



# **Microsoft SQL Server**データベースの保護

## SnapCenter software

NetApp  
November 06, 2025

# 目次

Microsoft SQL Serverデータベースの保護	1
ホストの追加とSnapCenter Plug-in for SQL Server Databaseのインストール	1
SQL Serverデータベースのバックアップ ポリシーの作成	1
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	3
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	4
SQL Serverリソース グループのバックアップ	5
SQL Serverデータベースのリストアとリカバリ	5
SQL Serverデータベースのバックアップのクローニング	6
クローン ライフサイクルの実行	8

# Microsoft SQL Serverデータベースの保護

## ホストの追加とSnapCenter Plug-in for SQL Server Databaseのインストール

SnapCenterは、 Azure NetApp Files上のSMB共有にある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ています。

SnapCenterの[Add Host]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、自動的にリモート ホストにインストールされます。

開始する前に

- この処理は、 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実行する必要があります。
- Windowsホストにプラグインをインストールする際、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

- 左側のナビゲーションペインで、 [ホスト] を選択します。
- 上部の\*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。
- \*追加\*を選択します。
- [Hosts]ページで次の操作を実行します。
  - [Host Type]フィールドで、ホスト タイプを選択します。
  - [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。
  - [Credentials]フィールドに、作成したクレデンシャルを入力します。
- \*インストールするプラグインの選択\*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。
- (オプション)[その他のオプション] をクリックして詳細を指定します。
- \*送信\*を選択します。
- ログ ディレクトリの構成を選択し、ホスト ログ ディレクトリの構成ページで、ホスト ログ ディレクトリの SMB パスを入力して、保存をクリックします。
- [送信] をクリックして、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可能です。

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\*をクリックします。
4. [Name]ページで、ポリシーの名前と説明を入力します。
5. ポリシー タイプ ページで、次の手順を実行します。
  - a. ストレージの種類として \* 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、完全バックアップと 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、[完全バックアップ]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、「コピーのみのバックア ップ」を選択します。
  - c. [Availability Group Settings]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. バックアップするプライマリまたはセカンダリのAGレプリカを選択します。
    - iii. バックアップの優先順位を選択します。
6. スナップショットとバックアップ ページで、次の手順を実行します。
  - a. スケジュールされた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の種類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、実行頻度を選択します。
  - b. [Database consistency check options]セクションで、次の操作を実行します。
    - i. 整合性チェックをデータベースの物理構造に制限し、破損したページ、チェックサム障害、およ びデータベースに影響する一般的なハードウェア障害を検出するには、[整合性構造をデータベー スの物理構造に制限する (PHYSICAL\_ONLY)]を選択します。
    - ii. すべての情報メッセージを抑制するには、すべての情報メッセージを抑制 (**NO\_INFOMSGS**)を選 択します。

このオプションはデフォルトで選択されています。

- iii. オブジェクトごとに報告されたすべてのエラーを表示するには、オブジェクトごとに報告された すべてのエラー メッセージを表示する (**ALL\_ERRORMSGGS**)を選択します。
- iv. 非クラスター化インデックスをチェックしない場合は、[非クラスター化インデックスをチェック しない (NOINDEX)]を選択します。

SQL Serverデータベースは、Microsoft SQL Serverの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な整合性と物理的な整合性をチェックしま

- す。
- v. 内部データベース スナップショットを使用する代わりにチェックを制限し、ロックを取得するには、[内部データベース スナップショット コピー]を使用する代わりにチェックを制限し、ロックを取得する (**TABLOCK**) 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て、完了時にログ バックアップを検証します。
  - d. \*検証スクリプト設定\*セクションで、検証操作の前または後に実行するプレ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、バックアップして保護するリソースをここに追加する必要があります。

リソース グループを使用することで、特定のアプリケーションに関連す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 グループはいずれのデータ保護ジョブにも必要になります。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ことも必要です。

### 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. [Name] ページで、次の操作を実行します。

フィールド	操作
Name	リソース グループの名前を入力します。
Tags	リソース グループを検索しやすくするために、ラベルを入力します。
Use custom name format for Snapshot copy	Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

4. [リソース] ページで、[ホスト] ドロップダウン リストからホスト名を選択し、[リソース タイプ] 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. \*利用可能\*リソース\*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\*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\*をクリックします。 \* 設定するポリシーの。
  - c. ポリシー *policy\_name* のスケジュールの追加ダイアログ ボックスでスケジュールを構成し、[OK] を

- クリックします。
- d. [Microsoft SQL Server scheduler]を選択します。
7. [Verification]ページで、次の手順を実行します。
- 検証サーバを選択します。
  - 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。  \*。
  - \*バックアップ後に検証を実行\*または\*スケジュールされた検証を実行\*を選択します。
  - [OK]をクリックします。
8. 通知ページの 電子メール設定 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 グループにもまだ含まれていないリソースは、[Resources]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 ファイルオーバー 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 Serverから到達可能である必要があります。

