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

NetApp solutions for SAP

NetApp
February 25, 2026

目次

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

ONTAP、 Azure NetApp Files、FSx for ONTAP全体でSnapCenterを使用して SAP HANA システムを保護します

スナップショットベースのバックアップとデータ レプリケーションを使用して、NetApp SnapCenterで SAP HANA システムを保護します。このソリューションでは、バックアップ戦略、整合性チェック、リカバリワークフローなど、 ONTAP AFFおよびASAシステム、 Azure NetApp Files、 Amazon FSx for ONTAP上の SAP HANA システムのSnapCenter構成と運用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

SAP システム更新操作と SAP HANA システムレプリケーションに関する追加のユースケース固有の詳細は、以下を参照してください。

- "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 System Replication - Backup and Recovery with SnapCenter』"

SnapCenterデータ保護とNetApp SnapMirrorアクティブ同期を組み合わせるためのベストプラクティスについては、以下で説明します。

- "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"

プラットフォーム固有のベストプラクティスに関する追加ドキュメントは、以下から入手できます。

- "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"
- "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"
- "『SAP HANA data protection on Azure NetApp Files with SnapCenter』（ブログとビデオ）"
- "『SAP System Refresh and Cloning operations on Azure NetApp Files with SnapCenter』（ブログとビデオ）"

NetApp Snapshot テクノロジーによる SAP HANA データ保護について学ぶ

NetApp Snapshot テクノロジーが、データベースのサイズに関係なく、数分で完了するバックアップで SAP HANA データベースを保護する方法をご覧ください。スナップショット コピー、高速リカバリのためのSnapRestore 、および二次保護のためのSnapVaultまたはAzure NetApp Filesバックアップによるレプリケーションを使用したバックアップおよびリカバリ戦略について学習します。

今日の企業では、SAP アプリケーションの継続的かつ中断のない可用性が求められています。企業は一貫し

たパフォーマンス レベルを期待しており、増え続けるデータ量やシステム バックアップなどの日常的なメンテナンス タスクのニーズに対応するため、日常的な操作を自動化する必要があります。SAP データベースのバックアップを実行することは重要なタスクであり、実稼働の SAP システムのパフォーマンスに大きな影響を与える可能性があります。

バックアップするデータの量が増える一方で、バックアップウィンドウは縮小しています。そのため、業務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時間を見つけるのは困難です。ビジネスコストを削減するために、SAP 実稼働システムと非実稼働システムのダウンタイムを最小限に抑える必要があるため、SAP システムの復元と回復に必要な時間は懸念事項です。

スナップショットバックアップを使用したバックアップとリカバリ

NetApp Snapshot テクノロジーを使用すると、数分でデータベースのバックアップを作成できます。スナップショット 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 ブロックが移動されないため、スナップショット コピーの作成に必要な時間はデータベースのサイズとは無関係です。さらに、スナップショット テクノロジを使用すると、すべての操作がストレージ システムで実行されるため、ライブ SAP システムのパフォーマンスに影響はありません。したがって、ピーク時のダイアログまたはバッチ アクティビティ期間を考慮せずに、スナップショット コピーの作成をスケジュールできます。NetApp上の SAP の顧客は通常、1 日中に複数のオンライン スナップショット バックアップをスケジュールします。たとえば、6 時間ごとにスケジュールするのが一般的です。これらのスナップショット バックアップは通常、プライマリ ストレージ システムに 3 ～ 5 日間保存された後、削除されるか、長期保存のためにより安価なストレージに階層化されます。

スナップショット コピーは、復元および回復操作にも重要な利点をもたらします。復元操作では、バックアップの状態に基づいてファイル システム内のデータが復元されます。リカバリ操作は、データベース ログ バックアップを使用して、データベースの状態を特定の時点までロールフォワードするために使用されます。

NetApp SnapRestoreテクノロジーにより、現在利用可能なスナップショット バックアップに基づいて、データベース全体またはデータベースの一部のみを復元できます。復元プロセスは、データベースのサイズに関係なく、数秒で完了します。1 日中に複数のオンライン スナップショット バックアップを作成できるため、従来の 1 日 1 回のバックアップ アプローチと比較して、回復プロセスに必要な時間が大幅に短縮されます。最大 24 時間ではなく、最大数時間前のスナップショット コピーを使用して復元を実行できるため、フォワード リカバリ中に適用する必要があるトランザクション ログが少なくなります。従来のストリーミング バックアップと比較して、復元と回復に必要な時間が大幅に短縮されます。

スナップショット 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 システムに保存されるため、 NetApp、スナップショット コピー バックアップをセカンダリ ロケーションへのバックアップの代わりとしてではなく補足として使用することをお勧めします。ほとんどの復元およびリカバリ アクションは、プライマリ ストレージ システム上のSnapRestoreを使用して管理されます。セカンダリ ロケーションからの復元は、スナップショット コピーを含むプライマリ ストレージ システムが使用できない場合にのみ必要です。プライマリ ストレージで使用できなくなったバックアップを復元する必要がある場合は、セカンダリ バックアップを使用することもできます。

セカンダリ ロケーション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スナップショット コピーに基づいています。したがって、SAP データベース サーバーとそのネットワークに負荷をかけることなく、データはプライマリ ストレージ システムから直接読み取られます。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、 SnapVaultまたは ANF バックアップ機能を使用してバックアップ データを宛先に複製します。

SnapVaultと ANF バックアップは、従来のバックアップに比べて大きな利点があります。すべてのデータがソースから宛先に転送される最初のデータ転送の後、後続のすべてのバックアップでは、変更されたブロックのみがセカンダリ ストレージに複製されます。 変更されたブロックのみが保存先に保存されるため、追加の完全データベース バックアップでは消費されるディスク領域が大幅に削減されます。プライマリ ストレージ システムの負荷およびフル バックアップに要する時間は大幅に削減されます。デスティネーションには変更されたブロックだけが格納されるため、データベースのフル バックアップを追加しても、消費するディスク ス

ペースが大幅に少なくて済みます。

Snapshotバックアップおよびリストア処理の実行時間

次の図は、スナップショット バックアップ操作を使用する顧客の HANA Studio を示しています。この画像は、HANA データベース (サイズ約 4 TB) がスナップショット バックアップ テクノロジを使用して 1 分 20 秒でバックアップされ、ファイルベースのバックアップ操作では 4 時間以上かかっていることを示しています。

バックアップ ワークフロー全体の実行時間のうち最も大きな部分は、HANA データベース スナップショット操作の実行に必要な時間です。ストレージ スナップショット バックアップ自体は、HANA データベースのサイズに関係なく、数秒で完了します。

[幅=624、高さ=267]

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スナップショット バックアップの目標復旧時間 (RTO) の比較を示します。RTO は、データベースの復元、回復、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。

NetApp Snapshot バックアップでは、復元時間はデータベースのサイズに依存せず、常に数秒の範囲になります。

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。

スナップショット バックアップは、SAP HANA データベースのパフォーマンスに影響を与えないため、通常はより高い頻度でスケジュールされます。たとえば、スナップショットのバックアップが 6 時間ごとにスケジュールされている場合、次のスナップショットが作成される直前に障害が発生すると、最悪のケースでは過去 6 時間のログを適用する必要があります。毎日のファイルベースのバックアップでは、最悪の場合、過去 24 時間のログを適用する必要があります。

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。

復元と回復のサンプル計算

次の図は、毎日のファイルベースのバックアップと、異なるスケジュールのスナップショット バックアップを使用した復元およびリカバリ操作の比較を示しています。

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。

[幅=624、高さ=326]

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、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に実行可能な復元操作が、全体的な計画ダウンタイムに大きな影響を与える例です。4 TB のデータベースの例では、計画されたダウンタイムを 8 時間短縮できます。つまり、スナップショット ベースのバックアップと復元操作を使用することで、エラーの分析と修正にさらに 8 時間かけることができます。

もう 1 つのユース ケースは、異なるデータ セットまたはパラメーターを使用して複数の反復でテストを実行する必要がある一般的なテスト サイクルです。高速バックアップおよび復元操作を活用すると、テスト サイクル内で保存ポイントを簡単に作成し、テストが失敗した場合や繰り返す必要がある場合に、システムを以前の保存ポイントのいずれかにリセットできます。これにより、テストをより早く終了したり、同時により多くのテストを実行できるようになり、テスト結果が向上します。

[幅=618、高さ=279]

スナップショット バックアップが実装されると、HANA データベースのコピーを必要とする他の複数のユース ケースに対応するために使用できるようになります。利用可能なスナップショット 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。この操作の実行時間は、ボリュームのサイズに関係なく数秒です。

最も一般的な使用ケースは、実稼働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る SAP システム リフレッシュです。ONTAPまたは ANF のクローン機能を利用すると、実稼働システムの任意の Snapshot コピーからテスト システムのボリュームを数秒でプロビジョニングできます。次に、新しいボリュームをテスト システムに接続し、HANA データベースを回復する必要があります。

2 番目のユースケースは、実稼働システムの論理的な破損に対処するために使用される修復システムの作成です。この場合、実動システムの古いスナップショット バックアップを使用して修復システムが開始されます。修復システムは、破損が発生する前のデータを含む実動システムと同一のクローンです。次に、修復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せずに、したがって災害復旧セットアップの RTO と復旧ポイント目標 (RPO) に影響を与えずに災害復旧フェールオーバー テストを実行する機能です。ONTAP SnapMirrorレプリケーションまたは 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を災害復旧サイトに複製すると、実稼働スナップショット バックアップも災害復旧サイトで使用できるようになるため、

災害復旧テスト用の新しいボリュームの作成に使用できるようになります。

[幅=627、高さ=328]

SnapCenterアーキテクチャについて学ぶ

SnapCenterサーバー、プラグイン コンポーネント、サポートされているストレージ プラットフォームなど、SAP HANA データ保護のためのSnapCenterアーキテクチャについて学習します。SnapCenter は、 ONTAPシステム、 Azure NetApp Files、および FSx for ONTAP上の SAP HANA データベースの集中バックアップ、復元、およびクローン管理を提供します。

SnapCenter は、アプリケーション一貫性のあるデータ保護のための統合プラットフォームです。SnapCenter は、集中管理と監視を提供し、アプリケーション固有のバックアップ、復元、クローン操作を管理する機能をユーザーに委任します。NetApp SnapCenter は、データベース管理者とストレージ管理者がさまざまなアプリケーションとデータベースのバックアップ、復元、およびクローン作成操作を管理するために使用できる単一のツールです。SnapCenter は、NetApp ONTAPストレージ システムに加えて、 Azure NetApp Filesと FSx for ONTAPもサポートしています。SnapCenter を使用すると、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複製することもできます。

SnapCenter には、 SnapCenterサーバーとSnapCenterプラグインが含まれています。プラグインは、さまざまなアプリケーションおよびインフラストラクチャ コンポーネントで利用できます。SnapCenterサーバーは Windows または Linux のいずれかで実行できます。

[幅=601、高さ=275]

SAP HANA のSnapCenterバックアップとリカバリについて学ぶ

SnapCenter は、ストレージベースのスナップショット コピー、自動保持管理、 NetApp ONTAP、 Azure NetApp Files、FSx for NetApp ONTAPとの統合を使用して、SAP HANA データベースの包括的なバックアップおよびリカバリ機能を提供します。このソリューションは、アプリケーション整合性のあるデータベース バックアップ、非データボリュームの保護、ブロック整合性チェック、 SnapVaultまたは ANF バックアップを使用したセカンダリ ストレージへのレプリケーションをサポートします。

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スナップショットコピーを使用した非データボリュームのバックアップ（例：/hana/shared）
- データベースブロックの整合性チェック操作
  - ファイルベースのバックアップを使用する
  - SAP HANA hdbpersdiagツールを使用する

- スナップショットバックアップのセカンダリバックアップ場所へのレプリケーション
  - SnapVault/ SnapMirrorの使用
  - Azure NetApp Files ANFバックアップの使用
- 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（スナップショットおよびファイルベース）
  - HANAログバックアップ用
- 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
  - 単一テナントの復元操作

データベース データのバックアップは、SAP HANA 用のSnapCenterプラグインと組み合わせてSnapCenterによって実行されます。プラグインは、SAP HANA 内部データベース スナップショットをトリガーし、ストレージ システム上に作成されるスナップショットが、SAP HANA データベースのアプリケーション整合性のあるイメージに基づくものとなるようにします。

SnapCenter、 SnapVaultまたはSnapMirror 機能を使用して、一貫性のあるデータベース イメージをセカンダリ バックアップまたは災害復旧の場所に複製できます。通常、プライマリ ストレージとセカンダリ ストレージのバックアップには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 はセカンダリ 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、ストレージベースのスナップショット バックアップと永続レイヤーの週次整合性チェックを組み合わせることを推奨しています。ファイルベースのバックアップを実行するか、SAP hdbpersdiag ツールを実行することにより、 SnapCenter内からブロック整合性チェックを実行できます。

構成された保持ポリシーに基づいて、 SnapCenter はプライマリ ストレージのデータ ファイル バックアップ、ログ ファイル バックアップ、および SAP HANA バックアップ カタログのハウスキーピングを管理します。

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。

- バックアップ操作:
  - 内部の HANA データベース スナップショットをトリガーして、永続化レイヤーでアプリケーションの一貫性のあるイメージを取得します。
  - データボリュームのストレージベースのスナップショットバックアップを作成します
  - 内部 HANA データベース スナップショットを閉じ、バックアップ操作を確認または中止します。この手順では、バックアップを HANA バックアップ カタログに登録します。

- 保持管理:
  - 定義された保持期間に基づいてストレージスナップショットバックアップを削除します
  - ストレージ層のスナップショットを削除します
  - SAP HANAバックアップカタログのエントリを削除します
  - 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。ログバックアップはファイルシステムとSAP HANAバックアップカタログから削除されます。

[幅=601、高さ=285]

SnapVault/ SnapMirrorまたは ANF バックアップを使用してセカンダリ バックアップが設定されている場合、プライマリ ボリュームで作成されたスナップショットはセカンダリ バックアップ ストレージに複製されます。SnapCenter は、セカンダリ バックアップの可用性に応じて、HANA バックアップ カタログとログ バックアップの保持を管理します。

[幅=601、高さ=278]

