



Microsoft SQL Server

ワークコードを保護する

NetApp Backup and Recovery

NetApp
February 10, 2026

目次

Microsoft SQL Server ワークロードを保護する	1
NetApp Backup and Recoveryを使用した Microsoft SQL ワークロードの保護の概要	1
プラグイン サービスからNetApp Backup and Recoveryにインポートするための前提条件	2
まずNetApp Consoleでシステムを作成する	2
SnapCenterプラグインをインストールするためのホスト要件を確認する	3
ユーザー アカウント制御のリモート制限を無効にする	3
Microsoft SQL Server ワークロードを検出し、オプションでNetApp Backup and Recovery のSnapCenterからインポートします。	5
Microsoft SQL Server ワークロードを検出し、オプションで SnapCenterリソースをインポートします	6
NetApp Backup and Recoveryで Microsoft SQL Server ワークロードをバックアップする	10
ワークロード保護ステータスの表示	10
検出されたホストのログディレクトリを構成する	10
保護グループを作成する	11
オンデマンドバックアップでワークロードを今すぐバックアップ	12
バックアップスケジュールを一時停止する	12
保護グループを削除する	12
ワークロードから保護を削除する	13
NetApp Backup and Recoveryを使用して Microsoft SQL Server のワークロードを復元する	13
ワークロードの復元の仕組み	14
復元方法	15
復元オプションからワークロードデータを復元します	15
インベントリオプションからワークロードデータを復元する	18
NetApp Backup and Recoveryを使用して Microsoft SQL Server ワークロードをクローンする	18
クローンを作成する	19
クローンの更新	21
クローンの更新をスキップする	22
クローンのスプリット	22
クローンを削除する	22
NetApp Backup and Recoveryで Microsoft SQL Server のインベントリを管理する	23
ホスト情報の管理	23
インスタンス情報の管理	25
データベース情報の管理	27
NetApp Backup and Recoveryで Microsoft SQL Server スナップショットを管理する	29
スナップショットを削除する	29
NetApp Backup and Recoveryで Microsoft SQL Server ワークロードのレポートを作成する	29
レポートを作成する	29

Microsoft SQL Server ワークロードを保護する

NetApp Backup and Recoveryを使用した Microsoft SQL ワークロードの保護の概要

NetApp Backup and Recoveryを使用して、オンプレミスのONTAPシステムから AWS 、 Azure、またはStorageGRIDに Microsoft SQL Server アプリケーション データをバックアップします。システムはポリシーに従って、クラウド アカウントにバックアップを自動的に作成して保存します。 3-2-1 戦略を使用します。つまり、データの 3 つのコピーを 2 つのストレージ システムに保存し、1 つのコピーをクラウドに保存します。

3-2-1 アプローチの利点は次のとおりです。

- ・複数のデータ コピーにより、内部および外部のサイバー セキュリティの脅威から保護されます。
- ・異なるタイプのメディアを使用すると、1 つのタイプに障害が発生した場合でも回復しやすくなります。
- ・オンサイト コピーから迅速に復元し、オンサイト コピーが侵害された場合はオフサイト コピーを使用できます。

NetApp Backup and Recovery は、 NetApp SnapMirrorを使用してスナップショットを作成し、それをバックアップの場所に転送することでバックアップを同期します。

データを保護するために、次の操作を実行できます。

- ・"SnapCenterからインポートする場合の追加項目を構成する"
- ・"Microsoft SQL Server ワークロードを検出し、オプションでSnapCenterリソースをインポートします"
- ・"ローカルONTAPプライマリストレージ上のローカル スナップショットを使用してワークロードをバックアップします。"
- ・"ワークロードをONTAPセカンダリストレージに複製する"
- ・"ワークロードをオブジェクトストアの場所にバックアップする"
- ・"今すぐワークロードをバックアップ"
- ・"ワークロードを復元する"
- ・"クローンワークロード"
- ・"ワークロードのインベントリを管理する"
- ・"スナップショットを管理する"

ワークロードをバックアップするには、バックアップおよび復元操作を管理するポリシーを作成します。見る"ポリシーを作成"詳細についてはこちらをご覧ください。

サポートされているバックアップ先

NetApp Backup and Recovery を使用すると、 Microsoft SQL Server インスタンスとデータベースを次のソース システムから次のセカンダリ システムおよびパブリック クラウド プロバイダーとプライベート クラウド プロバイダーのオブジェクトストレージにバックアップできます。スナップショットはソース システムに存在します。

ソースシステム	セカンダリシステム（レプリケーション）	宛先オブジェクトストア（バックアップ）
AWS のCloud Volumes ONTAP	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP	Amazon S3 ONTAP S3
Azure のCloud Volumes ONTAP	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム	Azure ブロブONTAP S3
オンプレミスのONTAPシステム	Cloud Volumes ONTAPオンプレミスONTAPシステム	Amazon S3 Azure Blob NetApp StorageGRID ONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	NA

サポートされている復元先

プライマリストレージまたはセカンダリシステム(複製されたボリューム)またはオブジェクトストレージ(バックアップファイル)にあるバックアップから、Microsoft SQL Server インスタンスとデータベースを次のシステムに復元できます。スナップショットはソースシステム上に存在し、同じシステムにのみ復元できます。

バックアップファイルの場所から	宛先システムへ
オブジェクトストア（バックアップ）	セカンダリシステム（レプリケーション）
Amazon S3	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP
Azure ブロブ	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム
StorageGRID	Cloud Volumes ONTAPオンプレミスONTAPシステム
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP



「オンプレミスのONTAPシステム」への参照には、FASとAFFシステムが含まれます。

プラグインサービスからNetApp Backup and Recoveryにインポートするための前提条件

Microsoft SQL Server 用のSnapCenter プラグインサービスからNetApp Backup and Recoveryにリソースをインポートする場合は、さらにいくつかの項目を構成する必要があります。

まずNetApp Consoleでシステムを作成する

SnapCenterからリソースをインポートする場合は、SnapCenterからインポートする前に、オンプレミスのすべてのSnapCenterクラスター ストレージをコンソールの[システム]ページに追加する必要があります。これにより、ホストリソースが正しく検出され、インポートされるようになります。

SnapCenter プラグインをインストールするためのホスト要件を確認する

SnapCenter Plug-in for Microsoft SQL Server からリソースをインポートするには、 SnapCenter Plug-in for Microsoft SQL Server をインストールするためのホスト要件が満たされていることを確認します。

SnapCenterの要件については、 "[NetApp Backup and Recoveryの前提条件](#)"。

ユーザーアカウント制御のリモート制限を無効にする

SnapCenterからリソースをインポートする前に、 SnapCenter Windows ホストのユーザー アカウント制御 (UAC) リモート制限を無効にします。ローカル管理者アカウントを使用してSnapCenter Server ホストまたは SQL ホストにリモートで接続する場合は、 UAC を無効にします。

セキュリティに関する考慮事項

UAC リモート制限を無効にする前に、次の問題を考慮してください。

- セキュリティ リスク: トーケン フィルタリングを無効にすると、特にローカル管理者アカウントが悪意のある人物によって侵害された場合に、システムがセキュリティ上の脆弱性にさらされる可能性があります。
- 注意して使用してください:
 - 管理タスクに不可欠な場合にのみ、この設定を変更してください。
 - 管理者アカウントを保護するために、強力なパスワードやその他のセキュリティ対策が実施されていることを確認します。

代替解決策

- リモート管理アクセスが必要な場合は、適切な権限を持つドメイン アカウントの使用を検討してください。
- リスクを最小限に抑えるために、セキュリティのベストプラクティスに準拠した安全なリモート管理ツールを使用します。

ユーザーアカウント制御のリモート制限を無効にする手順

1. 変更する `LocalAccountTokenFilterPolicy` SnapCenter Windows ホスト上のレジストリ キー。

次のいずれかを使用してこれを実行してください。手順は次のとおりです。

- 方法1: レジストリエディター
- 方法2: PowerShellスクリプト

方法1: レジストリエディターを使用してユーザーアカウント制御を無効にする

これは、ユーザー アカウント制御を無効にするために使用できる方法の 1 つです。

手順

- 次の手順に従って、 SnapCenter Windows ホストでレジストリ エディターを開きます。
 - Press **Windows+R**[実行]ダイアログ ボックスを開きます。
 - タイプ `regedit`、押すと `Enter`。

