



# Microsoft SQL Server

## NetApp Solutions

NetApp  
March 04, 2025

# 目次

Microsoft SQL Server	1
TR-4951：『Backup and Recovery for Microsoft SQL Server on AWS FSx ONTAP』	1
SnapCenter の設定	1
SnapCenter 新しくインストールされたユーザインターフェイス	1
バックアップポリシーを設定する	10
MSSQL Serverデータベースを設定および保護します	17
SnapCenter バックアップ処理	19
バックアップジョブを監視します	20
複数データベースのバックアップ処理	21
複数のSQL Serverデータベースを設定して保護します	30
複数のSQL Serverデータベースに対してオンデマンドバックアップを実行します	33
複数データベースのバックアップジョブを監視します	35
複数データベースバックアップのトランザクションログバックアップ	36
複数のMSSQL Serverデータベースを設定して保護します	42
複数のSQL Serverデータベースに対して、オンデマンドのトランザクションログバックアップをトリガーします	45
監視	47
リストアとリカバリ	47
SQL Serverデータベース上の削除されたテーブルの特定の時点へのリストア	48
リストアの進行状況を監視しています	53
詳細情報の入手方法	55
TR-4923：『SQL Server on AWS EC2 using Amazon FSx ONTAP』	55
はじめに	55
Amazon FSx ONTAPとSQL Serverを併用するメリット	56
開始する前に	57
SQL Server	
用のストレージを設定し、バックアップ、リストア、クローニングの各処理にSnapCenterを導入します	59
付録	79
詳細情報の入手方法	84
Azure NetApp Files 上の SQL Server	84
TR-4897：『SQL Server on Azure NetApp Files - Real Deployment View』	84
考慮すべき要因	85
リアルタイムの高レベル・リファレンス・デザイン	90
まとめ	97
詳細情報の入手方法	98
TR-4467：『SAP with Microsoft SQL Server on Windows』 - 『Best Practices Using NetApp Clustered Data ONTAP and SnapCenter』	98
Microsoft SQL Server環境の刷新	99

TR-4590 : 『Best Practice Guide for Microsoft SQL Server with ONTAP』	99
TR-4764 : 『Best Practices for Microsoft SQL Server with NetApp EF Series』	99

# Microsoft SQL Server

## TR-4951 : 『Backup and Recovery for Microsoft SQL Server on AWS FSx ONTAP』

著者：Niyaz Mohammed、Carine Ngwekwe - ネットアップソリューションエンジニアリング

このドキュメントでは、AWS FSx ONTAP with SnapCenterでMicrosoft SQL Serverのバックアップとリカバリを実行するために必要な手順について説明します。これには、次の情報が含まれます。

- NetApp SnapCenter の構成
- SnapCenter バックアップ処理
- FCIデータベースのバックアップ処理
- 複数データベースのバックアップ処理
- リストアとリカバリ

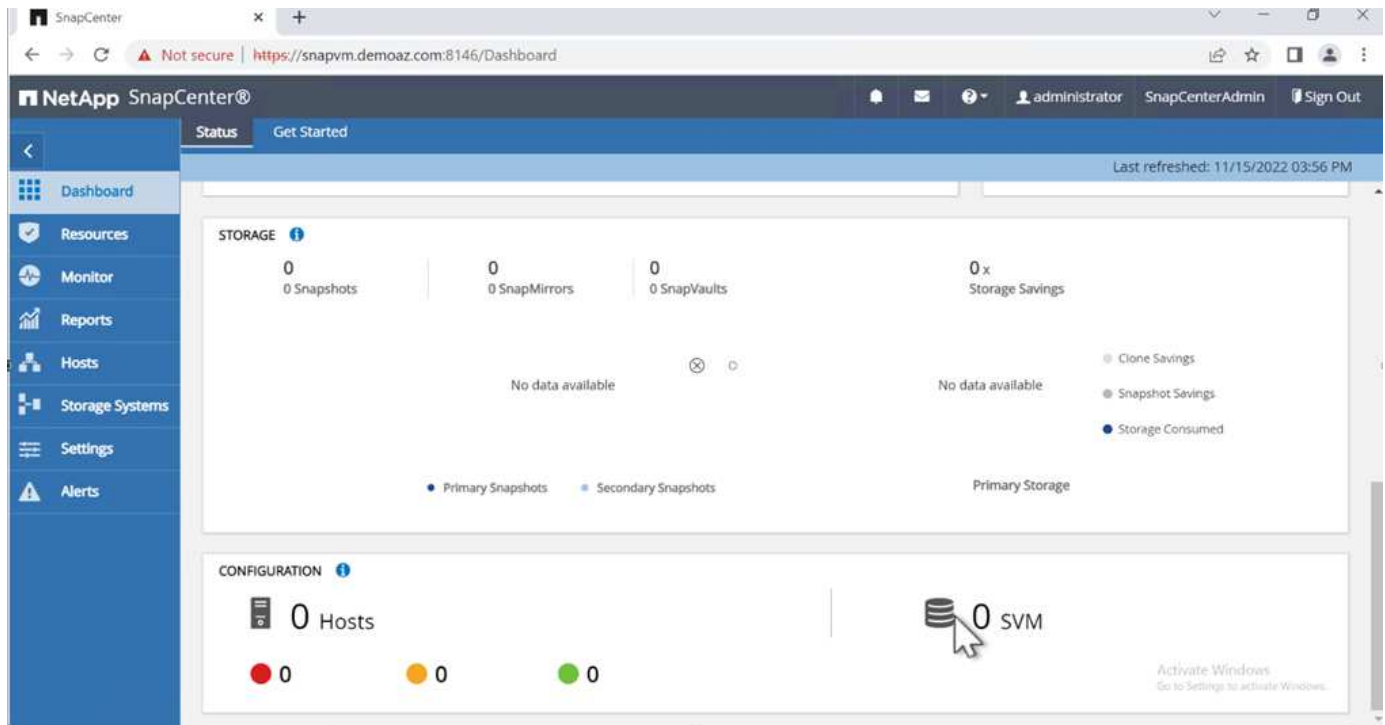
### SnapCenter の設定

SnapCenter の設定とMicrosoft SQL Serverリソースの保護について、次の手順を実行する必要があります。次の各手順については、以降のセクションで詳しく説明します。

1. SQL Serverのバックアップおよびリストアユーザのsysadminクレデンシャルを設定します。
2. ストレージを設定します。SnapCenterからAmazon FSx ONTAP Storage Virtual Machine (SVM) にアクセスするためのAmazon Web Services (AWS) 管理クレデンシャルを指定してください。
3. SnapCenter にSQL Serverホストを追加します。必要なSnapCenter プラグインを導入してインストールします。
4. ポリシーを設定する。バックアップ処理のタイプ、保持、およびオプションのSnapshotバックアップのレプリケーションを定義します。
5. Microsoft SQL Serverデータベースを設定して保護します。

### SnapCenter 新しくインストールされたユーザインターフェイス

SQL Serverバックアップのクレデンシャルを設定し、sysadmin権限を持つユーザをリストアします。

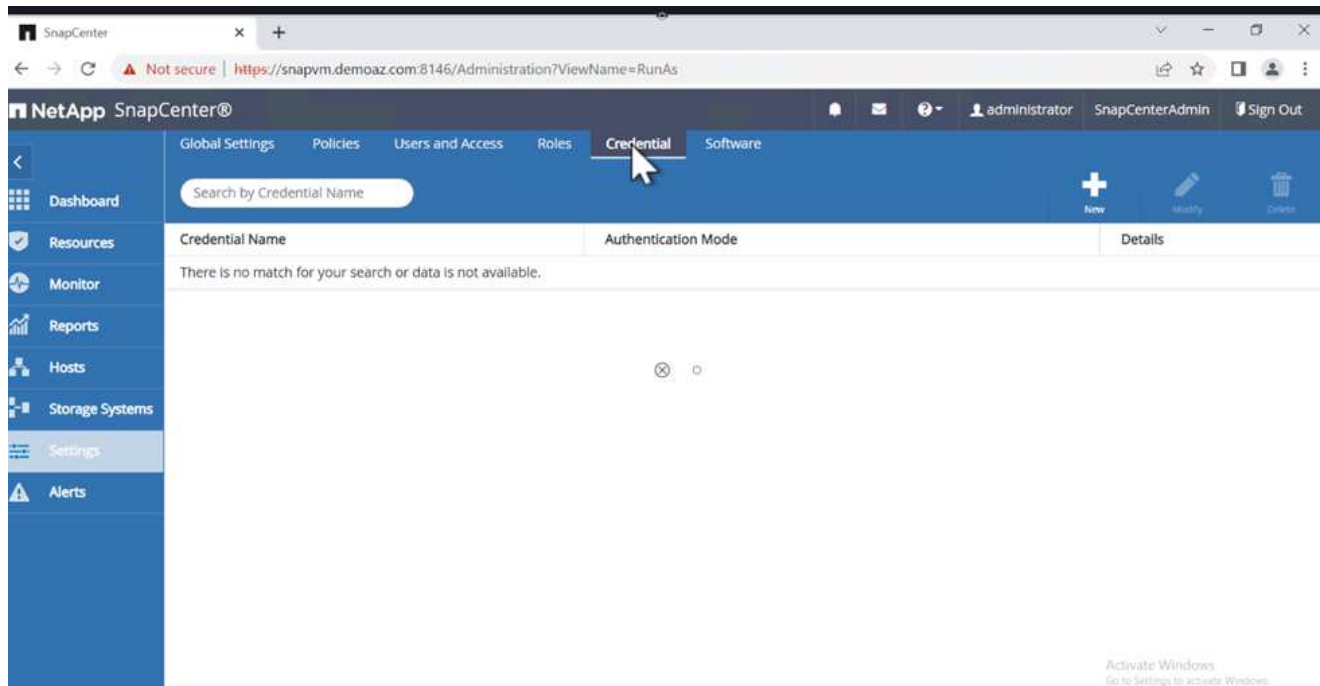


ロールベースアクセス制御（RBAC）を使用して、SnapCenter ホストとWindowsホストの個々のユーザにデータ保護機能と管理機能を委譲することを推奨します。ユーザには、データベースをホストしているSQL Serverへのアクセス権が必要です。ホストが複数ある場合は、ユーザ名とパスワードがさまざまなホストで同じである必要があります。さらに、SnapCenter がSQL Serverホストに必要なプラグインを導入できるようにするには、SnapCenter のドメイン情報を登録してクレデンシャルとホストを検証する必要があります。

次のセクションを展開して、各手順の実行方法の詳細な手順を確認します。

クレデンシャルを追加します

に移動し、[クレデンシャル]を選択して (+\*) をクリックします。



新しいユーザには、SQL Serverホストに対する管理者権限が必要です。

### Credential

Credential Name: Demoaz

Authentication Mode: Windows

Username: demoaz\clusteradmin

Password: .....

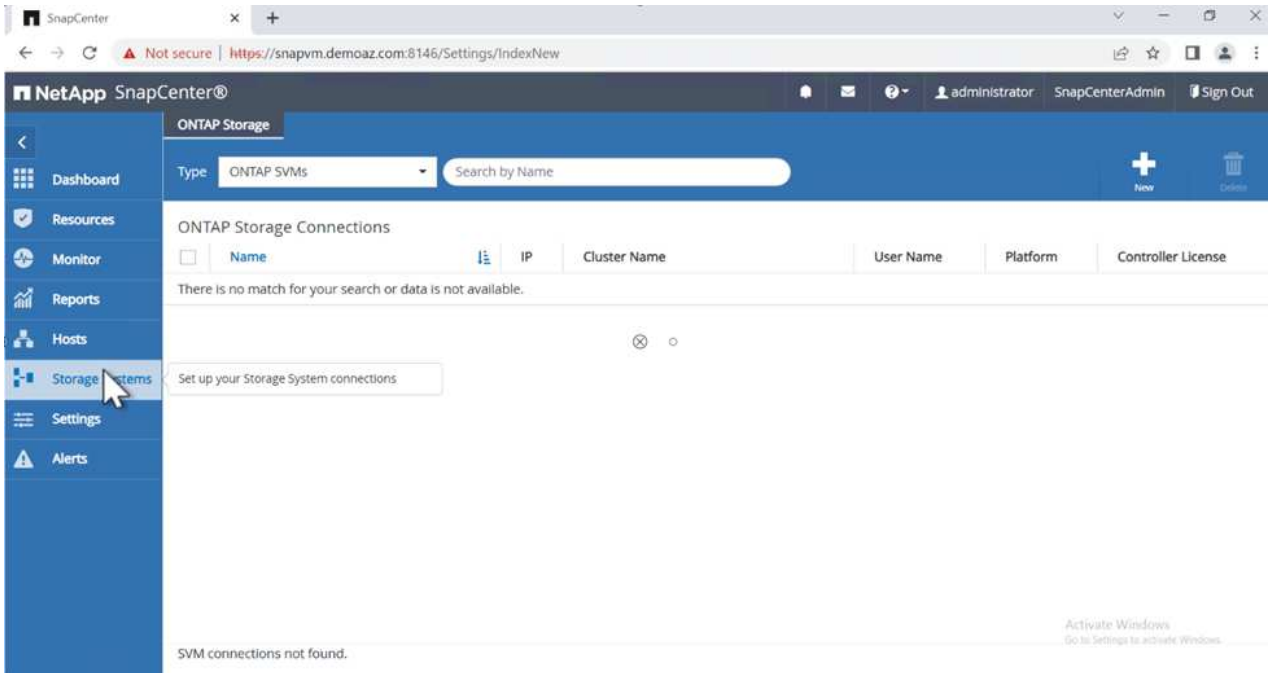
Setting credential...

Cancel OK

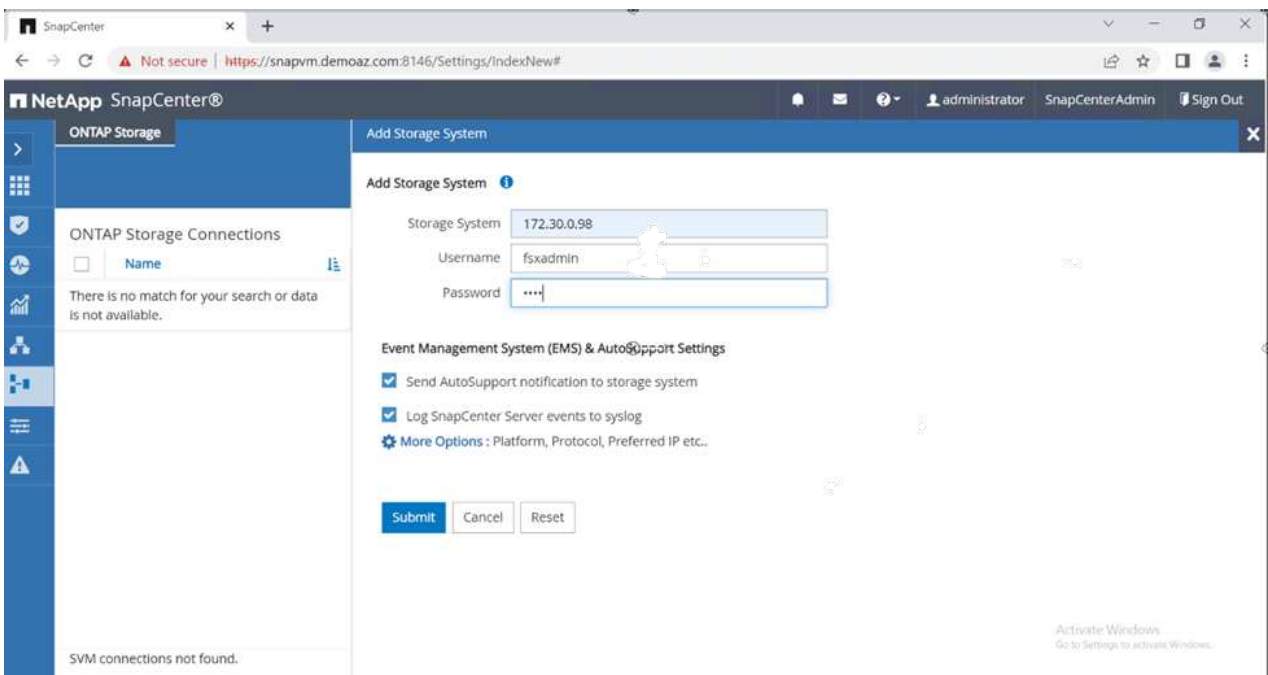
## ストレージを設定する

SnapCenter でストレージを設定するには、次の手順を実行します。

1. SnapCenter UIで、[ストレージシステム]\*を選択します。ストレージには、ONTAP SVM と ONTAP クラスタ\*の2種類があります。デフォルトのストレージタイプは「ONTAP SVM」です。
2. (+) をクリックしてストレージシステム情報を追加します。



3. FSx ONTAP管理\*エンドポイントを提供します。



4. これで、SVMがSnapCenter で設定されました。

NetApp SnapCenter®

ONTAP Storage

Type:  Search by Name

ONTAP Storage Connections

<input type="checkbox"/>	Name	IP	Cluster Name	User Name	Platform	Controller License
<input type="checkbox"/>	ESNSVMTESTRDS		rdsfsxTest01		FSx	Not applicable

Total 1

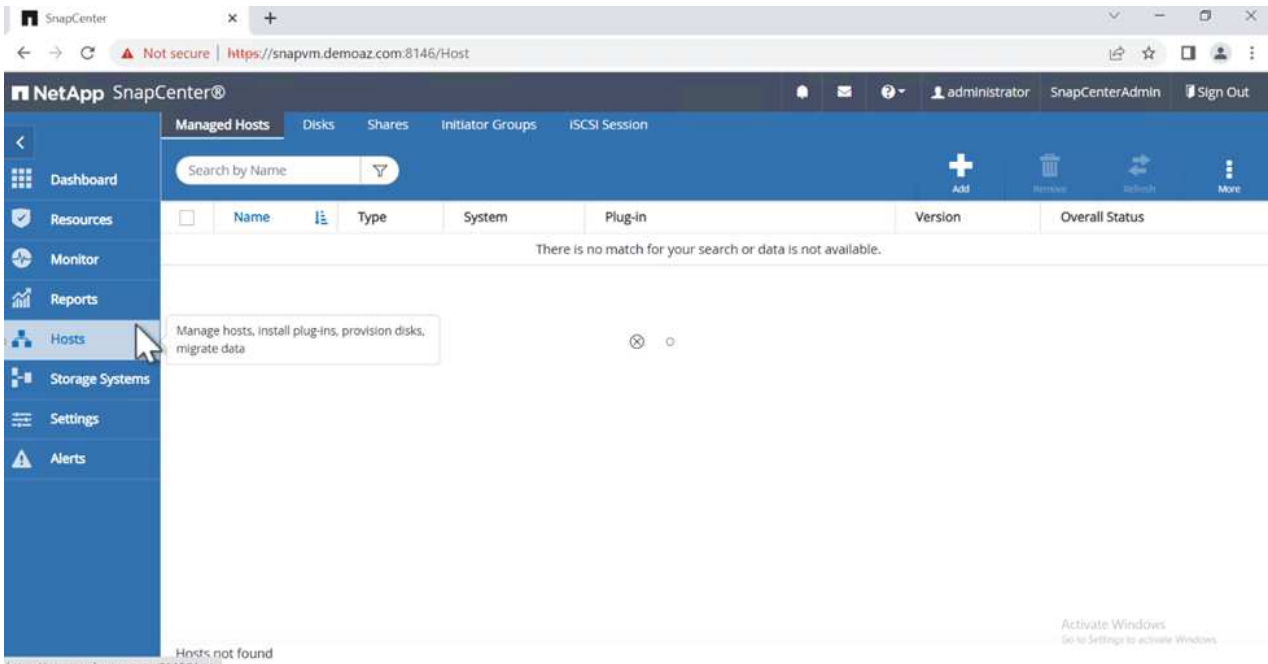
Activate Windows  
Go to Settings to activate Windows.



## SnapCenter にSQL Serverホストを追加します

SQL Serverホストを追加するには、次の手順を実行します。

1. [ホスト]タブで、 (+) をクリックしてMicrosoft SQL Serverホストを追加します。

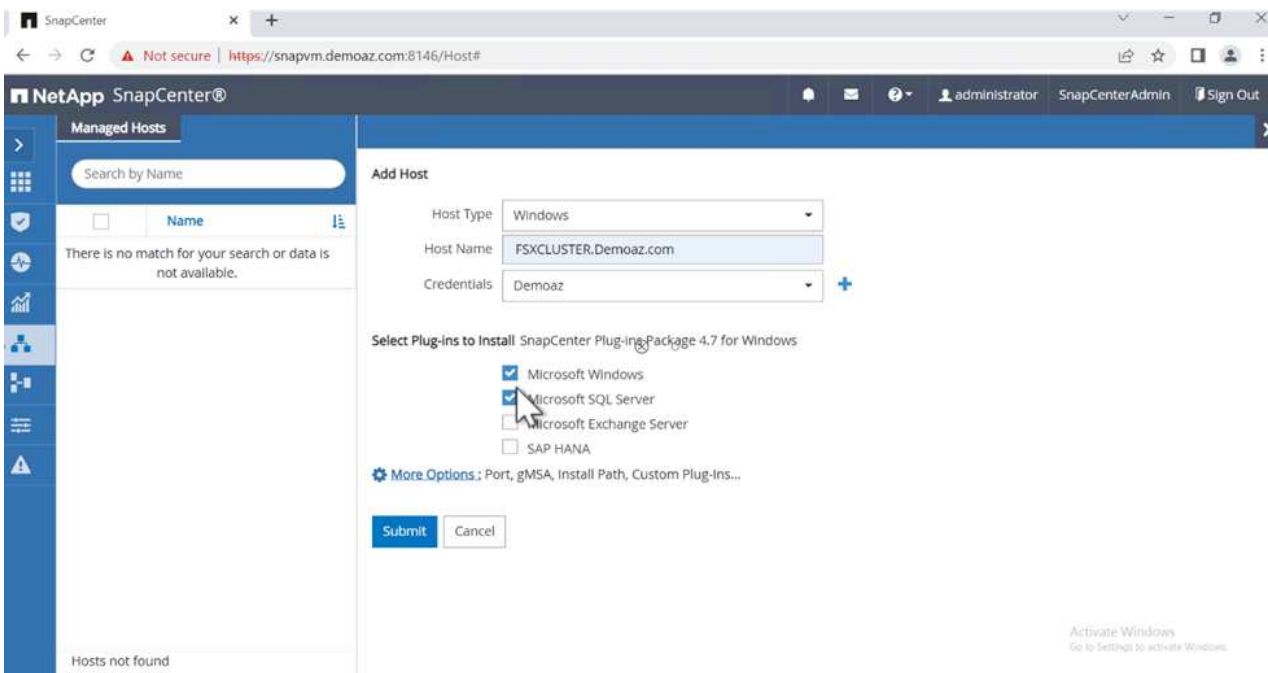


2. リモートホストの完全修飾ドメイン名 (FQDN) またはIPアドレスを指定します。

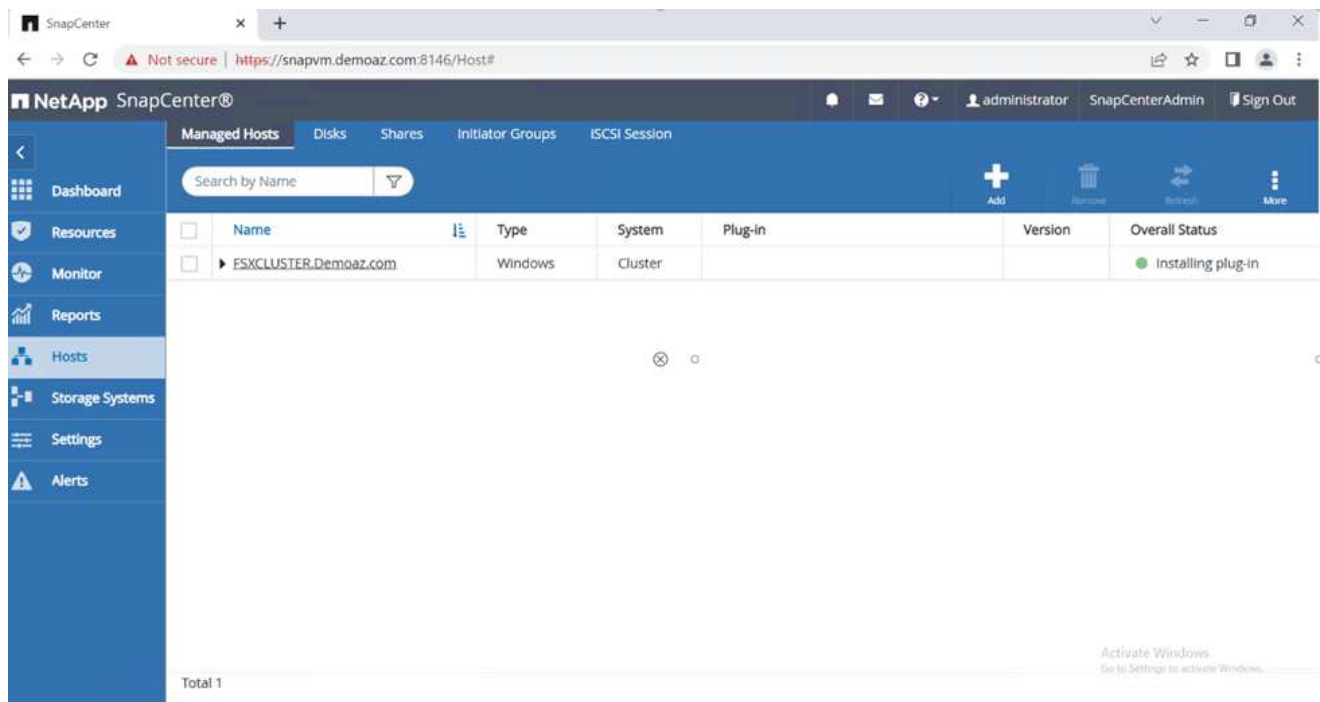


クレデンシャルがデフォルトで入力されています。

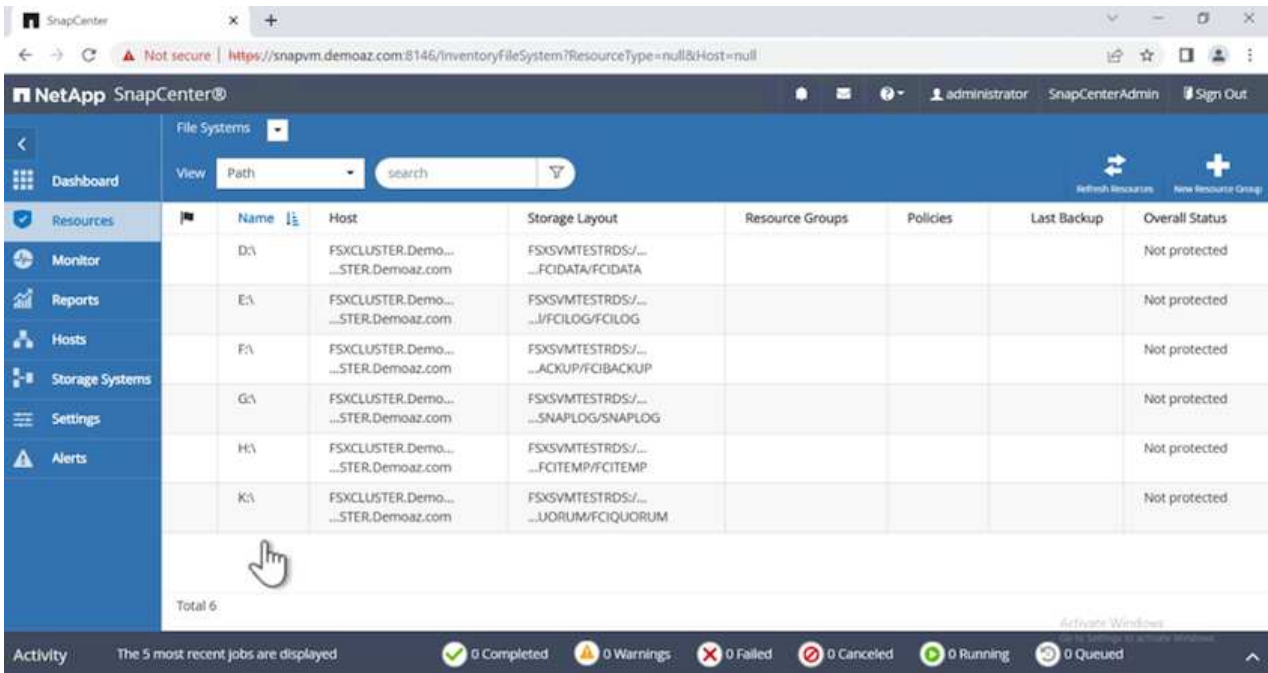
3. Microsoft WindowsおよびMicrosoft SQL Serverのオプションを選択して送信します。



