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

NetApp Solutions SAP

NetApp
June 27, 2024

目次

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 』

ネットアップ Nils Bauer

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。

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。

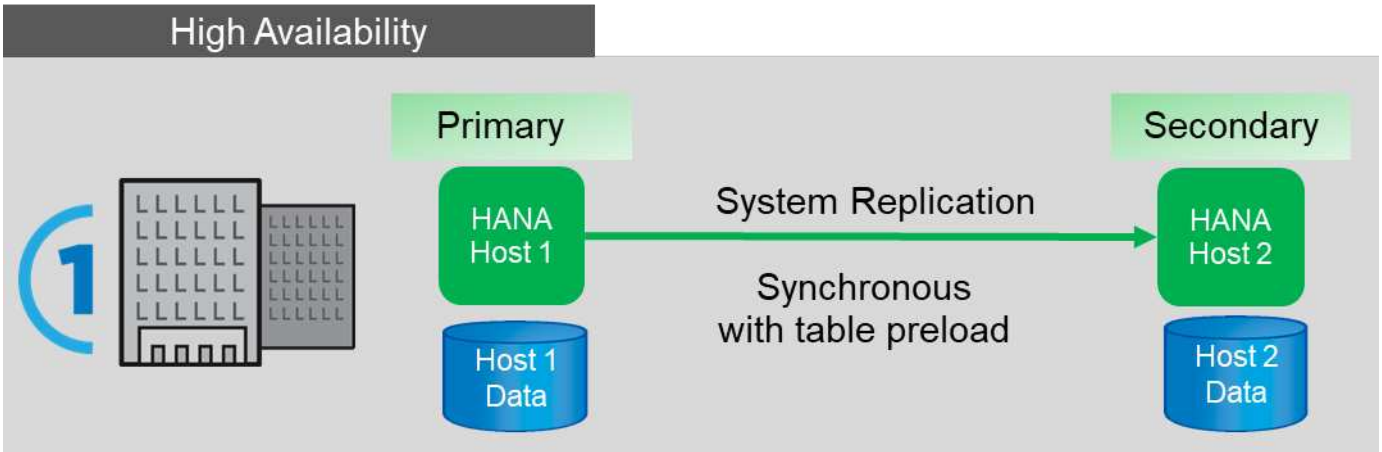
RPO がゼロで RTO が最小限のハイアベイラビリティ

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。

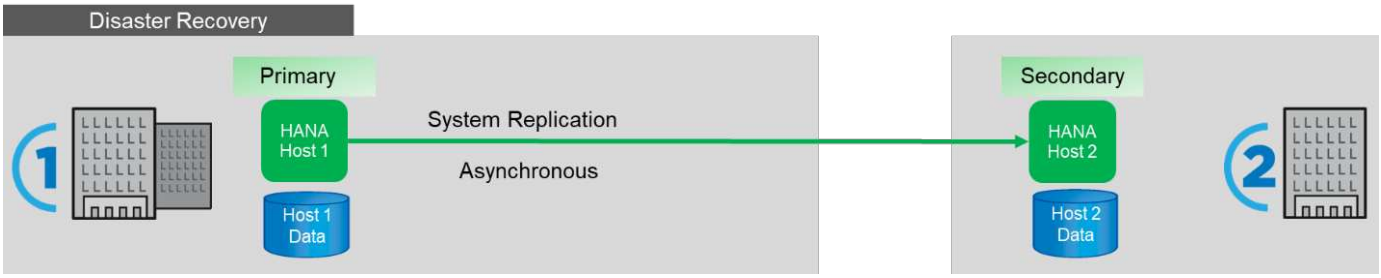
このドキュメントの残りの部分では、ハイアベイラビリティ解決策として構成された SAP システムレプリケーションを使用したバックアップ処理について説明します。



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。



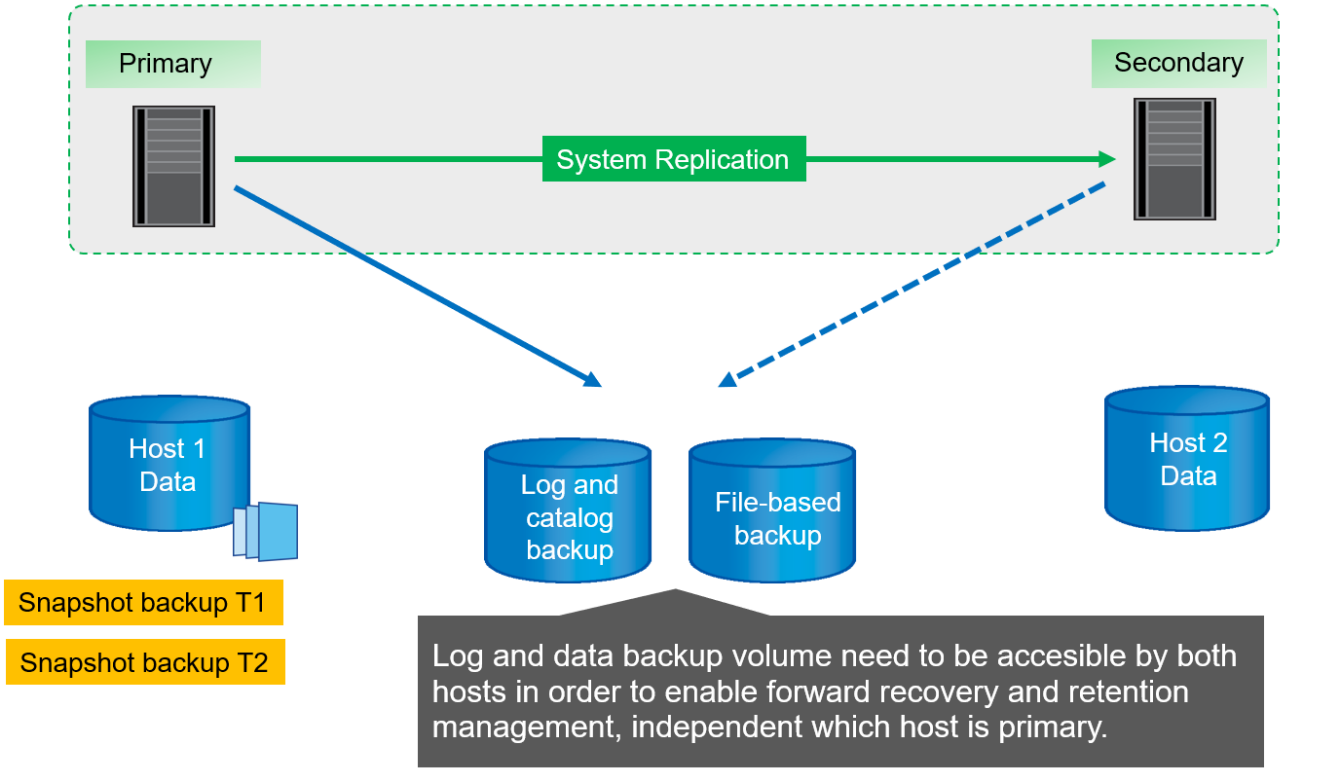
ストレージ **Snapshot** バックアップと **SAP** システムレプリケーション

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。

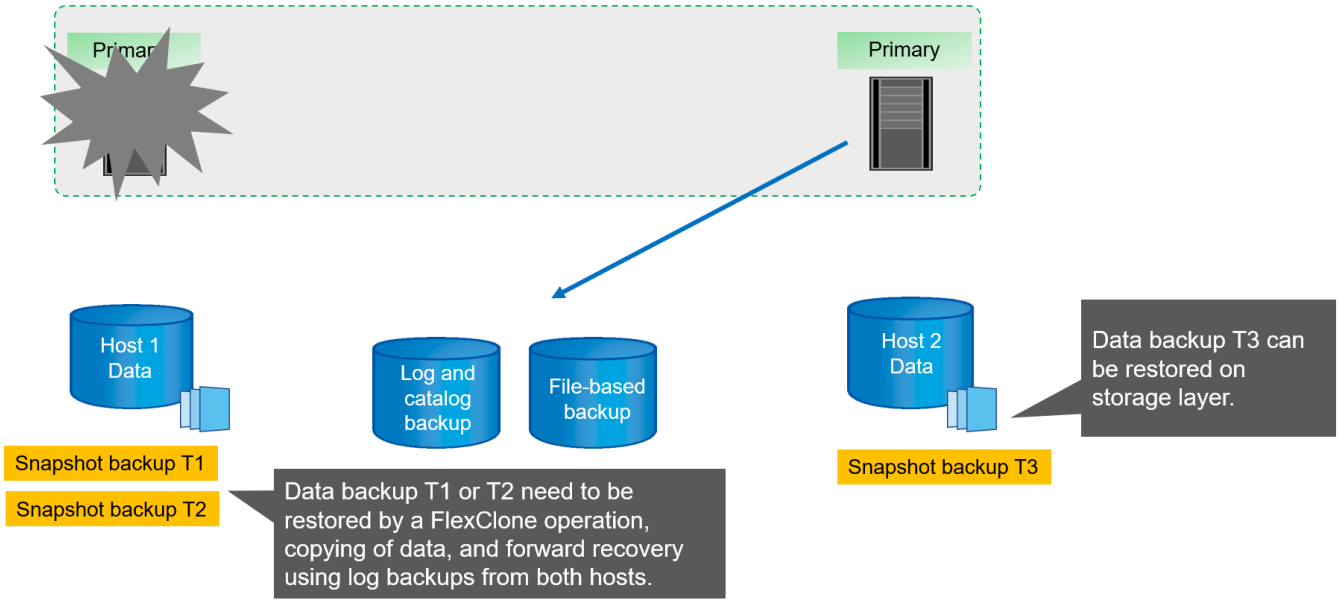
いずれかのバックアップをリストアに使用したり、両方のホストからログバックアップを使用してリカバリを転送したりするには、両方のホストからアクセスできる共有ログバックアップの場所が必要です。共有ストレージボリュームを使用することを推奨します。ただし、ログバックアップのデスティネーションは、共有ボリューム内のサブディレクトリに分ける必要があります。

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。

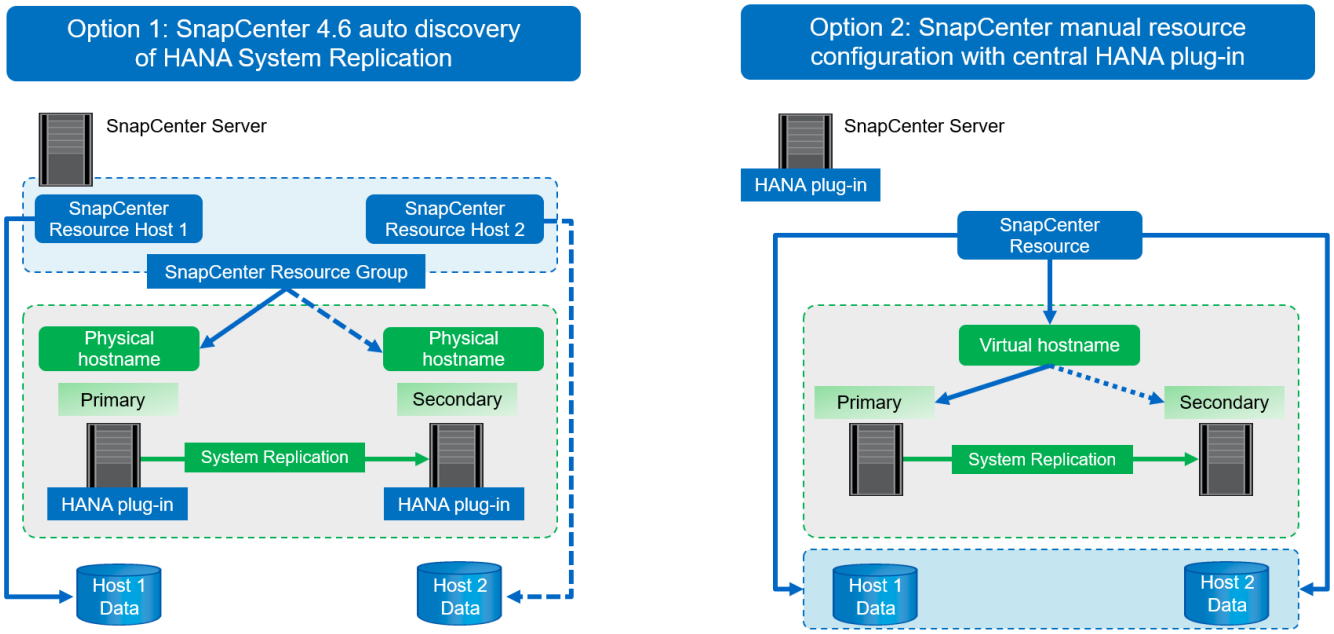
ホスト 2 で作成されたバックアップは、ストレージレイヤで直接リストアできます。ホスト 1 に作成したバックアップを使用する場合は、ホスト 1 のストレージボリュームからホスト 2 のストレージボリュームにバックアップをコピーする必要があります。フォワードリカバリでは、両方のホストからのログバックアップが使用されます。



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。

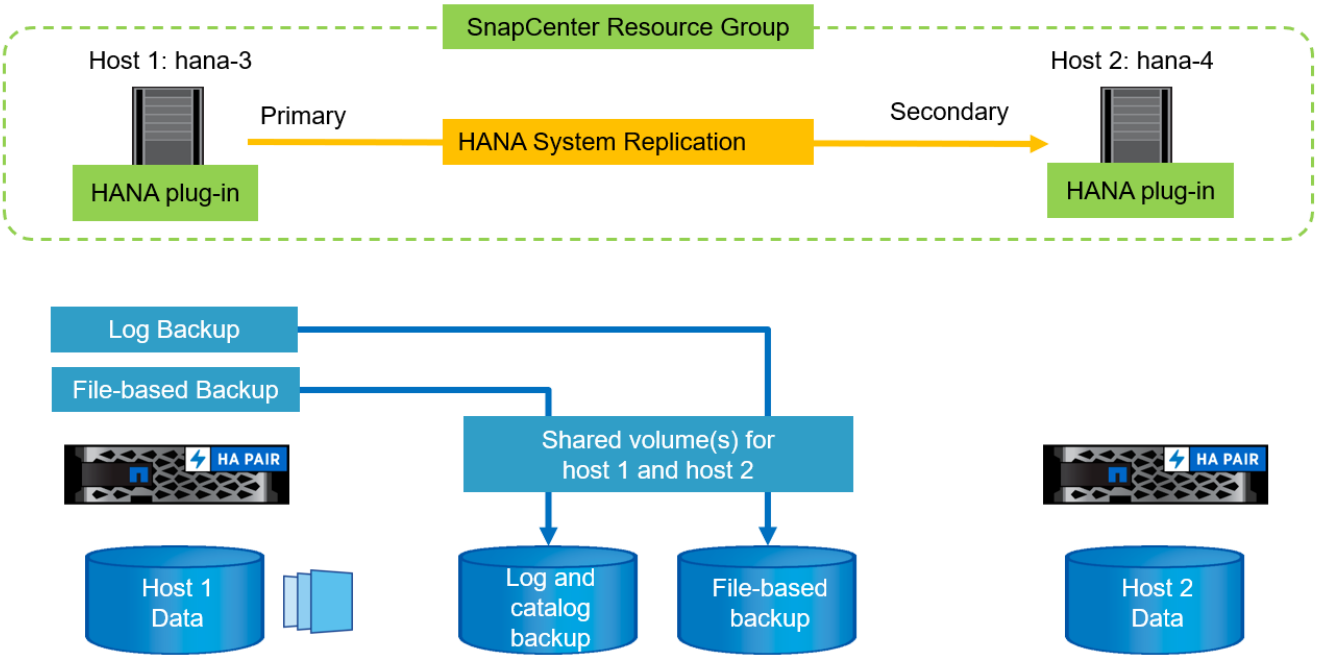
HANA システムデータベース用のデータベースユーザ「 SnapCenter 」が作成され、バックアップおよびリカバリ処理を実行するために必要な権限が付与されています（を参照） "SnapCenter を使用した SAP HANA のバックアップとリカバリ"）。HANA のユーザストアキーは、上記のデータベースユーザを使用して両方のホストで設定する必要があります。

```
ss2adm@hana- 3: / > hdbuserstore set SS2KEY hana- 3:33313 SNAPCENTER
<password>
```

```
ss2adm@hana- 4:/ > hdbuserstore set SS2KEY hana-4:33313 SNAPCENTER
<password>
```

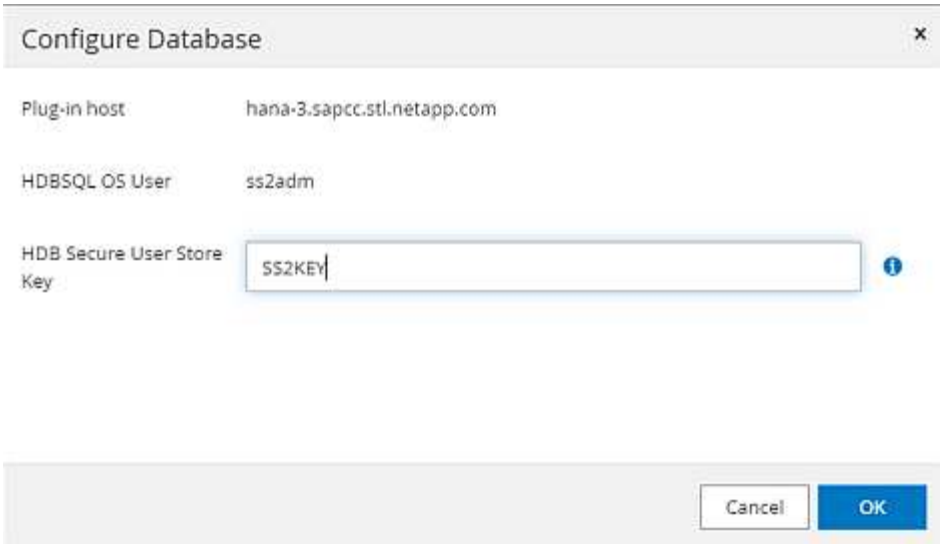
SnapCenter で HANA システムのレプリケーションを設定するには、大まかに見て次の手順を実行する必要があります。