### 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、[表示] ドロップダウンリストから データベース、インスタンス、または 可用性グループを選択します。
- [リソース] ページで、[スナップショット コピーにカスタム名形式を使用する] を選択し、スナップショット名に使用するカスタム名形式を入力します。
- [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。
  - を選択  スケジュールを構成するポリシーの [スケジュールの構成] 列で、
  - ポリシー *policy\_name* のスケジュールの追加 ダイアログ ボックスでスケジュールを構成し、[OK] を選択します。
- policy\_name* は選択したポリシーの名前です。
- [Microsoft SQL Server] スケジューラを使用する\*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。
- [Verification] ページで、次の手順を実行します。
  - 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. \*バックアップ後に検証を実行\*または\*スケジュールされた検証を実行\*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]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. \*バックアップ後に検証\*を選択します。
  - c. \*バックアップ\*を選択します。
10. モニター > ジョブ をクリックして、操作の進行状況を監視します。

## 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を対象に実行されます。

### 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. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] を選択します。
4. [Backup]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、「検証」を選択してオンデマンド バックアップを検証します。
  - c. \*バックアップ\*を選択します。
5. モニター > ジョブ を選択して、操作の進行状況を監視します。

## SQL Serverデータベースのリストアとリカバリ

SnapCenterを使用して、バックアップされたSQL Serverデータベースをリストアすることができます。データベース リストアは段階的に実施され、すべてのデータとログ ページが指定したSQL Serverバックアップから指定したデータベースにコピーされます。

### タスク概要

リストアのターゲットインスタンスに、SMB ADActiveディレクトリドメインに属し、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、別のホストへのリストアの実行中にこれ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 データベース 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、ストレージシステムから [バックアップ] を選択します。
5. 表からバックアップを選択し、 アイコン。
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. バックアップが作成されたのと同じ SQL サーバーにデータベースを復元する場合は、「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のと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. ログなしで完全バックアップのみを復元する必要がある場合は、「なし」を選択します。
  - b. 完全バックアップ後に利用可能なすべてのログ バックアップを復元するには、すべてのログ バックアップ 最新バックアップ復元操作を選択します。
  - c. ログ バックアップ別 を選択すると、ポイントインタイム復元操作が実行され、選択した日付のバックアップ ログまでのバックアップ ログに基づいてデータベースが復元されます。
  - d. 復元されたデータベースにトランザクション ログが適用されなくなる日時を指定するには、[特定の日付まで] を選択します。
  - e. すべてのログ バックアップ、ログ バックアップ別、または\*特定の日付まで\*を選択し、ログがカスタムの場所に配置されている場合は、\*カスタム ログ ディレクトリを使用する\*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. モニター > ジョブ ページを使用して復元プロセスを監視します。

## SQL Serverデータベースの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

のクローンを作成できます。作成されるクローンはシック クローンであり、親容量プール上に作成されます。

## タスク概要

クローニングのターゲットインスタンスに、SMB ADActiveディレクトリ 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、クローニングの実行中にこれ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

- 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、[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。
- データベースまたはリソース グループを選択します。
- コピーの管理 ビュー ページで、プライマリ ストレージ システムからのバックアップを選択します。
- バックアップを選択し、\*を選択します。  \*。
- クローン オプション ページで、必要な詳細をすべて入力します。
- [Location] 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。

- [Logs] ページで、次のいずれかのオプションを選択します。
  - ログなしで完全なバックアップのみをクローンする場合は、「なし」を選択します。
  - 完全バックアップ以降の日付の利用可能なすべてのログ バックアップを複製する場合は、[すべてのログ バックアップ] を選択します。
  - 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のクローンを作成する場合は、[次のログ バックアップまで] を選択します。
  - 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、[特定の日付まで] を選択します。
- スクリプト ページで、スクリプトのタイムアウト、パス、およびクローン操作の前または後に実行するプレスクリプトまたはポストスクリプトの引数をそれぞれ入力します。
- \*通知\*ページの\*電子メール設定\*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] を選択します。
- モニター > ジョブ を選択して、操作の進行状況を監視します。

## クローン ライフサイクルの実行

SnapCenterを使用して、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、\*を選択します。  \*。
6. クローン オプション ページで、必要な詳細をすべて入力します。
7. [Location] 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. スクリプト ページで、スクリプトのタイムアウト、パス、およびクローン操作の前または後に実行するプレスクリプトまたはポストスクリプトの引数をそれぞれ入力します。
9. [Schedule] ページで、次のいずれかを実行します。
  - クローンジョブをすぐに実行するには、[今すぐ実行] を選択します。
  - クローン操作を実行する頻度、クローン スケジュールを開始する日時、クローン操作を実行する日、スケジュールの有効期限、スケジュールの有効期限が切れた後にクローンを削除するかどうかを決定する場合は、[スケジュールの構成] を選択します。
10. \*通知\*ページの\*電子メール設定\*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、[完了] を選択します。
12. モニター > ジョブ を選択して、操作の進行状況を監視します。

## 著作権に関する情報

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

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

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

ネットアップは、ここに記載されているすべての製品に対する変更を隨時、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 5225.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

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

## 商標に関する情報

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