



SQL

Serverデータベース、インスタンス、可用性 グループをバックアップする

SnapCenter software

NetApp
January 09, 2026

目次

SQL Serverデータベース、インスタンス、可用性グループをバックアップする	1
バックアップのワークフロー	1
SnapCenterでのデータベースのバックアップ方法	1
リソースをバックアップに使用できるかどうかの確認	2
NetAppストレージシステムへのリソースの移行	4
SQL Serverデータベースのバックアップポリシーの作成	6
手順1：ポリシー名を作成します	7
手順2：ポリシーオプションを設定する	7
手順3：可用性グループを設定する	8
手順4：Snapshotとレプリケーションの設定を構成する	9
手順5：最新の状態へのリストア保持を設定する	9
手順6：Snapshotを設定する	10
手順7：セカンダリレプリケーションオプションを設定する	10
手順8：スクリプト設定を構成します	11
手順9：検証設定を構成します	12
ステップ10：概要を確認します	12
SQL Serverのリソースグループの作成とポリシーの適用	12
ASA R2システム上のMicrosoft SQL Serverリソースに対してリソースグループを作成し、セカンダリ保護を有効にする	15
SQLリソースのバックアップ	18
PowerShellコマンドレットを使用してストレージシステム接続とクレデンシャルを作成する	19
SQLリソースのバックアップ	20
SQL Serverリソースグループのバックアップ	25
SnapCenterジョブページでSQLリソースのバックアップ処理を監視する	26
[Activity]ペインで、SQLリソースに対するデータ保護処理を監視する	27
SnapCenter Plug-in for Microsoft SQL Serverのバックアップ処理をキャンセルする	27
[Topology]ページでのSQL Serverのバックアップとクローンの表示	28
PowerShellコマンドレットを使用したセカンダリバックアップ数のクリーンアップ	30

SQL Serverデータベース、インスタンス、可用性グループをバックアップする

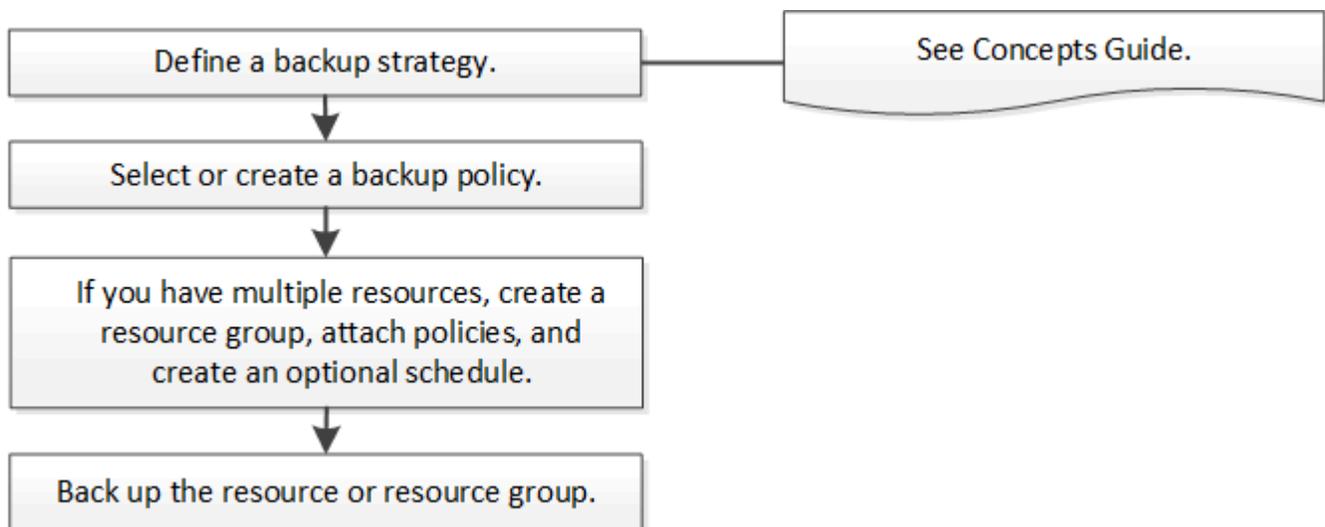
バックアップのワークフロー

SnapCenter Plug-in for Microsoft SQL Server をインストールした環境では、SnapCenter を使用して SQL Server リソースをバックアップすることができます。

スケジュールを設定して、複数のサーバで同時に複数のバックアップを実行することができます。

同じリソースに対してバックアップ処理とリストア処理を同時に実行することはできません。

次のワークフローは、バックアップ処理の実行順序を示しています。



ネットアップ以外のLUN、破損したデータベース、またはリストア中のデータベースを選択した場合、[Resources]ページの[Backup Now]、[Restore]、[Manage Backups]、および[Clone]オプションは無効になります。

PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、リカバリ、検証、クローニングの各処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterコマンドレットのヘルプを使用するか、"[SnapCenter ソフトウェアコマンドレットリファレンスガイド](#)"

SnapCenter でのデータベースのバックアップ方法

SnapCenterでは、Snapshotテクノロジーを使用して、LUNまたはVMDK上にあるSQL Serverデータベースをバックアップします。SnapCenterは、データベースのSnapshotを作成することによってバックアップを作成します。

[Resources]ページでフルデータベースバックアップの対象となるデータベースを選択すると、同じストレージボリューム上の他のすべてのデータベースがSnapCenterによって自動的に選択されます。LUNまたはVMDKにデータベースが1つだけ格納されている場合は、データベースを個別に選択解除したり、再度選択したりできます。LUNまたはVMDKに複数のデータベースが格納されている場合は、それらのデータベースを

グループとして選択解除したり、再度選択したりする必要があります。

1つのボリューム上のすべてのデータベースは、Snapshotを使用して同時にバックアップされます。同時バックアップデータベースの最大数が35で、ストレージボリュームに格納されているデータベースが35を超える場合は、データベース数を35で割った数のSnapshotが作成されます。



バックアップポリシーでは、Snapshotごとの最大データベース数を設定できます。

SnapCenterがSnapshotを作成すると、ストレージ・システム・ボリューム全体がSnapshotにキャプチャされます。ただし、バックアップは、バックアップが作成されたSQLホストサーバに対してのみ有効です。

他のSQLホストサーバのデータが同じボリューム上にある場合、このデータをSnapshotからリストアすることはできません。

- 詳細はこちら *

["リソースの休止処理またはグループ化処理が失敗する"](#)

