



# **Azure NetApp Files**で実行されているアプリケーションを保護 SnapCenter software

NetApp  
January 09, 2026

# 目次

Azure NetApp Filesで実行されているアプリケーションを保護	1
Azure NetApp Filesで実行されているアプリケーションを保護	1
制限事項	1
SnapCenterのインストールとクレデンシャルの作成	1
Azure仮想マシンへのSnapCenterのインストール	1
SnapCenterでAzureクレデンシャルを作成する	3
Azureストレージアカウントの設定	4
クレデンシャルを作成してプラグインホストを追加	4
SAP HANAデータベースを保護	5
ホストを追加してSnapCenter Plug-in for SAP HANA Databaseをインストールする	5
SAP HANAデータベースの追加	6
SAP HANAデータベースのバックアップポリシーの作成	7
リソースグループを作成してSAP HANAバックアップポリシーを適用	7
Azure NetApp Filesで実行されているSAP HANAデータベースのバックアップ	8
SAP HANAリソースグループのバックアップ	9
SAP HANAデータベースのリストアとリカバリ	10
SAP HANAデータベースのバックアップのクローニング	11
Microsoft SQL Serverデータベースの保護	12
ホストを追加してSnapCenter Plug-in for SQL Server Databaseをインストールする	12
SQL Serverデータベースのバックアップポリシーの作成	13
リソースグループの作成とSQLバックアップポリシーの適用	14
Azure NetApp Filesで実行されているSQL Serverデータベースのバックアップ	15
SQL Serverリソースグループのバックアップ	16
SQL Serverデータベースのリストアとリカバリ	17
SQL Serverデータベースバックアップのクローニング	18
Oracleデータベースの保護	20
ホストを追加してSnapCenter Plug-in for Oracle Databaseをインストールする	20
Oracleデータベースのバックアップポリシーの作成	20
リソースグループを作成してOracleバックアップポリシーを適用	21
Azure NetApp Filesで実行されているOracleデータベースをバックアップする	22
Oracleリソースグループのバックアップ	23
Oracleデータベースのリストアとリカバリ	24
Oracleデータベースバックアップのクローニング	26

# Azure NetApp Filesで実行されているアプリケーションを保護

## Azure NetApp Filesで実行されているアプリケーションを保護

SnapCenterは、Azure NetApp Files上にあるOracle、SQL、SAP HANAなどのアプリケーションの保護をサポートしています。6.0.1リリース以降のSnapCenterでは、Azure NetApp Filesバックアップ機能がサポートされています。この機能を使用すると、長期的なリカバリ、アーカイブ、コンプライアンスのためのフルマネージドバックアップソリューションが提供されるため、Azure NetApp Filesのデータ保護機能が拡張されます。

Azure NetApp Filesは、バックアップの長期保持にコストがかかるプレミアムストレージソリューションです。コストを最適化するために、Azure NetApp FilesストレージからAzureオブジェクトストアにバックアップを移動できます。SnapCenter 6.0.1以降では、Azure NetApp Files上にあるアプリケーションをAzure Blob Storage（オブジェクトストア）にバックアップおよびクローニングできます。短期的なリカバリ用にAzure NetApp FilesストレージにボリュームSnapshotコピーを2つ、長期的なリカバリ用にAzure Blob Storageにもう1つ、データのコピーを2つ保持できます。

Azure NetApp Filesバックアップを含むポリシーが有効でリソースに関連付けられている場合、SnapCenterはボリュームSnapshotの作成とAzure Blob Storageへのバックアップを処理します。SnapCenterによってバックアップヴォールトが作成され、ボリュームのバックアップが有効になります。ボリュームのバックアップを有効にした場合、SnapCenterは既存のバックアップを使用します。

### 制限事項

- FAS、ASA、AFF ONTAPおよびAmazon FSx for NetApp ONTAPストレージシステムのオブジェクトストレージ機能はサポートされません。
- OracleとSAP HANAのマウントワークフローとカタログワークフローは、オブジェクトストレージのバックアップではサポートされませんが、Snapshotではサポートされます。
- Oracle PDBクローンはオブジェクトストレージのバックアップではサポートされませんが、Snapshotではサポートされます。
- オブジェクトストレージからのバックアップ検証、REST APIのサポート、オブジェクトストレージからのクローンライフサイクル管理、およびオブジェクトストレージバックアップのレポート機能はサポートされていません。
- Azure Blob Storage上のバックアップからAzure NetApp Filesへのリストアはサポートされていません。クローニングオプションを使用することもできます。
- クローンスプリットはサポートされていません。

## SnapCenterのインストールとクレデンシャルの作成

### Azure仮想マシンへのSnapCenterのインストール

NetApp Support SiteからSnapCenterソフトウェアをダウンロードし、Azure仮想マシンにインストールできます。

## 開始する前に

- Azure Windows仮想マシンがSnapCenterサーバのインストール要件を満たしていることを確認します。詳細については、を参照してください "[SnapCenterサーバをインストールするための要件](#)"。
- Azure NetApp Filesを初めてお使いで、既存のNetAppアカウントをお持ちでない場合は、SnapCenterソフトウェアにアクセスできるように登録済みであることを確認してください。情報については、を参照してください "[登録してSnapCenterソフトウェアにアクセス](#)"。

## 手順

1. からSnapCenterサーバインストールパッケージをダウンロードし "[NetAppサポートサイト](#)" ます。
2. ダウンロードした.exeファイルをダブルクリックして、SnapCenterサーバのインストールを開始します。

インストールを開始すると、すべての事前チェックが実行され、最小要件を満たしていない場合は、該当するエラーまたは警告メッセージが表示されます。警告メッセージは無視してインストールを続行できますが、エラーは修正する必要があります。

3. SnapCenterサーバのインストールに必要な値があらかじめ入力されていることを確認し、必要に応じて変更します。

MySQL Serverリポジトリデータベースのパスワードを指定する必要はありません。SnapCenterサーバのインストール中に、パスワードが自動的に生成されます。



リポジトリデータベースのカスタムパスでは、特殊文字「%」はサポートされていません。パスに「%」を含めると、インストールは失敗します。

4. [今すぐインストール] をクリックします。

無効な値を指定した場合は、該当するエラーメッセージが表示されます。値を再入力してから、インストールを開始してください。



[Cancel] \* ボタンをクリックすると、実行中のステップが完了し、ロールバック操作が開始されます。SnapCenter サーバがホストから完全に削除されます。

ただし、「SnapCenter サーバサイトの再起動」または「SnapCenter サーバの起動を待機中」の処理が実行されているときに「\* キャンセル」をクリックすると、処理はキャンセルされずにインストールが続行されます。

## 製品を登録してサポートを有効にする

NetAppを初めてご利用になり、NetAppアカウントをお持ちでない場合は、製品を登録してサポートを有効にする必要があります。

## 手順

1. SnapCenterのインストール後、\*[ヘルプ]>[バージョン情報]\*に移動します。
2. [About SnapCenter\_]ダイアログボックスで、971で始まる20桁のSnapCenterインスタンスをメモします。
3. をクリックします <https://register.netapp.com>
4. [\* I am not a registered NetApp Customer\*] をクリックします。

5. 自分自身を登録するには、詳細を指定してください。
6. NetApp Reference SNフィールドは空白のままにします。
7. [Product Line]ドロップダウンから[\* SnapCenter \*]を選択します。
8. 課金プロバイダを選択します。
9. 20桁のSnapCenterインスタンスIDを入力します。
10. [Submit（送信）] をクリックします。

## SnapCenterでAzureクレデンシアルを作成する

Azure NetAppアカウントにアクセスするには、SnapCenterでAzureクレデンシアルを作成する必要があります。

開始する前に

- Azureでサービスプリンシパルを作成したことを確認します。
- サービスプリンシパルに関連付けられたテナントID、クライアントID、およびシークレットキーが使用可能であることを確認します。
  - テナントIDは、Azureポータルの[Entra ID]の[Overview]ページで確認できます。
  - クライアントIDは、エンタープライズアプリケーション/サービスプリンシパルのアプリケーションIDとも呼ばれます。これは、SnapCenterのサービスプリンシパルとして機能するために作成したエンタープライズアプリケーションの[Overview]ページにあるAzureポータルで確認できます。
  - クライアントシークレットキーは、シークレット値とも呼ばれます。このクライアントシークレットをAzure Portalで作成するには、[Entra ID]の\*に移動します。作成したエンタープライズアプリを選択したら、[証明書とシークレット]に移動し、[新しいクライアントシークレット]\*に移動します。