2. ポリシーに移動します。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

3. 作成または変更 `DWORD` 値 :

a. 場所: LocalAccountTokenFilterPolicy

b. 存在しない場合は、新しいものを作成してください DWORD (32ビット) 値の名前 LocalAccountTokenFilterPolicy。

4. 以下の値がサポートされています。このシナリオでは、値を 1:

◦ 0(デフォルト): UAC リモート制限が有効になります。ローカル アカウントには、リモート アクセス 時にフィルターされたトークンがあります。

◦ 1: UAC リモート制限は無効です。ローカル アカウントはトークン フィルタリングをバイパスし、リ モート アクセス時に完全な管理者権限を持ちます。

5. [OK]をクリックします。

6. レジストリ エディターを閉じます。

7. SnapCenter Windows ホストを再起動します。

レジストリの変更例

この例では、LocalAccountTokenFilterPolicy を「1」に設定し、UAC リモート制限を無効にします。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
```

```
"LocalAccountTokenFilterPolicy"=dword:00000001
```

方法2: PowerShellスクリプトを使用してユーザー アカウント制御を無効にする

これは、ユーザー アカウント制御を無効にするために使用できる別の方法です。



昇格された権限で PowerShell コマンドを実行すると、システム設定に影響する可能性があります。コマンドを実行する前に、コマンドとその意味を理解していることを確認してください。

手順

1. SnapCenter Windows ホストで管理者権限を使用して PowerShell ウィンドウを開きます。

a. スタート メニューをクリックします。

b. **PowerShell 7** または **Windows Powershell** を検索します。

c. そのオプションを右クリックし、[管理者として実行] を選択します。

2. PowerShell がシステムにインストールされていることを確認してください。インストール後、スタート メニューに表示されます。



PowerShell は、Windows 7 以降のバージョンにデフォルトで含まれています。

3. UAC リモート制限を無効にするには、次のコマンドを実行して LocalAccountTokenFilterPolicy を「1」に設定します。

```
Set-ItemProperty -Path  
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name  
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord
```

4. 現在の値が「1」に設定されていることを確認します。`LocalAccountTokenFilterPolicy``実行して:

```
Get-ItemProperty -Path  
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name  
"LocalAccountTokenFilterPolicy"
```

- 値が 1 の場合、UAC リモート制限は無効になります。
- 値が 0 の場合、UAC リモート制限が有効になります。

5. 変更を適用するには、コンピューターを再起動してください。

UAC リモート制限を無効にする PowerShell 7 コマンドの例:

値が「1」に設定されているこの例は、UAC リモート制限が無効になっていることを示します。

```
# Disable UAC remote restrictions

Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord

# Verify the change

Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"