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。

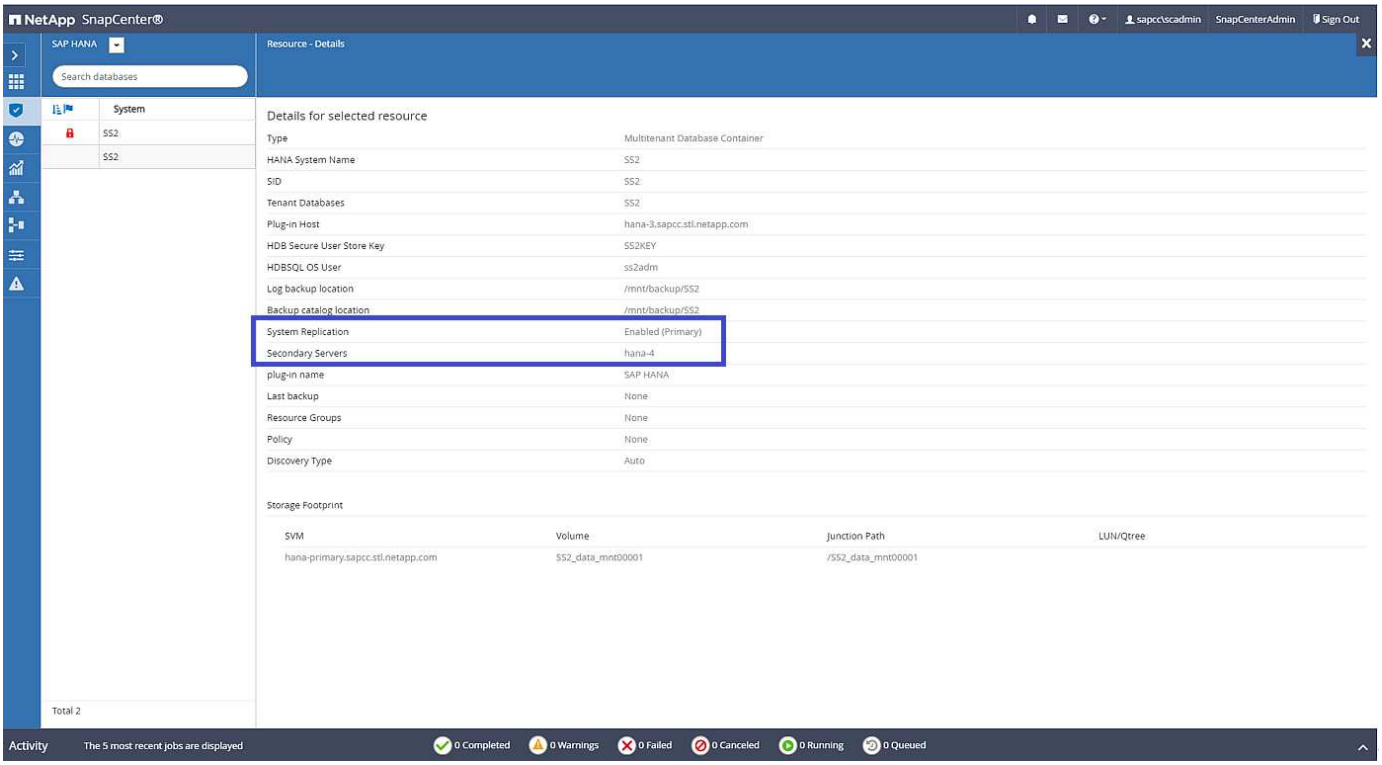


両方の HANA ホストに SnapCenter HANA プラグインをインストールすると、他の自動検出されたリソースと同じように、 HANA システムが SnapCenter リソースビューに表示されます。SnapCenter 4.6 以降では、追加の列に HANA システムレプリケーション（有効 / 無効、プライマリ / セカンダリ）のステータスが表示されます。

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。

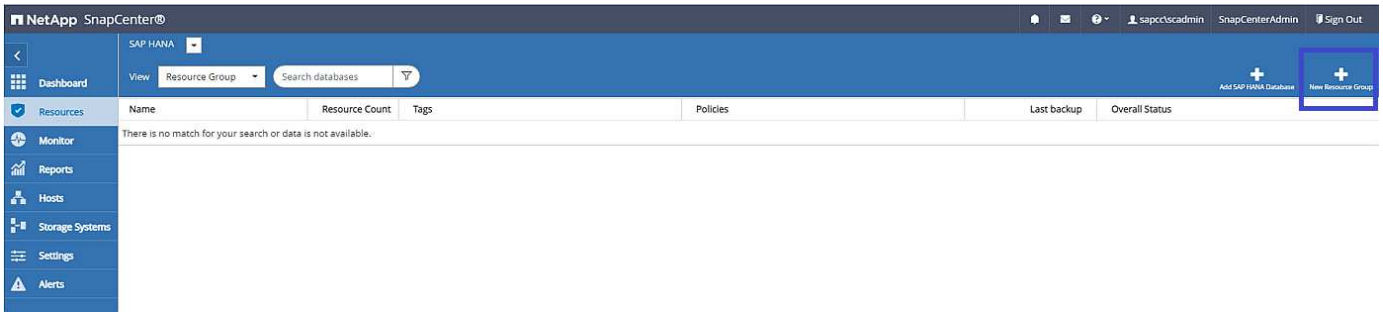


追加の自動検出ステップが実行され、 SnapCenter にリソースの詳細が表示されます。SnapCenter 4.6 では、システムレプリケーションのステータスとセカンダリサーバがこのビューに表示されます。

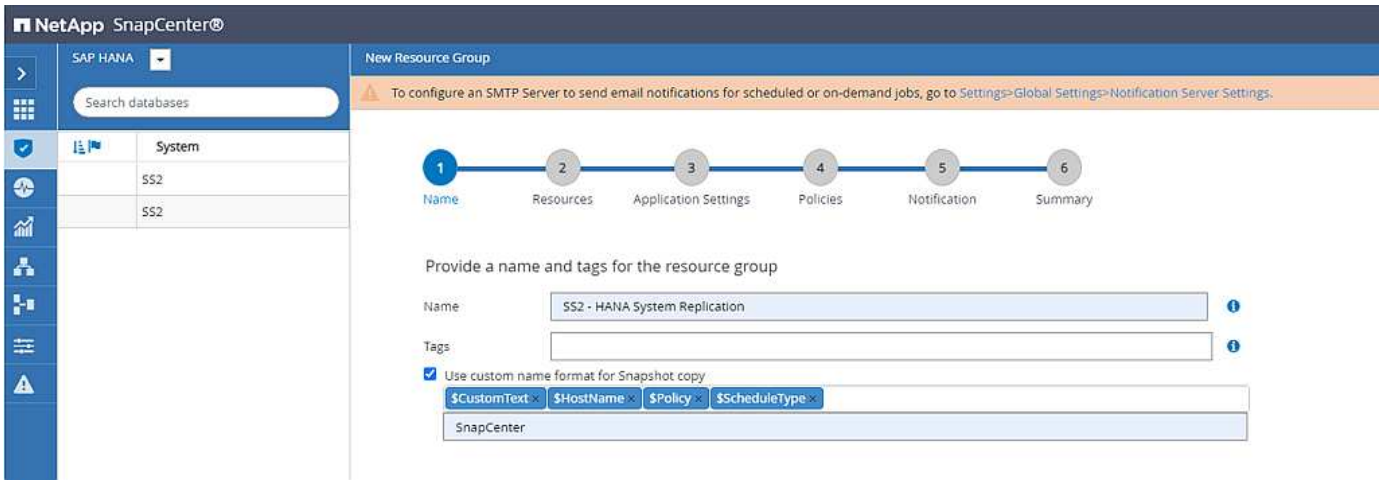


2 つ目の HANA リソースに対して同じ手順を実行すると、自動検出プロセスが完了し、両方の HANA リソースが SnapCenter で構成されます。

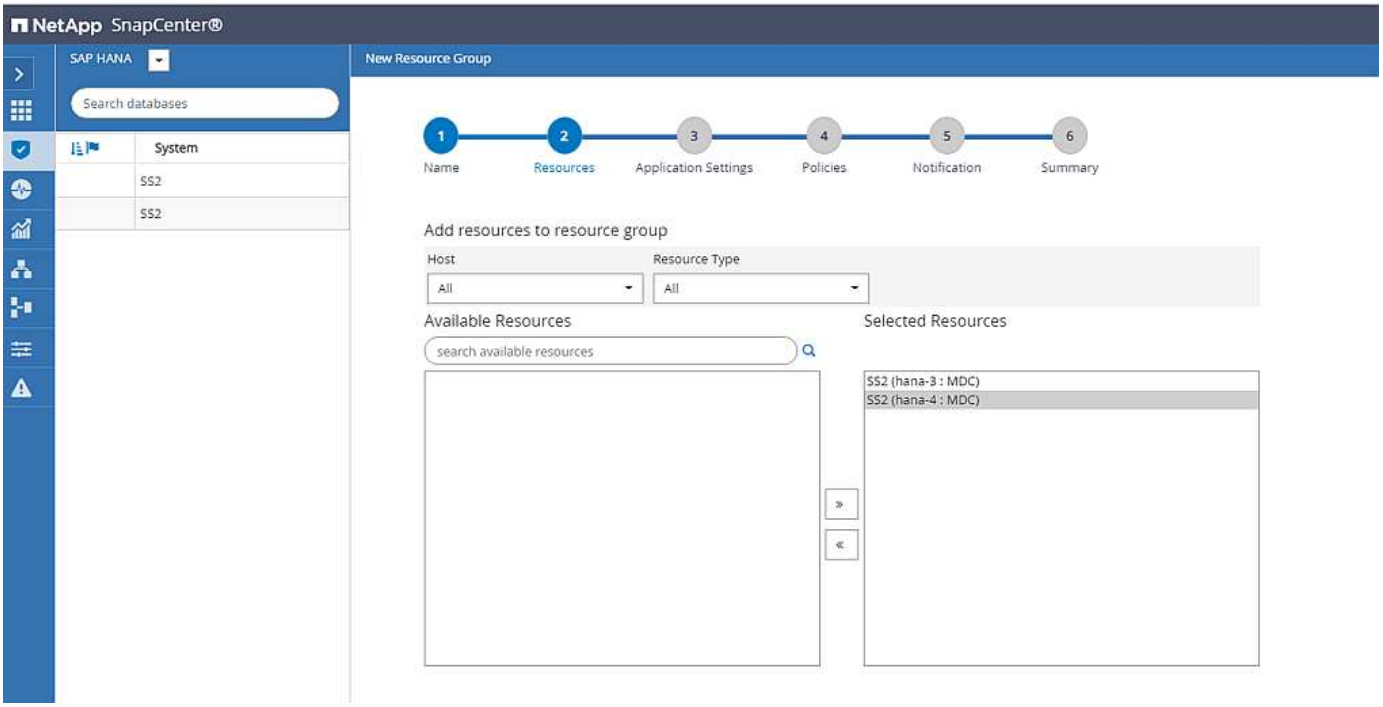
HANA システムレプリケーションを有効にしたシステムでは、両方の HANA リソースを含む SnapCenter リソースグループを設定する必要があります。