シークレット値は、作成時にのみアクセスできます。あとからアクセスすることはできません。

- サービスプリンシパルに権限を付与する必要があります。Contributorのロールにより、サービスプリンシパルはAzureで必要なアクションを実行できます。これは、[サブスクリプション]ページの[アクセス制御（IAM）]ページから付与できます。

手順

1. 左側のナビゲーションペインで、\* 設定 \* をクリックします。
2. [ 設定 ] ページで、[\* 資格情報 ] をクリックします。
3. [ 新規作成（New） ] をクリックする。
4. [クレデンシアル]ページで、クレデンシアルの作成に必要な次の情報を指定します。

フィールド	操作
クレデンシアル名	クレデンシアルの名前を入力します。
認証モード	ドロップダウンリストから*[Azure Credential]*を選択します。

フィールド	操作
テナントID	テナントIDを入力します。
クライアントID	クライアントIDを入力します。
クライアントシークレットキー	クライアントシークレットキーを入力します。

5. [OK]\*をクリックします。

## Azureストレージアカウントの設定

SnapCenterでAzureストレージアカウントを設定する必要があります。

Azureストレージアカウントには、サブスクリプションID、Azureクレデンシャル、およびAzure NetAppアカウントの詳細が含まれます。



Azure NetApp Filesには標準ライセンスと容量ベースライセンスは必要ありません。

### 手順

1. 左側のナビゲーションペインで、\* ストレージシステム \* をクリックします。
2. [ストレージシステム]ページで、[ **Azure NetApp Files** ]\*を選択し、[新規]\*をクリックします。
3. クレデンシャル、サブスクリプションID、およびNetAppアカウントをそれぞれのドロップダウンリストから選択します。
4. [Submit（送信）] をクリックします。

## クレデンシャルを作成してプラグインホストを追加

SnapCenter は、クレデンシャルを使用して SnapCenter 処理を実行するユーザを認証します

SnapCenterプラグインのインストールに使用するクレデンシャルと、データ保護処理を実行するためのクレデンシャルをそれぞれ作成する必要があります。

### 手順

1. 左側のナビゲーションペインで、\* 設定 \* をクリックします。
2. [ 設定 ] ページで、[\* 資格情報 ] をクリックします。
3. [ 新規作成（New） ] をクリックする。
4. [クレデンシャル]ページで、クレデンシャルの作成に必要な次の情報を指定します。

フィールド	操作
クレデンシャル名	クレデンシャルの名前を入力します。

フィールド	操作
認証モード	ド롭ダウンリストから認証モードを選択します。
認証タイプ	パスワードベース*または SSHキーベース*（Linuxホストのみ）を選択します。
ユーザ名	ユーザ名を指定します。
パスワード	[パスワードベースの認証]を選択した場合は、パスワードを指定します。
SSH秘密鍵	SSHキーベースの認証を選択した場合は、秘密鍵を指定します。
sudo権限を使用	<p>root以外のユーザのクレデンシャルを作成する場合は、[Use sudo privileges]チェックボックスを選択します。</p> <div>  <p>これはLinuxユーザにのみ該当します。</p> </div>

5. [OK]\*をクリックします。

## SAP HANAデータベースを保護

ホストを追加して**SnapCenter Plug-in for SAP HANA Database**をインストールする

SnapCenterの[ホストを追加]ページを使用してホストを追加し、プラグインパッケージをインストールする必要があります。プラグインはリモートホストに自動的にインストールされます。

開始する前に

- SnapCenter Admin ロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが必要です。
- Windowsホストにプラグインをインストールするときに、組み込みでないクレデンシャルを指定する場合や、ユーザがローカルワークグループに属している場合は、ホストのUACを無効にする必要があります。
- 一元化されたホストにインストールする場合は、SAP HANAクライアントソフトウェアがそのホストにインストールされていることを確認し、SAP HANAデータベースホストで必要なポートを開いてHDB SQLクエリをリモートで実行します。

手順

1. 左側のナビゲーションペインで、\* Hosts \*（ホスト）をクリックします。
2. [管理対象ホスト]\*タブが選択されていることを確認します。

3. [追加]\*をクリックします。
4. [Hosts]ページで、次の操作を実行します。
  - a. [Host Type]フィールドで、ホストタイプを選択します。
  - b. [Host name]フィールドに、ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。
  - c. [Credentials]フィールドに、作成したクレデンシャルを入力します。
5. [Select Plug-ins to Install]セクションで、インストールするプラグインを選択します。
6. （オプション）\*[その他のオプション]\*をクリックし、詳細を指定します。
7. [Submit（送信）]をクリックします。
8. ホストタイプがLinuxの場合は、フィンガープリントを確認し、\* Confirm and Submit \*をクリックします。

クラスタセットアップでは、クラスタ内の各ノードのフィンガープリントを検証する必要があります。

9. インストールの進行状況を監視します。

## SAP HANAデータベースの追加

SAP HANAデータベースは手動で追加する必要があります。

### タスクの内容

プラグインが一元化されたサーバにインストールされている場合は、リソースを手動で追加する必要があります。SAP HANAプラグインがHANAデータベースホストにインストールされている場合は、HANAシステムが自動的に検出されます。



自動検出はHANAマルチホスト構成ではサポートされていません。追加するには一元化されたプラグインを使用する必要があります。

### 手順

1. 左側のナビゲーションペインで、ドロップダウンリストから SnapCenter Plug-in for SAP HANA Database を選択し、\* Resources \* をクリックします。
2. リソースページで、\* SAP HANA データベースの追加 \* をクリックします。
3. [Provide Resource Details]ページで、次の操作を実行します。
  - a. リソースタイプとして、[Single Container]、[Multitenant Database Container]、または[Non-data Volume]のいずれかを入力します。
  - b. SAP HANAシステムの名前を入力します。
  - c. システムID（SID）を入力します。
  - d. プラグインホストを選択します。
  - e. SAP HANAシステムに接続するためのキーを入力します。
  - f. HDBのセキュアなユーザストアキーを設定するユーザ名を入力します。
4. [Provide Storage Footprint]ページで、ストレージタイプとして\* Azure NetApp Files \*を選択します。
  - a. Azure NetAppアカウントを選択します。



- b. 容量プールと関連付けられているボリュームを選択します。
  - c. [ 保存 ( Save ) ] をクリックします。
5. 概要を確認し、[ 完了 ] をクリックします。

## SAP HANAデータベースのバックアップポリシーの作成

SnapCenter を使用して SAP HANA データベースのリソースをバックアップする前に、バックアップ対象のリソースまたはリソースグループのバックアップポリシーを作成する必要があります。

### 手順

1. 左側のナビゲーションペインで、\* 設定 \* をクリックします。
2. [ 設定 ] ページで、[ \* ポリシー \* ] をクリックします。
3. [ 新規作成 ( New ) ] をクリックする。
4. [ 名前 ] ページで、ポリシー名と概要を入力します。
5. [Policy type] ページで、次の手順を実行します。
  - a. ストレージタイプとして \* Azure NetApp Files \* を選択します。
  - b. データベースの整合性チェックを実行する場合は、\*[ファイルベース]\*を選択します。
  - c. Snapshotテクノロジーを使用してバックアップを作成する場合は、\* Snapshotベース\*を選択します。
6. [Snapshot and backup] ページで、次の手順を実行します。
  - a. スケジュールバックアップの頻度を選択します。
  - b. 保持設定を指定します。
  - c. Azure NetApp Filesバックアップを有効にする場合は、\*[バックアップを有効にする]\*を選択し、保持設定を指定します。
7. 概要を確認し、[ 完了 ] をクリックします。

## リソースグループを作成してSAP HANAバックアップポリシーを適用


リソースグループはコンテナであり、バックアップおよび保護するリソースを追加する必要があります。

リソースグループを使用すると、特定のアプリケーションに関連付けられているすべてのデータを同時にバックアップできます。リソースグループはすべてのデータ保護ジョブに必要です。また、リソースグループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義する必要があります。