SAP HANA 向けのSnapCenterでサポートされている構成について学習します。

SnapCenter は、オンプレミスおよびクラウド ストレージ プラットフォーム全体にわたる幅広い SAP HANA システム アーキテクチャと展開シナリオをサポートしています。各環境でサポートされている SAP HANA 構成、プラットフォームの組み合わせ、ストレージ プロトコル、および利用可能なバックアップと復元操作について説明します。

サポートされているSAP HANA構成

SnapCenter は、次の HANA 構成と機能をサポートしています。

- SAP HANA 単一ホストシステム
- SAP HANA 複数ホストシステム
  - 中央プラグインの導入が必要です。 "SAP HANA 向けSnapCenterプラグインの導入オプション"。
- SAP HANA MDCシステム
  - 単一または複数のテナント
- 複数のパーティションを持つSAP HANAシステム
- SAP HANA システムレプリケーション
- SAP HANA 暗号化 (データ、ログ、バックアップ)

サポートされているプラットフォームとインフラストラクチャの構成

SnapCenter は、次のホスト プラットフォーム、ファイル システム、およびストレージ プラットフォームの組み合わせをサポートします。

ホストプラットフォーム	**SAP HANA** ストレージ接続とファイルシステム	ストレージプラットフォーム
VMware	ゲスト内NFSマウント	ONTAP AFF
VMware	VMFS を使用した FC データストア + XFS を使用した VM（Linux LVM ありまたはなし）	ONTAP AFFまたはASA
KVM	ゲスト内NFSマウント	ONTAP AFF
ベアメタルサーバー	NFSマウント	ONTAP AFF
ベアメタルサーバー	FC SAN + および XFS（Linux LVM ありまたはなし）	ONTAP AFFまたはASA (*)
Azure VM	NFSマウント	Azure NetApp Files
AWS EC2	NFSマウント	ONTAP向け FSx

(*): ASAサポートはSnapCenter 6.2リリース以降で利用可能

HANA および Linux プラグインは、Intel CPU プラットフォームでのみ使用できます。IBM Power上のLinuxの場合、中央HANAプラグインの展開は、以下の説明に従ってセットアップする必要があります。 "SAP HANA 向けSnapCenterプラグインの導入オプション"。

サポートされている機能と操作

略語の説明

- VBSR: ボリューム ベースのSnapRestore + ボリューム ベースのSnapRestoreは、ボリュームをスナップショットの状態に戻します。
- SFSR: 単一ファイルSnapRestore + 単一ファイルSnapRestoreを使用して、ボリューム内の特定のファイルまたは LUN を復元できます。

参照 "自動検出されたSAP HANAデータベースのリストア処理のタイプ"

ONTAP AFFおよび**ONTAP**向け **FSx**

以下の表の列 1 (NFS マウント) のみが FSx for ONTAPに関連します。

処理	**NFS** は、**VMware** または **KVM** を使用したベアメタルまたはゲストにマウントします。	**FC SAN +** ベアメタル	**FC**データストア **VMware VMFS**
HANAデータベースのスナップショットバックアップと復元操作			
スナップショットバックアップ	はい。	はい。	はい。
改ざん防止スナップショット	はい。	はい。	はい。
フル リストア	VBSR または SFSR（選択可能）	完全なLUNのSFSR	クローン、マウント、コピー

処理	**NFS** は、**VMware** または **KVM** を使用したベアメタルまたはゲストにマウントします。	**FC SAN +** ベアメタル	**FC**データストア **VMware VMFS**
単一テナントの復元	SFSR	クローン、マウント、コピー	クローン、マウント、コピー
* HANA データベースのSnapVaultバックアップおよびリストア操作*			
SnapVault レプリケーション	はい。	はい。	はい。
改ざん防止スナップショット	はい。	はい。	はい。
フル リストア	はい。	はい。	クローン、マウント、コピー
単一テナントの復元	はい。	クローン、マウント、コピー	クローン、マウント、コピー
プライマリスナップショットまたは**SnapVault**ターゲットからの**HANA**リカバリ操作			
自動リカバリMDCシングルテナント	はい。	はい。	はい。
自動リカバリMDC複数テナント	いいえ	いいえ	いいえ
非データボリュームのバックアップと復元			
スナップショットバックアップ	はい。	はい。	はい （*）
スナップショットからの復元	VBSR または SFSR（選択可能）	完全なLUNのSFSR	VBSR（*）
SnapVault レプリケーション	はい。	はい。	はい （*）
SnapVaultターゲットからの復元	はい。	はい。	はい （*）
SAP システムリフレッシュ			
プライマリスナップショットから	はい。	はい （**）	はい （**）
SnapVaultターゲットから	はい。	はい （**）	はい （**）
HAと**DR**			
HSRはスナップショットとSnapVaultをサポート	はい。	はい。	はい。
SCによるSnapMirrorレプリケーションの更新	はい。	はい。	はい。
SnapMirrorアクティブ同期	該当なし	はい。	はい。

(*): VMware 統合なし - クラッシュ イメージのスナップショットとフルボリュームの復元

(**): SnapCenterリリース 6.2 未満に必要な回避策

ONTAP ASA

処理	**FC SAN +** ベアメタル **(*)**	**FC**データストア **VMware VMFS**
HANAデータベースのスナップショットバックアップと復元操作		
スナップショットバックアップ	はい。	はい。
改ざん防止スナップショット	いいえ	いいえ
フル リストア	完全なLUNのSFSR	クローン、マウント、コピー
単一テナントの復元	クローン、マウント、コピー	クローン、マウント、コピー
* HANA データベースのSnapVaultバックアップおよびリストア操作*		
SnapVault レプリケーション	はい。	はい。
改ざん防止スナップショット	いいえ	いいえ
フル リストア	はい。	クローン、マウント、コピー
単一テナントの復元	クローン、マウント、コピー	クローン、マウント、コピー
プライマリスナップショットまたは**SnapVault**ターゲットからの**HANA**リカバリ操作		
自動リカバリMDCシングルテナント	はい。	はい。
自動リカバリMDC複数テナント	いいえ	いいえ
非データボリュームのバックアップと復元		
スナップショットバックアップ	はい。	はい （*）
スナップショットからの復元	完全なLUNのSFSR	完全なLUNのSFSR (*)
SnapVault レプリケーション	はい。	はい （*）
SnapVaultターゲットからの復元	はい。	はい （*）
SAP システムリフレッシュ		
プライマリスナップショットから	はい。	はい （**）
SnapVaultターゲットから	はい。	はい （**）
HAと**DR**		
HSRはスナップショットとSnapVaultをサポート	はい。	はい。
SnapCenterによってトリガーされるSnapMirrorレプリケーション更新	はい。	はい。
SnapMirrorアクティブ同期	はい。	はい。

(*): SnapCenter 6.2リリース以降でサポートされます

(**): SnapCenterリリース 6.2 未満に必要な回避策

Azure NetApp Files

処理	**NFS**マウント
HANAデータベースのスナップショットバックアップと復元操作	
スナップショットバックアップ	はい。
改ざん防止スナップショット	いいえ
完全なインプレース復元	ボリュームの復元またはSFSR（選択可能）
単一テナントの復元	SFSR
HANAデータベースの**ANF**バックアップおよび復元操作	
ANFバックアップレプリケーション	はい。
改ざん防止スナップショット	いいえ
完全なインプレース復元	はい。
単一テナントの復元	はい。
プライマリスナップショットまたは**ANF**バックアップから**HANA**リカバリ操作	
自動リカバリMDCシングルテナント	はい。
自動リカバリMDC複数テナント	いいえ
非データボリュームのバックアップと復元	
スナップショットバックアップ	はい。
スナップショットからの復元	音量を戻す
ANFバックアップレプリケーション	はい。
ANFバックアップからの完全なインプレース復元	いいえ （*）
SAP システムリフレッシュ	
プライマリスナップショットから	はい。
ANFバックアップから	はい。
HAと**DR**	
HSRはスナップショットとANFバックアップをサポート	はい。
SnapCenterによってトリガーされるクロスリージョンレプリケーションの更新	いいえ

(*): 現在のバージョンでは、復元操作はAzureポータルまたはCLIを使用して実行する必要があります。

SnapCenter のデータ保護の概念とベストプラクティスについて学習します

SAP HANA 環境向けのSnapCenterの展開オプション、データ保護戦略、バックアップ保持管理について学習します。SnapCenter は、データベース ホストまたは中央ホスト

へのプラグインの展開、自動検出と手動構成、ファイルベースのバックアップまたは hdbpersdiag を使用したブロック整合性チェック、プライマリ ストレージとセカンダリ ストレージにわたる包括的な保持管理をサポートします。

SAP HANA 向けSnapCenterプラグインの導入オプション

次の図は、 SnapCenterサーバー、SAP HANA データベース、およびストレージ システム間の通信の論理ビューを示しています。SnapCenterサーバーは、HANA と Linux プラグインを活用して、HANA データベースおよび Linux オペレーティング システムと通信します。

[幅=601、高さ=199]

SnapCenterプラグインの推奨されるデフォルトの展開オプションは、HANA データベース ホストへのインストールです。この展開オプションでは、 「SnapCenterでサポートされる構成」の章で説明されているすべての構成と機能が有効になります。いくつかの例外があり、 SnapCenterプラグインを HANA データベース ホストにインストールできず、中央プラグイン ホスト (SnapCenterサーバー自体など) で構成する必要があります。HANA 複数ホスト システムまたは IBM Power プラットフォーム上で実行される HANA システムには、中央プラグイン ホストが必要です。両方の展開オプションを組み合わせることもできます。たとえば、SnapCenterサーバーを複数のホスト システムの中央プラグイン ホストとして使用し、他のすべての単一ホスト HANA システムの HANA データベース ホストにプラグインを展開するなどです。

SnapCenterでは、HANA リソースを自動検出するか、手動で構成することができます。HANA および Linux プラグインがデータベース ホストにデプロイされるとすぐに、HANA システムがデフォルトで自動検出されます。SnapCenter の自動検出では、同じホスト上の複数の HANA インストールはサポートされません。中央プラグイン ホストを使用して管理される HANA システムは、 SnapCenterで手動で構成する必要があります。また、非データ ボリュームは、デフォルトでは手動で構成されたリソースです。

	プラグインの導入場所	**SnapCenter**リソース
HANAデータベース	データベースホスト	自動検出
HANAデータベース	中央プラグインホスト	手動設定
非データ量	N/A	手動設定

SnapCenter はHANA システムの中央プラグイン展開をサポートしていますが、プラットフォームと機能のサポートには制限があります。中央プラグイン ホストで構成された HANA システムでは、次のインフラストラクチャ構成と操作はサポートされません。

- FCデータストアを備えたVMware
- SnapMirrorアクティブ同期
- 中央プラグインホストとして使用した場合のSnapCenterサーバーの高可用性
- HANAシステムの自動検出
- 自動HANAデータベースリカバリ
- 自動SAPシステムリフレッシュ
- 単一テナントの復元

SAP HANA データベース ホストに導入された HANA 用SnapCenterプラグイン

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

は、HANA hdbsql クライアント ソフトウェアを使用して、HANA データベースに対して SQL コマンドを実行します。HANA hdb ユーザーストアは、HANA データベースにアクセスするためのユーザー資格情報、ホスト名、およびポート情報を提供するために使用されます。SnapCenter Linux プラグインは、ホスト ファイル システムの操作だけでなく、ファイル システムとストレージ リソースの自動検出もカバーするために使用されます。

HANA プラグインが HANA データベース ホストにデプロイされると、HANA システムはSnapCenterによって自動検出され、 SnapCenterで自動検出されたリソースとしてフラグが付けられます。

[幅=601、高さ=304]

SnapCenter サーバの高可用性

SnapCenter は2 ノードの HA 構成でセットアップできます。このような構成では、ロード バランサ (F5 など) を使用してSnapCenterホストにアクセスします。SnapCenterリポジトリ (MySQL データベース) はSnapCenterによって 2 つのホスト間で複製されるため、 SnapCenterデータは常に同期されます。

SnapCenterサーバーに HANA プラグインがインストールされている場合、 SnapCenterサーバー HA はサポートされません。SnapCenter HAの詳細については、以下をご覧ください。 "SnapCenterサーバを高可用性向けに構成する"。

[幅=601、高さ=307]

中央プラグインホスト

前の章で述べたように、中央プラグインは

- HANA 複数ホストシステム
- IBM Powerで稼働するHANAシステム

中央プラグイン ホストを使用する場合、HANA プラグインと SAP HANA hdbsql クライアントは、HANA データベース ホストの外部のホストにインストールする必要があります。このホストは、 SnapCenterサーバーなどの任意の Windows または Linux ホストにすることができます。

SnapCenterサーバーを Windows 上で実行する場合、Windows システムを中央プラグイン ホストとして使用できます。Linux 上でSnapCenterサーバーを実行する場合は、中央プラグイン ホストとして別のホストを使用する必要があります。

HANA 複数ホスト システムの場合、すべてのワーカー ホストとスタンバイ ホストの SAP HANA ユーザー ストア キーを中央プラグイン ホストで設定する必要があります。SnapCenter は、提供された各キーを使用してデータベースに接続しようとするため、システム データベース (HANA ネーム サーバー) の別のホストへのフェイルオーバーとは独立して動作できます。

[幅=601、高さ=314]

中央プラグイン ホストによって管理される複数の単一ホスト HANA システムの場合、HANA システムの個々の SAP HANA ユーザー ストア キーはすべて、中央プラグイン ホストで設定する必要があります。

[幅=601、高さ=338]

SAP HANA ブロック整合性チェック

SAP では、全体的なバックアップ戦略に定期的な HANA ブロック整合性チェックを含めることを推奨しています。従来のファイルベースのバックアップでは、このチェックはバックアップ操作ごとに実行されます。スナップショット バックアップでは、スナップショット バックアップ操作に加えて、たとえば週に 1 回、整合性チェックを実行する必要があります。

技術的には、ブロック整合性チェックを実行するには 2 つのオプションがあります。

- 標準のファイルベースまたはbackintベースのバックアップを実行する
- HANAツールhdbpersdiagの実行については、以下も参照してください。 "永続性整合性チェック | SAP ヘルプポータル"

HANA hdbpersdiag ツールは HANA インストールの一部であり、オフライン HANA データベースに対してブロック整合性チェック操作を実行できます。したがって、既存のスナップショット バックアップを hdbpersdiag に提示できるスナップショット バックアップと組み合わせて使用するのに最適です。

2 つのアプローチを比較すると、hdbpersdiag は HANA ブロック整合性チェックのファイルベースのバックアップに比べて大きな利点があります。1 つの次元は必要なストレージ容量です。ファイルベースのバックアップでは、各 HANA システムに対して少なくとも 1 つのバックアップのサイズが利用可能である必要があります。たとえば、永続サイズが 3 TB の HANA システムが 15 台ある場合、整合性チェックのためだけにさらに 45 TB が必要になります。hdbpersdiag では、既存のスナップショット バックアップまたは既存のスナップショット バックアップのFlexCloneに対して操作が実行されるため、追加のストレージ容量は必要ありません。2 番目の次元は、整合性チェック操作中の HANA ホストの CPU 負荷です。ファイルベースのバックアップでは HANA データベース ホストで CPU サイクルが必要になりますが、中央検証ホストと組み合わせて使用すると、hdbpersdiag 処理は HANA ホストから完全にオフロードできます。以下の表に主な特徴をまとめます。

	必要なストレージ容量	**HANA**ホストの**CPU**とネットワーク負荷
ファイルベースのバックアップ	HANA システムごとに最小 1 x データ バックアップ サイズ	高
HANA ホストのスナップショット ディレクトリを使用した hdbpersdiag (NFS のみ)	なし	中
FlexCloneボリュームでhdbpersdiagを実行するために使用される中央検証ホスト	なし	なし

NetApp、HANA ブロックの整合性チェックを実行するために hdbpersdiag を使用することを推奨しています。実装の詳細については、次の章を参照してください。 "SnapCenterによるブロック整合性チェック"。

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 バックアップをセカンダリ バックアップ サイトに複製する必要がありますか?
- バックアップはセカンダリ バックアップ ストレージにどれくらいの期間保存する必要がありますか?

