよびクローニング操作を実行するための適切な権限を持つWindowsユーザとして実行する必要があります。ユーザに適切な権限があるかどうかを確認するには、SnapCenter UIでSnapshotコピーとクローンを実行できる必要があります。

SnapCenter サーバ自体でLSCマスターおよびLSCサテライトを実行する必要はありません。LSCマスターおよびLSCサテライトは、任意のWindowsマシンで実行できます。LSCサテライトでPowerShellスクリプトを実行するための前提条件は、SnapCenter PowerShellコマンドレットがWindowsサーバにインストールされていることです。

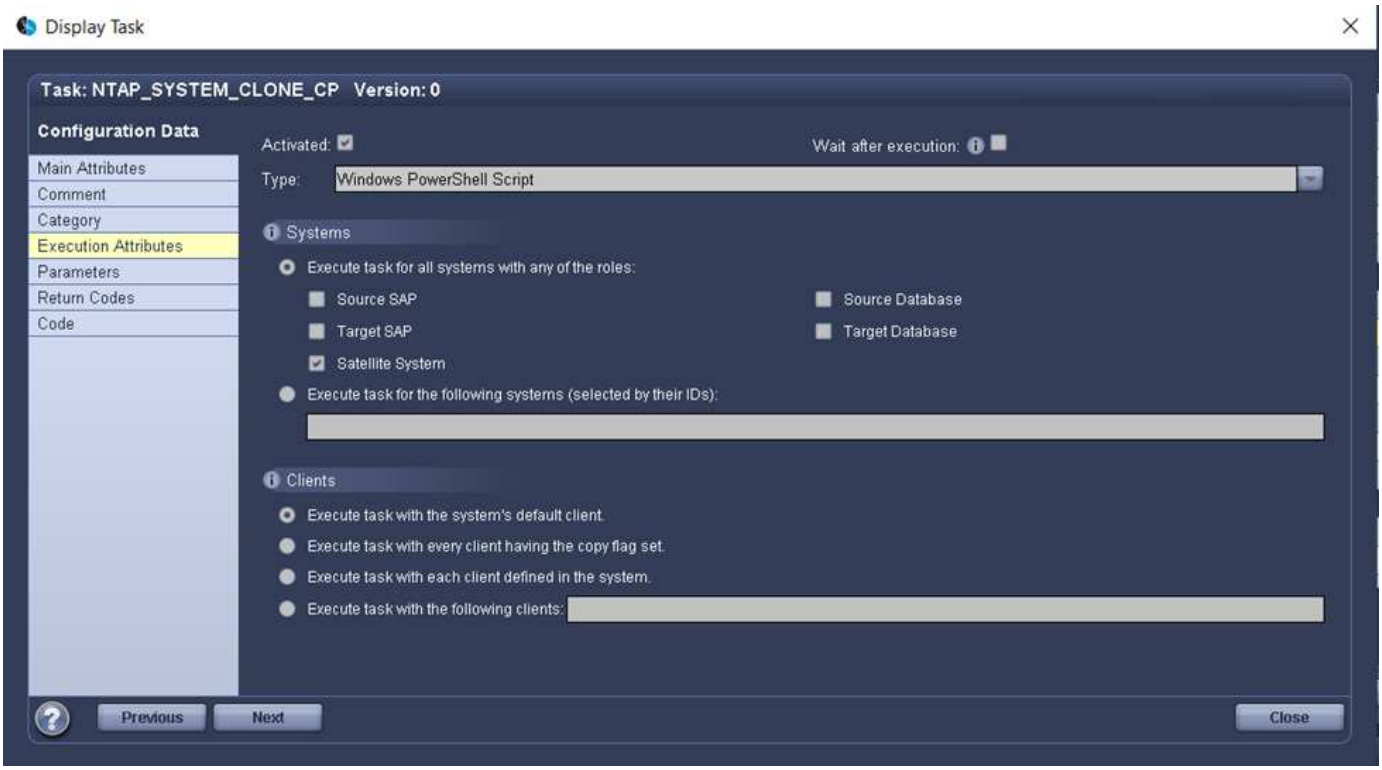
セントラルコミュニケーションホスト

中央通信ホストを使用してLSCとSnapCenter の間で統合する場合、コピーフェーズで実行する必要がある調整のみが実行されます。Snapshotコピーとクローンは、中央通信ホスト上のSnapCenter エージェントを使用して作成されます。したがって、新しく作成されたボリュームに関するすべての詳細情報は、ターゲットデータベースサーバではなく、中央通信ホストでのみ使用できます。ただし、これらの詳細は、クローンボリュームをマウントしてリカバリを実行するために、ターゲットデータベースサーバ上に必要です。これは、コピーフェーズで追加のタスクが2つ必要になる理由です。1つのタスクが中央通信ホストで実行され、1つのタスクがターゲットデータベースサーバで実行されます。これら2つのタスクを次の図に示します。

- * NTAP _ SYSTEM_CLONE_CP。このタスクでは、中央通信ホストで必要なSnapCenter 機能を実行するPowerShellスクリプトを使用して、Snapshotコピーおよびクローンを作成します。したがって、このタスクはLSCサテライト上で実行されます。この場合、このインスタンスはWindows上で実行されるLSCマスターです。このスクリプトは、クローンおよび新しく作成されたボリュームに関するすべての詳細を収集し、2番目のタスク「NTAP_Mnt_RECOVER_CP」に渡します。このタスクは、ターゲットデータベースサーバで実行されるLSCワーカーで実行されます。
- * NTAP_Mnt_RECOVER_CP。*このタスクは、ターゲットSAPシステムとSAP HANAデータベースを停止し、古いボリュームをアンマウントして、前のタスク「NTAP_SYSTEM_CLONE_CP」から渡されたパラメータに基づいて、新しく作成されたストレージクローンボリュームをマウントします。その後、ターゲットのSAP HANAデータベースがリストアおよびリカバリされます。

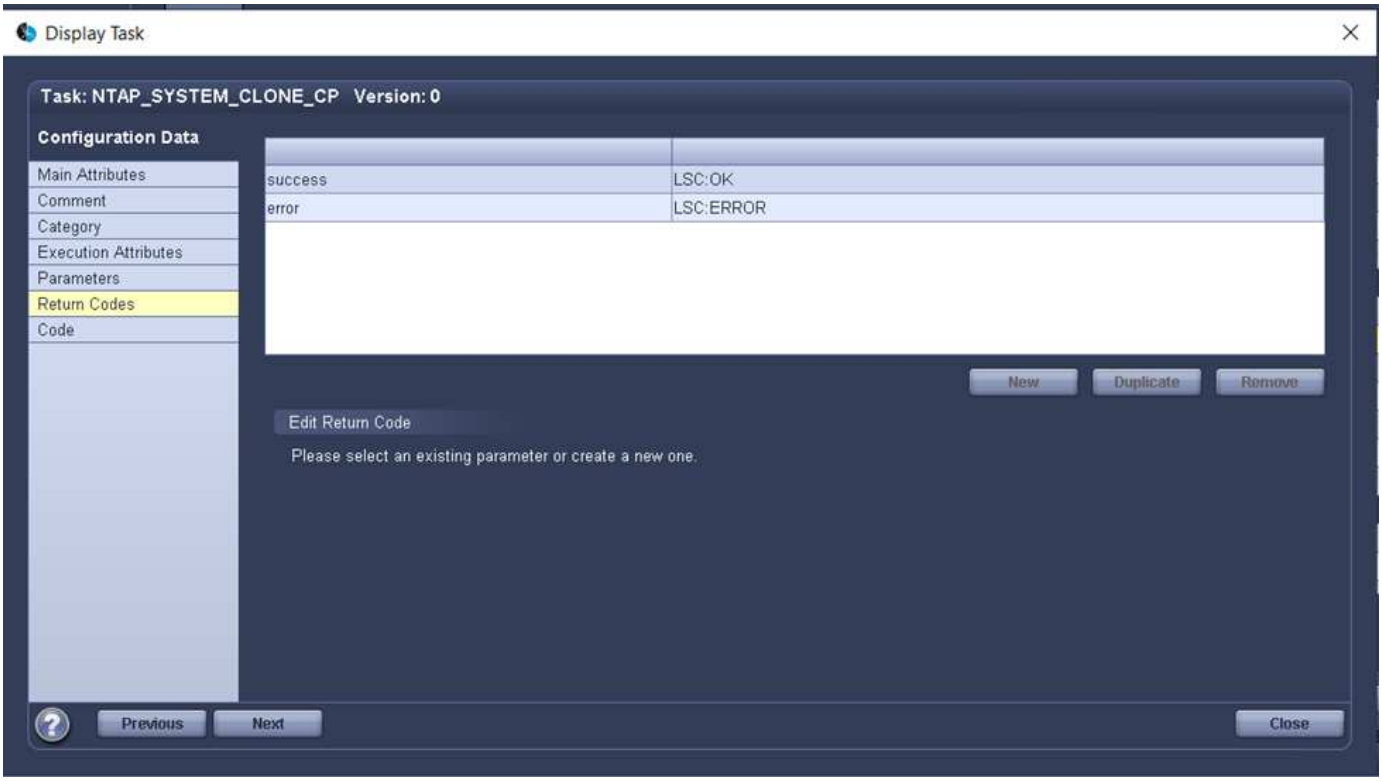
| | copy | Copy Phase | | phase |
|---|---|---|---|---|
| | copy 1 | NTAP_SYSTEM_CLONE | NetApp SnapShot and Clone | psh |
| | copy 2 | NTAP_SYSTEM_CLONE_CP | NetApp SnapShot and Clone | psh |
| | copy 3 | NTAP_MNT_RECOVER_CP | Mount Volume and Recover HANA Database | cmd |
| | copy 4 | LPDBBCKP | Backup Source DB in Filesystem | lsh |
| | copy 5 | LPDBCPYFLS | Copy DB Backup Files From Source to Target System | lsh |
| | copy 6 | LTDBRESTORE | Restore DB Files | lsh |
| | copy 7 | LTDBRESTORE_TENANT | Restore DB Files for Tenant Database | lsh |
| | post | Post Phase | | phase |

次の図は'タスク'NTAP_SYSTEM_CLONE_CP'の構成を示していますこれは、サテライトシステムで実行されるWindows PowerShellスクリプトです。この場合、サテライトシステムは、インストールされたLSCマスターを持つSnapCenter サーバになります。

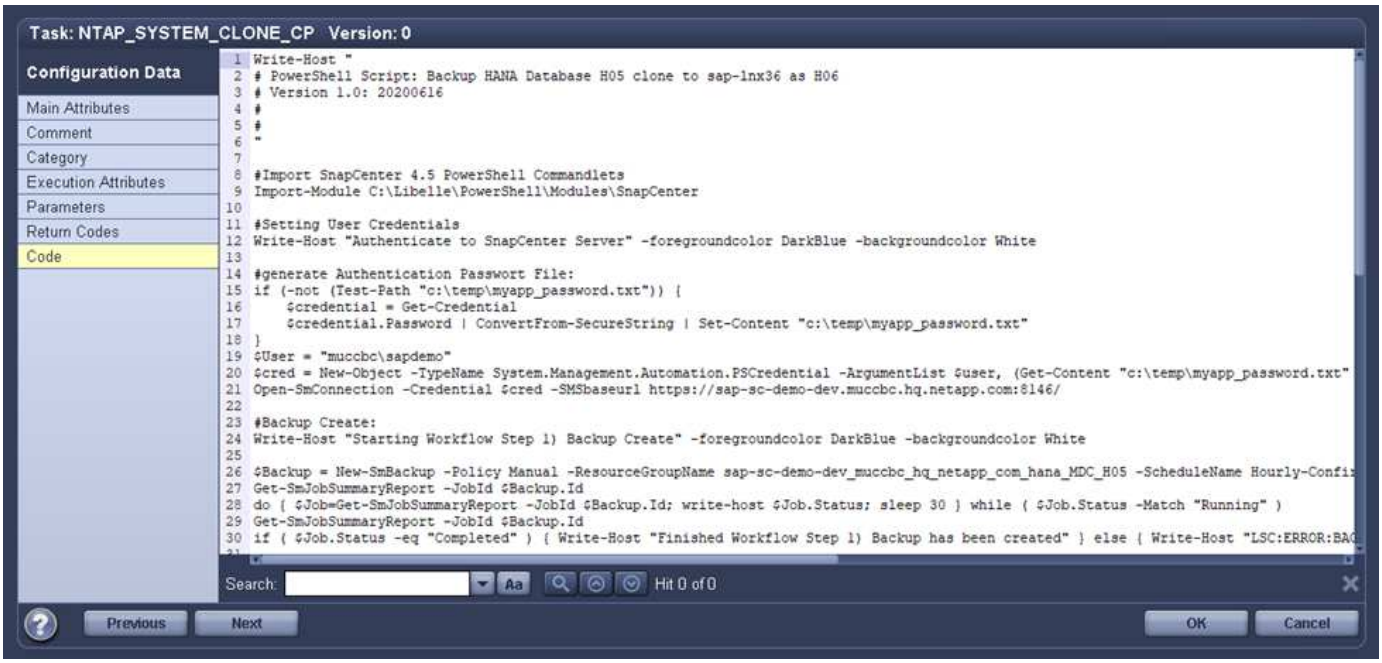



LSCは、Snapshotコピーおよびクローニング処理が成功したかどうかを認識する必要があるため、次の図に示すように、少なくとも2つの戻りコードタイプを定義する必要があります。スクリプトを正常に実行するには1つの戻りコードタイプ、スクリプトの実行に失敗するにはもう1つの戻りコードタイプです。

- 実行が成功した場合は、スクリプトから標準出力に「LSC：OK」を書き込む必要があります。
- 実行に失敗した場合は、スクリプトから標準出力に「LSC：error」を書き込む必要があります。




次の図は、中央通信ホスト上のSnapCenter エージェントを使用してSnapshotコピーとクローンを実行するために実行する必要があるPowerShellスクリプトの一部を示しています。このスクリプトは完了することを意図したものではありません。代わりに、スクリプトを使用して、LSCとSnapCenter の統合がどのように見えるか、および設定がどの程度簡単かを示します。

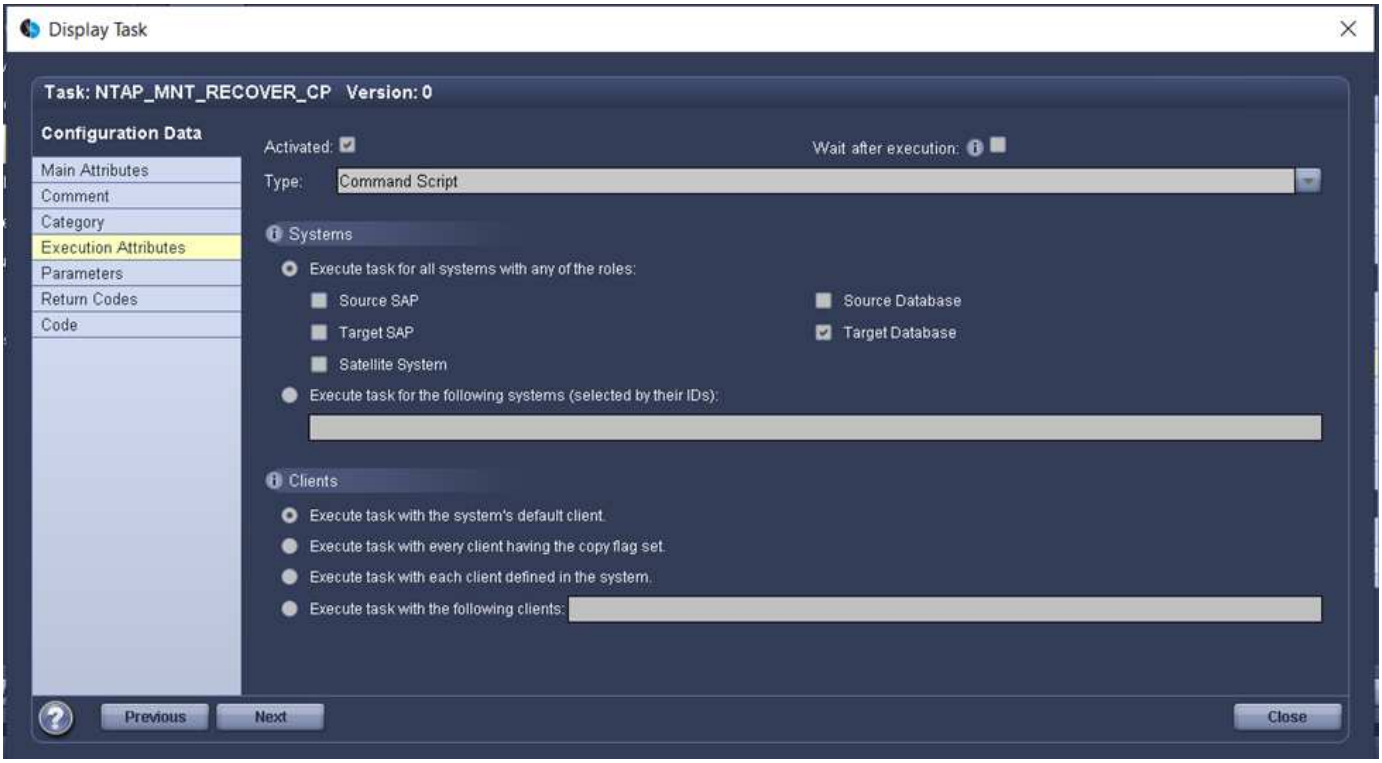



前述したように、クローンボリュームの名前を次のタスク「NTAP_Mnt_RECOVER_CP」に渡して、ターゲットサーバでクローンボリュームをマウントする必要があります。クローン・ボリュームの名前（ジャンクション・パスとも呼ばれます）は変数「$JunctionalPath」に格納されます。後続のLSCタスクへの引き渡しは、カスタムのLSC変数によって行われます。

```
echo $JunctionPath > $_task(current, custompath1)_$
```