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。

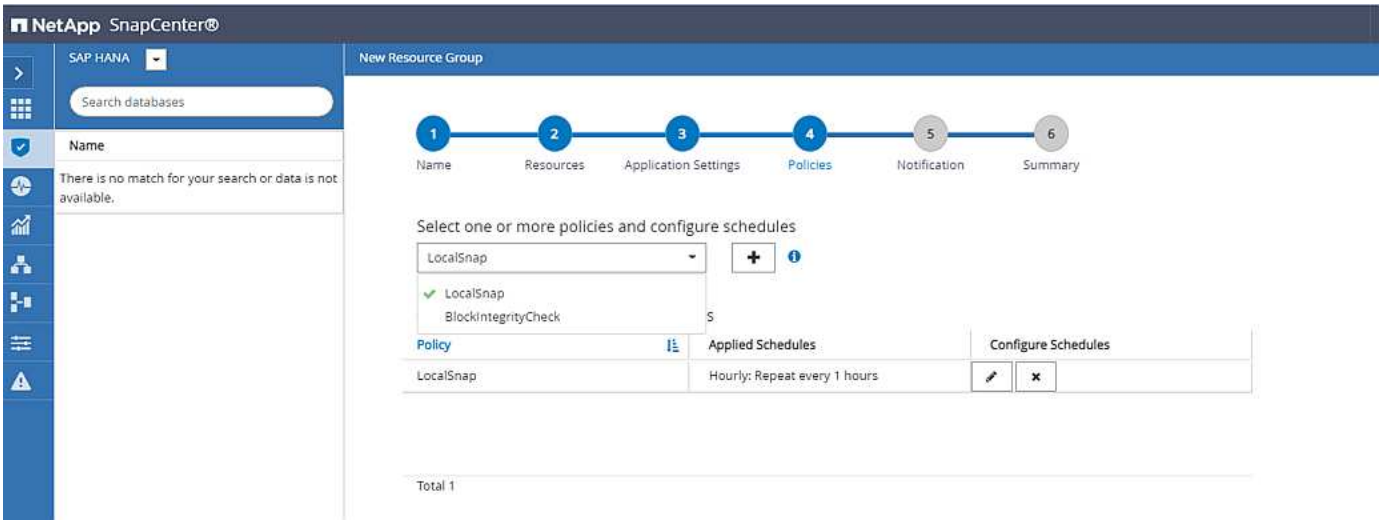


リソースグループに両方の HANA ホストを追加する必要があります。

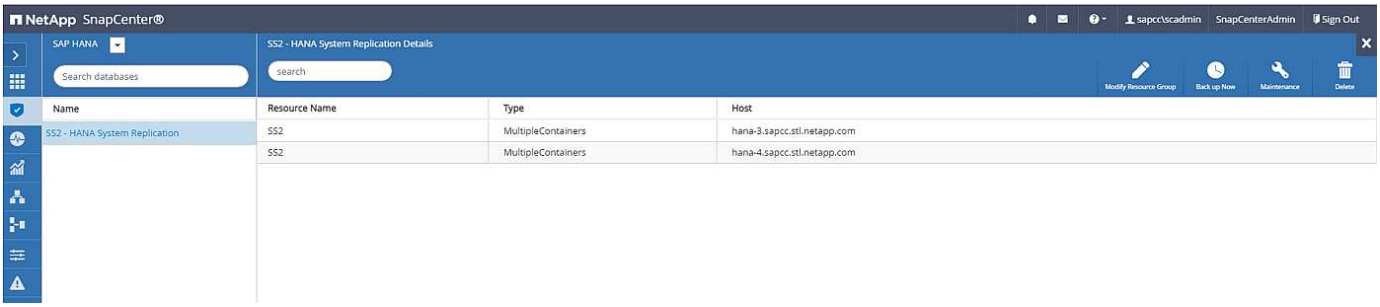


リソースグループにはポリシーとスケジュールが設定されます。

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。

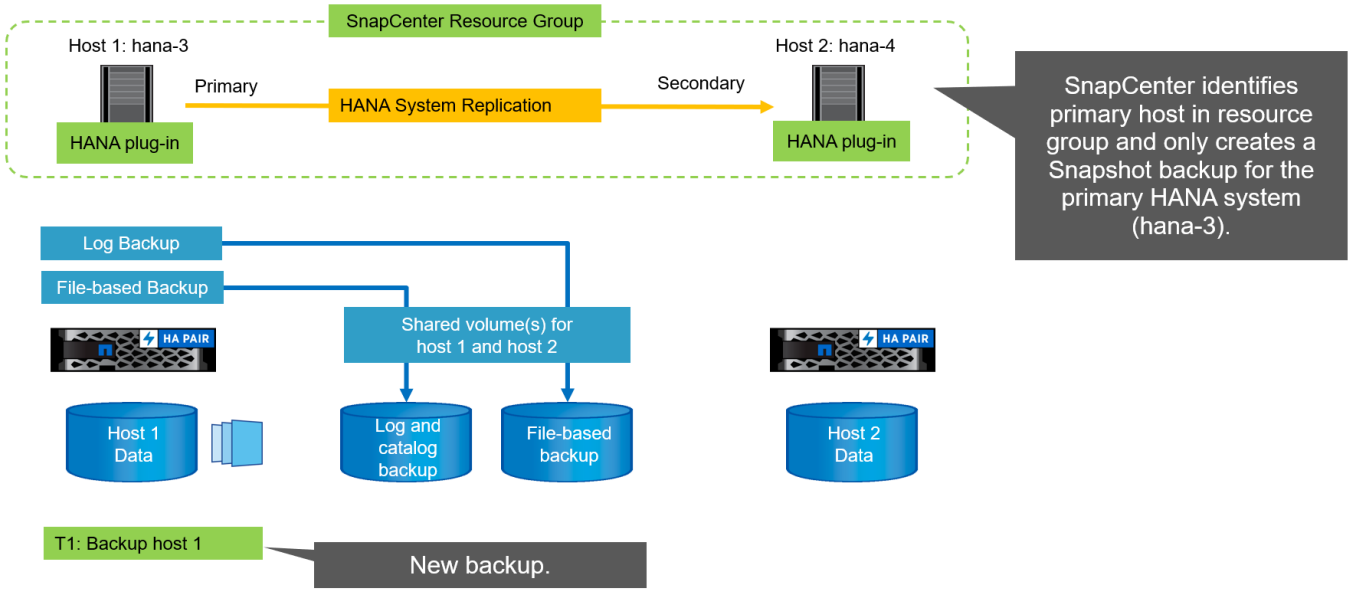


これでリソースグループの設定が終了し、バックアップを実行できるようになります。

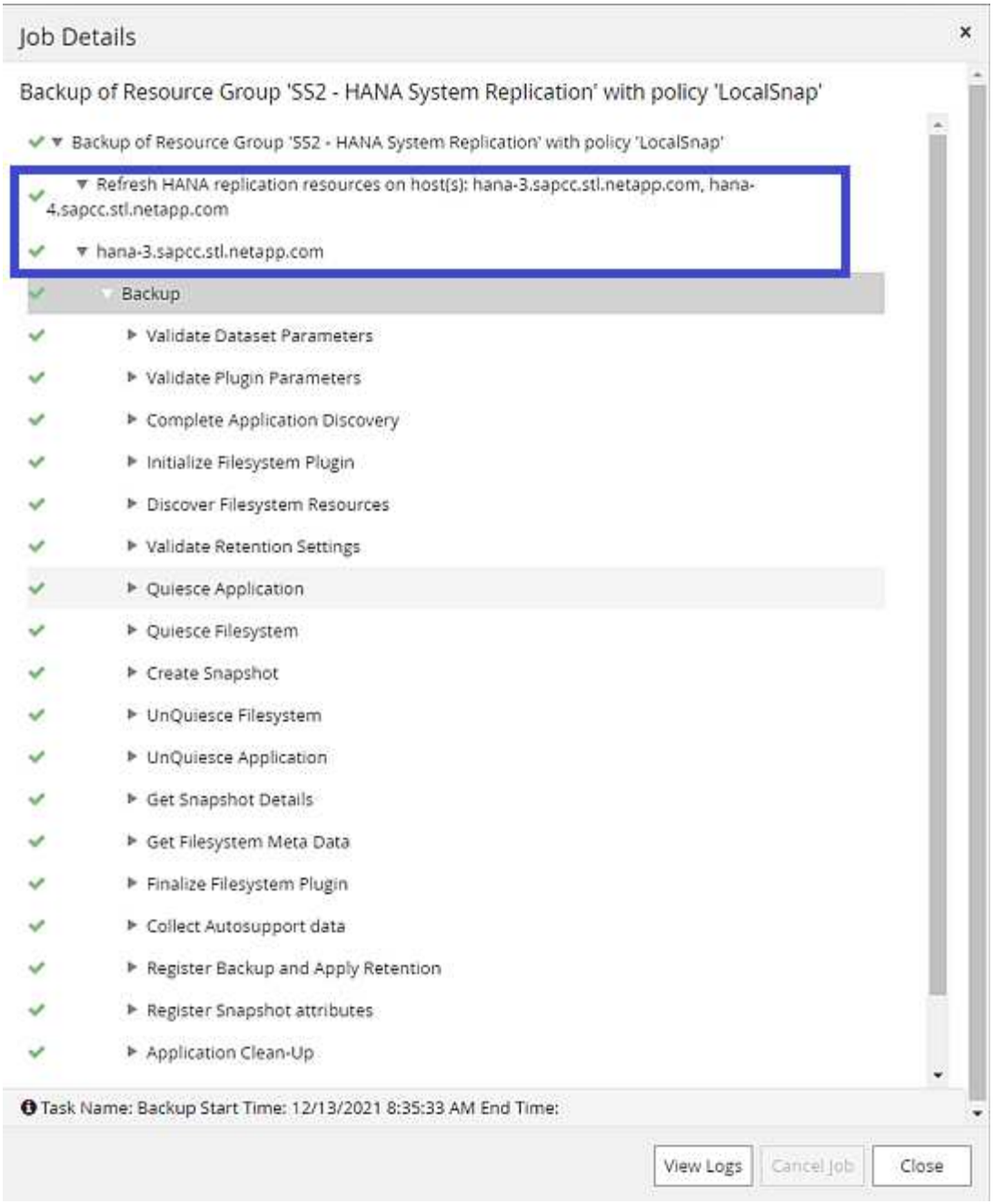


Snapshot のバックアップ処理

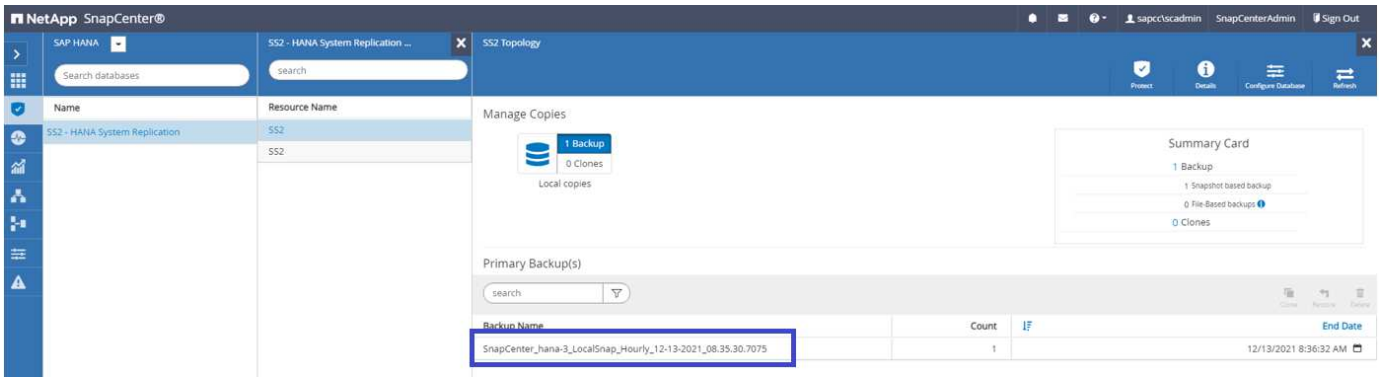
リソースグループのバックアップ処理が実行されると、 SnapCenter はどのホストがプライマリであるかを識別し、プライマリホストでのみバックアップをトリガーします。つまり、プライマリホストのデータボリュームのみが Snapshot されます。この例では、 HANA 3 が現在のプライマリホストであり、このホストでバックアップが実行されています。



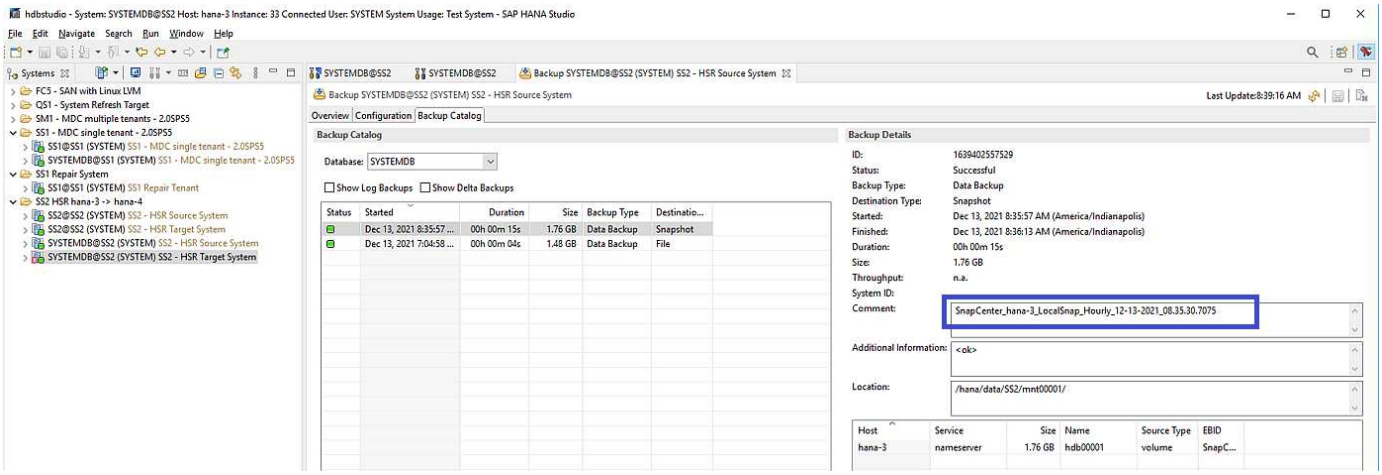
SnapCenter ジョブログには、識別処理と、現在のプライマリホスト HANA でのバックアップの実行が表示されます。



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。

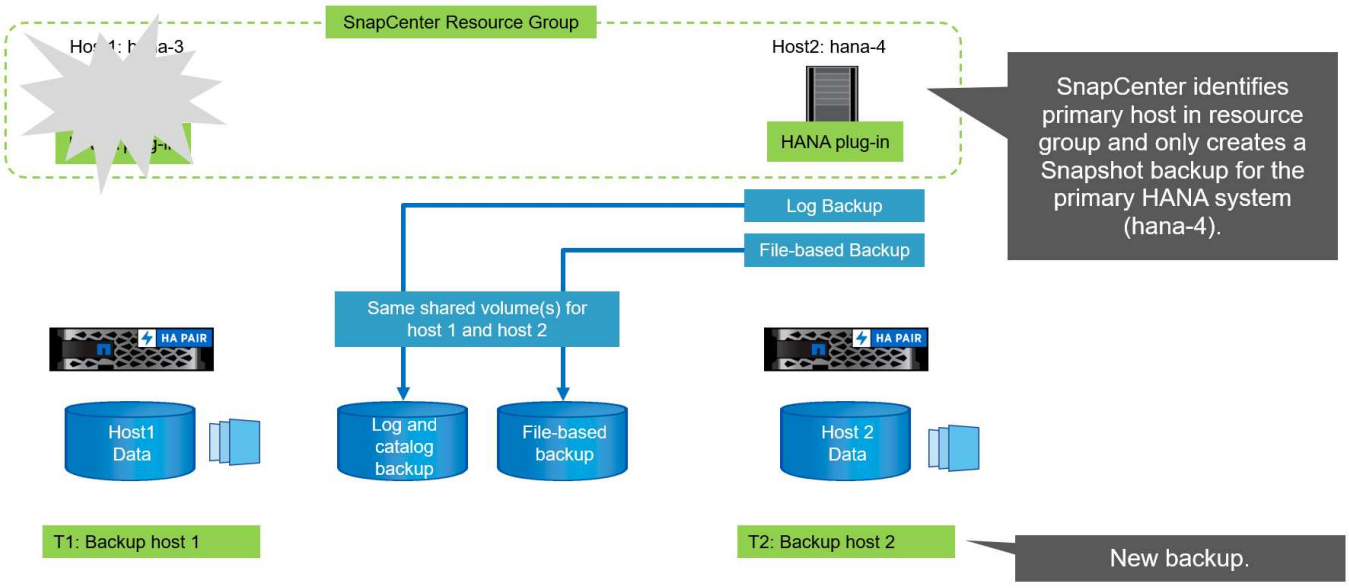


HANA のバックアップカタログにも同じ Snapshot バックアップが表示されます。

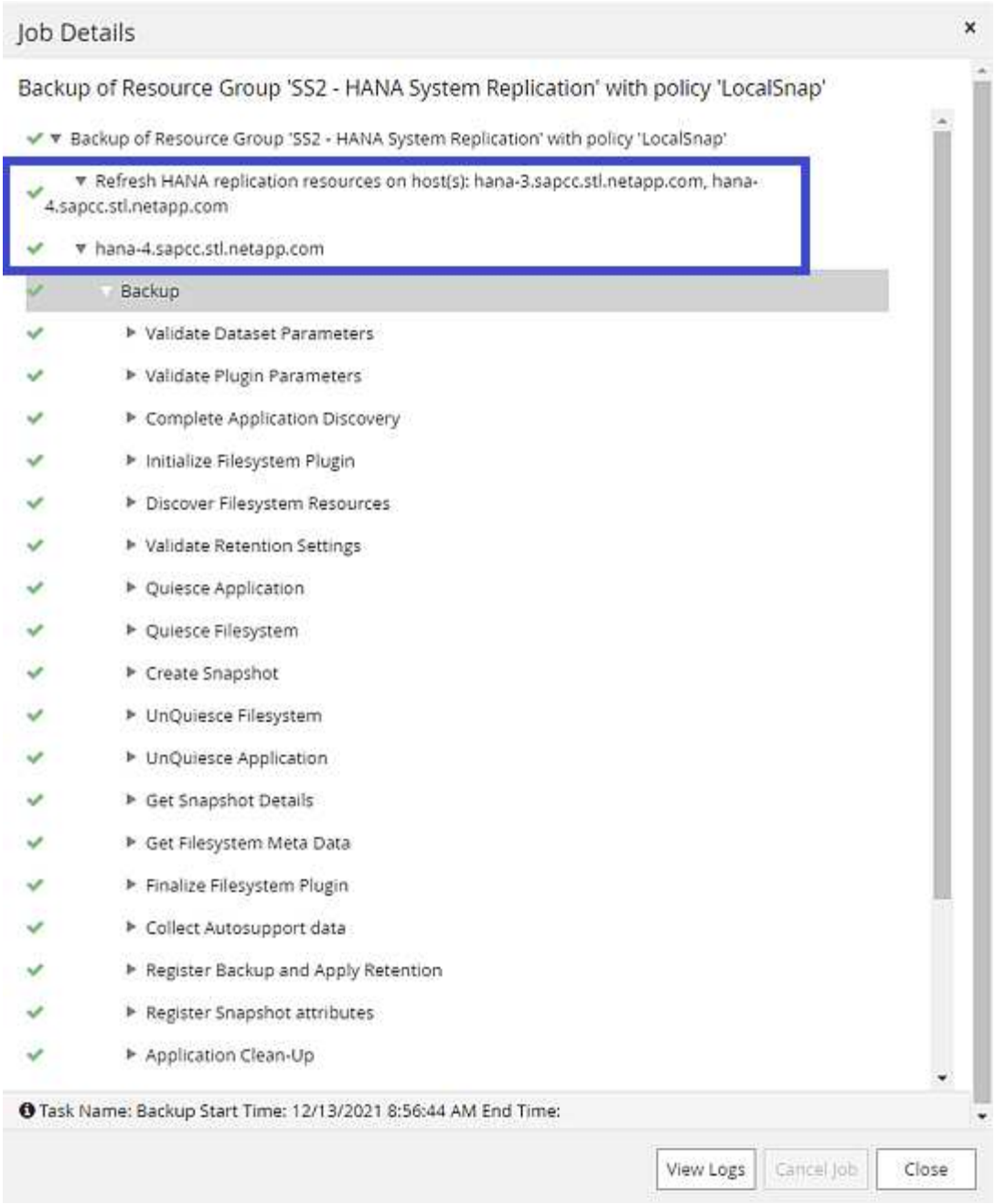


テイクオーバー処理が実行されると、それ以降の SnapCenter バックアップで元のセカンダリホスト（ Hana-4 ）がプライマリとして識別され、 Hana-4 でバックアップ処理が実行されるようになります。ここでも、新しいプライマリホスト（ HANA - 4 ）のデータボリュームのみが Snapshot されています。

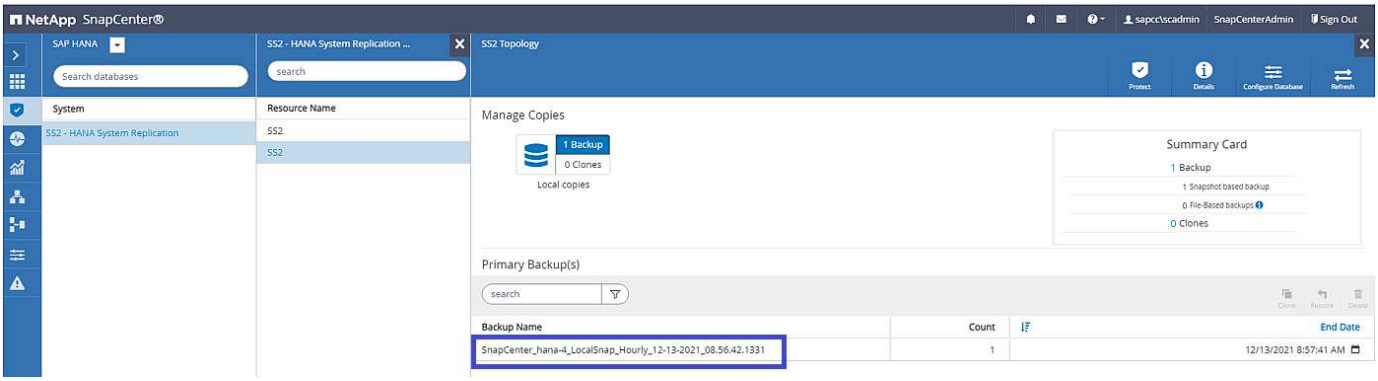
SnapCenter 識別ロジックで対応しているのは、 HANA ホストがプライマリとセカンダリの関係にあるシナリオと、 HANA ホストの 1 つがオフラインになっているシナリオだけです。