次の表は、システム タイプ運用、開発、テストのデータ保護パラメータの例を示しています。実稼働システムでは、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 1 日に 1 回セカンダリ バックアップ サイトに複製されます。テスト システムでは要件が低く、バックアップのレプリケーションは行われません。

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	12時間ごと
プライマリの保持	3 日	3 日	6日間
ブロック整合性チェック	週に 1 回	週に 1 回	いいえ
セカンダリ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
セカンダリバックアップの保持	2 週間	2 週間	いいえ

次の表は、上記のデータ保護パラメータに対して構成する必要があるポリシーとスケジュールを示しています。

ポリシー	バックアップタイプ	スケジュール頻度	プライマリの保持	**SnapVault** レプリケーション	二次保持
ローカルスナップ	Snapshot ベース	6 時間ごと	カウント=12	いいえ	該当なし
ローカルスナップとスナップボールト	Snapshot ベース	1 日に 1 回	カウント=2	はい。	カウント=14
SnapAndCallHdbpersdiag	Snapshot ベース	週に 1 回	カウント=2	いいえ	該当なし

ONTAPシステムまたは FSx for ONTAPの場合、 SnapCenter がSnapVault更新操作を実行する前に、 ONTAPでSnapVaultレプリケーションのデータ保護関係を設定する必要があります。セカンダリ保持は、 ONTAP保護ポリシー内で定義されます。

ANF バックアップの場合、 SnapCenterの外部で追加の構成は必要ありません。ANF バックアップのセカンダリ保持はSnapCenterによって管理されます。

この例の構成では、ブロック整合性チェック操作に hdbpersdiag が使用されます。詳細については、次の章をご覧ください。 "SnapCenterによるブロック整合性チェック"。

以下の図は、スケジュールとバックアップの保持期間をまとめたものです。SnapCenterを使用してログ バックアップの保持を管理する場合、最も古いスナップショット バックアップよりも古いログ バックアップはすべて削除されます。つまり、ログ バックアップは、利用可能なすべてのバックアップを最新の状態に回復するために必要な期間保持されます。

[幅=601、高さ=192]

暗号化ルートキーのバックアップ

HANA 永続暗号化を使用する場合は、標準のデータ バックアップに加えて、ルート キーのバックアップを作成することが重要です。データ ボリュームと HANA インストール ファイル システムが失われた場合に HANA データベースを回復するには、ルート キーのバックアップが必要です。詳細については、 "『 SAP HANA Administration Guide 』をご覧ください"。

ルート キーが変更された場合、新しいルート キーを使用して、以前に作成された古い HANA データベース バックアップを復元することはできないことに注意してください。バックアップの作成時にアクティブだったルート キーが常に必要になります。

バックアップ処理

SnapCenter は、単一または複数のテナントを持つ HANA MDC システムのスナップショット バックアップ操作をサポートします。SnapCenter は、HANA MDC システムの 2 つの異なる復元操作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復元することも、1 つのテナントだけを復元することもできます。SnapCenter がこれらの操作を実行できるようにするには、いくつかの前提条件があります。

MDC システムでは、テナント構成は必ずしも静的ではありません。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できません。単一テナントの復元操作を有効にするには、 SnapCenter は各スナップショット バックアップに含まれるテナントを認識する必要があります。さらに、スナップショット バックアップに含まれる各テナントに属するファイルとディレクトリを認識する必要があります。

したがって、バックアップ操作ごとに、 SnapCenter はテナント情報を識別します。これには、テナント名と対応するファイルおよびディレクトリ情報が含まれます。単一テナントの復元操作をサポートできるようにするには、このデータをスナップショット バックアップ メタデータに保存する必要があります。

アプリケーション自動検出のもう 1 つのステップは、HANA システム レプリケーション (HSR) のプライマリ ノードまたはセカンダリ ノードの検出です。HANA システムが HSR で構成されている場合、バックアップ SQL コマンドが HSR プライマリ ノードで実行されるように、 SnapCenter は各バックアップ操作でプライマリ ノードを識別する必要があります。参照 "『SAP HANA System Replication - Backup and Recovery with SnapCenter』"。

SnapCenter はHANA データ ボリューム構成も検出し、それをファイル システムとストレージ リソースにマッピングします。このアプローチにより、 SnapCenter はHANA ボリューム構成の変更 (複数のパーティションやボリュームの移行などのストレージ構成の変更など) を処理できます。

次のステップは、スナップショット バックアップ操作そのものです。この手順には、HANA データベース スナップショット、ストレージ スナップショット バックアップをトリガーする SQL コマンド、および HANA スナップショット操作を終了する SQL コマンドが含まれます。close コマンドを使用することで、HANA データベースはシステム 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。

[幅=601、高さ=237]

バックアップ保持管理

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のバックアップ（SnapVaultまたはANFバックアップ）
- 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 バックアップカタログとファイルシステム上のログバックアップ

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。

[幅=601、高さ=309]

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 ポリシーで定義された保持期間に従って、プライマリ ストレージ上およびSnapCenterリポジトリ内の Snapshot コピーを削除することにより、SAP HANA データベース バックアップと非データ ボリューム バックアップのハウスキーピングを処理します。保持管理は、 SnapCenter の各バックアップ ワークフローに含まれています。プライマリ ストレージのローカル バックアップも、SnapCenterで手動で削除できます。

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 ポリシーで定義された保持期間に従ってファイル システム上のバックアップを削除することにより、ファイルベースのバックアップのハウスキーピングを処理します。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。

セカンダリストレージでのバックアップの保持管理（**SnapVault**）

セカンダリ ストレージ (SnapVault) でのバックアップの保持管理は、 ONTAP保護関係で定義された保持に基づいてONTAPによって処理されます。SnapCenterリポジトリ内のセカンダリ ストレージ上のこれらの変更を同期するために、 SnapCenter 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のすべてのセカンダリ ストレージ バックアップをSnapCenterリポジトリと同期します。

クリーンアップ ジョブは、デフォルトで週に 1 回スケジュールされます。この週次スケジュールにより、セカンダリ ストレージで既に削除されているバックアップと比較すると、 SnapCenterおよび SAP HANA Studio でのバックアップの削除に遅延が生じます。この不一致を回避するために、顧客はスケジュールを 1 日 1 回など、より高い頻度に変更できます。クリーンアップジョブのスケジュールを調整する方法や手動で更新を開始する方法の詳細については、次の章を参照してください。 "セカンダリバックアップのクリーンアップ"。

セカンダリストレージでのバックアップの保持管理（**ANF**バックアップ）

ANF バックアップの保持は、 SnapCenterによって構成および処理されます。SnapCenter は、 SnapCenter バックアップ ポリシーで定義された保持期間に従ってバックアップを削除することにより、ANF バックアップのハウスキーピングを処理します。保持管理は、 SnapCenterの各バックアップ ワークフローに含まれています。

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 スナップショット、またはファイルベースを削除した場合、またはSnapCenter がセカンダリ ストレージでのバックアップの削除を識別した場合、このデータ バックアップは SAP HANA バックアップ カタログでも削除されます。プライマリ ストレージのローカル スナップショット バックアップの SAP HANA カタログ エントリを削除する前に、 SnapCenter はセカンダリ ストレージにバックアップがまだ存在す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 データベースはログ バックアップを自動的に作成します。これらの操作により、SAP HANA で設定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 リカバリには必要なくなるため、削除できます。SnapCenter は、次の手順を実行して、ファイルシステムレベルと SAP HANA バックアップカタログでのログファイルバックアップのハウスキーピングを処理します。

1. SnapCenter はSAP HANA バックアップ カタログを読み取り、最も古い成功したデータ 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。

> ポリシー構成でオンデマンド バックアップの保持期間が定義されている場合でも、ハウスキーピング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。したがって、通常、オンデマンド バックアップはSnapCenterで手動で削除して、これらのバックアップがSAP HANA バックアップ カタログでも削除され、ログ バックアップ ハウスキーピング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、「自動ログ バックアップ ハウスキーピングを非アクティブ化する」セクションで説明されているように無効にすることができます。

SAP HANA環境向けのSnapCenterの構成について学習します

共有リソース (資格情報、ストレージ システム、ポリシー) の初期構成と、個々の HANA システムのリソース固有の構成 (ホストの展開、自動検出、保護設定) の 2 段階のSnapCenterを使用して、SAP HANA 環境向けに SnapCenter を構成します。

複数の HANA システムを備えた SAP HANA 環境のSnapCenter構成は、主に次の 2 つの領域に分けられます。

- 初期設定
  - 資格情報、ストレージ、およびポリシーの構成。+ これらの設定またはリソースは通常、複数の HANA システムによって消費されます。
- HANAリソース固有の構成
  - ホスト、HANA、およびリソース保護の構成は、各 HANA システムごとに個別に実行する必要があります。

下の図は、さまざまな構成コンポーネントとそれらの依存関係を示しています。

すべての構成手順については、次のトピックで詳しく説明します。

> このドキュメントの説明とスクリーンショットは、 SnapCenterによって自動検出された HANA システムに基づいています。中央プラグインホストを使用して手動で構成されたリソースの追加または異なる構成手順については、以下で説明します。 "中央プラグインホスト構成"。

[幅=601、高さ=319]

SAP HANA 用のSnapCenter の初期設定を構成する

Azure サービス プリンシパルの資格情報を設定し、ストレージ システムを追加し、スナップショット バックアップ、ブロック整合性チェック、セカンダリ レプリケーションのポリシーを作成して、SAP HANA 環境の初期SnapCenter設定を構成します。

SnapCenter の初期構成には次の手順が含まれます。

1. クレデンシャルの設定
   a. Azure NetApp Files (ANF) で構成された HANA システムの場合、サービス プリンシパルを準備し、SnapCenterで構成する必要があります。
   b. HANA データベース ホストに HANA プラグインを自動的にインストールできるようにするには、ホスト資格情報を提供する必要があります。
2. ストレージシステムの構成：
   a. ANF で構成された HANA システムの場合、必要なNetAppアカウントを選択してSnapCenter構成に追加できます。
   b. ONTAPまたは FSx for ONTAPストレージ システムの場合、SVM または完全なストレージ クラスターのいずれかをSnapCenterに追加できます。

3. ポリシー設定
    a. スナップショット ベースのバックアップおよびブロック整合性チェック操作のポリシーは、ANF だけでなく、 ONTAPおよび FSx for ONTAPストレージ システムに対しても設定できます。
    b. SnapVaultまたはSnapMirrorを使用した改ざん防止スナップショットおよびセカンダリ バックアップのポリシーは、 ONTAPおよび FSx for ONTAPストレージ システムに対してのみ設定できます。
    c. ANFで構成されたHANAシステムの場合、ポリシーには以下を含めることができます。 "ANFバックアップ"。

> ⓘ 同じスナップショット バックアップ ポリシーを、HANA データベースだけでなく、HANA 共有ボリュームなどの非データ ボリュームにも使用できます。

以下の図は構成セクションをまとめたものです。

[幅=601、高さ=158]

次の章では、初期設定手順について説明します。

クレデンシャルの設定

HANAプラグインのデプロイメントの資格情報

資格情報は、[設定] セクションで [資格情報] タブを選択して構成されます。+ アイコンをクリックすると資格情報を追加できます。

[幅=601、高さ=118]

NetAppは、すべてのHANAデータベースホスト（例：scuser）にユーザーを設定し、sudo権限を設定することを推奨しています。 "ホストを追加してSnapCenter Plug-in for SAP HANA Databaseをインストールするための前提条件"。

[幅=287、高さ=247]