リソースをバックアップに使用できるかどうかの確認

リソースとは、インストールしたプラグインで管理されるデータベース、アプリケーションインスタンス、可用性グループなどのコンポーネントです。これらのリソースをリソースグループに追加してデータ保護ジョブを実行できますが、その前に使用可能なリソースを特定しておく必要があります。使用可能なリソースを確認することで、プラグインのインストールが正常に完了したことの確認にもなります。

開始する前に

- SnapCenterサーバのインストール、ホストの追加、ストレージシステム接続の作成、クレデンシャルの追加などのタスクを完了しておく必要があります。
- Microsoft SQLデータベースを検出するには、次のいずれかの条件を満たしている必要があります。
 - SnapCenter サーバにプラグインホストを追加したユーザには、Microsoft SQL Server に対して必要な権限（sysadmin）が割り当てられている必要があります。
 - 上記の条件を満たしていない場合は、SnapCenter サーバで、Microsoft SQL Server に対して必要な権限（sysadmin）を持つユーザを設定する必要があります。ユーザはMicrosoft SQL Serverインスタンスレベルで設定する必要があります。ユーザはSQLユーザまたはWindowsユーザです。
- Windowsクラスタ内のMicrosoft SQLデータベースを検出するには、フェイルオーバークラスタインスタンス（FCI）TCP/IPポートのブロックを解除する必要があります。
- データベースがVMware RDM LUNまたはVMDK上にある場合は、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録する必要があります。

詳細については、[を参照してください。](#) ["SnapCenter Plug-in for VMware vSphereの導入"](#)

- ホストにgMSAを追加し、gMSAにログインしてシステム管理Privilegesがある場合は、gMSAを使用してSQLインスタンスに接続されます。

タスクの内容

[詳細] ページの [全体のステータス *] オプションが [バックアップに使用できない] に設定されている場合

は、データベースをバックアップできません。次のいずれかに該当する場合、* Overall Status * オプションはバックアップに使用できない状態に設定されます。

- データベースが NetApp LUN 上にない。
- データベースが正常な状態でない。

データベースがオフライン、リストア中、リカバリの保留中、サスペクトなどの状態です。

- データベースに十分な権限がありません。

たとえば、ユーザにデータベースへの表示アクセス権しかない場合、データベースのファイルとプロパティを特定できないため、バックアップすることはできません。



SQL Server Standard Editionで可用性グループが設定されている場合、SnapCenterでバックアップできるのはプライマリデータベースのみです。

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、* View * ドロップダウン・リストから * Database *、* Instance *、または * Availability Group * を選択します。

をクリックし、ホスト名とSQL Serverインスタンスを選択してリソースをフィルタリングします。そのあとに  をクリックすると、フィルタ ペインが閉じます。

3. [リソースの更新] をクリックします。

新しく追加、名前変更、または削除されたリソースは、SnapCenterサーバインベントリに更新されます。



SnapCenter以外でデータベースの名前が変更された場合は、リソースを更新する必要があります。

リソースは、リソースタイプ、ホストまたはクラスタ名、関連するリソースグループ、バックアップタイプ、ポリシー、全体的なステータスなどの情報とともに表示されます。

- データベースがNetApp以外のストレージにある場合は、Not available for backup *[全体のステータス]*列にと表示されます。

NetApp以外のストレージにあるデータベースに対しては、データ保護処理を実行できません。

- データベースがNetAppストレージにあり、保護されていない場合は、Not protected *[全体のステータス]*列にと表示されます。
- データベースがNetAppストレージシステム上にあり、保護されている場合は、ユーザインターフェイスの*[全体のステータス]*列にメッセージが表示されます Backup not run。
- データベースがNetAppストレージシステム上にあり、保護されている場合に、そのデータベースのバックアップがトリガーされると、ユーザインターフェイスの* Overall Status *列にメッセージが表示されます Backup succeeded。



クレデンシャルの設定時にSQL認証を有効にした場合は、検出されたインスタンスまたはデータベースに赤い鍵のアイコンが表示されます。南京錠のアイコンが表示された場合は、リソースグループに追加するインスタンスまたはデータベースのクレデンシャルを指定する必要があります。

1. SnapCenter 管理者がリソースを RBAC ユーザに割り当てたら、RBAC ユーザはログインし、[* リソースの更新 *] をクリックして、リソースの最新の * 全体的なステータス * を確認する必要があります。

NetAppストレージシステムへのリソースの移行

SnapCenter Plug-in for Microsoft Windows を使用してネットアップストレージシステムをプロビジョニングしたら、SnapCenter グラフィカルユーザインターフェイス（GUI）または PowerShell コマンドレットを使用して、リソースをネットアップストレージシステムに移行するか、またはあるネットアップ LUN から別のネットアップ LUN に移行できます。

開始する前に

- SnapCenter サーバにストレージシステムを追加しておく必要があります。
- SQL Serverリソースをリフレッシュ（検出）しておく必要があります。

ウィザードの各ページのフィールドのほとんどはわかりやすいもので、説明を必要としません。以下の手順では、説明が必要な一部のフィールドを取り上げます。

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 *] ドロップダウン・リストから [* データベース *] または [* インスタンス *] を選択します。
3. リストからデータベースまたはインスタンスを選択し、* Migrate * をクリックします。
4. リソースページで、次の操作を実行します。

フィールド	操作
• データベース名 *（オプション）	移行用のインスタンスを選択した場合は、そのインスタンスのデータベースを「* Databases *」ドロップダウンリストから選択する必要があります。
• 目的地を選択 *	データファイルとログファイルの保存先を選択します。 データファイルとログファイルは、選択したネットアップドライブの下の Data フォルダと Log フォルダにそれぞれ移動されます。フォルダ構造内にフォルダが存在しない場合は、フォルダが作成され、リソースが移行されます。

フィールド	操作
<ul style="list-style-type: none"> データベースファイルの詳細を表示 * (オプション) 	<p>1つのデータベースの複数のファイルを移行する場合は、このオプションを選択します。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>このオプションは、* Instance * リソースを選択した場合には表示されません。</p> </div>
<ul style="list-style-type: none"> オプション * 	<p>「* 元の場所にある移行済みデータベースのコピーを削除する *」を選択して、ソースからデータベースのコピーを削除します。</p> <p>オプション：* データベースの接続を解除する前にテーブルに対して UPDATE STATISTICS を実行します。 *</p>

5. 検証ページで、次の操作を実行します。

フィールド	操作
<ul style="list-style-type: none"> データベース整合性チェックオプション * 	<p>移行前にデータベースの整合性をチェックするには、* Run Before * を選択します。移行後にデータベースの整合性をチェックするには、* Run After * を選択します。</p>