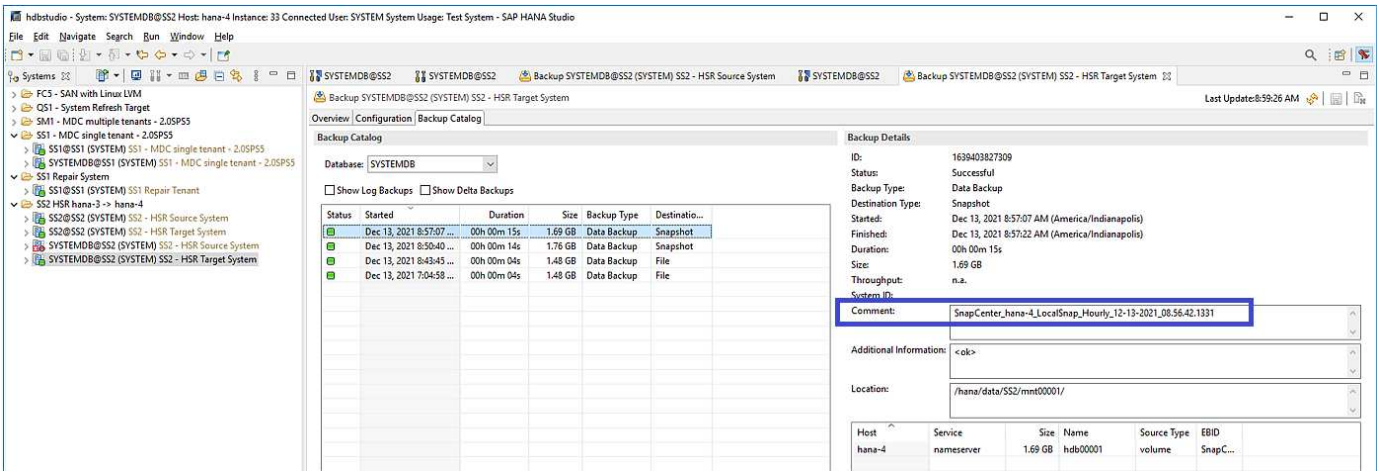
SnapCenter ジョブログには、識別処理と、現在のプライマリホスト HANA でのバックアップの実行が表示されます。



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。

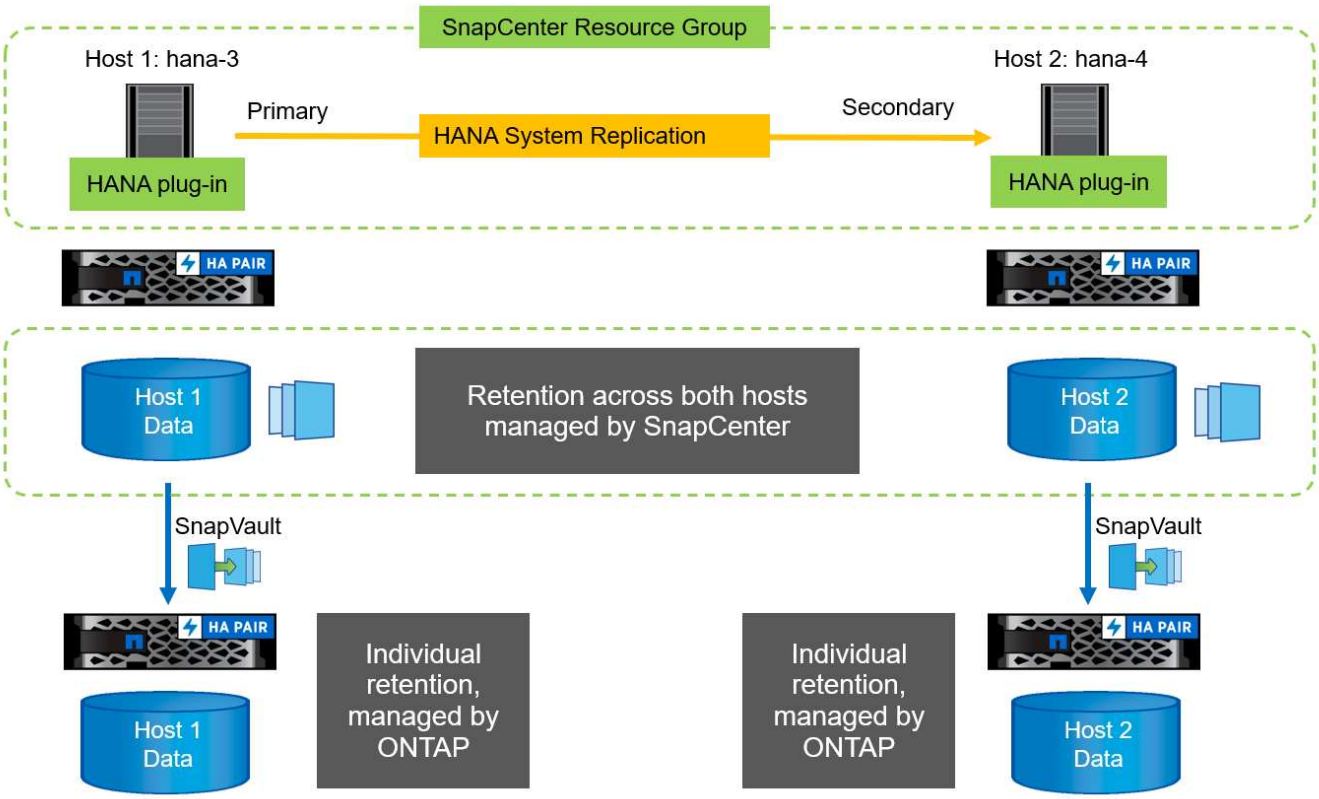
SnapVault レプリケーション

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。



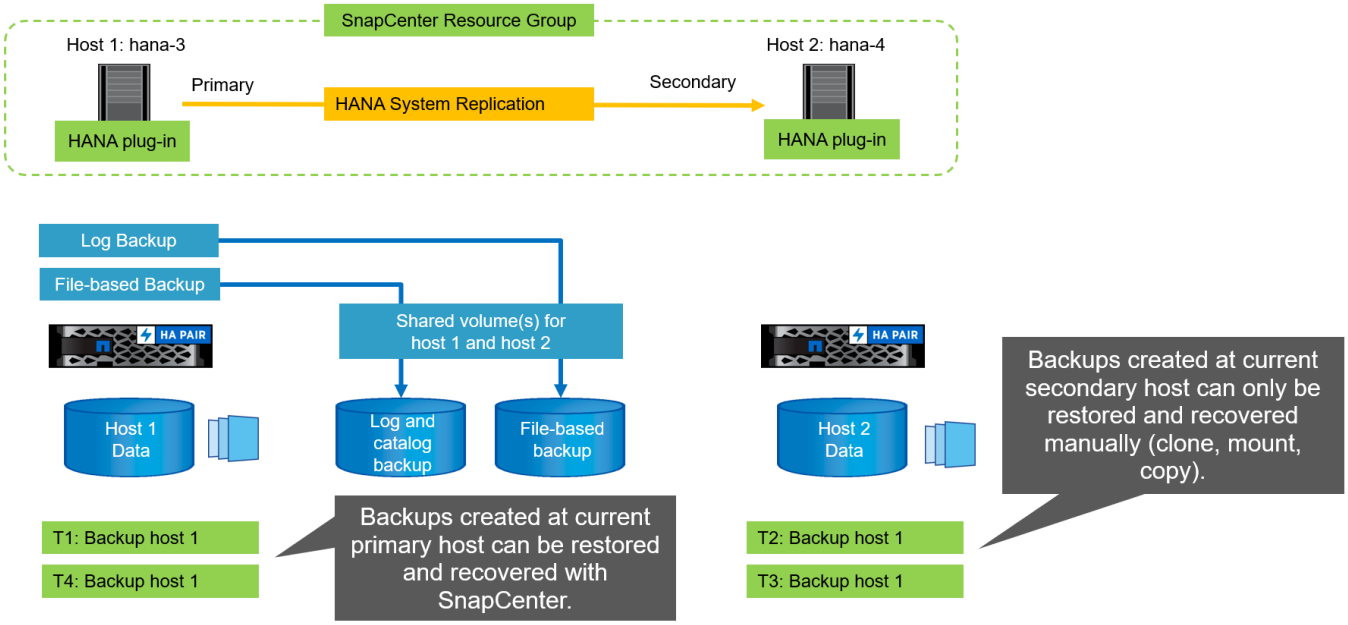
保持管理

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、特定のシナリオで手動による操作が必要です。詳細については、を参照してください [SnapVault Replication]。

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ください "TR-4614 ： 『 SAP HANA Backup and Recovery with SnapCenter 』 "。

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、を参照してください "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"。

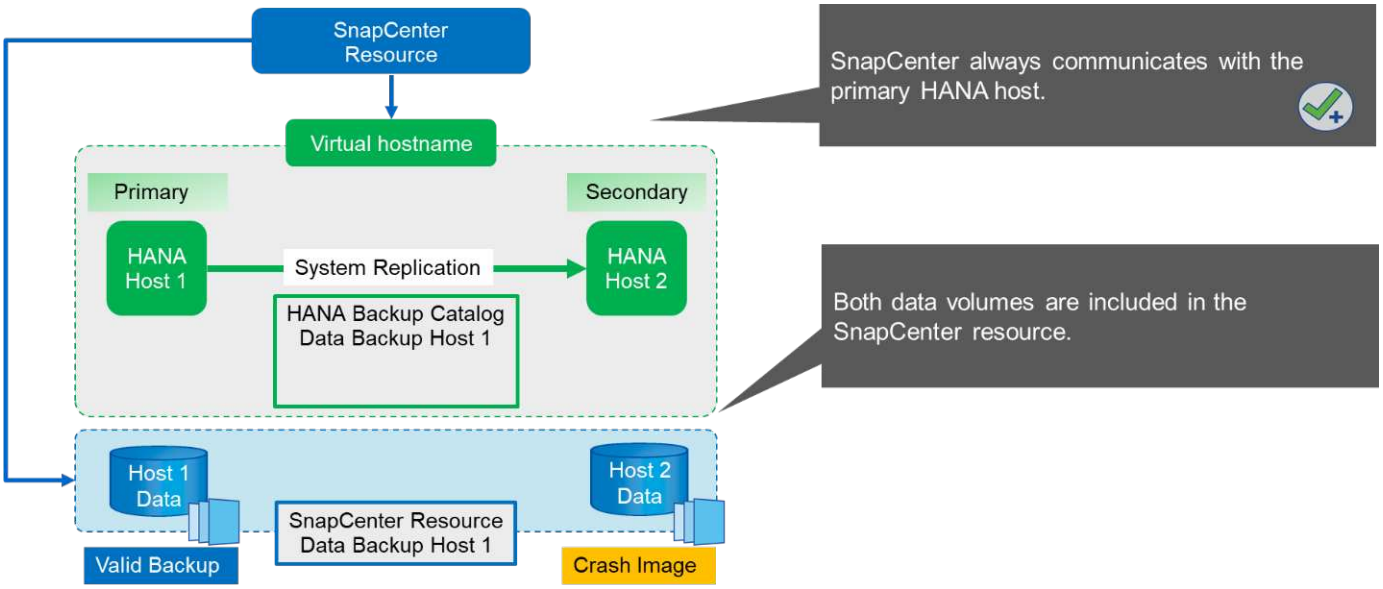
単一のリソースを使用する SnapCenter 構成

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。

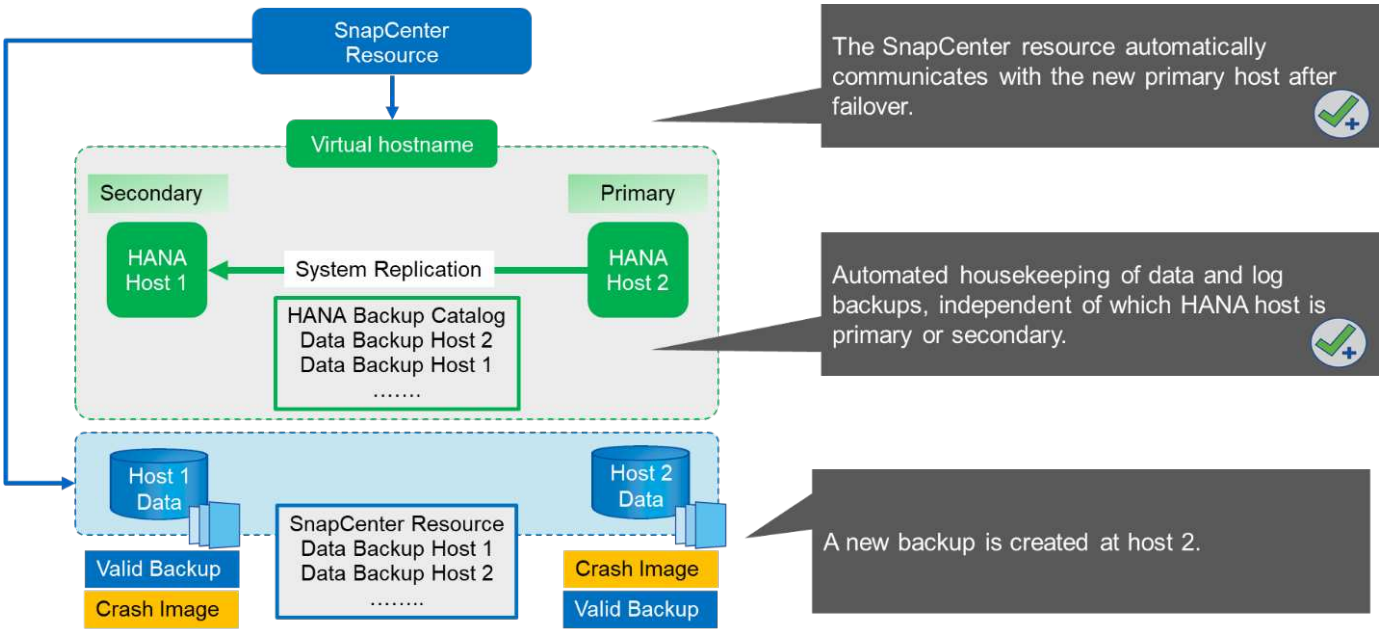
ホスト 1 をプライマリホストとするバックアップを実行すると、データベースと整合性のある Snapshot バックアップがホスト 1 のデータボリュームに作成されます。ホスト 2 のデータボリュームは SnapCenter リソースの一部であるため、このボリュームに対してもう 1 つの Snapshot コピーが作成されます。この Snapshot コピーはデータベースの整合性を維持するのではなく、セカンダリホストのクラッシュイメージにすぎません。

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。

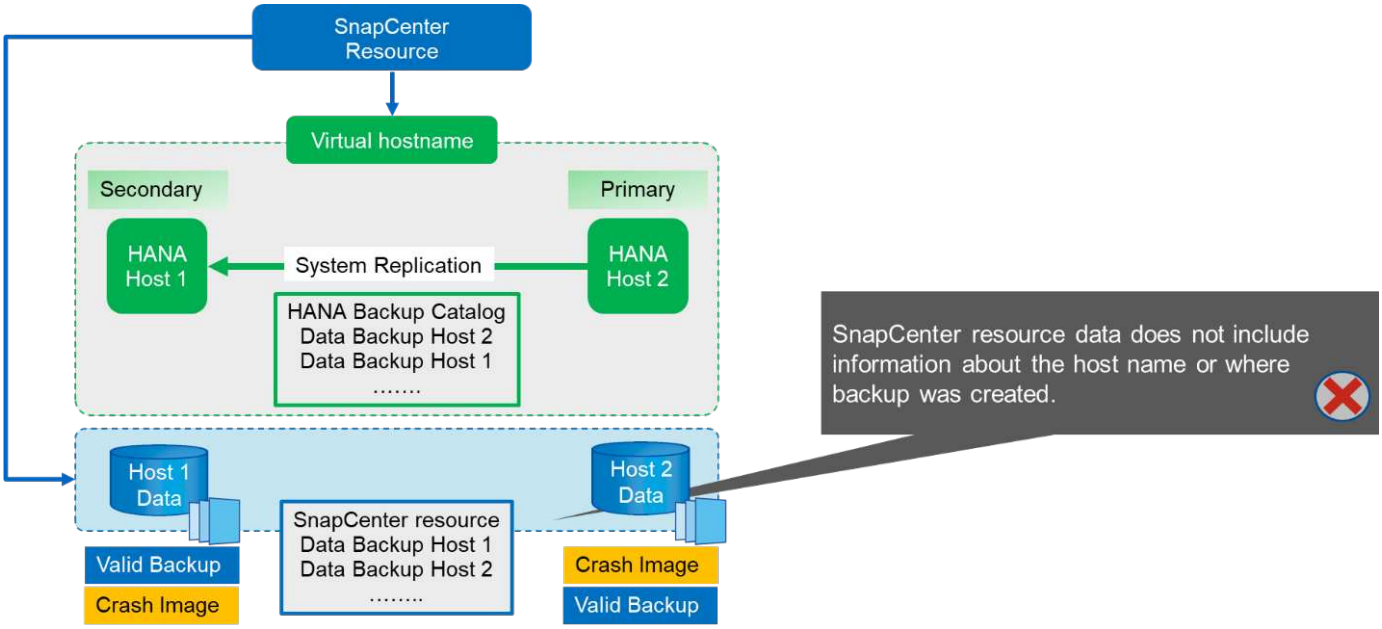
不要なデータバックアップやログバックアップは、定義された SnapCenter 保持ポリシーに基づいて削除され、プライマリまたはセカンダリのホストに関係なく、バックアップは削除されます。



の項で説明したように "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、リストアする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。