Azure NetApp Filesの資格情報

Azure サービス プリンシパルを準備する必要があります。これにより、 SnapCenter はANF ボリュームに対して必要な操作を実行できるようになります。以下の例は、含める必要のある最小限の権限を示しています。

```
    "assignableScopes": [
        "/subscriptions/xxx"
    ],
    "createdBy": "xxx",
    "createdOn": "2025-05-07T07:12:14.451483+00:00",
    "description": "Restricted Access for SnapCenter ",
    "id":
"/subscriptions/xxx/providers/Microsoft.Authorization/roleDefinitions/xxx"
,
    "name": "xxx",
    "permissions": [
```

```
        {
            "actions": [
            "Microsoft.NetApp/register/action",
            "Microsoft.NetApp/unregister/action",
            "Microsoft.NetApp/netAppAccounts/read",
            "Microsoft.NetApp/netAppAccounts/getKeyVaultStatus/action",
            "Microsoft.NetApp/netAppAccounts/migrateEncryption/action",
            "Microsoft.NetApp/netAppAccounts/transitionToCmk/action",
            "Microsoft.NetApp/netAppAccounts/capacityPools/read",
            "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
            "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/revert/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/poolChange/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/finalizeRelocation/
action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/revertRelocation/ac
tion",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/breakFileLocks/acti
on",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/getGroupIdListForLd
apUser/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/backups/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/backups/restoreFile
s/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/delete",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/restoreFi
les/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/read",
```

```
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/getMetad
ata/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/volumeQuotaRules/re
ad",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/latestRestoreStatus
/current/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/mountTargets/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/restoreStatus/read"
,
            "Microsoft.NetApp/netAppAccounts/snapshotPolicies/read",
            "Microsoft.NetApp/netAppAccounts/snapshotPolicies/write",

"Microsoft.NetApp/netAppAccounts/snapshotPolicies/listVolumes/read",

"Microsoft.NetApp/netAppAccounts/snapshotPolicies/volumes/read",
            "Microsoft.NetApp/netAppAccounts/volumeGroups/read",
            "Microsoft.NetApp/netAppAccounts/volumeGroups/write",
            "Microsoft.NetApp/locations/checknameavailability/action",
            "Microsoft.NetApp/locations/checkfilepathavailability/action",
            "Microsoft.NetApp/locations/operationresults/read",
            "Microsoft.NetApp/Operations/read",
            "Microsoft.Resources/resources/read",
            "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
            "Microsoft.Network/virtualNetworks/read",
            "Microsoft.Network/virtualNetworks/subnets/read",
            "Microsoft.Network/virtualNetworks/write",
            "Microsoft.Network/virtualNetworks/subnets/write",
            "Microsoft.NetApp/netAppAccounts/backupVaults/read",
            "Microsoft.NetApp/netAppAccounts/backupVaults/write",
            "Microsoft.NetApp/netAppAccounts/backupVaults/backups/read",
            "Microsoft.NetApp/netAppAccounts/backupVaults/backups/write",
            "Microsoft.NetApp/netAppAccounts/backupVaults/backups/delete",

"Microsoft.NetApp/netAppAccounts/backupVaults/backups/restoreFiles/action"
            ],
            "condition": null,
            "conditionVersion": null,
            "dataActions": [],
```

```
            "notActions": [],
            "notDataActions": []
        }
    ],
    "roleName": "SnapCenter-Restricted-Access",
    "roleType": "CustomRole",
    "type": "Microsoft.Authorization/roleDefinitions",
    "updatedBy": "xxx",
    "updatedOn": "2025-05-07T07:12:14.451483+00:00"
}
```

資格情報は、[設定] セクションで [資格情報] タブを選択して構成されます。資格情報は、+ アイコンをクリックして設定されます。

[幅=601、高さ=116]

次の画面で、資格情報の名前を指定し、認証モードとして Azure 資格情報を選択する必要があります。次に、テナント ID、クライアント ID、およびクライアント シークレット キーを構成する必要があります。

[幅=252、高さ=246]

ストレージシステムの構成：

ONTAPシステムと**ONTAP**用 **FSx**

ONTAPシステムまたは FSx for ONTAPは、クラスタの資格情報または必要な各 SVM の資格情報を提供することでSnapCenterに追加できます。クラスターの資格情報が提供されると、クラスターのすべての SVM がSnapCenterに追加されます。

ラボのセットアップでは、ストレージ クラスターをSnapCenterに追加しました。ONTAPクラスタは、ストレージ システム セクションでONTAPストレージ タブとONTAPクラスタ タイプを選択して構成されます。+ アイコンをクリックすると、新しいクラスターが追加されます。

[幅=601、高さ=117]

次の画面で、クラスター ユーザーの資格情報を入力する必要があります。

> クラスター ユーザー admin は使用しないでください。代わりに、必要な権限を持つ新しいユーザーを作成する必要があります。 "最小権限でのONTAPクラスタ ロールの作成"ASAシステムに必要な権限については、 "ASA r2システム用のONTAPクラスタロールを作成する"。

[幅=299、高さ=176]

SVM は、 ONTAPストレージ タブとONTAP SVMS タイプを選択して、ストレージ システム セクションで構成されます。+ アイコンをクリックすると、新しい SVM が追加されます。

次の画面で、クラスター ユーザーの資格情報を入力する必要があります。

SVM ユーザー vsadmin は使用しないでください。代わりに、必要な権限を持つ新しいユーザーを作成する必要があります。 "最小権限でのSVMロールの作成"ASAシステムに必要な権限については、 "ASA r2 システムの SVM ロールを作成する"。

SVM の DNS 名は、 ONTAPシステムで設定されている SVM 名と一致する必要があります。

[幅=331、高さ=199]

Azure NetApp Files

ANF 資格情報が構成されたら、ANF NetAppアカウントをSnapCenterに追加できます。NetAppアカウントは、ストレージ システム セクションで、 Azure NetApp Filesタブを選択して構成されます。+ アイコンをクリックすると、新しいNetAppアカウントが追加されます。

[幅=601、高さ=117]

ANF 資格情報とサブスクリプションを選択すると、 NetAppアカウントをSnapCenterに追加できます。

[幅=401、高さ=176]

SnapMirrorアクティブ同期を使用する場合のストレージ構成

具体的なストレージ構成手順については、以下を参照してください。 "SnapMirrorアクティブ同期を使用したストレージ構成"。

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、リソースとは独立して構成され、複数の SAP HANA システムに使用できます。

一般的な最小構成は、次のポリシーで構成されます。

- レプリケーションなしの1時間ごとのバックアップのポリシー
- SnapVaultまたは ANF バックアップ レプリケーションを使用した毎日のバックアップのポリシー
- 週次ブロック整合性チェック操作のポリシー
  - ファイルベースのバックアップを使用する
  - HANAツールhdbpersdiagを使用する

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。

ポリシーは、[設定] セクションで [ポリシー] タブを選択して構成します。+ アイコンをクリックすると、新しいポリシーが設定されます。以下の 2 つのスクリーンショットは、 Azure NetApp Filesで実行されている HANA システムのポリシーのリストと、 ONTAPストレージ システムまたは FSx for ONTAPで実行されている HANA システムのポリシーのリストを示しています。

[幅=601、高さ=133]

[幅=601、高さ=138]

ONTAPシステムと **FSx for ONTAP**によるスナップショット バックアップ

ONTAPシステムまたは FSx for ONTAPのスナップショット バックアップ ポリシーでは、ローカル スナップショットをレプリケーションまたはスナップショット ロック (改ざん防止スナップショット) 操作と組み合わせることができます。この例では、 SnapVaultを使用してセカンダリ ストレージにレプリケーションするポリシーを示します。

ポリシー名とオプションの説明を入力します。

[幅=376、高さ=103]

ONTAPストレージ タイプとスナップショット ポリシー スコープを選択します。

[幅=385、高さ=97]

このポリシーでは、日次スケジュール タイプが設定されています。毎日スナップショットが作成され、スナップショットのデルタはSnapVaultを使用してセカンダリ ストレージに複製されます。

スケジュール自体は、個々の HANA リソース保護構成を使用して構成されます。

ポリシーで設定されている保持期間は、プライマリ スナップショットに対してのみ有効です。SnapVaultターゲットでの保持は、第3章で説明されているように、HANAデータベースの個々のボリュームに対するONTAPレプリケーション関係を使用して設定されます。 "SAP HANA スナップショットバックアップ操作"。ポリシーで設定されているスナップショット ラベルは、 ONTAPレプリケーション関係で設定されているラベルと一致する必要があります。

スナップショット ロック (改ざん防止スナップショット) は、チェック ボックスをクリックしてロック期間を定義することで有効にできます。この機能を使用するには、ストレージ システムにSnapLockライセンスが必要であり、コンプライアンス クロックが設定されている必要があります。

ローカル スナップショットのみのポリシーは、1 時間ごとのスケジュールと[SnapVault の更新] チェック ボックスを無効にすることによって構成されます。

[幅=378、高さ=352]

概要画面には設定されたパラメータが表示されます。

[幅=385、高さ=119]

Azure NetApp Filesによるスナップショット バックアップ

Azure NetApp Filesのスナップショット バックアップ ポリシーでは、ローカル スナップショットと ANF バックアップを組み合わせて、スナップショット データを Azure BLOB に複製することができます。この例では、ANF バックアップを使用したレプリケーションに使用されるポリシーを示します。

ポリシー名とオプションの説明を入力します。

[幅=356、高さ=95]

Azure NetApp Filesストレージの種類とスナップショット ポリシーのスコープを選択します。

[幅=360、高さ=102]

このポリシーでは、日次スケジュール タイプが設定されています。毎日スナップショットが作成され、スナップショットのデルタは ANF バックアップを使用してバックアップ ボールトに複製されます。

スケジュール自体は、個々の HANA リソース保護構成を使用して構成されます。

ポリシーで設定されているスナップショットの保持は、ANF ボリュームのプライマリ スナップショットに対して有効です。ANF バックアップの保持は、バックアップ保持設定で構成されます。

ローカル スナップショットのみのポリシーは、1 時間ごとのスケジュールと [バックアップの有効化] チェック ボックスを無効にすることによって構成されます。

[幅=373、高さ=361]

概要画面には設定されたパラメータが表示されます。

[幅=376、高さ=138]

すべてのプラットフォームの整合性チェック操作をブロックする

HANA ツール **hdbpersdiag**

詳細は第 "SnapCenterによるブロック整合性チェック"。

ファイルベースのバックアップ

ポリシー名とオプションの説明を入力します。

[幅=346、高さ=95]

セットアップに応じてONTAPまたはAzure NetApp Filesストレージ タイプを選択し、ファイルベースのポリシー スコープを選択します。

[幅=357、高さ=98]

前述したように、ブロック整合性チェックを週に 1 回実行することをお勧めします。したがって、週単位のスケジュールが選択されます。

スケジュール自体は、個々の HANA リソース保護構成を使用して構成されます。

ファイルベースのバックアップが書き込まれるファイル システムには、保持設定で定義されているよりも 1 つのバックアップ分以上の十分な容量が必要です。これは、 SnapCenter が新しいバックアップを作成した後に古いバックアップを削除するためです。この例では、保持期間が 1 つで、バックアップ 2 つ分のスペースが必要です。構成可能な最小保持期間はゼロです。

[幅=351、高さ=173]

概要画面には設定されたパラメータが表示されます。

[幅=366、高さ=101]

SnapMirror Active Sync を使用する場合のポリシー設定

具体的なポリシー設定手順については、ドキュメントに記載されています。 "ポリシー構成SnapMirrorアクティブ同期"。

個々のSAP HANAデータベースのSnapCenterリソースを構成する

バックアップ ユーザーとユーザー ストア キーを作成し、セカンダリ バックアップのストレージ レプリケーションを設定し、自動検出用の HANA プラグインを展開し、ポリシーとスケジュールを使用してリソース保護を構成することで、 SnapCenterで個々の SAP HANA データベースを構成します。

SnapCenterでの HANA データベースの構成は、次の手順で行います。

1. SnapCenterバックアップユーザーはHANAシステムデータベースに設定され、SAP HANAユーザーストアキーはHANAデータベースホストに設定されている必要があります。
2. セカンダリストレージへのデータレプリケーションが必要な場合は、HANAデータボリュームのONTAPストレージレプリケーションを構成する必要があります。
3. SnapCenter HANAプラグインは、HANAデータベースホストに導入する必要があります。
   a. 自動検出プロセスが開始されます
   b. SAP HANAユーザーストアキーはSnapCenterで設定する必要があります
   c. 自動検出の第2フェーズが開始され、 SnapCenterによってHANAリソースが自動的に追加されます。
4. 新しく追加されたHANAリソースに対してHANAリソース保護を構成する必要があります

前のトピックで説明したSnapCenterの初期構成 "SnapCenter の初期設定" HANA データベース リソースの構成には資格情報、ストレージ システム、およびポリシーが必要になるため、最初に実行する必要があります。以下の図は、手順と依存関係をまとめたものです。

下の図は、さまざまな構成コンポーネントと依存関係を視覚化したものです。

[幅=601、高さ=315] 次のセクションでは、必要な構成手順について詳しく説明します。

SAP HANA バックアップユーザーと SAP HANA ユーザーストアの構成

NetApp、 SnapCenterを使用してバックアップ操作を実行するために、HANA データベースに専用のユーザーを構成することを推奨しています。2 番目のステップとして、このバックアップ ユーザーに対して SAP HANA ユーザー ストア キーが設定され、 SnapCenter設定で SAP HANA ユーザー ストア キーが提供されます。

次の図は、バックアップ ユーザー (この例では SNAPCENTER) を作成できる SAP HANA Studio を示しています。

バックアップ ユーザーには、バックアップ管理者、カタログ読み取り、データベース バックアップ管理者、およびデータベース回復オペレーターの権限を設定する必要があります。

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 コマンドはシステム データベース経由で実行されるため、バックアップ ユーザーはシステム データベースに作成する必要があります。

[幅=601、高さ=382]

HANA データベース ホスト上の **SAP HANA** ユーザー ストア構成

SnapCenter は、<sid>adm ユーザーを使用して HANA データベースと通信します。したがって、SAP HANA ユーザー ストア キーは、データベース ホスト上の <sid>adm ユーザーを使用して構成する必要があります。

hdbuserstore set <キー名> <ホスト>:<ポート> <データベースユーザー> <パスワード>

SAP HANA MDC システムの場合、HANA システム データベースのポートは 3<instanceNo>13 です。

SAP HANA ユーザーストアの構成例

出力には、インスタンス番号 = 00 の HANA システム用に構成されたキー SS1KEY が表示されます。

```
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 SS1SAPDBCTRL
ENV : hana-1:30013
USER: SAPDBCTRL
KEY SS1KEY
ENV : hana-1:30013
USER: SNAPCENTER
KEY SYSTEMKEY
ENV : hana-1:30013
USER: SYSTEM
ACTIVE RECORDS : 10
DELETED RECORDS : 15
NUMBER OF COMPLETE KEY: 3
Operation succeed.
ss1adm@hana-1:/usr/sap/SS1/HDB00>
```