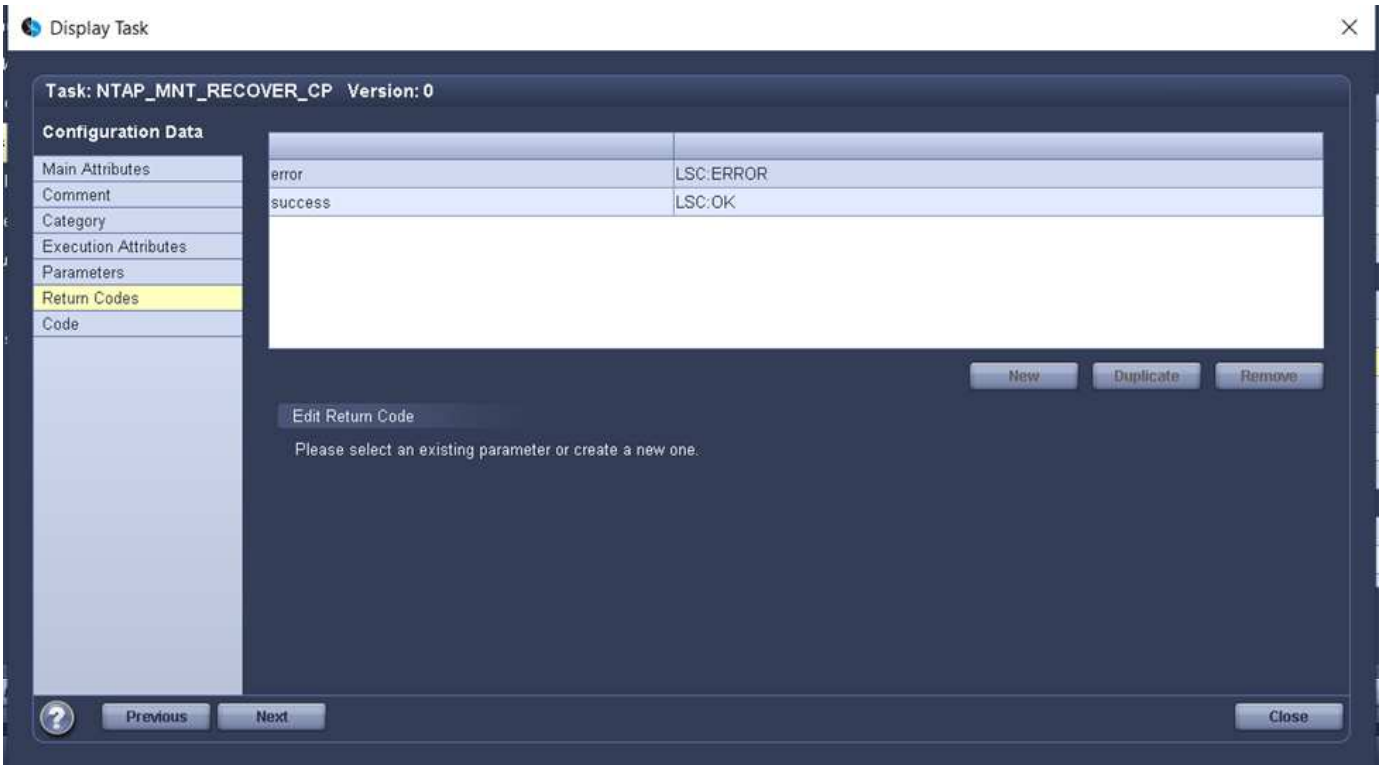
スクリプトはLSCマスター（サテライトシステムでもある）上で実行されるため、SnapCenter サーバ上のLSCマスターは、SnapCenter でバックアップおよびクローニング操作を実行するための適切な権限を持つWindowsユーザとして実行する必要があります。適切な権限があるかどうかを確認するには、ユーザがSnapCenter GUIでSnapshotコピーとクローンを実行できる必要があります。

次の図は'NTAP_Mnt_RECOVER_CP'タスクの構成を示していますLinuxシェルスクリプトを実行するため、これはターゲットデータベースシステムで実行されるコマンドスクリプトです。




LSCは、クローンボリュームのマウントを認識し、ターゲットデータベースのリストアとリカバリが成功したかどうかを確認する必要があるため、少なくとも2つの戻りコードタイプを定義する必要があります。1つはスクリプトを正常に実行するためのコードで、1つはスクリプトの実行に失敗したコードです。次の図に示します。

- 実行が成功した場合は、スクリプトから標準出力に「LSC：OK」を書き込む必要があります。
- 実行に失敗した場合は、スクリプトから標準出力に「LSC：error」を書き込む必要があります。

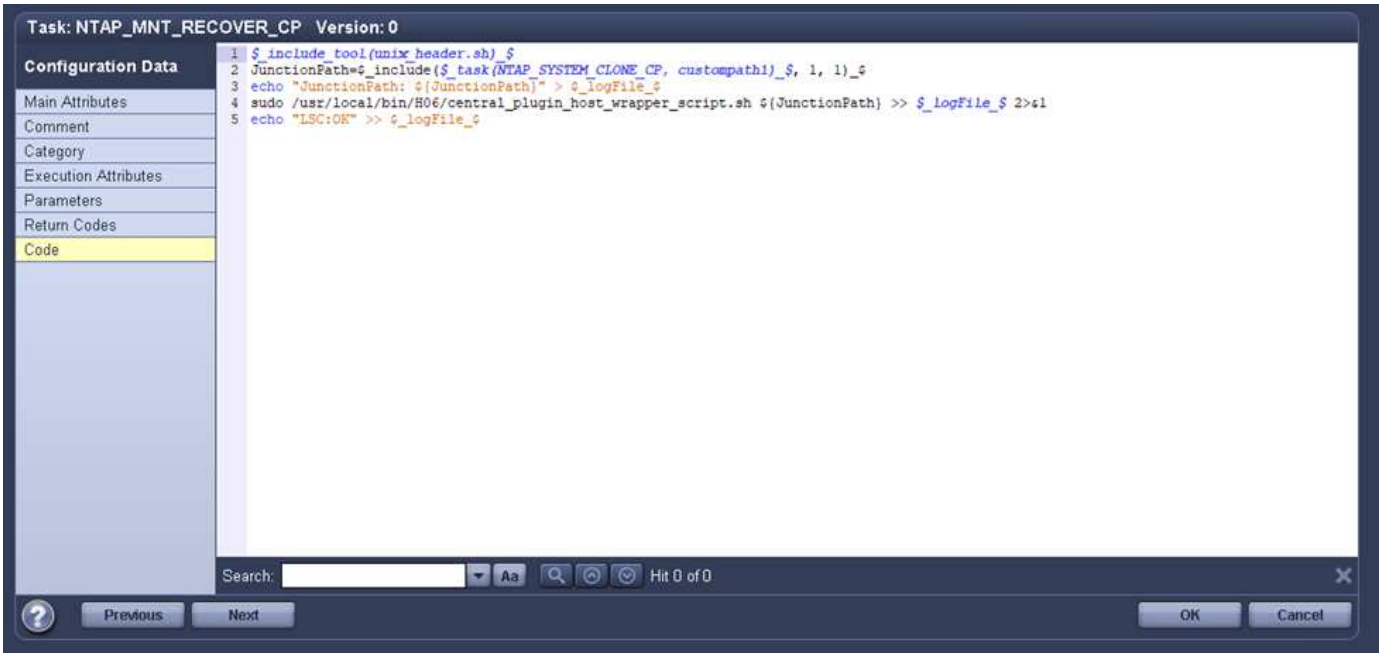



次の図に、Linux Shellスクリプトの一部を示します。このスクリプトでは、ターゲットデータベースの停止、古いボリュームのアンマウント、クローンボリュームのマウント、ターゲットデータベースのリストアとリカバリを行います。前のタスクでは、ジャンクションパスがLSC変数に書き込まれました。次のコマンドはこのLSC変数を読み取り、値をLinuxシェルスクリプトの「$JunctionalPath」変数に格納します。

```
JunctionPath=$_include($_task(NTAP_SYSTEM_CLONE_CP, custompath1)_$, 1,
1)_$
```

ターゲットシステム上のLSCワーカーは「<sidaadm>`」として実行されますが、マウントコマンドはrootユーザとして実行する必要があります。したがって'central_plugin_host_wrapper_script.shを作成する必要がありますスクリプト「central_plugin_host_wrapper_script.sh」は、「sudo」コマンドを使用して「NTAP_Mnt_recovery_CP」タスクから呼び出されます。スクリプトは'sudoコマンドを使用してUID 0で実行され'古いボリュームのアンマウント'クローンボリュームのマウント'ターゲット・データベースのリストアとリカバリなど'以降のすべての手順を実行できますsudoを使用してスクリプト実行を有効にするには'/etc/sudoers'に次の行を追加する必要があります

```
hn6adm ALL=(root)
NOPASSWD:/usr/local/bin/H06/central_plugin_host_wrapper_script.sh
```




**SAP HANA**システムの更新処理

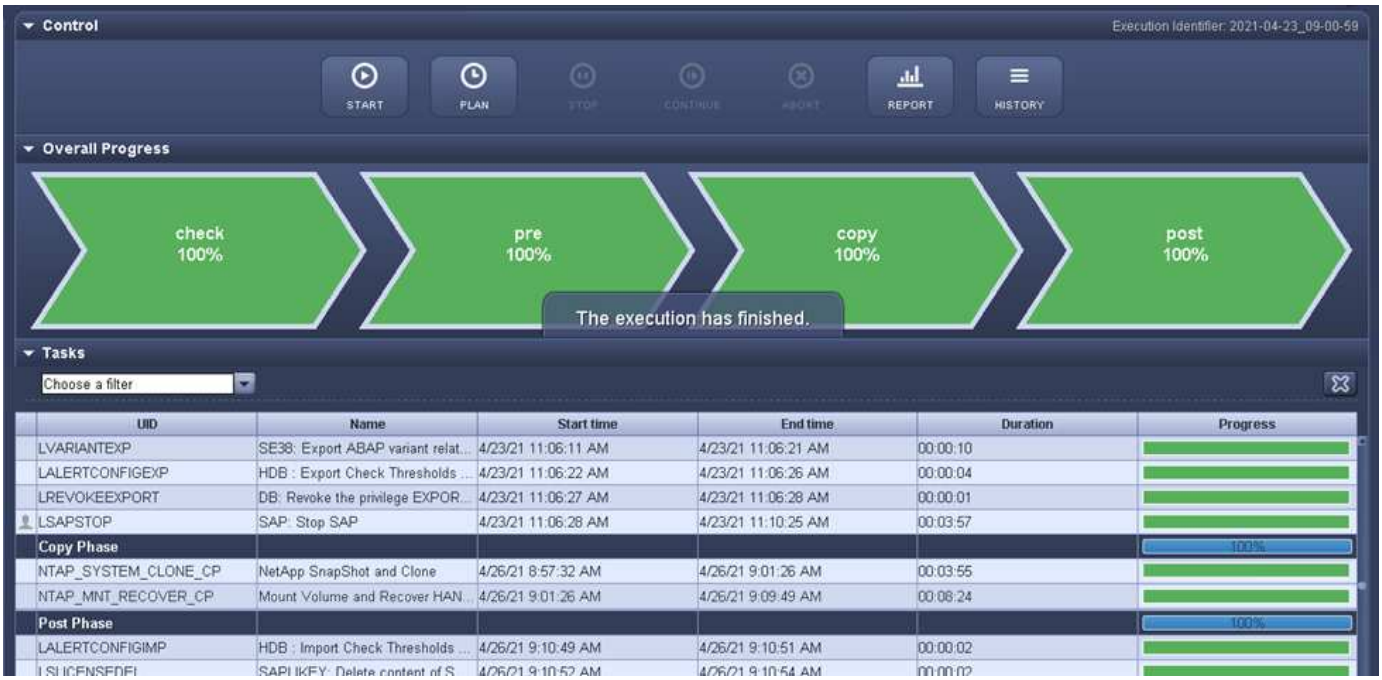
LSCとNetApp SnapCenter の間の必要な統合タスクがすべて実行されたので、完全に自動化されたSAPシステム更新を開始するのはワンクリックタスクです。

次の図は'標準インストールにおけるNTAP `_`SYSTEM`_CLONE」タスクを示していますこの出力からわかるように、Snapshotコピーとクローンを作成し、クローンボリュームをターゲットデータベースサーバにマウントし、ターゲットデータベースのリストアとリカバリには約14分かかりました。SnapshotとNetApp FlexCloneテクノロジを使用すれば、ソースデータベースのサイズに関係なく、このタスクの所要時間はほぼ同じです。




次の図に、セントラル通信ホストを使用する場合の「NTAP_SYSTEM_CLONE_CP」と「NTAP_Mnt_RECOVERY_CP」の2つのタスクを示します。この出力からわかるように、Snapshotコピー、クローン、ターゲットデータベースサーバへのクローンボリュームのマウント、ターゲットデータベース

のリストアとリカバリには約12分かかりました。これは、標準インストールを使用する場合に、これらの手順を実行するのに必要な時間と同じか、それより短くなります。繰り返しになりますが、SnapshotとNetApp FlexCloneテクノロジを使用すれば、ソースデータベースのサイズに関係なく、これらのタスクを短時間で一貫して実行できます。




## LSC、AzAcSnap、およびAzure NetApp Files を使用してSAP HANAシステムが更新されます

を使用します "Azure NetApp Files for SAP HANAの略"、Oracle、DB2 on Azureを利用すると、NetApp ONTAP の高度なデータ管理機能とデータ保護機能をMicrosoft Azure NetApp Files 標準サービスで利用できます。 "AzAcSnap" は、SAPシステムの更新処理を高速化して、SAP HANAシステムとOracleシステムのNetApp Snapshotコピーをアプリケーションと整合性のあるものにするための基盤です（DB2は現在AzAcSnapではサポートされていません）。

Snapshotコピーのバックアップは、オンデマンドで作成することも、バックアップ戦略の一環として定期的に作成することもでき、効率的に新しいボリュームにクローニングして、ターゲットシステムを迅速に更新することができます。AzAcSnapは、バックアップを作成して新しいボリュームにクローンを作成するために必要なワークフローを提供します。一方、Libelle SystemCopyは、完全なエンドツーエンドのシステム更新に必要な、前処理と後処理の手順を実行します。

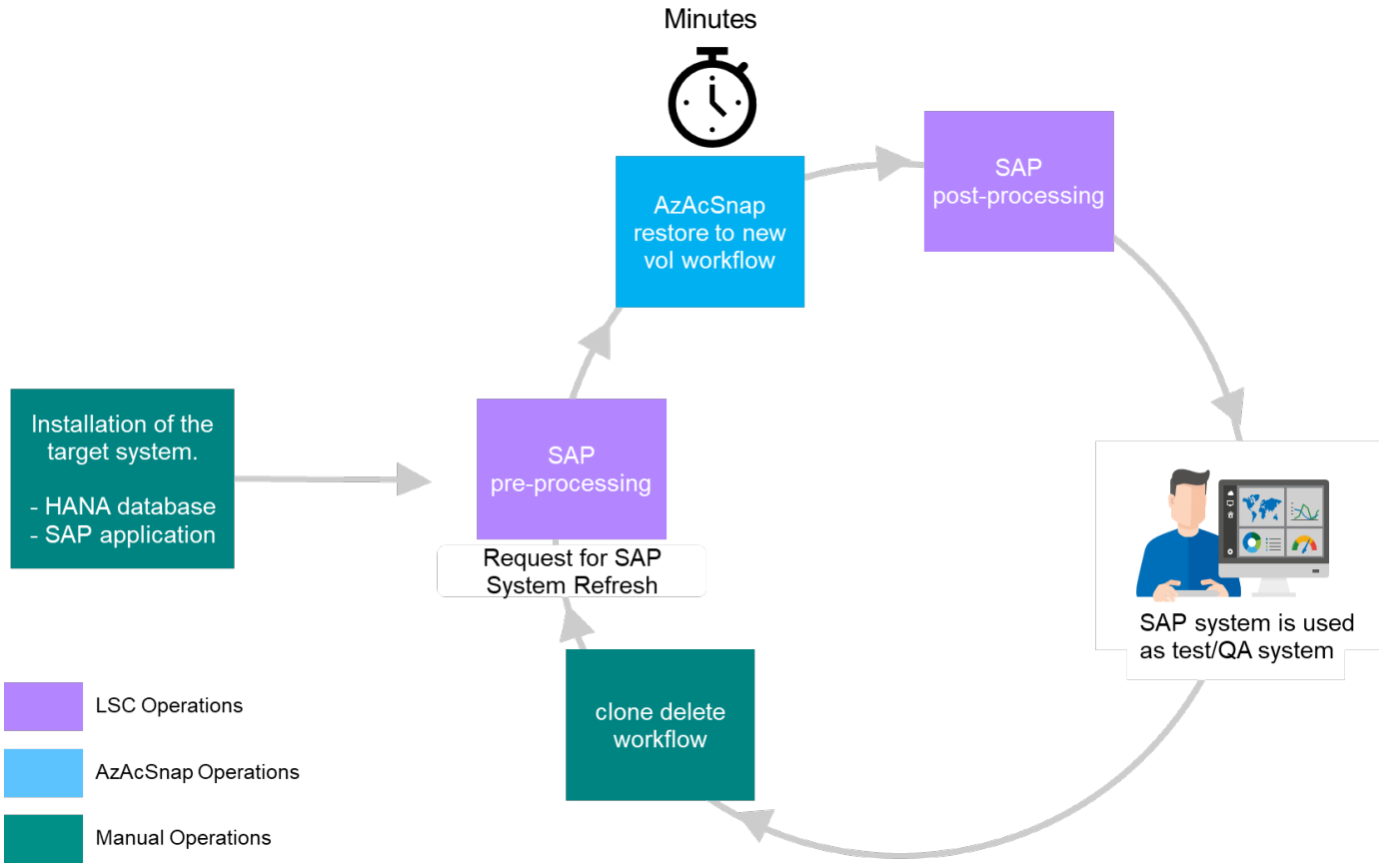
この章では、SAP HANAを基盤データベースとして使用したAzAcSnapおよびLibelle SystemCopyを使用したSAPシステムの自動更新について説明します。AzAcSnapはOracleでも利用できるため、AzAcSnap for Oracleを使用して同じ手順 を実装することもできます。その他のデータベースは、今後AzAcSnapによってサポートされる可能性があります。この場合、LSCおよびAzAcSnapを使用してこれらのデータベースのシステムコピー操作が有効になります。

次の図は、AzAcSnapおよびLSCを使用したSAPシステム更新ライフサイクルの一般的なワークフローを示しています。

- ターゲットシステムの初期インストールと準備を1回だけ行います。

- LSCによって実行されるSAP前処理操作。
- AzAcSnapで実行されるターゲットシステムへのソースシステムの既存のSnapshotコピーのリストア（またはクローニング）。
- LSCによって実行されるSAP後処理操作。

システムはテストシステムまたはQAシステムとして使用できます。新しいシステムの更新が要求されると、手順2でワークフローが再開されます。残りのクローンボリュームは手動で削除する必要があります。