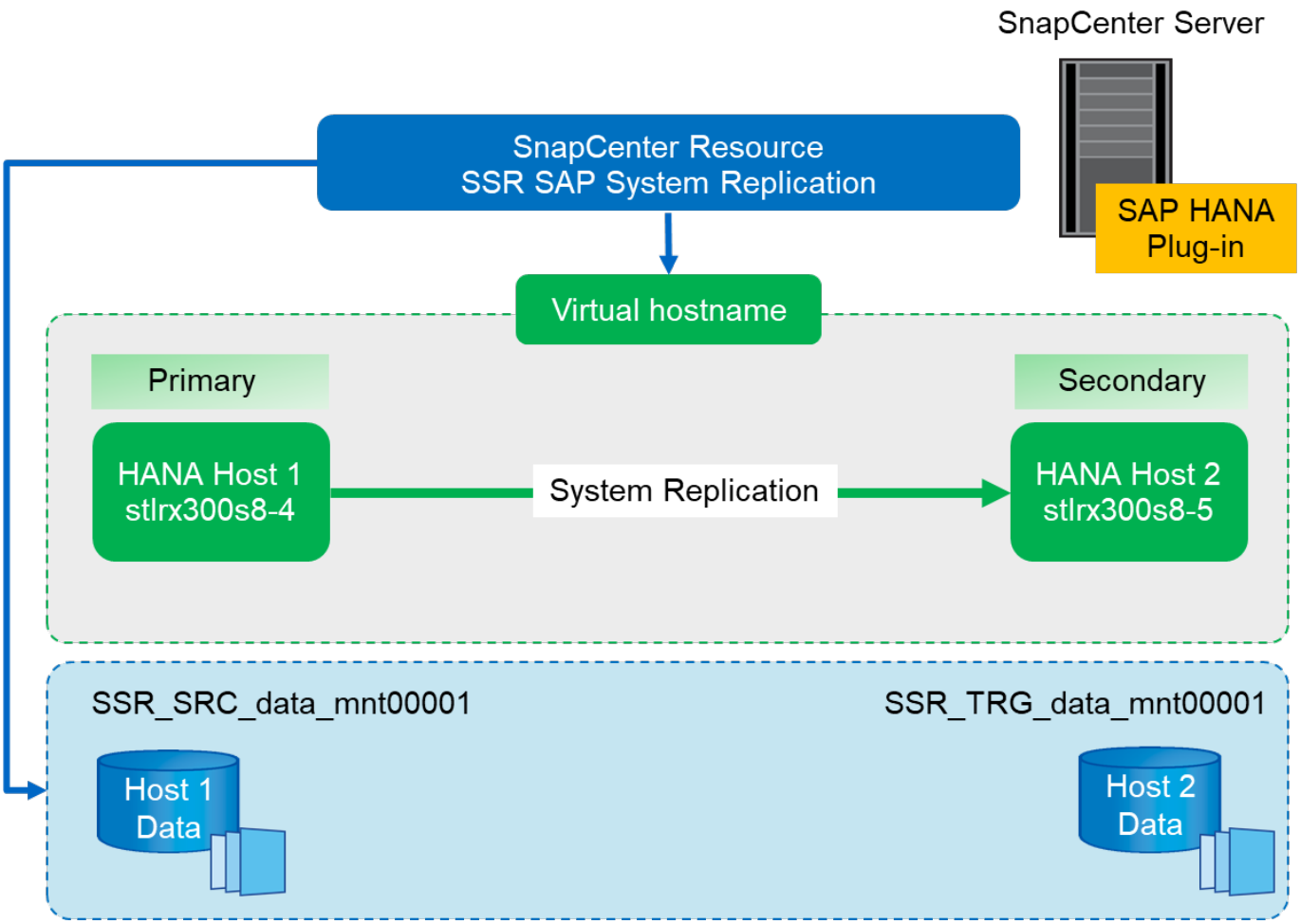
シングルリソースの SnapCenter 構成では、バックアップがどこに作成されたかが SnapCenter で認識されません。そのため、 SnapCenter のバックアップワークフローにバックアップ前のスクリプトを追加して、現在プライマリ SAP HANA ホストになっているホストを特定することを推奨します。

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。



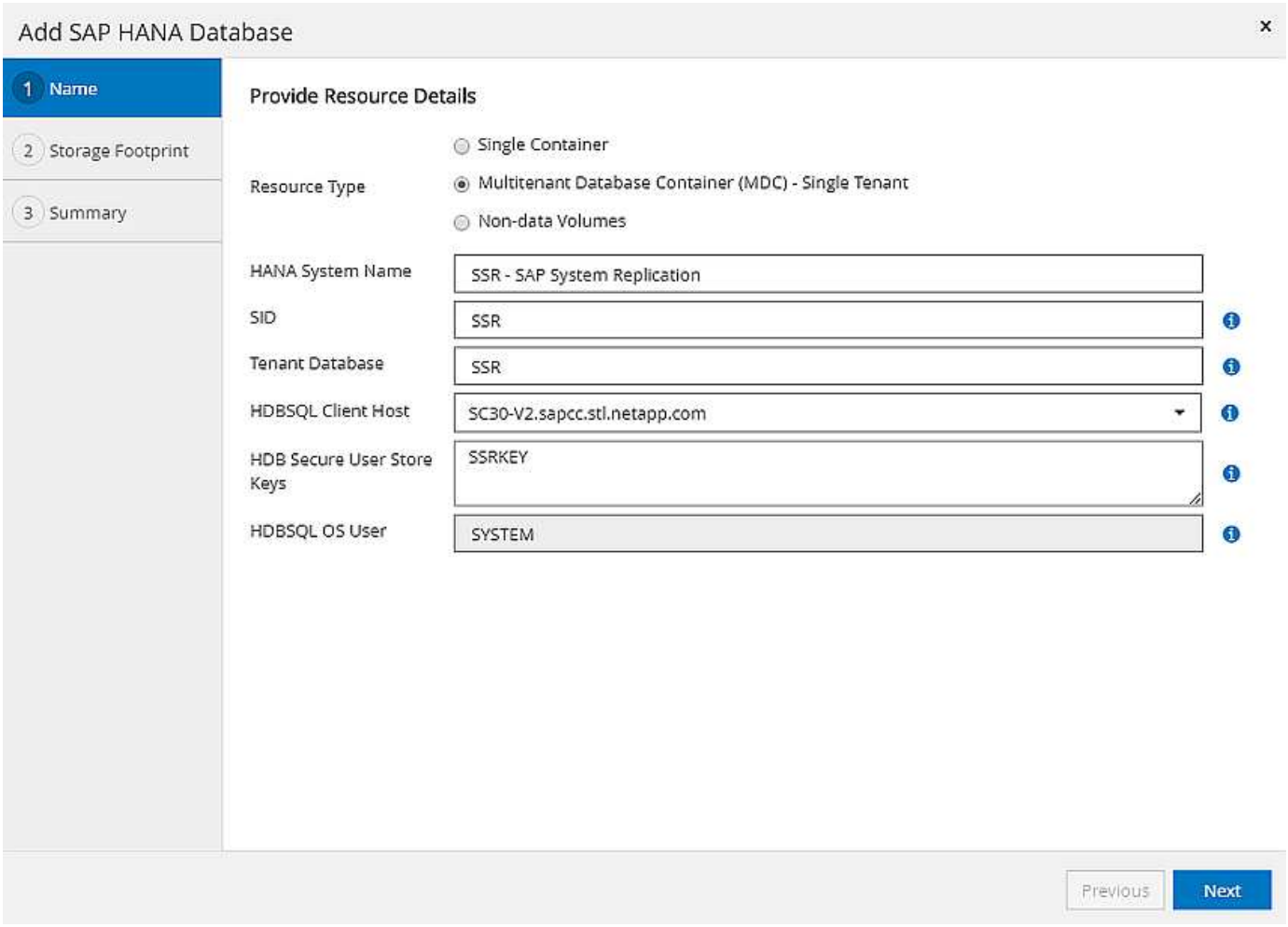
どの SAP HANA ホストがプライマリであっても、 1 つのホストがダウンしている場合でもバックアップ処理を実行するには、 SnapCenter SAP HANA プラグインを中央のプラグインホストに導入する必要があります。今回のラボ環境では、 SnapCenter サーバを中央プラグインホストとして使用し、 SnapCenter サーバに SAP HANA プラグインを導入しました。

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。

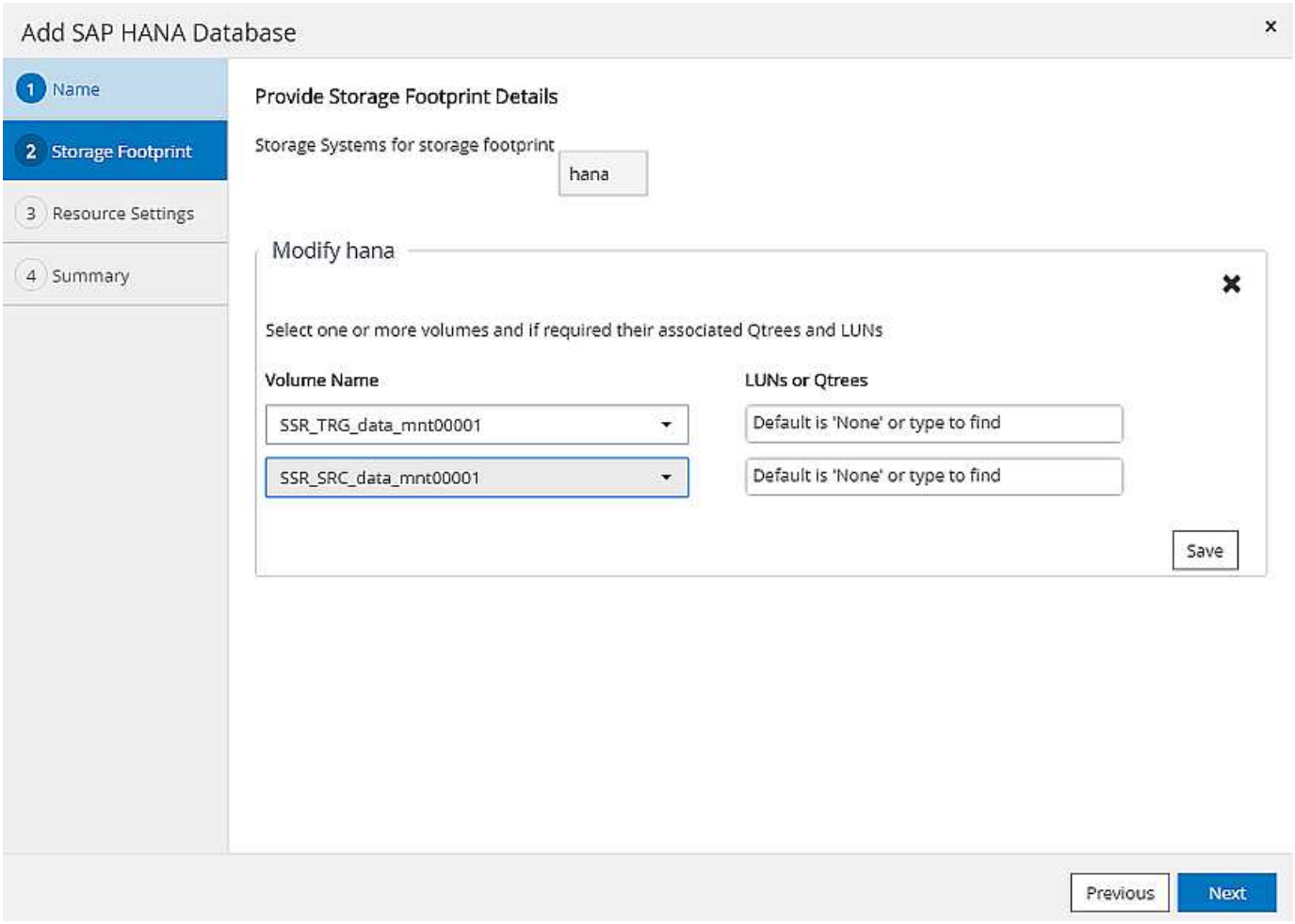
```
hdbuserstore.exe -u SYSTEM set SSRKEY ssr-vip:31013 SNAPCENTER <password>
```

SAP HANA プラグインの導入オプションとユーザストアの構成の詳細については、テクニカルレポート TR-4614 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 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