出力には、インスタンス番号 = 12 の HANA システム用に構成されたキー SM1KEY が表示されます。

```
sm1adm@hana-2:/usr/sap/SM1/HDB12> hdbuserstore list
DATA FILE : /usr/sap/SM1/home/.hdb/hana-2/SSFS_HDB.DAT
KEY FILE : /usr/sap/SM1/home/.hdb/hana-2/SSFS_HDB.KEY
KEY SM1SAPDBCTRL
ENV : hana-2:31213
USER: SAPDBCTRL
KEY SM1KEY
ENV : hana-2:31213
USER: SNAPCENTER
ACTIVE RECORDS : 7
DELETED RECORDS : 9
NUMBER OF COMPLETE KEY: 2
Operation succeed.
sm1adm@hana-2:/usr/sap/SM1/HDB12>
```

ストレージレプリケーション構成

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。

次のスクリーンショットは、 ONTAPシステム マネージャを使用した構成を示しています。FSx for ONTAPシステムの場合、レプリケーションはONTAP CLIを使用して実行する必要があります。 "概要- SnapVault によるバックアップレプリケーション"。

次の図は、SAP HANA システム SS1 のデータボリュームに対して構成された保護関係を示しています。この例では、SVM hana-primary のソース ボリューム SS1_data_mnt00001 が、SVM hana-backup とターゲットボリューム SS1_data_mnt00001_dst に複製されます。

[幅=601、高さ=183]

次の図は、このラボ セットアップ用に作成された保護ポリシーを示しています。保護関係に使用される保護ポリシーは、 SnapMirrorラベルと、セカンダリ ストレージでのバックアップの保持を定義します。この例では、使用されているラベルは Daily で、保持期間は 5 に設定されています。

ⓘ レプリケーション ポリシーのSnapMirrorラベルは、 SnapCenterポリシー構成で定義されたラベルと一致する必要があります。

ⓘ SnapCenter は、以前に作成されたアプリケーション整合性スナップショットに基づいて、バックアップ操作の一部としてSnapVault の更新をトリガーするため、関係のスケジュールは [なし] に設定する必要があります。

ⓘ セカンダリ 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で定義され、 ONTAP によって制御されます。

[幅=601、高さ=180]

ANFバックアップ構成

ANF バックアップには特別な準備は必要ありません。ANF バックアップが有効になっている最初のバックアップが実行されるとすぐに、 SnapCenterによって snapcenter-vault という名前の Azure バックアップ ボールトが作成されます。このバックアップ ボールトは、 SnapCenterによって実行される後続のすべての ANF バックアップ操作で使用されます。

[幅=601、高さ=227]

SAP HANA向けSnapCenterプラグインの導入

ホストの要件は次の通りです。 "SnapCenter Plug-ins Package for Linuxをインストールするホストの要件"。

HANA プラグインの展開は、 SnapCenter UI の [ホスト] セクションにある [追加] ボタンをクリックすることで実行されます。

[幅=601、高さ=145]

「ホストの追加」画面で、デプロイ プロセスに使用するホストの種類と名前、および資格情報を入力する必要があります。さらに、SAP HANA プラグインを選択する必要があります。[送信] をクリックすると、デプロイメント プロセスが開始されます。

この説明では、新しいホストを追加せず、 SnapCenter内の既存のホストの構成を示します。

[幅=601、高さ=154]

HANA自動検出

HANA プラグインの展開が完了すると、自動検出プロセスが開始されます。最初のフェーズでは、基本設定のみが検出され、 SnapCenter新しいリソースが作成され、UI のリソース セクションに赤い南京錠でマークされてリストされます。

[幅=601、高さ=169]

リソースをクリックすると、この HANA データベースの SAP HANA ユーザー ストア キーの入力を求められます。

[幅=316、高さ=180]

キーが提供された後、自動検出プロセスの第 2 フェーズが開始されます。自動検出プロセスでは、HANA システム内のすべてのテナント データベース、ログおよびカタログのバックアップ構成の詳細、および HANA システム レプリケーション ロールが検出されます。さらに、ストレージ フットプリントの詳細が自動的に検出されます。これらの設定は、リソースを選択して「詳細」ボタンをクリックすることで確認できます。

この自動検出プロセスはバックアップ操作ごとに実行されるため、バックアップ操作に関連する HANA システムに加えられた変更が自動的に検出されます。

[幅=601、高さ=219]

リソース保護の設定

自動検出プロセスが完了した後、リソースをクリックすると、リソース保護構成画面が開きます。このドキュメントのスクリーンショットは、既存のリソースの保護構成を示しています。

スナップショットのカスタム名形式を構成します。NetApp、どのバックアップがどのポリシーとスケジュール タイプで作成されたかを簡単に識別できるように、カスタム スナップショット名を使用することを推奨しています。

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。

- スケジュールされた1時間ごとのバックアップ: + SnapCenter_<ホスト名>_LocalSnap_Hourly_<タイムスタンプ>
- スケジュールされた毎日のバックアップ: + SnapCenter_<ホスト名>_LocalSnapAndSnapVault_Daily_<タイムスタンプ>

[幅=601、高さ=294]

次の画面では、バックアップ ワークフローのさまざまなステップで実行されるスクリプトを設定できます。

[幅=601、高さ=294]

これで、ポリシーがリソースに添付され、スケジュールが定義されます。

この例では、

- 毎週日曜日にブロック整合性チェックを実施
- 4時間ごとのローカルスナップショットバックアップ
- 毎日1回のSnapVaultレプリケーションによるスナップショットバックアップ

[幅=601、高さ=294]

電子メール通知を設定できます。

[幅=601、高さ=294]

リソース保護の構成が完了すると、定義された設定に従ってスケジュールされたバックアップが実行されます。

SnapCenterを設定して非データボリュームをバックアップする

実行可能ファイル、構成ファイル、トレース ファイル、アプリケーション サーバー データなどの非データ ボリュームをバックアップするようにSnapCenterを構成します。

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。

他の非データ ファイルを復元する必要がある状況から回復するために、 NetApp、 SAP HANA データベース バックアップを補強する非データ ボリューム用の追加バックアップ戦略を開発することを推奨しています。特定の要件に応じて、非データ ボリュームのバックアップはスケジュール頻度と保持設定が異なる場合があ

り、非データ ファイルが変更される頻度を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、構成ファイルだけでなく、SAP HANA トレース ファイルも含まれています。実行可能ファイルは SAP HANA データベースがアップグレードされたときにのみ変更されますが、SAP HANA 構成ファイルとトレース ファイルはより高いバックアップ頻度が必要になる場合があります。また、SAP アプリケーション サーバー ボリュームは、非データ ボリューム バックアップを使用してSnapCenterで保護できます。

SnapCenter の非データ ボリューム バックアップを使用すると、SAP HANA データベース バックアップと同じスペース効率で、関連するすべてのボリュームのスナップショット コピーを数秒で作成できます。違いは、SAP HANA データベースとのやり取りが不要であることです。

[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。

[幅=601、高さ=173]

[幅=601、高さ=112]

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。

[幅=332、高さ=310]

ONTAPシステムおよび FSx for ONTAPの場合は、ストレージ タイプONTAPを選択し、SVM とストレージ ボリュームをストレージ フットプリントとして追加して、[次へ] をクリックします。

[幅=332、高さ=312]

ANF の場合は、ストレージの種類としてAzure NetApp Files を選択し、 NetAppアカウントと容量プールを選択し、ANF ボリュームをストレージ フットプリントとして追加して、[次へ] をクリックします。

[幅=350、高さ=337]

概要ステップで、完了をクリックして設定を保存します。

必要なすべての非データ ボリュームに対してこれらの手順を繰り返します。新しいリソースの保護構成を続行します。

非データ ボリューム リソースのデータ保護構成は、SAP HANA データベース リソースのワークフローと同一であり、個々のリソース レベルで定義できます。

SAP HANA 用のSnapCenterセントラル プラグイン ホストを構成する

SAP HANA マルチホスト システムまたは IBM Power 上の HANA システムをサポートするには、 SnapCenter HANA プラグインを中央ホストに導入します。この手順には、Windows または Linux ホストへのプラグインのインストール、SAP HANA hdbsql クライアントの構成、保護された各 HANA システムのユーザー ストア キーの設定が含まれます。

議論したように "SAP HANA 向けSnapCenterプラグインの導入オプション"HANA プラグインは、HANA データベースの外部に導入して、SAP HANA の複数のホスト システムまたは IBM Power 環境上の SAP HANA に必要な中央プラグイン構成をサポートできます。

中央プラグイン ホストは任意の Windows ホストまたは Linux ホストにすることができますが、通常はSnapCenterサーバー自体が中央プラグイン ホストとして使用されます。

中央プラグイン ホストの構成は、次の手順で構成されます。

- SnapCenter HANAプラグインの導入
- SAP HANA hdbsql クライアントのインストールと構成
- 中央プラグインホストによって保護されている各 HANA システムの SAP HANA ユーザーストア構成

SnapCenter HANAプラグインの導入

ホストの要件は次の通りです。 "SnapCenter Plug-ins Package for Linuxをインストールするホストの要件"。

中央プラグイン ホストがホストとして追加され、SAP HANA プラグインがホストにインストールされます。以下のスクリーンショットは、Windows 上で実行されているSnapCenterサーバーへのプラグインの展開を示しています。

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。

[幅=601、高さ=166]

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。ソフトウェアは以下からダウンロードできます。 "SAP サポートポータル"。

HANA リソース構成中に構成された hdbsql OS ユーザーは、hdbsql 実行可能ファイルを実行できる必要があります。hdbsql 実行可能ファイルへのパスは、hana.properties ファイルまたは OS ユーザーの検索パス パラメーター (%PATH%、$PATH) で設定する必要があります。

Windows 上の中央プラグイン ホスト:

```
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 上の中央プラグインホスト:

```
cat /opt/NetApp/snapcenter/scc/etc/hana.properties

HANA_HDBSQL_CMD=/usr/sap/hdbclient/hdbsql
```

中央プラグインホストのSAP HANAユーザーストア構成

中央プラグイン ホストによって管理される HANA システムごとに、SAP HANA ユーザー ストア キーを構成する必要があります。中央プラグインホストでキーを設定する前に、データベースユーザーを以下の説明に従って作成する必要があります。 "SAP HANA バックアップユーザーと SAP HANA ユーザーストアの構成"。

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 ユーザーが hdbsql コマンドを実行し、リソース構成でデフォルトに設定されます。システム ユーザーはログオン ユーザーではないため、SAP HANA ユーザー ストアの構成は、-u <ユーザー> オプションを使用して別のユーザーで実行する必要があります。

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

SAP HANA の複数ホスト設定では、すべてのホストの SAP HANA ユーザー ストア キーを構成する必要があります。SnapCenter は、提供された各キーを使用してデータベースに接続しようとするため、システム データベース (HANA ネーム サーバー) の別のホストへのフェイルオーバーとは独立して動作できます。すべてのワーカーとスタンバイ ホストに対して SAP HANA ユーザー ストア キーが構成されています。HANA データベース ユーザー (この例では SNAPCENTER) は、システム データベースで構成されているユーザーです。