### 手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [ リソース ] ページで、[ \* 新しいリソースグループ \* ] をクリックします。
3. [ 名前 ] ページで、次の操作を実行します。

フィールド	操作
名前	リソースグループの名前を入力します。
タグ	リソースグループをあとで検索する際に役立つラベルを1つ以上入力します。
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの名前形式を入力します。

- Resources ページで、\* Host \* ドロップダウン・リストからホスト名を選択し、\* Resource Type \* ドロップダウン・リストからリソース・タイプを選択します。
- [ 使用可能なリソース ( Available Resources ) ] セクションからリソースを選択し、右矢印をクリックして [ 選択したリソース ( \* Selected Resources ) ] セクションに移動します。
- [Policies] ページで、次の手順を実行します。
  - ドロップダウンリストから1つ以上のポリシーを選択します。
  - [スケジュールの設定]列で、設定するポリシーの\*\*をクリックします 。
  - [Add schedules for policy\_name\_] ダイアログボックスで、スケジュールを設定し、[OK] をクリックします。
- [ 通知 ] ページの [ 電子メールの設定 \* ] ドロップダウンリストから、電子メールを送信するシナリオを選択します。
- 概要を確認し、[ 完了 ] をクリックします。

## Azure NetApp Filesで実行されているSAP HANAデータベースのバックアップ

どのリソースグループにも含まれていないリソースは、のページからバックアップすることができます。


### 手順

- 左側のナビゲーションペインで、\*[リソース]\*を選択し、リストから適切なプラグインを選択します。
- リソースページで、リソースタイプに基づいて **View** ] ドロップダウンリストからリソースをフィルタリングします。
- バックアップするリソースを選択します。
- [Resource]ページで、\*[Use custom name format for Snapshot copy]\*を選択し、Snapshot名に使用するカスタムの名前形式を入力します。
- [ アプリケーションの設定 ] ページで、次の操作を行います。
  - [Backups]\*矢印を選択して、追加のバックアップオプションを設定します。
  - [Scripts]\*の矢印を選択して、休止、Snapshot、および休止解除の処理のプリコマンドとポストコマンドを実行します。
  - [Custom Configurations]\*の矢印を選択し、このリソースを使用するすべてのジョブに必要なカスタム値のペアを入力します。

- d. Snapshotコピーツール> SnapCenter without File System Consistency \*を選択してSnapshotを作成します。

[ファイルシステムの整合性]オプションは、Windowsホストで実行されているアプリケーションにのみ適用されます。

6. [Policies] ページで、次の手順を実行します。

- a. ドロップダウンリストから1つ以上のポリシーを選択します。
- b. スケジュールを設定するポリシーの[スケジュールの設定]列で\*\*を選択します 。
- c. [Add schedules for policy\_policy\_name\_]ダイアログボックスで、スケジュールを設定し、\*[OK]\*を選択します。

\_policy\_name\_は、選択したポリシーの名前です。

7. [通知] ページの [電子メールの設定 \*] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメールアドレス、およびEメールの件名を指定する必要があります。SMTPは、\* Settings \* > \* Global Settings \* でも設定する必要があります。

8. 概要を確認し、\*[終了]\*を選択します。

9. [今すぐバックアップ]\*を選択します。

10. Backup (バックアップ) ページで、次の手順を実行します。

- a. リソースに複数のポリシーが関連付けられている場合は、\*[ポリシー]\*ドロップダウンリストから、バックアップに使用するポリシーを選択します。

オンデマンドバックアップ用に選択したポリシーにバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

11. 「\* Backup \*」を選択します。

12. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

## SAP HANAリソースグループのバックアップ

リソースグループは、ホスト上のリソースの集まりです。リソースグループのバックアップ処理は、リソースグループに定義されているすべてのリソースに対して実行されます。

### 手順

1. 左側のナビゲーションペインで、\*[リソース]\*を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[\* 表示] リストから[\* リソースグループ\*]を選択します。
3. [Resource Groups] ページで、バックアップするリソースグループを選択し、\*[Back up Now]\*を選択します。
4. Backup (バックアップ) ページで、次の手順を実行します。

- a. リソースグループに複数のポリシーが関連付けられている場合は、\*[ポリシー]\*ドロップダウンリストから、バックアップに使用するポリシーを選択します。

オンデマンドバックアップ用に選択したポリシーにバックアップスケジュールが関連付けられている場合、オンデマンドバックアップは、スケジュールタイプに指定した保持設定に基づいて保持されます。

- b. 「\* Backup \*」を選択します。

5. 処理の進捗状況を監視するために、[監視]>\*[ジョブ]\*を選択します。

## SAP HANAデータベースのリストアとリカバリ


バックアップからデータをリストアおよびリカバリできます。

### タスクの内容

自動検出されたHANAシステムでは、\* Complete Resource \*オプションを選択した場合、単一ファイルのSnapshotリストアテクノロジーを使用してリストアが実行されます。[高速リストア]チェックボックスが選択されている場合は、ボリューム復帰テクノロジーが使用されます。

手動で追加したリソースには、常にボリュームリバートテクノロジーが使用されます。

### 手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソースタイプに基づいて、**View**] ドロップダウンリストからリソースをフィルタリングします。
3. リソースを選択するか、リソースグループを選択してから、そのグループ内のリソースを選択します。
4. Manage Copies (コピーの管理) ビューから、プライマリまたはセカンダリ (ミラーまたはバックアップ) ストレージシステムから \* Backups (バックアップ) を選択します。
5. [Primary backup (s)] テーブルで、リストア元のバックアップを選択し、\*\*\*をクリックします 。
6. [Restore Scope] ページで、\*[Complete Resource]\*を選択します。

SAP HANAデータベースの設定されているすべてのデータボリュームがリストアされます。

7. 自動検出されたHANAシステムの場合は、[Recovery scope] ページで次の操作を実行します。
  - a. 可能な限り現在の時刻に近い状態にリカバリする場合は、\* Recover to most recent state \* を選択します。
  - b. 指定した時点にリカバリする場合は、\*[ポイントインタイムにリカバリ]\*を選択します。
  - c. 特定のデータバックアップにリカバリする場合は、\*指定したデータバックアップにリカバリする\*を選択します。
  - d. 今すぐリカバリしない場合は、\*[リカバリなし]\*を選択します。
  - e. ログバックアップの場所を指定します。
  - f. バックアップカタログの場所を指定します。
8. [リストア前] ページで、リストア・ジョブを実行する前に実行するプリ・リストアおよびアンマウント

・ コマンドを入力します。

9. [ポスト・オペレーション] ページで、マウントおよびリストア後のコマンドを入力して、リストア・ジョブの実行後に実行します。
10. [通知] ページの [電子メールの設定 \*] ドロップダウンリストから、電子メールを送信するシナリオを選択します。


また、送信者と受信者のEメールアドレスとEメールの件名を指定する必要があります。また、[\* 設定 \* (Settings \*) ]>[\* グローバル設定 \* (\* Global Settings \*) ] ページでも SMTP を設定する必要があります。

11. 概要を確認し、[完了] をクリックします。
12. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

## SAP HANAデータベースのバックアップのクローニング

SnapCenterでは、SAP HANAデータベースのバックアップを使用してSAP HANAデータベースをクローニングできます。作成されるクローンはシッククローンで、親容量プールに作成されます。

### 手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソースタイプに基づいて、**View**] ドロップダウンリストからリソースをフィルタリングします。
3. リソースまたはリソースグループを選択します。
4. [Manage Copies]ビューで、プライマリストレージシステムから\*[Backups]\*を選択します。
5. 表からデータバックアップを選択し、をクリックします .
6. Location ページで、次のアクションを実行します。
  - a. クローンHANAシステムを管理するためのSAP HANAプラグインがインストールされているホストを選択します。

一元化されたプラグインホストでもHANAシステムホストでもかまいません。



他のホストのHANAデータベースを管理する一元化されたホストにHANAプラグインをインストールした場合、クローンの作成または削除時に、ターゲットサーバが一元化されたホストであるため、SnapCenterではホスト側の処理（ファイルシステムのマウントまたはアンマウント）が意図的にスキップされます。マウントおよびアンマウント処理を実行するには、クローニング前またはクローニング後のカスタムスクリプトを使用する必要があります。