フィールド	操作
*DBCC CHECKDB オプション *	<ul style="list-style-type: none"> • 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、「* physical_only *」オプションを選択します。 • すべての情報メッセージを停止するには、「* NO_INFOMSGS *」オプションを選択します。 • 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には、* ALLERRORGS* オプションを選択します。 • 非クラスタ化インデックスをチェックしない場合は、* noindex * オプションを選択します。 <p>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。</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p>このオプションを選択すると、実行時間を短縮できます。</p> </div> <ul style="list-style-type: none"> • 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、チェックを制限してロックを取得するには、TABLOCKオプションを選択します。

6. 概要を確認し、[終了]をクリックします。

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。

開始する前に

- データ保護戦略を定義しておく必要があります。
- SnapCenter のインストール、ホストの追加、リソースの特定、ストレージシステム接続の作成などのタスクを実行して、データ保護の準備をしておく必要があります。
- ログバックアップ用のホストログディレクトリを設定しておく必要があります。
- SQL Serverリソースをリフレッシュ（検出）しておく必要があります。
- Snapshotをミラーまたはバックアップにレプリケートする場合は、SnapCenter管理者がソースボリュームとデスティネーションボリュームの両方のStorage Virtual Machine (SVM) をユーザに割り当てておく必要があります。

管理者によるユーザへのリソースの割り当て方法については、SnapCenterのインストール情報を参照してください。

- プリ스크립トとポストスクリプトでPowerShellスクリプトを実行する場合は、web.configファイルでusePowershellProcessforScriptsパラメータの値をtrueに設定する必要があります。

デフォルト値はfalseです。

- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、を参照してください ["SnapMirrorアクティブ同期のオブジェクト数の制限"](#)。

タスクの内容

- バックアップポリシーは、バックアップを管理および保持する方法、およびリソースまたはリソースグループをバックアップする頻度を規定する一連のルールです。レプリケーションとスクリプトの設定を指定することもできます。ポリシーでオプションを指定することで、別のリソースグループにポリシーを再利用して時間を節約できます。

scripts_pathは、プラグインホストのSMCoreServiceHost.exe.ConfigファイルにあるPredefinedWindowsScriptsDirectoryキーを使用して定義します。

必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

キーの値は、api/4.7/configsettingsを介してSwaggerから表示できます

GET APIを使用すると、キーの値を表示できます。Set APIはサポートされていません。

• SnapLock

- [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。

Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、保持されるSnapshotの数がポリシーで指定されている数よりも多くなる可能性があります。

ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLockヴォールトSnapshotから作成されたクローンにSnapLockヴォールトの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順1：ポリシー名を作成します

1. 左側のナビゲーションペインで、*[設定]*を選択します。
2. [設定]ページで、*[ポリシー]*を選択します。
3. [New]*を選択します。
4. [名前*]ページで、ポリシーの名前と詳細を入力します。

手順2：ポリシーオプションを設定する

1. [Policy type]ページで、次の手順を実行します。

- a. ストレージタイプを選択します。
- b. ポリシーの範囲を選択します。

フルバックアップとログバックアップ

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し、トランザクションログを切り捨てます。

- i. [フルバックアップおよびログバックアップ*]を選択します。
- ii. Snapshotごとにバックアップするデータベースの最大数を入力します。



同時に複数のバックアップ処理を実行する場合は、この値を増やす必要があります。

フルバックアップ

データベースファイルをバックアップします。

- i. [* Full backup*]を選択します。
- ii. Snapshotごとにバックアップするデータベースの最大数を入力します。デフォルト値は100



同時に複数のバックアップ処理を実行する場合は、この値を増やす必要があります。

ログバックアップ

- i. トランザクションログをバックアップします。
- ii. 「* Log backup *」を選択します。

コピーのみのバックアップ

- i. 別のバックアップ・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。

トランザクションログをそのまま保持すると、すべてのバックアップアプリケーションでデータベースをリストアできます。通常、他の状況ではコピーのみのオプションを使用しないでください。



Microsoft SQL では、セカンダリ・ストレージのフル・バックアップおよびログ・バックアップ* オプションと * コピーのみのバックアップ* オプションはサポートされていません。

手順3：可用性グループを設定する

1. 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。
 - a. 優先バックアップレプリカのみにバックアップ。

優先バックアップレプリカのみをバックアップする場合は、このオプションを選択します。優先バックアップレプリカは、SQL ServerのAGに対して設定されたバックアップ設定によって決まります。

- b. バックアップするレプリカを選択します。

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。

- c. バックアップ優先度の選択（最小および最大バックアップ優先度）

バックアップのAGレプリカを決定する最小バックアップ優先順位と最大バックアップ優先順位を指定します。たとえば、最小優先度を10、最大優先度を50に設定できます。この場合、優先度が10より大きく50未満のすべてのAGレプリカがバックアップ対象とみなされます。

デフォルトでは、最小プライオリティは1、最大プライオリティは100です。



クラスタ構成では、ポリシーで設定された保持設定に従って、バックアップがクラスタの各ノードで保持されます。AGの所有者ノードが変更された場合、保持設定に従ってバックアップが作成され、以前の所有者ノードのバックアップが保持されます。AGの保持設定はノードレベルでのみ適用されます。

手順4：Snapshotとレプリケーションの設定を構成する

1. [Snapshot and Replication]ページで、次の手順を実行します。

- a. スケジュールタイプを指定するには、「* on demand *」、「* Hourly *」、「* Daily *」、「* Weekly *」、または「* Monthly *」を選択します。

ポリシーに対して選択できるスケジュールタイプは1つだけです。



リソースグループを作成する際に、バックアップ処理のスケジュール（開始日、終了日、頻度）を指定できます。これにより、ポリシーとバックアップ頻度が同じであるリソースグループを作成できますが、各ポリシーに異なるバックアップスケジュールを割り当てることができます。



午前2時にスケジュールを設定している場合、夏時間（DST）中はスケジュールはトリガーされません。

手順5：最新の状態へのリストア保持を設定する

1. [Up-to-the-minute retention settings]セクションで、[Backup type]ページで選択したバックアップタイプに応じて、次の操作を1つ以上実行します。

特定のコピー数

特定の数のSnapshotのみを保持します。

1. [*最新の<日数>日数に適用可能なログバックアップを保持する] オプションを選択し、保持する日数を指定します。この上限に近づいた場合は、古いコピーを削除できます。