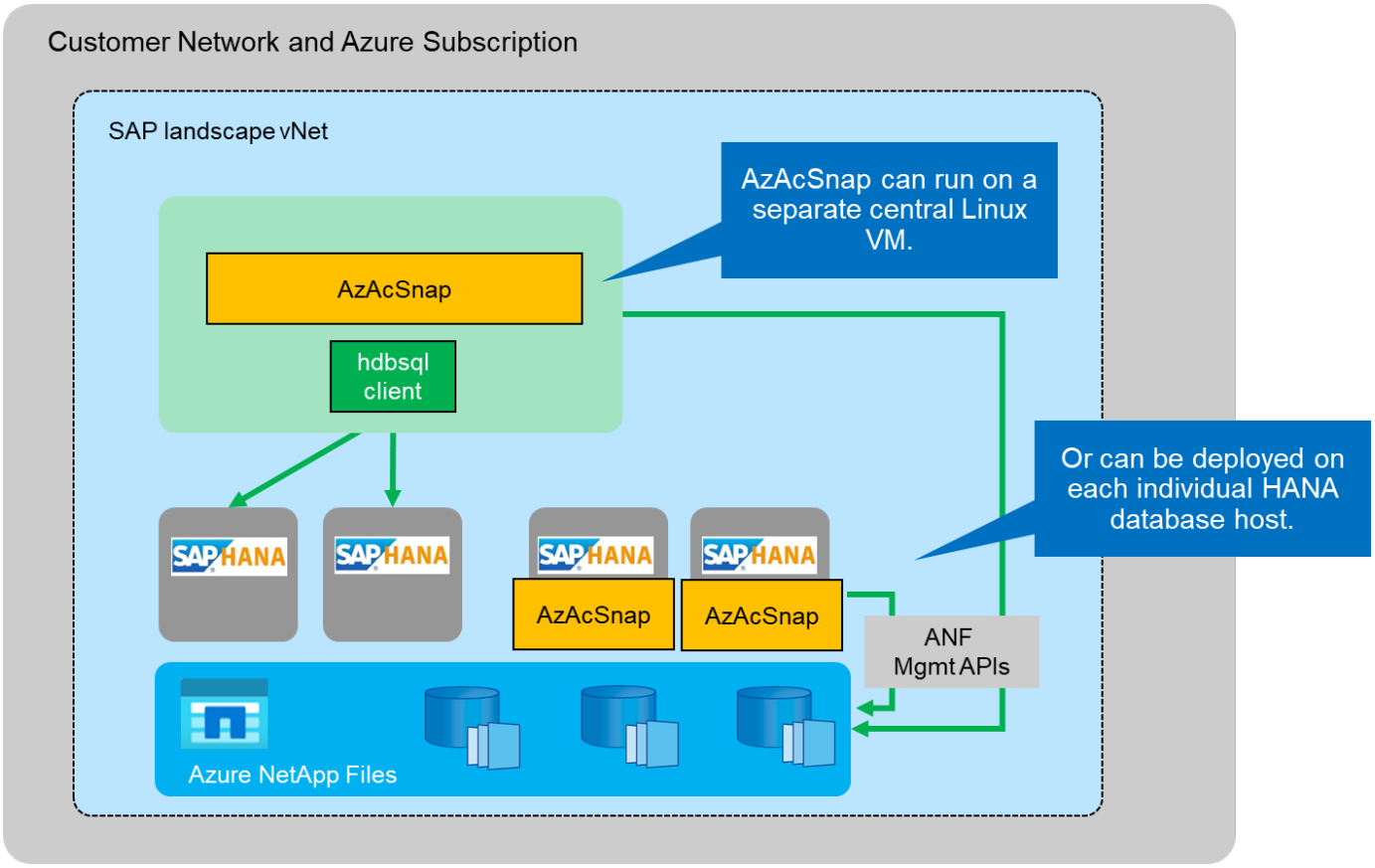



前提条件および制限事項

次の前提条件を満たしている必要があります。

**AzAcSnap**がインストールされ、ソースデータベース用に設定されている

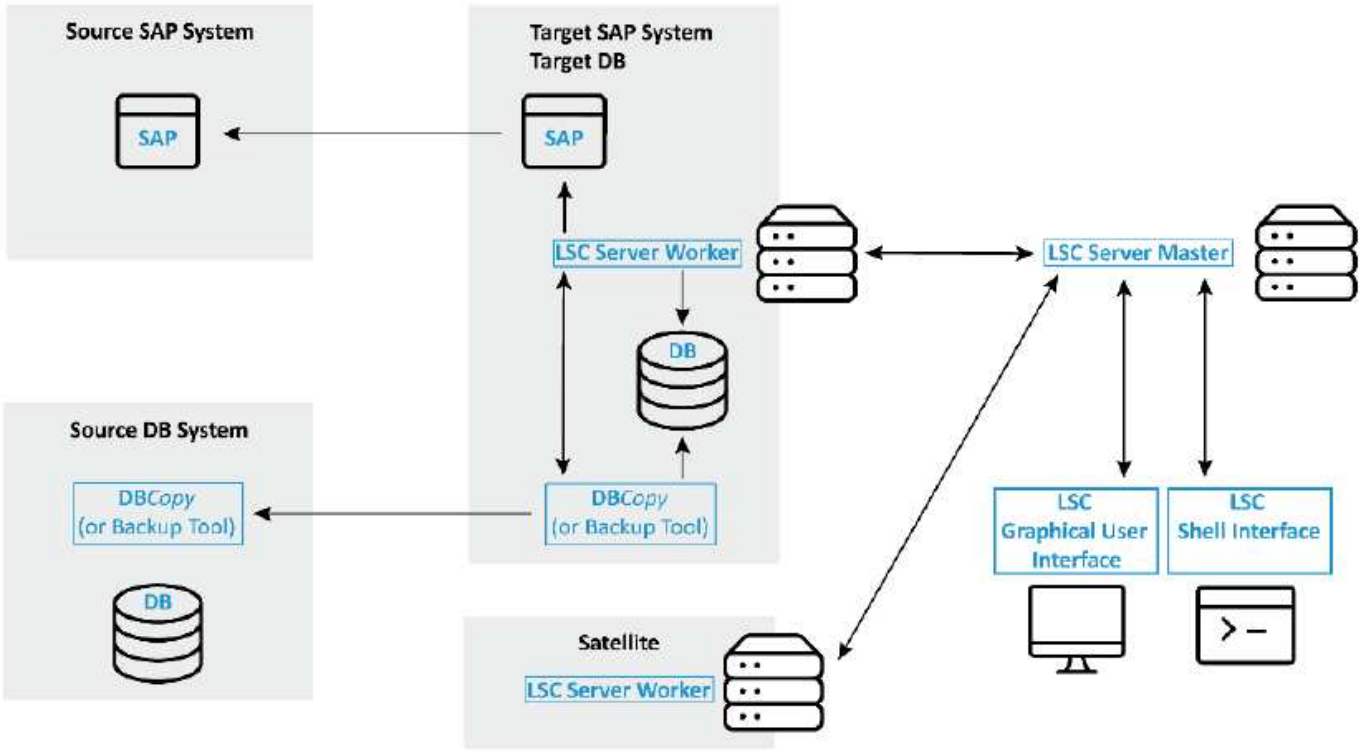
一般に、AzAcSnapには次の図に示すように、2つの導入オプションがあります。




AzAcSnapは、すべてのDB構成ファイルが一元的に格納されている中央のLinux VMにインストールして実行できます。AzAcSnapは、すべてのデータベースに（hdbsqlクライアントを介して）すべてのデータベースと、これらすべてのデータベースに設定されたHANAユーザストアキーにアクセスできます。分散型の展開では、AzAcSnapは各データベースホストに個別にインストールされ、通常はローカルデータベースのDB構成のみが格納されます。どちらの展開オプションもLSC統合でサポートされています。ただし、このドキュメントのラボセットアップではハイブリッドアプローチを採用しました。AzAcSnapは、すべてのDB構成ファイルとともに中央のNFS共有にインストールされました。この中央インストール共有は、「/mnt/software/AZACSNAP/snapshot-tool」の下のすべてのVMにマウントされました。その後、このツールはDB VM上でローカルに実行され、

**Libelle SystemCopy**がソースおよびターゲットの**SAP**システム用にインストールおよび設定されていること

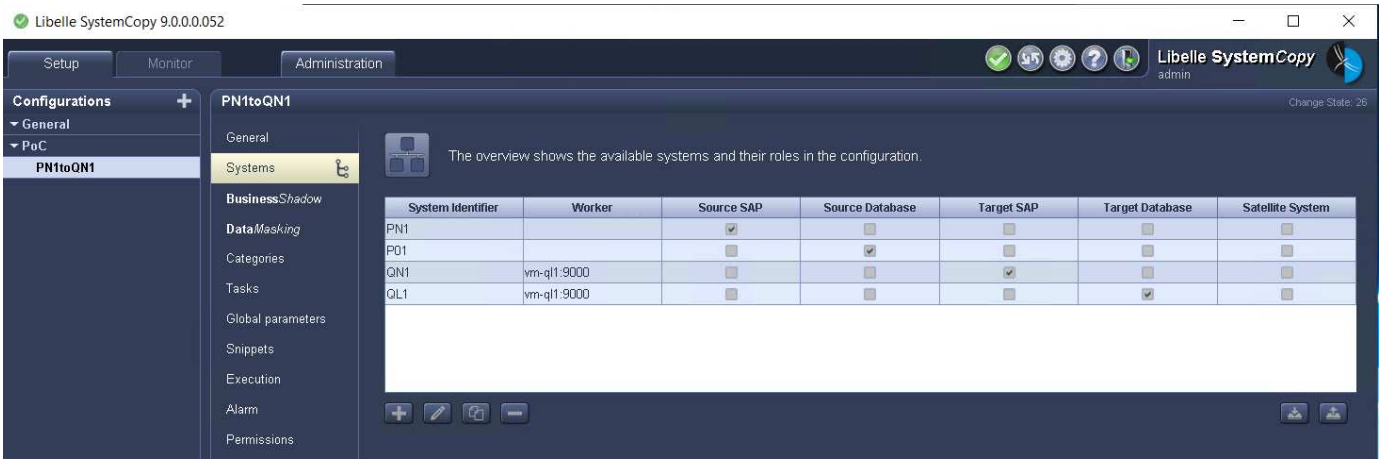
Libelle SystemCopyの展開は、次のコンポーネントで構成されています。




- *LSC Master.*という名前が示すように、これはLibelleベースのシステムコピーの自動ワークフローを制御するマスターコンポーネントです。
- * LSC Worker。* LSCワーカーは通常、ターゲットSAPシステム上で実行され、自動システムコピーに必要なスクリプトを実行します。
- * LSC Satellite。* LSCサテライトは、追加のスクリプトを実行する必要があるサードパーティシステムで実行されます。LSCマスターは、LSCサテライトシステムの役割も果たします。

Libelle SystemCopy（LSC）GUIが適切なVMにインストールされている必要があります。この実習セットアップでは、LSC GUIは別のWindows VMにインストールされていますが、LSCワーカーとともにDBホストでも実行できます。LSCワーカーは、少なくともターゲットDBのVMにインストールする必要があります。選択したAzAcSnap展開オプションによっては、LSCワーカーの追加インストールが必要な場合があります。AzAcSnapが実行されるVMにLSCワーカーインストールが必要です。

LSCをインストールした後、ソースおよびターゲットデータベースの基本設定をLSCガイドラインに従って実行する必要があります。次の図は、このドキュメントのラボ環境の構成を示しています。ソースとターゲットのSAPシステムおよびデータベースの詳細については、次のセクションを参照してください。



また、SAPシステムに適した標準のタスクリストを設定する必要があります。LSCのインストールおよび設定の詳細については、LSCインストールパッケージの一部であるLSCユーザマニュアルを参照してください。

### 既知の制限

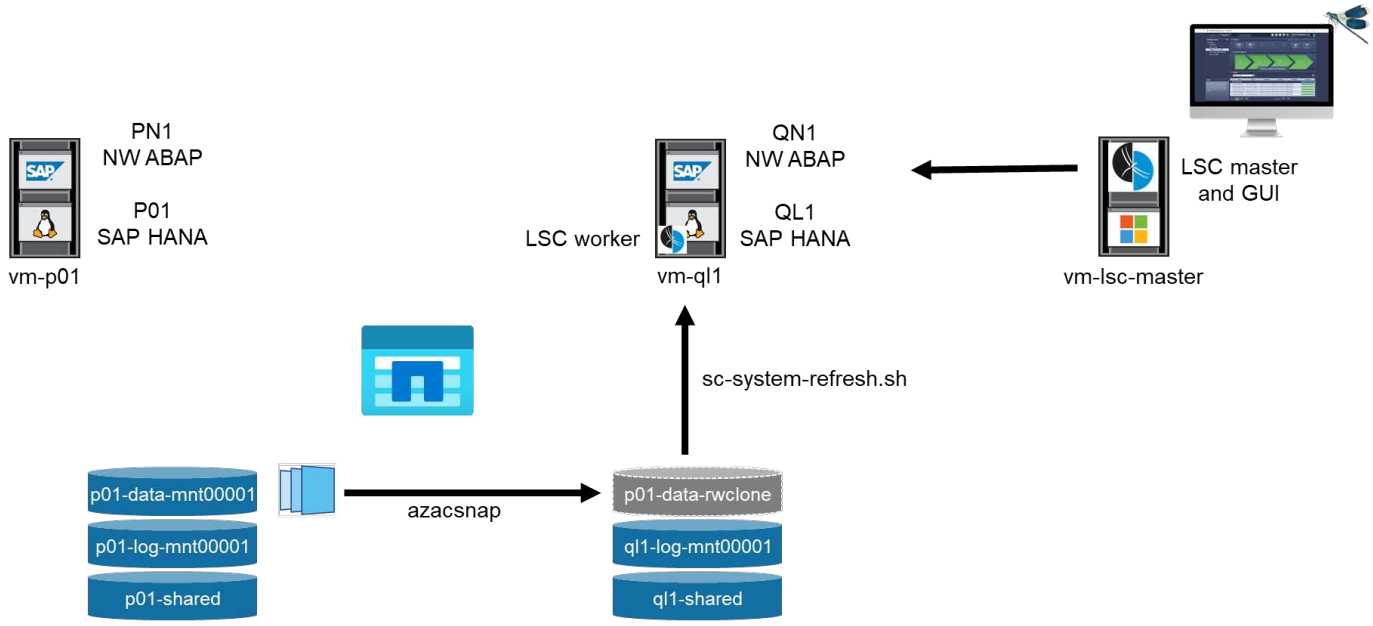
ここで説明するAzAcSnapとLSCの統合は、SAP HANAのシングルホストデータベースでのみ機能します。SAP HANAマルチホスト（またはスケールアウト）配置もサポートできますが、このような配置では、コピーフェーズおよびアンダーレイアウトスクリプトのLSCカスタムタスクをいくつか調整または拡張する必要があります。このような機能強化については、本ドキュメントでは説明していません。

SAPシステムの更新機能が統合される際には、ソースシステムのSnapshotコピーが最新で正常に作成され、ターゲットシステムの更新が実行されます。他の古いSnapshotコピーを使用する場合は、の対応するロジックを指定します ZAZACSNAPRESORE カスタムタスクを調整する必要があります。このプロセスについては、本ドキュメントでは説明しません。

### ラボのセットアップ

このラボ環境は、ソースのSAPシステムとターゲットのSAPシステムで構成され、どちらもSAP HANAのシングルホストデータベースで実行されます。

次の図は、ラボのセットアップを示しています。



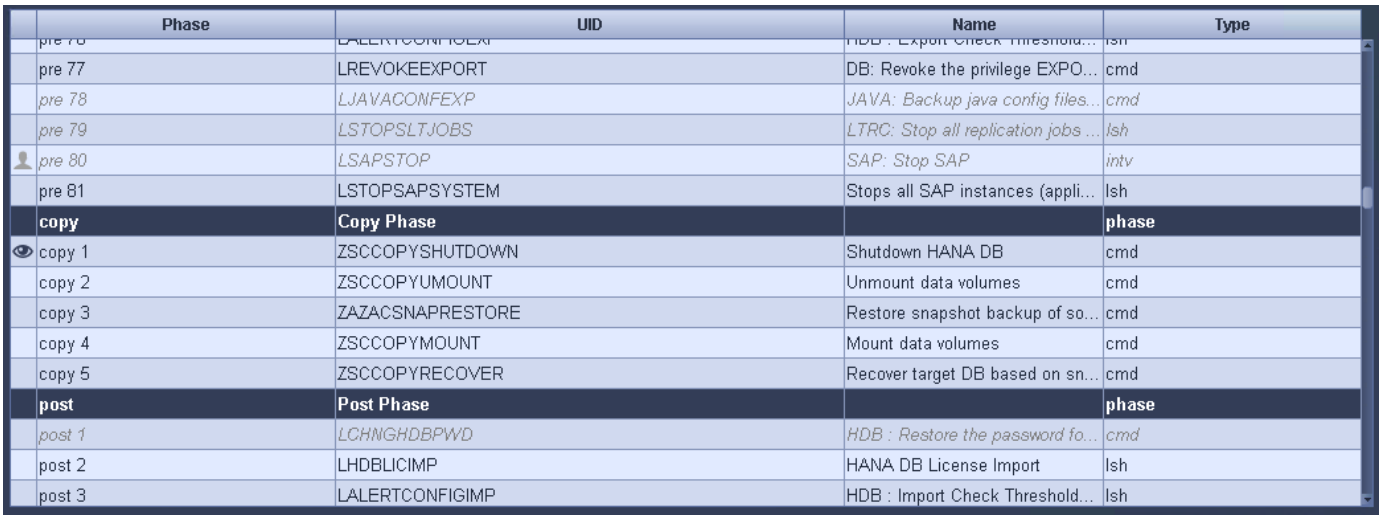

このボリュームには、次のシステム、ソフトウェアバージョン、およびAzure NetApp Files ボリュームが含まれています。

- * P01。* SAP HANA 2.0 SP5データベース。ソースデータベース、シングルホスト、シングルユーザテナント
- * PN1.* SAP NetWeaver ABAP 7.51ソースのSAPシステム：
- * VM-P01。* SLES 15 SP2、AzAcSnapがインストールされている場合。ソースVMでP01とPN1をホストしています。
- * QL1.* SAP HANA 2.0 SP5データベース。ターゲットデータベース、シングルホスト、シングルユーザテナントのシステム更新

- * QN1.* SAP NetWeaver ABAP 7.51システム更新の対象となるSAPシステム：
- * VM-QL1.* LSCワーカーがインストールされたSLES 15 SP2。ターゲットのVMでQL1とQN1をホストしています。
- LSCマスターバージョン9.0.0.052。
- * VM-LSC-MMASTER.* Windows Server 2016。LSCマスターおよびLSC GUIをホストします。
- 専用DBホストにマウントされたP01とQL1のデータ、ログ、共有のAzure NetApp Files ボリューム。
- スクリプト、AzAcSnapのインストール、すべてのVMにマウントされた構成ファイル用のCentral Azure NetApp Files ボリューム。