- a. 既存のバックアップからクローニングするSAP HANA SIDを入力します。
- b. クローンボリュームをエクスポートするホスト名またはIPアドレスを入力します。
- c. SAP HANAデータベースANFボリュームが手動のQoS容量プールに設定されている場合は、クローンボリュームのQoSを指定します。

クローンボリュームにQoSが指定されていない場合は、ソースボリュームのQoSが使用されます。自動QoS容量プールを使用している場合、指定したQoS値は無視されます。

7. [Scripts]ページで、次の手順を実行します。

- a. クローニング処理の前後に実行するプリコマンドやポストコマンドを入力します。
- b. mountコマンドを入力して、ファイルシステムをホストにマウントします。

ソースHANAシステムが自動検出され、クローンターゲットホストプラグインがSAP HANAホストにインストールされている場合、SnapCenterはクローンターゲットホスト上の既存のHANAデータボリュームを自動的にアンマウントし、新しくクローニングされたHANAデータボリュームをマウントします。

8. [通知] ページの [電子メールの設定 \*] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

9. 概要を確認し、[完了] をクリックします。

10. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。



ANFクローンはすでに選択したSnapshotから作成された独立したボリュームであるため、ANFクローンではクローンスプリットは無効になります。

## Microsoft SQL Serverデータベースの保護

ホストを追加して**SnapCenter Plug-in for SQL Server Database**をインストールする

SnapCenterは、Azure NetApp Files上のSMB共有上のSQLインスタンスのデータ保護をサポートしています。スタンドアロン構成と可用性グループ（AG）構成がサポートされます。

SnapCenterの[ホストを追加]ページを使用してホストを追加し、プラグインパッケージをインストールする必要があります。プラグインはリモートホストに自動的にインストールされます。

開始する前に

- SnapCenter Admin ロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが必要です。
- Windowsホストにプラグインをインストールするときに、組み込みでないクレデンシャルを指定する場合や、ユーザがローカルワークグループに属している場合は、ホストのUACを無効にする必要があります。

手順

1. 左側のナビゲーションペインで、**Hosts** を選択します。
2. 上部で [Managed Hosts] タブが選択されていることを確認します。
3. 「\* 追加」を選択します。
4. [Hosts]ページで、次の手順を実行します。
  - a. [Host Type]フィールドで、ホストタイプを選択します。
  - b. [Host name]フィールドに、ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。

- c. [Credentials]フィールドに、作成したクレデンシャルを入力します。
5. [インストールするプラグインを選択してください\*]セクションで、インストールするプラグインを選択します。
6. (オプション) \*[その他のオプション]\*をクリックし、詳細を指定します。
7. [送信]を選択します。
8. を選択し、[ホストログディレクトリの設定]ページでホストログディレクトリの**SMB**パスを入力し、[保存]\*をクリックします。
9. [送信]\*をクリックし、インストールの進行状況を監視します。

## SQL Serverデータベースのバックアップポリシーの作成

SnapCenter を使用して SQL Server リソースをバックアップする前に、リソースまたはリソースグループのバックアップポリシーを作成することができます。また、リソースグループの作成時や単一のリソースのバックアップ時にバックアップポリシーを作成することもできます。

### 手順

1. 左側のナビゲーションペインで、\* 設定 \* をクリックします。
2. [設定] ページで、[\* ポリシー \*] をクリックします。
3. [新規作成 (New)] をクリックする。
4. [名前] ページで、ポリシー名と概要を入力します。
5. [Policy type] ページで、次の手順を実行します。
  - a. ストレージタイプとして\* Azure NetApp Files \*を選択します。
  - b. バックアップタイプを選択します。
    - i. データベースファイルとトランザクションログをバックアップする場合は、\*[フルバックアップとログバックアップ]\*を選択します。
    - ii. データベースファイルのみをバックアップする場合は、\*[フルバックアップ]\*を選択します。
    - iii. トランザクションログのみをバックアップする場合は、\*[ログバックアップ]\*を選択します。
    - iv. 別のアプリケーションを使用してリソースをバックアップする場合は、\*[バックアップのみをコピー]\*を選択します。
  - c. 可用性グループの設定セクションで、次の操作を実行します。
    - i. レプリカのみにバックアップする場合は、[Backup on preferred backup replica]を選択します。
    - ii. バックアップのプライマリAGレプリカまたはセカンダリAGレプリカを選択します。
    - iii. バックアップ優先度を選択します。
6. [Snapshot and backup] ページで、次の手順を実行します。
  - a. スケジュールバックアップの頻度を選択します。
  - b. 選択したバックアップタイプに応じて、保持設定を指定します。
  - c. Azure NetApp Filesバックアップを有効にする場合は、\*[バックアップを有効にする]\*を選択し、保持設定を指定します。

7. [Verification] ページで、次の手順を実行します。

- a. Run verification for following backup schedules セクションで、スケジュール頻度を選択します。
- b. Database consistency check options セクションで、次の操作を実行します。
  - i. 整合性チェックの対象をデータベースの物理構造に限定し、データベースに影響を与える正しくないページ、チェックサム障害、および一般的なハードウェア障害を検出するには、「\*」を選択します。
  - ii. すべての情報メッセージを非表示にするには、\*[すべての情報メッセージを非表示 (NO\_INFOMSGS)]\*を選択します。

デフォルトで選択されています。

- iii. レポートされたエラーをオブジェクトごとにすべて表示する場合は、このオプションを選択します。
- iv. 非クラスタ化インデックスをチェックしない場合は、「\* 非クラスタ化インデックスをチェックしない」を選択します。

SQL Serverデータベースは、Microsoft SQL Server Database Consistency Checker (DBCC) を使用して、データベース内のオブジェクトの論理的および物理的な整合性をチェックします。

- v. 内部データベースSnapshotを使用する代わりにチェックを制限してロックを取得する場合は、\*[内部データベースSnapshotコピー (TABLOCK) を使用する代わりにチェックを制限してロックを取得する]\*を選択します。
- c. [ログ・バックアップ\*] セクションで、[完了時にログ・バックアップを検証する\*]を選択し、完了時にログ・バックアップを検証します。
- d. 検証スクリプトの設定\* セクションで、検証処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

8. 概要を確認し、[完了]をクリックします。

## リソースグループの作成とSQLバックアップポリシーの適用

リソースグループはコンテナであり、バックアップおよび保護するリソースを追加する必要があります。

リソースグループを使用すると、特定のアプリケーションに関連付けられているすべてのデータを同時にバックアップできます。リソースグループはすべてのデータ保護ジョブに必要です。また、リソースグループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義する必要があります。



### 手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[\* 新しいリソースグループ\*] をクリックします。
3. [名前] ページで、次の操作を実行します。

フィールド	操作
名前	リソースグループの名前を入力します。



フィールド	操作
タグ	リソースグループをあとで検索する際に役立つラベルを1つ以上入力します。
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの名前形式を入力します。

4. Resources ページで、\* Host \* ドロップダウン・リストからホスト名を選択し、\* Resource Type \* ドロップダウン・リストからリソース・タイプを選択します。
5. [使用可能なリソース ( Available Resources ) ] セクションからリソースを選択し、右矢印をクリックして [ 選択したリソース ( \* Selected Resources ) ] セクションに移動します。
6. [Policies] ページで、次の手順を実行します。
  - a. ドロップダウンリストから1つ以上のポリシーを選択します。
  - b. [スケジュールの設定]列で、設定するポリシーの\*\*をクリックします 。
  - c. [Add schedules for policy\_name\_] ダイアログボックスで、スケジュールを設定し、[OK] をクリックします。
  - d. Microsoft SQL Server スケジューラを選択します。
7. [Verification] ページで、次の手順を実行します。
  - a. 検証サーバを選択します。
  - b. 検証スケジュールを設定するポリシーを選択し、\*\*をクリックします 。
  - c. または[スケジュールされた検証を実行する]\*を選択します。
  - d. [OK]\*をクリックします。
8. [ 通知 ] ページの [ 電子メールの設定 \* ] ドロップダウンリストから、電子メールを送信するシナリオを選択します。
9. 概要を確認し、[ 完了 ] をクリックします。