特定の日数

バックアップコピーを特定の日数だけ保持します。

1. [*最新の<日数>フル・バックアップに適用可能なログ・バックアップを保持する] オプションを選択し、ログ・バックアップ・コピーを保持する日数を指定します。

手順6：Snapshotを設定する

1. フルバックアップの保持設定では、次の操作を実行します。

- a. 保持するSnapshotの総数を指定してください

- i. 保持するSnapshotの数を指定するには、*保持するコピー*を選択します。
- ii. Snapshotの数が指定した数を超えると、最も古いコピーから順にSnapshotが削除されます。



デフォルトでは、保持数の値は2に設定されています。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗する可能性があります。



最大保持値は1018です。保持数を使用しているNetApp ONTAPバージョンでサポートされる値よりも大きい値に設定すると、バックアップは失敗します。

2. Snapshotを保持する時間の長さ

- a. Snapshotを保持してから削除するまでの日数を指定する場合は、*[コピーの保持期間]*を選択します。

3. スナップショット コピーのロック期間 を選択し、期間を日数、月数、または年数で指定します。

SnapLock保持期間は100年未満にする必要があります。

4. ポリシーラベルを選択します。



リモート レプリケーションのプライマリ スナップショットにSnapMirrorラベルを割り当てることで、プライマリ スナップショットによってスナップショット レプリケーション操作をSnapCenterからONTAPセカンダリ システムにオフロードできるようになります。これは、ポリシー ページでSnapMirrorまたはSnapVaultオプションを有効にしなくても実行できます。

手順7：セカンダリレプリケーションオプションを設定する

1. [Select secondary replication options]セクションで、次のセカンダリレプリケーションオプションの一方または両方を選択します。

SnapMirrorの更新

ローカルSnapshotコピーの作成後にSnapMirrorを更新します。

1. 別のボリュームにバックアップセットのミラーコピーを作成する場合（SnapMirror）は、このオプションを選択します。

このオプションは、SnapMirrorのアクティブな同期に対して有効にする必要があります。

セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。[Topology]ページの[Refresh]*ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリのSnapLock有効期限が更新されます。

を参照して "[\[Topology\]ページでのSQL Serverのバックアップとクローンの表示](#)"

SnapVaultの更新

Snapshotコピーの作成後にSnapVault を更新

1. ディスクツーディスクのバックアップレプリケーションを実行する場合は、このオプションを選択します。

セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。[Topology]ページの[Refresh]*ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリのSnapLock有効期限が更新されます。

SnapLockがONTAPのセカンダリ（SnapLock Vault）にのみ設定されている場合、[Topology]ページの*[Refresh]*ボタンをクリックすると、ONTAPから取得したセカンダリのロック期間が更新されます。

SnapLock Vaultの詳細については、を参照してください。 "[SnapVaultデスティネーションでSnapshotコピーをWORM状態にコミットする](#)"

を参照して "[\[Topology\]ページでのSQL Serverのバックアップとクローンの表示](#)"

エラー再試行回数

1. レプリケーションの最大試行回数を入力します。この回数を超えると処理が停止します。

手順8：スクリプト設定を構成します

1. 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。

たとえば、SNMPトラップの更新、アラートの自動化、ログの送信を行うスクリプトを実行できます。



プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathからの相対パスである必要があります。



セカンダリストレージがSnapshotの最大数に達しないように、ONTAPでSnapMirror保持ポリシーを設定する必要があります。

手順9：検証設定を構成します

[Verification] ページで、次の手順を実行します。

1. 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。
2. Database consistency check options セクションで、次の操作を実行します。
 - a. 整合性構造をデータベースの物理構造に制限する (physical_only)
 - 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。
 - b. すべての情報メッセージを抑制 (INFOMSGSなし)
 - i. すべての情報メッセージを停止するには、「*」を選択します (NO_INFOMSGS)。デフォルトで選択されています。
 - c. レポートされたすべてのエラーメッセージをオブジェクトごとに表示する (ALL_ERRORMSGs)
 - i. 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。
 - d. クラスタ化されていないインデックスをチェックしない (NOINDEX)
 - i. 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。
 - e. 内部データベーススナップショット (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
 - i. 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。
3. [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。
4. 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。



プリスクリプトまたはポストスクリプトのパスにドライブまたは共有を含めることはできません。パスはscripts_pathからの相対パスである必要があります。

ステップ10：概要を確認します

1. 概要を確認し、*[終了]*を選択します。

SQL Serverのリソースグループの作成とポリシーの適用

リソースグループはコンテナであり、一緒にバックアップして保護するリソースを追加します。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。

リソースを個別に保護する場合、新しいリソースグループを作成する必要はありません。保護されたリソースでバックアップを作成することができます。

タスクの内容

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期が設定されていない新しいデータベースを、SnapMirrorアクティブ同期が設定されたリソースを含む既存のリソースグループに追加することはできません。
- SnapMirror Active Syncのフェイルオーバーモードでは、既存のリソースグループに新しいデータベースを追加することはできません。リソースグループにリソースを追加できるのは、通常の状態またはフェイルバック状態のみです。

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*]を選択します。



最近 SnapCenter にリソースを追加した場合は、[*リソースの更新*]をクリックして、新しく追加したリソースを表示します。

3. [New Resource Group] をクリックします。
4. [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	リソースグループ名を入力します。  リソースグループ名は250文字以内にする必要があります。
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。たとえば、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。
Snapshotコピーにカスタムの名前形式を使用する	オプション：Snapshotのカスタムの名前と形式を入力します。たとえば、customText_resourcegroup_policy_hostname やresourcegroup_hostnameなどです。デフォルトでは、Snapshot名にタイムスタンプが追加されません。

5. Resources ページで、次の手順を実行します。

- a. ホスト名、リソースタイプ、およびSQL Serverインスタンスをドロップダウンリストから選択して、リソースのリストをフィルタリングします。



最近リソースを追加した場合は、リソースリストを更新しないと、使用可能なリソースのリストにリソースが表示されません。

- b. [使用可能なリソース] セクションから [選択したリソース] セクションにリソースを移動するには、次のいずれかの手順を実行します。
 - 同じボリューム上のすべてのリソースを [選択したリソース] セクションに移動するには、* 同一ストレージボリューム上のすべてのリソースを自動選択 * 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)] セクションに移動する。

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。



**をクリックしてポリシーを作成することもできます 。

[選択したポリシーのスケジュールを設定] セクションに、選択したポリシーが一覧表示されます。

- b. [Configure schedules for selected policies] セクションで、スケジュールを設定するポリシーの [Configure Schedules] 列にある***をクリックします 。
- c. [Add schedules for policy_name_] ダイアログボックスで、開始日、有効期限、頻度を指定してスケジュールを設定し、[*OK] をクリックします。