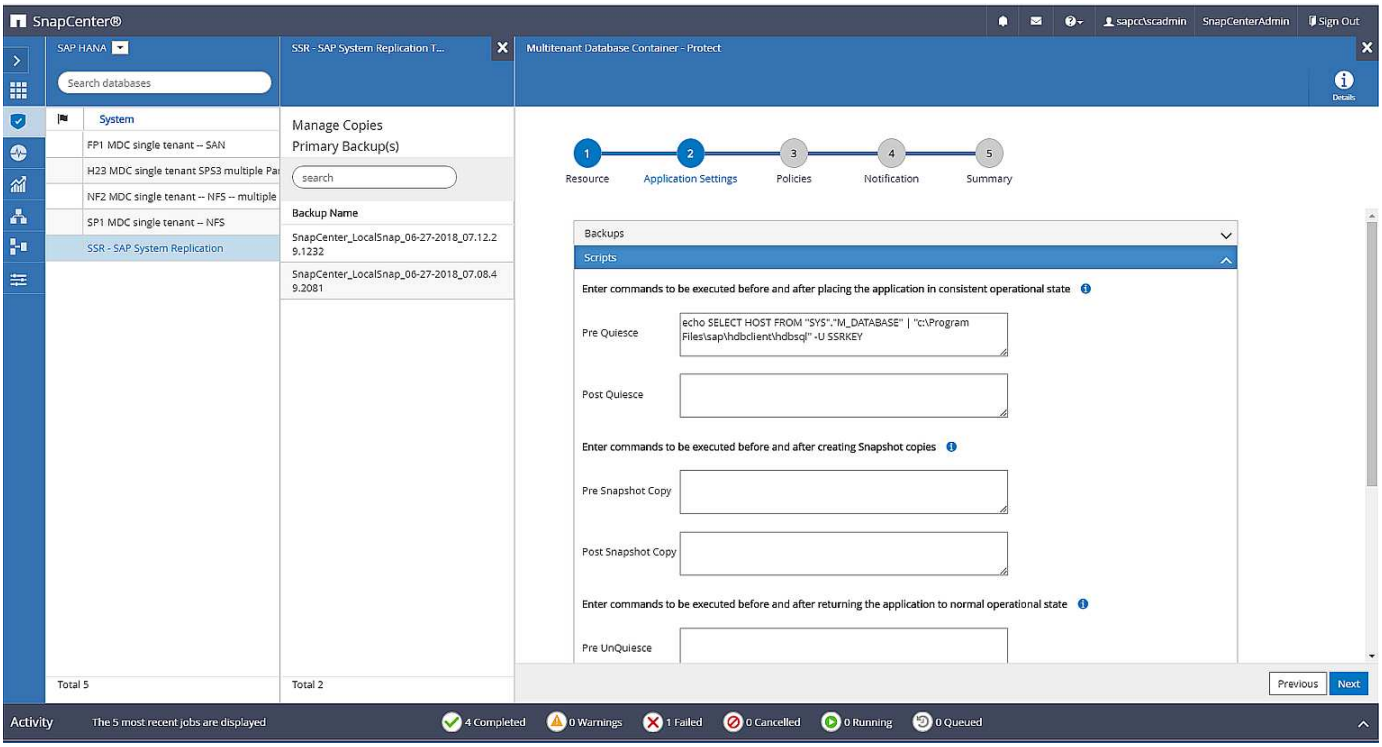


次の図に示すように、両方の SAP HANA ホストのデータボリュームがストレージ設置面積構成に含まれています。



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
```

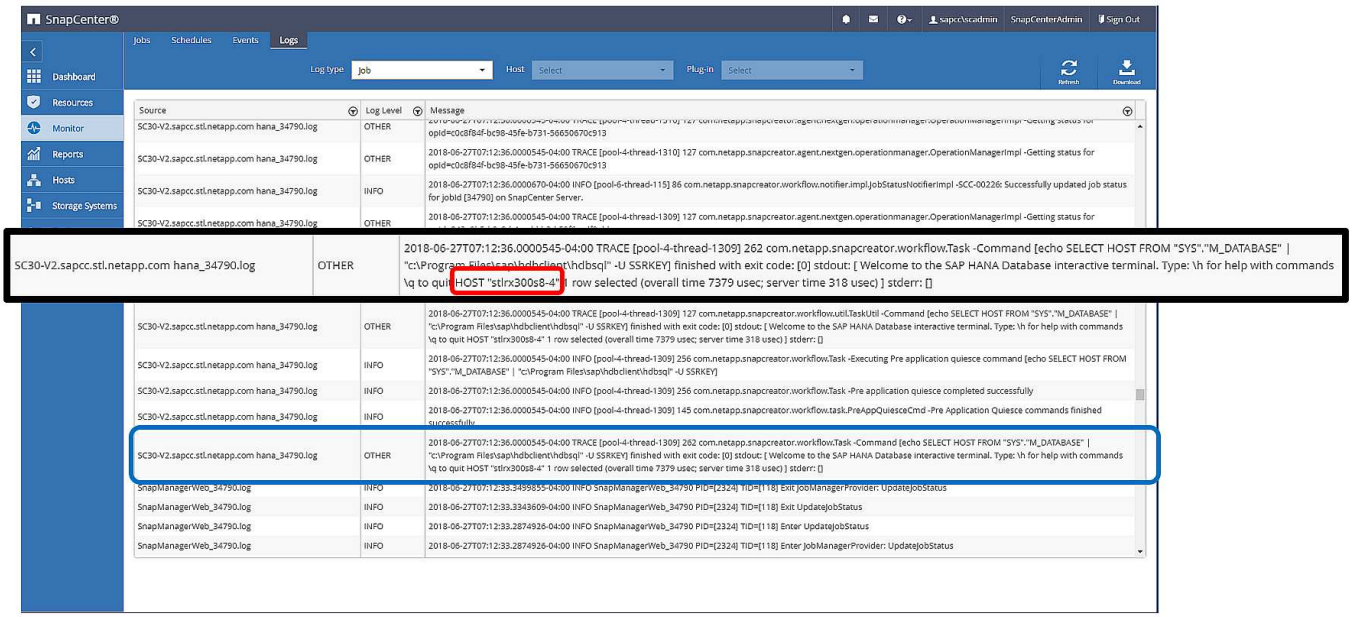


SnapCenter バックアップ処理

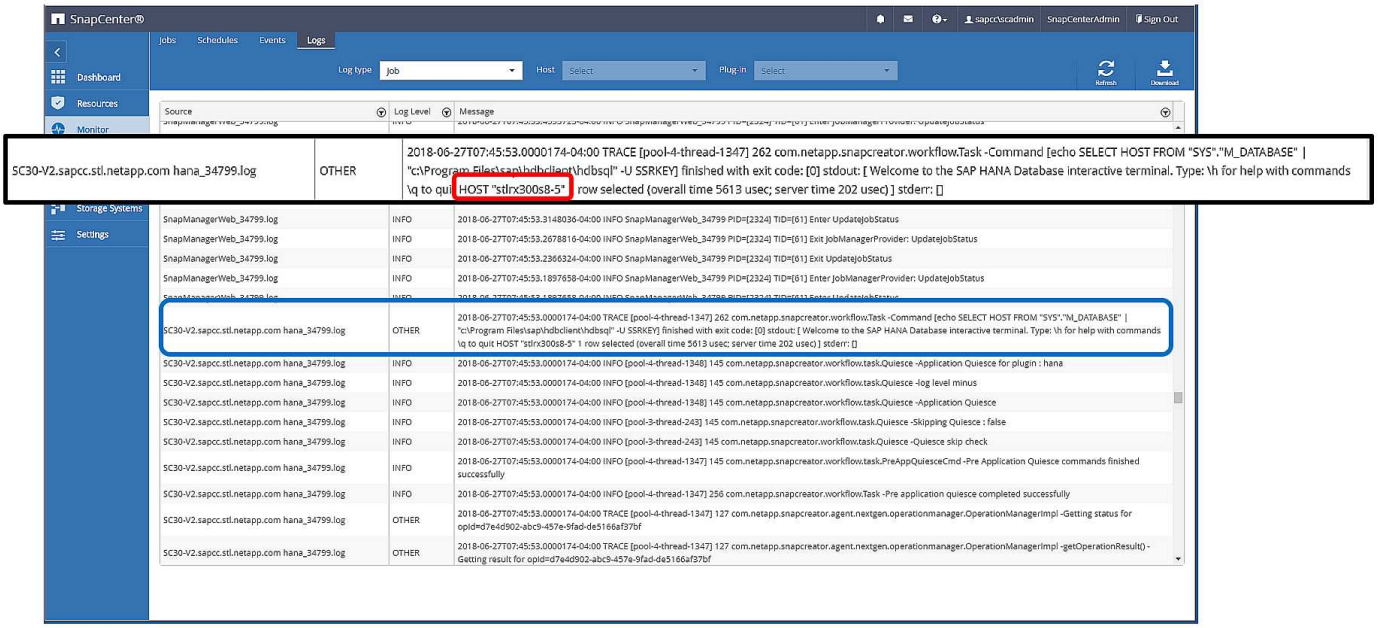
バックアップ処理が通常どおり実行されるようになりました。不要なデータバックアップとログバックアップの削除は、プライマリまたはセカンダリの SAP HANA ホストとは無関係に実行されます。

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。

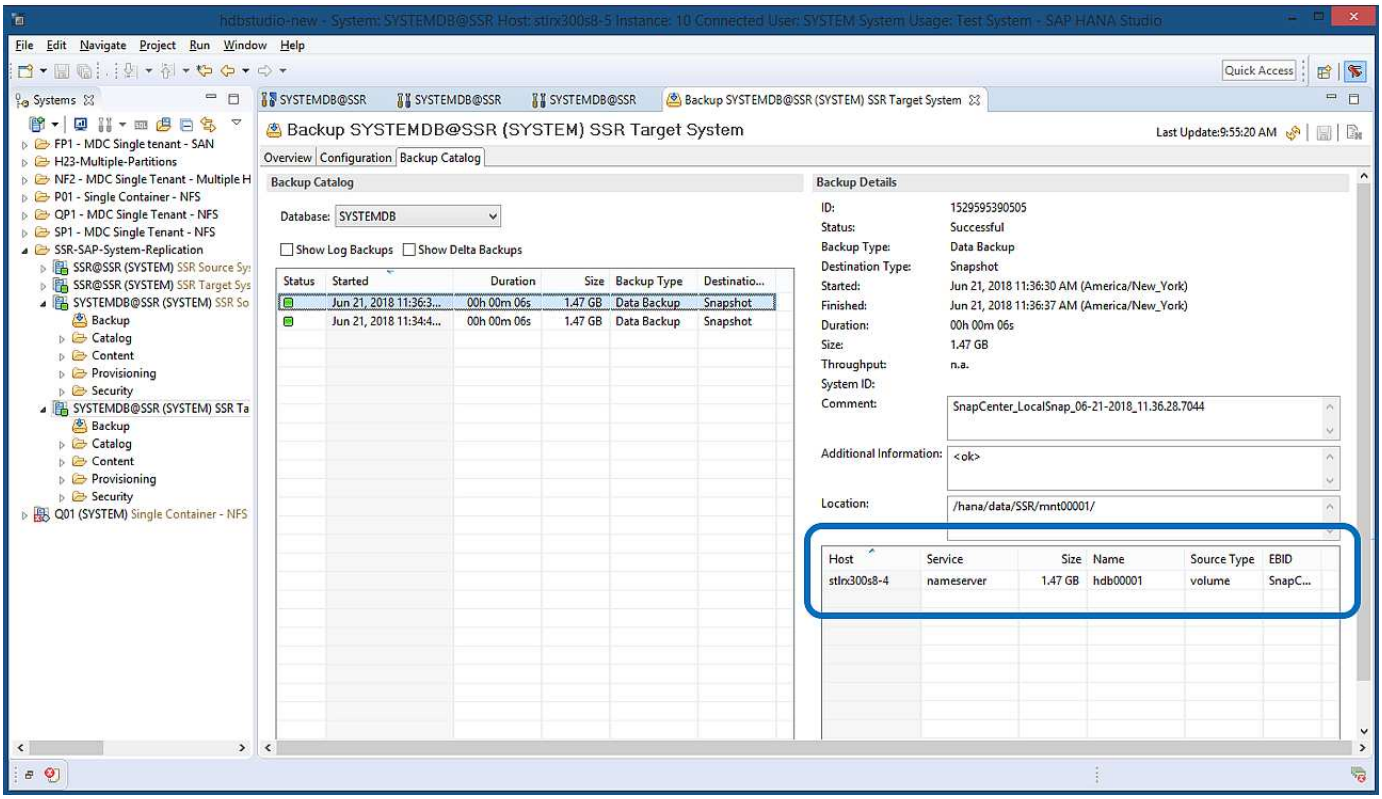


この図は、ホスト 2 がプライマリホストであるバックアップジョブログを示しています。



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。



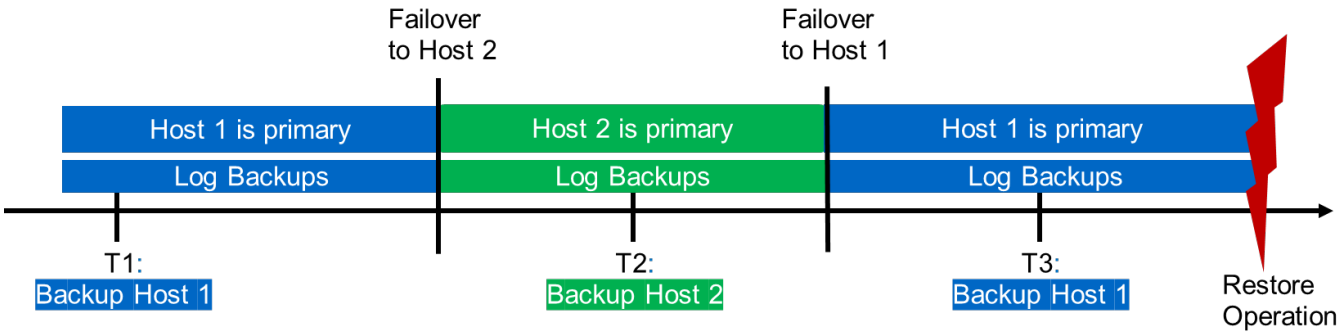
リストアとリカバリ

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

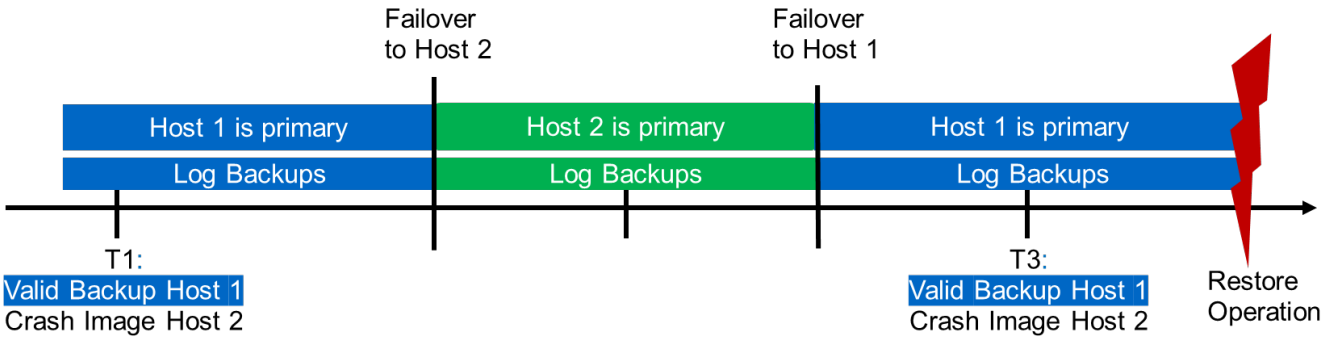
単一の SnapCenter リソース構成では、両方の SAP HANA システムレプリケーションホストの両方のストレージボリュームに Snapshot コピーが作成されます。フォワードリカバリに使用できるのは、プライマリ SAP HANA ホストのストレージボリュームに作成された Snapshot バックアップのみです。セカンダリ SAP HANA ホストのストレージボリュームに作成された Snapshot コピーは、フォワードリカバリに使用できないクラッシュイメージです。

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、を参照してください "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"。

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。

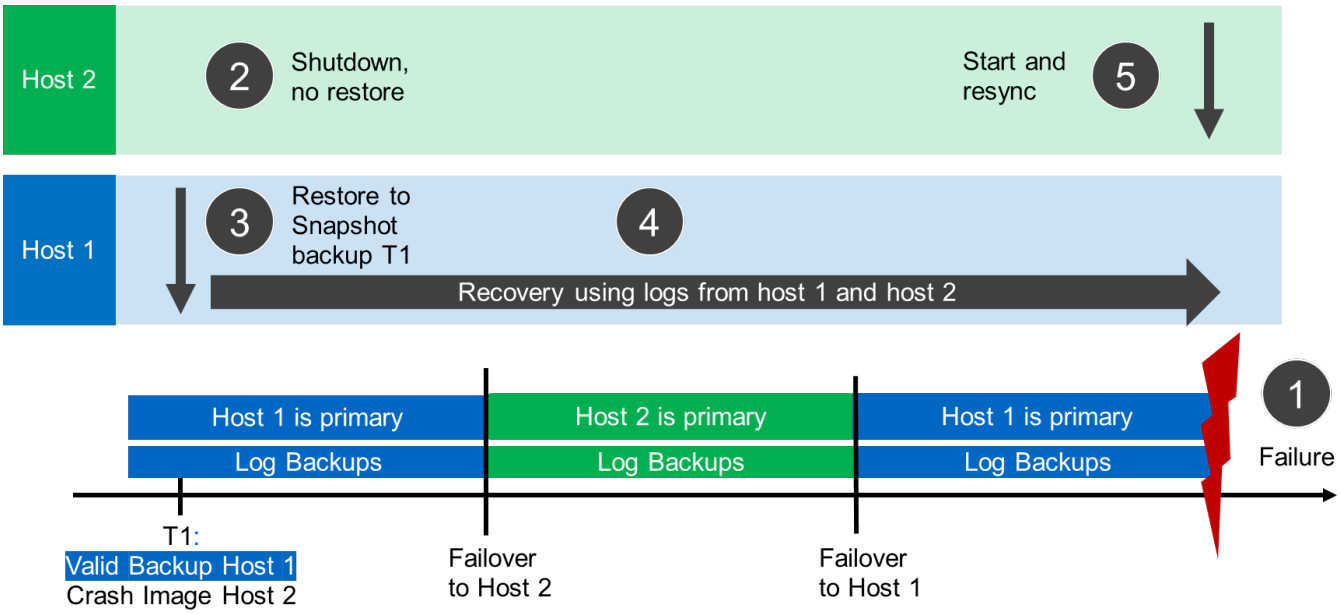


有効なバックアップの **SnapCenter** リストアのみを実行してください

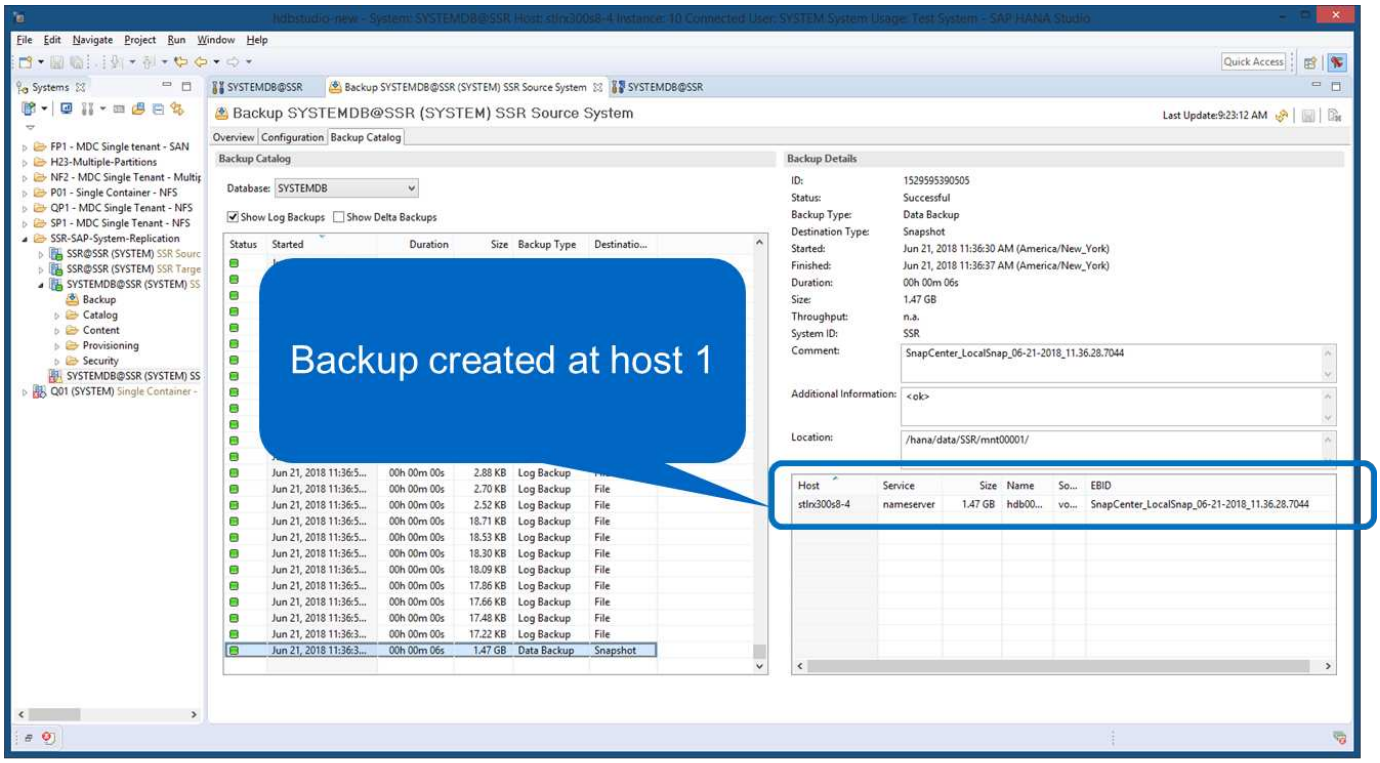