# Output

LocalAccountTokenFilterPolicy : 1
```

Microsoft SQL Server ワークロードを検出し、オプションで NetApp Backup and Recovery の SnapCenter からインポートします。

NetApp Backup and Recovery、サービスを使用するために、まず Microsoft SQL Server ワークロードを検出する必要があります。 SnapCenter がすでにインストールされている

場合は、オプションでSnapCenterからバックアップデータとポリシーをインポートできます。

必要なNetApp Consoleロール バックアップおよびリカバリのスーパー管理者。 詳細はこちら["バックアップとリカバリの役割と権限"](#)。 ["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"](#)。

Microsoft SQL Server ワークロードを検出し、オプションでSnapCenterリソースをインポートします

検出中に、 NetApp Backup and Recovery は組織内のシステム内の Microsoft SQL Server インスタンスとデータベースを分析します。

NetApp Backup and Recovery は、 Microsoft SQL Server アプリケーションを評価します。このサービスは、現在のバックアップ保護ポリシー、スナップショット、バックアップおよびリカバリ オプションなどの既存の保護レベルを評価します。

検出は次のように行われます。

- SnapCenterがすでにある場合は、 NetApp Backup and Recovery UI を使用してSnapCenterリソースをNetApp Backup and Recoveryにインポートします。



SnapCenterがすでにある場合は、まずSnapCenterからインポートする前に前提条件を満たしていることを確認してください。たとえば、 SnapCenterからインポートする前に、オンプレミスのSnapCenterクラスタストレージシステムをNetApp Consoleに追加する必要があります。見る["SnapCenterからリソースをインポートするための前提条件"](#)。

- SnapCenterがまだない場合は、vCenter を手動で追加して検出を実行することで、ワークロードを検出できます。

SnapCenterがすでにインストールされている場合は、 **SnapCenterリソースをNetApp Backup and Recoveryにインポートします。**

SnapCenterがすでにインストールされている場合は、次の手順に従ってSnapCenterリソースをNetApp Backup and Recoveryにインポートします。 NetApp Consoleは、 SnapCenterからリソース、ホスト、資格情報、スケジュールを検出するため、すべての情報を再作成する必要はありません。

これは次の方法で実行できます。

- 検出中に、 SnapCenterからリソースをインポートするオプションを選択します。
- 検出後、インベントリ ページからSnapCenterリソースをインポートするオプションを選択します。
- 検出後、[設定] メニューからSnapCenterリソースをインポートするオプションを選択します。 詳細については、 ["NetApp Backup and Recoveryを構成する"](#)。

これは 2 つの部分から成るプロセスです。

- SnapCenter Server アプリケーションとホストリソースをインポートする
- 選択したSnapCenterホストリソースを管理する

SnapCenter Server アプリケーションとホスト リソースをインポートする

この最初のステップでは、 SnapCenterからホスト リソースをインポートし、それらのリソースをNetApp Backup and Recoveryインベントリ ページに表示されます。その時点では、リソースはまだNetApp Backup and Recoveryによって管理されていません。

 SnapCenterホスト リソースをインポートした後、 NetApp Backup and Recovery は保護管理を自動的に引き継ぎません。そのためには、 NetApp Backup and Recoveryでインポートされたリソースを管理することを明示的に選択する必要があります。これにより、 NetApp Backup and Recoveryによってそれらのリソースをバックアップする準備が整います。

手順

1. NetApp Consoleの左側のナビゲーションから、保護 > バックアップとリカバリ を選択します。
2. *在庫*を選択します。
3. *リソースの検出*を選択します。
4. NetApp Backup and Recovery のワークフロー リソースの検出ページで、 * SnapCenterからのインポート* を選択します。
5. * SnapCenterアプリケーションの資格情報*を入力してください:
 - a. * SnapCenter FQDN または IP アドレス*: SnapCenterアプリケーション自体の FQDN または IP アドレスを入力します。
 - b. ポート: SnapCenterサーバーのポート番号を入力します。
 - c. ユーザー名とパスワード: SnapCenterサーバーのユーザー名とパスワードを入力します。
 - d. コンソール エージェント: SnapCenterのコンソール エージェントを選択します。
6. * SnapCenterサーバー ホストの資格情報*を入力してください:
 - a. 既存の資格情報: このオプションを選択すると、すでに追加されている既存の資格情報を使用できます。資格情報の名前を選択します。
 - b. 新しい資格情報の追加: 既存のSnapCenterホスト資格情報がない場合は、新しい資格情報を追加できます。資格情報名、認証モード、ユーザー名、およびパスワードを入力します。
7. インポートを選択してエントリを検証し、 SnapCenterサーバーを登録します。



SnapCenterサーバーがすでに登録されている場合は、既存の登録詳細を更新できます。

結果

インベントリ ページには、MS SQL ホスト、インスタンス、データベースを含むインポートされたSnapCenterリソースが表示されます。

インポートされたSnapCenterリソースの詳細を表示するには、[アクション] メニューから [詳細の表示] オプションを選択します。

SnapCenterホストリソースの管理

SnapCenterリソースをインポートした後、 NetApp Backup and Recoveryでそれらのホスト リソースを管理します。これらのリソースを管理することを選択すると、 NetApp Backup and Recovery はSnapCenterからインポートしたリソースをバックアップおよびリカバリできるようになります。これらのリソースはSnapCenter Server では管理できなくなります。

手順

1. SnapCenterリソースをインポートした後、[バックアップとリカバリ] メニューから [インベントリ] を選択します。
2. [インベントリ] ページで、今後NetApp Backup and Recoveryで管理するインポート済みのSnapCenterホストを選択します。
3. アクションアイコンを選択します **...> 詳細を表示** をクリックして、ワークロードの詳細を表示します。
4. インベントリ > ワークロードページから、アクションアイコンを選択します **...> 管理** をクリックして、ホストの管理ページを表示します。
5. *管理*を選択します。
6. [ホストの管理] ページで、既存の vCenter を使用するか、新しい vCenter を追加するかを選択します。
7. *管理*を選択します。

インベントリ ページには、新しく管理されたSnapCenterリソースが表示されます。

オプションで、[アクション] メニューから [レポートの生成] オプションを選択して、管理対象リソースのレポートを作成することもできます。

インベントリページから検出後に**SnapCenter**リソースをインポートする

すでにリソースを検出している場合は、インベントリ ページからSnapCenterリソースをインポートできます。

手順

1. コンソールの左側のナビゲーションから、保護 > *バックアップとリカバリ*を選択します。
2. *在庫*を選択します。
3. インベントリ ページで、* SnapCenterリソースのインポート*を選択します。
4. SnapCenterリソースをインポートするには、上記の * SnapCenterリソースのインポート* セクションの手順に従います。

SnapCenterがインストールされていない場合は、**vCenter**を追加してリソースを検出します。

SnapCenterがまだインストールされていない場合は、vCenter 情報を追加して、NetAppバックアップおよびリカバリでワークロードを検出できます。各コンソール エージェント内で、ワークロードを検出するシステムを選択します。

VMware 環境がある場合、これはオプションです。

手順

1. コンソールの左側のナビゲーションから、保護 > *バックアップとリカバリ*を選択します。

初めて Backup and Recovery にログインし、コンソールにシステムがあるがリソースが検出されていない場合は、[新しいNetApp Backup and Recovery へようこそ] ページが表示され、[リソースの検出] オプションが表示されます。

2. *リソースの検出*を選択します。
3. 次の情報を入力してください。

- a. ワークロード タイプ: このバージョンでは、Microsoft SQL Server のみが利用可能です。
- b. **vCenter 設定:** 既存の vCenter を選択するか、新しい vCenter を追加します。新しい vCenter を追加するには、vCenter FQDN または IP アドレス、ユーザー名、パスワード、ポート、プロトコルを入力します。



vCenter 情報を入力する場合は、vCenter 設定とホスト登録の両方の情報を入力します。ここで vCenter 情報を追加または入力した場合は、次に詳細設定でプラグイン情報も追加する必要があります。

- c. ホスト登録: 資格情報の追加を選択し、検出するワークロードを含むホストに関する情報を入力します。



vCenter サーバーではなくスタンドアロン サーバーを追加する場合は、ホスト情報のみを入力します。

4. *Discover*を選択します。