この処理は、ポリシーに指定されている頻度ごとに実行する必要があります。設定されたスケジュールは、[選択したポリシーのスケジュールの設定 *] セクションの [適用されたスケジュール] 列に一覧表示されます。

- d. Microsoft SQL Server スケジューラを選択します。

スケジュールポリシーに関連付けるスケジューラインスタンスも選択する必要があります。

[Microsoft SQL Server scheduler] を選択しない場合、デフォルトは [Microsoft Windows scheduler] になります。

サードパーティのバックアップスケジュールが SnapCenter バックアップスケジュールと重複している場合はサポートされません。Windows スケジューラまたは SQL Server エージェントで作成されたバックアップジョブのスケジュールを変更したり、名前を変更したりしないでください。

7. [Verification] ページで、次の手順を実行します。

- a. [* Verification server*] ドロップダウン・リストから検証サーバを選択します。

このリストには、SnapCenter で追加されたすべての SQL Server が含まれます。検証サーバ (ローカルホストまたはリモートホスト) は複数選択できます。



検証サーバのバージョンは、プライマリデータベースをホストしているSQLサーバのバージョンおよびエディションと一致している必要があります。

- a. Load locators * (ロケータのロード) をクリックして、 SnapMirror ボリュームと SnapVault ボリュームをロードし、セカンダリ・ストレージ上で検証を実行します。
- 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. [Add Verification Schedules policy_name]ダイアログボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	[Run verification after backup] を選択します。
検証のスケジュールを設定	[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。

設定されたスケジュールは、[適用されたスケジュール]列に一覧表示されます。確認して編集するに

はをクリックし、削除するに  はをクリックします 。

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。

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。リソースグループで実行された操作のレポートを添付する場合は、[ジョブレポートの添付 (Attach Job Report)] を選択します。



Eメール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtServerを使用して、SMTPサーバの詳細を指定しておく必要があります。

9. 概要を確認し、[完了]をクリックします。

関連情報

["SQL Serverデータベースのバックアップポリシーの作成"](#)

ASA R2システム上のMicrosoft SQL Serverリソースに対してリソースグループを作成し、セカンダリ保護を有効にする

リソースグループを作成して、ASA R2システム上のリソースを追加する必要があります。リソースグループの作成時にセカンダリ保護をプロビジョニングすることもできます。

開始する前に

- ONTAP 9.xリソースとASA R2リソースの両方を同じリソースグループに追加しないでください。

- ONTAP 9.xリソースとASA R2リソースの両方を含むデータベースがないことを確認してください。

タスクの内容

- セカンダリ保護は、ログインしているユーザに「* SecondaryProtection *」機能が有効なロールが割り当てられている場合にのみ使用できます。
- セカンダリ保護を有効にした場合、プライマリおよびセカンダリ整合グループの作成時にリソースグループがメンテナンスモードになります。プライマリとセカンダリの整合グループが作成されると、リソースグループはメンテナンスモードを終了します。
- SnapCenterでは、クローンリソースのセカンダリ保護はサポートされません。

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、[* 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。

- a. [Name]フィールドにリソースグループの名前を入力します。



リソースグループ名は250文字以内にする必要があります。

- b. 後でリソースグループを検索できるように、[Tag]フィールドに1つ以上のラベルを入力します。

たとえば、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。

- c. 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。

たとえば、customText_resource group_policy_hostnameやresource group_hostnameなどです。デフォルトでは、Snapshot名にタイムスタンプが追加されます。

- d. バックアップしない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。



必要に応じて、プレフィックスを含め、アプリケーションで設定されたものとまったく同じ宛先を使用する必要があります。

4. [リソース] ページで、*[ホスト]*ドロップダウンリストからデータベースホスト名を選択します。



リソースが Available Resources セクションに表示されるのは、リソースが正常に検出された場合のみです。最近追加したリソースは、リソースリストを更新するまで使用可能なリソースのリストに表示されません。

5. [Available Resources]セクションからASA R2リソースを選択し、[Selected Resources]セクションに移動します。
6. [Application Settings] ページで、バックアップオプションを選択します。
7. [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。



をクリックしてポリシーを作成することもできます。

[選択したポリシーのスケジュールを設定] セクションに、選択したポリシーが一覧表示されます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、 をクリックします。
- c. [Add schedules for policy_name] ウィンドウで、スケジュールを設定し、**[OK]** をクリックします。

ここで、_policy_name_は 選択したポリシーの名前です。

設定されたスケジュールは、[適用されたスケジュール] 列に一覧表示されます。

サードパーティのバックアップスケジュールがSnapCenterバックアップスケジュールと重複している場合はサポートされません。

8. 選択したポリシーでセカンダリ保護が有効になっている場合は、[Secondary Protection]ページが表示され、次の手順を実行する必要があります。

- a. レプリケーションポリシーのタイプを選択します。



同期レプリケーションポリシーはサポートされていません。

- b. 使用する整合グループサフィックスを指定します。
- c. [デスティネーションクラスタ]と[デスティネーションSVM]のドロップダウンで、使用するピアクラスタとSVMを選択します。



クラスタとSVMのピアリングはSnapCenterではサポートされていません。クラスタとSVMのピアリングを実行するには、System ManagerまたはONTAP CLIを使用する必要があります。



リソースがSnapCenterの外部ですでに保護されている場合、それらのリソースは[Secondary Protected Resources]セクションに表示されます。

1. [Verification]ページで、次の手順を実行します。
 - a. Load locators * (ロケータのロード) をクリックして、SnapMirror または SnapVault ボリュームをロードし、セカンダリ・ストレージ上で検証を実行します。
 - b. [Configure Schedules]列内をクリックし  て、ポリシーのすべてのスケジュールタイプに対して検証スケジュールを設定します。
 - c. [Add Verification Schedules policy_name]ダイアログボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	[Run verification after backup] を選択します。

状況	操作
検証のスケジュールを設定	[Run scheduled verification] を選択し、ドロップダウン・リストからスケジュール・タイプを選択します。

- d. セカンダリ・ストレージ・システムのバックアップを検証するには、セカンダリ・サイトで * Verify on secondary location * を選択します。
- e. [OK]*をクリックします。

設定した検証スケジュールは、Applied Schedules 列にリスト表示されます。

2. [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。リソースグループで実行された操作のレポートを添付する場合は、[ジョブレポートの添付 (Attach Job Report)] を選択します。