SQL Serverパッケージがインストールされます。



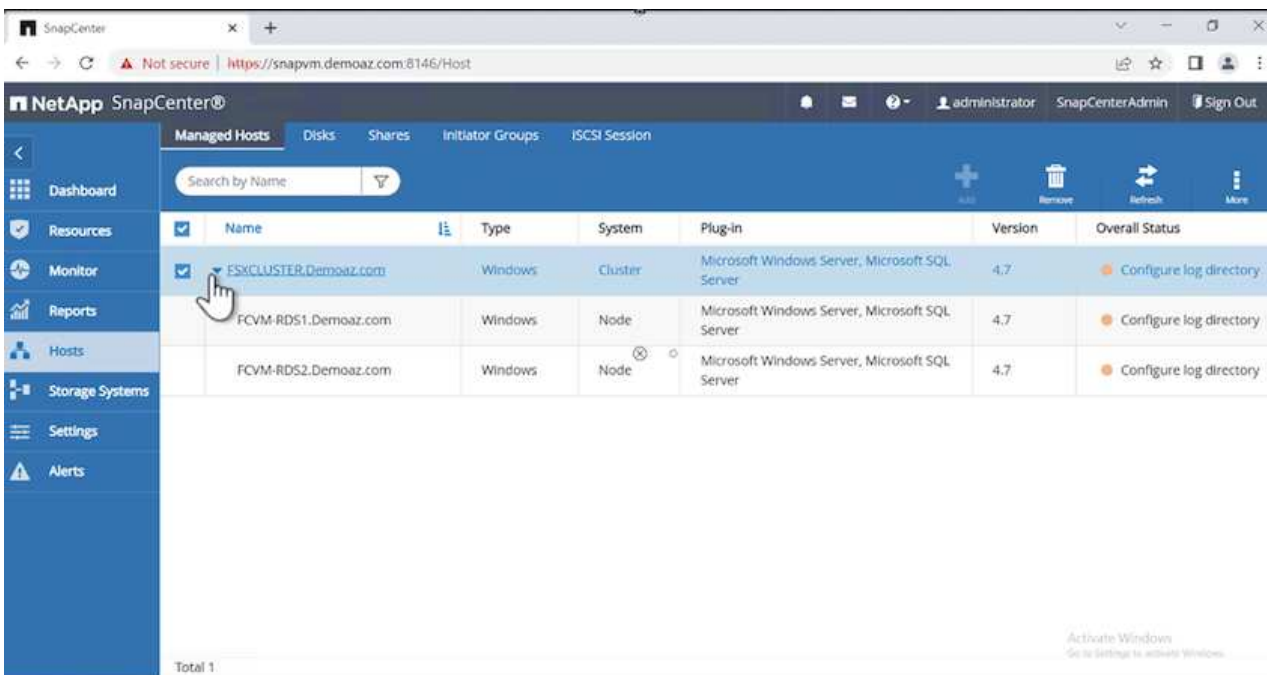
1. インストールが完了したら、\*[リソース]タブに移動して、FSx ONTAP iSCSIボリュームがすべて存在するかを確認します。



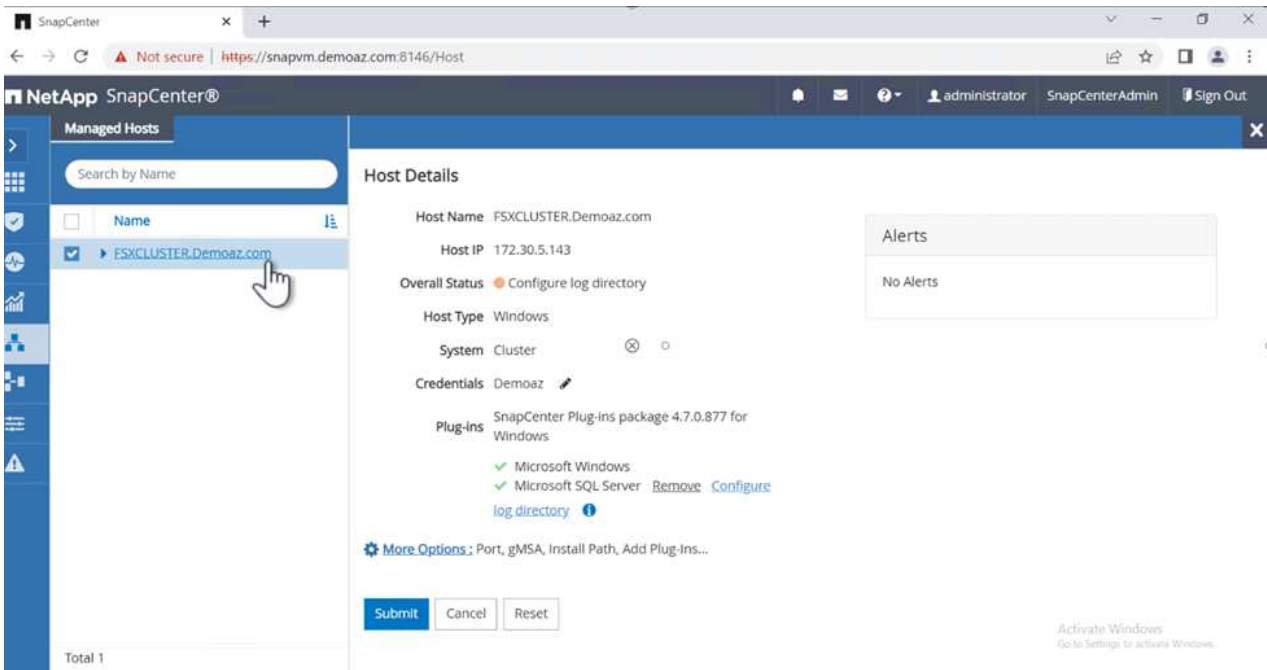
## ログディレクトリの設定

ホストログディレクトリを設定するには、次の手順を実行します。

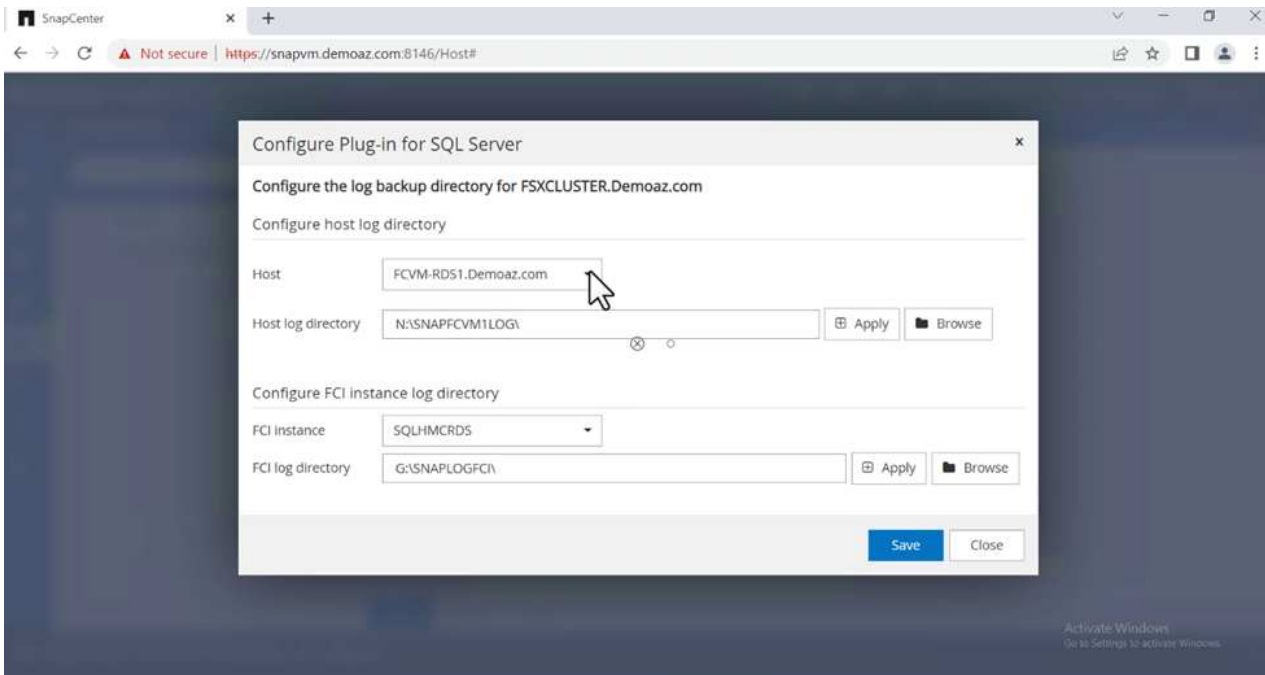
1. チェックボックスをクリックします。新しいタブが開きます。



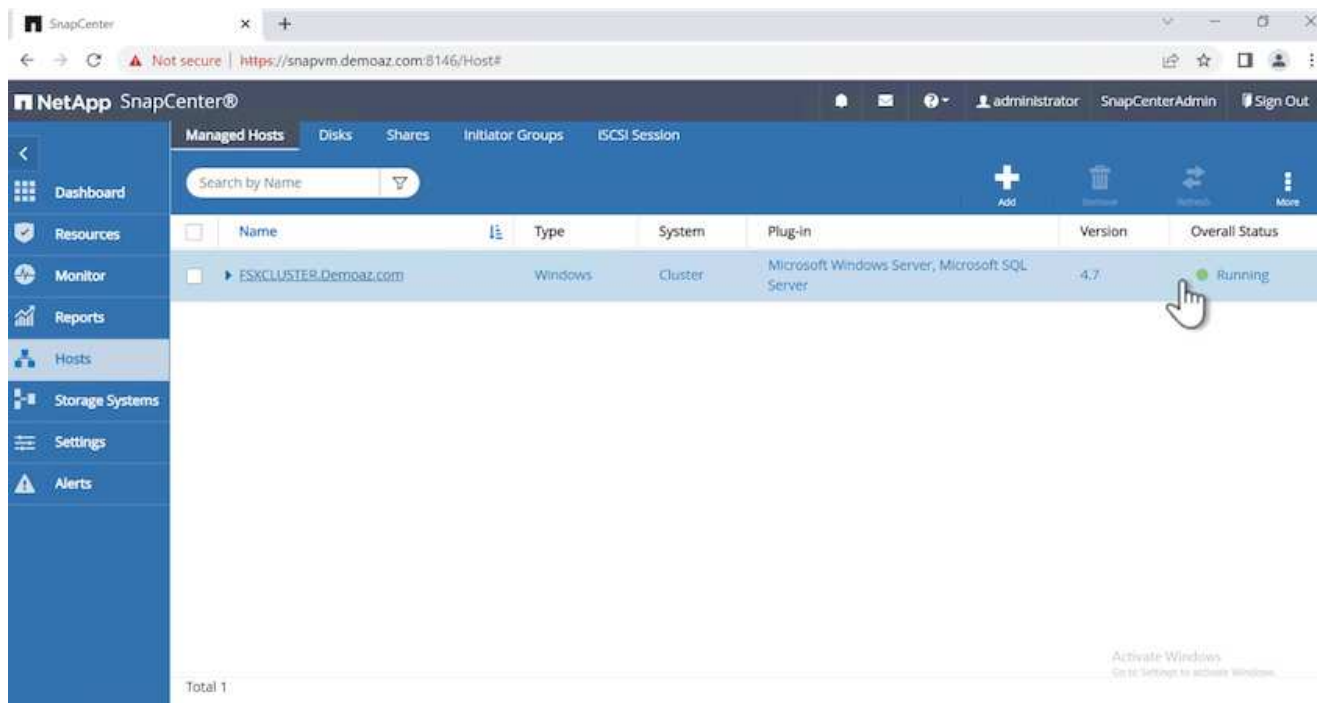
2. [Configure log directory]\*リンクをクリックします。



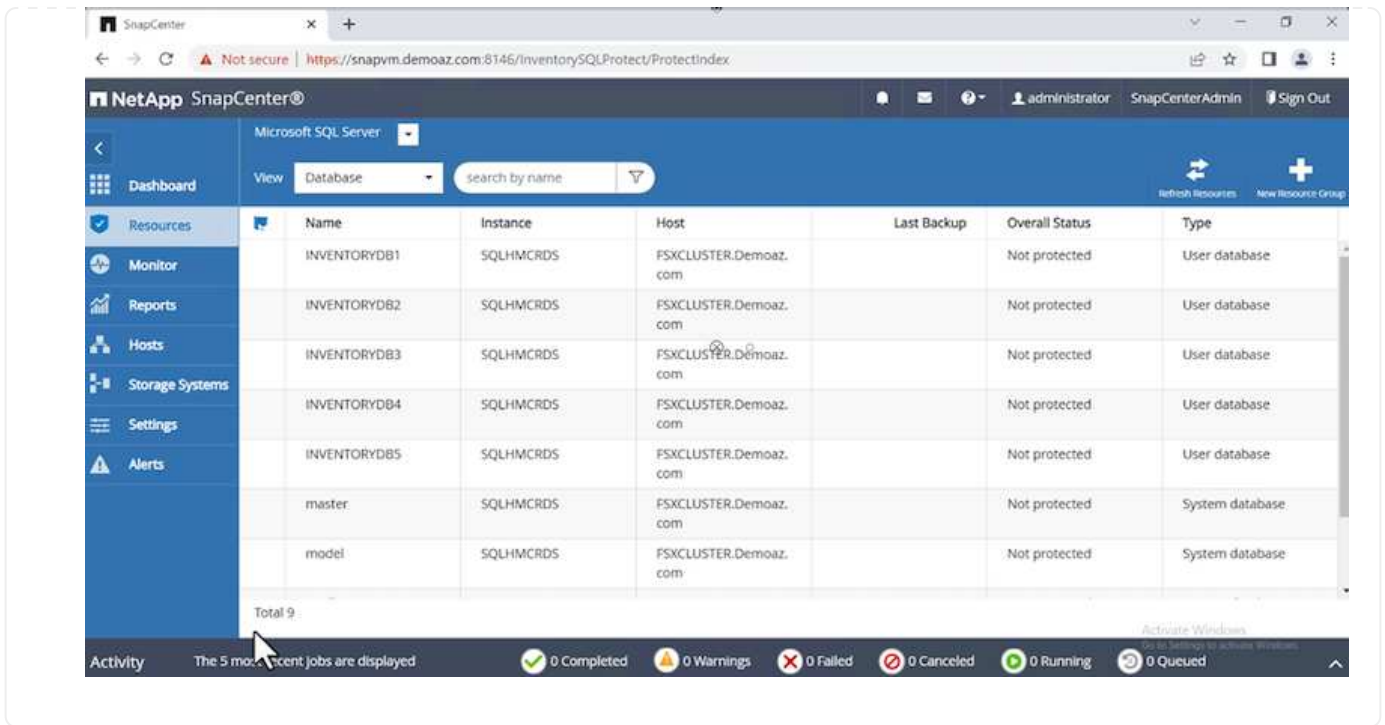
3. ホストログディレクトリとFCIインスタンスログディレクトリのドライブを選択します。[保存 (Save)] をクリックします。クラスタの2つ目のノードに対して同じ手順を繰り返します。ウィンドウを閉じます。



ホストは実行中の状態になります。



1. [リソース]タブには、すべてのサーバとデータベースが表示されます。



## バックアップポリシーを設定する

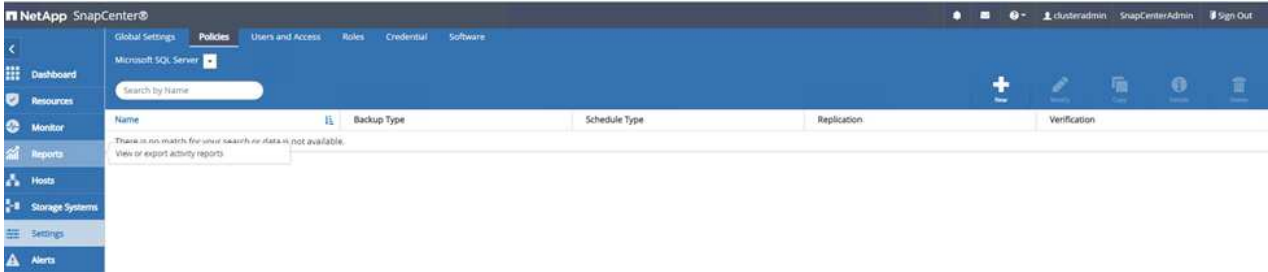
バックアップポリシーは、バックアップの管理、スケジュール設定、および保持方法を規定する一連のルールです。企業のSLAに基づくバックアップの種類と頻度を確認できます。

次のセクションを展開して、各手順の実行方法の詳細な手順を確認します。

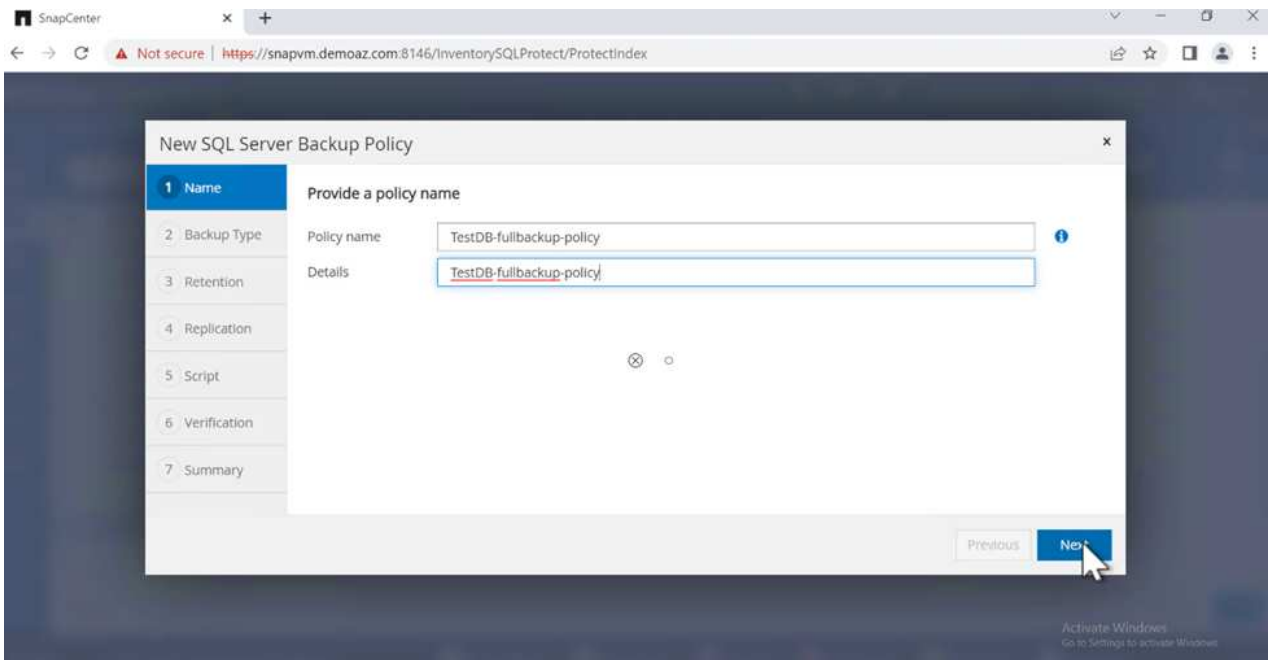
## FCIデータベースのバックアップ操作を設定します

FCIデータベースのバックアップポリシーを設定するには、次の手順を実行します。

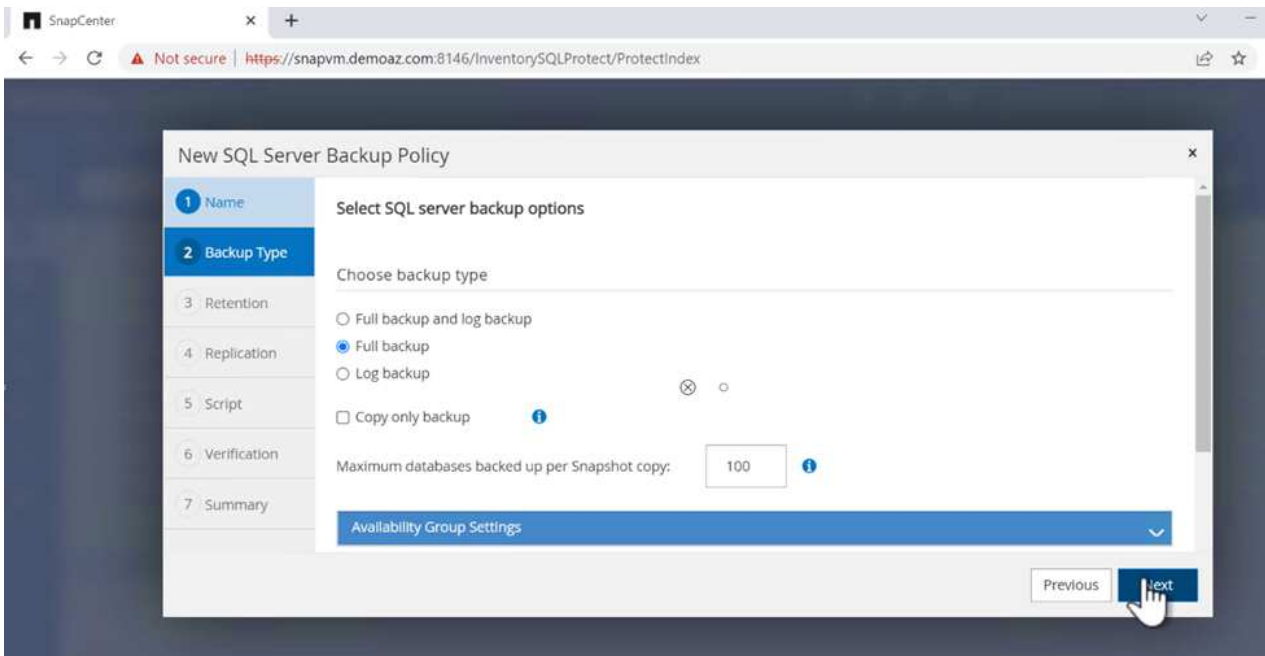
1. に移動し、左上の[ポリシー]を選択します。次に、[New]\*をクリックします。



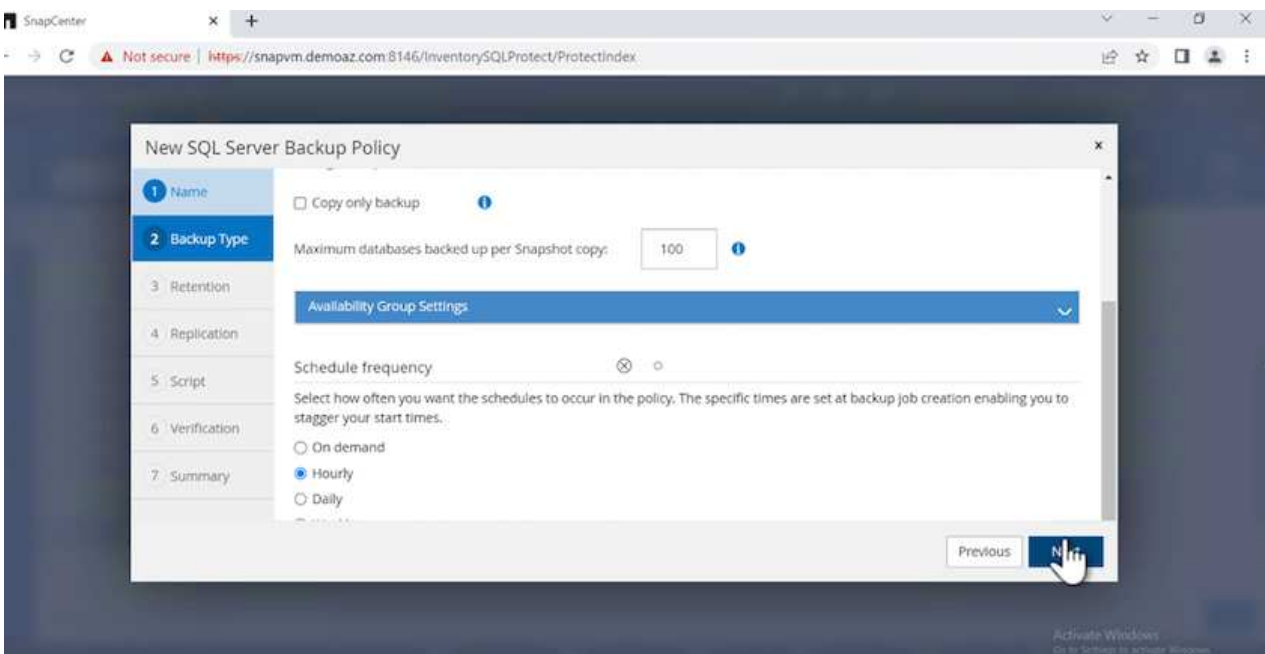
2. ポリシー名と概要 を入力します。「\*次へ\*」をクリックします。



3. バックアップタイプとして\*[フルバックアップ]\*を選択します。



4. スケジュール頻度を選択します（会社のSLAに基づきます）。「\*次へ\*」をクリックします。



5. バックアップの保持設定を行います。

New SQL Server Backup Policy x

- 1 Name
- 2 Backup Type
- 3 Retention**
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

### Retention settings

Retention settings for up-to-the-minute restore operation ⓘ

Keep log backups applicable to last  full backups

Keep log backups applicable to last  days

### Full backup retention settings ⓘ

Weekly

Total Snapshot copies to keep

Keep Snapshot copies for  days

6. レプリケーションオプションを設定します。



New SQL Server Backup Policy ×

**1** Name

**2** Backup Type

**3** Retention

**4** Replication

**5** Script

**6** Verification

**7** Summary

Select secondary replication options ⓘ

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label  ⓘ

Error retry count  ⓘ

7. バックアップジョブの実行前と実行後に実行する実行スクリプトを指定します（存在する場合）。

## New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Script timeout  secs

Previous Next

8. バックアップスケジュールに基づいて検証を実行します。

### New SQL Server Backup Policy

- Name
- Backup Type
- Retention
- Replication
- Script
- Verification**
- Summary

**Select the options to run backup verification**

Run verifications for the following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

Weekly

**Database consistency checks options**

Limit the integrity structure to physical structure of the database (PHYSICAL\_ONLY)

Suppress all information message (NO\_INFOMSGS)

Display all reported error messages per object (ALL\_ERRORMSG)

Do not check non-clustered indexes (NOINDEX)

Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)

**Verification script settings**

Script timeout: 60 secs

Prescript full path:

Prescript arguments: Choose optional arguments...