```
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-61\S-1-5-18\SSFS_HDB.DAT
KEY FILE : C:\ProgramData\.hdb\SNAPCENTER-61\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>
```

HANA 手動リソース構成

リソース ビューの [追加] ボタンをクリックすると、手動で構成された HANA システム リソースがSnapCenterに作成されます。

[幅=601、高さ=189]

次の画面では、いくつかのシステムパラメータを指定する必要があります。

- プラグインホスト: 中央プラグインホストを選択する必要があります
- SAP HANA ユーザー ストア キー: 単一ホスト HANA システムの場合、中央プラグイン ホストで準備されたキー名を指定する必要があります。複数ホストの HANA システムの場合、システムのすべてのキーのコンマ区切りリストを提供する必要があります。
- HDBSQL OS ユーザー: 中央プラグイン ホストが Windows 上で実行されている場合、ユーザーは SYSTEM ユーザーとして事前選択されます。それ以外の場合は、SAP HANA ユーザー ストア キーに使用されているユーザーを提供する必要があります。

[幅=384、高さ=357]

次のステップとして、ストレージ フットプリントを構成する必要があります。HANA システムに属するすべてのONTAPまたは ANF ボリュームをここに追加する必要があります。

[幅=385、高さ=359]

リソース保護の構成は、自動検出された HANA システムと同じ方法で実行できるようになりました。

SnapCenterでの SAP HANA スナップショットのバックアップ操作について学習します。

SnapCenterを使用して SAP HANA スナップショット バックアップを実行します。データベース スナップショット バックアップ、ブロック整合性チェック、非データ ボリューム バックアップ、 SnapVaultまたはAzure NetApp Filesバックアップを使用したバックアップ レプリケーションについて学習します。

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。

SnapCenter は次のバックアップ操作をサポートしています。

- HANA データベースのスナップショットバックアップ操作
- ブロック整合性チェック操作
- 非データボリュームのスナップショットバックアップ
- HANA データベースまたは非データ ボリュームのバックアップ用のSnapVaultまたは ANF バックアップを使用したバックアップ レプリケーション

以下のセクションでは、 SnapCenterによって自動検出された単一ホスト HANA システム (HANA データベース ホストに展開された HANA プラグイン) のさまざまな操作について説明します。

SnapCenterでの SAP HANA スナップショットのバックアップ

SnapCenterリソース トポロジには、 SnapCenterによって作成されたバックアップのリストが表示されます。次の図は、プライマリ ストレージで使用可能なバックアップを示しており、最新のバックアップが強調表示されています。

[幅=601、高さ=293]

セカンダリ ストレージのバックアップは、Vault コピー アイコンをクリックすると一覧表示されます。

[幅=601、高さ=294]

次のスクリーンショットは、改ざん防止スナップショットが設定されているシステム SM1 のバックアップのリストを示しています。

[幅=601、高さ=293]

SAP HANA Studio での SAP HANA スナップショット バックアップ

SAP HANA MDC システムのストレージ スナップショットを使用してバックアップを実行すると、データ ボリュームのスナップショット 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

データとすべてのテナント 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に、SAP HANA は、 SnapCenter がスナップショット バックアップをトリガーするたびに、システム データベースとすべてのテナント データベースを組み合わせた内部データベース スナップショットを内部的に実行します。その結果、SAP HANA バックアップ カタログに、システム データベース用に 1 つ、テナント データベースごとに 1 つ、合計 2 つの個別のバックアップ エントリが作成されます。

SAP HANA バックアップ カタログでは、 SnapCenterバックアップ名は、外部バックアップ ID (EBID) と同様にコメント フィールドとして保存されます。これは、システム データベースの次のスクリーンショットと、その後のテナント データベース SS1 のスクリーンショットに示されています。どちらの図も、コメント フィールドに保存されているSnapCenterバックアップ名と EBID を強調表示しています。

[幅=601、高さ=289]

[幅=601、高さ=296]

SnapCenter は自身のバックアップのみを認識します。たとえば、SAP HANA Studio を使用して作成された追加のバックアップは、SAP HANA カタログに表示されますが、 SnapCenterには表示されません。また、ストレージシステム上で直接作成されたスナップショットはSnapCenterでは表示されません。

ストレージ層での**SAP HANA**スナップショットバックアップ

ストレージ層のバックアップを表示するには、 NetApp System Manager を使用してデータベース ボリュームを選択します。次のスクリーンショットは、プライマリ ストレージのデータベース ボリューム SS1_data_mnt00001 の利用可能なバックアップを示しています。強調表示されたバックアップは、前の画像のSnapCenterと SAP HANA Studio に表示されたバックアップであり、同じ命名規則が適用されます。

[幅=601、高さ=294]

次のスクリーンショットは、セカンダリ ストレージ システムのレプリケーション ターゲット ボリューム hana_SS1_data_mnt00001_dest の使用可能なバックアップを示しています。

[幅=601、高さ=294]

ANF を使用した **SAP HANA** スナップショット バックアップ

次のスクリーンショットは、Azure NetApp Filesを使用した HANA システムのトポロジ ビューを示しています。この HANA システムでは、ローカル スナップショット バックアップと、ANF バックアップを使用したバックアップ レプリケーションが構成されています。

[幅=601、高さ=303]

ANF ボリューム上のスナップショット バックアップは、Azure ポータルを使用して一覧表示できます。

[幅=601、高さ=258]

バックアップ アイコンをクリックすると、ANF バックアップで複製されたバックアップを一覧表示できます。

[幅=601、高さ=304]

ANF バックアップは、Azure ポータルにも一覧表示されます。

[幅=601、高さ=216]

非データボリュームのスナップショットバックアップ

SnapCenterリソース トポロジには、非データ ボリュームのバックアップのリストが表示されます。次の図には、HANA 共有ボリュームのバックアップがリストされています。

[幅=601、高さ=294]

HANA データベース バックアップのバックアップ ワークフロー

HANA データベース スナップショット バックアップのバックアップ ワークフローは、主に 3 つのセクションで構成されます。

- 自動検出
  - アプリケーション検出、例
    - SnapCenterはテナント構成の変更を検出します
    - SnapCenterはHANAシステムレプリケーションプライマリノードを検出します
  - ファイルシステムとストレージの検出、例
    - SnapCenterはボリューム構成の変更を検出します
    - SnapCenterはHANAの複数パーティション構成を検出します
- HANAとスナップショットのバックアップ操作
  - HANA データベース スナップショットをトリガーする
  - ストレージスナップショットを作成する
  - HANA データベースのスナップショットを確認し、HANA バックアップ カタログにバックアップを登録します。
- 保持管理
  - 定義された保持期間に基づいてスナップショットバックアップを削除します
    - SnapCenterリポジトリ
    - ストレージ
    - HANAバックアップカタログ
  - ログバックアップの保持管理
    - ファイルシステムとHANAバックアップカタログ上のログバックアップを削除する

[幅=339、高さ=475]

非データボリュームのバックアップワークフロー

非データ ボリュームの場合、バックアップ ワークフローはスナップショット操作と保持管理操作で構成されます。

[幅=329、高さ=404]

セカンダリバックアップのクリーンアップ

記載の通り "セカンダリバックアップの保持管理"セカンダリ 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、毎週のデフォルト スケジュールでクリーンアップ ジョブを実行して、 ONTAP がセカンダリ バックアップ ストレージのバックアップを削除したかどうかを定期的に確認します。

SnapCenterクリーンアップ ジョブは、セカンダリ バックアップ ストレージで削除されたバックアップが特定された場合、 SnapCenterリポジトリと SAP HANA バックアップ カタログ内のバックアップを削除します。

[幅=601、高さ=158]

[幅=267、高さ=330]

このスケジュールされたクリーンアップが完了するまで、SAP HANA とSnapCenter には、セカンダリ 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ます。これにより、セカンダリ バックアップ ストレージ上の対応するストレージ ベースのスナップショット バックアップがすでに削除されている場合でも、追加のログ バックアップが保持されることになります。NetApp、不要になったログ バックアップを保持しないように、スケジュールを週次から日次に変更することを推奨しています。

SnapCenter クリーンアップジョブの頻度を変更します

SnapCenter は、デフォルトで毎週すべてのリソースに対してクリーンアップ ジョブ SnapCenter_RemoveSecondaryBackup を実行します。これは、 SnapCenter PowerShell コマンドレットを使用して変更できます。

```
SnapCenterPS C:\> Open-SmConnection

Enter username/password
User: sapcc\scadmin
Password for user sapcc\scadmin: **********

SnapCenterPS C:\> Set-SmSchedule -ScheduleInformation
@{"ScheduleType"="Daily";"StartTime"="03:45 AM";"DaysInterval"="1"}
-TaskName SnapCenter_RemoveSecondaryBackup

TaskName : SnapCenter_RemoveSecondaryBackup
Hosts : {}
StartTime : 8/25/2025 3:45:00 AM
DaysoftheMonth :
MonthsofTheYear :
DaysInterval : 1
DaysOfTheWeek :
AllowDefaults : False
ReplaceJobIfExist : False
UserName :
Password :
SchedulerType : Daily
```

```
RepeatTask_Every_Hour : 1
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 :
ScheduleCategory :
PolicyId : 0
PolicyName :
ProtectionGroupId : 0
ProtectionGroupName :
PluginCode : NONE
PolicyType : None
ReportTriggerName :
PolicyScheduleId : 0
HoursOfTheDay :
DayStartTime :
MinuteOffset : ZeroMinutes
SnapMirrorLabel :
BackupType :
SnapCenterPS C:\>
```

構成は、 SnapCenter UI の [モニター - スケジュール] ビューでも確認できます。

[幅=601、高さ=257]

リソースレベルの手動更新

必要に応じて、リソースのトポロジ ビューでセカンダリ バックアップの手動クリーンアップを実行することもできます。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と、 SnapCenter はセカンダリ バックアップ ストレージ上のバックアップを表示します。SnapCenter は、[更新] アイコンを使用してクリーンアップ操作を実行し、このリソースのバックアップを同期します。

[幅=601、高さ=291]

SnapCenterでSAP HANAブロック整合性チェックを実行する

SAP hdbpersdiag ツールを使用するか、ファイルベースのバックアップを実行して、SAP HANA ブロック整合性チェックを実行します。ローカル スナップショット ディレクトリ アクセス、 FlexCloneボリュームを使用した中央検証ホスト、スケジュールと自動化のためのSnapCenter統合などの構成オプションについて学習します。

以下の表は、ブロック整合性チェックのどの方法が環境に最適かを判断するのに役立つ主要なパラメータをまとめたものです。

	ローカルスナップショットディレクトリを使用する **HANA hdbpersdiag** ツール	中央検証ホストを備えた **HANA hdbpersdiag** ツール	ファイルベースのバックアップ
サポートされている構成	NFSのみ ベアメタル、ANF、FSx ONTAP、VMware、または KVM のゲスト内マウント	すべてのプロトコルとプラットフォーム	すべてのプロトコルとプラットフォーム
HANAホストのCPU負荷	中	なし	高
HANAホストでのネットワーク使用率	高	なし	高
ランタイム	ストレージボリュームの完全な読み取りスループットを活用	ストレージボリュームの完全な読み取りスループットを活用	通常、ターゲットシステムの書き込みスループットによって制限されます
容量要件	なし	なし	HANA システムごとに少なくとも 1 倍のバックアップ サイズ
SnapCenter統合	バックアップ後のスクリプト	クローン作成およびクローン作成後のスクリプト、クローン削除	組み込み機能
スケジュール設定中	SnapCenterスケジューラ	外部でスケジュールされたクローン作成および削除ワークフローを実行する PowerShell スクリプト	SnapCenterスケジューラ

次の章では、ブロック整合性チェック操作のさまざまなオプションの構成と実行について説明します。

ローカルスナップショットディレクトリを使用した**hdbpersdiag**による整合性チェック

SnapCenter内では、毎日のスケジュールと 2 つの保持期間を持つ hdbpersdiag 操作専用のポリシーが作成されます。週次スケジュールは使用しません。その場合、少なくとも 2 つのスナップショット バックアップ (最小保持期間 = 2) が作成され、そのうちの 1 つは最大 2 週間前のものになるためです。

HANA システムのSnapCenterリソース保護構成内に、hdbpersdiag ツールを実行するバックアップ後のスクリプトが追加されます。バックアップ後のスクリプトは、リソースに設定されている他のポリシーでも呼び出

されるため、スクリプト内で現在アクティブなポリシーを確認する必要があります。スクリプト内では、現在の曜日も確認し、毎週日曜日に 1 回だけ hdbpersdiag 操作を実行します。次に、現在のスナップショット バックアップ ディレクトリの対応する hdb* ディレクトリ内の各データ ボリュームに対して HANA hdbpersdiag が呼び出されます。hdbpersdiag による整合性チェックでエラーが報告された場合、 SnapCenterジョブは失敗としてマークされます。

> サンプル スクリプト call-hdbpersdiag.sh は現状のまま提供されており、 NetAppサポートの対象外です。ng-sapcc@netapp.com に電子メールでスクリプトをリクエストできます。

以下の図は、整合性チェックの実装の高レベルの概念を示しています。

[幅=601、高さ=248]

最初のステップとして、スナップショット ディレクトリへのアクセスを許可して、HANA データベース ホストで ".snapshot" ディレクトリが表示されるようにする必要があります。

- ONTAPシステムおよびFSX for ONTAP:スナップショットディレクトリアクセスボリュームパラメータを設定する必要があります
- ANF: スナップショット パスの非表示ボリューム パラメータを構成する必要があります。

次のステップとして、バックアップ後のスクリプトで使用される名前と一致するポリシーを構成する必要があります。このスクリプトの例では、名前は SnapAndCallHdbpersdiag にする必要があります。前に説明したように、日次スケジュールは、週次スケジュールで古いスナップショットが保持されるのを回避するために使用されます。

[幅=414、高さ=103]

[幅=424、高さ=108]

[幅=433、高さ=336]

リソース保護構成内で、バックアップ後のスクリプトが追加され、ポリシーがリソースに割り当てられます。[幅=601、高さ=294]

[幅=601、高さ=281]

最後に、スクリプトは HANA ホストの allowed_commands.config ファイルで構成する必要があります。

```
hana-1:/ # cat /opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/hdbpersdiag/call-hdbpersdiag.sh
```

スナップショット バックアップ操作は 1 日に 1 回実行されるようになり、スクリプトは hdbpersdiag チェックが週に 1 回、日曜日にのみ実行されるように処理します。

> スクリプトは、データ ボリュームの暗号化に必要な "-e" コマンドライン オプションを使用して hdbpersdiag を呼び出します。HANA データ ボリューム暗号化を使用しない場合は、パラメータを削除する必要があります。

以下の出力はスクリプトのログ ファイルを示しています。

```
20251024055824###hana-1###call-hdbpersdiag.sh: Current policy is
SnapAndCallHdbpersdiag
20251024055824###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001
20251024055827###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001/ (4.8 GB,
5100273664 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (94276 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251024055827###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001.
20251024055827###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003
20251024055828###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
```

```
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003/
(320.0 MB, 335544320 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (4099 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
UndoContainerDirectory OK
DRLoadedTable OK
20251024055828###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003.
20251024055828###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003
20251024055833###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003/
(4.6 GB, 4898947072 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
```

```
Default Converter Pages OK
Static Converter Pages OK
RowStore Converter Pages OK
Logical Pages (100817 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
DRLoadedTable OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251024055833###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003.
20251024060048###hana-1###call-hdbpersdiag.sh: Current policy is
LocalSnapAndSnapVault, consistency check is only done with Policy
SnapAndCallHdbpersdiag
20251024080048###hana-1###call-hdbpersdiag.sh: Current policy is
LocalSnap, consistency check is only done with Policy SnapAndHdbpersdiag
```

中央検証ホストを使用した**hdbpersdiag**による整合性チェック

下の図は、ソリューションのアーキテクチャとワークフローの概要を示しています。中央検証ホストを使用すると、検証ホストを使用して複数の異なる HANA システムの一貫性をチェックできます。このソリューションは、 SnapCenter のクローン作成および削除ワークフローを活用して、検証ホストに対してチェックする必要がある HANA システムからクローン ボリュームを接続します。HANA hdbpersdiag ツールを実行するには、クローン後のスクリプトが使用されます。2 番目のステップとして、 SnapCenterクローン削除ワークフローを使用して、クローンされたボリュームをマウント解除して削除します。

> ⓘ HANA システムがデータ ボリューム暗号化で構成されている場合は、hdbpersdiag を実行する前に、ソース HANA システムの暗号化ルート キーを検証ホストにインポートする必要があります。参照 "データベース復旧前にバックアップしたルートキーをインポートする | SAP ヘルプポータル"

[幅=601、高さ=257]

HANA ツール hdbpersdiag は各 HANA インストールに含まれていますが、スタンドアロン ツールとして使用することはできません。したがって、通常の HANA システムをインストールして、中央検証ホストを準備する必要があります。

最初の1回限りの準備手順:

- 中央検証ホストとして使用するSAP HANAシステムのインストール
- SnapCenterでのSAP HANAシステムの構成

- 検証ホストでのSnapCenter SAP HANA プラグインのデプロイ。SAP HANA システムはSnapCenterによって自動検出されます。

- 初期インストール後の最初の hdbpersdiag 操作は、次の手順で準備されます。
  - ターゲットのSAP HANAシステムをシャットダウン
  - 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:/mnt/sapcc-share/hdbpersdiag # cat
/opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/hdbpersdiag/call-hdbpersdiag-flexclone.sh
```