Eメール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtServerを使用して、SMTPサーバの詳細を指定しておく必要があります。

3. 概要を確認し、[完了]をクリックします。

SQLリソースノハツクアツフノヨウケン

SQLリソースをバックアップする前に、いくつかの要件を満たしていることを確認する必要があります。

- ネットアップ以外のストレージシステムからNetAppストレージシステムにリソースを移行しておく必要があります。
- バックアップポリシーを作成しておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合は、ストレージユーザに割り当てられた ONTAP ロールに「"napmirror all"」権限を含める必要があります。ただし、「vsadmin」ロールを使用している場合、「'SnapMirro all」権限は必要ありません。
- Active Directory (AD) ユーザが開始したバックアップ処理は、そのADユーザまたはグループにSQLインスタンスクレデンシャルが割り当てられていないと失敗します。SQL インスタンスの資格情報は、* 設定 * > * ユーザーアクセス * ページから AD ユーザーまたはグループに割り当てる必要があります。
- ポリシーを適用してリソースグループを作成しておく必要があります。
- リソースグループに異なるホストの複数のデータベースが含まれている場合、ネットワークの問題が原因で、一部のホストでのバックアップ処理が遅くトリガーされることがあります。Set-SmConfigSettings PSコマンドレットを使用して、web.configでFMaxRetryForUninitializedHostsの値を設定する必要があります。

PowerShellコマンドレットを使用してストレージシステム接続とクレデンシャルを作成する

PowerShellコマンドレットを使用してデータ保護処理を実行するには、Storage Virtual Machine (SVM) 接続とクレデンシャルを作成しておく必要があります。

開始する前に

- PowerShellコマンドレットを実行できるようにPowerShell環境を準備しておく必要があります。
- ストレージ接続を作成するには、Infrastructure Adminロールに必要な権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

ホスト・プラグインのインストールは'ストレージ・システム接続の追加中は実行しないでくださいホスト・キャッシュが更新されず'データベース・ステータスが SnapCenter GUI に表示される場合がありますこれは'バックアップには使用できませんまたは NetApp ストレージには使用できません

- ストレージシステム名は一意である必要があります。

SnapCenter では、異なるクラスタに同じ名前のストレージシステムを複数配置することはサポートされていません。SnapCenterでサポートする各ストレージシステムには、一意の名前と一意の管理LIF IPアドレスが必要です。

手順

1. Open-SmConnectionコマンドレットを使用して、PowerShell Core接続セッションを開始します。

この例では、PowerShellセッションを開きます。

```
PS C:\> Open-SmConnection
```

2. Add-SmStorageConnectionコマンドレットを使用して、ストレージシステムへの新しい接続を作成します。

新しいストレージシステム接続を作成する例を次に示します。

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Add-SmCredentialコマンドレットを使用して、新しいクレデンシャルを作成します。

この例では、Windowsクレデンシャルを使用してFinanceAdminという新しいクレデンシャルを作成します。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

コマンドレットで使用できるパラメータとその説明については、`RUN_Get-Help` コマンド `NAME` を実行して参照できます。または、を参照することもできます "[SnapCenter ソフトウェアコマンドレットリファレンスガイド](#)"。

SQLリソ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。

タスクの内容

- バックアップ処理を最適化するには、Windowsクラスタ名とIPアドレスのリバースルックアップレコードをDNSサーバに作成する必要があります。
- Windowsクレデンシャル認証の場合、プラグインのインストール前にクレデンシャルを設定する必要があります。
- SQL Serverインスタンス認証の場合、プラグインのインストール後にクレデンシャルを追加する必要があります。
- gMSA 認証の場合 'gMSA を有効にして使用するには '**Add Host** ページまたは **Modify Host** ページで SnapCenter にホストを登録するときに gMSA を設定する必要があります
- gMSAを使用してホストを追加し、gMSAにログインおよびシステム管理者権限があれば、gMSAからSQLインスタンスへの接続が許可されます。
 - SnapCenterは、SQLインスタンスの認証が設定されているかどうかを検証します。認証が設定されている場合、このクレデンシャルを使用してSQLインスタンスにアクセスします。
 - 認証が設定されていない場合は、gMSAを使用してSQLプラグインが現在動作しているかどうかを確認します。プラグインが動作している場合は、SQLインスタンスへの接続の確立に使用されます。
 - SQLインスタンスの両方の認証が設定されておらず、プラグインが動作していない場合、SQLインスタンスはWindowsクレデンシャル認証を介してアクセスされます。

SnapCenter UI

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*、*インスタンス*、または*可用性グループ*を選択します。

- a. バックアップするデータベース、インスタンス、または可用性グループを選択します。

インスタンスのバックアップを作成する場合、そのインスタンスの前のバックアップステータスやタイムスタンプに関する情報はリソースページに表示されません。

トポロジビューでは、バックアップステータス、タイムスタンプ、バックアップがインスタンスのものかデータベースのものかを区別できません。

3. [リソース]ページで、[Snapshotコピーのカスタム名形式]*チェックボックスを選択し、Snapshot名に使用するカスタムの名前形式を入力します。

たとえば、customText_policy_hostnameやresource_hostnameなどです。デフォルトでは、Snapshot名にタイムスタンプが追加されます。

4. [Policies] ページで、次のタスクを実行します。

- a. [Policies] セクションで、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。

ポリシーを作成するには、**を選択し  てポリシーウィザードを開始します。

[選択したポリシーのスケジュールを設定する*]セクションに、選択したポリシーが一覧表示されます。

- 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. [ポリシーのスケジュールを追加]* 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` 選択したポリシーの名前が表示されます。

設定されたスケジュールは、[* Applied Schedules] 列に表示されます。

- a. Microsoft SQL Server スケジューラを使用する * を選択し、スケジューリング・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. [* Verification server*] ドロップダウン・リストから検証サーバを選択します。

検証サーバ（ローカルホストまたはリモートホスト）は複数選択できます。



検証サーバのバージョンは、プライマリデータベースをホストしているSQL Serverのエディションのバージョン以上である必要があります。

- a. セカンダリ・ストレージ・システム上のバックアップを検証するには 'セカンダリ・ロケータをロード' 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、**を選択します 。
- c. Add Verification Schedules_policy_name_dialog box で、次の処理を実行します。

状況	操作
バックアップ後に検証を実行	[バックアップ後に検証を実行] を選択します。
検証のスケジュールを設定	[スケジュールされた検証を実行する] を選択します。