## Azure NetApp Filesで実行されているSQL Serverデータベースのバックアップ



どのリソースグループにも含まれていないリソースは、のページからバックアップすることができます。

### 開始する前に

Azure WindowsフェイルオーバークラスタにクラスタIPが割り当てられていない場合やSnapCenterから到達できない場合は、ロードバランサを作成する必要があります。ロードバランサのIPが設定され、SnapCenterサーバから到達可能である必要があります。

### 手順

1. 左側のナビゲーションペインで、\*[リソース]\*を選択し、リストから適切なプラグインを選択します。
2. [リソース]ページで、[表示]ドロップダウンリストから\*、[インスタンス]、または[可用性グループ]\*を選択します。

3. [Resource] ページで、\*[Use custom name format for Snapshot copy]\*を選択し、Snapshot名に使用するカスタムの名前形式を入力します。
4. [Policies] ページで、次の手順を実行します。
  - a. ドロップダウンリストから1つ以上のポリシーを選択します。
  - b. スケジュールを設定するポリシーの[スケジュールの設定]列で\*\*を選択します 。
  - c. [Add schedules for policy\_policy\_name\_]ダイアログボックスで、スケジュールを設定し、\*[OK]\*を選択します。  
  
\_policy\_name\_ は、選択したポリシーの名前です。
  - d. を選択し、スケジュールポリシーに関連付けられている[スケジューラインスタンス]\*ドロップダウンリストからスケジューラインスタンスを選択します。
5. [Verification] ページで、次の手順を実行します。
  - a. 検証サーバを選択します。
  - b. 検証スケジュールを設定するポリシーを選択し、\*\*をクリックします 。
  - c. または[スケジュールされた検証を実行する]\*を選択します。
  - d. [OK] をクリックします。
6. [通知] ページの [電子メールの設定 \*] ドロップダウンリストから、電子メールを送信するシナリオを選択します。
7. 概要を確認し、[完了] をクリックします。
8. [今すぐバックアップ]\*を選択します。
9. Backup (バックアップ) ページで、次の手順を実行します。
  - a. リソースに複数のポリシーが関連付けられている場合は、\*[ポリシー]\*ドロップダウンリストから、バックアップに使用するポリシーを選択します。
  - b. [Verify after backup]\*を選択します。
  - c. 「\* Backup \*」を選択します。
10. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

## SQL Server リソースグループのバックアップ

複数のリソースで構成されるリソースグループをバックアップできます。リソースグループのバックアップ処理は、リソースグループに定義されているすべてのリソースに対して実行されます。

### 手順

1. 左側のナビゲーションペインで、\*[リソース]\*を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[\* 表示] リストから [\* リソースグループ \*] を選択します。
3. [Resource Groups] ページで、バックアップするリソースグループを選択し、\*[Back up Now]\*を選択します。

4. Backup（バックアップ）ページで、次の手順を実行します。
  - a. リソースグループに複数のポリシーが関連付けられている場合は、\*[ポリシー]\*ドロップダウンリストから、バックアップに使用するポリシーを選択します。
  - b. バックアップ後、**verify** を選択して、オンデマンドバックアップを検証します。
  - c. 「\* Backup \*」を選択します。
5. 処理の進捗状況を監視するために、[監視]>\*[ジョブ]\*を選択します。


## SQL Serverデータベースのリストアとリカバリ

SnapCenter を使用して SQL Server データベースを復元できます。データベースの復元は、指定された SQL Server バックアップから指定されたデータベースにすべてのデータとログ ページをコピーする多段階のプロセスです。

### 開始する前に

- SMB ADactive Directory ドメインに属し、ファイル権限を適切に設定する権限を持つ Active Directory ユーザーを使用して、ターゲット インスタンスを構成します。
- SnapCenterインスタンス レベルで資格情報を構成します。
- SQLデータベースがCIFS共有上に存在する場合、プラグインホストのRunASアカウントとSQLサービスアカウント（ドメインアカウント）が `BUILTIN\Administrators` ONTAPの CIFS サーバーのグループ。
- SMB 構成では、ターゲット インスタンスの SQL 認証はサポートされません。必要な権限を持つ Active Directory ユーザーを使用して、SnapCenterでターゲット インスタンスを構成します。
- SnapCenterプラグイン サービス アカウントが Active Directory ユーザーでない場合は、代替ホストに復元するときに、ソース ボリュームを完全に制御できるユーザーが使用可能であることを確認します。

### 手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [リソース]ページで、[表示]リストから\*または[リソースグループ]\*を選択します。
3. リストからデータベースまたはリソースグループを選択します。
4. [コピーの管理]ビューで、\*[バックアップ]\*をストレージシステムから選択します。
5. 表からバックアップを選択し、アイコンをクリックします 。
6. [Restore Scope]ページで、次のいずれかのオプションを選択します。
  - a. データベースを同じ SQL サーバーに復元するには、「バックアップが作成されたのと同じホストにデータベースを復元する」を選択します。
  - b. バックアップが作成された同じホストまたは別のホスト内の別の SQL サーバーにデータベースを復元する場合は、[データベースを別のホストに復元] を選択します。
7. [Recovery Scope]ページで、次のいずれかのオプションを選択します。
  - a. ログなしでフルバックアップのみをリストアする必要がある場合は、「\* なし」を選択します。
  - b. フルバックアップ後に使用可能なすべてのログバックアップをリストアする場合は、\*[すべてのログバックアップ\*最新の状態へのバックアップリストア処理]を選択します。

- c. 「ログバックアップによる \*」を選択してポイントインタイムリストア処理を実行します。この場合、選択した日付のバックアップログまで、バックアップログに基づいてデータベースがリストアされます。
  - d. リストアされたデータベースにトランザクション・ログを適用しない日時を指定するには、[\* までの特定の日付]を選択します。
  - e. すべてのログ・バックアップ\*、ログ・バックアップ\*、または\*を指定日までに\*とログがカスタム・ロケーションにある場合は、\*カスタム・ログ・ディレクトリを使用\*を選択し、ログの場所を指定します。
8. [Pre-Ops and Post Ops]ページで、必要な詳細を指定します。
  9. [通知]ページの[電子メールの設定\*]ドロップダウンリストから、電子メールを送信するシナリオを選択します。
  10. 概要を確認し、[完了]をクリックします。
  11. [\* Monitor \* > \* Jobs \*]ページを使用してリストア・プロセスを監視します。

## SQL Serverデータベースバックアップのクローニング

SnapCenterを使用すると、データベースのバックアップを使用してSQLデータベースをクローニングできます。作成されるクローンはシッククローンで、親容量プールに作成されます。


### タスクの内容

クローンのターゲットインスタンスに、SMB ADActive Directoryドメインに属し、ファイル権限を適切に設定する権限があるActive Directoryユーザが設定されていることを確認する必要があります。クレデンシャルはSnapCenterでインスタンスレベルで設定する必要があります。

ターゲットインスタンスのSQL認証は、SMB構成ではサポートされません。ターゲットインスタンスは、必要な権限を持つActive Directoryユーザを使用してSnapCenterで設定する必要があります。

SnapCenter Plug-inサービスのサービスアカウントがActive Directoryユーザでない場合は、クローンの実行中にソースボリュームを偽装して必要な処理を実行できるように、ソースボリュームを完全に制御できるユーザが必要です。

### 手順

1. 左側のナビゲーションペインで、\*[リソース]\*を選択し、リストから適切なプラグインを選択します。
2. [リソース]ページで、[\* 表示]リストから[\* データベース\*]または[\* リソースグループ\*]を選択します。
3. データベースまたはリソースグループを選択します。
4. [コピーの管理]ビューページで、プライマリストレージシステムからバックアップを選択します。
5. バックアップを選択し、\*\*を選択します .
6. [クローンオプション]\*ページで、必要なすべての詳細を指定します。
7. [場所]ページで、クローンを作成するストレージの場所を選択します。

SQL ServerデータベースANFボリュームが手動のQoS容量プールに設定されている場合は、クローンボリュームのQoSを指定します。


クローンボリュームにQoSが指定されていない場合は、ソースボリュームのQoSが使用されます。自動QoS容量プールを使用している場合、指定したQoS値は無視されます。