サンプル スクリプト call-hdbpersdiag-flexclone.sh は現状のまま提供されており、 NetAppサポートの対象外です。ng-sapcc@netapp.com に電子メールでスクリプトをリクエストできます。

手動ワークフロー実行

ほとんどの場合、整合性チェック操作は、次の章で説明するように、スケジュールされた操作として実行されます。ただし、手動のワークフローを理解しておくと、自動化されたプロセスに使用されるパラメータを理解するのに役立ちます。

クローン作成ワークフローは、チェックするバックアップをシステムから選択し、バックアップからクローンをクリックすることによって開始されます。

[幅=601、高さ=247]

次の画面では、検証ホストのホスト名、SID、およびストレージ ネットワーク インターフェイスを指定する必要があります。

検証ホストにインストールされている HANA システムの SID を常に使用することが重要です。そうしないと、ワークフローは失敗します。

[幅=431、高さ=115]

次の画面で、クローン後のコマンドとして call-hdbpersdiag-fleclone.sh スクリプトを追加する必要があります。

[幅=442、高さ=169]

ワークフローが開始されると、 SnapCenter は選択したスナップショット バックアップに基づいてクローンボリュームを作成し、検証ホストにマウントします。

注: 以下の出力例は、ストレージ プロトコルとして NFS を使用する HANA システムに基づいています。FC または VMware VMDK を使用する HANA システムの場合、デバイスは同様に /hana/data/SID/mnt00001 にマウントされます。

```
hana-7:/mnt/sapcc-share/hdbpersdiag # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 16G 8.0K 16G 1% /dev
tmpfs 25G 0 25G 0% /dev/shm
tmpfs 16G 474M 16G 3% /run
tmpfs 16G 0 16G 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 9.0G 48G 16% /
/dev/mapper/system-root 60G 9.0G 48G 16% /home
/dev/mapper/system-root 60G 9.0G 48G 16% /.snapshots
/dev/mapper/system-root 60G 9.0G 48G 16% /root
/dev/mapper/system-root 60G 9.0G 48G 16% /opt
/dev/mapper/system-root 60G 9.0G 48G 16% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 9.0G 48G 16% /srv
/dev/mapper/system-root 60G 9.0G 48G 16% /usr/local
/dev/mapper/system-root 60G 9.0G 48G 16% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 9.0G 48G 16% /var
/dev/mapper/system-root 60G 9.0G 48G 16% /tmp
/dev/sda1 500M 5.1M 495M 2% /boot/efi
192.168.175.117:/QS1_shared/usr-sap 251G 15G 236G 6% /usr/sap/QS1
192.168.175.86:/sapcc_share 1.4T 858G 568G 61% /mnt/sapcc-share
192.168.175.117:/QS1_log_mnt00001 251G 335M 250G 1% /hana/log/QS1/mnt00001
192.168.175.117:/QS1_shared/shared 251G 15G 236G 6% /hana/shared
tmpfs 3.2G 20K 3.2G 1% /run/user/467
tmpfs 3.2G 0 3.2G 0% /run/user/0
192.168.175.117:/SS2_data_mnt00001_Clone_10292511250337819 250G 6.4G 244G
3% /hana/data/QS1/mnt00001
```

以下の出力は、クローン後のコマンド call-hdbpersdiag-flexclone.sh のログ ファイルを示しています。

```
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag for source system SS2.
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Clone mounted at
/hana/data/QS1/mnt00001.
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00001
20251029112600###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00001/ (3.1 GB, 3361128448 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
```

```
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (65388 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251029112600###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00001.
20251029112601###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00002.00003
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00002.00003/ (288.0 MB, 301989888 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (4099 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
UndoContainerDirectory OK
DRLoadedTable OK
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00002.00003.
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00003.00003
20251029112606###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
```

```
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00003.00003/ (3.7 GB, 3942645760 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
Static Converter Pages OK
RowStore Converter Pages OK
Logical Pages (79333 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
DRLoadedTable OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251029112606###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00003.00003.
```

スクリプトは、データ ボリュームの暗号化に必要な "-e" コマンドライン オプションを使用して hdbpersdiag を呼び出します。HANA データ ボリューム暗号化を使用しない場合は、パラメータを削除する必要があります。クローン後のスクリプトが終了すると、 SnapCenterジョブも終了します。

[幅=279、高さ=344]

次のステップとして、 SnapCenterクローン削除ワークフローを実行して、検証ホストをクリーンアップし、FlexCloneボリュームを削除します。

ソース システムのトポロジ ビューでクローンを選択し、削除ボタンをクリックします。

[幅=601、高さ=165]

SnapCenter は、検証ホストからクローン ボリュームをアンマウントし、ストレージ システムからクローン ボリュームを削除します。

PowerShell スクリプトを使用したSnapCenterワークフローの自動化

前のセクションでは、 SnapCenter UI を使用してクローン作成ワークフローとクローン削除ワークフローを実行しました。すべてのワークフローは PowerShell スクリプトまたは REST API 呼び出しで実行することも可能で、さらなる自動化が可能になります。次のセクションでは、 SnapCenterクローン作成ワークフローとクローン削除ワークフローを実行する基本的な PowerShell スクリプトの例について説明します。

> サンプル スクリプト call-hdbpersdiag-flexclone.sh および clone-hdbpersdiag.ps1 は現状のまま提供されており、 NetAppサポートの対象外です。スクリプトは、ng-sapcc@netapp.com に電子メールでリクエストできます。

PowerShell のサンプル スクリプトは、次のワークフローを実行します。

- コマンドラインパラメータSIDとソースホストに従って最新のスナップショットバックアップを検索します
- 前の手順で定義したスナップショット バックアップを使用して、 SnapCenterクローン作成ワークフローを実行します。ターゲット ホスト情報と hdbpersdiag 情報はスクリプトで定義されます。call-hdbpersdiag-flexclone.sh スクリプトは、クローン後のスクリプトとして定義され、ターゲット ホストで実行されます。
  - $result = New-SmClone -AppPluginCode hana -BackupName $backupName -Resources @{"Host"="$sourceHost";"UID"="$uid"} -CloneToInstance "$verificationHost" -NFSExportIPs $exportIpTarget -CloneUid $targetUid -PostCloneCreateCommands $postCloneScript
- SnapCenterクローン削除ワークフローを実行します。以下のテキストは、 SnapCenterサーバーで実行されたサンプル スクリプトの出力を示しています。

以下のテキストは、 SnapCenterサーバーで実行されたサンプル スクリプトの出力を示しています。

```
C:\Users\scadmin>pwsh -command "c:\netapp\clone-hdbpersdiag.ps1 -sid SS2
-sourceHost hana-3.sapcc.stl.netapp.com"
Starting verification
Connecting to SnapCenter
Validating clone/verification request - check for already existing clones
Get latest back for [SS2] on host [hana-3.sapcc.stl.netapp.com]
Found backup name [SnapCenter_hana-3_LocalSnapKeep2_Hourly_11-21-
2025_07.56.27.5547]
Creating clone from backup [hana-
3.sapcc.stl.netapp.com/SS2/SnapCenter_hana-3_LocalSnapKeep2_Hourly_11-21-
2025_07.56.27.5547]: [hana-7.sapcc.stl.netapp.com/QS1]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Completed]
Removing clone [SS2 - HANA System Replication__clone__169851_MDC_SS2_07-
09-2025_07.44.09]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Completed]
Verification completed

C:\Users\scadmin>
```

このスクリプトは、データ ボリュームの暗号化に必要な "-e" コマンドライン オプションを使用して hdbpersdiag を呼び出します。HANA データ ボリューム暗号化を使用しない場合は、パラメータを削除する必要があります。

以下の出力は、call-hdbpersdiag-flexclone.sh スクリプトのログ ファイルを示しています。

```
20251121085720###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag for source system SS2.
20251121085720###hana-7###call-hdbpersdiag-flexclone.sh: Clone mounted at
/hana/data/QS1/mnt00001.
```

```
20251121085720###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00001
20251121085723###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
  #0 /hana/data/QS1/mnt00001/hdb00001/ (3.1 GB, 3361128448 bytes)
Tips:
  Type 'help' for help on the available commands
  Use 'TAB' for command auto-completion
  Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
                      Default Anchor Page OK
                             Restart Page OK
                   Default Converter Pages OK
                  RowStore Converter Pages OK
              Logical Pages (65415 pages) OK
                    Logical Pages Linkage OK
Checking entries from restart page...
                       ContainerDirectory OK
                  ContainerNameDirectory OK
                  FileIDMappingContainer OK
                  UndoContainerDirectory OK
                             LobDirectory OK
                     MidSizeLobDirectory OK
                             LobFileIDMap OK
20251121085723###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00001.
20251121085723###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00002.00003
20251121085724###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
  #0 /hana/data/QS1/mnt00001/hdb00002.00003/ (288.0 MB, 301989888 bytes)
Tips:
  Type 'help' for help on the available commands
  Use 'TAB' for command auto-completion
  Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
                      Default Anchor Page OK
                             Restart Page OK
                   Default Converter Pages OK
                  RowStore Converter Pages OK
```

```
              Logical Pages (4099 pages) OK
                   Logical Pages Linkage OK
Checking entries from restart page...
                  UndoContainerDirectory OK
                           DRLoadedTable OK
20251121085724###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00002.00003.
20251121085724###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00003.00003
20251121085729###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
  #0 /hana/data/QS1/mnt00001/hdb00003.00003/ (3.7 GB, 3942645760 bytes)
Tips:
  Type 'help' for help on the available commands
  Use 'TAB' for command auto-completion
  Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
                     Default Anchor Page OK
                            Restart Page OK
                 Default Converter Pages OK
                  Static Converter Pages OK
                RowStore Converter Pages OK
             Logical Pages (79243 pages) OK
                   Logical Pages Linkage OK
Checking entries from restart page...
                      ContainerDirectory OK
                  ContainerNameDirectory OK
                  FileIDMappingContainer OK
                  UndoContainerDirectory OK
                            LobDirectory OK
                           DRLoadedTable OK
                     MidSizeLobDirectory OK
                            LobFileIDMap OK
20251121085729###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00003.00003.
hana-7:/mnt/sapcc-share/hdbpersdiag #
```

ファイルベースのバックアップ

SnapCenter 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が選択されたポリシーを使用して、ブロック整合性チェックの実行をサポートします。

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 はシステムとすべてのテナント

データベースの標準の SAP HANA ファイル バックアップを作成します。

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。

[幅=601、高さ=293]

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。

[幅=601、高さ=293]

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。

[幅=351、高さ=433]

SnapCenter は、ファイルベースのデータ バックアップ操作に HANA データベースで構成されたバックアップ パスを使用します。

```
hana-1:/hana/shared/SS1/HDB00/backup/data # ls -al *
DB_SS1:
total 3717564
drwxr-xr-- 2 ss1adm sapsys 4096 Aug 22 11:03 .
drwxr-xr-- 4 ss1adm sapsys 4096 Jul 27 2022 ..
-rw-r----- 1 ss1adm sapsys 159744 Aug 17 05:32 SnapCenter_SnapCenter_hana-
1_BlockIntegrityCheck_Weekly_08-17-2025_05.32.00.4493_databackup_0_1
-rw-r----- 1 ss1adm sapsys 83898368 Aug 17 05:32
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_08-17-
2025_05.32.00.4493_databackup_2_1
-rw-r----- 1 ss1adm sapsys 3707777024 Aug 17 05:32
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_08-17-
2025_05.32.00.4493_databackup_3_1
SYSTEMDB:
total 3339236
drwxr-xr-- 2 ss1adm sapsys 4096 Aug 22 11:03 .
drwxr-xr-- 4 ss1adm sapsys 4096 Jul 27 2022 ..
-rw-r----- 1 ss1adm sapsys 163840 Aug 17 05:32 SnapCenter_SnapCenter_hana-
1_BlockIntegrityCheck_Weekly_08-17-2025_05.32.00.4493_databackup_0_1

-rw-r----- 1 ss1adm sapsys 3405787136 Aug 17 05:32
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_08-17-
2025_05.32.00.4493_databackup_1_1
```

SnapCenterを使用した SAP HANA データベースの復元とリカバリ

自動または手動のリカバリ オプションを備えたSnapCenterを使用して、SAP HANA システムを復元およびリカバリします。これには、完全なシステム復元、 ONTAP上の HANA データベース、 Azure NetApp Files、および FSx for ONTAPの単一テナント復元が含まれます。

SnapCenter は、次の復元およびリカバリ操作をサポートしています。

- 単一テナントのSAP HANA MDCシステム
  - エンドツーエンドの自動復元と回復
  - エンドツーエンドの自動復元と手動リカバリ（選択可能）
- 複数のテナントを持つSAP HANA MDCシステム
  - エンドツーエンドの自動復元、リカバリは手動で行う必要がある
- 単一テナントのリストア
  - エンドツーエンドの自動復元、リカバリは手動で行う必要がある

自動リカバリは、HANA プラグインが HANA データベース ホストに展開され、HANA システムがSnapCenterによって自動検出された場合にのみサポートされます。中央プラグイン ホスト構成では、 SnapCenterによる復元操作後に手動でリカバリを実行する必要があります。

Azure NetApp Filesでは、プライマリANFボリュームまたはANFバックアップに対してリストア処理がサポートされます。プライマリANFボリュームの場合はボリュームリバート、ANFバックアップの場合は単一ファイルリストアを使用したIn Placeリストアが実行されます。どちらの場合も、アプリケーションボリュームグループ構成は維持されます。

ボリューム暗号化が有効でSAPローカルセキュアストア（LSS）が使用されている場合、バックアップが取得されてからLSS内のルートキーバックアップパスワードが変更されていない限り、SnapCenterによるリカバリがサポートされます。パスワードが変更され、異なるパスワードを持つ古いSnapshotを使用してリストアとリカバリが実行された場合、リカバリは手動で実行する必要があり、リカバリステートメントで古いパスワードを提供する必要があります：'"RECOVER DATA USING SNAPSHOT CLEAR LOG ENCRYPTION ROOT KEYS BACKUP PASSWORD 'old-password'"