検証サーバでストレージ接続が確立されていないと、検証処理は失敗して「Failed to mount disk」というエラーメッセージが表示されます。

- d. 「* OK *」を選択します。

設定されたスケジュールは、[適用されたスケジュール] 列に一覧表示されます。

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。

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。リソースグループで実行された操作のレポートを添付する場合は、[ジョブレポートの添付 (Attach Job Report)] を選択します。



Eメール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtServerを使用して、SMTPサーバの詳細を指定しておく必要があります。

7. 概要を確認し、*[終了]*を選択します。

データベーストポロジページが表示されます。

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を適用している場合は、「* Policy *」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. 「* Verify after backup *」を選択して、バックアップを検証します。

c. 「 * Backup * 」を選択します。



WindowsスケジューラまたはSQL Serverエージェントで作成されたバックアップジョブの名前は変更しないでください。

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。

暗黙的なリソースグループが作成されます。これを表示するには、[User Access]ページでそれぞれのユーザまたはグループを選択します。暗黙的なリソースグループタイプは「リソース」です。

10. 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。

終了後

- MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

"MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"

- VMDK上のアプリケーションデータをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープサイズが十分でないと、バックアップが失敗することがあります。Javaヒープサイズを増やすには、スクリプトファイル/opt/netapp/init_scripts/scvserviceを探します。このスクリプトでは、コマンドによって do_start method SnapCenter VMwareプラグインサービスが開始されます。このコマンドを次のように更新し `Java -jar -Xmx8192M -Xms4096M` ます。

関連情報

"SQL Serverデータベースのバックアップポリシーの作成"

"Windowsスケジューラエラーでバックアップが失敗する"

"リソースの休止処理またはグループ化処理が失敗する"

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定したユーザのSnapCenterサーバとの接続セッションを開始します。

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmPolicyコマンドレットを使用して、バックアップポリシーを作成します。

この例では、SQLバックアップタイプがFULLBACKUPの新しいバックアップポリシーを作成しています。

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

この例では、WindowsファイルシステムのバックアップタイプがCrashConsistentの新しいバックアップポリシーを作成しています。

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Get-SmResourcesコマンドレットを使用して、ホストリソースを検出します。

この例では、指定したホストでMicrosoft SQLプラグインのリソースを検出しています。

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

この例では、指定したホスト上のWindowsファイルシステムのリソースを検出しています。

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Add-SmResourceGroupコマンドレットを使用して、SnapCenterに新しいリソースグループを追加します。

この例では、ポリシーとリソースを指定して新しいSQLデータベースバックアップリソースグループを作成しています。

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

この例では、ポリシーとリソースを指定して新しいWindowsファイルシステムバックアップリソースグループを作成します。

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. New-SmBackupコマンドレットを使用して、新しいバックアップジョブを開始します。

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy FinancePolicy
```

6. Get-SmBackupReportコマンドレットを使用して、バックアップジョブのステータスを表示します。

次に、指定した日付に実行されたすべてのジョブのジョブ概要レポートを表示する例を示します。

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

コマンドレットで使用できるパラメータとその説明については、RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "[SnapCenter ソフトウェアコマンドレットリファレンスガイド](#)"。

SQL Serverリソースグループのバックアップ

リソースグループは、[Resources]ページからオンデマンドでバックアップできます。リソースグループにポリシーが適用され、スケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが実行されます。

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。

リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、を選択しでタグを選択します。その後、を選択してフィルタペインを閉じることができます.

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. 複数のポリシーをリソースグループに関連付けている場合は、「* Policy *」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せん。

- 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。

ポリシーの * verify * オプションは、スケジュールされたジョブにのみ適用されます。

- 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データベースのバックアップポリシーの作成"

"SQL Serverのリソースグループの作成とポリシーの適用"

"Windowsスケジューラエラーでバックアップが失敗する"

SnapCenterジョブページでSQLリソースのバックアップ処理を監視する

[SnapCenterJobs]ページを使用して、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

-  実行中
-  完了済み
-  失敗
-  完了（警告あり）または警告のため開始できませんでした
-  キューに登録済み
-  キャンセル済み

手順

1. 左側のナビゲーションペインで、**Monitor** をクリックします。
2. [モニター] ページで、[* ジョブ *] をクリックします。
3. Jobs（ジョブ） ページで、次の手順を実行します。
 - a. をクリックして、リストの内容をバックアップ処理だけに絞り込みます。
 - b. 開始日と終了日を指定します。
 - c. [* タイプ] ドロップダウン・リストから、[*Backup] を選択します。
 - d. [Status](ステータス*) ドロップダウンから、バックアップステータスを選択します。
 - e. [適用 (Apply)] をクリックして、正常に完了した操作を表示する。
4. バックアップジョブを選択し、[* 詳細 *] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスは表示されますが 、ジョブの詳細をクリックすると、バックアップ処理の子タスクの一部が進行中であるか、警告サインが表示されていることがあります。

5. [ジョブの詳細] ページで、[* ログの表示 *] をクリックします。

View logs ボタンをクリックすると、選択した操作の詳細なログが表示されます。

[Activity]ペインで、SQLリソースに対するデータ保護処理を監視する

[アクティビティ (Activity)]パネルには、最近実行された5つの操作が表示されまた、操作が開始された日時と操作のステータスも表示されます。

[Activity (アクティビティ)]ペインには、バックアップ、リストア、クローン、およびスケジュールされたバックアップ処理に関する情報が表示されます。

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. [Activity]ペインでをクリックすると、ペインアイコン] 最新の5つの処理が表示されます。

いずれかの処理をクリックすると、*[ジョブの詳細]*ページに処理の詳細が表示されます。

SnapCenter Plug-in for Microsoft SQL Serverのバックアップ処理をキャンセルする

実行中、キューに格納されている、または応答しないバックアップ処理をキャンセルできます。バックアップ処理をキャンセルすると、作成されたバックアップがSnapCenterサーバに登録されていない場合、SnapCenterサーバは処理を停止し、ストレージからすべてのSnapshotを削除します。バックアップがすでにSnapCenterサーバに登録されている場合、キャンセルがトリガーされても、作成済みのSnapshotはロールバックされません。

開始する前に

- リストア処理をキャンセルするには、SnapCenter管理者またはジョブ所有者としてログインする必要があります。
- キャンセルできるのは、キューに登録されているか実行中のログ処理またはフルバックアップ処理だけです。
- 検証の開始後に処理をキャンセルすることはできません。

検証前に処理をキャンセルすると、処理はキャンセルされ、検証処理は実行されません。

- バックアップ処理は、[Monitor]ページまたは[Activity]ペインからキャンセルできます。
- SnapCenter GUIに加え、PowerShellコマンドレットを使用して処理をキャンセルすることもできます。
- キャンセルできない操作に対しては、[ジョブのキャンセル]ボタンが無効になっています。
- ロールの作成中に 'このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できるようにする * を選択した場合は 'そのロールを使用している間に '他のメンバーのキューに入っているバックアップ操作をキャンセルできます

手順

次のいずれかを実行します。

アクセス元	アクション
監視ページ	<ol style="list-style-type: none"> 1. 左側のナビゲーションペインで、[モニタ]>*[ジョブ]*を選択します。 2. ジョブを選択し、*[ジョブのキャンセル]*を選択します。
[Activity]ペイン	<ol style="list-style-type: none"> 1. バックアップジョブを開始したら、[Activity]ペインでを選択して、 [Activity]ペインアイコン"] 最新の5つの処理を表示します。 2. 処理を選択します。 3. [ジョブの詳細]ページで、*[ジョブのキャンセル]*を選択します。

結果

処理がキャンセルされ、リソースが以前の状態に戻ります。キャンセルした処理がキャンセルまたは実行中の状態で応答しない場合は、コマンドレットを実行してバックアップ処理を強制的に停止する必要があります