このプロセスには数分かかる場合があります。

5. 詳細設定に進みます。

検出中に詳細設定オプションを設定し、プラグインをインストールします

詳細設定を使用すると、登録されているすべてのサーバーにプラグイン エージェントを手動でインストールできます。これにより、すべてのSnapCenterワークロードをNetApp Backup and Recoveryにインポートして、そこでバックアップとリストアを管理できるようになります。 NetApp Backup and Recovery、プラグインをインストールするために必要な手順が示されています。

手順

1. 「リソースの検出」ページで、右側の下矢印をクリックして「詳細設定」に進みます。
2. 「ワークロード リソースの検出」ページで、次の情報を入力します。
 - プラグインのポート番号を入力: プラグインが使用するポート番号を入力します。
 - インストール パス: プラグインをインストールするパスを入力します。
3. SnapCenterエージェントを手動でインストールする場合は、次のオプションのチェックボックスをオンにします。
 - 手動インストールを使用する: プラグインを手動でインストールするには、このボックスをオンにします。
 - クラスター内のすべてのホストを追加: 検出中にクラスター内のすべてのホストをNetApp Backup and Recoveryに追加するには、このボックスをオンにします。
 - オプションのインストール前チェックをスキップ: オプションのインストール前チェックをスキップするには、このチェックボックスをオンにします。たとえば、メモリやスペースの考慮事項が近い将来に変更されることがわかっていて、今すぐプラグインをインストールしたい場合などに、これを実行することができます。
4. *Discover*を選択します。

NetApp Backup and Recoveryダッシュボードに進みます

1. NetApp Consoleメニューから、保護 > バックアップとリカバリ を選択します。
2. ワークロード タイル (Microsoft SQL Server など) を選択します。
3. 「バックアップとリカバリ」メニューから、「ダッシュボード」を選択します。
4. データ保護の健全性を確認します。新しく検出され、保護され、バックアップされたワークロードに基づいて、危険にさらされているワークロードまたは保護されているワークロードの数が増加します。

"[ダッシュボードに表示される内容を学ぶ](#)"。

NetApp Backup and Recoveryで Microsoft SQL Server ワークロードをバックアップする

オンプレミスのONTAPシステムから Amazon Web Services、Microsoft Azure、またはStorageGRIDに Microsoft SQL Server アプリケーション データをバックアップします。システムは自動的にバックアップを作成し、データ保護のためにクラウド アカウント内のオブジェクトストアに保存します。

- ・スケジュールに従ってワークロードをバックアップするには、バックアップおよび復元操作を管理するポリシーを作成します。見る["ポリシーを作成"](#)手順についてはこちらをご覧ください。
- ・バックアップを開始する前に、検出されたホストのログ ディレクトリを構成します。
- ・今すぐワークロードをバックアップします (今すぐオンデマンド バックアップを作成します)。

ワークロード保護ステータスの表示

バックアップを開始する前に、ワークロードの保護ステータスを表示します。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、バックアップおよびリカバリ バックアップ管理者、バックアップおよびリカバリ リストア管理者、バックアップおよびリカバリ クローン管理者、またはバックアップおよびリカバリ ビューアー ロール。詳細はこちラ["バックアップとリカバリの役割と権限"](#)。["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"](#)。

手順

1. NetApp Backup and Recoveryメニューから、インベントリ を選択します。
2. 保護の詳細を表示するには、ワークロードを選択します。
3. アクションアイコンを選択します **...>** 詳細を表示。
4. ホスト、保護グループ、可用性グループ、インスタンス、およびデータベースのタブで詳細を確認します。

検出されたホストのログディレクトリを構成する

ワークロードをバックアップする前に、検出されたホストのアクティビティ ログ パスを設定して操作ステータスを追跡します。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、バックアップおよびリカバリ バックアップ管理者、またはバックアップおよびリカバリ リストア管理者のロール。 "すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"。

手順

1. NetApp Backup and Recoveryメニューから、インベントリを選択します。
2. 保護の詳細を表示するには、ワークロードを選択します。
3. アクションアイコンを選択します **...> 詳細を表示**。
4. ホストを選択します。
5. アクションアイコンを選択します **...> ログディレクトリを設定**します。
6. ホストパスを入力するか、ホストまたはノードのリストを参照して、ホストログを保存する場所を見つけます。
7. ログを保存するものを選択します。



表示されるフィールドは、フェールオーバー クラスター インスタンスやスタンドアロンなど、選択した展開モデルによって異なります。

8. *保存*を選択します。

保護グループを作成する

複数のワークロードのバックアップおよび復元操作を管理するための保護グループを作成します。保護グループは、ワークロードの論理的なグループです。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、またはバックアップおよびリカバリ バックアップ管理者ロール。 "すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"。

手順

1. NetApp Backup and Recoveryメニューから、インベントリを選択します。
2. 保護の詳細を表示するには、ワークロードを選択します。
3. アクションアイコンを選択します **...> 詳細を表示**。
4. *保護グループ*タブを選択します。
5. *保護グループの作成*を選択します。
6. 保護グループの名前を指定します。
7. 保護グループに含めるインスタンスまたはデータベースを選択します。
8. *次へ*を選択します。
9. 保護グループに適用する*バックアップポリシー*を選択します。

ポリシーを作成する場合は、「新しいポリシーの作成」を選択し、指示に従ってポリシーを作成します。見る"ポリシーを作成"詳細についてはこちらをご覧ください。

10. *次へ*を選択します。

- 構成を確認します。
- 保護グループを作成するには、[作成] を選択します。

オンデマンドバックアップでワークロードを今すぐバックアップ

システムに変更を加える前にオンデマンド バックアップを実行して、データが保護されていることを確認してください。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、またはバックアップおよびリカバリ バックアップ管理者ロール。 "[すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します](#)"。

手順

- メニューから*インベントリ*を選択します。
- 保護の詳細を表示するには、ワークロードを選択します。
- アクションアイコンを選択します **...>** 詳細を表示。
- 保護グループ、インスタンス、または*データベース*タブを選択します。
- バックアップするインスタンスまたはデータベースを選択します。
- アクションアイコンを選択します **...>** 今すぐバックアップ。
- バックアップに適用するポリシーを選択します。
- スケジュール層を選択します。
- *今すぐバックアップ*を選択します。

バックアップスケジュールを一時停止する

メンテナンスやトラブルシューティング中にバックアップを一時的に停止するには、スケジュールを一時停止します。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、またはバックアップおよびリカバリ バックアップ管理者ロール。 "[すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します](#)"。

手順

- NetApp Backup and Recoveryメニューから、インベントリ を選択します。
- 保護の詳細を表示するには、ワークロードを選択します。
- アクションアイコンを選択します **...>** 詳細を表示。
- 保護グループ、インスタンス、または*データベース*タブを選択します。
- 一時停止する保護グループ、インスタンス、またはデータベースを選択します。
- アクションアイコンを選択します **...>** 一時停止。

保護グループを削除する

保護グループを削除すると、保護グループとそれに関連付けられているすべてのバックアップ スケジュールが削除されます。保護グループが不要になった場合は削除することができます。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、またはバックアップおよびリカバリ バックアップ管理者ロール。 "すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"。

手順

1. NetApp Backup and Recoveryメニューから、インベントリを選択します。
2. 保護の詳細を表示するには、ワークロードを選択します。
3. アクションアイコンを選択します **...> 詳細を表示**。
4. *保護グループ*タブを選択します。
5. アクションアイコンを選択します **...> 保護グループを削除**します。

ワークロードから保護を削除する

ワークロードのバックアップが不要になった場合、またはNetApp Backup and Recoveryでの管理を停止する場合は、ワークロードから保護を削除できます。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、またはバックアップおよびリカバリ バックアップ管理者ロール。 "すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"。

手順