Postscript full path:

Postscript arguments: Choose optional arguments...

Previous Next

9. [サマリ]\*ページには、バックアップポリシーの詳細が表示されます。エラーはここで修正できます。

SnapCenter

Not secure | https://snapvm.demoaz.com:8146/InventorySQLProtect/ProtectIndex

### New SQL Server Backup Policy

- Name
- Backup Type
- Retention
- Replication
- Script
- Verification
- Summary**

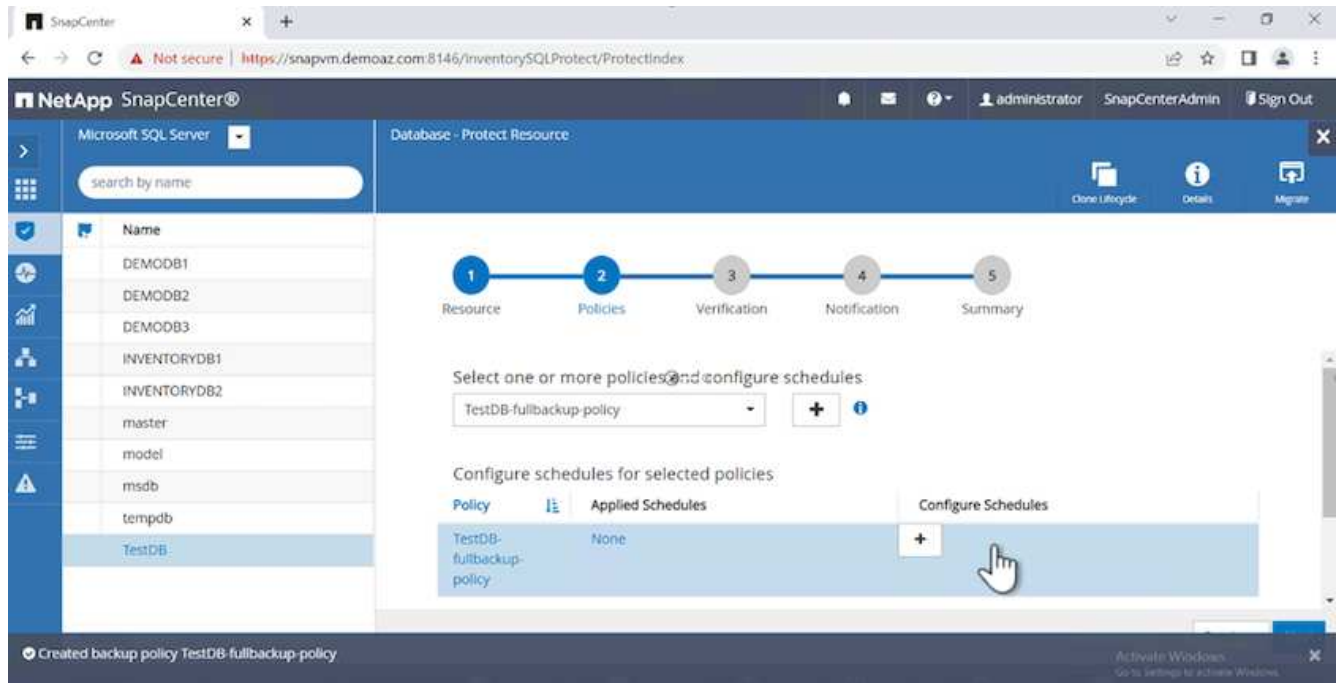
Summary	
Policy name	TestDB-fullbackup-policy
Details	TestDB-fullbackup-policy
Backup type	Full backup
Availability group settings	Backup only on preferred backup replica
Schedule Type	Hourly <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>
UTM retention	Total backup copies to retain : 7
Hourly Full backup retention	Total backup copies to retain : 7
Replication	none
Backup prescript settings	undefined
	Prescript arguments:

Previous Finish

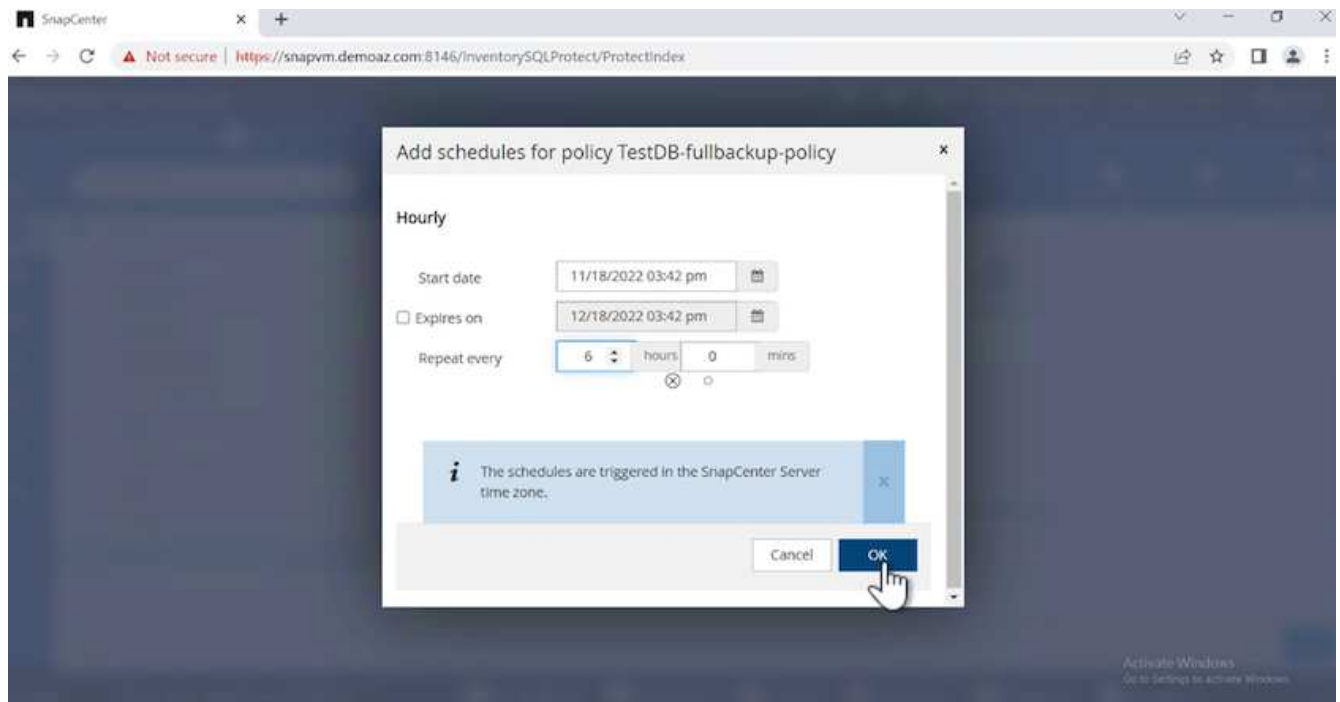
Activate Windows  
Go to Settings to activate Windows

## MSSQL Serverデータベースを設定および保護します

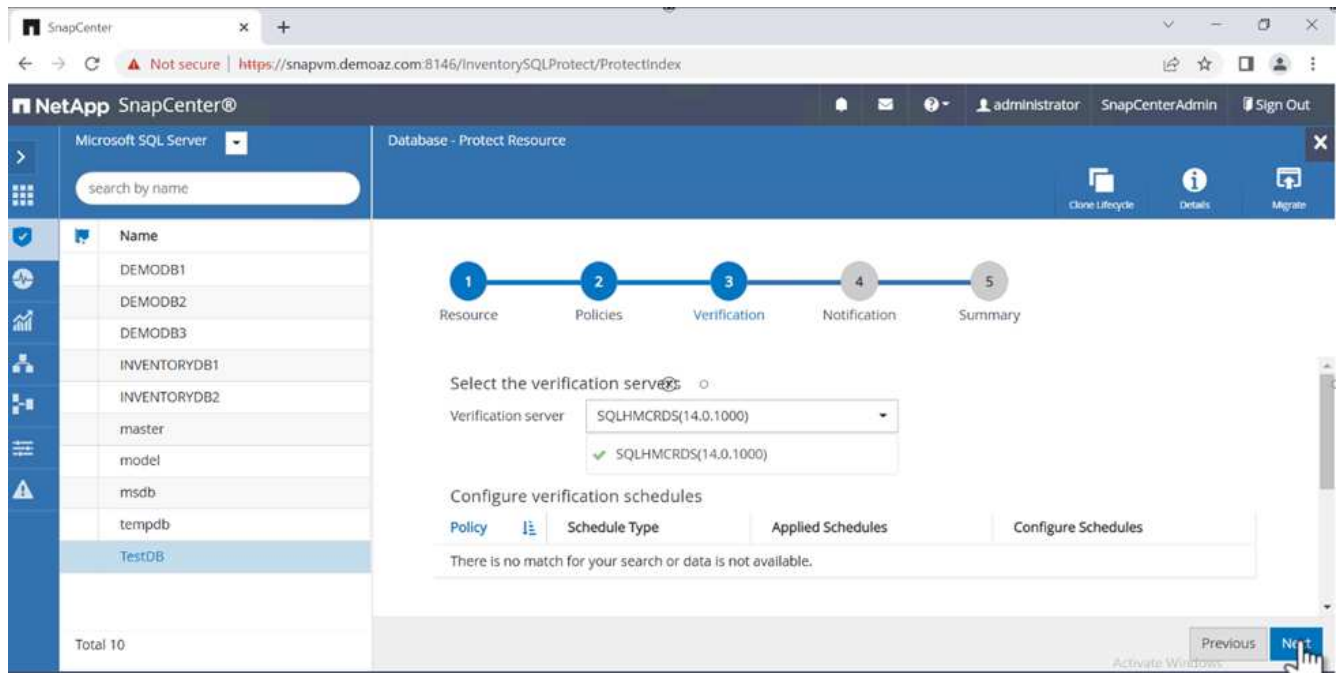
1. バックアップポリシーの開始日と有効期限を設定します。



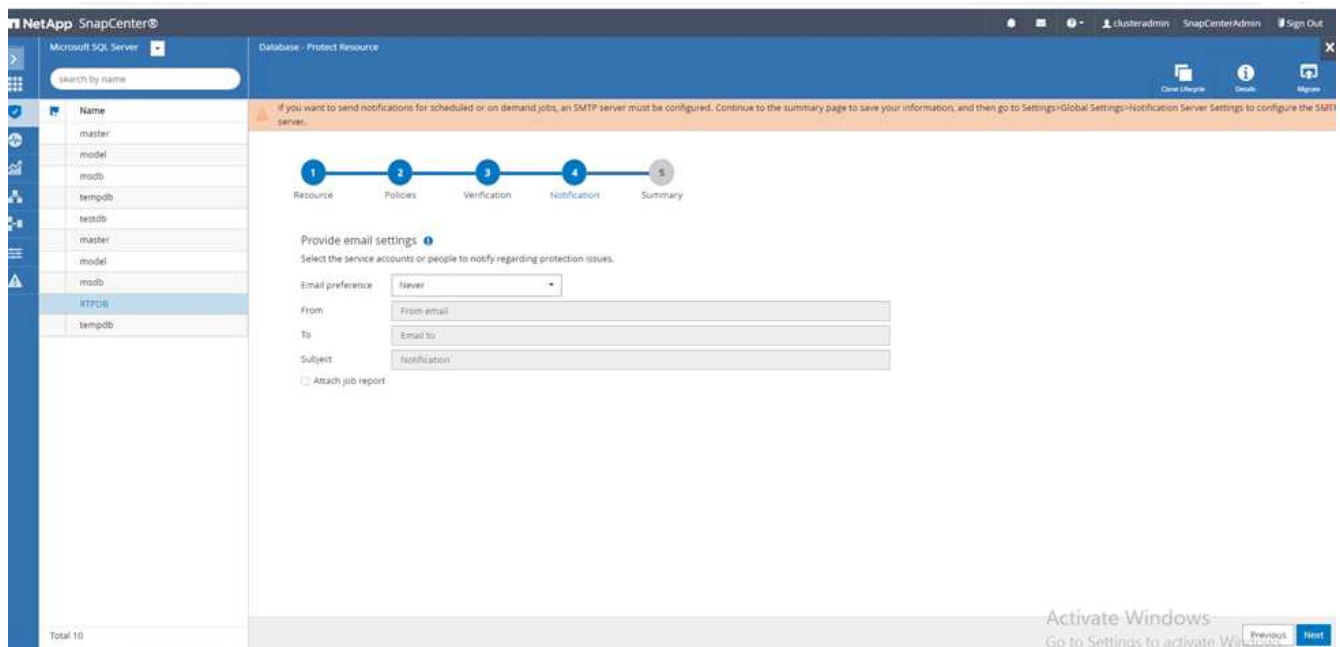
2. バックアップのスケジュールを定義します。これを行うには、 (+) をクリックしてスケジュールを設定します。[開始日]と[有効期限]に日付を入力します。会社のSLAに基づいて時間を設定します。



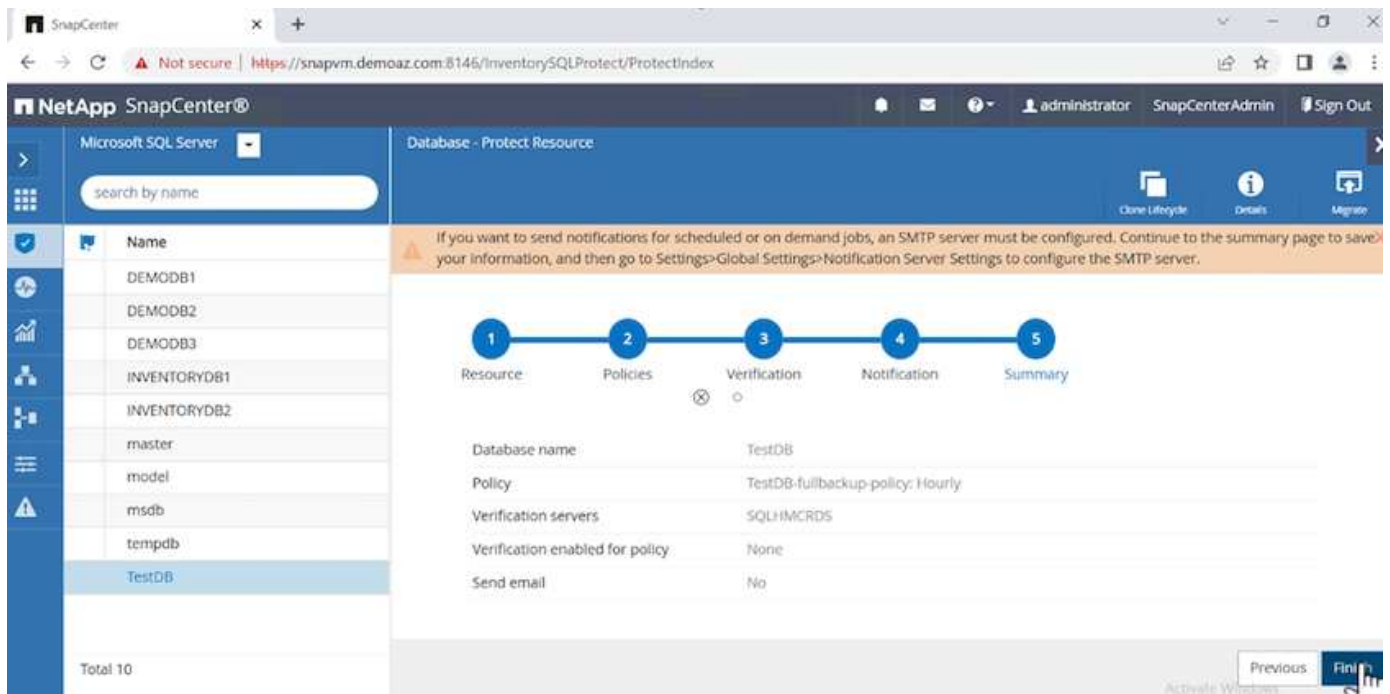
3. 検証サーバを設定ドロップダウンメニューからサーバーを選択します。



4. 設定したスケジュールを確認するには、プラス記号をクリックして確定します。
5. Eメール通知の情報を入力します。「\* 次へ \*」をクリックします。



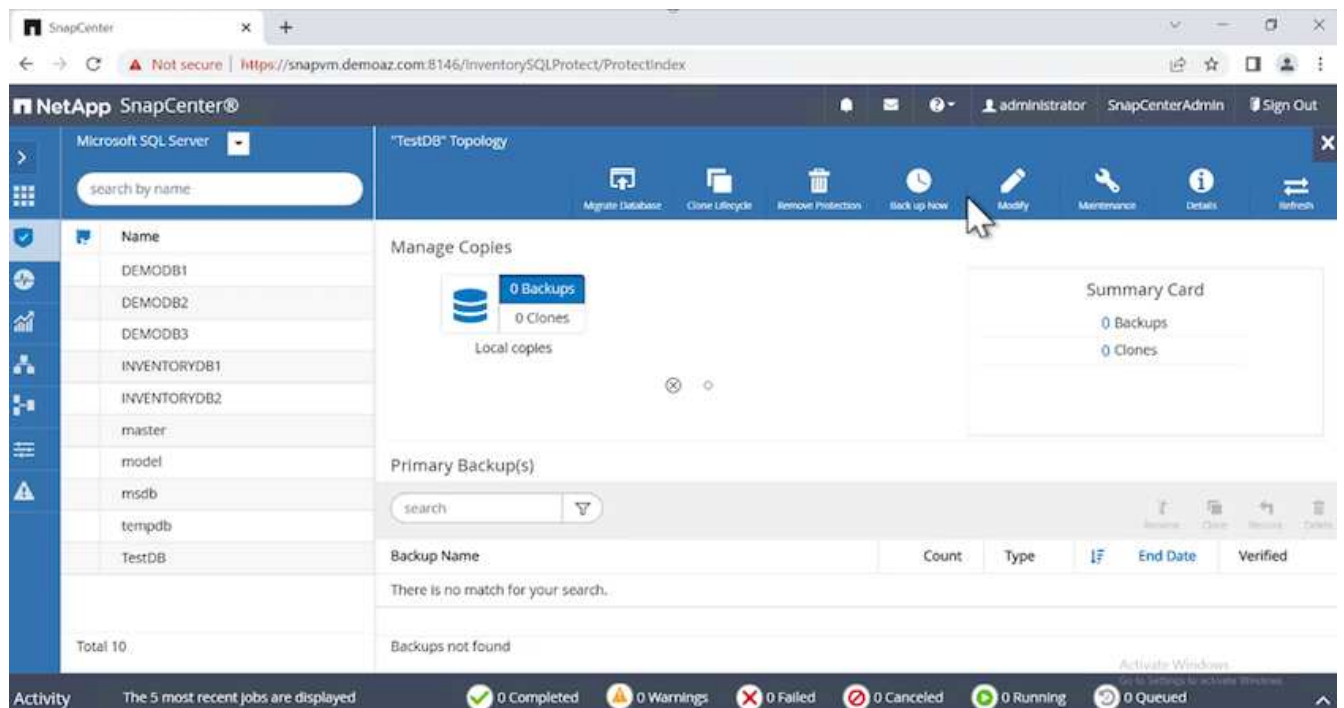
これで、SQL Serverデータベースのバックアップポリシーの概要が設定されました。



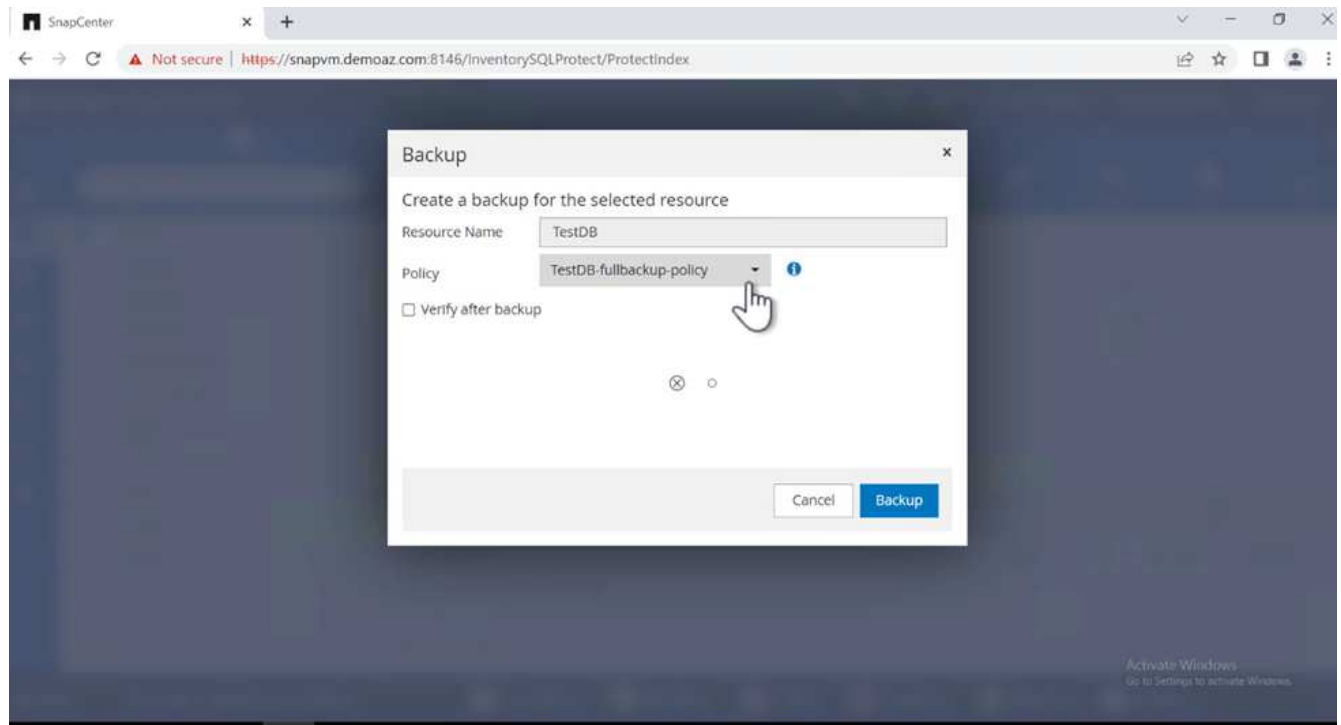
## SnapCenter バックアップ処理

SQL Serverのオンデマンドバックアップを作成するには、次の手順を実行します。

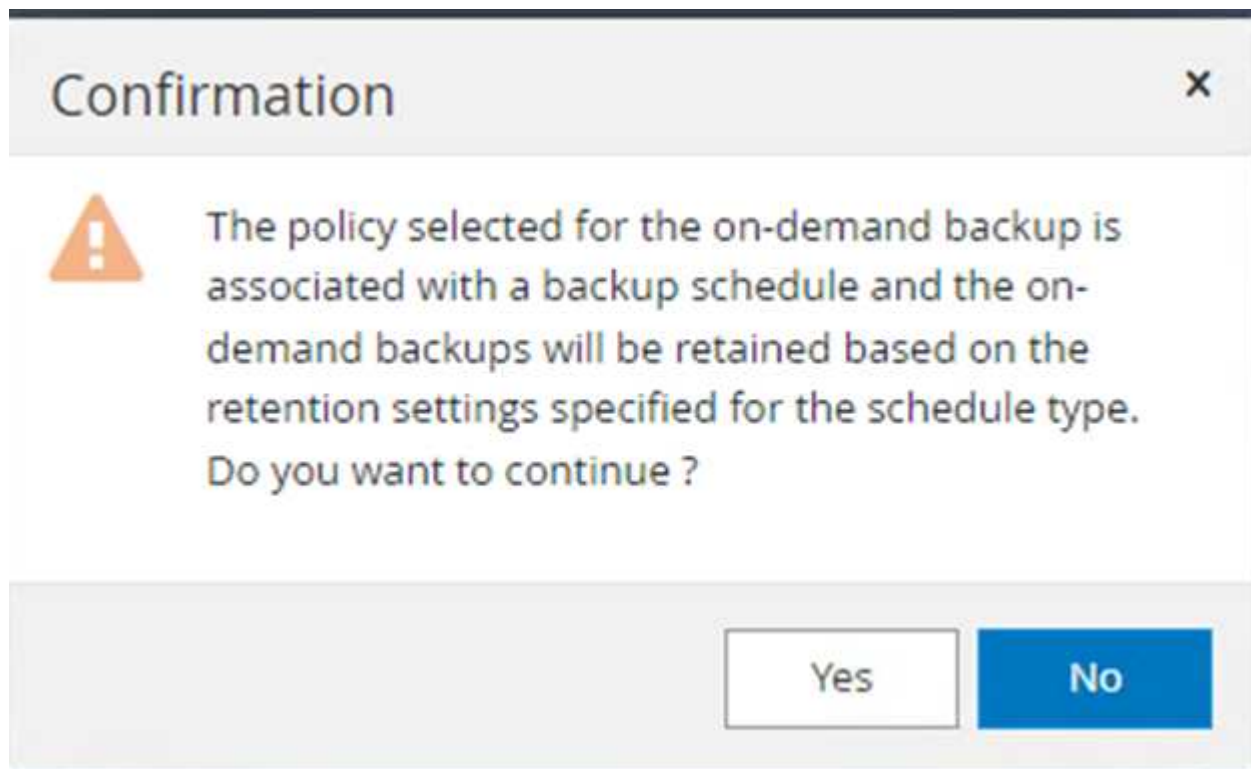
1. [リソース]ビューでリソースを選択し、\*[今すぐバックアップ]\*を選択します。