最初の**1**回限りの準備手順

最初のSAPシステムの更新を実行する前に、AzAcSnapで実行されるAzure NetApp Files のSnapshotコピーおよびクローニングベースのストレージ処理を統合する必要があります。また、データベースの起動と停止、およびAzure NetApp Files ボリュームのマウントまたはアンマウントを実行する補助スクリプトも実行する必要があります。必要なすべてのタスクは、コピーフェーズの一部としてLSCでカスタムタスクとして実行されます。次の図は、LSCタスクリスト内のカスタムタスクを示しています。



| | Phase | UID | Name | Type |
|---|---|---|---|---|
| | pre 77 | LREVOKEEXPORT | DB: Revoke the privilege EXPO... | cmd |
| | *pre 78* | *LJAVACONFEXP* | *JAVA: Backup java config files...* | *cmd* |
| | *pre 79* | *LSTOPSLTJOBS* | *LTRC: Stop all replication jobs ...* | *lsh* |
| | *pre 80* | *LSAPSTOP* | *SAP: Stop SAP* | *intv* |
| | pre 81 | LSTOPSAPSYSTEM | Stops all SAP instances (appli... | lsh |
| | **copy** | **Copy Phase** | | **phase** |
| | copy 1 | ZSCCOPYSHUTDOWN | Shutdown HANA DB | cmd |
| | copy 2 | ZSCCOPYUMOUNT | Unmount data volumes | cmd |
| | copy 3 | ZAZACSNAPRESTORE | Restore snapshot backup of so... | cmd |
| | copy 4 | ZSCCOPYMOUNT | Mount data volumes | cmd |
| | copy 5 | ZSCCOPYRECOVER | Recover target DB based on sn... | cmd |
| | **post** | **Post Phase** | | **phase** |
| | *post 1* | *LCHNGHDBPWD* | *HDB : Restore the password fo...* | *cmd* |
| | post 2 | LHDBLICIMP | HANA DB License Import | lsh |
| | post 3 | LALERTCONFIGIMP | HDB : Import Check Threshold... | lsh |

5つのコピー・タスクの詳細については'以下を参照してくださいこれらのタスクの一部では、サンプルスクリプト「sc-system-refresh.sh」を使用して、必要なSAP HANAデータベースのリカバリ処理と、データボリュームのマウントおよびアンマウントをさらに自動化します。スクリプトは、LSCに対する実行が成功したことを示すために、システム出力で「LSC:SUCCESS」メッセージを使用します。カスタムタスクおよび使用可能なパラメータの詳細については、LSCユーザマニュアルおよびLSC開発者ガイドを参照してください。このラボ環境のすべてのタスクは、ターゲットDB VMで実行されます。

> サンプルスクリプトは現状のまま提供されており、ネットアップではサポートしていません。スクリプトは、mailto：ng-sapcc@netapp.com [ ng-sapcc@netapp.com ^]にEメールで送信できます。

**Sc-system-refresh.sh**構成ファイル

前述したように、補助スクリプトを使用して、データベースの起動と停止、Azure NetApp Files ボリュームのマウントとアンマウント、およびSnapshotコピーからのSAP HANAデータベースのリカバリを行います。スクリプト「sc-system-refresh.sh」は中央NFS共有に格納されます。スクリプトでは、ターゲットデータベースごとに構成ファイルが必要です。このファイルは、スクリプト自体と同じフォルダに格納する必要がありま

す。コンフィギュレーションファイルには、「sc-system-refresh-<target DB SID>.cfg」という名前（この実習環境では「sc-system-refresh-ql1.cfg」など）を付ける必要があります。ここで使用する構成ファイルでは、固定/ハードコーディングされたソースDB SIDを使用します。いくつかの変更により、スクリプトと構成ファイルを拡張して、ソースDB SIDを入力パラメータとして取得できます。

特定の環境に応じて、次のパラメータを調整する必要があります。

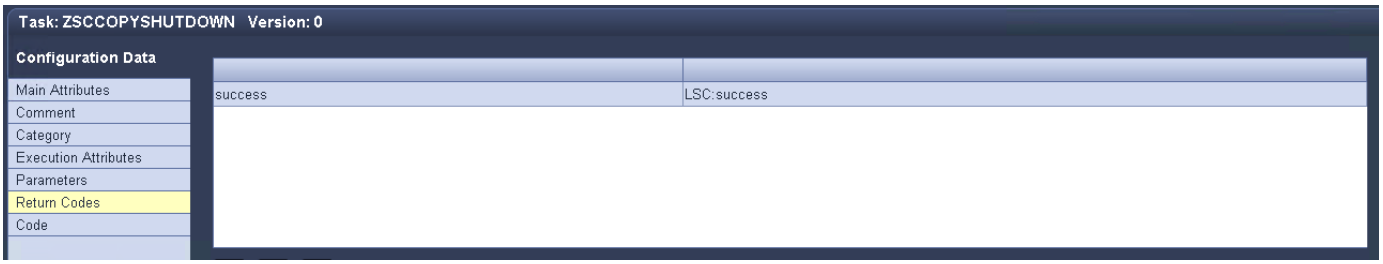
```
# hdbuserstore key, which should be used to connect to the target database
KEY=”QL1SYSTEM”
# single container or MDC
export P01_HANA_DATABASE_TYPE=MULTIPLE_CONTAINERS
# source tenant names { TENANT_SID [, TENANT_SID]* }
export P01_TENANT_DATABASE_NAMES=P01
# cloned vol mount path
export CLONED_VOLUMES_MOUNT_PATH=`tail -2
/mnt/software/AZACSNAP/snapshot_tool/logs/azacsnap-restore-azacsnap-
P01.log | grep -oe “[0-9]*\.[0-9]*\.[0-9]*\.[0-9]*:/.* “`
```

#### ZSCCOPYSHUTDOWN

このタスクは、ターゲットのSAP HANAデータベースを停止します。このタスクの[コード]セクションには、次のテキストが含まれています。

```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/scripts/sc-system-refresh/sc-system-refresh.sh shutdown
$_system(target_db, id)_$ > $_logfile_$
```

スクリプト「sc-system-refresh.sh」は’shutdownコマンドとDB SIDの2つのパラメータを取り’sapcontrolを使用してSAP HANAデータベースを停止しますシステム出力は標準のLSCログファイルにリダイレクトされます。前述のように、「lsc：success」メッセージは、正常に実行されたことを示します。




#### ZSCCOPYUMOUNT

このタスクでは、ターゲットのDBオペレーティングシステム（OS）から古いAzure NetApp Files データボリュームをアンマウントします。このタスクのコードセクションには、次のテキストが含まれています。

```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/scripts/sc-system-refresh/sc-system-refresh.sh umount
$_system(target_db, id)_$ > $_logfile_$
```

前のタスクと同じスクリプトが使用されます。渡される2つのパラメータは'umount'コマンドとDB SIDです

#### ZAZACSNAPRESORE

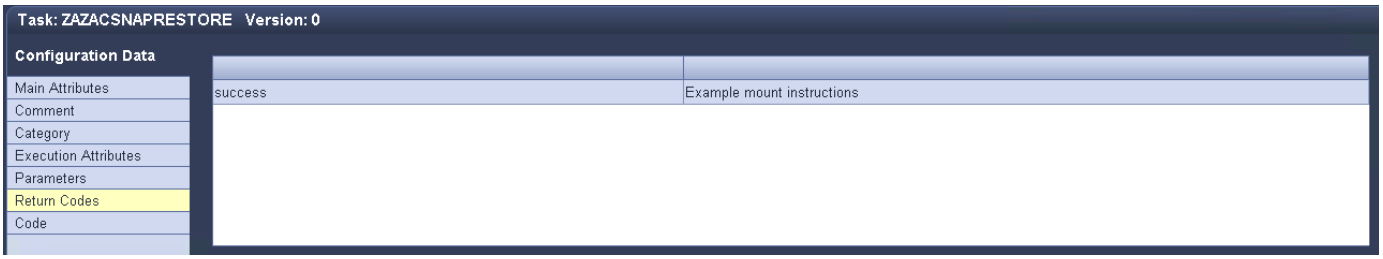
このタスクでは、AzAcSnapを実行して、ソースデータベースの最新の成功したSnapshotコピーを、ターゲットデータベースの新しいボリュームにクローニングします。この処理は、従来のバックアップ環境でのバックアップのリダイレクトリストアに相当します。ただし、Snapshotコピーとクローニング機能を使用すれば、最大のデータベースであっても数秒でこのタスクを実行できます。従来のバックアップでは、このタスクに数時間かかることもありました。このタスクのコードセクションには、次のテキストが含まれています。

```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/AZACSNAP/snapshot_tool/azacsnap -c restore --restore
snaptovol --hanasid $_system(source_db, id)_$
--configfile=/mnt/software/AZACSNAP/snapshot_tool/azacsnap
-$_system(source_db, id)_$.json > $_logfile_$
```

AzAcSnapの'restore'コマンド・ライン・オプションに関する完全なドキュメントはAzureのドキュメントを参照してください "Azure Application Consistent Snapshotツールを使用してリストア"。この呼び出しでは、ソースDBのJSON DB構成ファイルが、「azacsnap -<source DB SID>」という命名規則に従って中央のNFS共有にあることが前提となります。JSON形式（このラボ環境では'azacsnap-p0P01 JSONなど）

> AzAcSnapコマンドの出力は変更できないため、このタスクにはデフォルトの「LSC:SUCCESS」メッセージを使用できません。そのため'AzAcSnap出力の文字列'Example mount instructionsが'成功した戻りコードとして使用されます5.0 GAバージョンのAzAcSnapでは、この出力はクローニングプロセスが成功した場合にのみ生成されます。

次の図に、新しいボリュームへのAzAcSnapリストア成功メッセージを示します。




#### ZSCCOPYMOUNT

このタスクでは、ターゲットDBのOSに新しいAzure NetApp Files データボリュームをマウントします。このタスクのコードセクションには、次のテキストが含まれています。

```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/scripts/sc-system-refresh/sc-system-refresh.sh mount
$_system(target_db, id)_$ > $_logfile_$
```

sc-system-refresh.shスクリプトが再び使用され'mountコマンドとターゲットDB SIDが渡されます

#### ZSCCOPYRECOVER

このタスクでは、リストア（クローン）されたSnapshotコピーに基づいて、システムデータベースとテナントデータベースのSAP HANAデータベースのリカバリを実行します。ここで使用するリカバリ・オプションは、フォワード・リカバリに適用される特定のデータベース・バックアップ（追加ログなしなど）を対象としています。したがって、リカバリ時間は非常に短くなります（最大で数分）。この処理の実行時間は、リカバリプロセス後に自動的に実行されるSAP HANAデータベースの起動によって決まります。起動時間を短縮するために、必要に応じて、次のAzureのドキュメントに従ってAzure NetApp Files データボリュームのスループットを一時的に向上させることができます。 "ボリュームクォータの動的な増減"。このタスクのコードセクションには、次のテキストが含まれています。

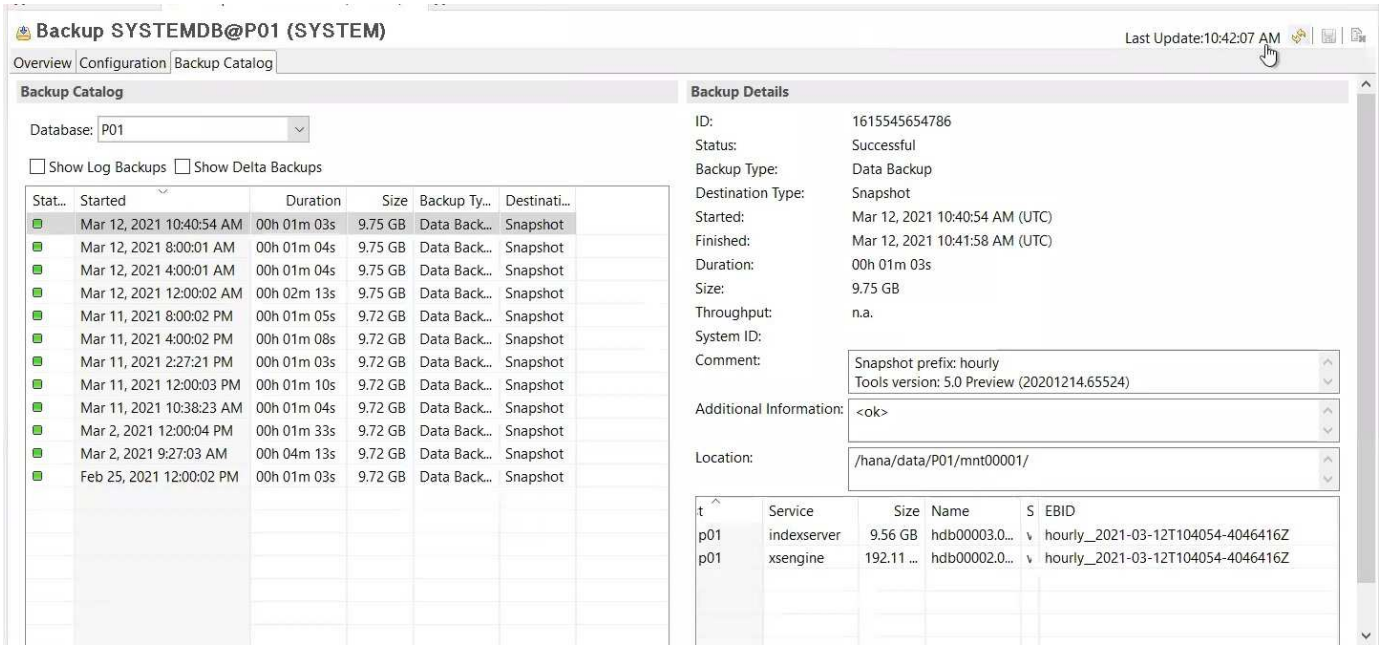
```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/scripts/sc-system-refresh/sc-system-refresh.sh recover
$_system(target_db, id)_$ > $_logfile_$
```

このスクリプトは'recover'コマンドとターゲットDB SIDとともに再び使用されます

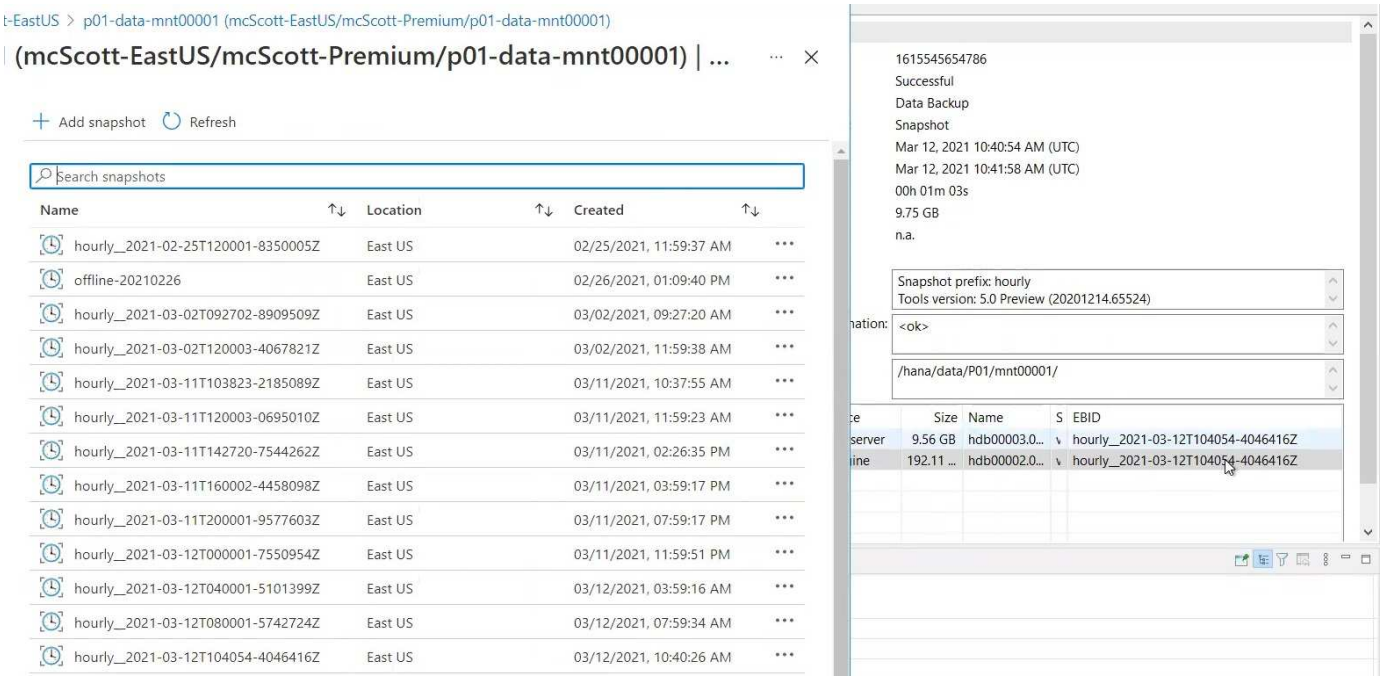
### SAP HANAシステムの更新処理

このセクションでは、ラボシステムの更新処理のサンプルとして、このワークフローの主な手順を記載します。

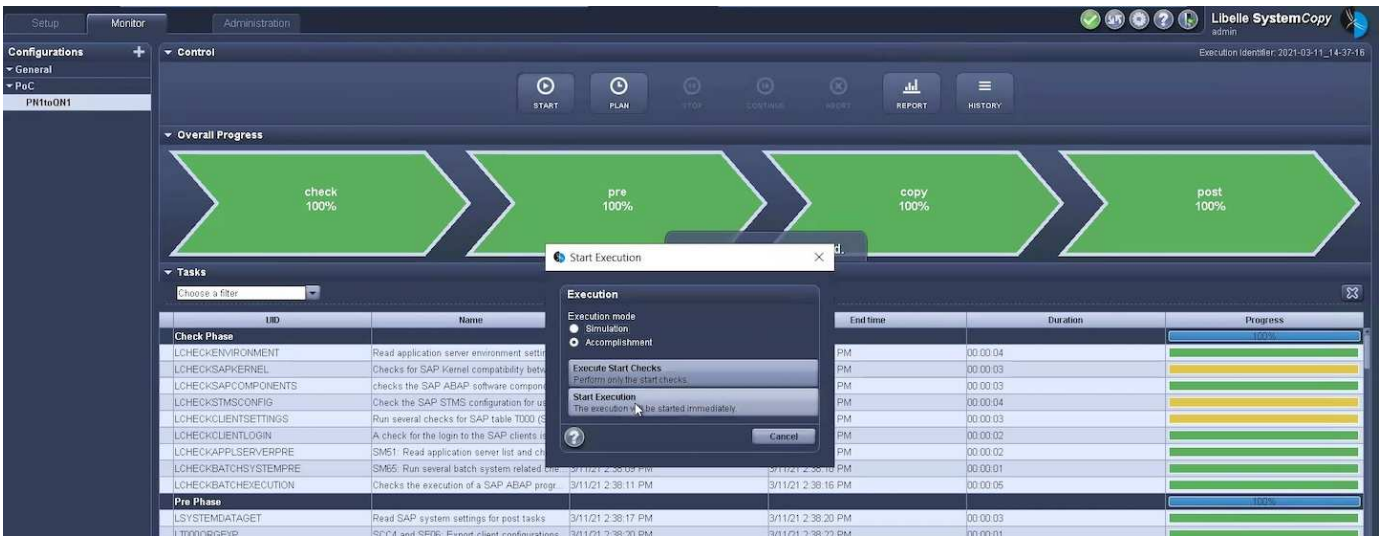
バックアップカタログに記載されたP01ソースデータベースの定期的なSnapshotコピーとオンデマンドSnapshotコピーが作成されている。