8. Logs ページで、次のいずれかのオプションを選択します。
  - a. ログなしでフルバックアップのみをクローニングする場合は、\*[なし]\*を選択します。
  - b. フルバックアップ後の日付のログバックアップをすべてクローニングする場合は、\*[すべてのログバックアップ]\*を選択します。
  - c. 選択した日付のバックアップログまでに作成されたバックアップログに基づいてデータベースをクローニングする場合は、\*[By log backups until]\*を選択します。
  - d. 指定した日時以降にトランザクションログを適用しない場合は、\*[By specific date until]\*を選択します。
9. [Script \*] ページで、クローニング処理の前後に実行するプリスクリプトまたはポストスクリプトのスクリプトタイムアウト、パス、および引数を入力します。
10. [Notification] ページの [Email preference] ドロップダウンリストから、電子メールを送信するシナリオを選択します。
11. 概要を確認し、\*[終了]\*を選択します。
12. 処理の進捗状況を監視するために、[監視]>\*[ジョブ]\*を選択します。

## クローンライフサイクルの実行

SnapCenter を使用すると、リソースグループまたはデータベースからクローンを作成できます。クローニングはオンデマンドで実行することも、リソースグループまたはデータベースに対して定期的なクローニング処理をスケジュール設定することもできます。バックアップを定期的にクローニングすると、クローンを使用してアプリケーションの開発、データの取り込み、またはデータのリカバリを行うことができます。

## 手順

1. 左側のナビゲーションペインで、\*[リソース]\*を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[\* 表示] リストから [\* データベース \*] または [\* リソースグループ \*] を選択します。
3. データベースまたはリソースグループを選択します。
4. [コピーの管理]ビューページで、プライマリストレージシステムからバックアップを選択します。
5. バックアップを選択し、\*\*を選択します 。
6. [クローンオプション]\* ページで、必要なすべての詳細を指定します。
7. [場所] ページで、クローンを作成するストレージの場所を選択します。

SQL ServerデータベースANFボリュームが手動のQoS容量プールに設定されている場合は、クローンボリュームのQoSを指定します。

クローンボリュームにQoSが指定されていない場合は、ソースボリュームのQoSが使用されます。自動QoS容量プールを使用している場合、指定したQoS値は無視されます。

8. [Script \*] ページで、クローニング処理の前後に実行するプリスクリプトまたはポストスクリプトのスクリプトタイムアウト、パス、および引数を入力します。
9. [スケジュール] ページで、次のいずれかの操作を実行します。

- クローニングジョブをすぐに実行する場合は、「\* Run Now \*」を選択します。
  - クローニング処理の実行頻度、クローニングスケジュールを開始するタイミング、クローニング処理を実行する曜日、スケジュールの有効期限、およびスケジュールの有効期限が切れたあとにクローン削除するかどうかを指定する場合は、\*[スケジュールの設定]\*を選択します。
10. **[Notification]** ページの **[\*Email preference]** ドロップダウンリストから、電子メールを送信するシナリオを選択します。
  11. 概要を確認し、\*[終了]\*を選択します。
  12. 処理の進捗状況を監視するために、**[監視]>\*[ジョブ]\***を選択します。

## Oracleデータベースの保護

ホストを追加して**SnapCenter Plug-in for Oracle Database**をインストールする

[ホストの追加]ページを使用してホストを追加し、SnapCenter Plug-ins Package for LinuxまたはSnapCenter Plug-ins Package for AIXをインストールできます。プラグインはリモートホストに自動的にインストールされます。

ホストの追加とプラグインパッケージのインストールは、ホストごとまたはクラスタごとに実行できます。クラスタ（Oracle RAC）にプラグインをインストールする場合、プラグインはクラスタのすべてのノードにインストールされます。Oracle RAC One Nodeの場合は、アクティブノードとパッシブノードの両方にプラグインをインストールする必要があります。

手順

1. 左側のナビゲーションペインで、\* Hosts \*（ホスト）をクリックします。
2. [管理対象ホスト]\*タブが選択されていることを確認します。
3. [追加]\*をクリックします。
4. [Hosts]ページで、次の操作を実行します。
  - a. [Host Type]フィールドで、ホストタイプを選択します。
  - b. [Host name]フィールドに、ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。
  - c. [Credentials]フィールドに、作成したクレデンシャルを入力します。
5. [Select Plug-ins to Install]セクションで、インストールするプラグインを選択します。
6. （オプション）\*[その他のオプション]\*をクリックし、詳細を指定します。
7. [Submit（送信）]をクリックします。
8. 指紋を確認し、\* 確認して送信 \* をクリックします。

クラスタセットアップでは、クラスタ内の各ノードのフィンガープリントを検証する必要があります。

9. インストールの進行状況を監視します。

## Oracleデータベースのバックアップポリシーの作成

SnapCenter を使用して Oracle データベースリソースをバックアップする前に、バック

アップ対象のリソースまたはリソースグループのバックアップポリシーを作成する必要があります。

#### 手順

1. 左側のナビゲーションペインで、\* 設定 \* をクリックします。
2. [ 設定 ] ページで、[ \* ポリシー \* ] をクリックします。
3. ドロップダウンリストから[Oracle Database]を選択します。
4. [ 新規作成 ( New ) ] をクリックする。
5. [ 名前 ] ページで、ポリシー名と概要を入力します。
6. [Policy type]ページで、次の手順を実行します。
  - a. ストレージタイプとして\* Azure NetApp Files \*を選択します。
  - b. バックアップタイプとして、オンラインバックアップまたはオフラインバックアップを選択します。
  - c. Oracle Recovery Manager ( RMAN ) を使用してバックアップをカタログ化する場合は、[ \* Catalog backup with Oracle Recovery Manager ( RMAN ) \* ] を選択します。
  - d. バックアップ後にアーカイブ・ログのプルーニングを行う場合は、バックアップ後にアーカイブ・ログをプルーニング \* を選択します。
  - e. アーカイブログの削除設定を指定します。
7. [Snapshot and backup]ページで、次の手順を実行します。
  - a. スケジュールバックアップの頻度を選択します。
  - b. 保持設定を指定します。
  - c. Azure NetApp Filesバックアップを有効にする場合は、\*[バックアップを有効にする]\*を選択し、保持設定を指定します。
8. スクリプトページで、バックアップ処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。
9. [Verification]ページで、検証処理を実行するバックアップスケジュールを選択し、検証処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。
10. 概要を確認し、[ 完了 ] をクリックします。

## リソースグループを作成して**Oracle**バックアップポリシーを適用

リソースグループはコンテナであり、バックアップおよび保護するリソースを追加する必要があります。

リソースグループを使用すると、特定のアプリケーションに関連付けられているすべてのデータを同時にバックアップできます。リソースグループはすべてのデータ保護ジョブに必要です。また、リソースグループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義する必要があります。



#### 手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [ リソース ] ページで、[ \* 新しいリソースグループ \* ] をクリックします。



3. [名前] ページで、次の操作を実行します。

フィールド	操作
名前	リソースグループの名前を入力します。
タグ	リソースグループをあとで検索する際に役立つラベルを1つ以上入力します。
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの名前形式を入力します。
アーカイブログファイルのデスティネーション	アーカイブログファイルのデスティネーションを指定します。

4. Resources ページで、\* Host \* ドロップダウン・リストからホスト名を選択し、\* Resource Type \* ドロップダウン・リストからリソース・タイプを選択します。
5. [使用可能なリソース ( Available Resources ) ] セクションからリソースを選択し、右矢印をクリックして [ 選択したリソース ( \* Selected Resources ) ] セクションに移動します。
6. [Policies] ページで、次の手順を実行します。
  - a. ドロップダウンリストから1つ以上のポリシーを選択します。
  - b. [スケジュールの設定]列で、設定するポリシーの\*\*をクリックします 。
  - c. [Add schedules for policy\_name\_] ダイアログボックスで、スケジュールを設定し、[OK] をクリックします。
7. [Verification] ページで、次の手順を実行します。
  - a. 検証サーバを選択します。
  - b. 検証スケジュールを設定するポリシーを選択し、\*をクリックします。 
  - c. または[スケジュールされた検証を実行する]\*を選択します。
  - d. [OK]\*をクリックします。
8. [通知] ページの [ 電子メールの設定 \*] ドロップダウンリストから、電子メールを送信するシナリオを選択します。
9. 概要を確認し、[完了] をクリックします。