2. ダイアログボックスで、[バックアップ]\*をクリックします。



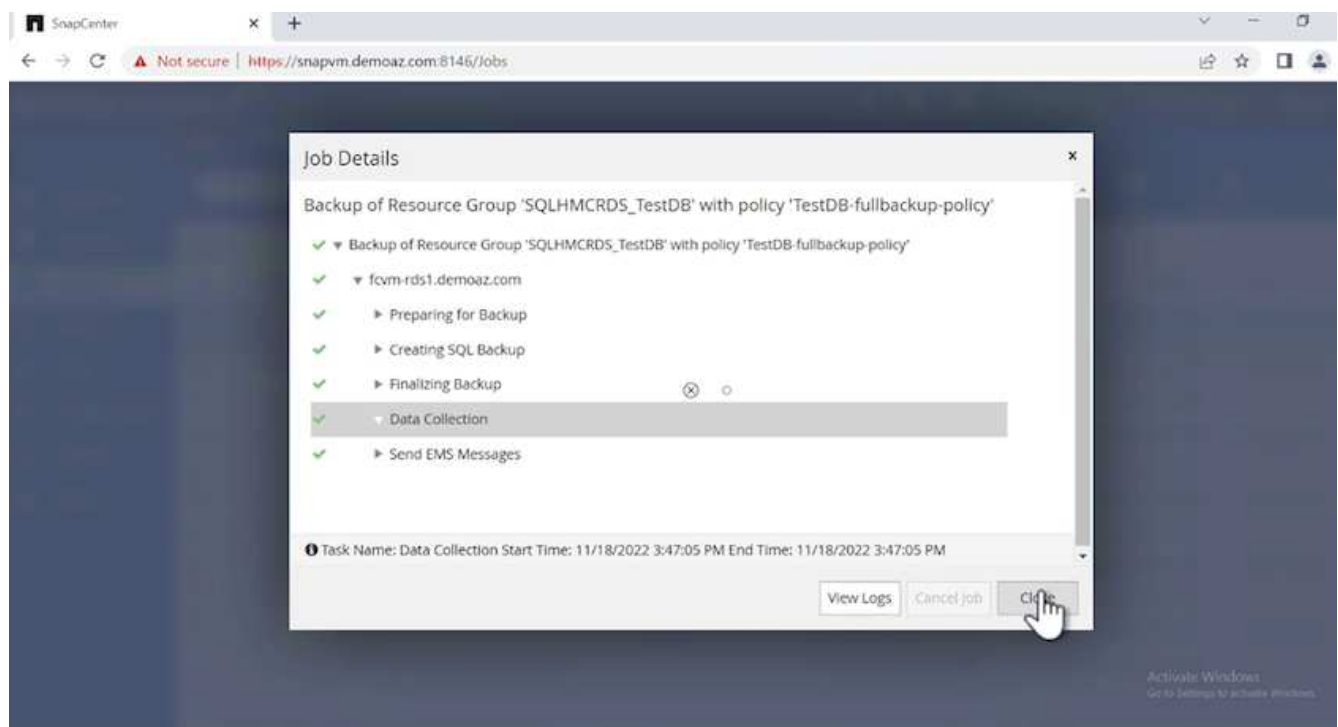
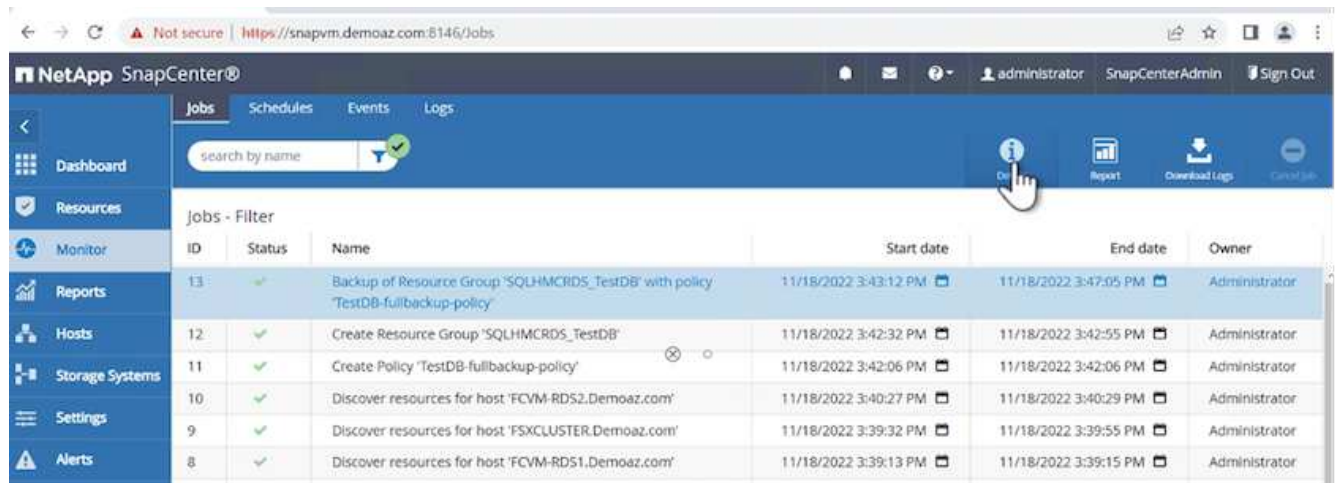
3. 確認画面が表示されます。「\*はい\*」をクリックして確定します。



## バックアップジョブを監視します

1. [監視]タブでジョブをクリックし、右側の\*[詳細]\*を選択してジョブを表示します。





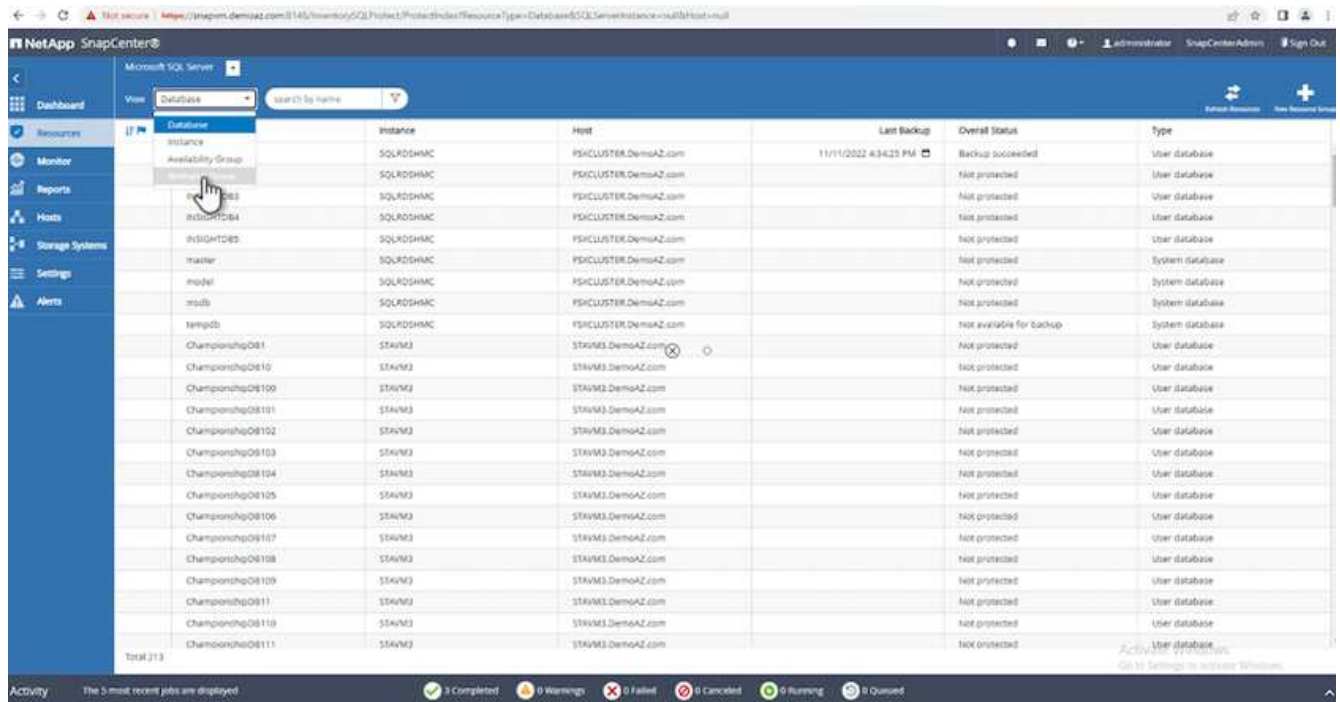
バックアップが完了すると、[Topology]ビューに新しいエントリが表示されます。

## 複数データベースのバックアップ処理

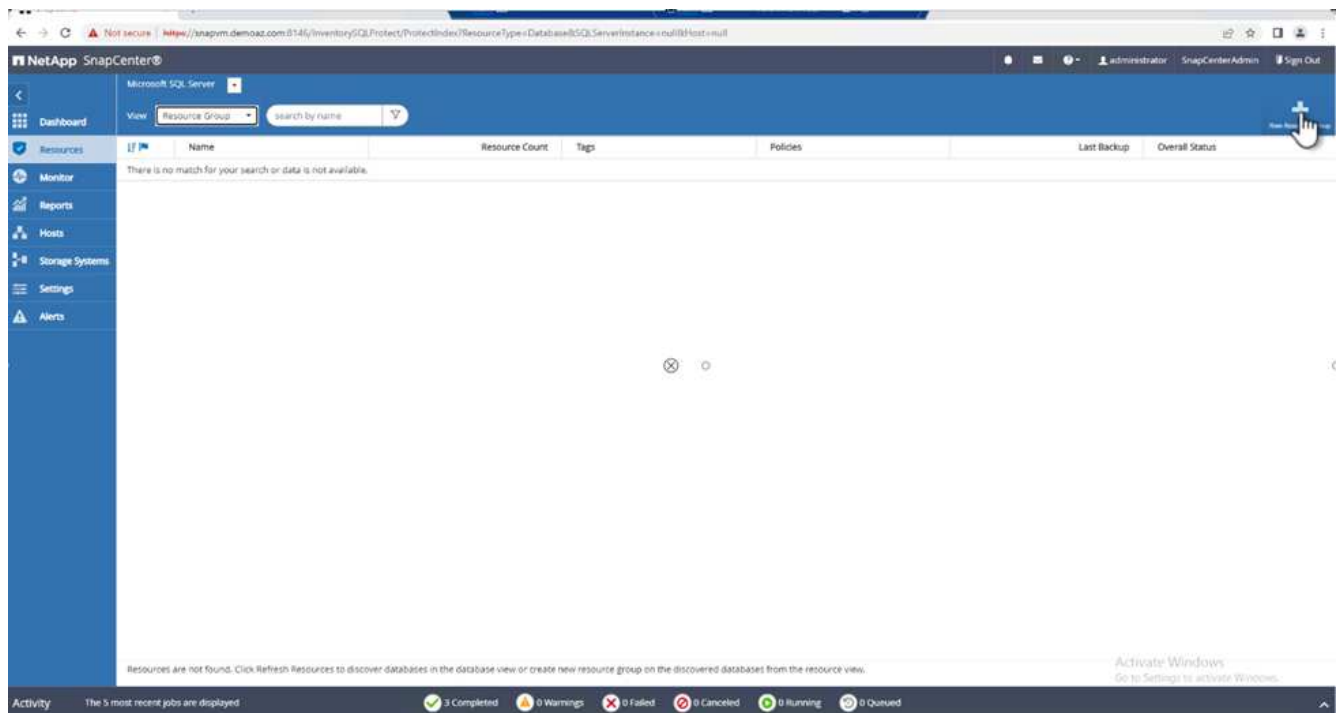
複数のSQL Serverデータベースのバックアップポリシーを設定するには、次の手順を実行してリソースグループポリシーを作成します。

1. [表示]メニューの\*[リソース]\*タブで、ドロップダウンメニューを使用してリソースグループに変更します。

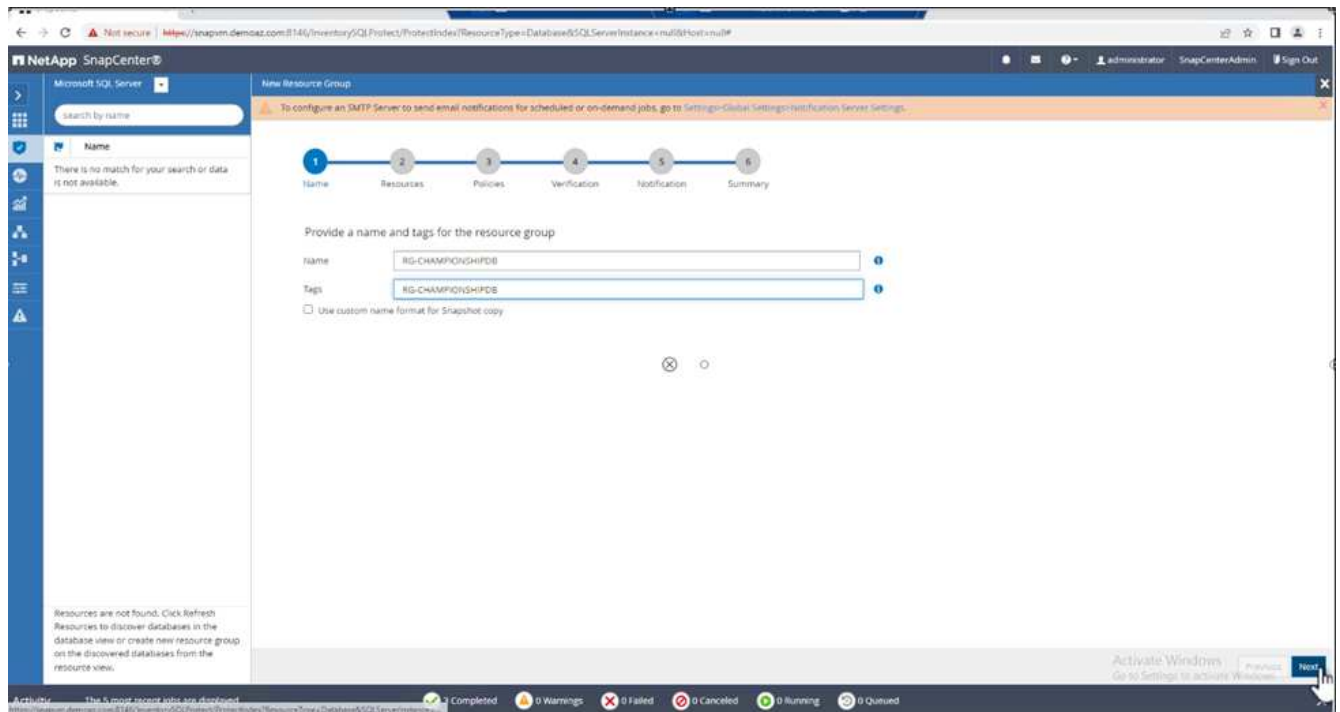




2. (+) をクリックすると、新しいリソースグループが表示されます。

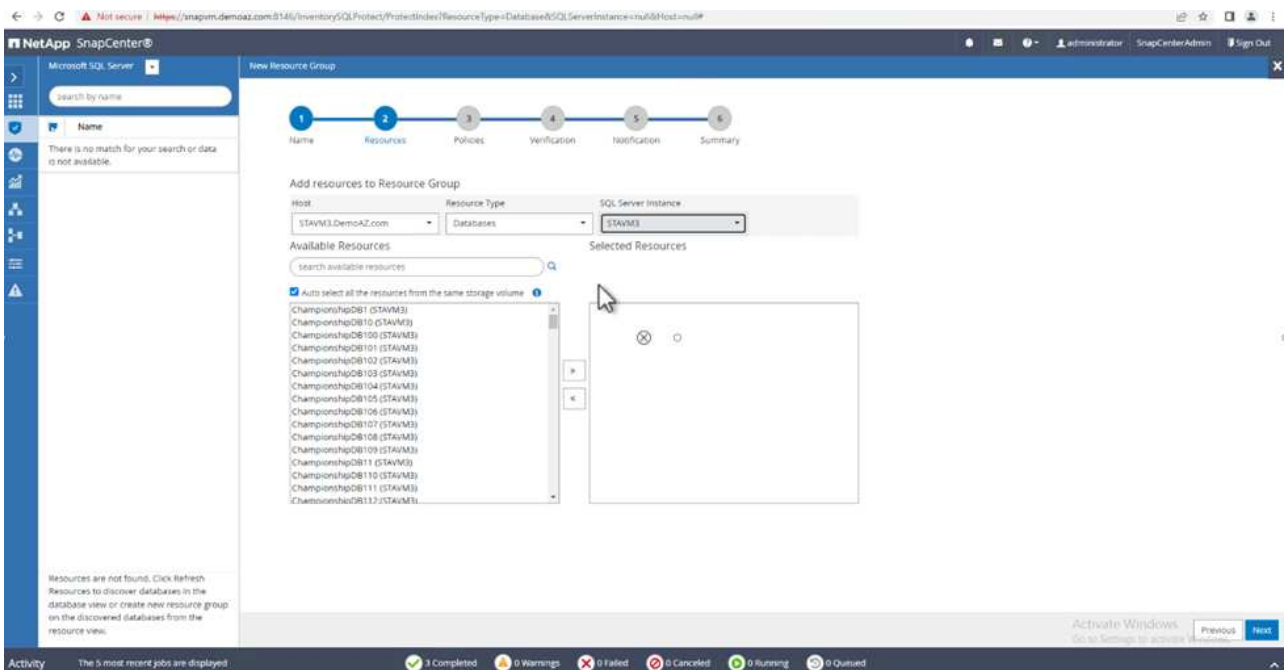


3. 名前とタグを指定します。「\* 次へ \*」をクリックします。

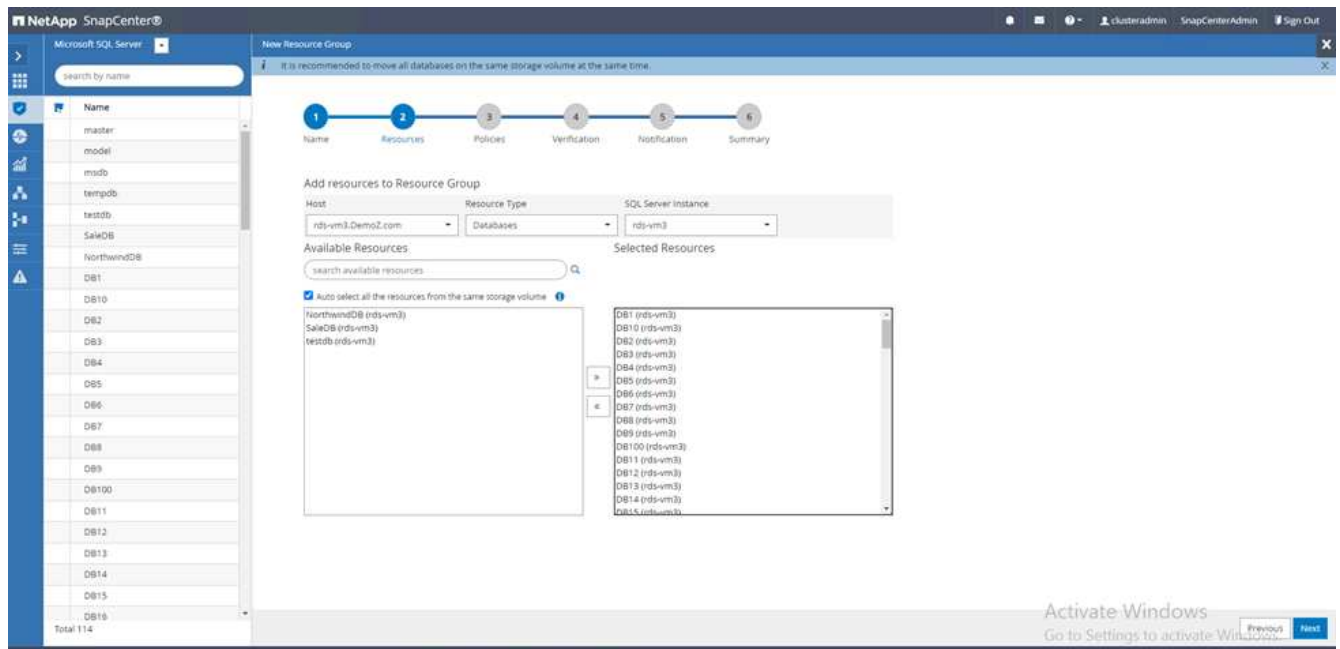


#### 4. リソースグループにリソースを追加します。

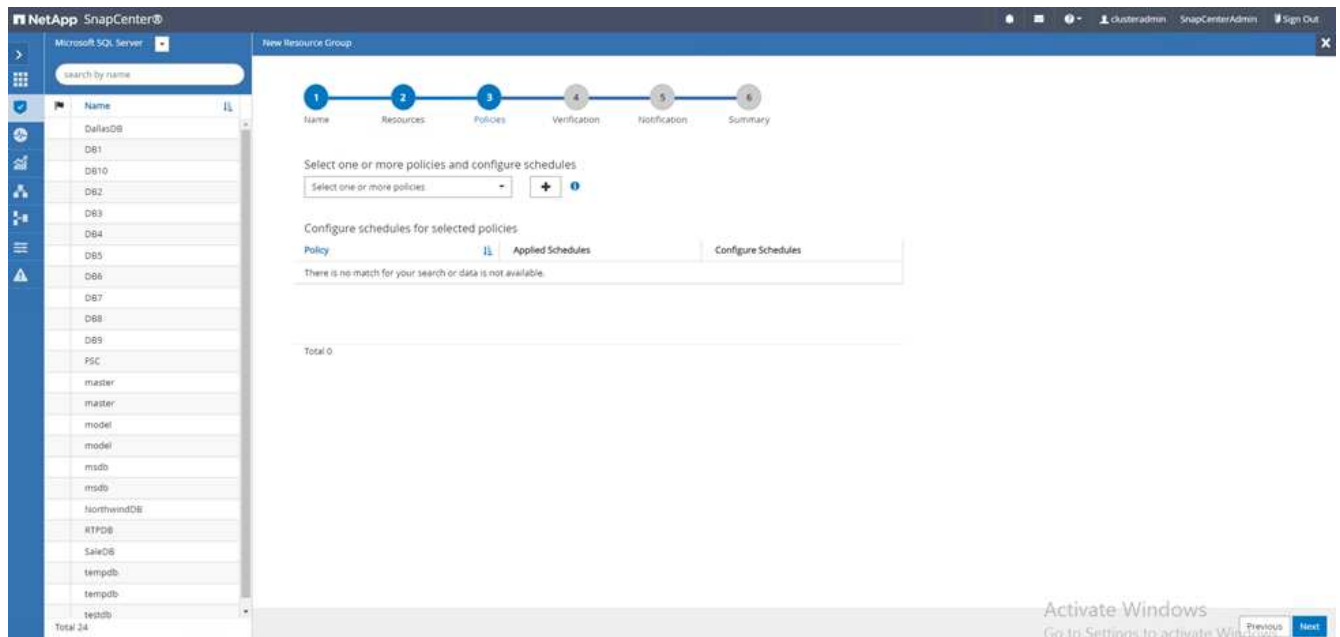
- \*ホスト\*データベースをホストするドロップダウンメニューからサーバを選択します。
- リソースタイプ。\*ドロップダウンメニューから[データベース]\*を選択します。
- \*SQL Serverインスタンス\*サーバを選択します。