次の図に、このセクションで説明するリストアとリカバリのシナリオの概要を示します。

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。



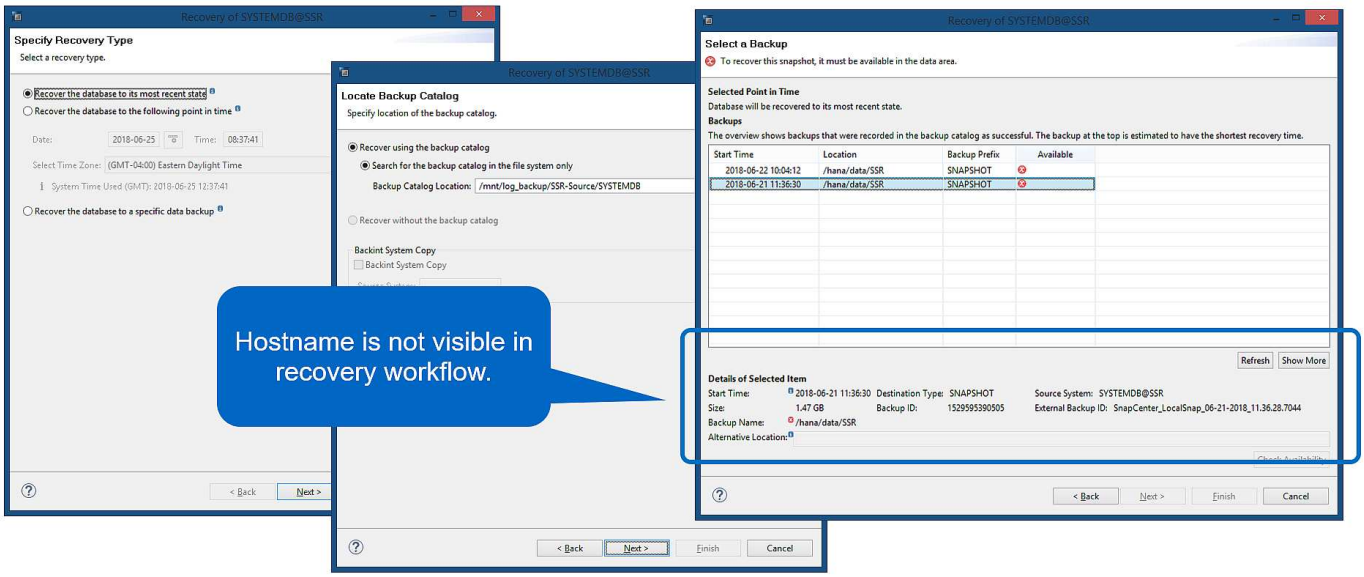
次の図は、 SAP HANA Studio の SAP HANA バックアップカタログを示しています。強調表示されたバックアップは、 T1 のホスト 1 で作成されたバックアップを示しています。



25

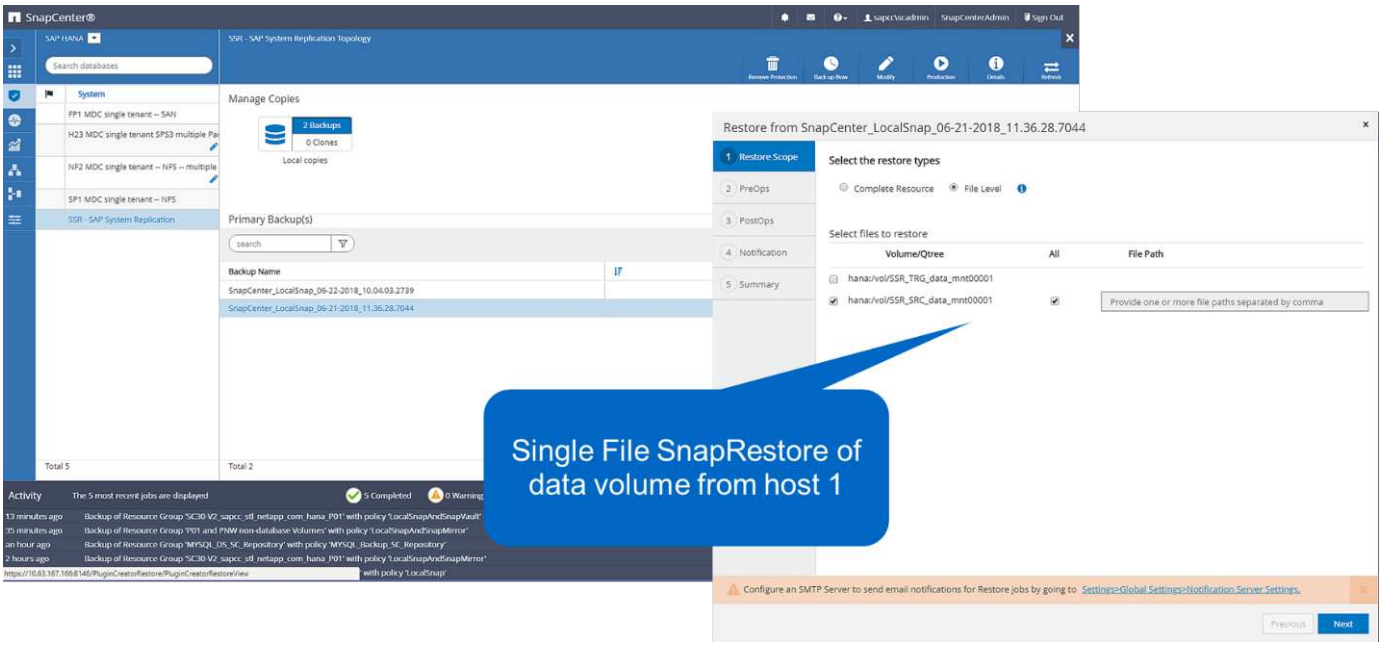
リストア処理とリカバリ処理は SAP HANA Studio で開始されます。次の図に示すように、バックアップが作成されたホストの名前はリストアとリカバリのワークフローには表示されません。

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。

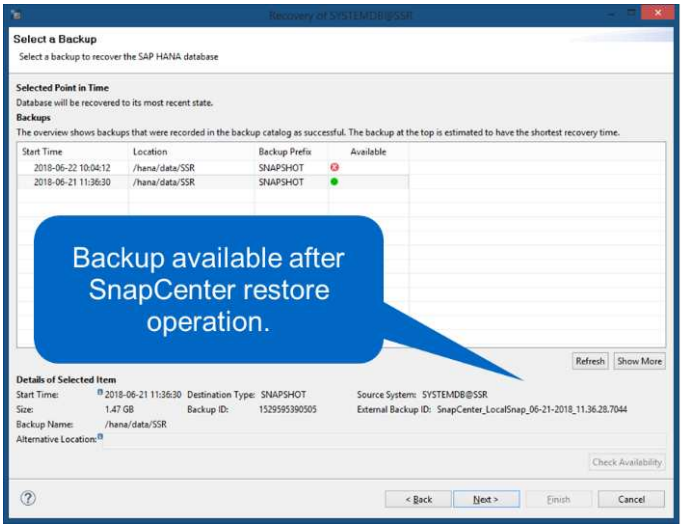


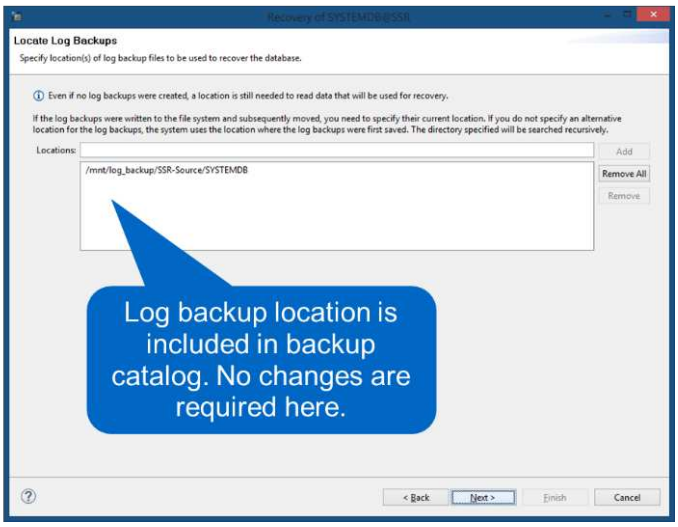
SnapCenter では、バックアップが選択され、ファイルレベルのリストア処理が実行されます。ファイルレベ

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。



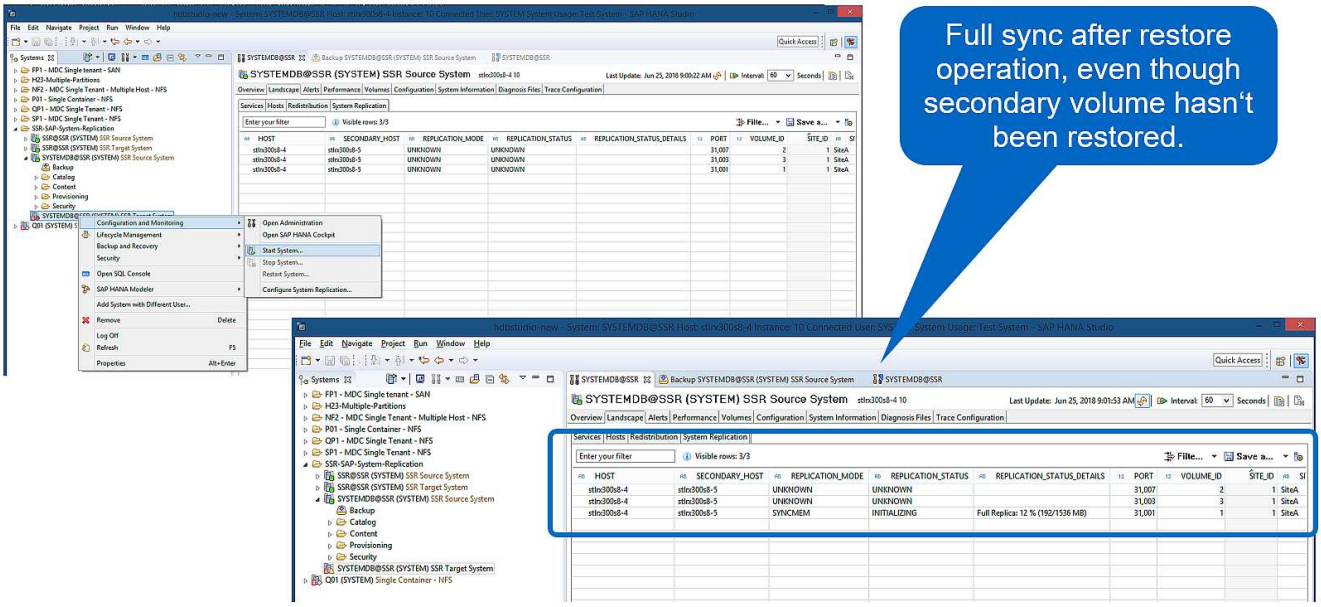
リストア処理が完了すると、 SAP HANA Studio でバックアップが緑色で強調表示されます。ホスト 1 とホスト 2 のログバックアップのファイルパスがバックアップカタログに含まれているため、追加のログバックアップの場所を入力する必要はありません。





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。

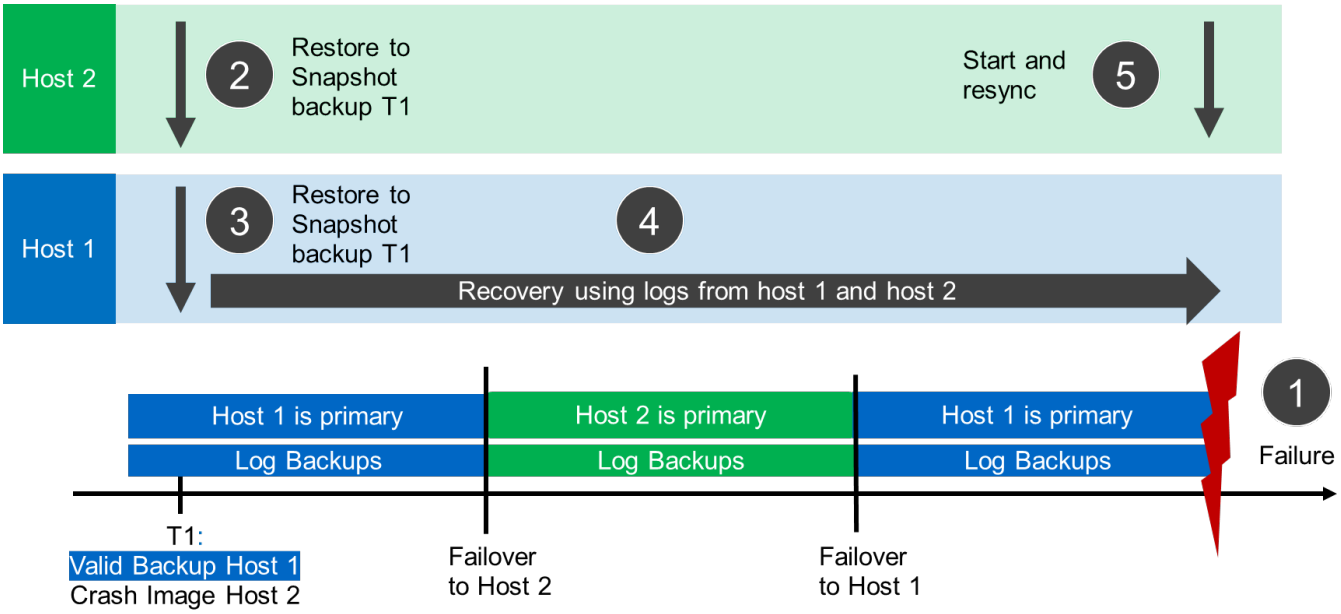


有効なバックアップとクラッシュイメージの **SnapCenter** リストア

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。

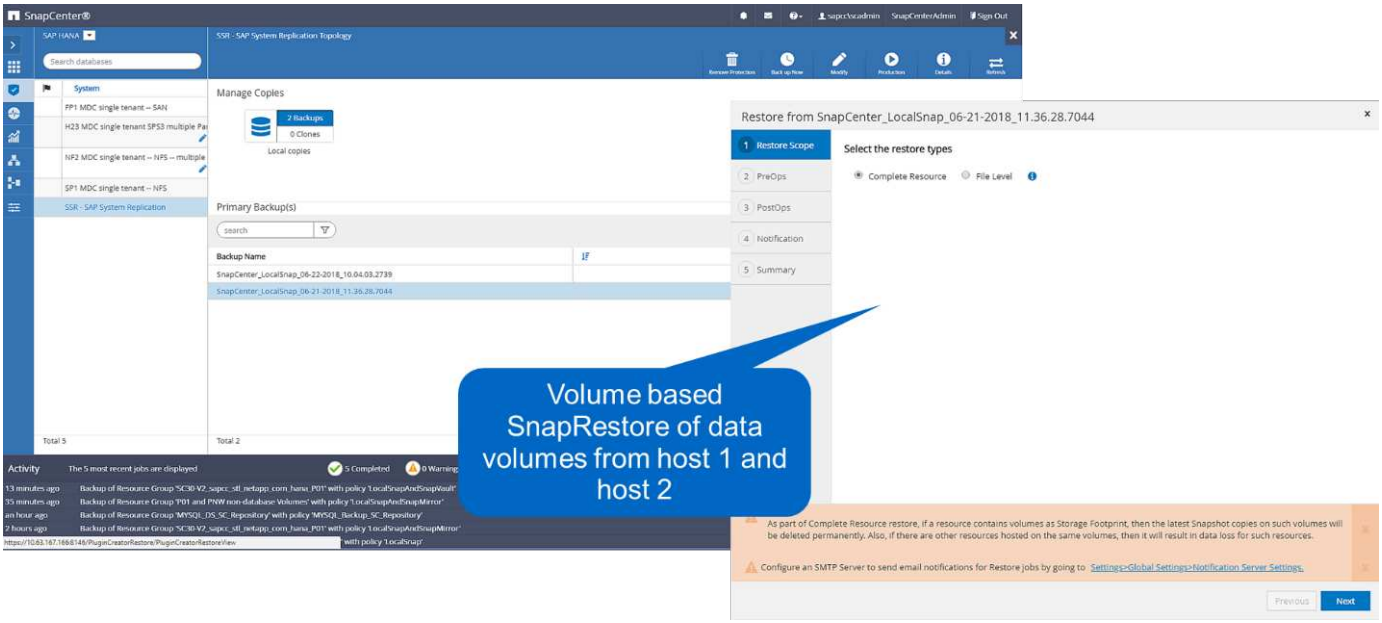
T1 のホスト 1 にバックアップが作成されました。ホスト 2 へのフェイルオーバーが実行されました。特定の時点で、ホスト 1 へのフェイルオーバーが再度実行されます。現在の時点では、ホスト 1 がプライマリホストになります。

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。

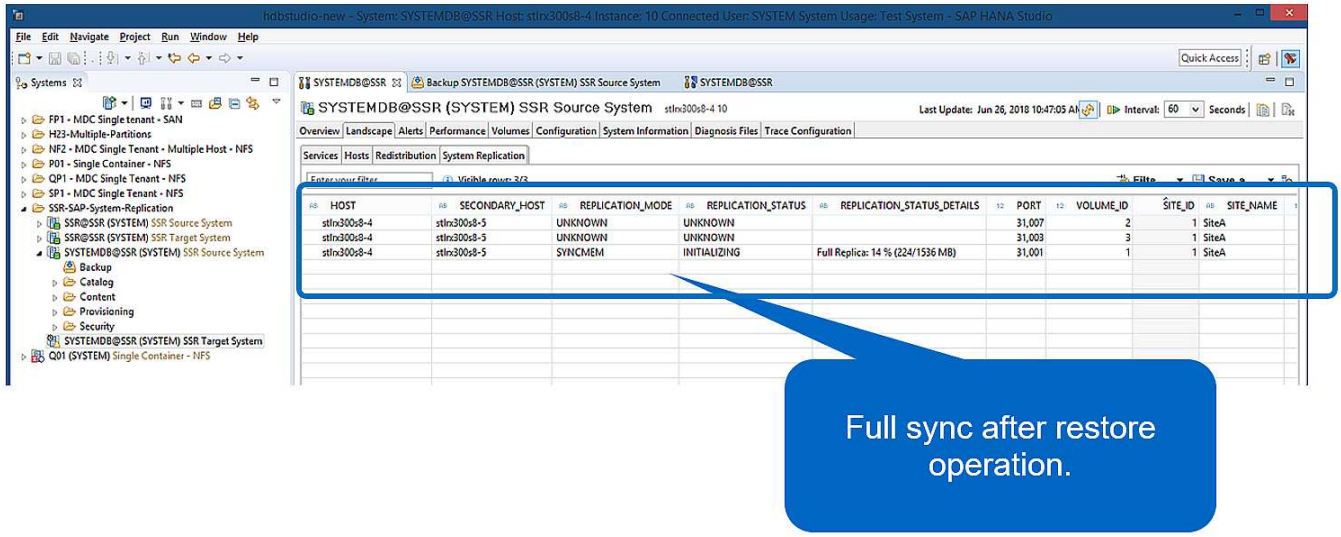