1. NetApp Backup and Recoveryメニューから、インベントリを選択します。
2. 保護の詳細を表示するには、ワークロードを選択します。
3. アクションアイコンを選択します **...> 詳細を表示**。
4. 保護グループ、インスタンス、または*データベース*タブを選択します。
5. 保護グループ、インスタンス、またはデータベースを選択します。
6. アクションアイコンを選択します **...> 保護を解除**。
7. [保護の削除] ダイアログ ボックスで、バックアップとメタデータを保持するか削除するかを選択します。
8. 操作を確認するには、[削除] を選択します。

NetApp Backup and Recoveryを使用して Microsoft SQL Server のワークロードを復元する

NetApp Backup and Recoveryを使用して Microsoft SQL Server ワークロードを復元します。スナップショット、セカンダリストレージに複製されたバックアップ、またはオブジェクトストレージ内のバックアップを使用します。ワークロードを元のシステム、同じクラウド アカウントを持つ別のシステム、またはオンプレミスのONTAPシステムに復元します。

これらの場所から復元

異なる開始場所からワークロードを復元できます。

- ・ プライマリロケーションから復元

- ・複製されたリソースから復元する
- ・オブジェクトストアのバックアップから復元する

これらのポイントに復元する

データを最新のスナップショットまたは以下のポイントに復元できます。

- ・スナップショットからの復元
- ・ファイル名、場所、最終有効日が分かっている場合は、特定の時点に復元します。
- ・最新のバックアップに復元する

オブジェクトストレージからの復元に関する考慮事項

オブジェクトストレージ内のバックアップファイルを選択し、そのバックアップに対して Ransomware Resilience がアクティブになっている場合 (バックアップポリシーで DataLock と Ransomware Resilience を有効にした場合)、データを復元する前に、バックアップファイルに対して追加の整合性チェックを実行するよう求められます。スキャンを実行することをお勧めします。

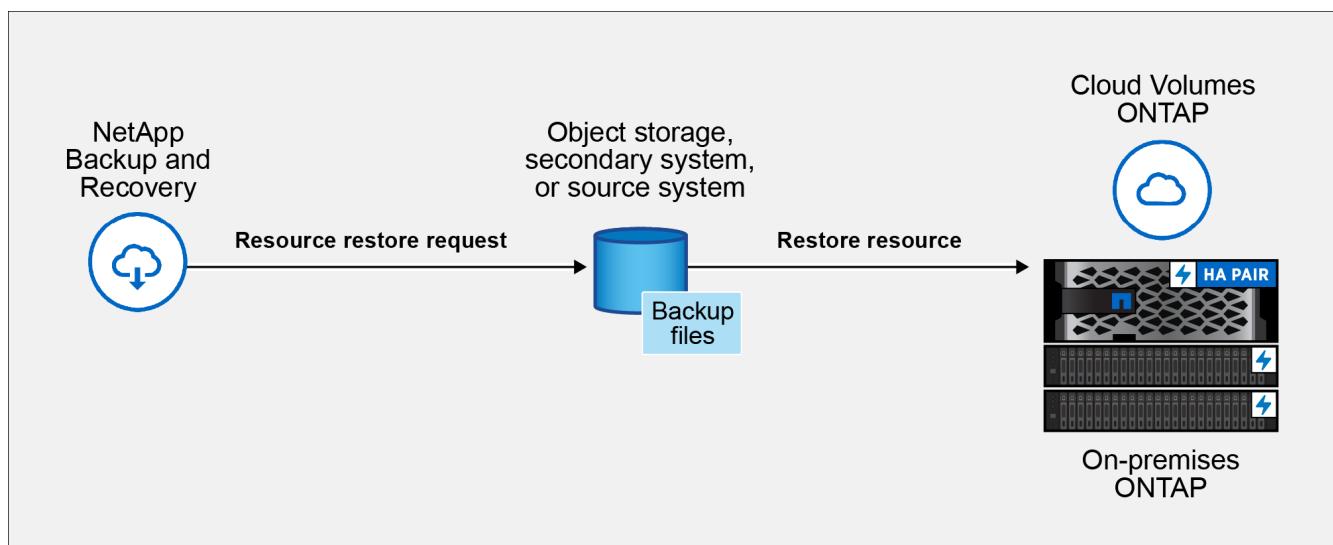


バックアップファイルにアクセスするには、クラウドプロバイダーに追加料金を支払う必要があります。

ワークロードの復元の仕組み

ワークロードを復元すると、次のことが起こります。

- ・バックアップファイルからワークロードを復元すると、NetApp Backup and Recovery はバックアップのデータを使用して新しいリソースを作成します。
- ・複製されたワークロードから復元する場合、ワークロードを元のシステムまたはオンプレミスのONTAPシステムに復元できます。



- ・オブジェクトストレージからバックアップを復元する場合、データを元のシステムまたはオンプレミスのONTAPシステムに復元できます。

復元方法

次のいずれかの方法を使用してワークロードを復元します。

- 復元ページから: リソースの名前、場所、または最終有効日がわからない場合に、このオプションを使用してリソースを復元します。フィルターを使用してスナップショットを検索します。
- インベントリ ページから: 特定のリソースの名前、場所、最終有効日がわかっている場合は、このオプションを使用してそのリソースを復元します。リストを参照してリソースを見つけます。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、またはバックアップおよびリカバリ バックアップ管理者ロール。 "[すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します](#)"。

復元オプションからワークロードデータを復元します

復元オプションを使用してデータベース ウォークロードを復元します。

手順

- NetApp Backup and Recoveryメニューから、[復元] を選択します。
- 復元するデータベースを選択します。フィルターを使用して検索します。
- 復元オプションを選択します:
 - スナップショットからの復元
 - ファイル名、場所、最終有効日が分かっている場合は、特定の時点に復元します。
 - 最新のバックアップに復元する

スナップショットからワークロードを復元する

- 復元オプション ページから続行して、*スナップショットからの復元*を選択します。
スナップショットのリストが表示されます。
- 復元するスナップショットを選択します。
- *次へ*を選択します。

次に、宛先オプションが表示されます。

- 宛先の詳細ページで、次の情報を入力します。
 - 宛先設定: データを元の場所に復元するか、別の場所に復元するかを選択します。別の場所の場合は、ホスト名とインスタンスを選択し、データベース名を入力して、スナップショットを復元する宛先パスを入力します。
 - 復元前のオプション:
 - 復元中に同じ名前のデータベースを上書きする: 復元中、元のデータベース名は保持されます。
 - SQL データベースのレプリケーション設定を保持: 復元操作後も SQL データベースのレプリケーション設定を保持します。
 - 復元前にトランザクションログのバックアップを作成する: 復元操作の前にトランザクションログのバックアップを作成します。* 復元前のトランザクションログ バックアップが失敗した場合

は復元を終了: トランザクション ログ バックアップが失敗した場合は復元操作を停止します。

- **Prescript:** 復元操作の前に実行するスクリプトの完全なパス、スクリプトが取る引数、およびスクリプトが完了するまでの待機時間を入力します。

- 復元後のオプション:

- *動作可能*ですが、追加のトランザクション ログを復元するためには使用できません。これにより、トランザクション ログ バックアップが適用された後、データベースがオンラインに戻ります。
- *非動作*ですが、追加のトランザクション ログを復元するために使用できます。トランザクション ログ バックアップを復元しながら、復元操作後にデータベースを非動作状態に維持します。このオプションは、追加のトランザクション ログを復元するのに役立ちます。
- *読み取り専用モード*で、追加のトランザクション ログを復元できます。データベースを読み取り専用モードで復元し、トランザクション ログ バックアップを適用します。
- **Postscript:** 復元操作後に実行するスクリプトの完全なパスと、スクリプトが受け取る引数を入力します。

5. *復元*を選択します。

特定の時点に復元する

NetApp Backup and Recovery は、ログと最新のスナップショットを使用して、データのポイントインタイムリストアを作成します。

1. 復元オプション ページから続行して、*特定の時点に復元*を選択します。
2. *次へ*を選択します。
3. 「特定の時点への復元」 ページで、次の情報を入力します。
 - データ復元の日時: 復元するデータの正確な日時を入力します。この日付と時刻は、Microsoft SQL Server データベース ホストからのものです。
4. *検索*を選択します。
5. 復元するスナップショットを選択します。
6. *次へ*を選択します。
7. 宛先の詳細ページで、次の情報を入力します。
 - 宛先設定: データを元の場所に復元するか、別の場所に復元するかを選択します。別の場所の場合は、ホスト名とインスタンスを選択し、データベース名を入力して、宛先パスを入力します。
 - 復元前のオプション:
 - 元のデータベース名を保持: 復元中に、元のデータベース名が保持されます。
 - SQL データベースのレプリケーション設定を保持: 復元操作後も SQL データベースのレプリケーション設定を保持します。
 - **Prescript:** 復元操作の前に実行するスクリプトの完全なパス、スクリプトが取る引数、およびスクリプトが完了するまでの待機時間を入力します。
 - 復元後のオプション:
 - *動作可能*ですが、追加のトランザクション ログを復元するためには使用できません。これにより、トランザクション ログ バックアップが適用された後、データベースがオンラインに戻ります。

- *非動作*ですが、追加のトランザクション ログを復元するために使用できます。トランザクション ログ バックアップを復元しながら、復元操作後にデータベースを非動作状態に維持します。このオプションは、追加のトランザクション ログを復元するのに役立ちます。
- *読み取り専用モード*で、追加のトランザクション ログを復元できます。データベースを読み取り専用モードで復元し、トランザクション ログ バックアップを適用します。
- **Postscript:** 復元操作後に実行するスクリプトの完全なパスと、スクリプトが受け取る引数を入力します。

8. *復元*を選択します。

最新のバックアップに復元する

このオプションは、最新の完全バックアップとログ バックアップを使用して、データを最後の正常な状態に復元します。システムは最後のスナップショットから現在までのログをスキャンします。このプロセスでは、変更とアクティビティを追跡して、データの最新かつ正確なバージョンを復元します。

1. 復元オプション ページから続行して、*最新のバックアップに復元*を選択します。

NetApp Backup and Recovery、復元操作に使用できるスナップショットが表示されます。

2. 「最新の状態に復元」ページで、ローカル、セカンダリ ストレージ、またはオブジェクト ストレージのスナップショットの場所を選択します。
3. *次へ*を選択します。
4. 宛先の詳細ページで、次の情報を入力します。
 - 宛先設定: データを元の場所に復元するか、別の場所に復元するかを選択します。別の場所の場合は、ホスト名とインスタンスを選択し、データベース名を入力して、宛先パスを入力します。
 - 復元前のオプション:
 - 復元中に同じ名前のデータベースを上書きする: 復元中、元のデータベース名は保持されます。
 - **SQL** データベースのレプリケーション設定を保持: 復元操作後も SQL データベースのレプリケーション設定を保持します。
 - 復元前にトランザクション ログ バックアップを作成する: 復元操作の前にトランザクション ログ バックアップを作成します。
 - 復元前のトランザクション ログ バックアップが失敗した場合は復元を終了: トランザクション ログ バックアップが失敗した場合は復元操作を停止します。
 - **Prescript:** 復元操作の前に実行するスクリプトの完全なパス、スクリプトが取る引数、およびスクリプトが完了するまでの待機時間を入力します。
 - 復元後のオプション:
 - *動作可能*ですが、追加のトランザクション ログを復元するためには使用できません。これにより、トランザクション ログ バックアップが適用された後、データベースがオンラインに戻ります。
 - *非動作*ですが、追加のトランザクション ログを復元するために使用できます。トランザクション ログ バックアップを復元しながら、復元操作後にデータベースを非動作状態に維持します。このオプションは、追加のトランザクション ログを復元するのに役立ちます。
 - *読み取り専用モード*で、追加のトランザクション ログを復元できます。データベースを読み取り専用モードで復元し、トランザクション ログ バックアップを適用します。

- **Postscript**: 復元操作後に実行するスクリプトの完全なパスと、スクリプトが受け取る引数を入力します。
5. *復元*を選択します。

インベントリオプションからワークロードデータを復元する

インベントリ ページからデータベース ワークロードを復元します。インベントリ オプションを使用すると、インスタンスではなくデータベースのみを復元できます。

手順

1. NetApp Backup and Recoveryメニューから、インベントリ を選択します。
2. 復元するリソースが配置されているホストを選択します。
3. *アクション*を選択します **...アイコン**をクリックし、[詳細を表示] を選択します。
4. Microsoft SQL Server ページで、データベース タブを選択します。
5. 「データベース」メニューで、「保護」ステータスのデータベースを選択します。
6. *アクション*を選択します **...アイコン**をクリックし、[復元] を選択します。

「復元」ページから復元する場合と同じ 3 つのオプションが表示されます。

- スナップショットからの復元
 - 特定の時点に復元する
 - 最新のバックアップに復元する
7. 復元ページから復元オプションについて同じ手順を続行します。

NetApp Backup and Recoveryを使用して Microsoft SQL Server ワークロードをクローンする

NetApp Backup and Recoveryを使用して、開発、テスト、または保護のために Microsoft SQL Server アプリケーション データを VM に複製します。SQL Server ワークロードのインスタント スナップショットまたは既存のスナップショットからクローンを作成します。

次のクローンの種類から選択します。

- **インスタント スナップショットとクローン**: バックアップから作成されたソース データのポイントインタイム コピーであるインスタント スナップショットから、Microsoft SQL Server ワークロードのクローンを作成できます。クローンは、パブリック クラウド アカウントまたはプライベート クラウド アカウントのオブジェクトストアに保存されます。データが失われたり破損したりした場合に、クローンを使用してワークロードを復元できます。
- **既存のスナップショットからのクローン作成**: ワークロードで使用可能なスナップショットのリストから既存のスナップショットを選択できます。このオプションは、特定の時点からクローンを作成する場合に便利です。プライマリ ストレージまたはセカンダリ ストレージにクローンを作成します。

次の保護目標を達成できます。

- ・ クローンを作成する
- ・ クローンの更新
- ・ クローンのスプリット
- ・ クローンを削除する

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、またはバックアップおよびリカバリ バックアップ管理者ロール。 "[すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します](#)"。

クローンを作成する

Microsoft SQL Server ワークロードのクローンを作成できます。クローンとは、バックアップから作成されたソース データのコピーです。クローンは、パブリック クラウド アカウントまたはプライベート クラウド アカウントのオブジェクト ストアに保存されます。データが失われたり破損したりした場合に、クローンを使用してワークロードを復元できます。

既存のスナップショットまたはインスタント スナップショットからクローンを作成できます。インスタント スナップショットは、バックアップから作成されたソース データの特定時点のコピーです。データが失われたり破損したりした場合に、クローンを使用してワークロードを復元できます。

手順

1. NetApp Backup and Recoveryメニューから、クローン を選択します。
2. *新しいクローンを作成*を選択します。
3. クローンの種類を選択します:
 - 既存のスナップショットからのクローン作成とデータベースの更新: スナップショットを選択し、クローン オプションを構成します。
 - インスタント スナップショットとクローン: ソース データのスナップショットを今すぐ作成し、そのスナップショットからクローンを作成します。このオプションは、ソース ワークロードの最新データからクローンを作成する場合に便利です。
4. データベース ソース セクションを完了します。
 - 単一クローンまたは一括クローン: 単一クローンを作成するか、複数クローンを作成するかを選択します。 *一括クローン*を選択すると、既に作成した保護グループを使用して一度に複数のクローンを作成できます。このオプションは、異なるワークロードに対して複数のクローンを作成する場合に便利です。
 - ソース データベース ホスト、インスタンス、および名前: クローンのソース データベース ホスト、インスタンス、および名前を選択します。ソース データベースは、クローンの作成元となるデータベースです。
5. データベース ターゲット セクションを完了します。
 - ターゲット データベース ホスト、インスタンス、および名前: クローンのターゲット データベース ホスト、インスタンス、および名前を選択します。ターゲット データベースは、クローンが作成される場所です。

必要に応じて、ターゲット名のドロップダウン リストから サフィックス を選択し、クローンされたデータベース名にサフィックスを追加します。サフィックスを追加しない場合、クローンされたデータベース名はソース データベース名と同じになります。

- **QoS (最大スループット):** クローンのサービス品質 (QoS) 最大スループットを MBps 単位で選択します。 QoS は、最大スループットや IOPS など、クローンのパフォーマンス特性を定義します。

6. *マウント*セクションを完了します。

- マウント ポイントの自動割り当て: オブジェクト ストア内のクローンのマウント ポイントを自動的に割り当てます。
- マウント ポイント パスの定義: クローンのマウント ポイントを入力します。マウント ポイントは、オブジェクト ストア内でクローンがマウントされる場所です。ドライブ文字を選択し、データ ファイル のパスを入力し、ログ ファイルのパスを入力します。

7. *次へ*を選択します。

8. 復元ポイントを選択します:

- 既存のスナップショット: ワークロードで使用可能なスナップショットのリストから既存のスナップショットを選択します。このオプションは、特定の時点からクローンを作成する場合に便利です。
- インスタント スナップショットとクローン: ワークロードで使用可能なスナップショットのリストから最新のスナップショットを選択します。このオプションは、ソース ワークロードの最新データからクローンを作成する場合に便利です。

9. *インスタント スナップショットとクローン*の作成を選択した場合は、クローンの保存場所を選択します。

- ローカル ストレージ: ONTAPシステムのローカル ストレージにクローンを作成するには、このオプションを選択します。ローカル ストレージは、ONTAPシステムに直接接続されたストレージです。
- セカンダリ ストレージ: ONTAPシステムのセカンダリ ストレージにクローンを作成するには、このオプションを選択します。セカンダリ ストレージは、バックアップおよびリカバリのワークロードに使用されるストレージです。

10. データとログの保存先を選択します。

11. *次へ*を選択します。

12. *詳細オプション*セクションを完了します。

13. インスタント スナップショットとクローンを選択した場合は、次のオプションを完了します。

- クローンの更新スケジュールと有効期限: インスタントクローンを選択した場合は、クローンの更新を開始する日付を入力します。クローン スケジュールは、クローンがいつ作成されるかを定義します。
 - スケジュールの有効期限が切れた場合にクローンを削除: クローンの有効期限が切れた場合にクローンを削除する場合。
 - クローンの更新間隔: クローンを更新する頻度を選択します。クローンを毎時、毎日、毎週、毎月、または四半期ごとに更新することを選択できます。このオプションは、クローンをソース ワークロードに合わせて最新の状態に保つ場合に便利です。
- プレスクリプトとポストスクリプト: オプションで、クローンの作成前と作成後に実行するスクリプトを追加します。これらのスクリプトは、クローンの設定や通知の送信などの追加タスクを実行できます。
- 通知: オプションで、ジョブ レポートとともにクローン作成ステータスに関する通知を受信する電子メール アドレスを指定します。クローン作成ステータスに関する通知を受信するための Webhook URL を指定することもできます。成功通知と失敗通知の両方、またはどちらか一方のみの通知を指定することができます。
- タグ: 後でリソース グループを検索する際に役立つラベルを選択し、[適用] を選択します。たとえば、複数のリソース グループに「HR」をタグとして追加すると、後で「HR」タグに関連付けられている

すべてのリソース グループを見つけることができます。

14. *作成*を選択します。
15. クローンが作成されると、*インベントリ*ページで確認できます。

クローンの更新

Microsoft SQL Server ワークロードのクローンを更新できます。クローンを更新すると、クローンはそのソース ワークロードの最新データで更新されます。これは、クローンをソース ワークロードに合わせて最新の状態に保つ場合に便利です。

データベース名を変更したり、最新のインスタント スナップショットを使用したり、既存の運用スナップショットから更新したりすることができます。

手順

1. NetApp Backup and Recoveryメニューから、クローン を選択します。
2. 更新するクローンを選択します。
3. アクションアイコンを選択します **…> クローンを更新。**
4. *詳細設定*セクションを完了します。