更新処理には、3月12日の最新バックアップが使用されています。バックアップの詳細セクションに、このバックアップの外部バックアップID（EBID）が表示されます。次の図に示すように、Azure NetApp Files データボリューム上の、対応するSnapshotコピーバックアップのSnapshotコピー名を指定します。



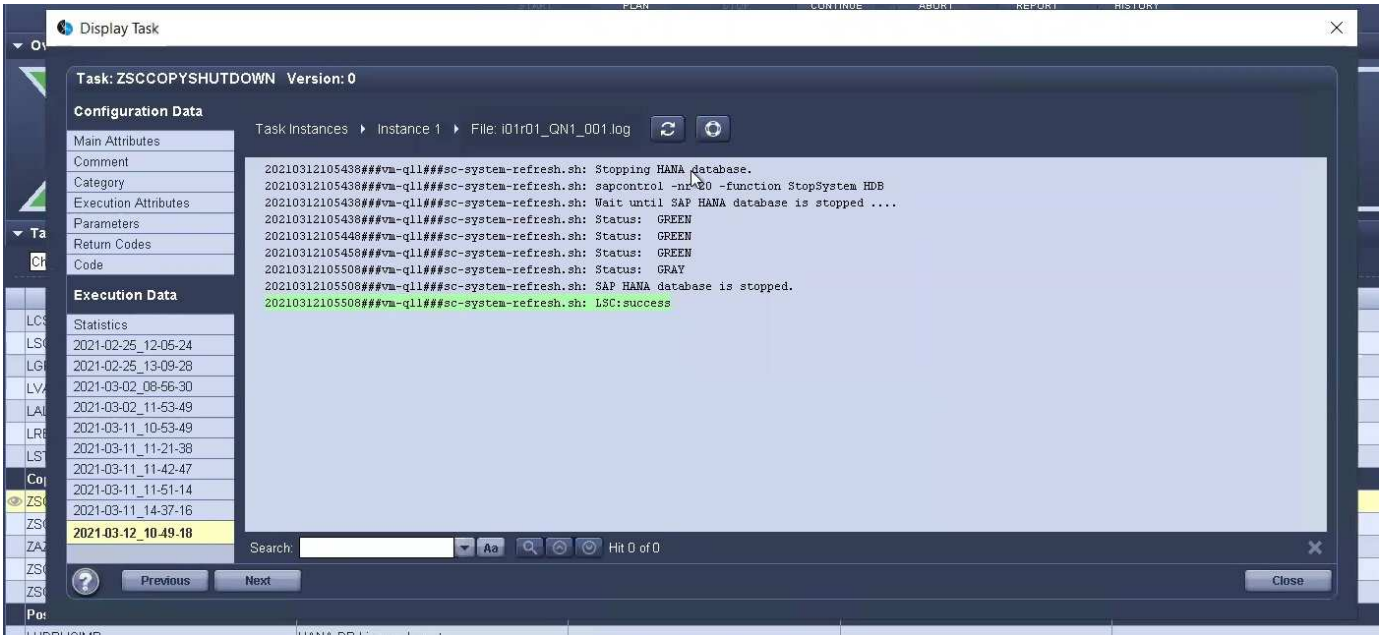

更新操作を開始するには、LSC GUIで正しい設定を選択し、[実行の開始]をクリックします。



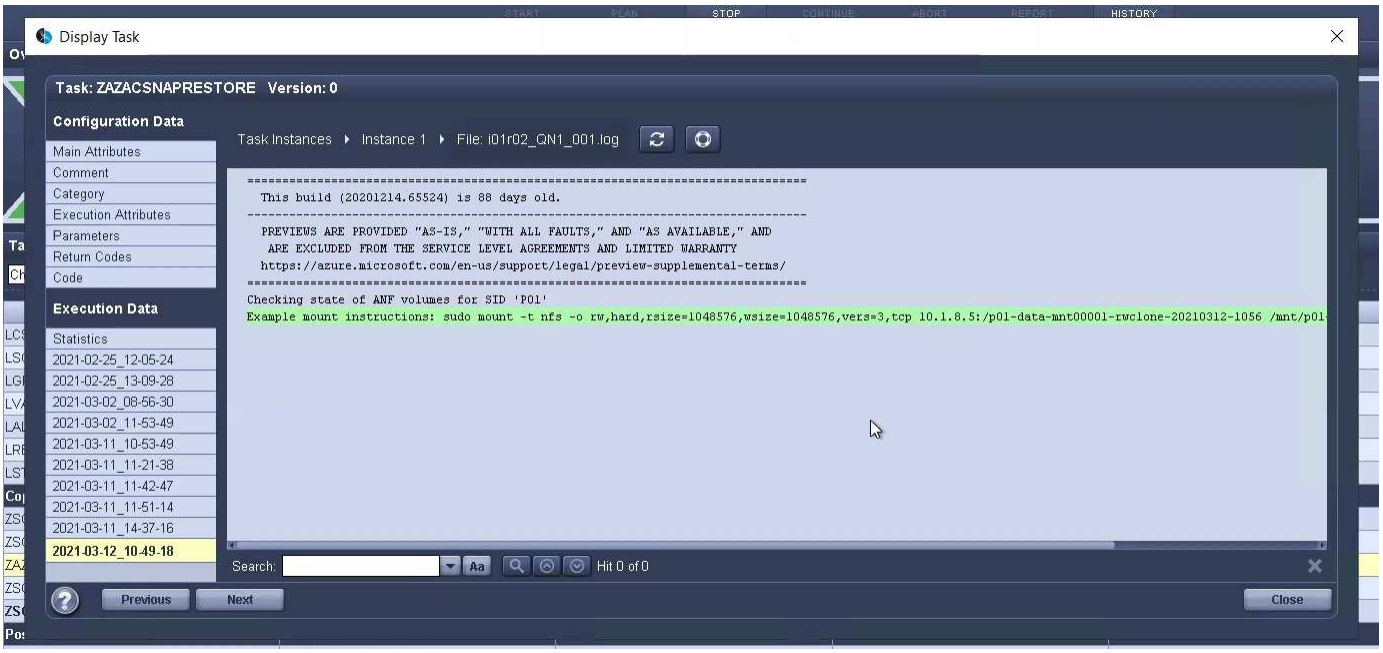

LSCは、チェックフェーズのタスクの実行を開始し、プリフェーズの設定済みタスクを実行します。

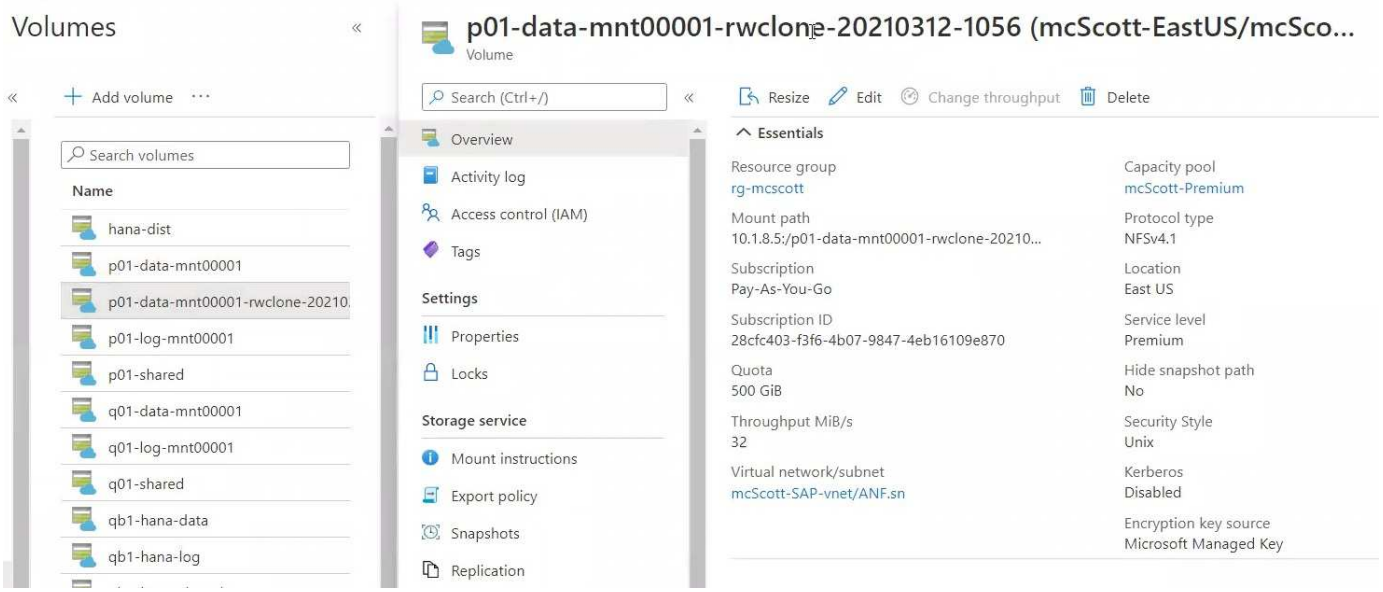



移行前フェーズの最後のステップとして、移行先のSAPシステムが停止します。次のコピーフェーズでは、前のセクションで説明したステップが実行されます。まず、ターゲットのSAP HANAデータベースが停止し、古いAzure NetApp Files ボリュームがOSからアンマウントされます。

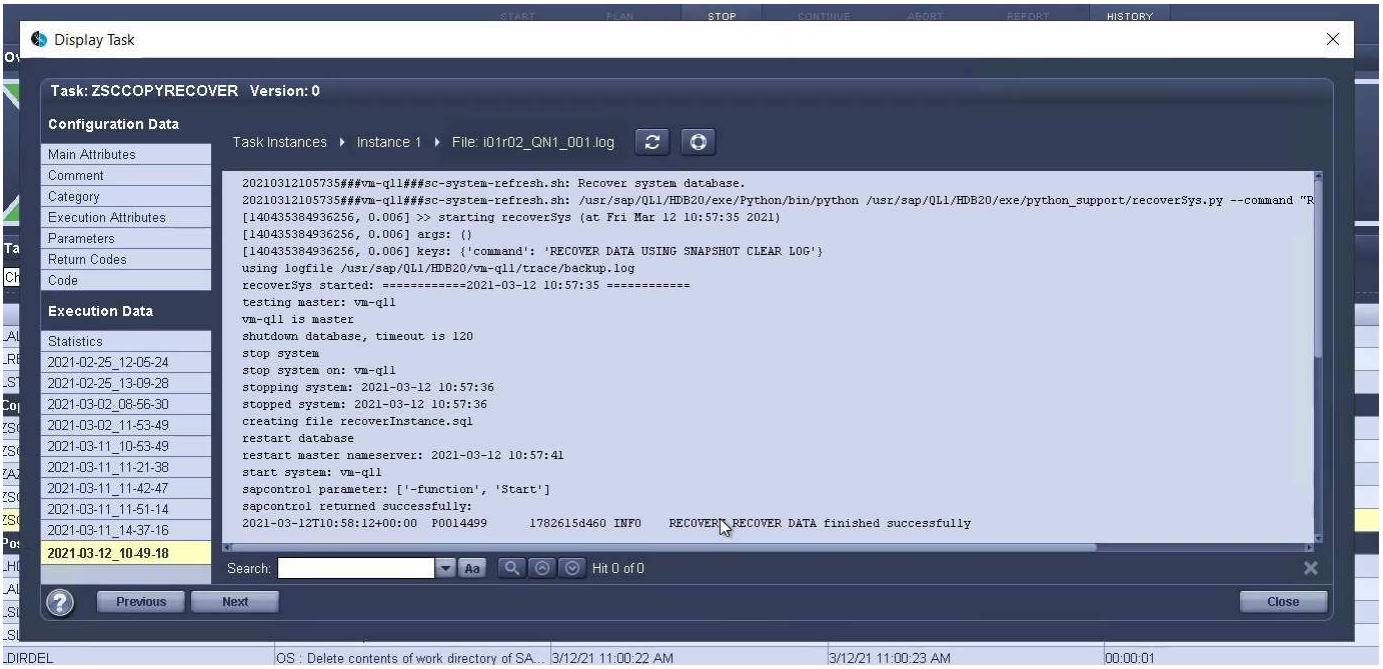



次に、ZAZACSNAPRESTOREタスクで、P01システムの既存のSnapshotコピーからクローンとして新しいボリュームを作成します。次の2つの図は、LSC GUIでのタスクのログ、およびAzureポータルでのクローンAzure NetApp Files ボリュームを示しています。




その後、この新しいボリュームがターゲットDBホストとシステムデータベースにマウントされ、テナントデータベースが、包含するSnapshotコピーを使用してリカバリされます。リカバリが完了すると、SAP HANAデータベースが自動的に起動します。このSAP HANAデータベースの起動は、コピーフェーズのほとんどの時間を占めています。残りの手順は、データベースのサイズに関係なく、通常数秒で終了します。次の図は、SAPが提供するPythonリカバリスクリプトを使用してシステムデータベースをリカバリする方法を示しています。




コピーフェーズ後、LSCはPostフェーズで定義されたすべてのステップで継続します。システムの更新プロセスが完了すると'ターゲット・システムは再び稼働し'完全に使用可能になりますこのラボシステムでは、SAPシステムの更新に必要な合計実行時間は約25分でした。このうち、コピーフェーズで消費される時間は5分未満です。




## 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。

- ネットアップの製品マニュアル

  "https://docs.netapp.com"

バージョン履歴

| バージョン | 日付 | ドキュメントバージョン履歴 |
| --- | --- | --- |
| バージョン 1.0 以降 | 2022年4月 | 初版リリース |

# 解決策概要

## SB-3978 ：『 Lifecycle Management for SAP HANA 』

ネットアップは、 SAP Landscape Management （ SAP LaMa ）など、 SAP 管理者が日々の運用で使用するツールに完全に統合されたライフサイクル管理解決策を提供することで、機能の実装が遅いという課題や、自動化の欠如、生産性の低下に対処しています。プリプロセスからポストプロセスまで、プロビジョニングのワークフローを簡易化することを目的としています。本番用システムのコピーを作成するために必要なソフトウェアレイヤとストレージレイヤのタスクもすべて含みます。この解決策を使用すると、管理者はマウスを数回クリックするだけで開発およびテスト環境を作成できるため、ライフサイクル管理が向上します。

https://www.netapp.com/pdf.html?item=/media/6996-sb-3978pdf.pdf

## SB-3965: SAP HANAのバックアップとリカバリ

### 課題

SAP HANA のバックアップおよびリストア操作では、組織は次の課題に直面します。• 本番環境の SAP システムでパフォーマンスの低下を伴う長時間のバックアップ操作• 長時間のリストアおよびリカバリ操作による許容できないシステムダウンタイム• アプリケーションの重要度によるバックアップウィンドウの短縮• 論理破損を軽減するための柔軟なソリューションの必要性

### 主要なソリューション・コンポーネント

NetApp ONTAP ® データ管理ソフトウェアを実行するNetApp ® ストレージ ソリューションをNetApp SnapCenter ® データ保護ソフトウェアと組み合わせて使用すれば、これらすべての課題に対応できます。また、 ONTAPソフトウェアに含まれるNetApp Snapshot™ テクノロジーを使用すると、数秒以内にあらゆるサイズのデータセットのバックアップを作成したり、復元操作を実行したりできます。 SAP HANA は、有効なバックアップ操作としてストレージベースのスナップショット コピーの使用をサポートしています。

https://www.netapp.com/pdf.html?item=/media/6997-sb-3965pdf.pdf

## SB-3968: SAP HANAの災害復旧

### 課題

IT 組織ではビジネス継続性が不可欠です。顧客がビジネスを遂行するために必要とするミッションクリティカルなアプリケーションに対して、高可用性サービスを提供できる必要があります。そうしないと、顧客の生産性は低下し、eコマース組織は収益に直接的な影響を受ける可能性があります。

### 主要なソリューション・コンポーネント

NetApp は、IT 組織があらゆるビジネス ニーズに対応できるように災害復旧計画を構築または適応できるようにするためのテクノロジとツールの包括的なポートフォリオを開発しました。

https://www.netapp.com/pdf.html?item=/media/6998-sb-3968pdf.pdf

# SB-4292：AnsibleによるSAP自動化

本ドキュメントでは、NetApp®ストレージシステムをオンプレミス、パブリッククラウドインフラサービス（IaaS）環境、ハイブリッドクラウドのいずれで運用している場合でも、Ansible Playbookとカスタムスクリプトを使用して、SAP Landscape Management（LaMa）に統合する方法について説明します。

## 解決策の概要

SAPシステムは非常に複雑です。しかし、SAPを使用している企業では、これらのシステムがビジネスプロセスの中心となっています。SAPシステム管理者は、日常的な運用タスクを自動化することで、より多くのシステムをより少ない労力で管理し、再現可能な結果を生み出し、人為的ミスを減らすことができます。

本ドキュメントでは、NetApp®ストレージシステムをオンプレミス、パブリッククラウドインフラサービス（IaaS）環境、ハイブリッドクラウドのいずれで運用している場合でも、Ansible Playbookとカスタムスクリプトを使用して、SAP Landscape Management（LaMa）に統合する方法について説明します。この統合により、SAP管理者は、NetApp Snapshot™およびNetApp FlexClone®テクノロジを使用して、SAPシステムの更新タスクを高速化できます。