## Azure NetApp Filesで実行されているOracleデータベースをバックアップする

どのリソースグループにも含まれていないリソースは、のページからバックアップすることができます。

### 手順

1. 左側のナビゲーションペインで、\*[リソース]\*を選択し、リストから適切なプラグインを選択します。
2. [リソース]ページで、[表示]ドロップダウンリストから\*[データベース]\*を選択します。



3. [Resource]ページで、\*[Use custom name format for Snapshot copy]\*を選択し、Snapshot名に使用するカスタムの名前形式を入力します。
4. [Policies] ページで、次の手順を実行します。
  - a. ドロップダウンリストから1つ以上のポリシーを選択します。
  - b. スケジュールを設定するポリシーの[スケジュールの設定]列で\*\*を選択します 。
  - c. [Add schedules for policy\_policy\_name\_]ダイアログボックスで、スケジュールを設定し、\*[OK]\*を選択します。
5. [Verification] ページで、次の手順を実行します。
  - a. 検証サーバを選択します。
  - b. 検証スケジュールを設定するポリシーを選択し、\*\*をクリックします 。
  - c. または[スケジュールされた検証を実行する]\*を選択します。
  - d. [OK] をクリックします。
6. [ 通知 ] ページの [ 電子メールの設定 \* ] ドロップダウンリストから、電子メールを送信するシナリオを選択します。
7. 概要を確認し、[ 完了 ] をクリックします。
8. [今すぐバックアップ]\*を選択します。
9. Backup （バックアップ） ページで、次の手順を実行します。
  - a. リソースに複数のポリシーが関連付けられている場合は、\*[ポリシー]\*ドロップダウンリストから、バックアップに使用するポリシーを選択します。
  - b. [ バックアップ ] をクリックします。
10. 操作の進行状況を監視するには、 \* Monitor \* > \* Jobs \* をクリックします。

## Oracleリソースグループのバックアップ

複数のリソースで構成されるリソースグループをバックアップできます。リソースグループのバックアップ処理は、リソースグループに定義されているすべてのリソースに対して実行されます。


### 手順

1. 左側のナビゲーションペインで、\*[リソース]\*を選択し、リストから適切なプラグインを選択します。
2. [ リソース ] ページで、[ \* 表示 ] リストから [ \* リソースグループ \* ] を選択します。
3. [Resource Groups]ページで、バックアップするリソースグループを選択し、\*[Back up Now]\*を選択します。
4. Backup （バックアップ） ページで、次の手順を実行します。
  - a. リソースグループに複数のポリシーが関連付けられている場合は、\*[ポリシー]\*ドロップダウンリストから、バックアップに使用するポリシーを選択します。
  - b. 「 \* Backup \* 」を選択します。
5. 処理の進捗状況を監視するために、[監視]>\*[ジョブ]\*を選択します。

## Oracleデータベースのリストアとリカバリ

データ損失が発生した場合は、SnapCenter を使用して 1 つ以上のバックアップからアクティブファイルシステムにデータをリストアし、そのあとにデータベースをリカバリできます。

### 手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから\*または[リソースグループ]\*を選択します。
3. リストからデータベースまたはリソースグループを選択します。
4. [Manage Copies] ビューで、プライマリストレージシステムから\*[Backups]\*を選択します。
5. 表からバックアップを選択し、\*\*をクリックします 。
6. Restore Scope ページで、次のタスクを実行します。
  - a. RAC環境でデータベースのバックアップを選択した場合は、RACを選択します。
  - b. 次の操作を実行します。
    - i. データベースファイルのみをリストアする場合は、\*[すべてのデータファイル]\*を選択します。
    - ii. 表領域のみをリストアする場合は、\*[表領域]\*を選択します。
    - iii. Data GuardスタンバイデータベースまたはActive Data GuardスタンバイデータベースのREDOログファイルをリストアする場合は、\* Redo log files \*を選択します。
    - iv. [プラグブルデータベース]\*を選択し、リストアするPDBを指定します。
    - v. Pluggable Database ( PDB ) tablespaces \* を選択し、リストアする PDB とその PDB の表領域を指定します。
    - vi. バックアップを作成したSQL Serverにデータベースをリストアする場合は、\*[バックアップが作成されたホストにデータベースをリストアする]\*を選択します。
    - vii. バックアップを作成するホストまたは別のホストにある別のSQL Serverにデータベースをリストアする場合は、\*[別のホストにデータベースをリストアする]\*を選択します。
    - viii. リストアとリカバリに必要な場合は、「\* データベースの状態を変更」を選択して、データベースの状態をリストアとリカバリ処理の実行に必要な状態に変更します。
    - ix. バックアップ後に新しいデータファイルが追加された場合や、LUN が LVM ディスクグループに追加、削除、再作成された場合にインプレースリストアを実行するには、\* Force in place restore \* を選択します。
7. [Recovery Scope] ページで、次のいずれかのオプションを選択します。
  - a. 最後のトランザクションまでリカバリする場合は、\*[すべてのログ]\*を選択します。
  - b. 特定のSCNにリカバリする場合は、\* Until SCN (System Change Number) \*を選択します。
  - c. 特定の日にリカバリする場合は、\*[日時]\*を選択します。
  - d. リカバリしない場合は\*[リカバリなし]\*を選択します。
  - e. 外部アーカイブログファイルの場所を指定する場合は、\*[Specify external archive log locations]\*を選択します。

8. [Pre-Ops and Post Ops]ページで、必要な詳細を指定します。
9. [ 通知 ] ページの [ 電子メールの設定 \* ] ドロップダウンリストから、電子メールを送信するシナリオを選択します。
10. 概要を確認し、[ 完了 ] をクリックします。
11. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。


#### ポイントインタイムリカバリを使用した表領域のリストアとリカバリ

データベース内の他の表領域に影響を与えることなく、破損または削除された表領域のサブセットをリストアできます。SnapCenterは、RMANを使用して表領域のポイントインタイムリカバリ（PITR）を実行します。

#### 手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [リソース]ページで、[表示]リストから\*または[リソースグループ]\*を選択します。
3. タイプが単一インスタンス（マルチテナント）のデータベースを選択します。
4. [コピーの管理]ビューで、ストレージ・システムから[\* バックアップ \*]を選択します。

バックアップがカタログ化されていない場合は、バックアップを選択し、\* Catalog \* をクリックします。

5. カタログ化されたバックアップを選択し、\*\*をクリックします .
6. Restore Scope ページで、次のタスクを実行します。
  - a. RAC環境でデータベースのバックアップを選択した場合は、\* RAC \*を選択します。
  - b. 表領域のみをリストアする場合は、\*[表領域]\*を選択します。
  - c. リストアとリカバリに必要な場合は、「\* データベースの状態を変更」を選択して、データベースの状態をリストアとリカバリ処理の実行に必要な状態に変更します。
7. [Recovery Scope]ページで、次のいずれかのオプションを選択します。
  - a. 特定のSCNにリカバリする場合は、\* Until SCN（System Change Number）\*を選択します。
  - b. 特定の日にリカバリする場合は、\*[日時]\*を選択します。
8. [Pre-Ops and Post Ops]ページで、必要な詳細を指定します。
9. [ 通知 ] ページの [ 電子メールの設定 \* ] ドロップダウンリストから、電子メールを送信するシナリオを選択します。
10. 概要を確認し、[ 完了 ] をクリックします。
11. [\* Monitor \* > \* Jobs \*] ページを使用してリストア・プロセスを監視します。


#### ポイントインタイムリカバリを使用したプラグブルデータベースのリストアとリカバリ

コンテナデータベース（CDB）内の他のPDBに影響を与えることなく、破損またはドロップされたプラグブルデータベース（PDB）をリストアおよびリカバリできます。SnapCenterは、RMANを使用してPDBのポイントインタイムリカバリ（PITR）を実行します。