SAP HANA Studio でのリストアとリカバリの処理は、のセクションで説明する手順と同じです "有効なバックアップの SnapCenter リストアのみを実行してください"。

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。



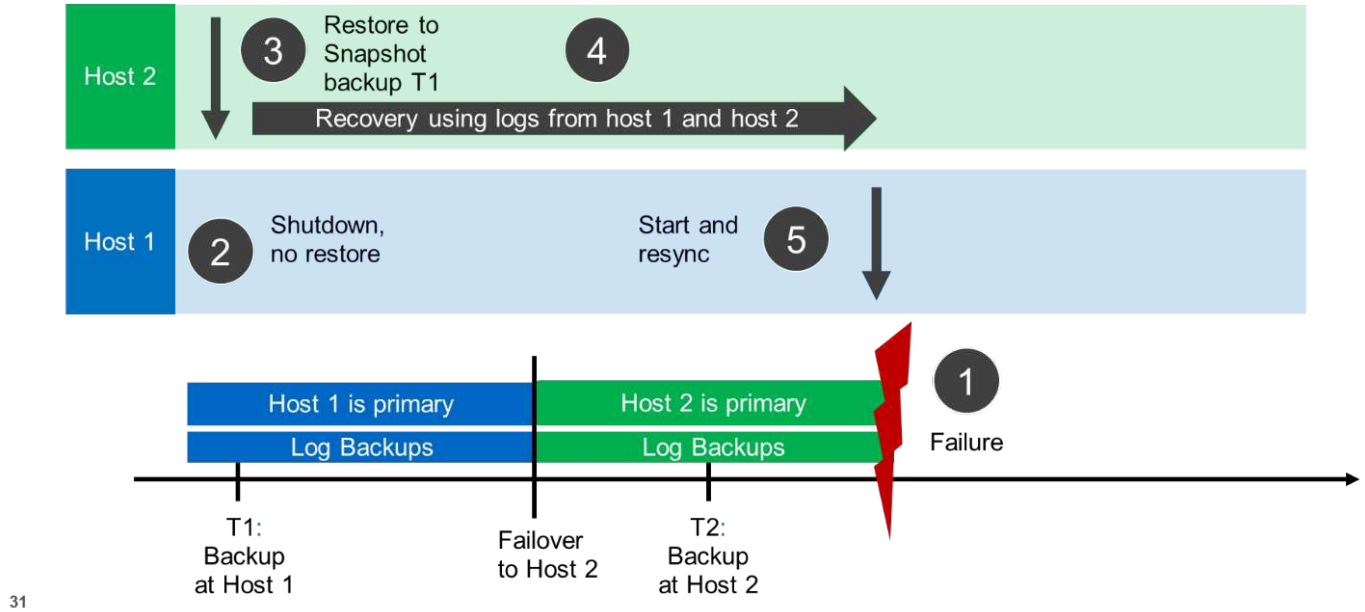
もう一方のホストで作成されたバックアップからのリストアとリカバリ

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。

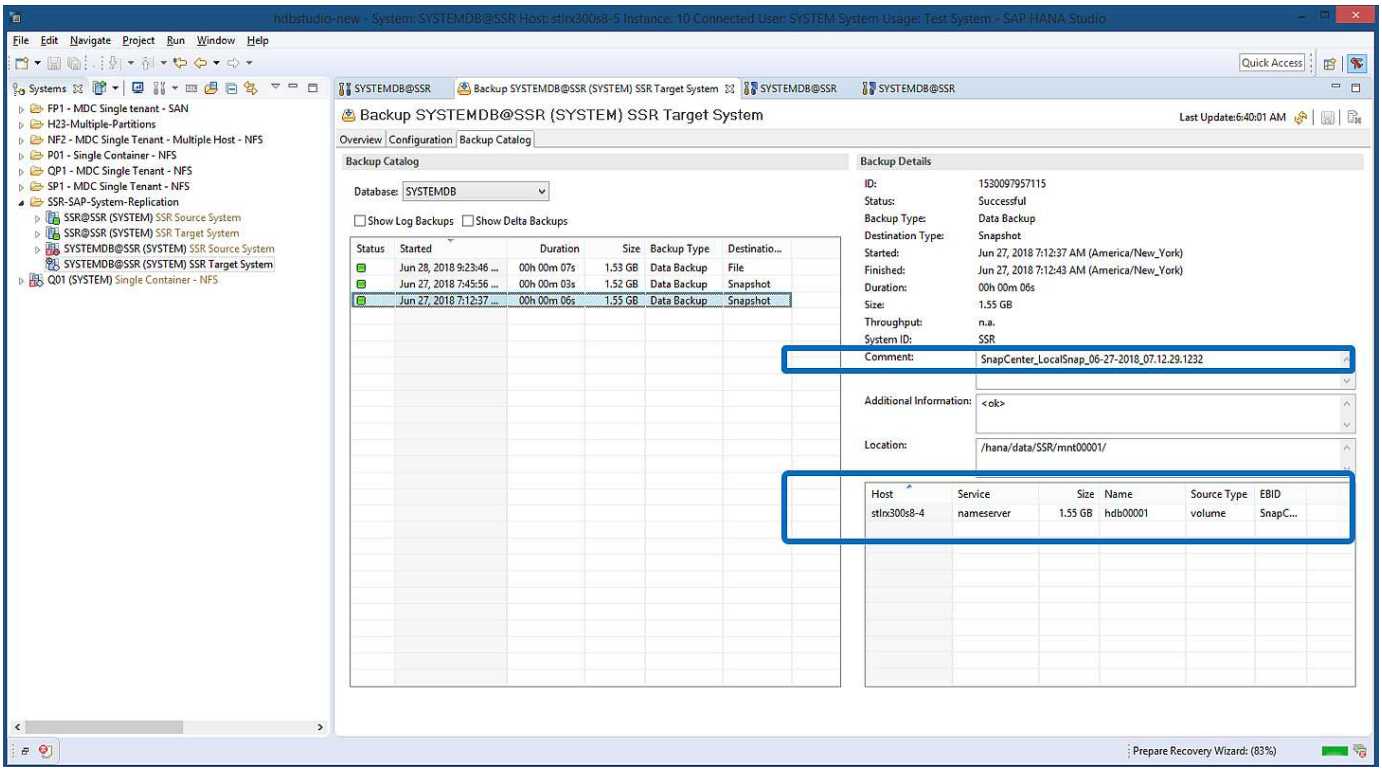
T1 のホスト 1 にバックアップが作成されました。ホスト 2 へのフェイルオーバーが実行されました。現在の時点では、ホスト 2 がプライマリホストになります。

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

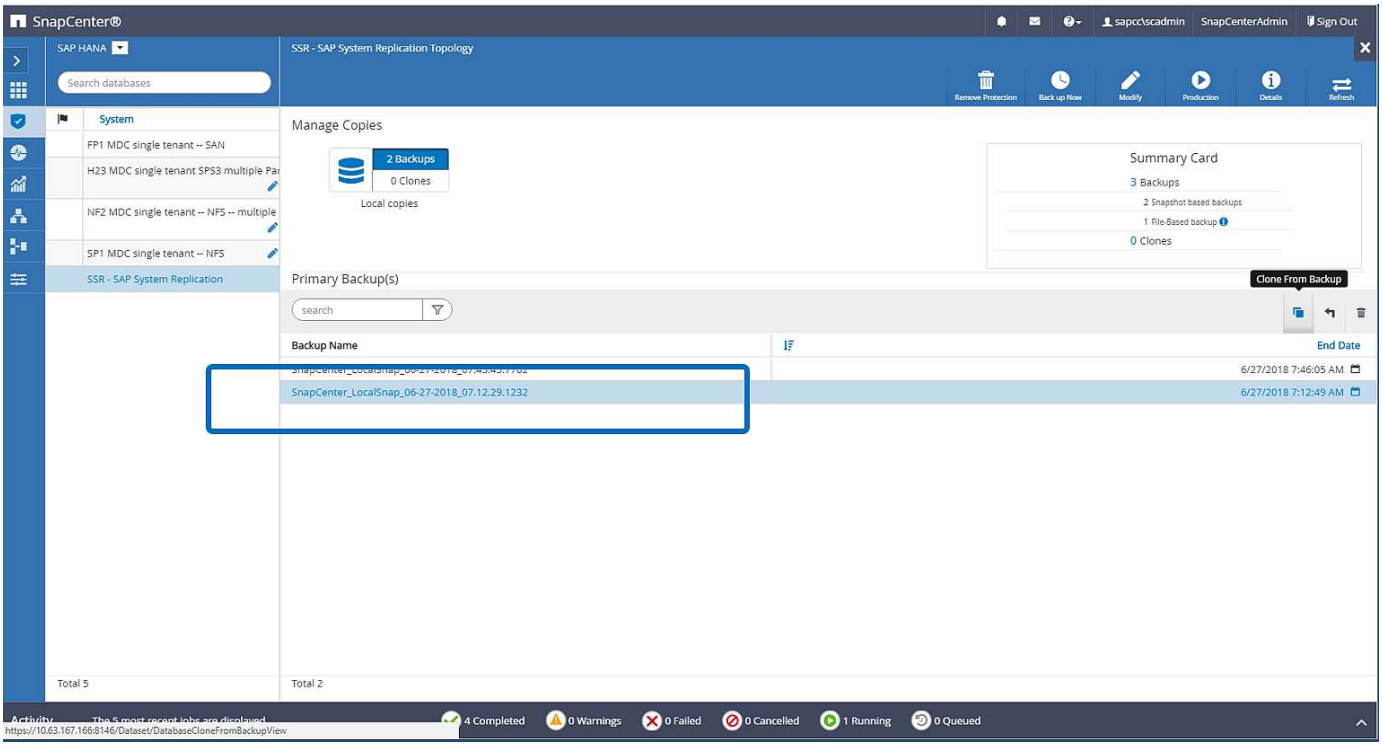
次の図は、 SAP HANA のバックアップカタログを示しており、リストア処理とリカバリ処理に使用した、ホスト 1 で作成されたバックアップを強調表示しています。



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。

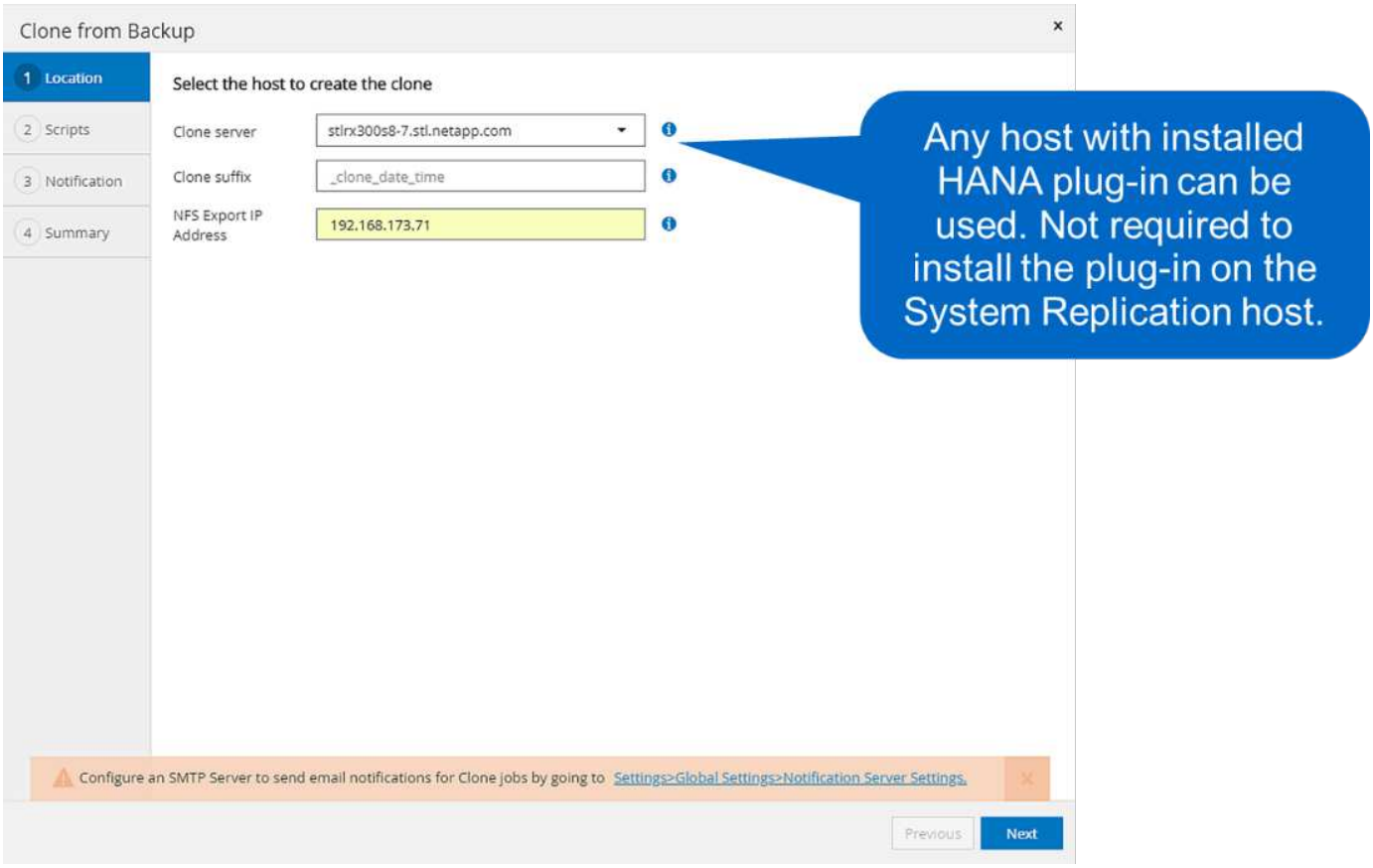
SnapCenter で、バックアップが選択され、クローニング処理が開始されます。



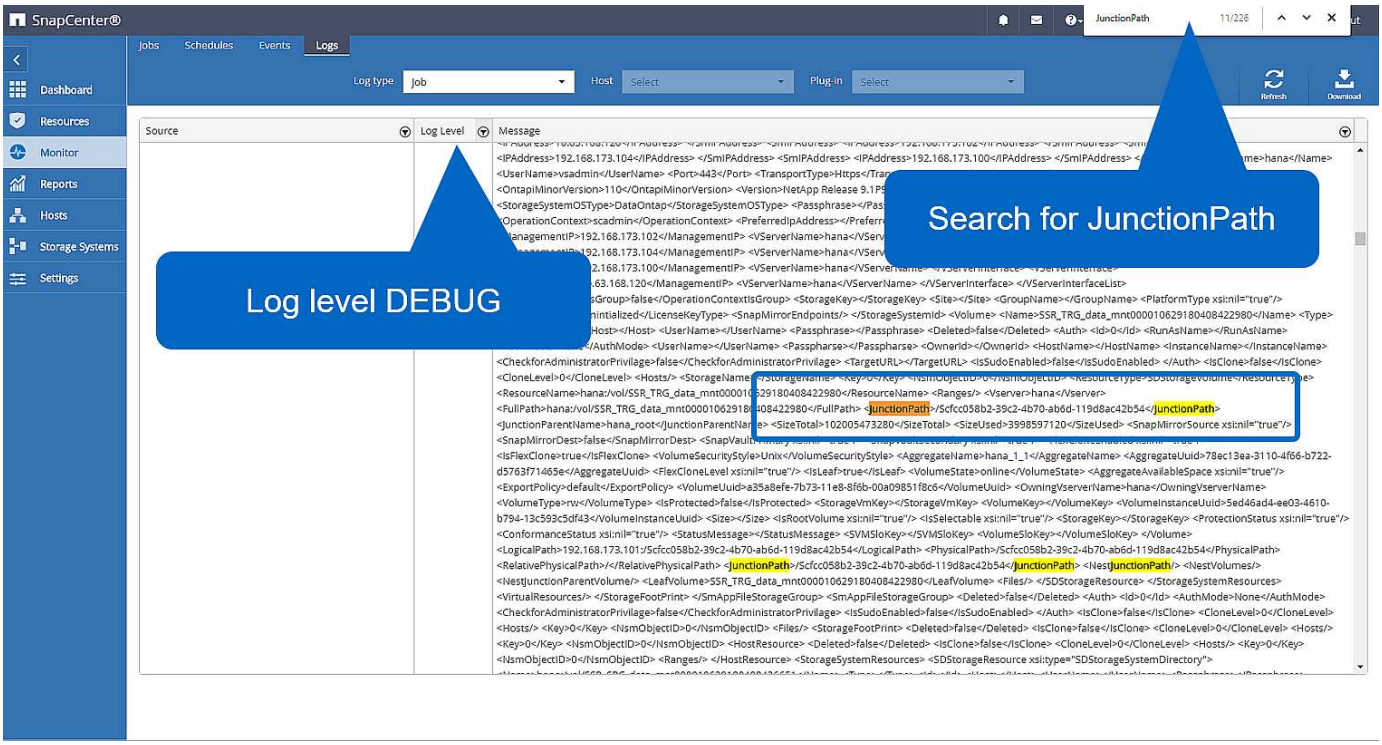
クローンサーバおよび NFS エクスポートの IP アドレスを指定する必要があります。

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が、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

  "https://www.netapp.com/us/media/tr-4614.pdf"

- 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

  "https://docs.netapp.com/us-en/netapp-solutions-sap/lifecycle/sc-copy-clone-introduction.html"

- 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	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