### 対象者

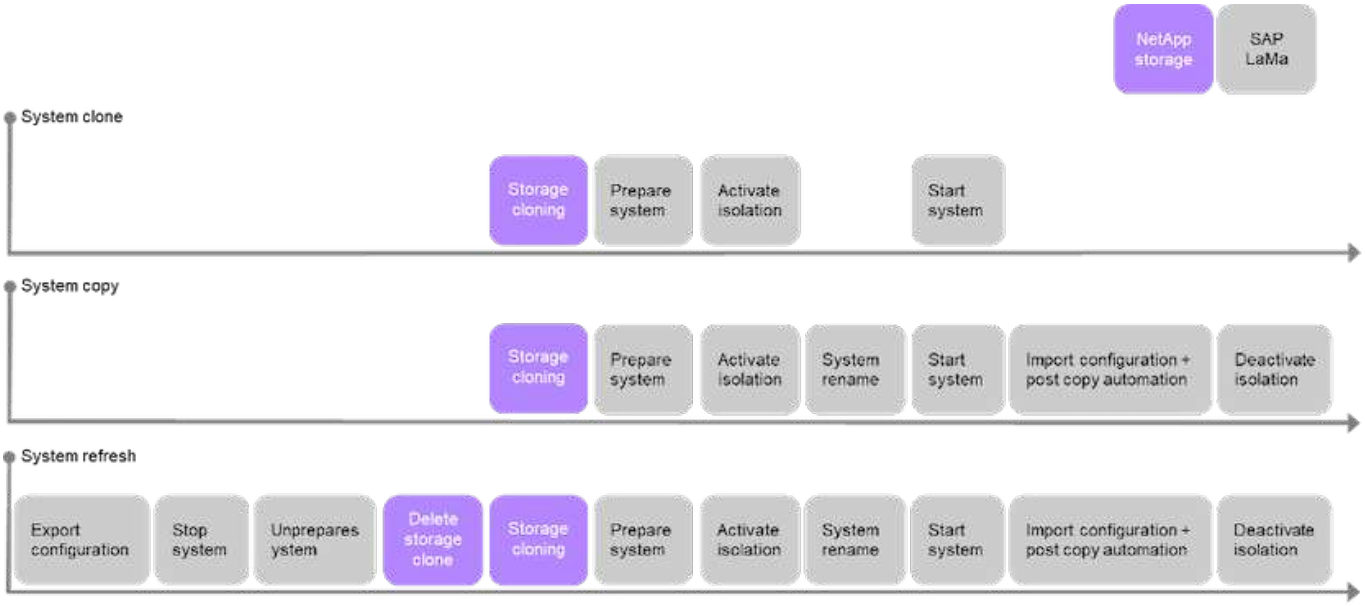
本ドキュメントは、Ansibleの自動化にあまり経験がない（またはまったく経験がない）SAPシステム管理者を対象としています。Ansibleの使用を開始し、最初のプレイブックを実行し、SAP LaMaベースの最初のシステム更新処理を設定して実行するのに役立ちます。

### SAPシステムのクローニング、コピー、更新のシナリオ

SAPシステムのコピーは、SAPシステムのクローニング、SAPシステムのコピー、SAPシステムの更新という3つのプロセスの同義語としてよく使用されます。ワークフローとユースケースが異なるため、処理を区別することが重要です。

- * SAPシステムのクローン*。SAPシステムクローンは、ソースSAPシステムの同一のクローンです。SAPシステムクローンは、一般に論理的な破損に対処したり、ディザスタリカバリのシナリオをテストしたりするのに使用されます。システムのクローニング処理では、ホスト名、インスタンス番号、およびSecure Identifier（SID；セキュア識別子）は同じままです。そのため、本番環境と通信できないように、ターゲットシステムの適切なネットワークフェンシングを設定することが重要です。
- * SAPシステムのコピー*。SAPシステムのコピーは、ソースSAPシステムのデータを使用して新しいターゲットSAPシステムをセットアップすることです。たとえば、本番システムのデータを含む追加のテストシステムを新しいターゲットシステムにすることができます。ソース・システムとターゲット・システムでは、ホスト名、インスタンス番号、およびSIDが異なります。
- * SAPシステムの更新*。SAPシステムの更新とは、既存のターゲットSAPシステムをソースSAPシステムのデータで更新することです。ターゲットシステムは通常、品質管理システムなどのSAPトランスポート環境の一部であり、本番用システムのデータで更新されます。ソース・システムとターゲット・システムでは、ホスト名、インスタンス番号、およびSIDが異なります。

次の図はNetApp、SAPシステムのLaMaストレージに関連するクローニング、コピー、更新の各ワークフローの手順を示しています。

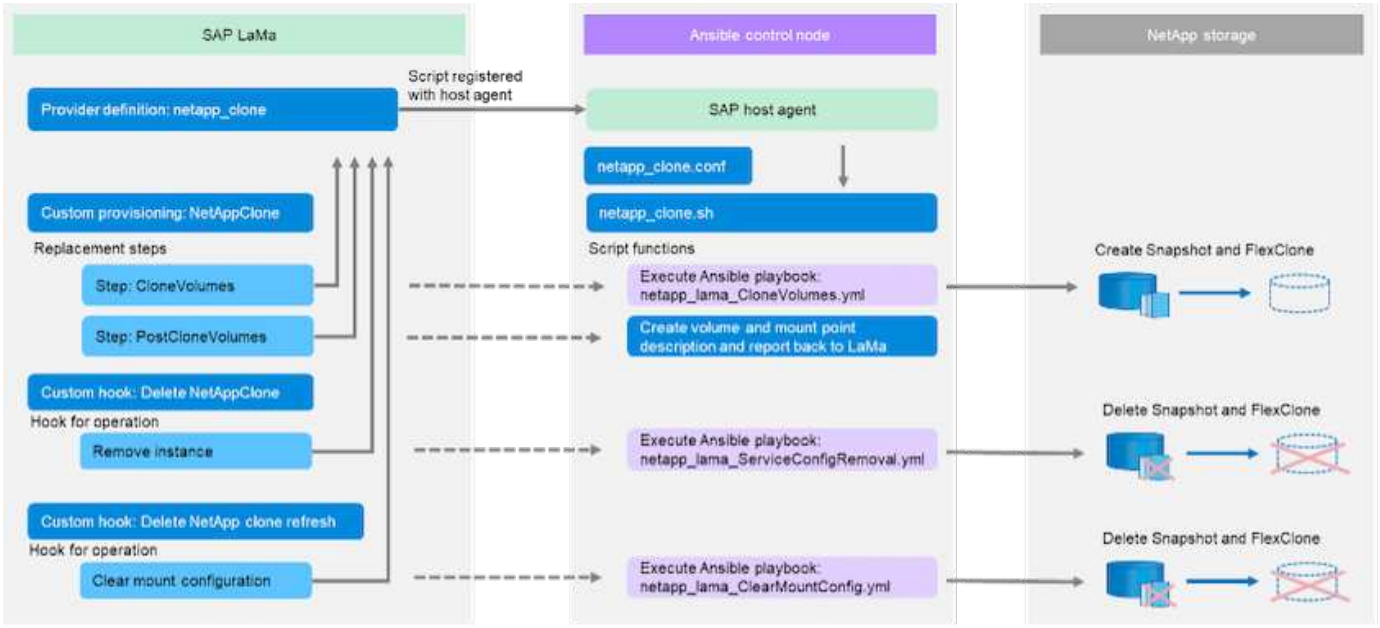



解決策テクノロジ

ソリューション全体は、次の主要コンポーネントで構成されています。

- SAP LaMaシステム
- NetAppストレージシステム
- SAPホストエージェントがインストールされたAnsibleコントロールノード。Red Hat Ansible Automation Platformを使用することを推奨します。Red Hat Ansible Automation Platformには次のようなメリットがあります。
  - AIを使用して自動化タスクに関するコードの推奨事項を生成
  - イベントドリブンな自動化で手動タスクを削減
  - 定義され、一貫性があり、移植性が高い
  - 環境全体で自動化を拡張
  - 事前パッケージ化されたコンテンツで自動化を加速
  - 豊富なレポート機能とオブザーバビリティ指標による自動化の追跡と管理
  - タスク、モジュール、プレイブックの作成

次の図は、SAPホストエージェントから実行されたシェルスクリプトによってトリガーされる、SAP LaMaストレージシステムとNetAppストレージシステムが、専用のAnsibleホスト上のAnsible Playbookを介してどのように統合されるかを示しています。

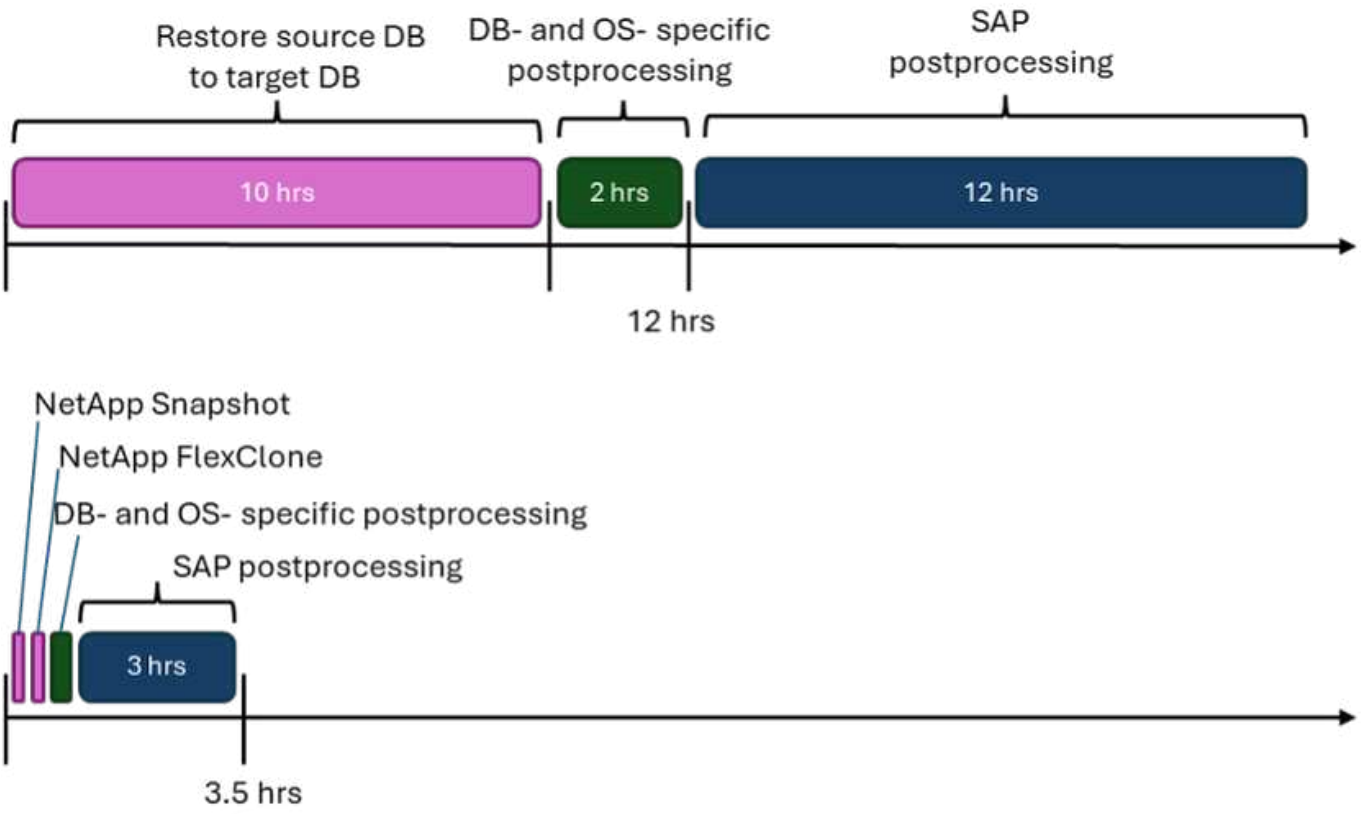



ユースケースの概要

テストやトレーニングを目的として、ソースシステムのデータをターゲットシステムで利用できるようにする必要があるシナリオはいくつかあります。これらのテストシステムとトレーニングシステムは、ソースシステムのデータで定期的に更新して、テストとトレーニングが最新のデータセットで確実に実行されるようにする必要があります。このようなシステム更新処理は、インフラ、データベース、アプリケーションの各レイヤでの複数のタスクで構成され、自動化のレベルによっては数日かかることがあります。

インフラレイヤとデータベースレイヤで必要なタスクを高速化、自動化するには、SAP LaMaとNetAppのクローニングワークフローを使用します。SAP LaMaでは、ソースシステムからターゲットシステムにバックアップをリストアする代わりに、NetApp SnapshotとFlexCloneテクノロジを使用しているため、次の図に示すように、データベースを起動するために必要なタスクを数時間ではなく数分で実行できます。クローニングプロセスに要する時間はデータベースのサイズに左右されないため、非常に大規模なシステムでも数分で作成できます。オペレーティングシステムとデータベースレイヤ、およびSAPのポストプロセス側のタスクを自動化することで、実行時間をさらに短縮できます。

次の図は、自動化を使用すると運用効率が向上する可能性があることを示しています。




さまざまなテクノロジコンポーネントの統合

Ansibleを使用してSAP LaMaをNetAppストレージシステムと統合するには、Ansible Playbookを実行できるノードが必要です。Ansible Automation Platformの使用を推奨します。SAP LaMaから起動したこのホストでシェルスクリプトとAnsible Playbookを実行するには、このサーバでSAPホストエージェントを実行する必要があります。SAP Host AgentはSAP LaMaとの双方向通信を引き継ぎ、実際のプレイブックをトリガーするシェルスクリプトを実行します。

この疎結合アーキテクチャにより、SAP LaMaだけでなく、SAP LaMa外からもワークフローを自由に開始できます。プレイブックと対応するロジックは1回だけ設定する必要があり、さまざまなシナリオやユースケースで使用できます。

## まとめ

NetApp、SAP LaMa、Ansible自動化プラットフォームを組み合わせることで、SAPシステム管理に関連する最も複雑で時間のかかるタスクに必要な時間と労力を大幅に削減できる強力なソリューションを提供します。また、この組み合わせは、人為的ミスがシステム間で引き起こす構成のずれを回避するのにも役立ちます。

システムの更新、コピー、クローン、ディザスタリカバリのテストは非常に機密性の高い手順であるため、このようなソリューションを実装すると、貴重な管理時間を節約できます。また、SAPシステム管理者に対する組織の他の組織の信頼を強化することもできます。テストなどの目的でシステムをコピーするのがどれだけ簡単か、トラブルシューティングにかかる時間をどれだけ節約できるかがわかります。

## 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。

- "NetApp ONTAP®向けAnsible Playbookを使用した運用の自動化"
- "NetApp固有のAnsibleドキュメント"
- "NetApp ONTAP Ansibleモジュールと完全なドキュメント"
- "Red Hat Ansible自動化プラットフォーム"

### バージョン履歴

| バージョン | 日付 | 概要を更新します |
| --- | --- | --- |
| バージョン0.1 | 03.2023 | 第1稿。 |
| バージョン0.2 | 01.2024 | 見直しと若干の修正 |
| バージョン0.3 | 06.2024 | HTML形式に変換 |

# SB-4293：AlpacaとNetApp SnapCenterによるSAPシステムのコピー、更新、クローニングのワークフローの自動化

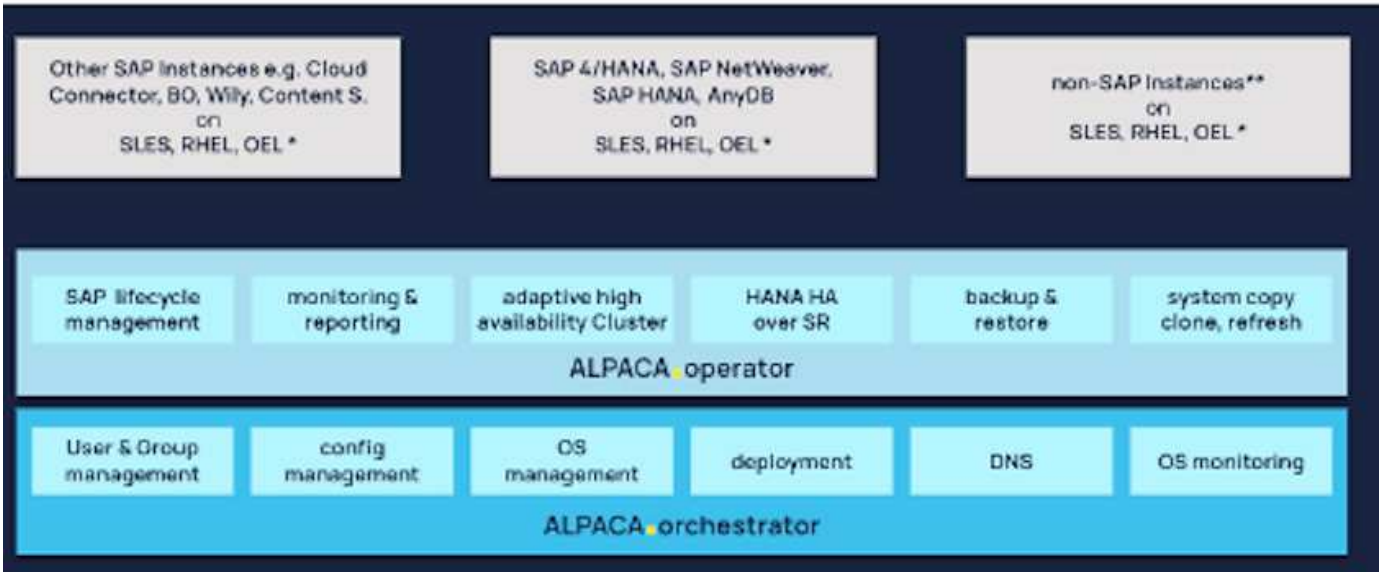
本ドキュメントでは、NetApp®Snapshot™およびFlexClone®テクノロジをAlpaca自動化ワークフローに統合する方法について説明します。

### 解決策の概要

SAPのシステムとソリューションの運用は非常に複雑です。ただし、SAPを使用している企業では、システムとサービスがビジネスプロセスの中心となります。SAPシステム管理者は、システムのコピーや更新などの日常的な運用タスクを自動化することで、より多くのシステムをより少ない労力で管理し、再現可能な結果を生み出し、人為的ミスを減らすことができます。

本ドキュメントでは、NetApp®Snapshot™およびFlexClone®テクノロジをAlpaca自動化ワークフローに統合する方法について説明します。

ランドスケープをプロアクティブに自動化—Cloud and Anywhere（Alpaca）スイートは、SAPランドスケープ全体にわたる詳細な監視と監視を可能にする包括的な管理インターフェイスです。Alpacaは、SAPインフラの運用を合理化、迅速化し、最適な可用性と透明性を確保します。インフラを含む環境全体を管理するための包括的なツールを提供し、サービスの中断、ジョブの停止、輻輳などの異常をプロアクティブに通知します。このスイートは、マルチクラウドシナリオを含め、オンプレミス、ハイブリッド、オールクラウドの各環境でシームレスに動作し、あらゆるインフラへの適応性を確保するように設計されています。このモジュールベースのフレームワークは、SAPの標準的な管理タスクと通常の管理タスク、および停止時のフェイルオーバーなどの複雑なシナリオを自動化します。 管理者/専門家、オペレーター、マネージャーは、高度な制御と自動化をこれらの専門家に提供します。




このドキュメントでは、Snapshotベースのバックアップのオーケストレーション、リストアの実行、FlexCloneボリュームの作成を行うツールであるNetApp SnapCenter®とAlpacaをどのように統合するかについて説明します。この統合により、SAP管理者は、SAPシステムの日常的な運用タスクを大幅に高速化できます。NetAppのSnapshot、FlexClone、SnapRestore®テクノロジは、ポインタベースのストレージテクノロジであるため、バックアップ、リストア、クローニングの処理を高速化します。このアプローチは高速であり、（既存データではなく）新規データや変更されたデータだけをストレージメディアに書き込む必要があるため、クローン処理中のストレージオーバーヘッドも削減されます。これは、オンプレミスのNetAppストレージシステムであっても、大手クラウドプロバイダ3社のいずれかにあるNetAppストレージソリューションであっても当てはまります。