単一テナントによるSAP HANA MDCシステムの自動リストアとリカバリ

復元操作は、リソース トポロジ ビューでスナップショット バックアップを選択し、[復元] をクリックすることによって開始されます。

[幅=601、高さ=294]

ANF、FSx for ONTAP 、またはONTAPストレージ システム上の NFS を使用する HANA システムでは、プライマリ ボリューム スナップショットのボリューム復元操作の有無にかかわらず、完全な復元を選択できます。

- ボリュームを元に戻さない完全なリソースでは、Single File SnapRestore (SFSR) を使用してデータベースのすべてのファイルを復元します。
- ボリュームの復元を含む完全なリソースでは、ボリューム ベースの復元操作 (VBSR) を使用して、完全なボリュームを選択したスナップショットの状態に戻します。

アクティブなSnapVaultまたはSnapMirrorレプリケーション スナップショットよりも古いスナップショットに復元する必要がある場合、ボリュームの復元は使用できません。

ボリュームの復元操作では、復元操作に選択されたスナップショットよりも新しいすべてのスナップショット バックアップが削除されます。

SFSR による復元はボリュームの復元操作とほぼ同じくらい高速ですが、バックグラウンド プロセスがメタデータ操作を完了するまで、すべてのスナップショット操作がブロックされます。

[幅=300]

FC SAN を使用するベアメタル ホスト上の HANA システムでは、ボリュームの復元 (VBSR) はサポートされておらず、代わりに復元操作には常に SFSR が使用されます。VMFS を使用した VMware 上で実行される HANA システムでは、クローン、マウント、コピー操作が使用されます。

[幅=345、高さ=325]

セカンダリ バックアップから復元する場合は、アーカイブの場所を選択する必要があります。

[幅=345、高さ=323]

リカバリ スコープを使用すると、ログ バックアップを使用せずに、「最新の状態」、「ポイント イン タイム」、またはセーブ ポイント リカバリを選択できます。リカバリなしを選択した場合、 SnapCenterは復元操作のみを実行し、リカバリは説明されているように手動で行う必要があります。 "HANA Studio を使用した手動リカバリ"。

SnapCenter は、ログ バックアップとカタログ バックアップの場所に SAP HANA で構成されたパスを使用します。追加の場所に階層化されたバックアップがある場合は、これらの追加パスを追加できます。

[幅=346、高さ=324]

オプションで、復元前および復元後のスクリプトを追加できます。

[幅=348、高さ=326]

[幅=359、高さ=335]

概要画面で [完了] をクリックすると、復元および回復操作が開始されます。

[幅=361、高さ=336]

復元と回復のワークフローは、主に 3 つのセクションに分けられます。

- HANAシステムのシャットダウン
- リストア処理を実行します
  - ファイルシステム固有の準備、例：アンマウント操作
  - スナップショットの復元操作
  - ファイルシステム固有の後処理、例えばマウント操作
- HANAリカバリPITリカバリ
  - システムデータベースのリカバリ
  - テナントデータベースのリカバリ

[幅=357、高さ=439]

HANA Studio を使用した手動リカバリ

SAP HANA Studio とSnapCenterを使用して、単一または複数のテナントを持つ SAP HANA MDC システムを復元および回復するには、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. 回復の種類を選択し、バックアップ カタログの場所を指定します。
   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、プライマリ ストレージから復元する場合は [ローカル コピー] を選択し、セカンダリ バックアップ ストレージから復元する場合は [ボールト 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。
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。
   c. 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。
   d. 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。
5. 複数のテナントを持つ HANA システムの場合は、テナントごとに手順 4 を繰り返します。

SAP HANA Cockpit を使用した手動リカバリも同じ手順で実行されます。

次のセクションでは、単一テナントの SAP HANA MDC システムの復元およびリカバリ操作の手順について説明します。

HANA Studio で、[バックアップとリカバリ] および [システム データベースのリカバリ] を選択します。

[幅=450、高さ=368]

シャットダウン操作を確認します。HANA システムがまだ実行されている場合にのみ必要です。

[幅=349、高さ=83]

回復操作を選択します。この例では、最新の状態に回復します。

[幅=345、高さ=359]

バックアップ カタログの場所を指定します。

[幅=343、高さ=356]

HANA Studio は、HANA バックアップ カタログに保存されている最新のバックアップを一覧表示します。

バックアップ カタログの内容に基づいて、利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、最新のバックアップです。

[幅=391、高さ=283]

SnapCenter GUI から、リソース トポロジ ビューを選択し、復元するバックアップ (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。復元を開始するには、「復元」アイコンをクリックします。

[幅=601、高さ=294]

SnapCenter復元ウィザードが起動します。ボリュームベースの復元を使用するには、復元タイプとして「完全なリソースとボリュームの復元」を選択します。

[幅=346、高さ=325]

SnapCenterワークフローからリカバリ操作を除外するには、「リカバリなし」を選択します。

[幅=358、高さ=336]

「完了」をクリックすると復元操作が開始されます。

[幅=361、高さ=339]

SnapCenterは現在、復元操作を実行しています。

- ファイルシステム固有の準備、例：アンマウント操作
- スナップショットの復元操作
- ファイルシステム固有の後処理、例：マウント操作

[幅=322、高さ=398]

スナップショットがSnapCenterによって復元されると、HANA データ ボリュームのシステムおよびテナント データベース サブディレクトリで snapshot_databackup_0_1 ファイルが使用できるようになります。このファイルは、HANA データベース スナップショットの作成中に HANA データベースによって作成されました。HANA はバックアップ操作が完了するとファイルを削除するため、ファイルはスナップショット バックアップ内でのみ表示されます。これらのファイルは、あらゆる回復操作に必要です。リカバリ後、ファイルは HANA データベースによって削除されます。

```
hana-1:~ # cd /hana/data/SS1/mnt00001/
hana-1:/hana/data/SS1/mnt00001 # ls -al *
-rw-r--r-- 1 ss1adm sapsys 16 Aug 26 06:00 nameserver.lck
hdb00001:
total 4992236
drwxr-x--- 2 ss1adm sapsys 4096 Aug 26 06:00 .
drwxr-x--- 5 ss1adm sapsys 4096 Aug 26 06:00 ..
-rw-r----- 1 ss1adm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 ss1adm sapsys 5100273664 Aug 26 06:00 datavolume_0000.dat
-rw-r----- 1 ss1adm sapsys 36 Aug 25 10:30 landscape.id
-rw-r----- 1 ss1adm sapsys 163840 Aug 26 06:00 snapshot_databackup_0_1
hdb00002.00003:
total 201420
drwxr-xr-- 2 ss1adm sapsys 4096 Nov 3 2020 .
drwxr-x--- 5 ss1adm sapsys 4096 Aug 26 06:00 ..
-rw-r--r-- 1 ss1adm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r--r-- 1 ss1adm sapsys 335544320 Aug 26 06:00 datavolume_0000.dat
hdb00003.00003:
total 4803140
drwxr-xr-- 2 ss1adm sapsys 4096 Aug 26 06:00 .
drwxr-x--- 5 ss1adm sapsys 4096 Aug 26 06:00 ..
-rw-r--r-- 1 ss1adm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r--r-- 1 ss1adm sapsys 4898947072 Aug 26 06:00 datavolume_0000.dat
-rw-r----- 1 ss1adm sapsys 159744 Aug 26 06:00 snapshot_databackup_0_1
hana-1:/hana/data/SS1/mnt00001 #
```

SAP HANA Studio に移動し、「更新」をクリックして利用可能なバックアップのリストを更新します。SnapCenterで復元されたバックアップは、バックアップ リストに緑色のアイコンで表示されます。バックアップを選択し、「次へ」をクリックします。

[幅=400、高さ=290]

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。

SAP HANA Studio は、ログ バックアップとカタログ バックアップの場所に SAP HANA で構成されたパスを使用します。追加の場所に階層化されたバックアップがある場合は、これらの追加パスを追加できます。

[幅=465、高さ=296]

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。

[幅=466、高さ=296]

リカバリ設定を確認し、 [完了] をクリックします。

SQL ステートメントの表示をクリックすると、HANA Studio はリカバリ操作のために実行される SQL コマンドを表示します。

[幅=464、高さ=295]

回復プロセスが開始されます。システム データベースの回復が完了するまで待ちます。

[幅=376、高さ=239]

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。

[幅=476、高さ=315]

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。

[幅=342、高さ=355]

リカバリタイプを指定して、 Next （次へ）をクリックします。

[幅=343、高さ=356]

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。

[幅=342、高さ=355]

テナント データベースのシャットダウンを確認します。

[幅=348、高さ=85]

システム データベースの回復前にデータ ボリュームの復元が実行されているため、テナント バックアップはすぐに利用できます。緑色で強調表示されたバックアップを選択し、「次へ」をクリックします。

[幅=433、高さ=349]

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。

SAP HANA Studio は、ログ バックアップとカタログ バックアップの場所に SAP HANA で構成されたパスを使用します。追加の場所に階層化されたバックアップがある場合は、これらの追加パスを追加できます。

[幅=384、高さ=310]

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。

[幅=384、高さ=310]

リカバリ設定を確認し、 [完了] をクリックします。

SQL ステートメントの表示をクリックすると、HANA Studio はリカバリ操作のために実行される SQL コマンドを表示します。

[幅=380、高さ=307]

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。

[幅=378、高さ=305]

テナントのリカバリが完了すると、SAP HANA システムが起動して実行されます。

複数のテナントを持つ SAP HANA MDC システムの場合、テナントごとにテナント回復を繰り返す必要があります。

SQLコマンドによる手動リカバリ

HANA システムのリカバリには SQL ステートメントを使用することもできます。

まず、システム データベースを回復する必要があります。

```
HDBSettings.sh recoverSys.py --command="RECOVER DATABASE UNTIL TIMESTAMP
'2026-08-26 10:55:49' USING CATALOG PATH ('mnt/log-backup/SYSTEMDB') USING
LOG PATH ('mnt/log-backup/SYSTEMDB') USING SNAPSHOT"
```

2 番目の手順として、システム データベースに接続し、テナント データベースの回復を開始する必要があります。この例では、テナント データベースは SS1 です。

```
hdbsql SYSTEMDB=> RECOVER DATABASE FOR SS1 UNTIL TIMESTAMP '2026-08-26
10:55:49' USING CATALOG PATH ('mnt/log-backup/DB_SS1') USING LOG PATH
('mnt/log-backup/DB_SS1') USING SNAPSHOT
```

単一テナントの復元と回復

SnapCenterを使用した単一テナントの復元およびリカバリ操作は、前のトピックで説明したワークフローと

非常によく似ています。 "HANA Studio を使用した手動リカバリ"。

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. [テナント データベースの回復] を選択し、テナント データベースのシャットダウンを確認します。
   b. 回復の種類を選択し、バックアップ カタログの場所を指定します。
   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、プライマリ ストレージから復元する場合は [ローカル コピー] を選択し、セカンダリ バックアップ ストレージから復元する場合は [ボールト 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. テナントの復元プロセスを開始します。
3. 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. 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. 回復プロセスを開始します。回復プロセスが完了すると、テナント データベースが起動します。

非データボリュームの復元

非データ ボリュームの復元操作は、非データ ボリューム リソースのトポロジ ビューでスナップショット バックアップを選択し、[復元] をクリックすることによって開始されます。

[幅=601、高さ=294]

NFS の非データ ボリュームの場合、完全なリソース (VBSR) またはファイル レベル (SFSR) の復元操作を選択できます。ファイル レベルの復元では、復元操作の対象としてすべてのファイルまたは個々のファイルを定義できます。

[幅=369、高さ=344]

SAP HANA の高度なSnapCenterオプションを構成する

ゲスト内 NFS マウントの VMware 警告メッセージの抑制、自動ログ バックアップ ハウスキーピングの無効化、HANA データベース接続の SSL 暗号化の有効化など、SAP HANA 環境向けの高度なSnapCenter設定を構成します。

仮想化環境とゲスト内マウントに関する警告メッセージ

たとえば、NFS ゲスト内マウントを使用して VMware を使用する場合、 SnapCenter はSnapCenter VMware プラグインを使用する必要があるという警告メッセージを発行します。VMWare プラグインはゲスト内マウントには必要ないため、警告メッセージは無視してオフにすることができます。この警告を抑制するようにSnapCenterを構成するには、次の構成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。

[幅=601、高さ=176]

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 ハウスキーピングはデフォルトで有効になっていますが、HANA プラグイン ホスト レベルで無効にすることができます。PowerShell コマンドを使用します:

コマンド Set- SmConfigSettings -Plugin - HostName <pluginhostname> - PluginCode hana - configSettings @{"LOG_CLEANUP_DISABLE" = "Y"} は、この SAP HANA ホストのログ バックアップ ハウスキーピングを無効にします。

HANA データベースとのセキュアな通信を有効にします

HANA データベースが安全な通信で構成されている場合、 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。

SSL 通信を構成するためのさまざまなオプションがあります。デフォルトでは、 SnapCenter は-e ssltrustcert hdbsql コマンドライン オプションを使用します。このオプションを使用すると、サーバー証明書の検証なしの SSL 通信が実行され、SSL が有効になっていない HANA システムでもこのオプションは機能します。

サーバー側および/またはクライアント側で証明書の検証が必要な場合は、異なる hdbsql コマンドライン オプションが必要になり、SAP HANA セキュリティ ガイドの説明に従って PSE 環境を適宜構成する必要があります。

これは、必要なオプションを使用して hdbsql を呼び出すラッパー スクリプトを使用することで実現できます。hana.properties ファイルで hdbsql 実行可能ファイルを構成する代わりに、ラッパー スクリプトが追加されます。

```
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 オプションを使用して hdbsql を呼び出します。

```
#/bin/bash
/usr/sap/SM1/HDB12/exe/hdbsql <command line options> $*
```

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サーバーで PowerShell を開きます。Open-SmConnection コマンドを実行してSnapCenter Server に接続し、開いたログイン ウィンドウでユーザー名とパスワードを指定します。
2. 自動検出を無効にするには、Set-SmConfigSettings コマンドを実行します。

HANA ホスト hana-2 の場合、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>

Verify the configuration by running the Get- SmConfigSettings command.

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 #
```