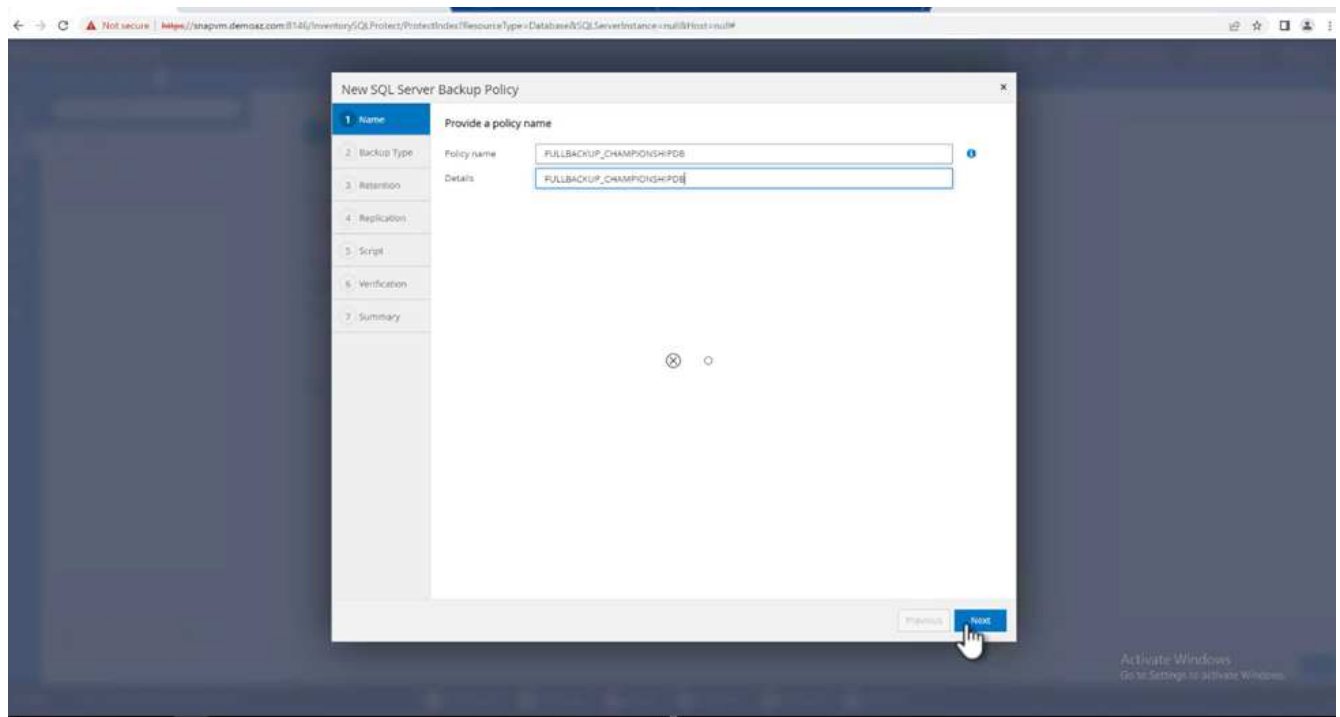
デフォルトでは、オプション[同じストレージボリュームからすべてのリソースを自動選択する]が選択されています。このオプションの選択を解除し、リソースグループに追加する必要があるデータベースのみを選択し、矢印をクリックして追加し、[次へ]\*をクリックします。



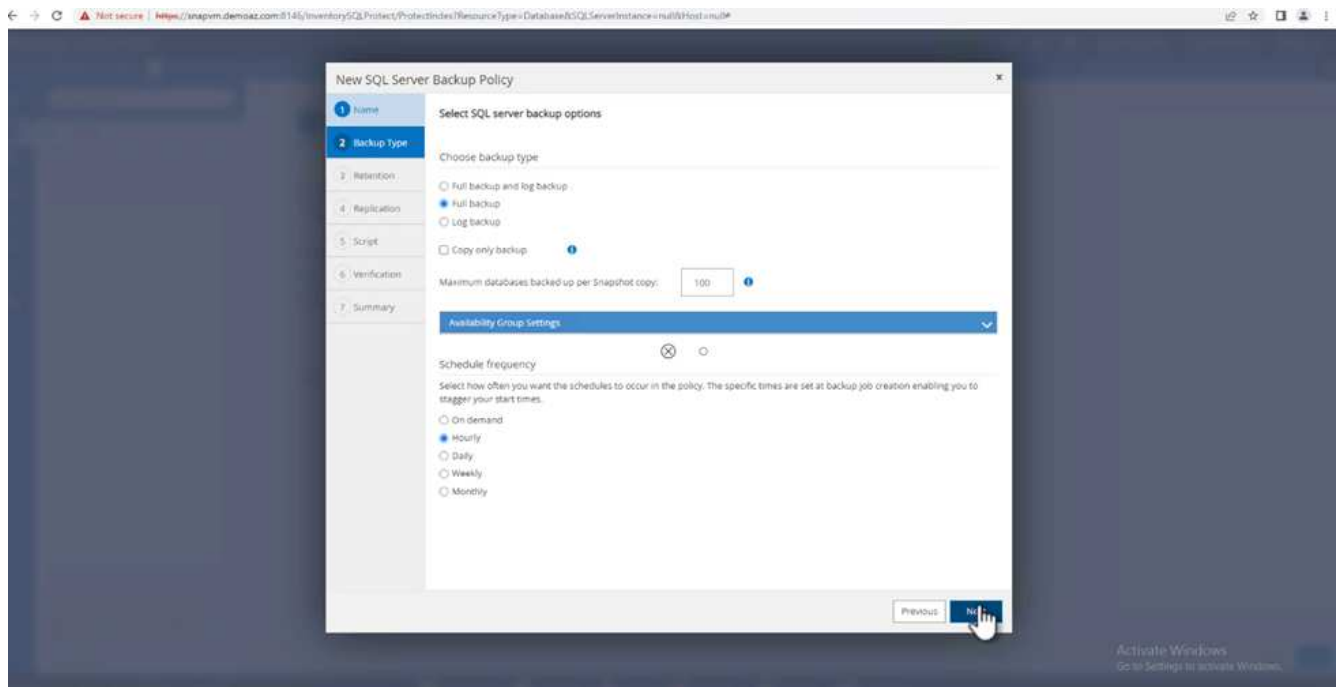
5. ポリシーで、 (+) をクリックします。



6. リソースグループポリシー名を入力します。



7. 会社のSLAに応じて\*[フルバックアップ]\*とスケジュール頻度を選択します。



8. 保持設定を行います。

New SQL Server Backup Policy x

- 1 Name
- 2 Backup Type
- 3 Retention**
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

### Retention settings

Retention settings for up-to-the-minute restore operation ⓘ

Keep log backups applicable to last  full backups

Keep log backups applicable to last  days

### Full backup retention settings ⓘ

Weekly

Total Snapshot copies to keep

Keep Snapshot copies for  days

9. レプリケーションオプションを設定します。

New SQL Server Backup Policy x

**1** Name

**2** Backup Type

**3** Retention

**4** Replication

**5** Script

**6** Verification

**7** Summary

**Select secondary replication options** ⓘ

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label: Choose ⓘ

Error retry count: 3 ⓘ

[Previous](#) [Next](#)

10. バックアップの実行前に実行するスクリプトを設定します。「\* 次へ \*」をクリックします。

New SQL Server Backup Policy x

- Name
- Backup Type
- Retention
- Replication
- Script**
- Verification
- Summary

**Specify optional scripts to run before performing a backup job**

Prescript full path

Prescript arguments

**Specify optional scripts to run after performing a backup job**

Postscript full path

Postscript arguments

Script timeout  secs

11. 次のバックアップスケジュールの検証を確認します。

New SQL Server Backup Policy x

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

**Select the options to run backup verification**

Run verifications for the following backup schedules

---

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

Hourly

---

Database consistency checks options

Limit the integrity structure to physical structure of the database (PHYSICAL\_ONLY)

Suppress all information message (NO\_INFOMSGS)

Display all reported error messages per object (ALL\_ERRORMSG5)

Do not check non-clustered indexes (NOINDEX)

Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK) ⊗ ○

---

Verification script settings i

Script timeout:  SECS

Prescript full path:

Prescript arguments:

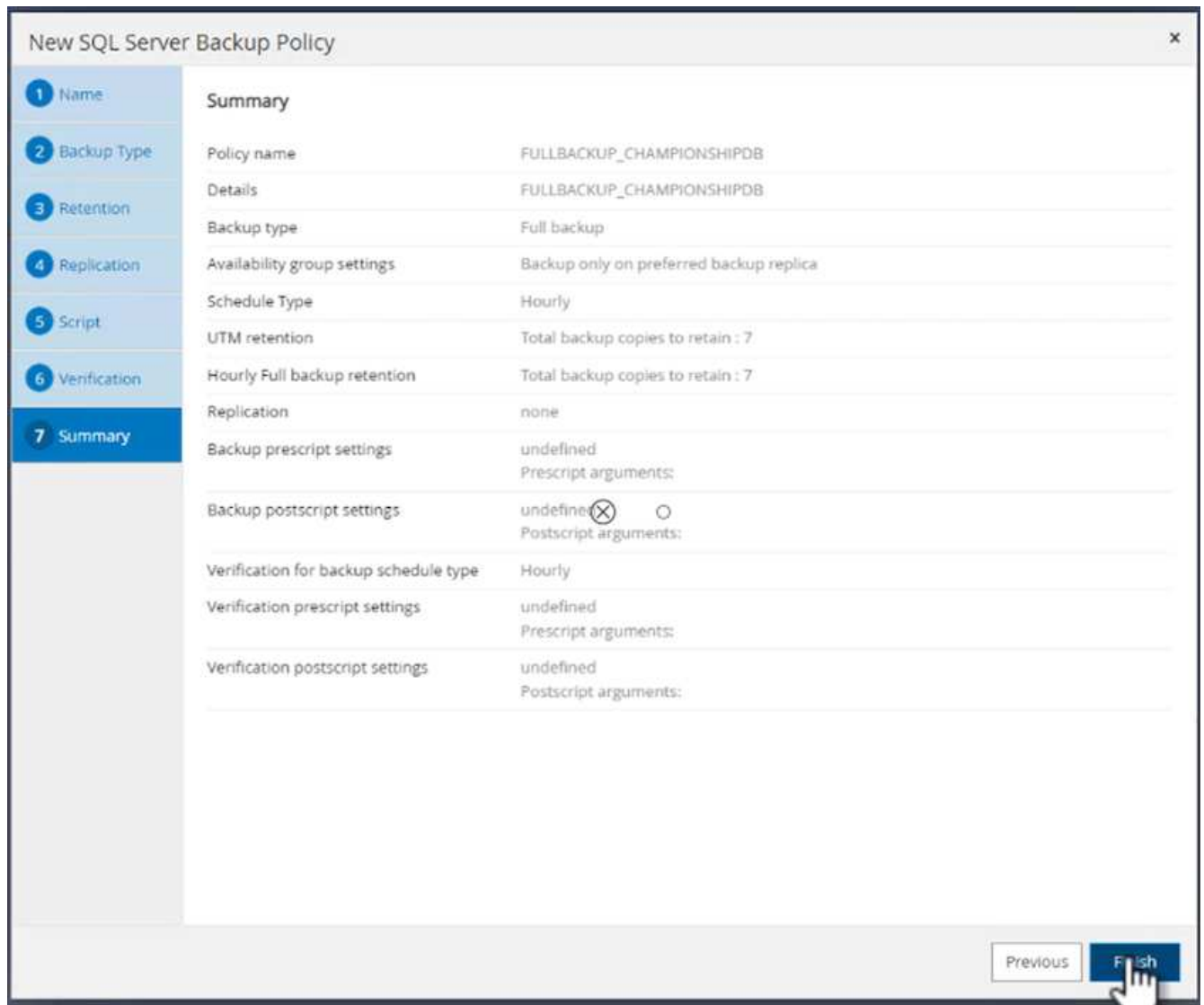
Postscript full path:

Postscript arguments:

Previous Next

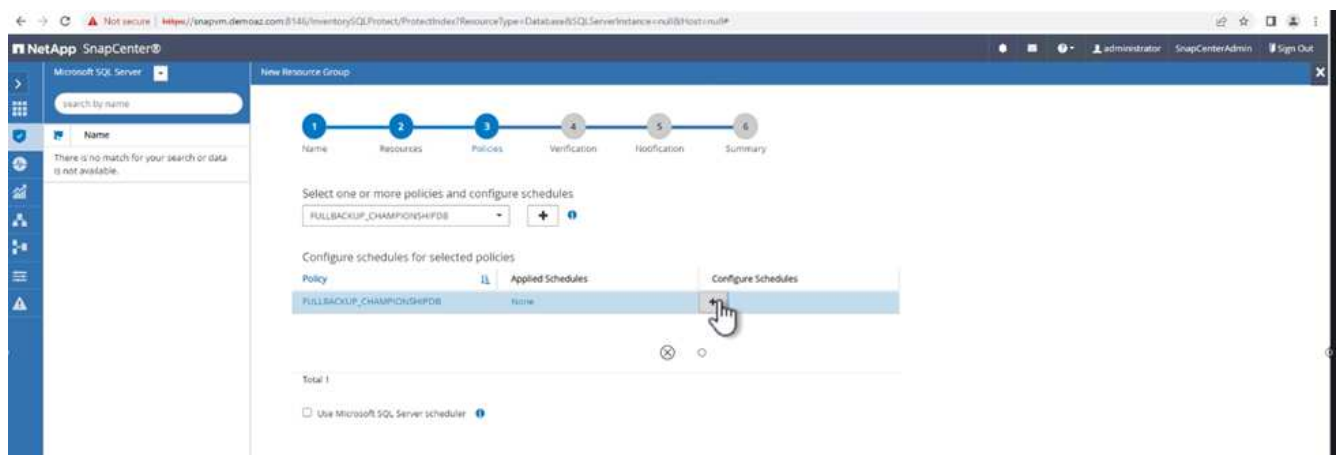
12. [概要]ページで、情報を確認し、\*[完了]\*をクリックします。





## 複数のSQL Serverデータベースを設定して保護します

1. (+) 記号をクリックして、開始日と終了日を設定します。



2. 時刻を設定します。

## Add schedules for policy FULLBACKUP\_CHAMPIONSHIPDB



### Hourly

Start date

11/11/2022 05:30 pm



Expires on

12/11/2022 05:27 pm



Repeat every

1



hours

0

mins



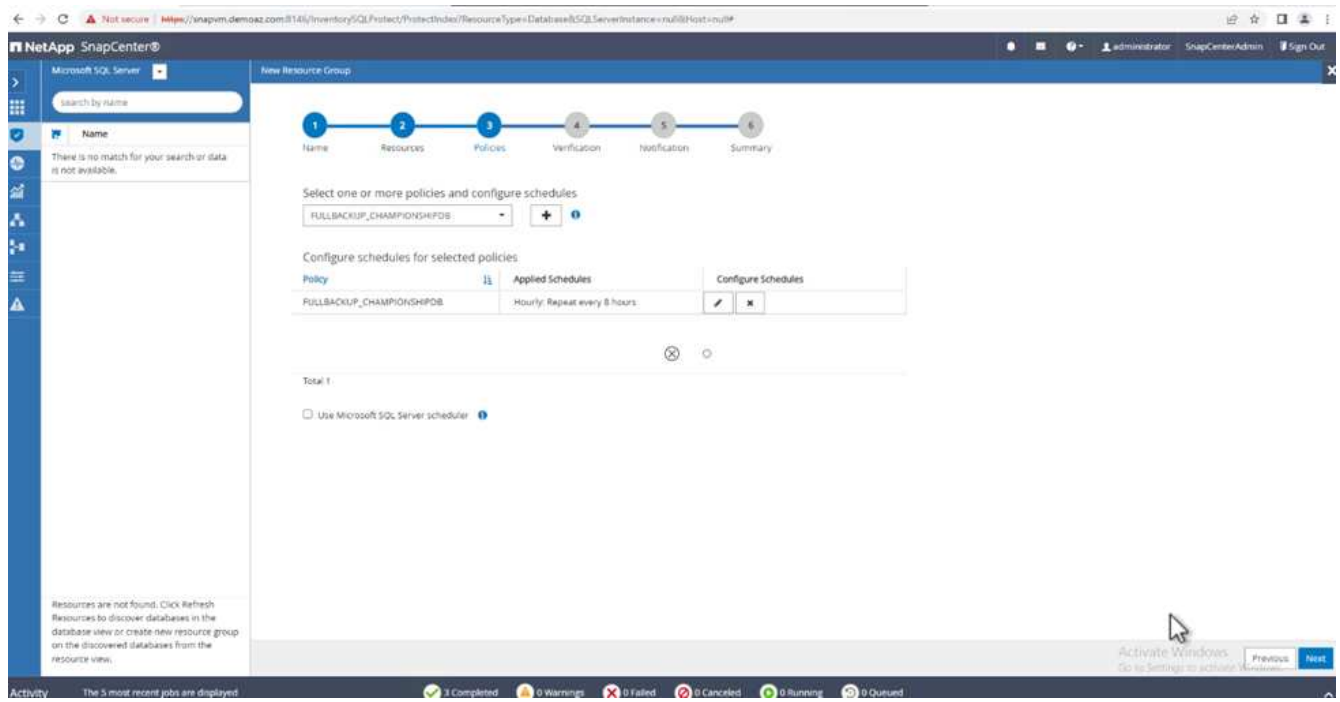
The schedules are triggered in the SnapCenter Server time zone.



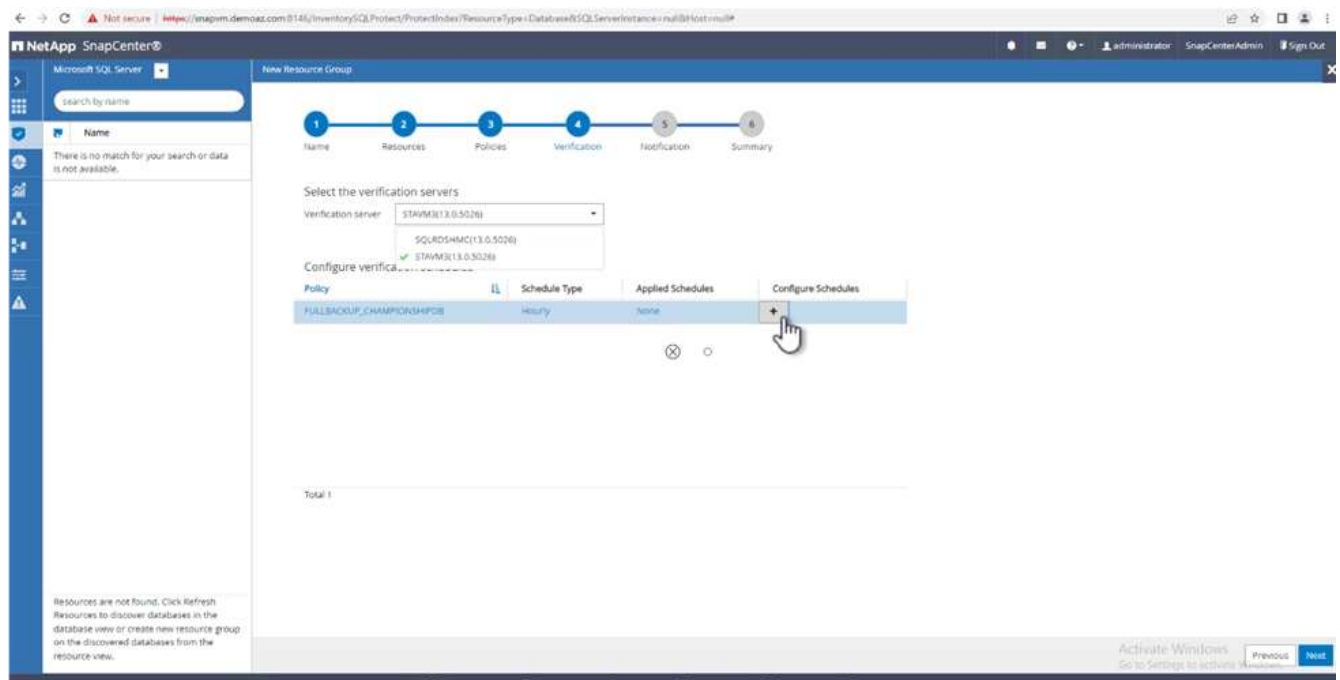
Cancel

OK

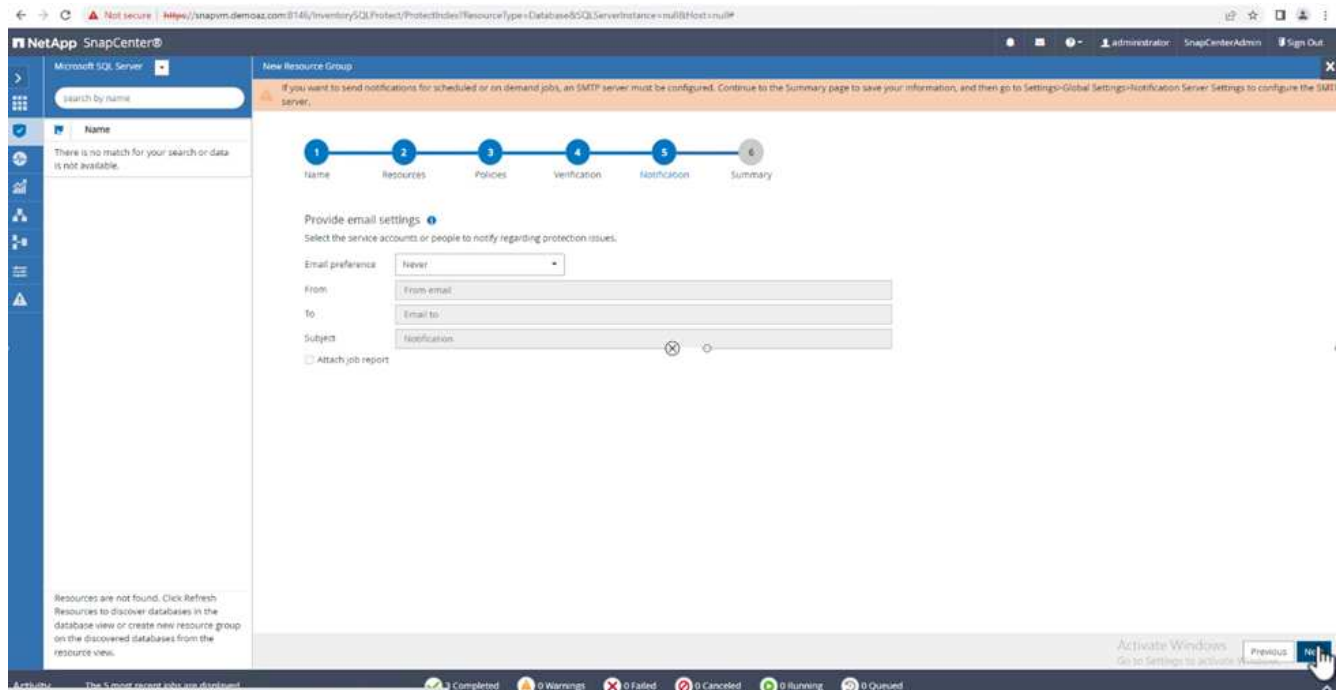




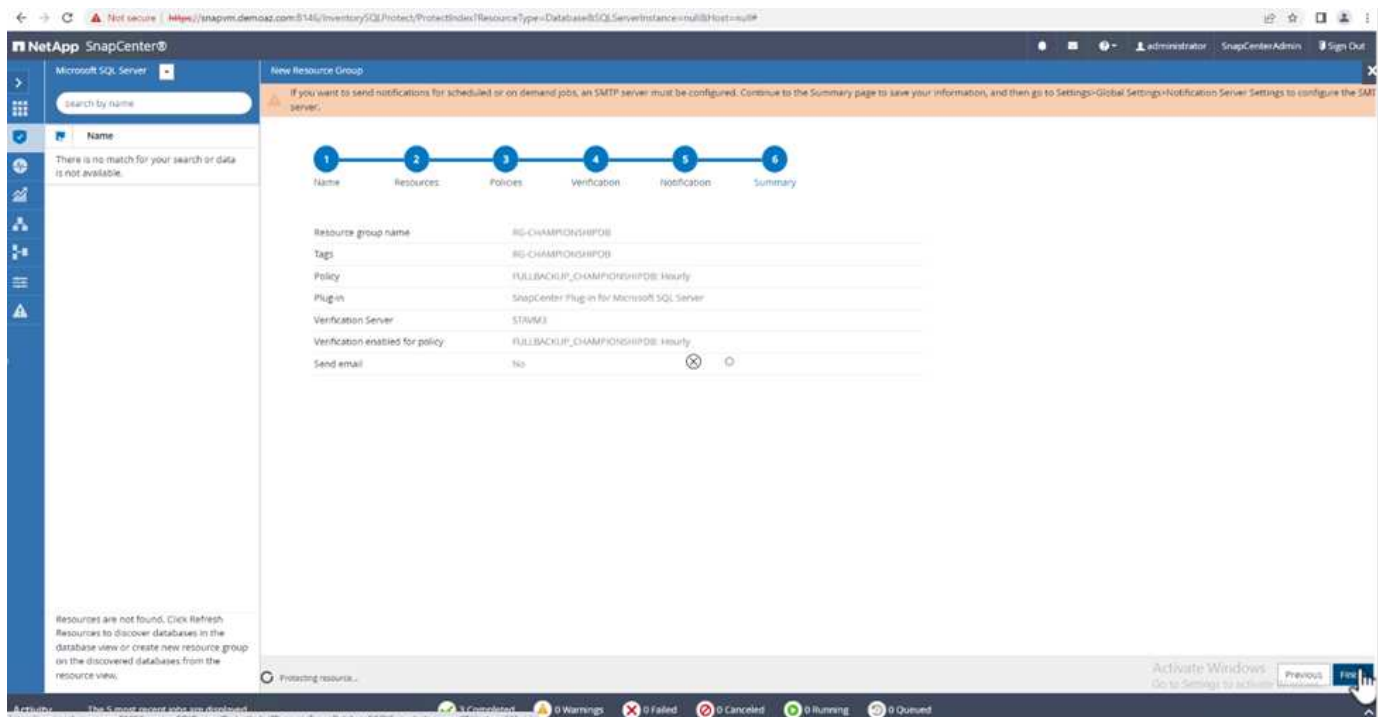
3. [検証]タブで、サーバを選択し、スケジュールを設定して\*[次へ]\*をクリックします。