 - 回復範囲: すべてのログ バックアップを回復するか、特定の時点までのログ バックアップを回復するかを選択します。このオプションは、クローンを特定の時点に復元する場合に便利です。
 - クローンの更新スケジュールと有効期限: インスタントクローン を選択した場合は、クローンの更新を開始する日付を入力します。クローン スケジュールは、クローンがいつ作成されるかを定義します。
 - スケジュールの有効期限が切れたたらクローンを削除: クローンの有効期限が切れたたらクローンを削除する場合。
 - クローンの更新間隔: クローンを更新する頻度を選択します。クローンを毎時、毎日、毎週、毎月、または四半期ごとに更新することを選択できます。このオプションは、クローンをソース ワークロードに合わせて最新の状態に保つ場合に便利です。
 - iGroup 設定: クローンの iGroup を選択します。iGroup は、クローンへのアクセスに使用されるイニシエーターの論理グループです。既存の iGroup を選択するか、新しい iGroup を作成することができます。プライマリまたはセカンダリONTAPストレージシステムから iGroup を選択します。
 - プレスクリプトとポストスクリプト: オプションで、クローンの作成前と作成後に実行するスクリプトを追加します。これらのスクリプトは、クローンの設定や通知の送信などの追加タスクを実行できます。
 - 通知: オプションで、ジョブ レポートとともにクローン作成ステータスに関する通知を受信する電子メール アドレスを指定します。クローン作成ステータスに関する通知を受信するための Webhook URL を指定することもできます。成功通知と失敗通知の両方、またはどちらか一方のみの通知を指定することができます。
 - タグ: 後でリソース グループを検索するときに役立つ 1 つ以上のラベルを入力します。たとえば、複数のリソース グループに「HR」をタグとして追加すると、後で HR タグに関連付けられているすべてのリソース グループを見つけることができます。
5. 続行するには、更新確認ダイアログボックスで「更新」を選択します。

クローンの更新をスキップする

クローンを変更せずに維持するには、クローンの更新をスキップします。

手順

1. NetApp Backup and Recoveryメニューから、クローンを選択します。
2. 更新をスキップするクローンを選択します。
3. アクションアイコンを選択します **...> 更新をスキップ**。
4. [更新をスキップする] 確認ダイアログボックスで、次の操作を行います。
 - a. 次の更新スケジュールのみをスキップするには、[次の更新スケジュールのみをスキップ]を選択します。
 - b. 続行するには、[スキップ]を選択します。

クローンのスプリット

Microsoft SQL Server ワークロードのクローンを分割できます。クローンを分割すると、クローンから新しいバックアップが作成されます。新しいバックアップを使用してワークロードを復元できます。

クローンを独立したクローンまたは長期クローンとして分割することを選択できます。ウィザードには、SVM の一部であるアグリゲートのリスト、それらのサイズ、およびクローン ボリュームが存在する場所が表示されます。NetApp Backup and Recovery は、クローンを分割するのに十分なスペースがあるかどうかも示します。クローンを分割すると、クローンはその保護のために独立したデータベースになります。

クローンジョブは削除されず、他のクローンに再度再利用できます。

手順

1. NetApp Backup and Recoveryメニューから、クローンを選択します。
2. クローンを選択します。
3. アクションアイコンを選択します **...> 分割クローン**。
4. 分割クローンの詳細を確認し、「分割」を選択します。
5. 分割クローンが作成されると、*インベントリ*ページで確認できます。

クローンを削除する

Microsoft SQL Server ワークロードのクローンを削除できます。クローンを削除すると、オブジェクトストアからクローンが削除され、ストレージ領域が解放されます。

ポリシーによってクローンが保護されている場合、クローンおよびそのジョブの両方が削除されます。

手順

1. NetApp Backup and Recoveryメニューから、クローンを選択します。
2. クローンを選択します。
3. アクションアイコンを選択します **...> クローンを削除**。
4. クローンの削除確認ダイアログボックスで、削除の詳細を確認します。

- a. クローンまたはそのストレージにアクセスできない場合でも、クローンされたリソースをSnapCenterから削除するには、[強制削除]を選択します。
 - b. *削除*を選択します。
5. クローンを削除すると、インベントリ ページから削除されます。

NetApp Backup and Recoveryで Microsoft SQL Server のインベントリを管理する

NetApp Backup and Recovery は、Microsoft SQL Server ホスト、データベース、インスタンスの管理に役立ちます。インベントリの保護設定を表示、変更、または削除できます。

在庫管理に関連する次のタスクを実行できます。

- ホスト情報の管理
 - スケジュールを中断
 - ホストを編集または削除する
- インスタンス情報の管理
 - 資格情報をリソースに関連付ける
 - オンデマンドバックアップを開始して今すぐバックアップ
 - 保護設定を編集する
- データベース情報の管理
 - データベースを保護する
 - データベースを復元する
 - 保護設定を編集する
 - オンデマンドバックアップを開始して今すぐバックアップ
- ログ ディレクトリを構成します ([インベントリ] > [ホスト])。スナップショット内のデータベース ホストのログをバックアップする場合は、まずNetApp Backup and Recoveryでログを構成します。詳細については、["NetApp Backup and Recovery設定を構成する"](#)。

ホスト情報の管理

ホスト情報を管理して、適切なホストが保護されるようにすることができます。ホスト情報を表示、編集、削除できます。

必要なNetApp Consoleロール ストレージ ビューア、バックアップおよびリカバリ スーパー管理者、バックアップおよびリカバリ バックアップ管理者、バックアップおよびリカバリ リストア管理者、またはバックアップおよびリカバリ クローン管理者のロール。["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"](#)。

- ログディレクトリを構成します。詳細については、["NetApp Backup and Recovery設定を構成する"](#)。
- スケジュールを中断

- ・ホストを編集する
- ・ホストを削除する

ホストの管理

システム内で検出されたホストを管理できます。個別に、またはグループとして管理できます。



「ホスト」列で「管理対象外」ステータスのホストを管理できます。NetApp Backup and Recovery はすでに「管理対象」ステータスのホストを管理しています。

NetApp Backup and Recoveryでホストを管理すると、SnapCenterそれらのホスト上のリソースは管理されなくなります。

必要なNetApp Consoleロール ストレージ ビューアー、またはバックアップおよびリカバリのスーパー管理者。 "すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"。

手順

1. メニューから*インベントリ*を選択します。
2. 保護の詳細を表示するには、ワーカロードを選択します。
3. アクションアイコンを選択します **...> 詳細を表示**。
4. *ホスト*タブを選択します。
5. 1つ以上のホストを選択します。複数のホストを選択した場合は、一括操作オプションが表示され、*管理*(最大5台のホスト)*を選択できます。
6. アクションアイコンを選択します **...> 管理**。
7. ホストの依存関係を確認します。
 - vCenter が表示されない場合は、鉛筆アイコンを選択して、vCenter の詳細を追加または編集します。
 - vCenter を追加する場合は、[vCenter の登録] を選択して vCenter も登録する必要があります。
8. 設定をテストするには、「設定の検証」を選択します。
9. ホストを管理するには、[管理] を選択します。

スケジュールを中断

ホストのメンテナンス中にバックアップおよび復元操作を停止するには、スケジュールを一時停止します。

手順

1. NetApp Backup and Recoveryメニューから、インベントリを選択します。
2. スケジュールを一時停止するホストを選択します。
3. アクション*を選択します **... アイコンをクリックし、[*スケジュールの一時停止]を選択します。**
4. 確認ダイアログボックスで、[一時停止]を選択します。

ホストを編集する

vCenter サーバー情報、ホスト登録資格情報、および詳細設定オプションを変更できます。

手順

1. NetApp Backup and Recoveryメニューから、インベントリを選択します。
2. 編集するホストを選択します。
3. *アクション*を選択します アイコンをクリックし、[ホストの編集]を選択します。
4. ホスト情報を編集します。
5. *完了*を選択します。

ホストを削除する

ホスト情報を削除すると、サービス料金を停止できます。

手順

1. NetApp Backup and Recoveryメニューから、インベントリを選択します。
2. 削除するホストを選択します。
3. *アクション*を選択します アイコンをクリックし、[ホストの削除]を選択します。
4. 確認情報を確認し、「削除」を選択します。

インスタンス情報の管理

次の方法でインスタンス情報を管理し、リソース保護のための適切な資格情報を割り当て、リソースをバックアップすることができます。

- ・インスタンスを保護する
- ・アソシエイト資格
- ・資格情報の関連付けを解除する
- ・編集保護
- ・今すぐバックアップ

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、バックアップおよびリカバリ バックアップ管理者ロール。["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"](#)。

データベースインスタンスを保護する

リソース保護のスケジュールと保持を管理するポリシーを使用して、データベース インスタンスにポリシーを割り当てることができます。

手順

1. NetApp Backup and Recoveryメニューから、インベントリを選択します。