対象者

このドキュメントは、SAPシステムのコピーを手動で実行したことがあり、Alpacaを使用してこの作業を自動化したいSAPシステム管理者を対象としています。NetApp SnapCenterによってオーケストレーションされたNetAppのSnapshotテクノロジとFlexCloneテクノロジをAlpacaのワークフローと組み合わせることで、SAPシステムのコピーを完全に自動化する時間を短縮できます。

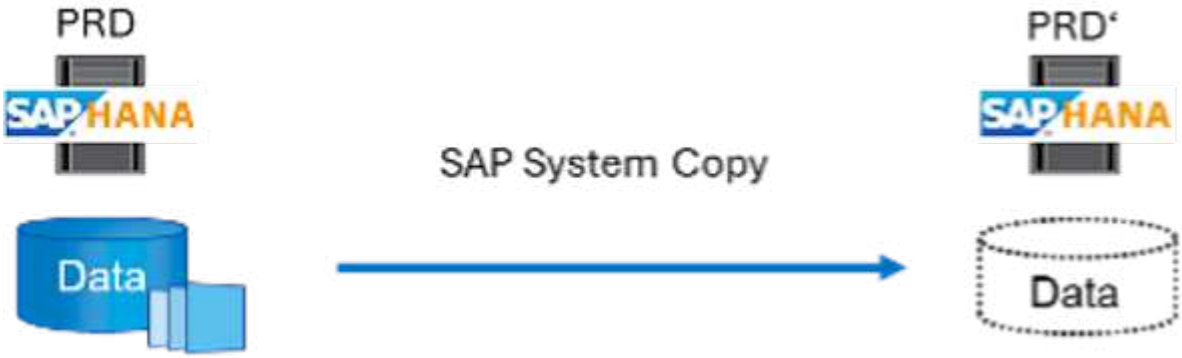
**SAP**システムのクローニング、コピー、更新のシナリオ

SAPシステムのコピーは、SAPシステムのクローニング、SAPシステムのコピー、SAPシステムの更新という3つのプロセスの同義語としてよく使用されます。ワークフローとユースケースが異なるため、これらの処理を区別することが重要です。

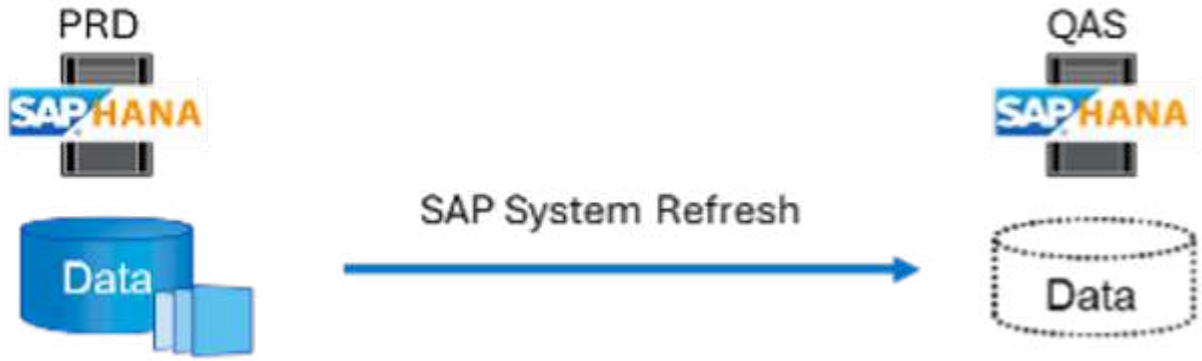
- * SAPシステムのクローン*。SAPシステムクローンは、ソースSAPシステムの同一のクローンです。SAPシステムクローンは、一般に論理的な破損に対処したり、ディザスタリカバリのシナリオをテストしたりするのに使用されます。システムのクローニング処理では、ホスト名、インスタンス番号、およびSecure Identifier（SID；セキュア識別子）は同じままです。そのため、ターゲットシステムに適切なネットワークフェンシングを確立して、本番環境と通信しないようにすることが重要です。




- * SAPシステムのコピー*。SAPシステムのコピーは、ソースSAPシステムのデータを使用して新しいターゲットSAPシステムをセットアップすることです。たとえば、本番システムのデータを含む追加のテストシステムを新しいターゲットシステムにすることができます。ホスト名、インスタンス番号、SIDは、ソースシステムとターゲットシステムで異なります。 新しいシステムはソースシステムから分離されていません。




- * SAPシステムの更新*。SAPシステムの更新とは、既存のターゲットSAPシステムをソースSAPシステムのデータで更新することです。ターゲットシステムは通常、サンドボックスシステムなどのSAPトランスポート環境の一部であり、本番システムのデータで更新されます。ソース・システムとターゲット・システムでは、ホスト名、インスタンス番号、およびSIDが異なります。



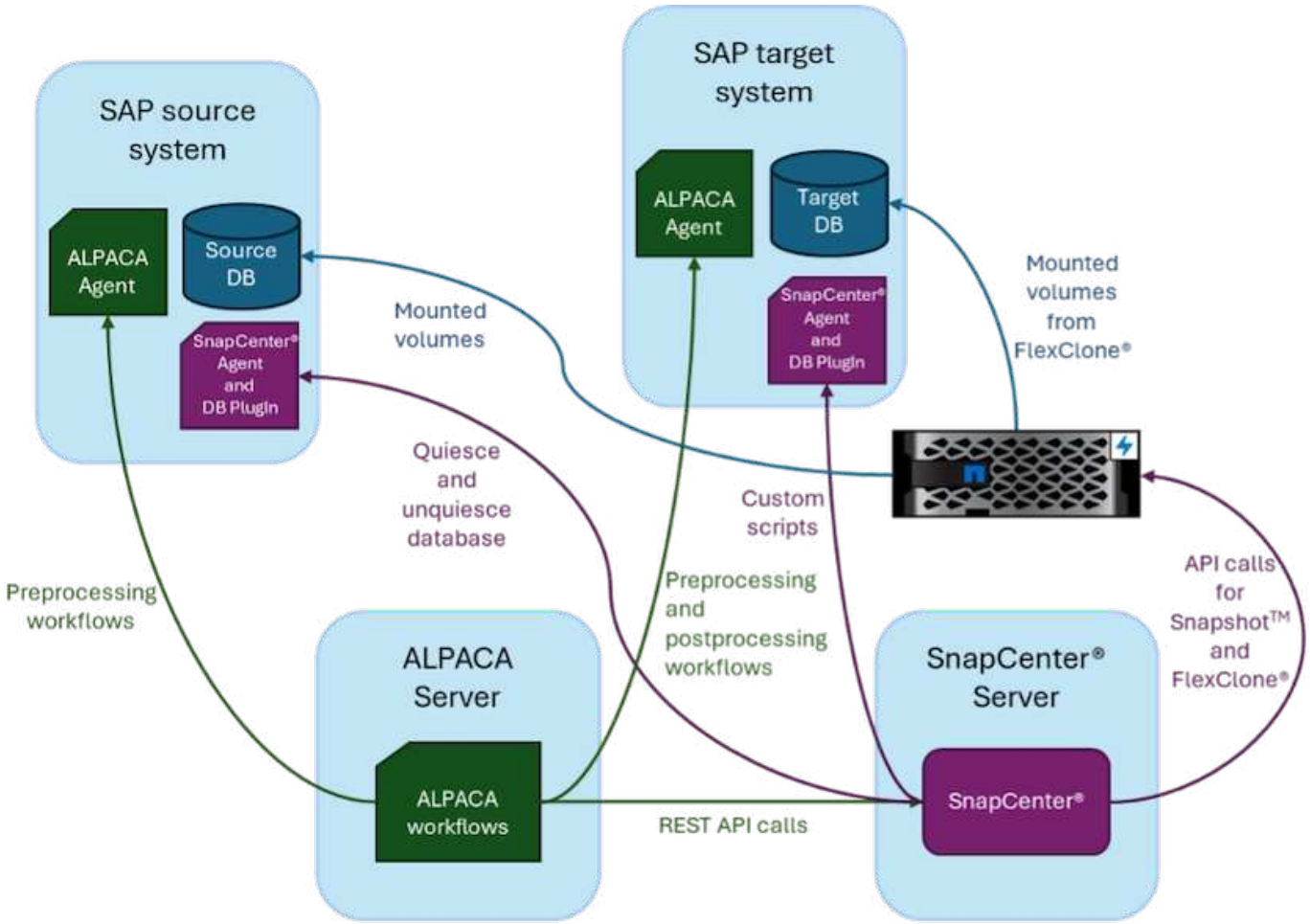

これらは3つの異なるユースケースですが、データ管理プロセスは変わりません。3つのユースケースでは、同じデータ管理テクノロジ、NetApp SnapshotとFlexCloneを使用しています。

解決策テクノロジ

ソリューション全体は、次の主要コンポーネントで構成されています。

- SnapCenterエージェントとSnapCenterデータベースプラグインがインストールされたSAPソースシステム
- SnapCenterエージェントとSnapCenterデータベースプラグインがインストールされたSAPターゲットシステム
- SAPソースシステムとSAPターゲットシステムが構成されたAlpacaシステム
- NetApp SnapCenter Server
- NetAppストレージシステム：
  - オンプレミスの物理ハードウェア：AFF-A、AFF-C、ASA-A、ASA-C、FASシリーズ
  - オンプレミスのSoftware-Defined Storage：ONTAP®Select
  - NetAppクラウドストレージ：
    - Cloud Volumes ONTAP for AWS、Google Cloud、Azure
    - Azure NetApp Files
    - NetApp ONTAP 対応の Amazon FSX

次の図は、Alpacaサーバ、NetApp SnapCenterサーバ、NetAppストレージシステム、SAPソースシステム、SAPターゲットシステムを示しており、すべてがどのように統合されているかを示しています。その目的は、SnapCenter REST APIを使用して統合を可能な限り柔軟にし、既存のコンポーネント内ですでに行われている設定作業を最大限に再利用できるようにすることです。

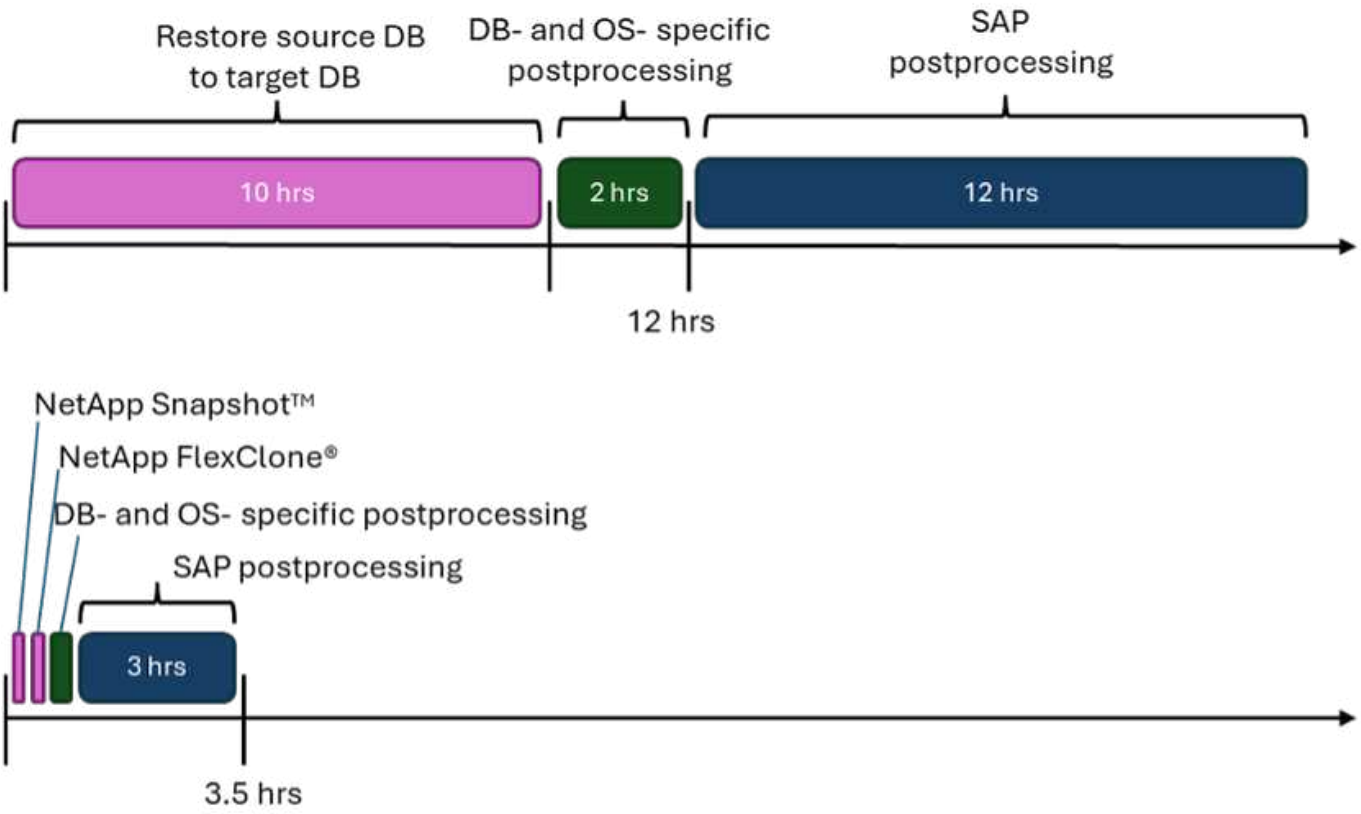


## ユースケースの概要

テストやトレーニングを目的として、ソースシステムのデータをターゲットシステムで利用できるようにする必要があるシナリオはいくつかあります。これらのテストシステムとトレーニングシステムは、ソースシステムのデータで定期的に更新して、テストとトレーニングが最新のデータセットで確実に実行されるようにする必要があります。このようなシステム更新処理は、インフラ、データベース、アプリケーションの各レイヤでの複数のタスクで構成され、自動化のレベルによっては数日かかることがあります。

運用を高速化し、タスクを自動化し、インフラ、データベース、アプリケーションレベルでの人為的ミスを排除するために、Alpaca Workflowsを使用できます。この統合では、ソースシステムからターゲットシステムにバックアップをリストアするのに時間がかかり、リソースを大量に消費しますが、その代わりにNetApp のSnapshotテクノロジとFlexCloneテクノロジを使用します。データベースのスピンアップに必要なすべてのタスクが、数時間ではなく数分で完了します。クローニングプロセスに要する時間はデータベースのサイズに左右されないため、非常に大規模なシステムでも数分で作成できます。Alpacaは、SAPの後処理側だけでなく、オペレーティングシステムやデータベースのレベルでもタスクを自動化することで、実行時間をさらに短縮します。

次の図は、自動化を使用すると運用効率が向上する可能性があることを示しています。




## テクノロジコンポーネントの統合

AlpacaワークフローへのSnapCenterの実際の統合は、シェルスクリプトを使用してNetApp SnapCenter REST APIにアクセスすることで構成されています。このREST APIベースの統合では、SAPソースシステムのSnapshotコピーが作成され、FlexCloneボリュームが作成されてSAPターゲットシステムにマウントされます。ストレージ管理者やSAP管理者は、SnapCenterによってトリガーされ、SnapCenterエージェントによって実行されるスクリプトを開発して、日常的な運用タスクを自動化する方法を知っています。シェルスクリプトを介してSnapCenterタスクをトリガーするこの疎結合アーキテクチャにより、Alpacaをエンドツーエンドの自動化のワークフローエンジンとして使用することで、既存の自動化手順を再利用して目的の結果を迅速に

達成することができます。

## まとめ

AlpacaとNetAppのデータ管理テクノロジを組み合わせることで、SAPシステム管理に関連する最も複雑で時間のかかるタスクに必要な時間と労力を大幅に削減できる強力なソリューションを提供します。また、この組み合わせは、人為的ミスがシステム間で引き起こす構成のずれを回避するのにも役立ちます。

システムの更新、コピー、クローン、ディザスタリカバリのテストは非常に機密性の高い手順であるため、このようなソリューションを実装することで貴重な管理時間を節約できます。また、基幹業務担当者がSAPシステム管理者に持つ信頼を強化することもできます。トラブルシューティングにかかる時間をどれだけ節約できるか、テストやその他の目的でシステムをコピーするのがどれだけ簡単かがわかります。これは、ソースシステムとターゲットシステムの運用場所（オンプレミス、パブリッククラウド、ハイブリッドクラウド、ハイブリッドマルチクラウド）に関係なく当てはまります。

## 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、次のドキュメントおよびWebサイトを参照してください。

- "アルパカ"
- "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"
- "SnapCenter ServerとプラグインでサポートされるREST API"

## バージョン履歴

| バージョン | 日付 | 概要を更新します |
|---|---|---|
| バージョン0.1 | 04.2024 | 第1稿。 |
| バージョン0.2 | 06.2024 | HTML形式に変換 |

# SB-4294：AvantraとNetApp SnapCenterによるSAPシステムのコピー、更新、クローニングのワークフローの自動化

このドキュメントでは、AvantraとNetApp SnapCenter®プラットフォームの統合方法について説明します。

## 解決策の概要

SAPシステムとソリューションの運用は非常に複雑です。ただし、SAPを使用している企業では、これらのシステムとサービスがビジネスプロセスの中心となります。SAPシステム管理者は、システムのコピーや更新などの日常的な運用タスクを自動化することで、より多くのシステムをより少ない労力で管理し、再現可能な結果を生み出し、人為的ミスを減らすことができます。

このドキュメントでは、NetApp®Snapshot™およびFlexClone®テクノロジをAvantra自動化ワークフローに統合する方法について説明します。Avantraは、IT運用とサービスの自動管理に重点を置いたIT管理プラットフォームです。ITインフラを監視、自動化、管理するためのソリューションを提供し、ITシステムの効率と信頼性を向上させます。Avantraを使用すると、企業はIT環境をプロアクティブに監視し、問題を早期に検出し、トラブルシューティングやシステムパフォーマンスの最適化のための自動アクションを実行できます。通常、

このプラットフォームは他のIT管理ツールと統合されており、クラウド、オンプレミス、ハイブリッドインフラなどのさまざまな環境に導入できます。

このドキュメントでは、AvantraとNetApp SnapCenter®プラットフォームの統合方法について説明します。NetApp SnapCenterは、Snapshotベースのバックアップのオーケストレーション、リストアの実行、およびFlexCloneボリュームの作成を行うためのツールです。この統合により、SAP管理者はNetAppの手法を使用して、SAPシステムの日常的な運用タスクを大幅にスピードアップできます。Snapshot、FlexClone、NetApp SnapRestore®ソフトウェアはポインタベースのNetAppストレージテクノロジであるため、バックアップ、リストア、クローニングの処理を高速化できます。このアプローチは速いです。また、オンプレミスのNetAppストレージシステムであるか、大手クラウドプロバイダ3社のいずれかにあるNetAppストレージソリューションであるかに関係なく、新規データや変更されたデータのみがストレージメディアに書き込まれるため、クローン処理時のストレージオーバーヘッドも削減されます。