#### 手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [リソース]ページで、[表示]リストから\*または[リソースグループ]\*を選択します。
3. タイプが単一インスタンス（マルチテナント）のデータベースを選択します。
4. [コピーの管理]ビューで、ストレージ・システムから[\* バックアップ \*]を選択します。


バックアップがカタログ化されていない場合は、バックアップを選択し、\* Catalog \* をクリックします。

5. カタログ化されたバックアップを選択し、\*\*をクリックします 。
6. Restore Scope ページで、次のタスクを実行します。
  - a. RAC環境でデータベースのバックアップを選択した場合は、\* RAC \*を選択します。
  - b. PDB内のPDBと表領域のどちらをリストアするかに応じて、次のいずれかの操作を実行します。
    - PDBをリストアする場合は、\*[Pluggable databases (PDB)]\*を選択します。
    - PDB内の表領域をリストアする場合は、\*[Pluggable database (PDB) tablespaces]\*を選択します。
7. [Recovery Scope]ページで、次のいずれかのオプションを選択します。
  - a. 特定のSCNにリカバリする場合は、\* Until SCN (System Change Number) \*を選択します。
  - b. 特定の日にリカバリする場合は、\*[日時]\*を選択します。
8. [Pre-Ops and Post Ops]ページで、必要な詳細を指定します。
9. [通知] ページの [電子メールの設定 \*] ドロップダウンリストから、電子メールを送信するシナリオを選択します。
10. 概要を確認し、[完了] をクリックします。
11. [\* Monitor \* > \* Jobs \*] ページを使用してリストア・プロセスを監視します。

## Oracleデータベースバックアップのクローニング

SnapCenterを使用すると、データベースのバックアップを使用してOracleデータベースをクローニングできます。作成されるクローンはシッククローンで、親容量プールに作成されます。

### 手順

1. 左側のナビゲーションペインで、\* リソース \* をクリックし、リストから適切なプラグインを選択します。
2. [リソース]ページで、[表示]リストから\*または[リソースグループ]\*を選択します。
3. データベースを選択します。
4. [Manage Copies]ビューページで、プライマリストレージシステムのバックアップを選択します。
5. データバックアップを選択し、\*\*をクリックします .
6. [Name]ページで、データベース（CDBまたは非CDB）をクローニングするか、プラグブルデータベース（PDB）をクローニングするかを選択します。

7. [Locations]ページで、必要な詳細を指定します。

OracleデータベースANFボリュームが手動のQoS容量プールに設定されている場合は、クローンボリュームのQoSを指定します。

クローンボリュームにQoSが指定されていない場合は、ソースボリュームのQoSが使用されます。自動QoS容量プールを使用している場合、指定したQoS値は無視されます。

8. [Credentials]ページで、次のいずれかを実行します。

- a. [Credential name for sys user]で、クローンデータベースのsysユーザパスワードの定義に使用するクレデンシャルを選択します。
- b. クローンホスト上のASMインスタンスへの接続に対してOS認証が有効になっている場合は、ASMインスタンスのクレデンシャル名で\*なし\*を選択します。

それ以外の場合は、「sys」ユーザまたはクローンホストに適用できる「SYSASM」権限を持つユーザが設定されたOracle ASMクレデンシャルを選択します。

9. [Pre-Ops]ページでプリスクリプトのパスと引数を指定し、[Database parameter settings]セクションで、データベースの初期化に使用される事前入力済みのデータベースパラメータの値を変更します。

10. クローンデータベースのリカバリを実行する場合は、[Post-Ops]ページで、**[Recover database]\***と[Until Cancel]\*がデフォルトで選択されます。

- a. [Until Cancel]\*を選択すると、SnapCenterは、クローニング対象として選択されたデータバックアップのあとに、破損していない一連のアーカイブログを含む最新のログバックアップをマウントすることでリカバリを実行します。
- b. [日付と時刻]\*を選択すると、SnapCenterは指定した日時までデータベースをリカバリします。
- c. [Until SCN]\*を選択すると、SnapCenterは指定したSCNまでデータベースをリカバリします。
- d. [外部アーカイブログの場所を指定する]\*を選択すると、SnapCenterは指定したSCNまたは選択した日時に基づいて、最適な数のログバックアップを特定してマウントします。
- e. デフォルトでは、クローンデータベースにソースデータベースと区別する一意の番号（DBID）を生成する場合は、\*[Create new DBID]\*チェックボックスが選択されています。

ソースデータベースのDBIDをクローンデータベースに割り当てる場合は、チェックボックスをオフにします。このシナリオでは、ソースデータベースがすでに登録されている外部のRMANカタログにクローンデータベースを登録すると、処理は失敗します。

- f. クローンデータベースのデフォルトの一時表領域用の一時ファイルを作成する場合は、\*[一時表領域用の一時ファイルを作成する]\*チェックボックスを選択します。
- g. [クローンの作成時に適用するSQLエントリを入力してください]\*に、クローン作成時に適用するSQLエントリを追加します。
- h. [クローン処理後に実行するスクリプトの入力]\*で、クローン処理のあとに実行するポストスクリプトのパスと引数を指定します。

11. [通知]ページの[電子メールの設定]\*ドロップダウンリストから、電子メールを送信するシナリオを選択します。


12. 概要を確認し、\*[終了]\*を選択します。

13. 処理の進捗状況を監視するために、[監視]>\*[ジョブ]\*を選択します。

## プラグブルデータベースのクローニング

プラグブルデータベース（PDB）は、同じホストまたは代替ホスト上の別のターゲットCDBまたは同じターゲットCDBにクローニングできます。クローニングされたPDBを目的のSCNまたは日時にリカバリすることもできます。

### 手順

1. 左側のナビゲーションペインで、\*リソース\*をクリックし、リストから適切なプラグインを選択します。
2. [リソース]ページで、[表示]リストから\*または[リソースグループ]\*を選択します。
3. タイプが単一インスタンス（マルチテナント）のデータベースを選択します。
4. [Manage Copies]ビューページで、プライマリストレージシステムのバックアップを選択します。
5. バックアップを選択し、\*\*をクリックします 。
6. [名前]ページで\*[PDBクローン]\*を選択し、その他の詳細を指定します。
7. [Locations]ページで、必要な詳細を指定します。
8. [Pre-Ops]ページでプリスクリプトのパスと引数を指定し、[Database parameter settings]セクションで、データベースの初期化に使用される事前入力済みのデータベースパラメータの値を変更します。
9. [Post-Ops]ページでは、クローンデータベースのリカバリが実行される場合、デフォルトで\*[Until Cancel]\*が選択されます。
  - a. [Until Cancel]\*を選択すると、SnapCenterは、クローニング対象として選択されたデータバックアップのあとに、破損していない一連のアーカイブログを含む最新のログバックアップをマウントすることでリカバリを実行します。
  - b. [日付と時刻]\*を選択すると、SnapCenterは指定した日時までデータベースをリカバリします。
  - c. [外部アーカイブログの場所を指定する]\*を選択すると、SnapCenterは指定したSCNまたは選択した日時に基づいて、最適な数のログバックアップを特定してマウントします。
  - d. デフォルトでは、クローンデータベースにソースデータベースと区別する一意の番号（DBID）を生成する場合は、\*[Create new DBID]\*チェックボックスが選択されています。

ソースデータベースのDBIDをクローンデータベースに割り当てる場合は、チェックボックスをオフにします。このシナリオでは、ソースデータベースがすでに登録されている外部のRMANカタログにクローンデータベースを登録すると、処理は失敗します。
  - e. クローンデータベースのデフォルトの一時表領域用の一時ファイルを作成する場合は、\*[一時表領域用の一時ファイルを作成する]\*チェックボックスを選択します。
  - f. [クローンの作成時に適用するSQLエントリを入力してください]\*に、クローン作成時に適用するSQLエントリを追加します。
  - g. [クローン処理後に実行するスクリプトの入力]\*で、クローン処理のあとに実行するポストスクリプトのパスと引数を指定します。
10. [通知]ページの[電子メールの設定\*]ドロップダウンリストから、電子メールを送信するシナリオを選択します。
11. 概要を確認し、\*[終了]\*を選択します。
12. 処理の進捗状況を監視するために、[監視]>\*[ジョブ]\*を選択します。



## 著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

## 商標に関する情報

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