2. 表示するワークフローを選択し、[表示]を選択します。
3. *インスタンス*タブを選択します。
4. インスタンスを選択します。
5. *アクション*を選択します アイコンをクリックし、[保護]を選択します。

6. ポリシーを選択するか、新しいポリシーを作成します。

ポリシー作成の詳細については、["ポリシーを作成します。"](#)。

7. バックアップの前後に実行するスクリプトに関する情報を提供します。

- 事前スクリプト: 保護アクションがトリガーされる前にスクリプトを自動的に実行するには、スクリプトのファイル名と場所を入力します。これは、保護ワークフローの前に実行する必要がある追加のタスクや構成を実行するのに役立ちます。
- 事後スクリプト: 保護アクションが完了した後にスクリプトを自動的に実行するには、スクリプトのファイル名と場所を入力します。これは、保護ワークフローの後に実行する必要がある追加のタスクや構成を実行するのに役立ちます。

8. スナップショットを検証する方法についての情報を提供します。

- 保存場所: 検証スナップショットを保存する場所を選択します。
- 検証リソース: 検証するリソースがローカル スナップショット上にあるか、ONTAPセカンダリ ストレージ上にあるかを選択します。
- 検証スケジュール: 時間ごと、日ごと、週ごと、月ごと、または年ごとの頻度を選択します。

資格情報をリソースに関連付ける

保護が行われるように、資格情報をリソースに関連付けることができます。

詳細については、["資格情報を含むNetApp Backup and Recoveryの設定を構成する"](#)。

手順

1. NetApp Backup and Recoveryメニューから、インベントリを選択します。
2. 表示するワークフローを選択し、[表示]を選択します。
3. *インスタンス*タブを選択します。
4. インスタンスを選択します。
5. *アクション*を選択します アイコンをクリックし、[資格情報の関連付け]を選択します。
6. 既存の資格情報を使用するか、新しい資格情報を作成します。

保護設定を編集する

ポリシーを変更したり、新しいポリシーを作成したり、スケジュールを設定したり、保持設定を設定したりできます。

手順

1. NetApp Backup and Recoveryメニューから、インベントリを選択します。
2. 表示するワークフローを選択し、[表示]を選択します。
3. *インスタンス*タブを選択します。
4. インスタンスを選択します。
5. *アクション*を選択します アイコンをクリックし、[保護の編集]を選択します。

ポリシー作成の詳細については、["ポリシーを作成します。"](#)。

今すぐバックアップ

データをすぐに保護するために今すぐバックアップしてください。

手順

1. NetApp Backup and Recoveryメニューから、インベントリを選択します。
2. 表示するワークロードを選択し、[表示]を選択します。
3. *インスタンス*タブを選択します。
4. インスタンスを選択します。
5. *アクション*を選択します *** アイコンをクリックし、[今すぐバックアップ]を選択します。
6. バックアップの種類を選択し、スケジュールを設定します。

アドホックバックアップの作成の詳細については、["ポリシーを作成します。"](#)。

データベース情報の管理

データベース情報は次の方法で管理できます。

- データベースを保護する
- データベースを復元する
- 保護の詳細を表示
- 保護設定を編集する
- 今すぐバックアップ

データベースを保護する

ポリシーを変更したり、新しいポリシーを作成したり、スケジュールを設定したり、保持設定を設定したりできます。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、バックアップおよびリカバリ バックアップ管理者ロール。["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します。"](#)

手順

1. NetApp Backup and Recoveryメニューから、インベントリを選択します。
2. 表示するワークロードを選択し、[表示]を選択します。
3. *データベース*タブを選択します。
4. データベースを選択します。
5. *アクション*を選択します *** アイコンをクリックし、[保護]を選択します。

ポリシー作成の詳細については、["ポリシーを作成します。"](#)。

データベースを復元する

データを保護するためにデータベースを復元します。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、バックアップおよびリカバリ バックアップ管理者ロール。 "[すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します](#)"。

1. *データベース*タブを選択します。
2. データベースを選択します。
3. *アクション*を選択します アイコンをクリックし、[復元] を選択します。

ワークロードの復元については、以下を参照してください。 "[ワークロードを復元する](#)"。

保護設定を編集する

ポリシーを変更したり、新しいポリシーを作成したり、スケジュールを設定したり、保持設定を設定したりできます。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、バックアップおよびリカバリ バックアップ管理者ロール。 "[すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します](#)"。

手順

1. NetApp Backup and Recoveryメニューから、インベントリ を選択します。
2. 表示するワークロードを選択し、[表示] を選択します。
3. *データベース*タブを選択します。
4. データベースを選択します。
5. *アクション*を選択します アイコンをクリックし、[保護の編集] を選択します。

ポリシー作成の詳細については、 "[ポリシーを作成します](#)"。

今すぐバックアップ

今すぐ Microsoft SQL Server インスタンスとデータベースをバックアップして、データを保護できます。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、バックアップおよびリカバリ バックアップ管理者ロール。 "[すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します](#)"。

手順

1. NetApp Backup and Recoveryメニューから、インベントリ を選択します。
2. 表示するワークロードを選択し、[表示] を選択します。
3. *インスタンス*または*データベース*タブを選択します。
4. インスタンスまたはデータベースを選択します。
5. *アクション*を選択します アイコンをクリックし、[今すぐバックアップ] を選択します。

NetApp Backup and Recoveryで Microsoft SQL Server スナップショットを管理する

Microsoft SQL Server スナップショットは、NetApp Backup and Recoveryから削除することで管理できます。

スナップショットを削除する

削除できるのはローカル スナップショットのみです。

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、バックアップおよびリカバリ バックアップ管理者ロール。 "[すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します](#)"。

手順

1. NetApp Backup and Recoveryで、**Inventory** を選択します。
2. ワークロードを選択し、[表示] を選択します。
3. *データベース*タブを選択します。
4. スナップショットを削除するデータベースを選択します。
5. [アクション] メニューから、[保護の詳細を表示] を選択します。
6. 削除するローカル スナップショットを選択します。



その行の 場所 列のローカル スナップショット アイコンが青色で表示されていることを確認します。

7. *アクション*を選択します *** アイコンをクリックし、[ローカル スナップショットの削除] を選択します。
8. 確認ダイアログボックスで、[削除] を選択します。

NetApp Backup and Recoveryで Microsoft SQL Server ワークロードのレポートを作成する

NetApp Backup and Recoveryでは、Microsoft SQL Server ワークロードのレポートを作成して、成功したバックアップと失敗したバックアップの数、バックアップの種類、ストレージシステム、タイムスタンプなどのバックアップの状態と詳細を表示します。

レポートを作成する

必要なNetApp Consoleロール ストレージ ビューアー、バックアップおよびリカバリ スーパー管理者、バックアップおよびリカバリ バックアップ管理者、バックアップおよびリカバリ リストア管理者、バックアップおよびリカバリ クローン管理者。 詳細はこちら "[バックアップとリカバリの役割と権限](#)"。 "[すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します](#)"。

1. NetApp Backup and Recoveryメニューから、レポート オプションを選択します。
2. *レポートの作成*を選択します。

3. レポート範囲の詳細を入力します:
 - レポート名: レポートの一意の名前を入力します。
 - レポート タイプ: アカウント別またはワークロード (Microsoft SQL Server) 別にレポートを作成するかどうかを選択します。
 - ホストを選択: ワークロードで選択した場合は、レポートを生成するホストを選択します。
 - コンテンツの選択: レポートにすべてのバックアップの概要を含めるか、各バックアップの詳細を含めるかを選択します。 （「アカウント別」を選択した場合）
4. レポート範囲を入力: レポートに過去 1 日、過去 7 日間、過去 30 日間、前四半期、または前年度のデータを含めるかどうかを選択します。
5. レポート配信の詳細を入力します。レポートを電子メールで配信する場合は、[電子メールを使用してレポートを送信] をオンにします。レポートを送信するメールアドレスを入力します。

設定ページで電子メール通知を構成します。電子メール通知の設定の詳細については、["設定を構成する"](#)。

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。