4. Eメールを送信するように通知を設定します。

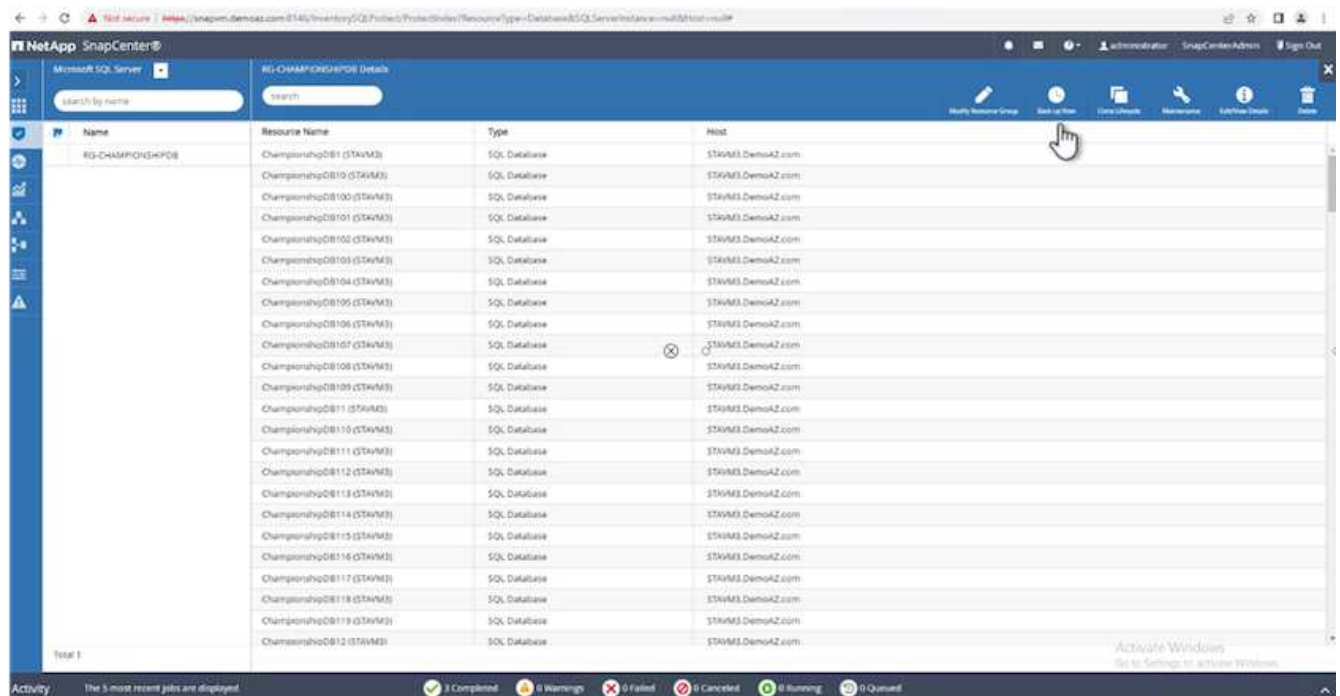


これで、複数のSQL Serverデータベースをバックアップするようにポリシーが設定されました。

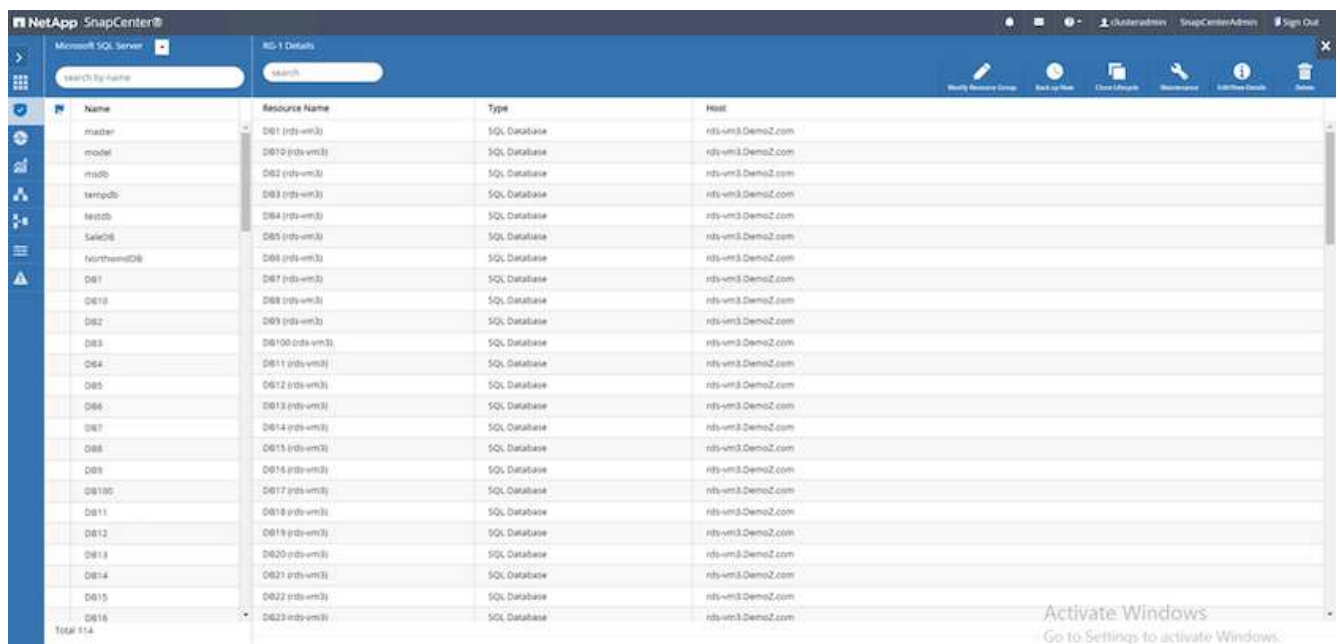


複数の**SQL Server**データベースに対してオンデマンドバックアップを実行します

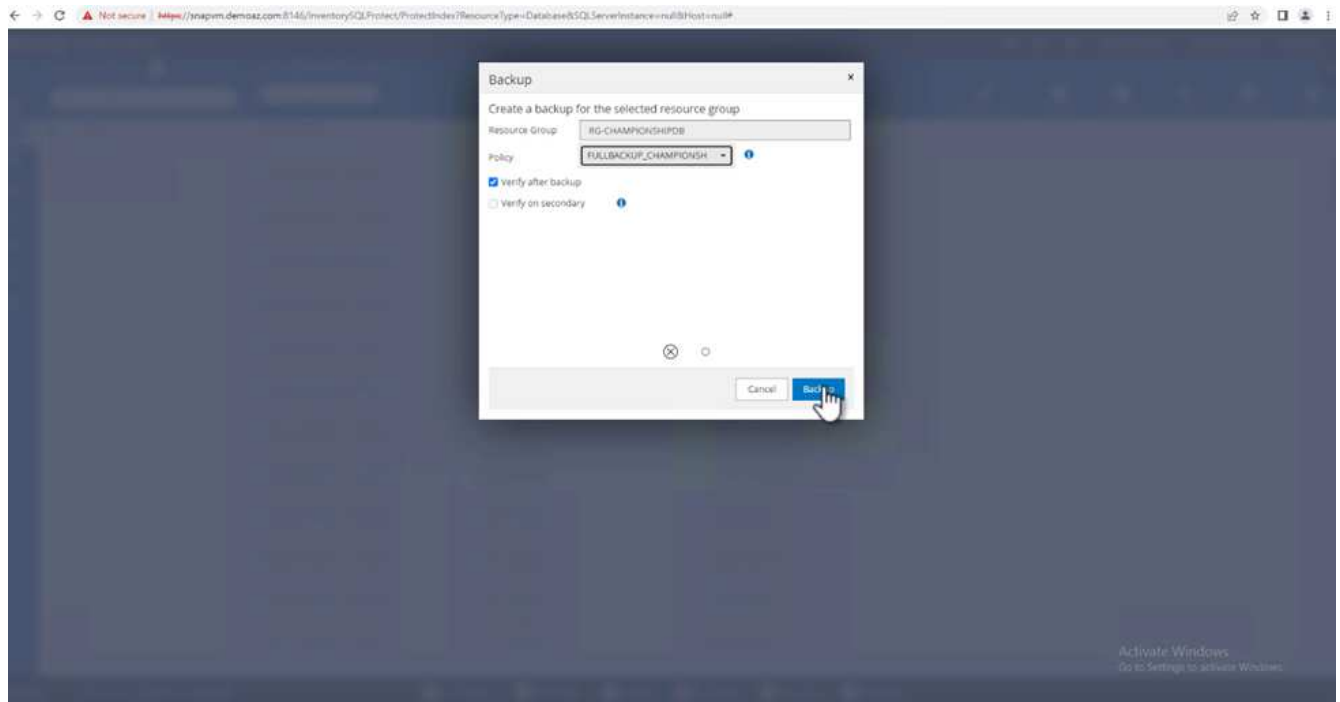
1. [リソース]タブで、[表示]を選択します。ドロップダウンメニューから\*[リソースグループ]\*を選択します。



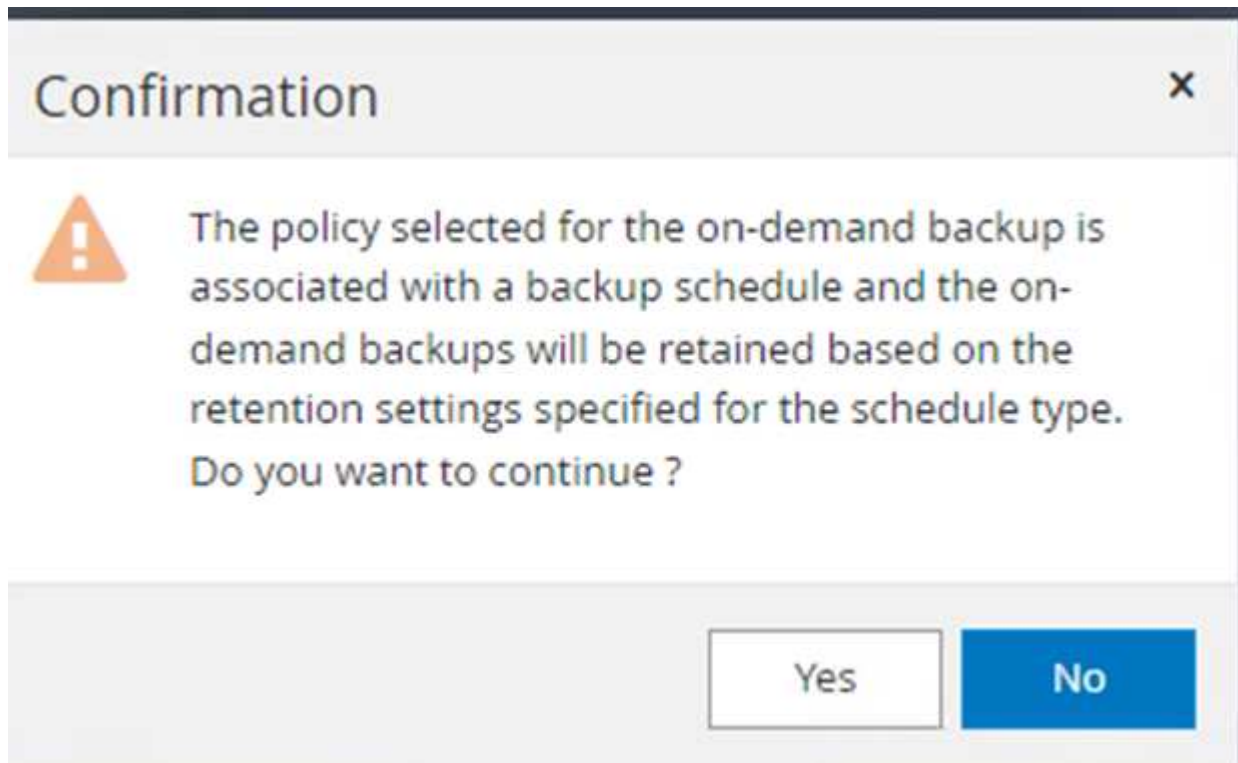
2. リソースグループ名を選択します。
3. 右上の\*[今すぐバックアップ]\*をクリックします。



4. 新しいウィンドウが開きます。[Verify after backup]\*チェックボックスをクリックし、[backup]をクリックします。

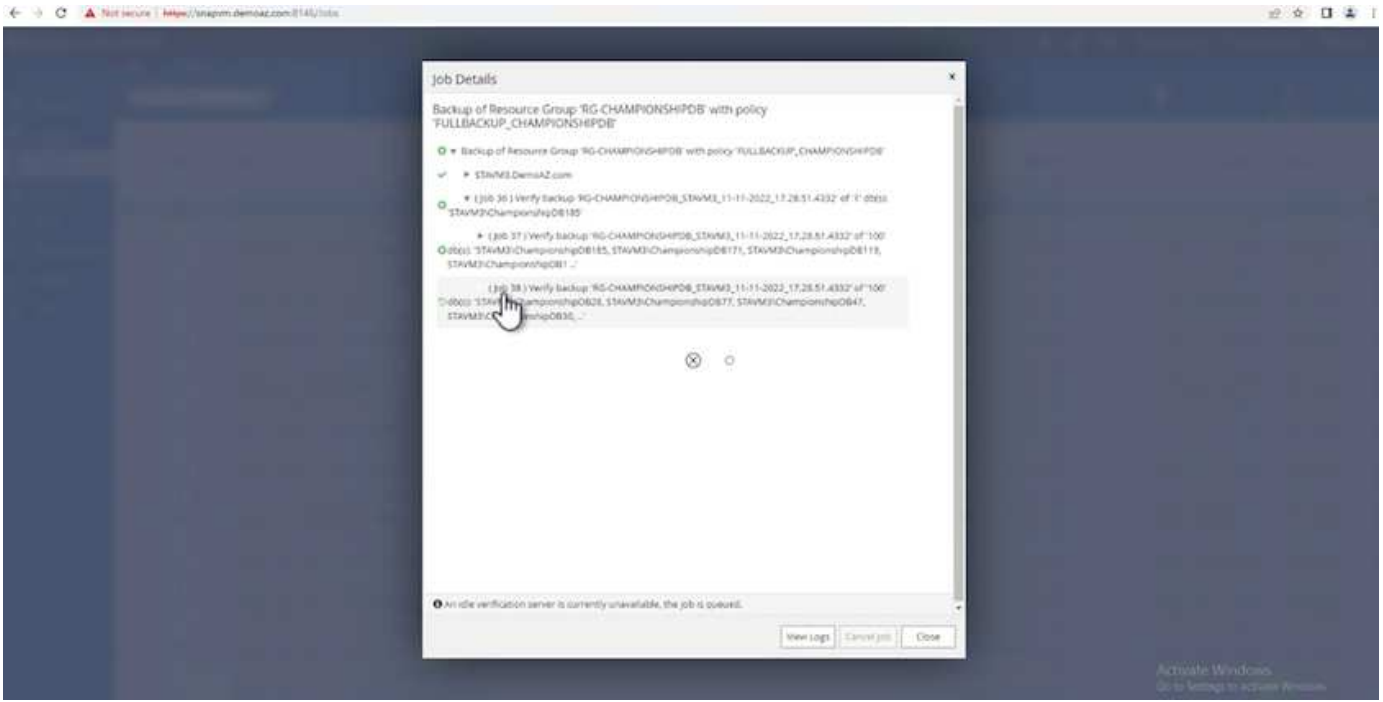


5. 確認メッセージが表示されます。「\*はい\*」をクリックします。

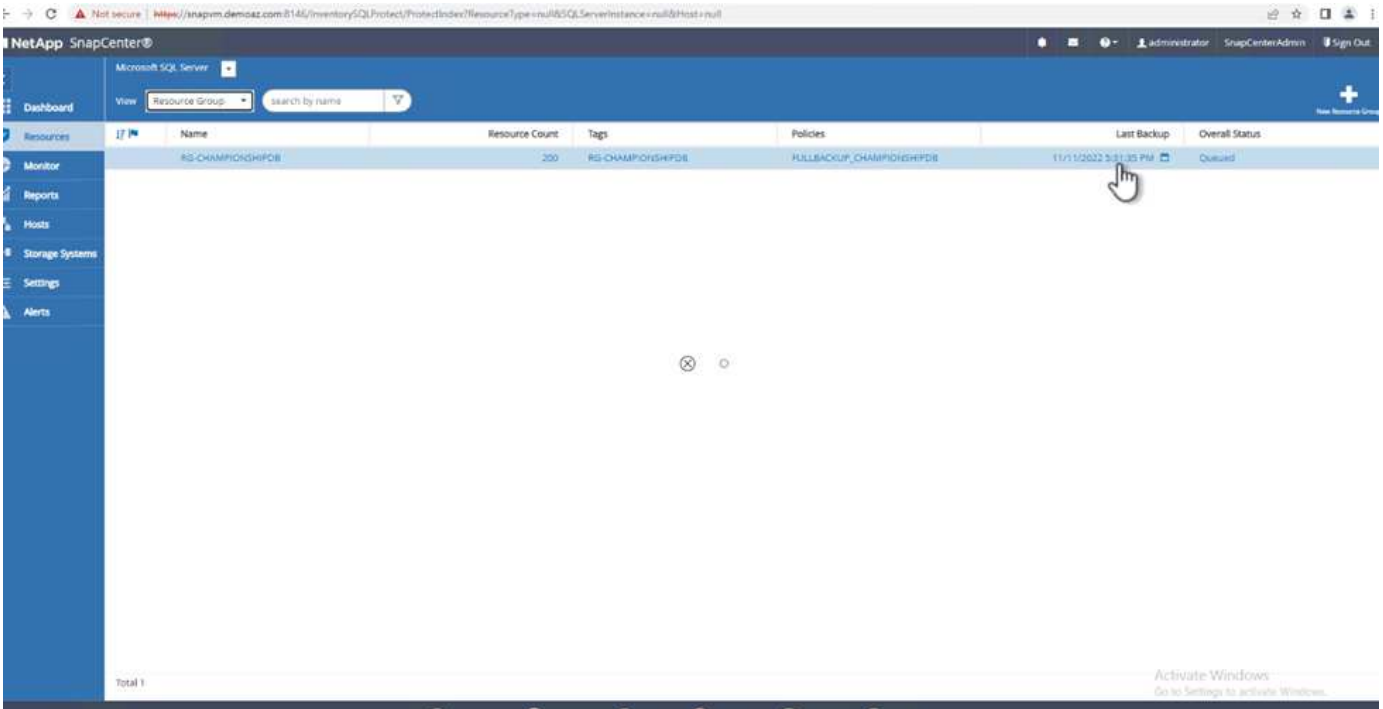


複数データベースのバックアップジョブを監視します

左側のナビゲーションバーで\*をクリックし、バックアップジョブを選択します。[詳細]\*をクリックしてジョブの進捗状況を確認します。



バックアップが完了するまでの時間を確認するには、\*[リソース]\*タブをクリックします。



## 複数データベースバックアップのトランザクションログバックアップ

SnapCenter は、完全復旧モデル、バルクログ復旧モデル、シンプル復旧モデルをサポートしています。簡易リカバリモードでは、トランザクションログバックアップはサポートされません。