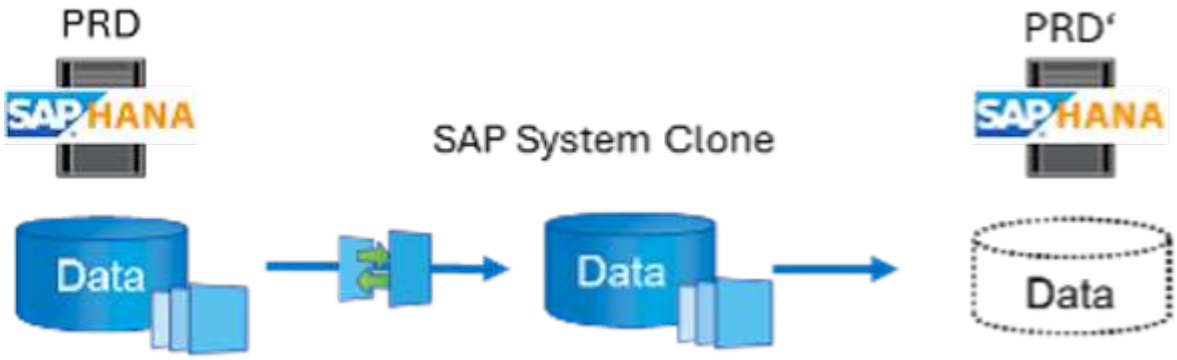
## 対象者

このドキュメントは、以前にSAPシステムのコピーを手動で実行したことがあり、Avantraを使用してこの作業を自動化したいSAPシステム管理者を対象としています。NetApp SnapCenterによってオーケストレーションされたNetApp SnapshotとFlexCloneテクノロジをAvantraのワークフローと組み合わせる目的は、SAPシステムのコピーを完全に自動化することで高速化することです。

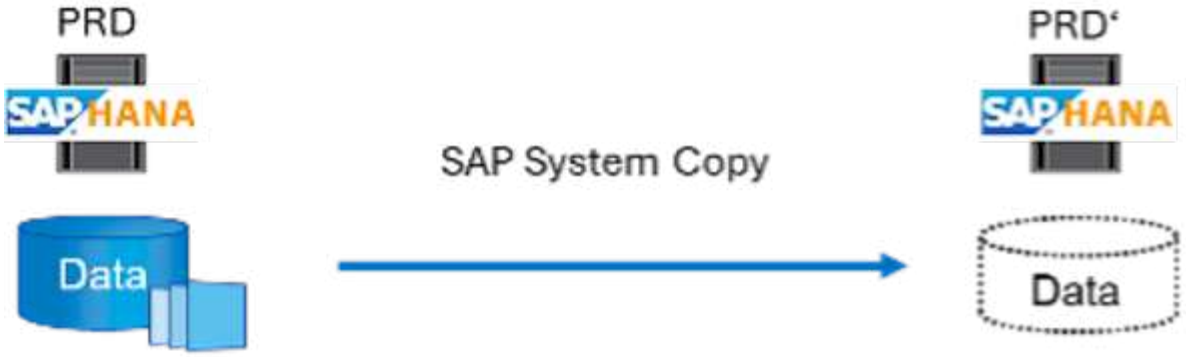
## SAPシステムのクローニング、コピー、更新のシナリオ

SAPシステムのコピーという用語は、多くの場合、SAPシステムのクローニング、SAPシステムのコピー、SAPシステムの更新の3つのプロセスを総称して使用されます。ワークフローとユースケースが異なるため、処理を区別することが重要です。

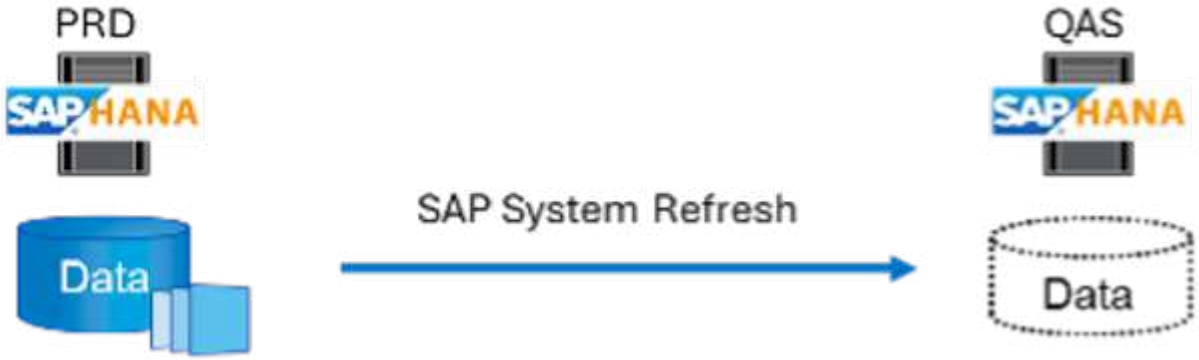
- * SAPシステムのクローン*。SAPシステムクローンは、ソースSAPシステムの同一のクローンです。SAPシステムクローンは、一般に論理的な破損に対処したり、ディザスタリカバリのシナリオをテストしたりするのに使用されます。システムのクローニング処理では、ホスト名、インスタンス番号、およびSecure Identifier（SID；セキュア識別子）は同じままです。そのため、本番環境と通信できないように、ターゲットシステムの適切なネットワークフェンシングを設定することが重要です。




- * SAPシステムのコピー*。SAPシステムのコピーは、ソースSAPシステムのデータを使用して新しいターゲットSAPシステムをセットアップすることです。たとえば、本番システムのデータを含む追加のテストシステムをターゲットシステムにすることができます。ホスト名、インスタンス番号、SIDは、ソースシステムとターゲットシステムで異なります。 新しいシステムはソースシステムから分離されていません。




- * SAPシステムの更新。*SAPシステムの更新とは、既存のターゲットSAPシステムをソースSAPシステムのデータで更新することです。ターゲットシステムは通常、サンドボックスシステムなどのSAPトランスポート環境の一部であり、本番システムのデータで更新されます。ホスト名、インスタンス番号、SIDはソースシステムとターゲットシステムで異なります。




3つのユースケースがありますが、データ管理プロセスは変わりません。3つのユースケースでは、基盤となるデータ管理テクノロジであるNetApp SnapshotとFlexCloneが活用されています。

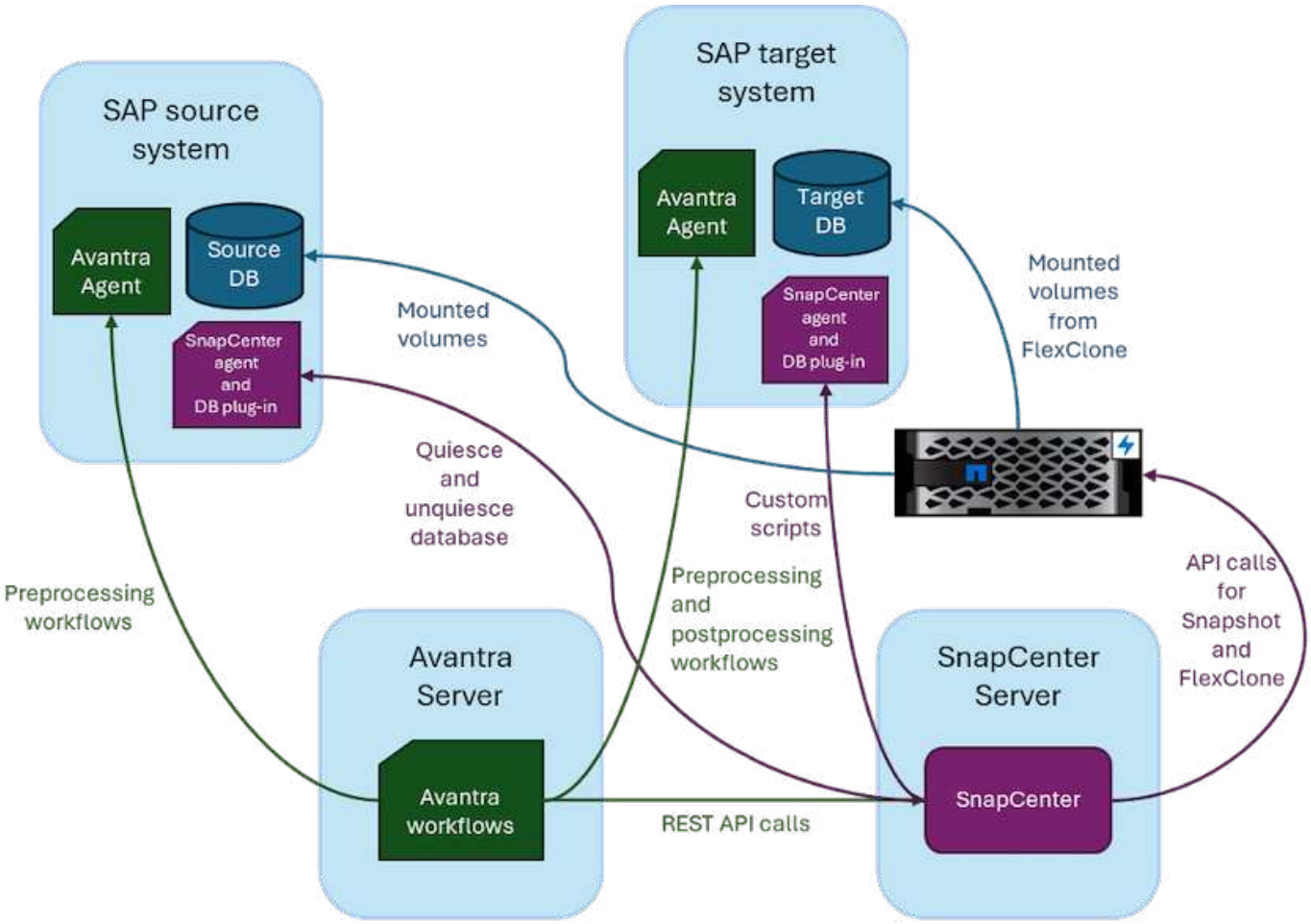
解決策テクノロジ

ソリューション全体は、次の主要コンポーネントで構成されています。

- SnapCenterエージェントとSnapCenterデータベースプラグインがインストールされたSAPソースシステム
- SnapCenterエージェントとSnapCenterデータベースプラグインがインストールされたSAPターゲットシステム
- SAPソースシステムとSAPターゲットシステムが構成されたAvantraシステム
- NetApp SnapCenter Server
- NetAppストレージシステム：
  - オンプレミスの物理ハードウェア：NetApp AFF Aシリーズ、AFF Cシリーズ、ASA Aシリーズ、ASA Cシリーズ、またはFASシリーズ
  - オンプレミスのSoftware-Defined Storage：NetApp ONTAP®Select
  - NetAppクラウドストレージ：
    - NetApp Cloud Volumes ONTAP®をAWS、Google Cloud、Azureに導入

- Azure NetApp Files
- Amazon FSx for NetApp ONTAP（AWS）

次の図は、Avantraサーバ、NetApp SnapCenterサーバ、NetAppストレージシステム、SAPソースシステムとSAPターゲットシステム、およびすべての統合方法を示しています。その目的は、既存のコンポーネント内ですでに行われている設定作業を最大限に再利用できるように、SnapCenter REST APIを使用して統合を可能な限り柔軟にすることでした。

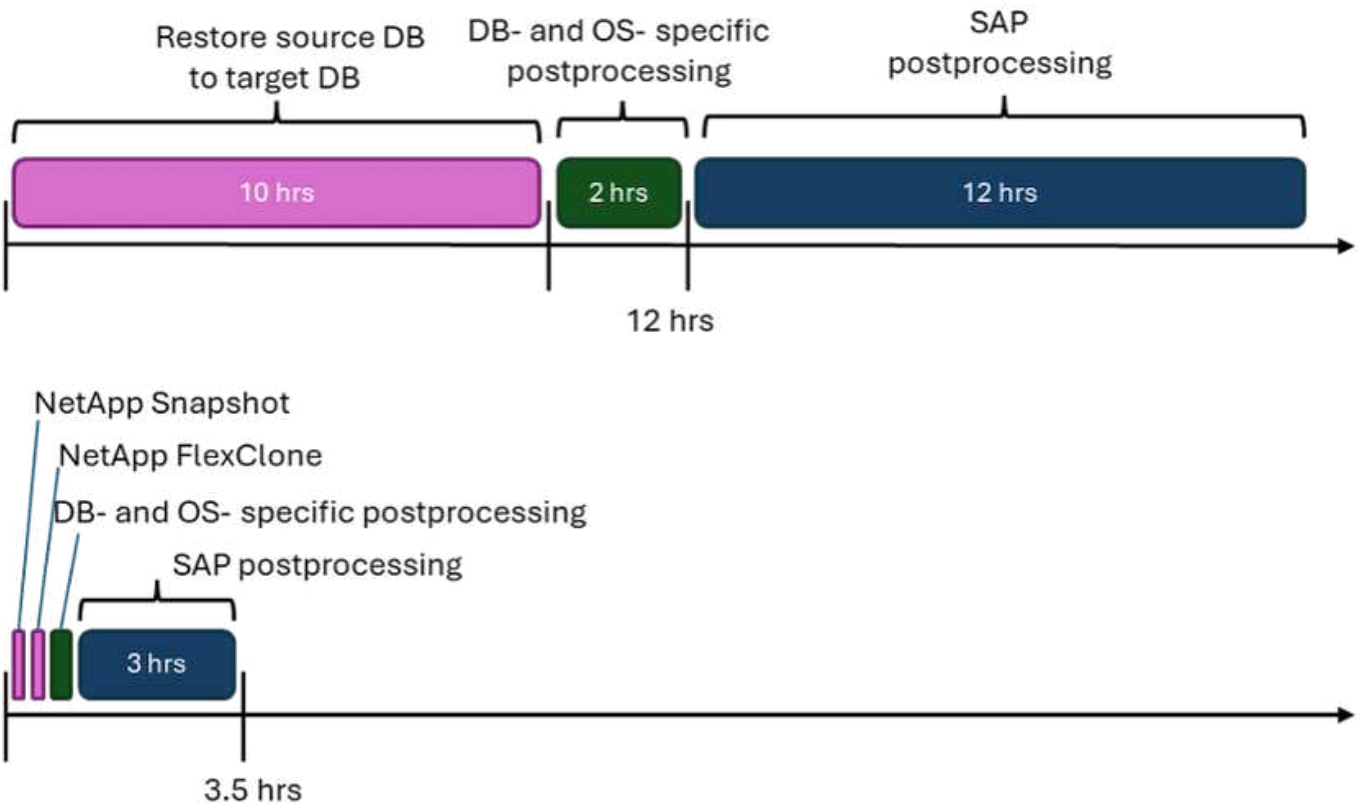



ユースケースの概要

テストやトレーニングを目的として、ソースシステムのデータをターゲットシステムで利用できるようにする必要があるシナリオはいくつかあります。これらのテストシステムとトレーニングシステムは、ソースシステムのデータで定期的に更新して、テストとトレーニングが最新のデータセットで確実に実行されるようにする必要があります。このようなシステム更新処理は、インフラ、データベース、アプリケーションの各レイヤでの複数のタスクで構成され、自動化のレベルによっては数日かかることがあります。

時間を短縮し、運用タスクを自動化し、インフラストラクチャ、データベース、アプリケーションレベルで人的エラーを排除するために、Avantraワークフローを使用できます。この統合では、ソースシステムからターゲットシステムにバックアップをリストアする（時間がかかり、リソース消費量も多い）代わりに、NetApp SnapshotとFlexCloneテクノロジを使用します。データベースのスピンアップに必要なすべてのタスクが、数時間ではなく数分で完了します。クローニングプロセスに要する時間はデータベースのサイズに左右されないため、非常に大規模なシステムでも数分で作成できます。Avantraは、SAPの後処理側だけでなく、オペレーティングシステムおよびデータベースレベルでもタスクを自動化することで、実行時間をさらに短縮します。

次の図は、自動化を使用すると運用効率が向上する可能性があることを示しています。




さまざまなテクノロジコンポーネントの統合

AvantraワークフローでのSnapCenterの実際の統合は、JavaScriptを使用してNetApp SnapCenter REST APIにアクセスすることで構成されています。このREST APIベースの統合では、SAPソースシステムのSnapshotコピーが作成され、FlexCloneボリュームが作成されてSAPターゲットシステムにマウントされます。

ストレージ管理者やSAP管理者は、SnapCenterによってトリガーされ、SnapCenterエージェントによって実行されるスクリプトを開発して、毎日繰り返される運用タスクを自動化するための時間とノウハウを投入してきました。JavaScriptを使用してSnapCenterタスクをトリガーするこの疎結合アーキテクチャを使用すると、既存の自動化手順を再利用して、エンドツーエンドの自動化のワークフローエンジンとしてAvantraを使用して、目的の結果を迅速に達成できます。

## まとめ

AvantraとNetAppのデータ管理テクノロジーを組み合わせることで、SAPシステム管理に関連する最も複雑で時間のかかるタスクに必要な時間と労力を大幅に削減できる強力なソリューションを提供します。また、この組み合わせは、人為的ミスがシステム間で引き起こす構成のずれを回避するのにも役立ちます。

システムの更新、コピー、クローン、ディザスタリカバリのテストは非常に機密性の高い手順であるため、このようなソリューションを実装することで貴重な管理時間を節約できます。また、基幹業務のスタッフがSAPシステム管理者に持つ信頼を強化することもできます。トラブルシューティングにかかる時間をどれだけ節約できるか、テストやその他の目的でシステムをコピーするのがどれだけ簡単かを確認できます。このソリューションには、ソースシステムとターゲットシステムがオンプレミス、パブリッククラウド、ハイブリッドマルチクラウド環境、ハイブリッドマルチクラウド環境のどこで運用されているかに関係なく、これらのメリットがあります。

## 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。

- "アバントラ"
- "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"
- "SnapCenter Serverとプラグインでサポートされる REST API"

## バージョン履歴

| バージョン | 日付 | 概要を更新します |
| --- | --- | --- |
| バージョン0.1 | 03.2024 | 第1稿。 |
| バージョン0.2 | 03.2024 | NetAppの同僚からのフィードバックの統合。 |
| バージョン0.3 | 04.2024 | 要求された変更を統合してNetAppブランディングに準拠 |
| バージョン0.4 | 06.2024 | HTML形式に変換 |

# 法的通知

著作権に関する声明、商標、特許などにアクセスできます。

## 著作権

"https://www.netapp.com/company/legal/copyright/"

## 商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

## 特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

## プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

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。