```
Cancel-SmJob -JobID <int> -Force。
```

[Topology]ページでのSQL Serverのバックアップとクローンの表示

リソースのバックアップまたはクローニングを準備するときに、プライマリストレージとセカンダリストレージ上のすべてのバックアップとクローンの図を表示すると役立つことがあります。

タスクの内容

[Topology]ページでは、選択したリソースまたはリソースグループに使用可能なすべてのバックアップとクローンを確認できます。これらのバックアップとクローンの詳細を表示し、選択してデータ保護処理を実行できます。

[コピーの管理 (Manage Copies)] ビューの次のアイコンを確認して、プライマリストレージまたはセカンダリストレージ (ミラーコピーまたはバックアップコピー) でバックアップとクローンが使用可能かどうかを判断できます。

- 
 プライマリストレージにあるバックアップとクローンの数が表示されます。
- 
 SnapMirrorテクノロジーを使用してセカンダリストレージにミラーリングされたバックアップとクローンの数が表示されます。
- 
 SnapVaultテクノロジーを使用してセカンダリストレージにレプリケートされたバックアップとクローンの数が表示されます。

- 表示されるバックアップの数には、セカンダリストレージから削除されたバックアップも含まれません。

たとえば、バックアップを4つだけ保持するポリシーを使用して6つのバックアップを作成した場合、バックアップの数は6と表示されます。



mirror-vaultタイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジビューに表示されますが、トポロジビューのミラーバックアップ数にはバージョンに依存しないバックアップは含まれません。

セカンダリ関係がSnapMirrorのアクティブな同期（当初はSnapMirrorビジネス継続性[SM-BC]としてリリース）である場合は、次のアイコンも表示されます。

-  レプリカサイトは稼働しています。
-  レプリカサイトはダウンしています。
-  セカンダリミラー関係またはバックアップ関係が再確立されていません。

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*]ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リソースの詳細ビューまたはリソースグループの詳細ビューでリソースを選択します。

選択したリソースがクローンデータベースの場合はクローンデータベースを保護し、[Topology]ページにクローンのソースが表示されます。詳細*をクリックして、クローニングに使用されたバックアップを表示します。

リソースが保護されている場合は、選択したリソースのトポロジページが表示されます。

4. [Summary]カードで、プライマリストレージとセカンダリストレージにあるバックアップとクローンの数の概要を確認します。

サマリカード*セクションには、バックアップとクローンの合計数が表示されます。

「*Refresh*」ボタンをクリックすると、ストレージの照会が開始され、正確な数が表示されます。

SnapLockが有効なバックアップが作成された場合、*[Refresh]*ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでは、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

アプリケーションリソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限がONTAPから取得されます。

SnapMirrorのアクティブな同期の場合、*[リフレッシュ]*ボタンをクリックすると、プライマリサイトとレプリカサイトの両方をONTAPに照会して、SnapCenterバックアップインベントリが更新されます。週次

スケジュールでは、SnapMirrorのアクティブな同期関係を含むすべてのデータベースに対してもこの処理が実行されます。

- SnapMirrorのアクティブな同期（ONTAP 9.14.1のみ）では、フェイルオーバー後に新しいプライマリデスティネーションに対する非同期ミラー関係または非同期ミラーバックアップ関係を手動で設定する必要があります。ONTAP 9.15.1以降では、新しいプライマリデスティネーションに対して非同期ミラーまたは非同期ミラーバックアップが自動的に設定されます。
- フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。[リフレッシュ]*をクリックできるのは、バックアップが作成されてからです。

5. [コピーの管理]表示で、プライマリ・ストレージまたはセカンダリ・ストレージから * バックアップ * または * クローン * をクリックして、バックアップまたはクローンの詳細を表示します。

バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、名前変更、削除の各処理を実行します。



セカンダリストレージにあるバックアップは、名前の変更や削除はできません。

7. テーブルからクローンを選択し、* Clone Split * をクリックします。
8. クローンを削除する場合は、表でクローンを選択し、 をクリックします。

PowerShellコマンドレットを使用したセカンダリバックアップ数のクリーンアップ

Snapshotがないセカンダリバックアップのバックアップ数をクリーンアップするには、Remove-SmBackupコマンドレットを使用します。このコマンドレットは、[Manage Copies]トポロジに表示されるSnapshotの総数が、セカンダリストレージのSnapshotの保持設定と一致しない場合に使用できます。

PowerShellコマンドレットを実行できるようにPowerShell環境を準備しておく必要があります。

コマンドレットで使用できるパラメータとその説明については、RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "[SnapCenter ソフトウェアコマンドレットリファレンスガイド](#)"。

手順

1. Open-SmConnectionコマンドレットを使用して、指定したユーザのSnapCenterサーバとの接続セッションを開始します。

```
Open-SmConnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. CleanupSecondaryBackupsパラメータを使用して、セカンダリバックアップ数をクリーンアップします。

この例では、Snapshotを含まないセカンダリバックアップのバックアップ数をクリーンアップしています。

```
Remove-SmBackup -CleanupSecondaryBackups
```

```
Remove-SmBackup
```

```
Are you sure want to remove the backup(s).
```

```
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help  
(default is "Y"):
```

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。