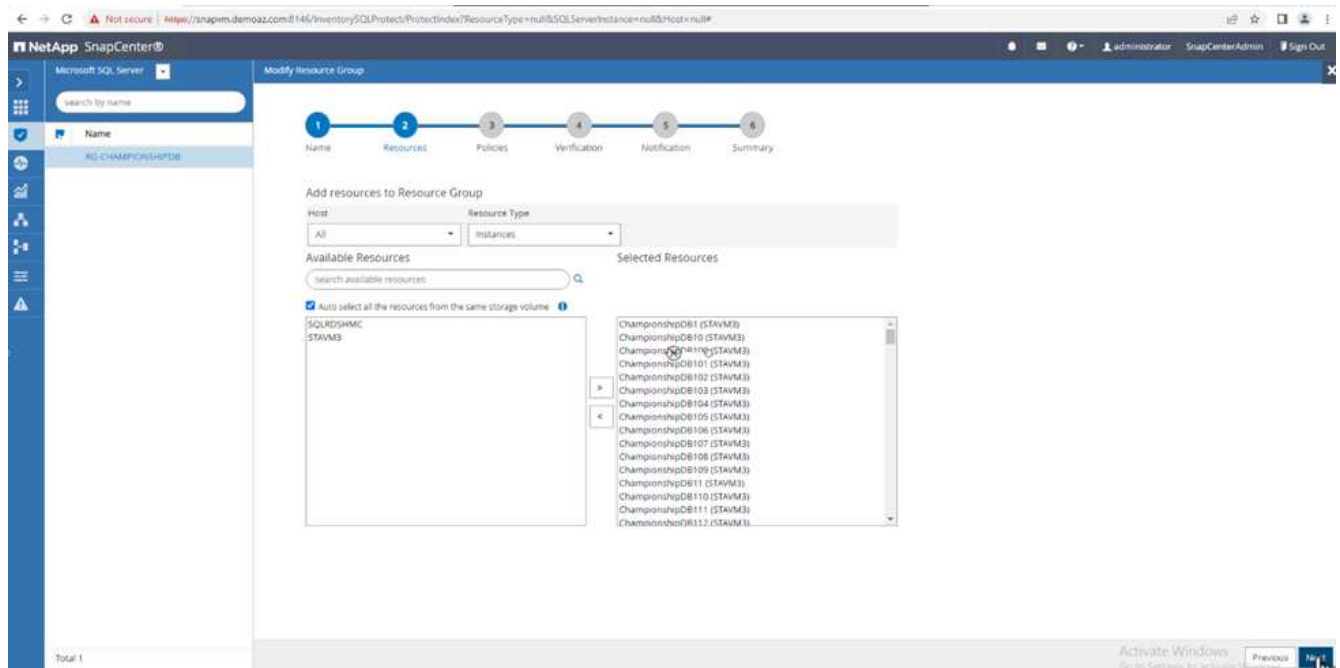
トランザクションログバックアップを実行するには、次の手順を実行します。

1. [リソース]タブで、[表示]メニューを[データベース]から[リソースグループ]に変更します。

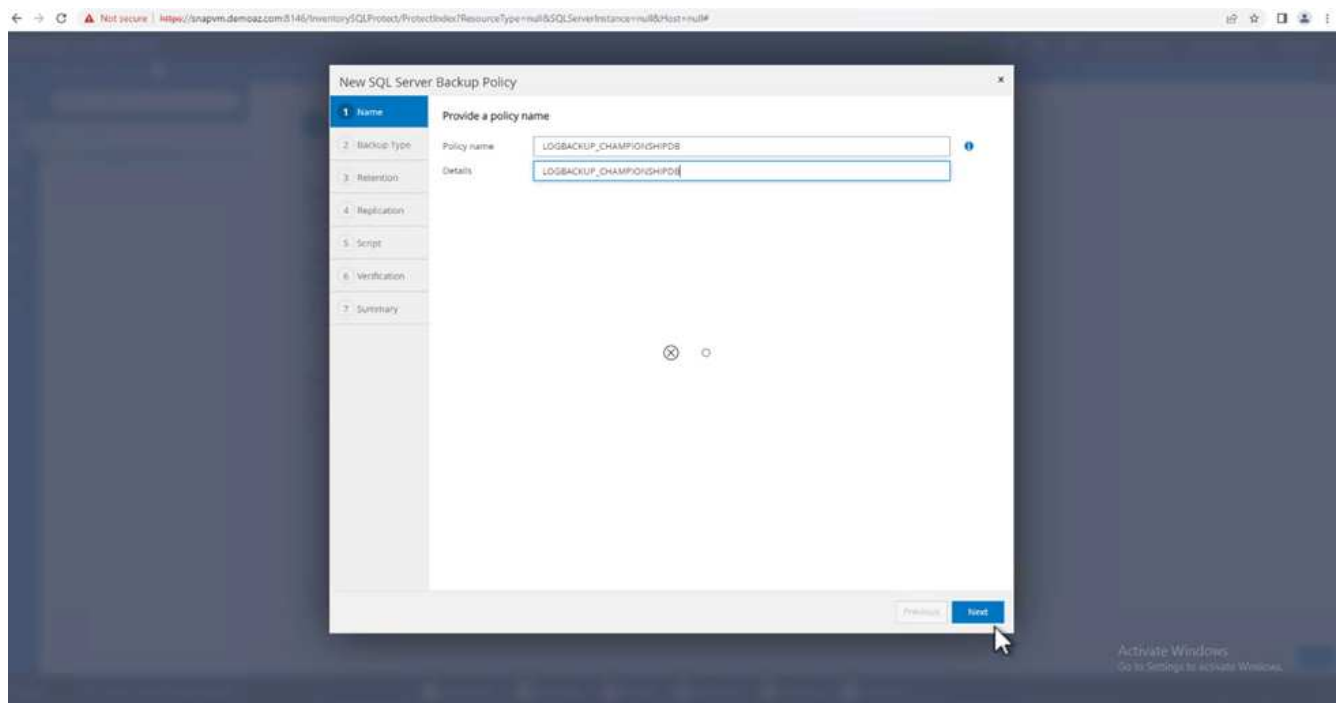








5. ポリシー名を入力します。



6. SQL Serverバックアップオプションを選択します。
7. ログバックアップを選択します。
8. 会社のRTOに基づいてスケジュール頻度を設定します。「\*次へ\*」をクリックします。

New SQL Server Backup Policy ×

**1** Name

**2** Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

### Select SQL server backup options

Choose backup type

Full backup and log backup

Full backup

Log backup

Copy only backup i

Maximum databases backed up per Snapshot copy:  i

Availability Group Settings ▼

### Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

On demand

Hourly

Daily

Weekly

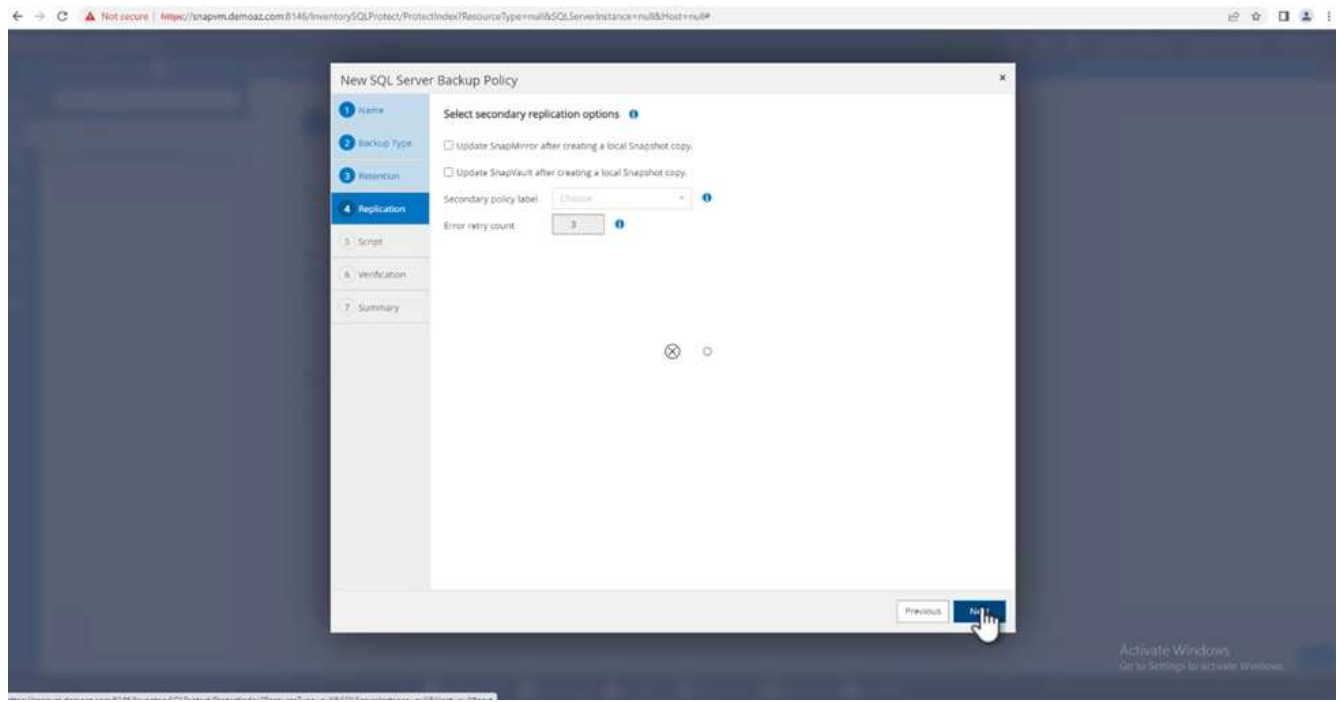
Monthly

9. ログバックアップの保持設定を行います。「\* 次へ \*」をクリックします。

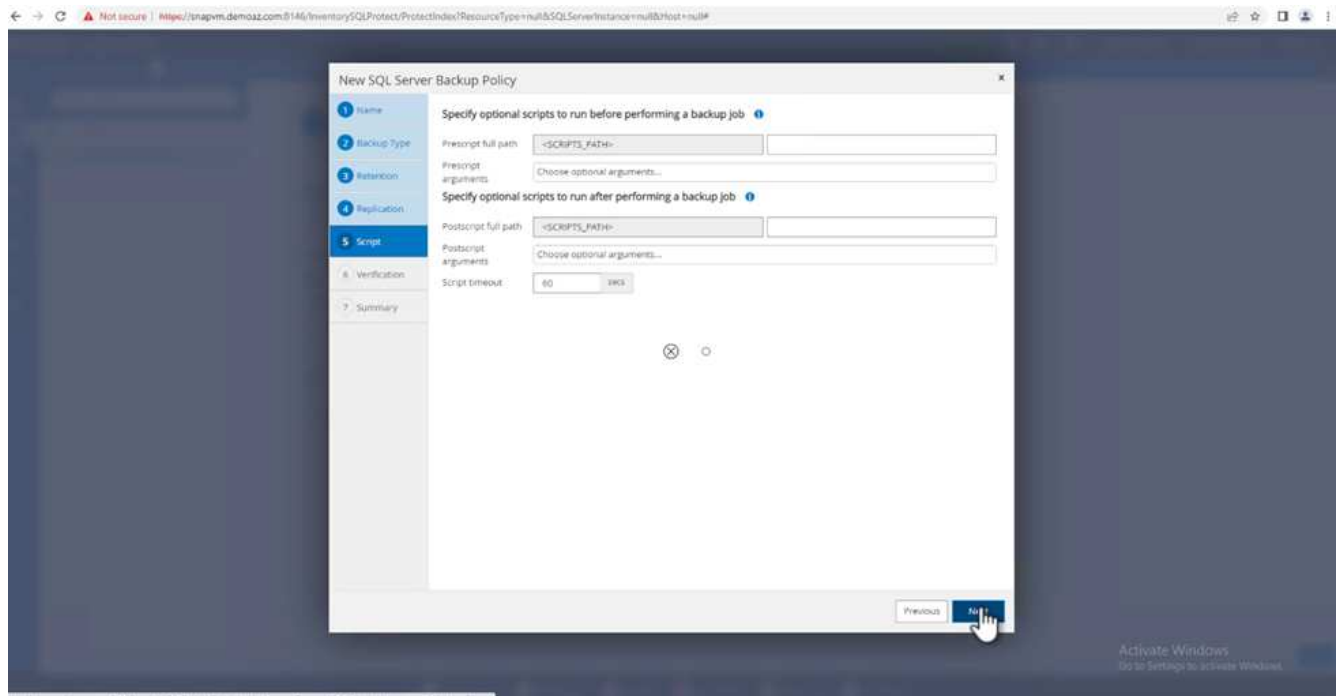
1 Name	<b>Log backup retention settings</b>  Up-to-the-minute (UTM) retention settings retains log backups created as part of full backup and full and log backup operations. UTM retention settings also decides for how many full backups the log backups are to be retained. For example, if UTM retention settings is configured to retain log backups of the last 5 full backups, then the log backups of the last 5 full backups are retained and the rest are deleted.
2 Backup Type	
<b>3 Retention</b>	
4 Replication	
5 Script	
6 Verification	
7 Summary	

Previous Next

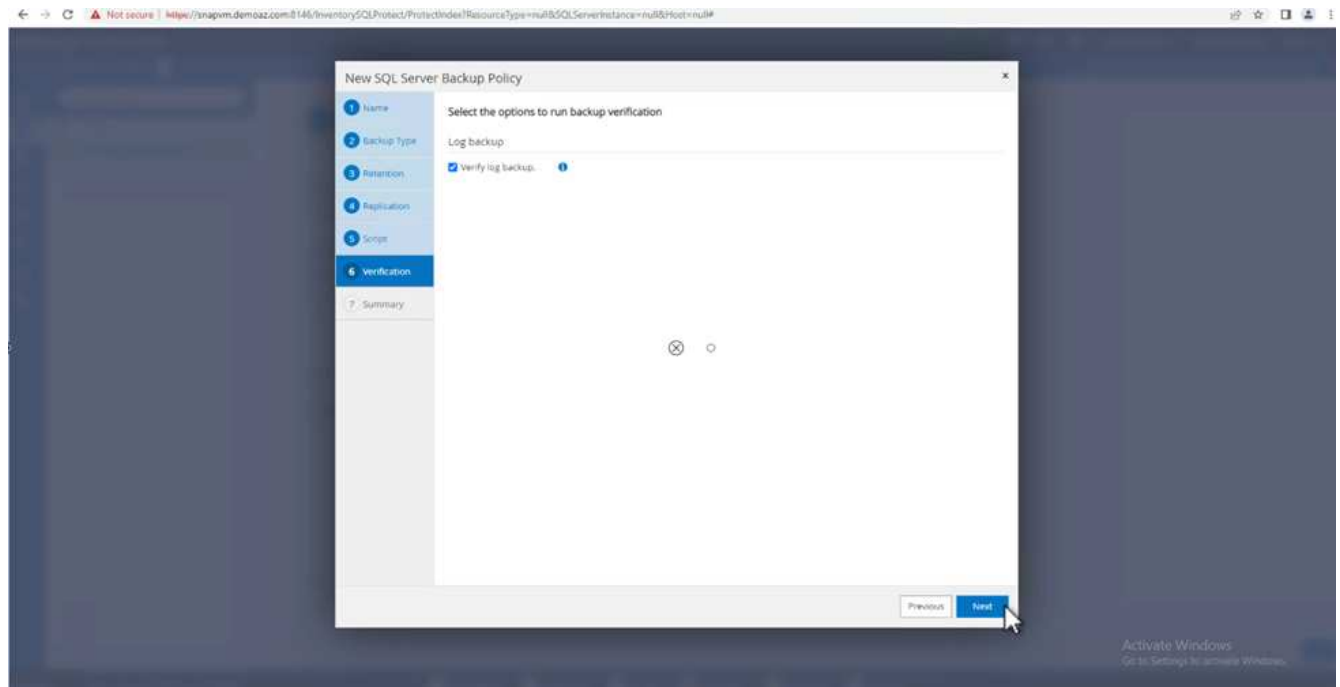
10. (オプション) レプリケーションオプションを設定します。



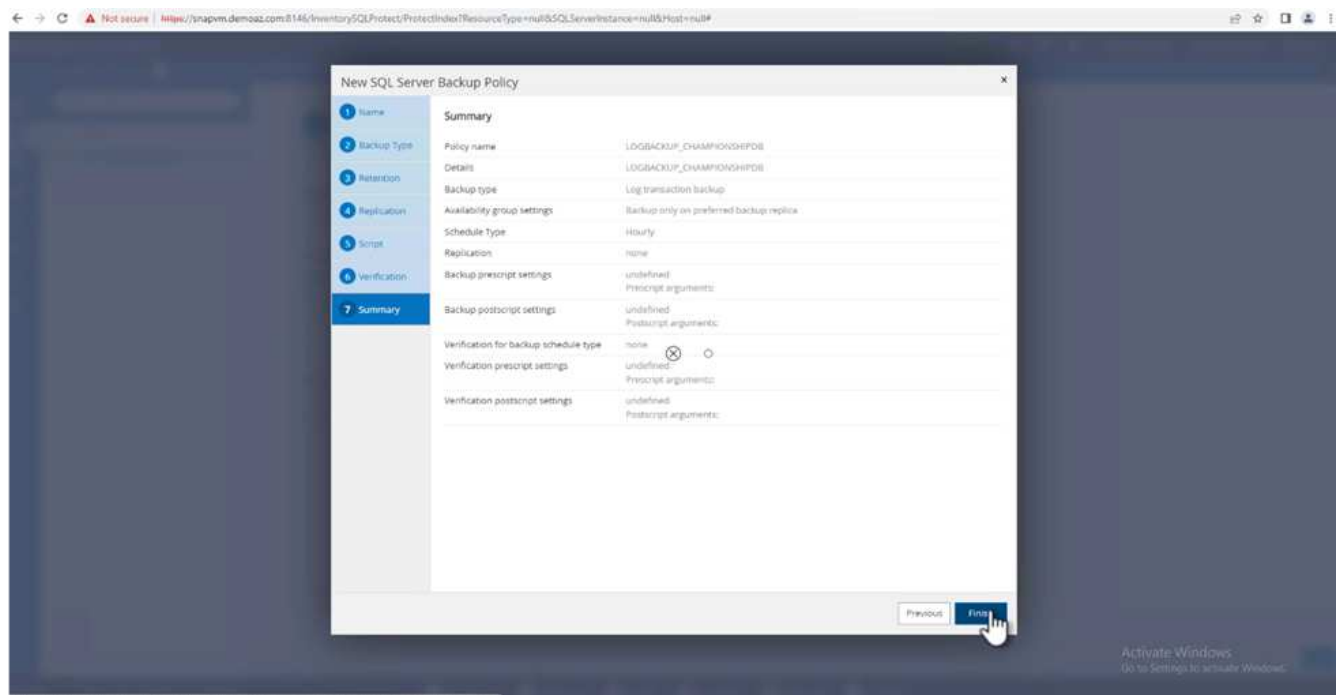
11. (オプション) バックアップジョブの実行前に実行するスクリプトを設定します。



12. (任意) バックアップ検証を設定します。

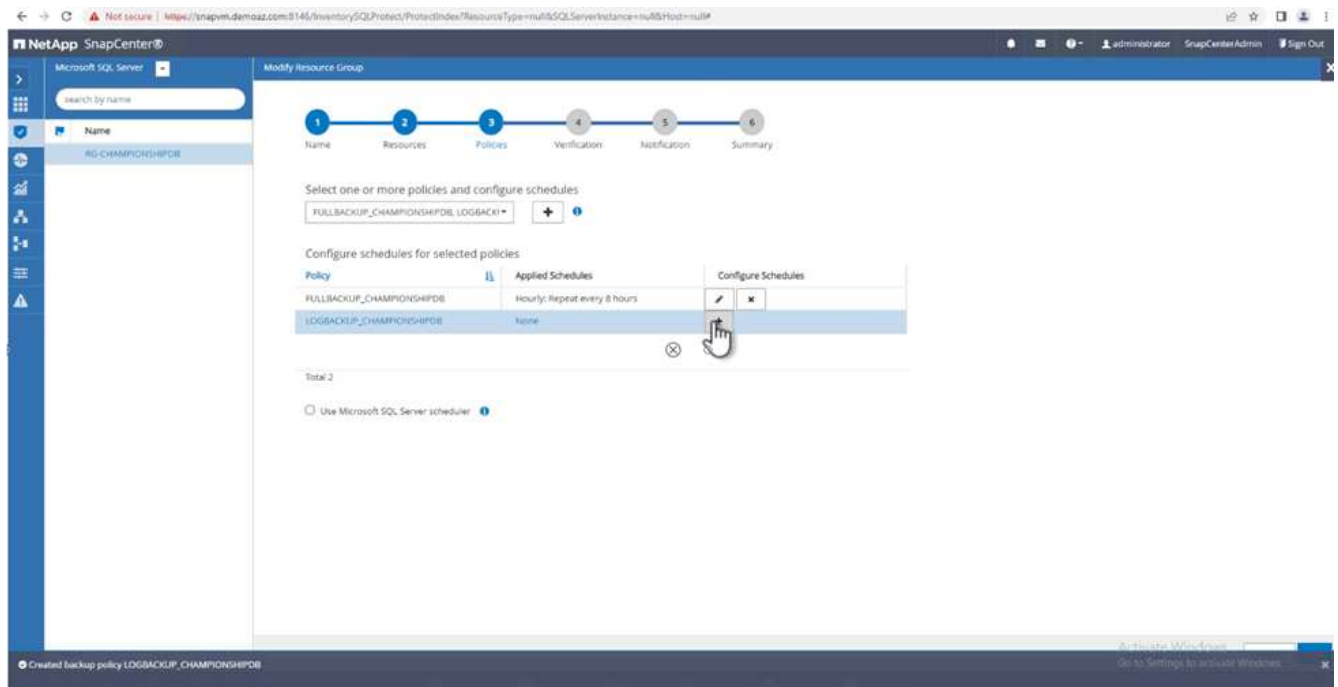


13. [概要]ページで、\*[完了]\*をクリックします。

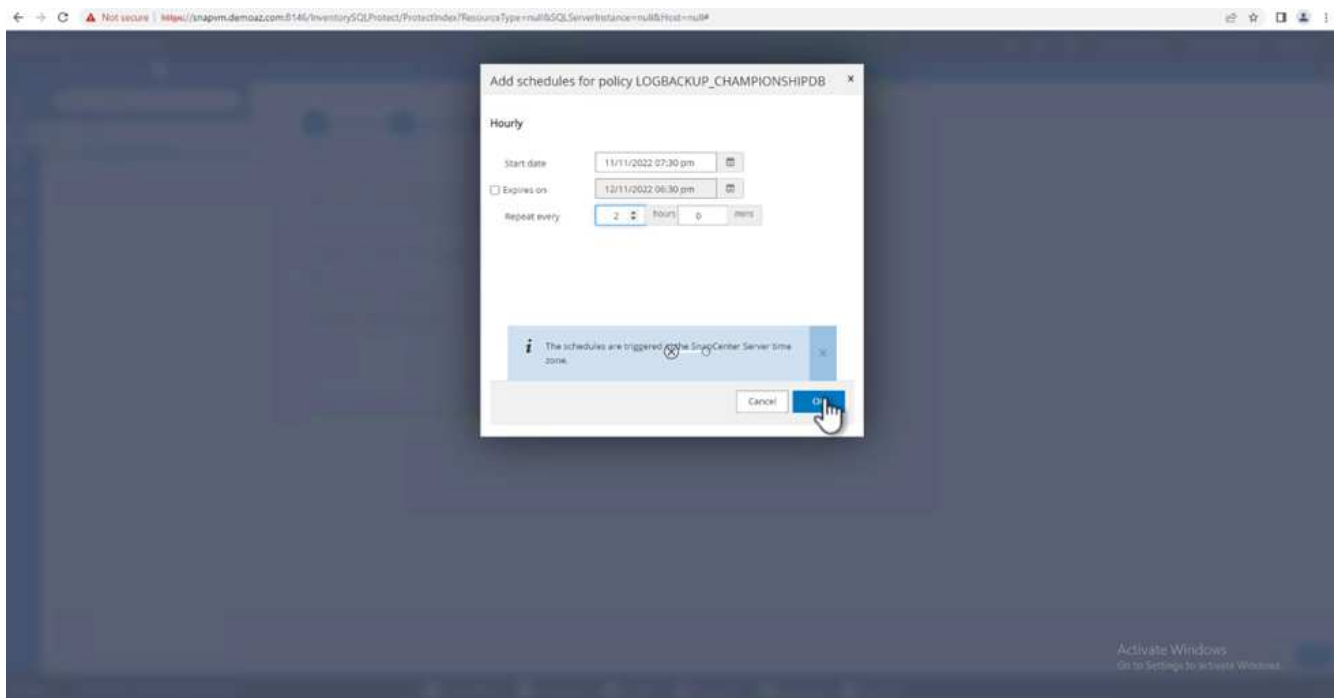


## 複数のMSSQL Serverデータベースを設定して保護します

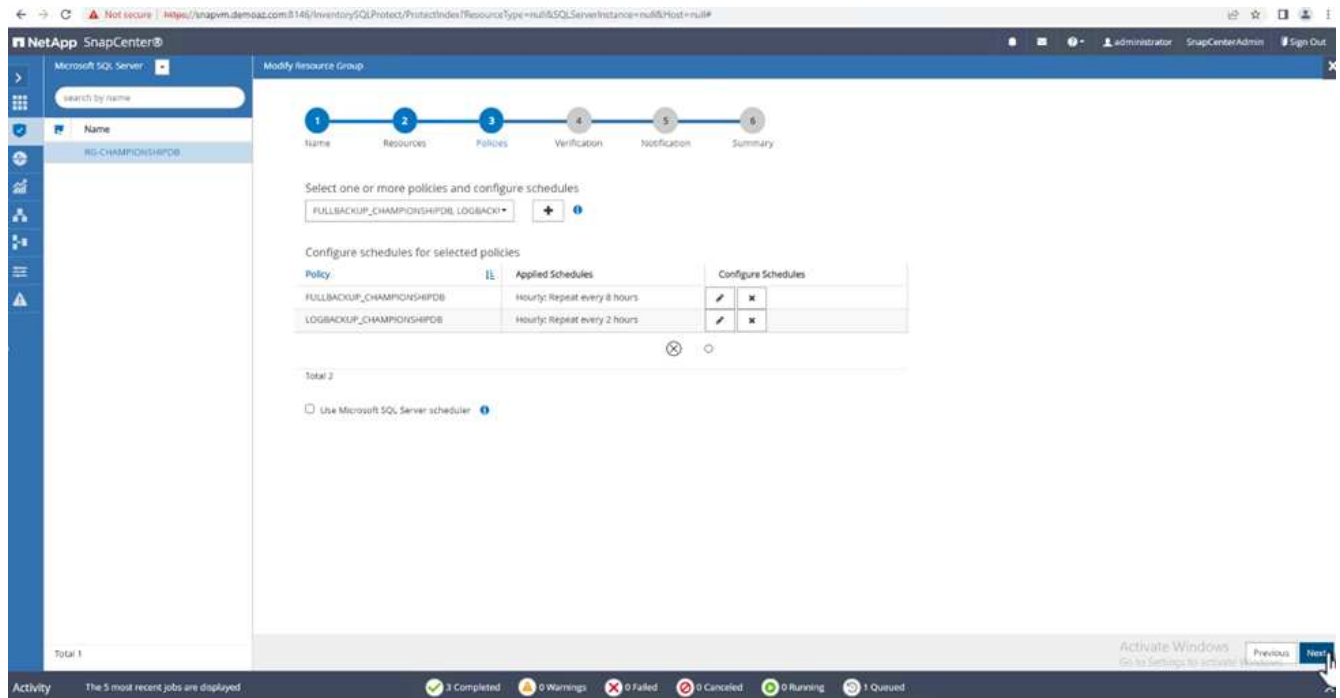
1. 新しく作成したトランザクションログバックアップポリシーをクリックします。



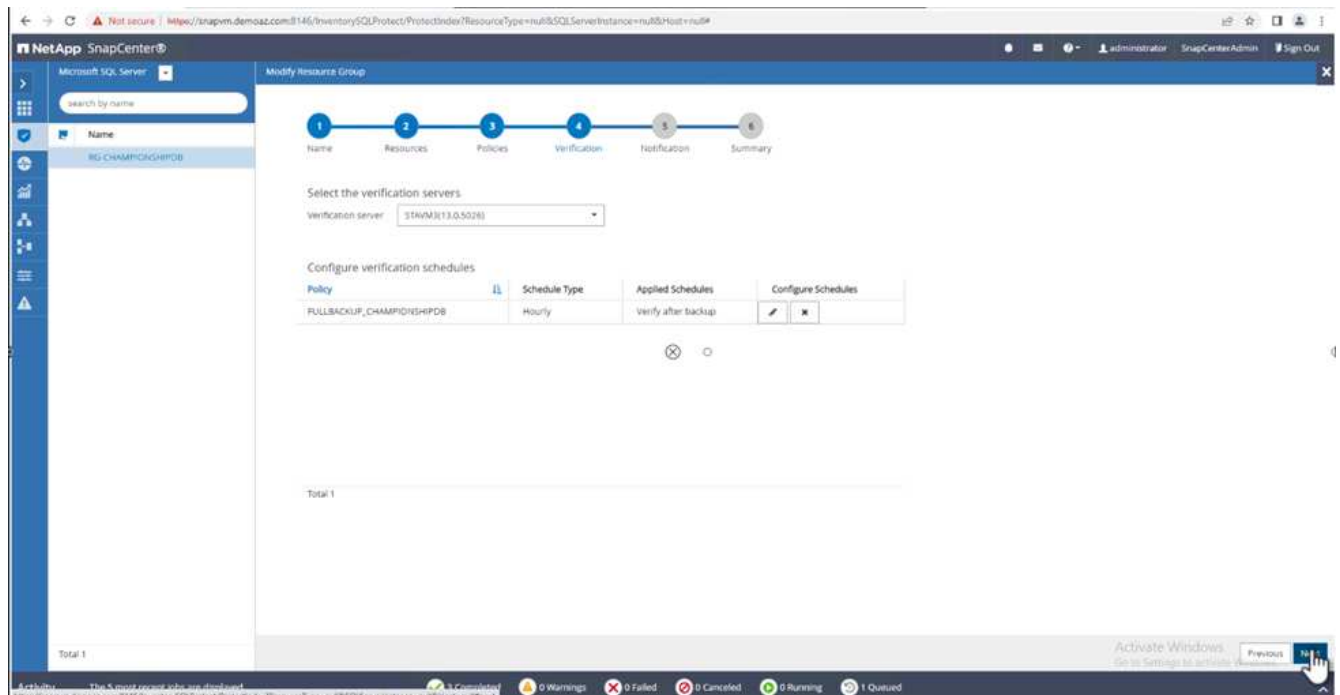
2. \*開始日\*と\*有効期限\*日付を設定します。
3. SLA、RTP、およびRPOに応じて、ログバックアップポリシーの頻度を入力します。[OK]をクリックします。



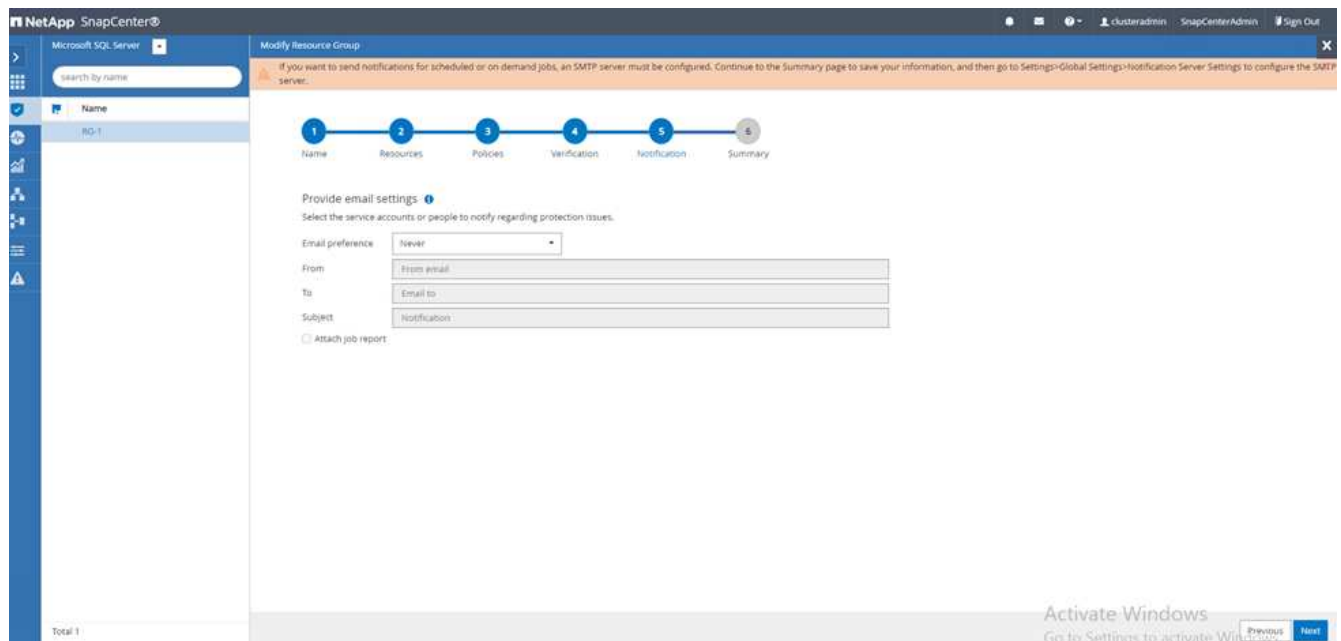
4. 両方のポリシーを表示できます。「\*次へ\*」をクリックします。



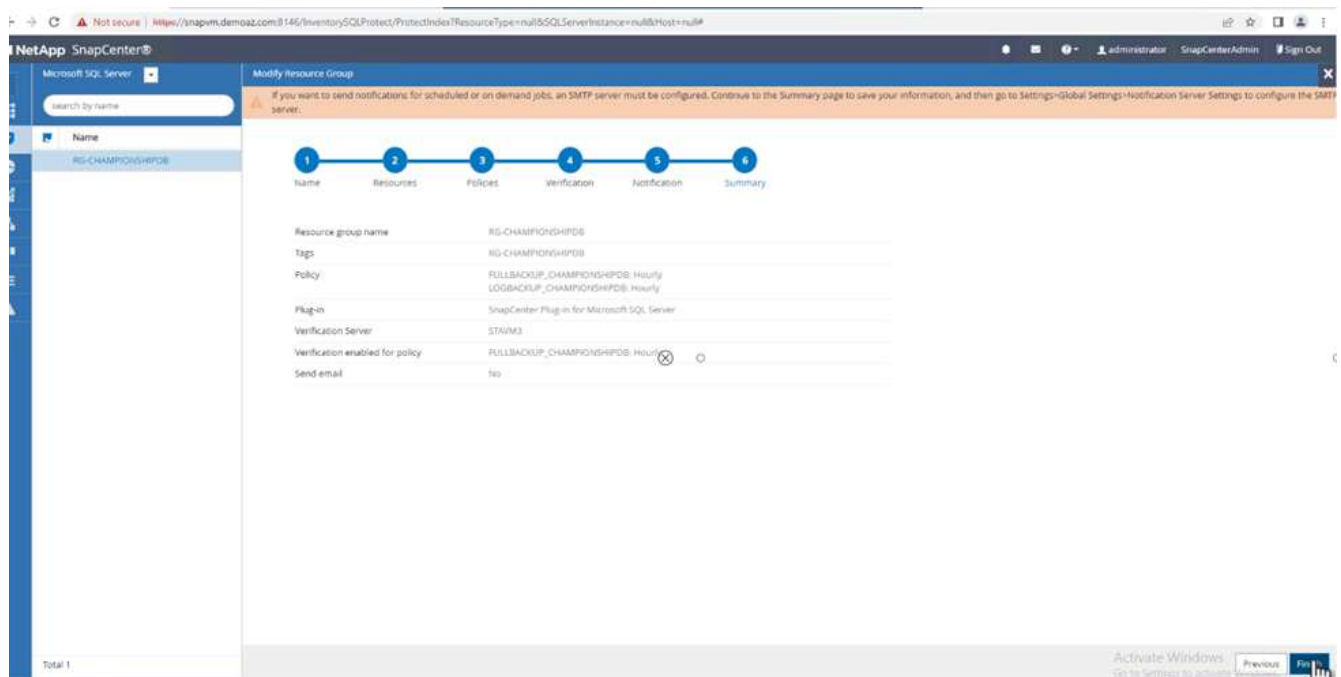
## 5. 検証サーバを設定



## 6. Eメール通知を設定します。



7. [概要]ページで、\*[完了]\*をクリックします。

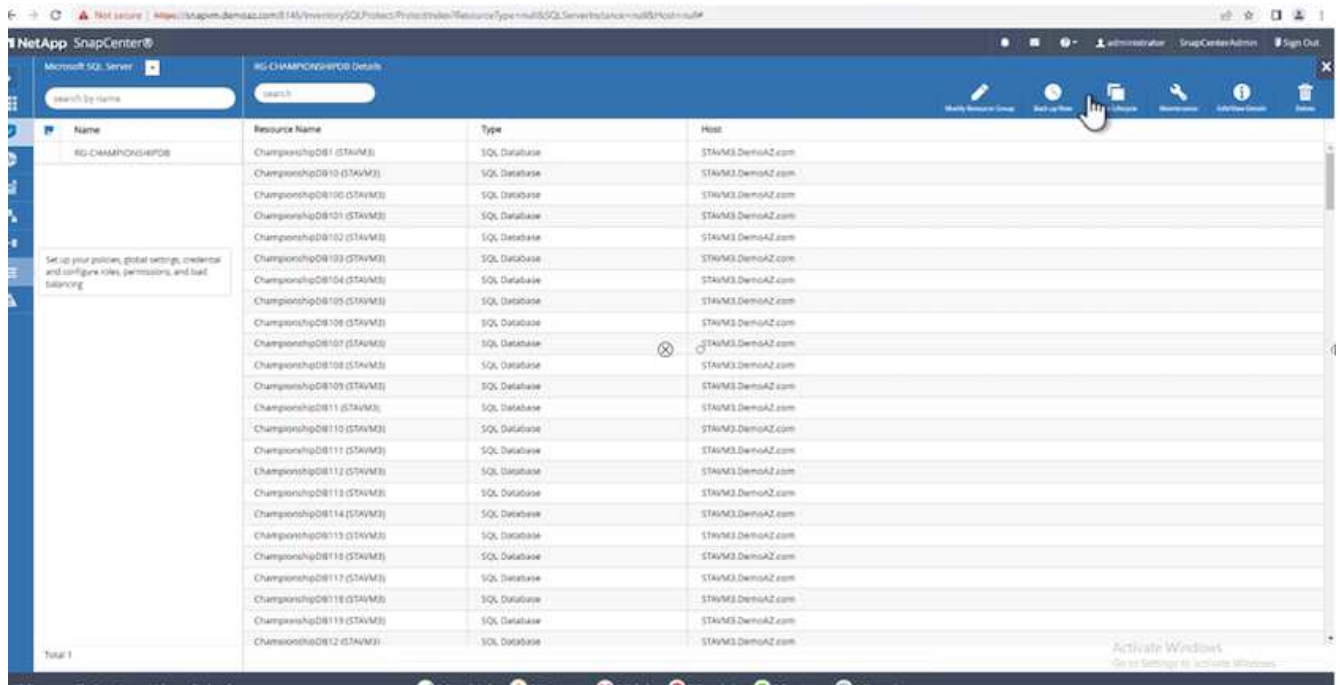


複数のSQL Serverデータベースに対して、オンデマンドのトランザクションログバックアップをトリガーします

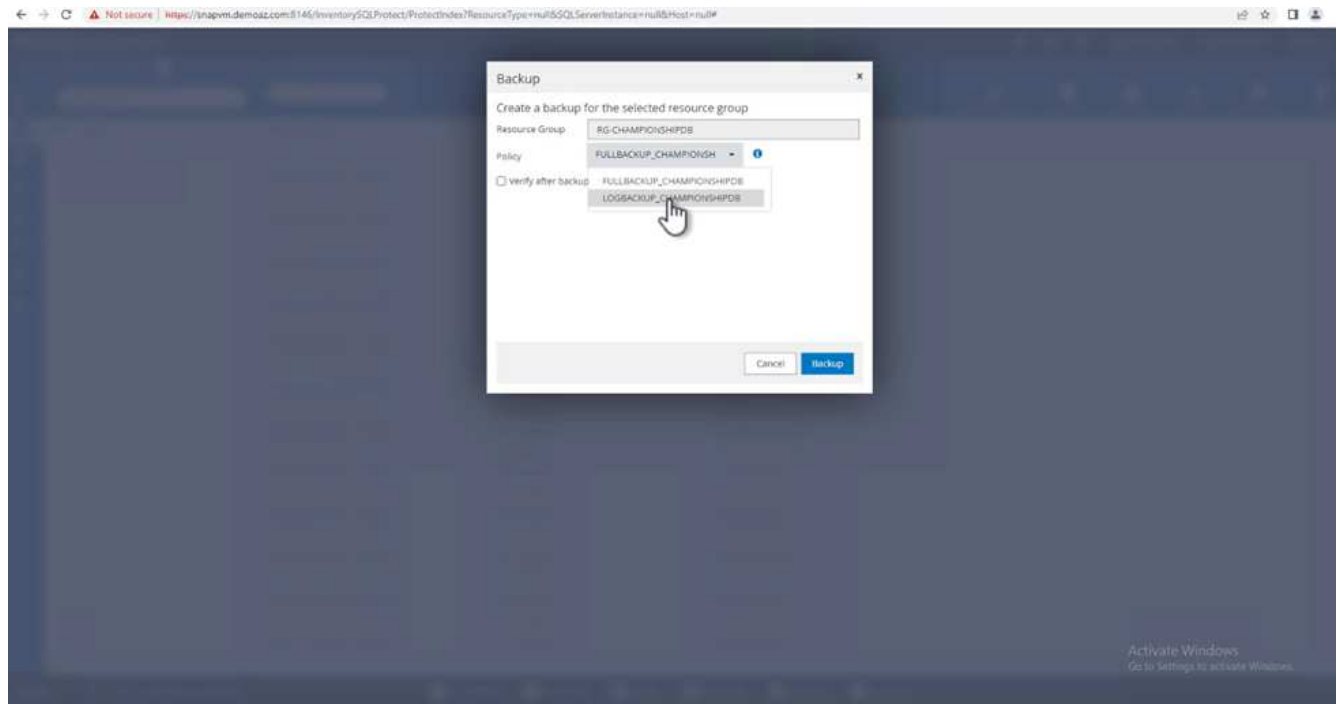
複数のSQL Serverデータベースのトランザクションログのオンデマンドバックアップをトリガーするには、次の手順を実行します。

1. 新しく作成したポリシーページで、ページの右上にある\*[今すぐバックアップ]\*を選択します。

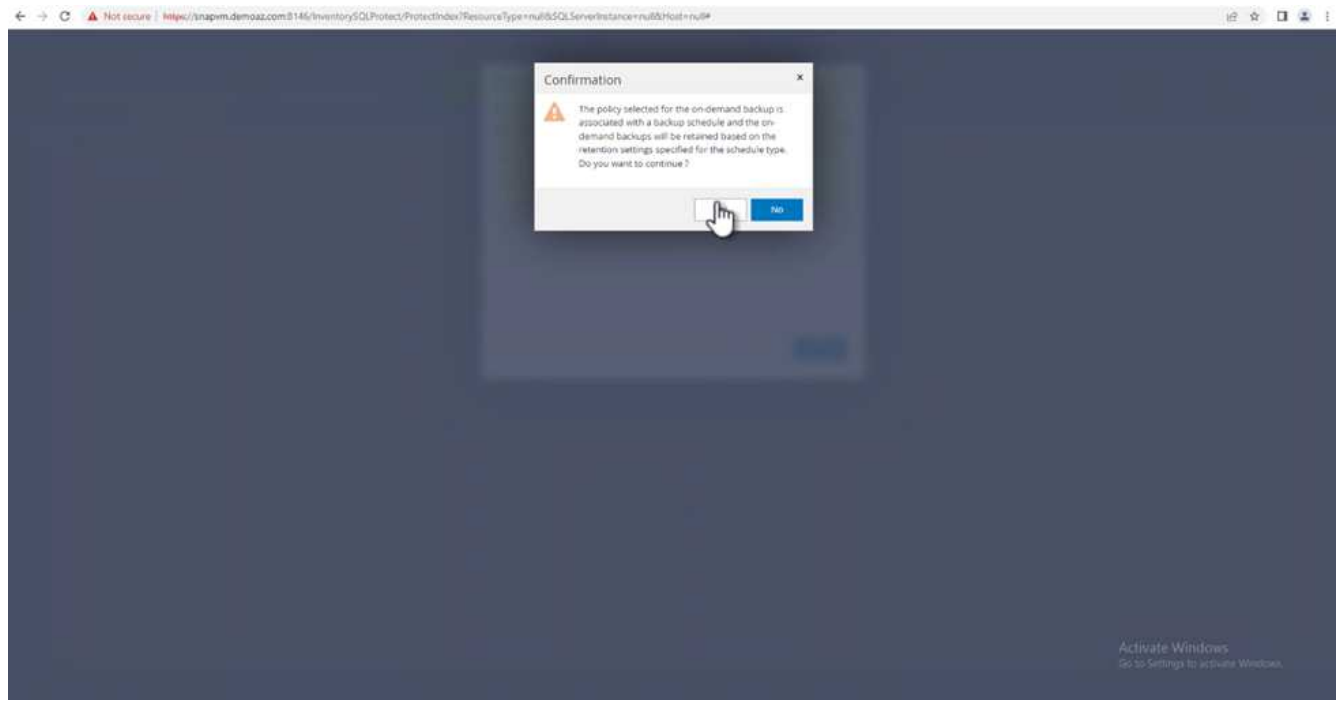




- [ポリシー]\*タブのポップアップで、ドロップダウンメニューからバックアップポリシーを選択し、トランザクションログバックアップを設定します。

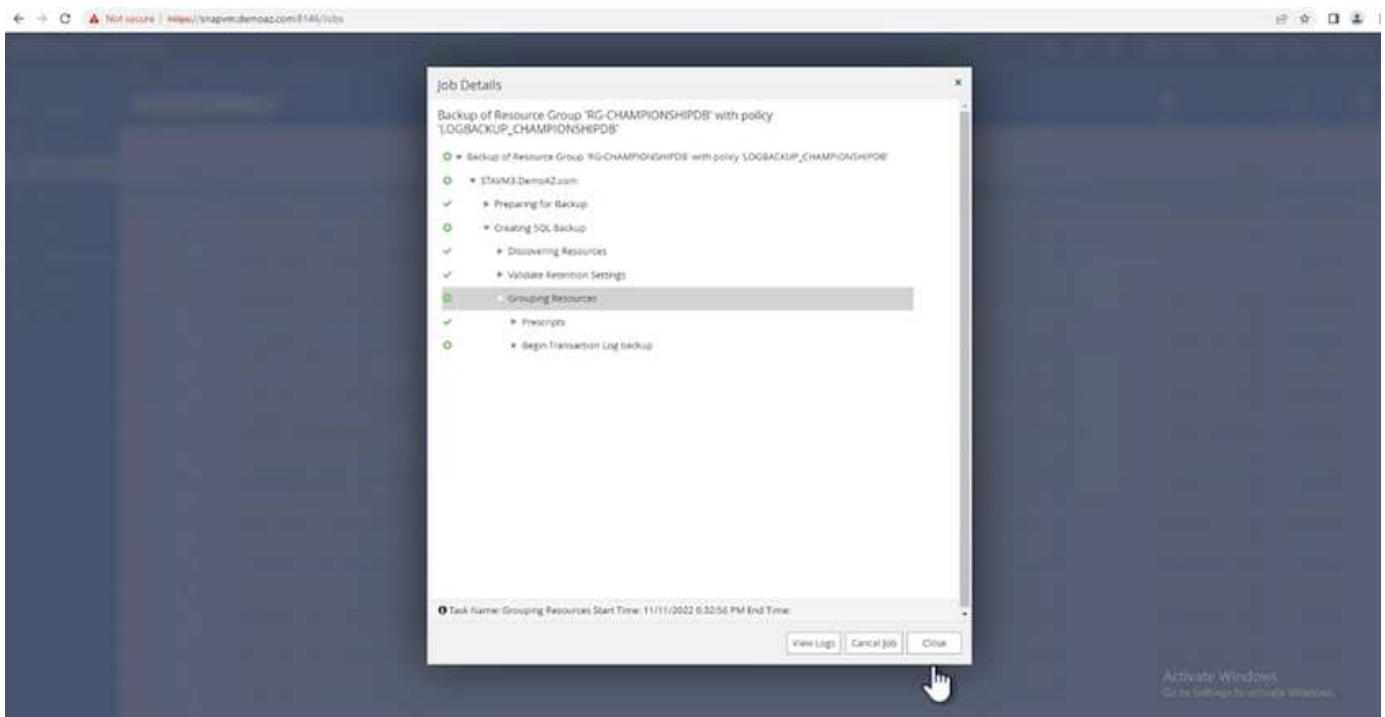


- [バックアップ]をクリックします。新しいウィンドウが表示されます。
- [はい]\*をクリックしてバックアップポリシーを確認します。



## 監視

[監視]\*タブに移動し、バックアップジョブの進捗状況を監視します。



## リストアとリカバリ

SnapCenter でSQL Serverデータベースをリストアするには、次の前提条件を参照してください。

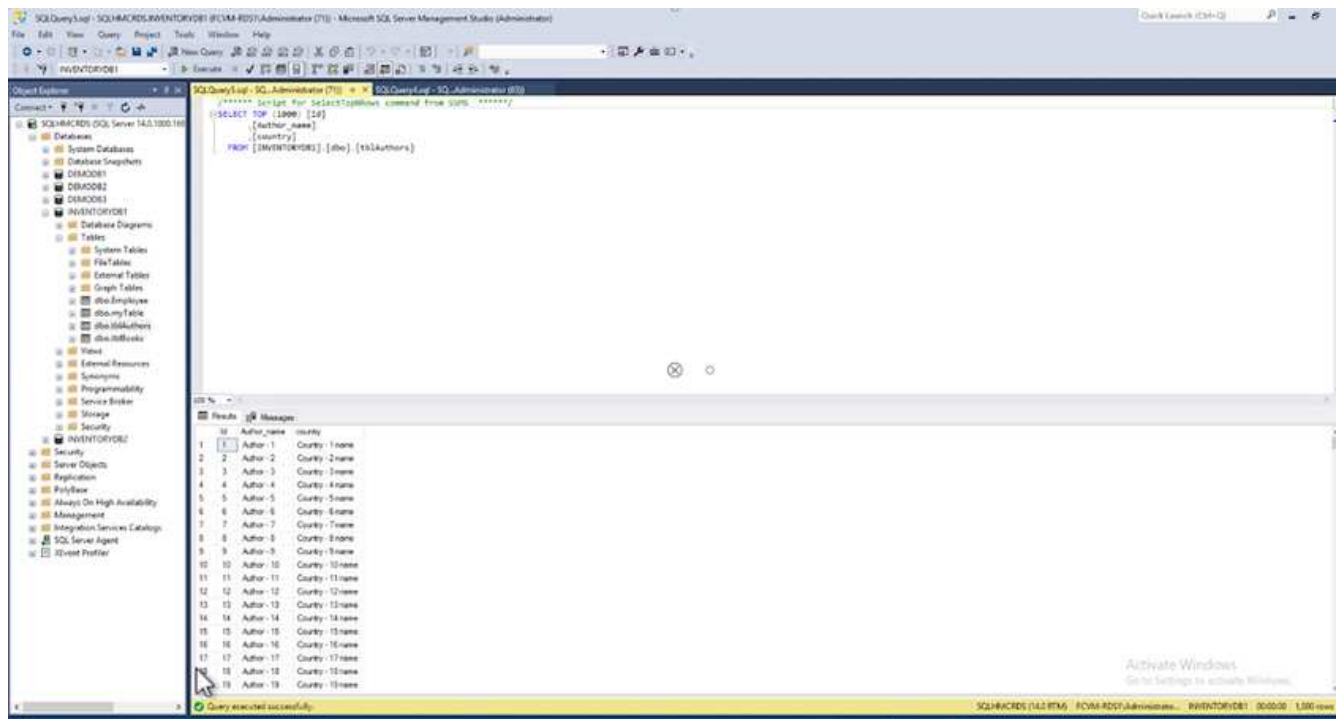
- リストア・ジョブを完了するには、ターゲット・インスタンスがオンラインで実行中である必要があります。

- リモート管理サーバまたはリモート検証サーバでスケジュール設定しているジョブも含め、SQL Serverデータベースに対して実行されるSnapCenter 処理を無効にする必要があります。
- カスタムログディレクトリのバックアップを別のホストにリストアする場合は、SnapCenter サーバとプラグインホストに同じバージョンのSnapCenter がインストールされている必要があります。
- システムデータベースは代替ホストにリストアできます。
- SnapCenter では、SQL Serverクラスタグループをオフラインにすることなく、Windowsクラスタ内のデータベースをリストアできます。

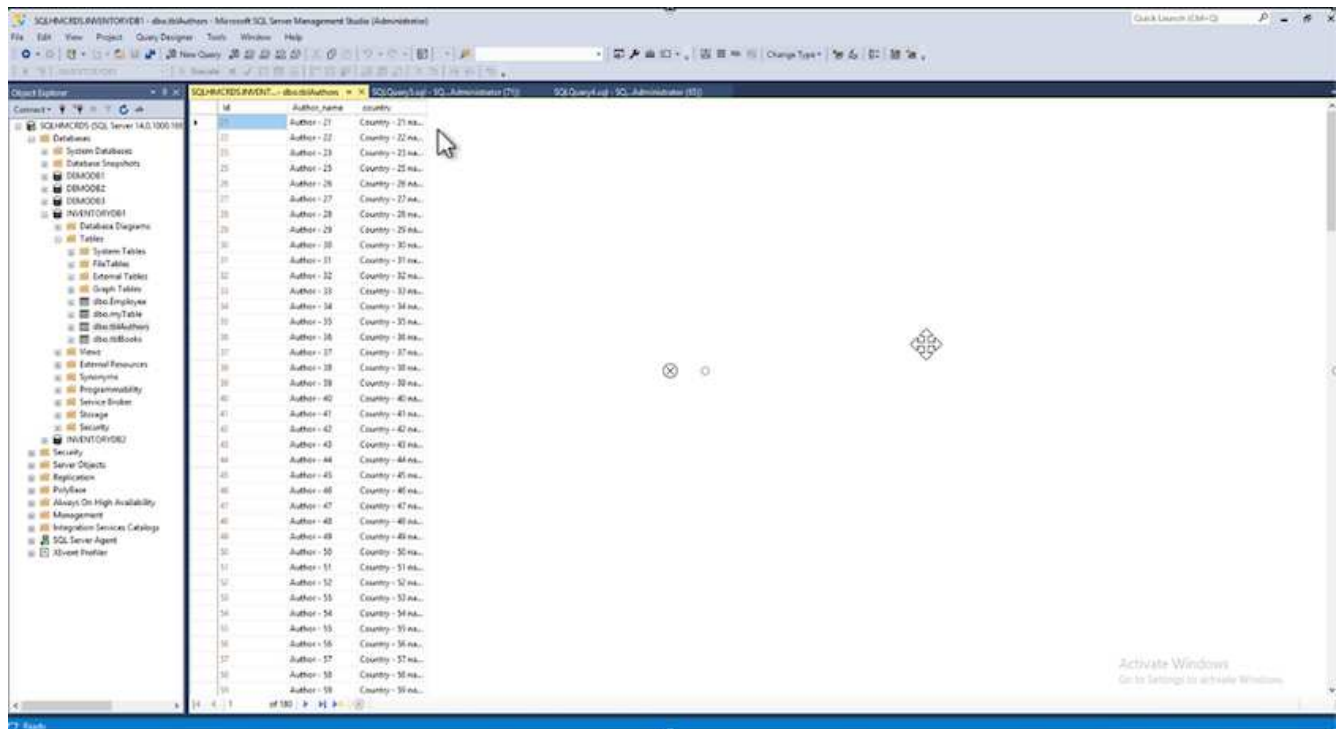
## SQL Serverデータベース上の削除されたテーブルの特定の時点へのリストア

SQL Serverデータベースを特定の時点にリストアするには、次の手順を実行します。

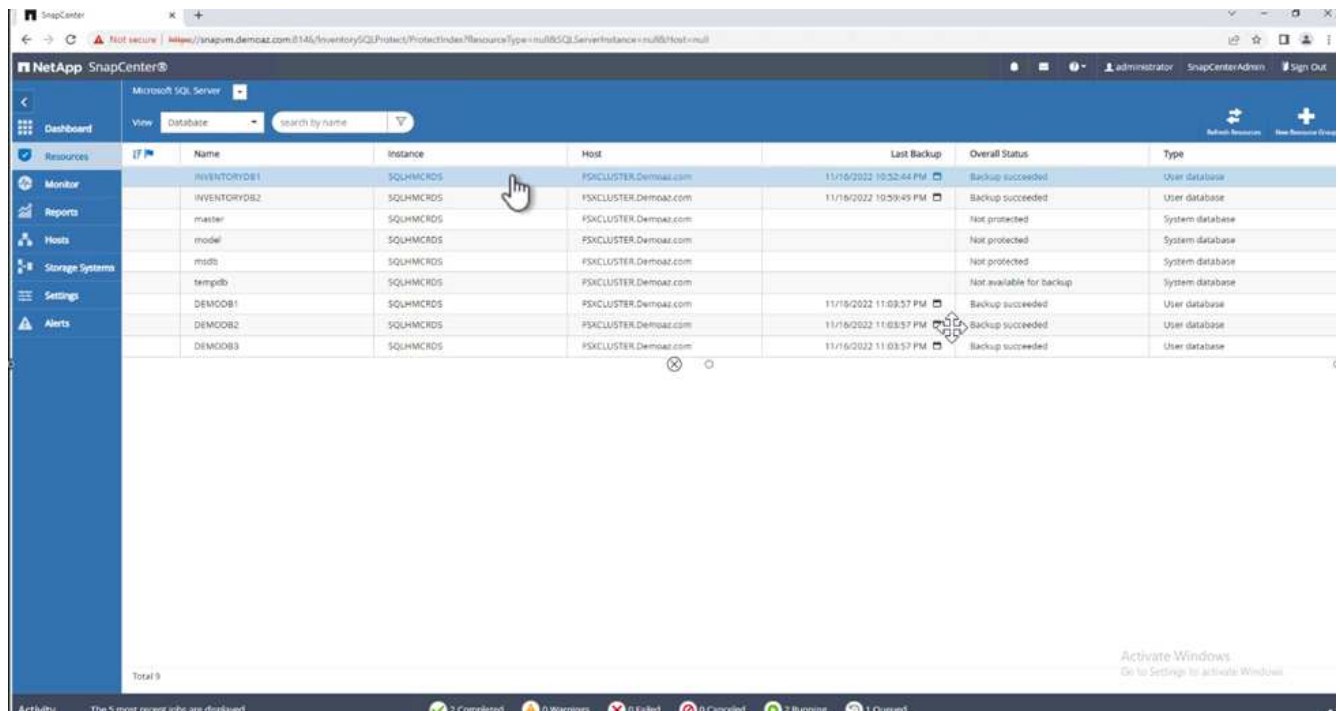
1. 次のスクリーンショットは、テーブルを削除する前のSQL Serverデータベースの初期状態を示しています。



スクリーンショットは、テーブルから20行が削除されたことを示しています。

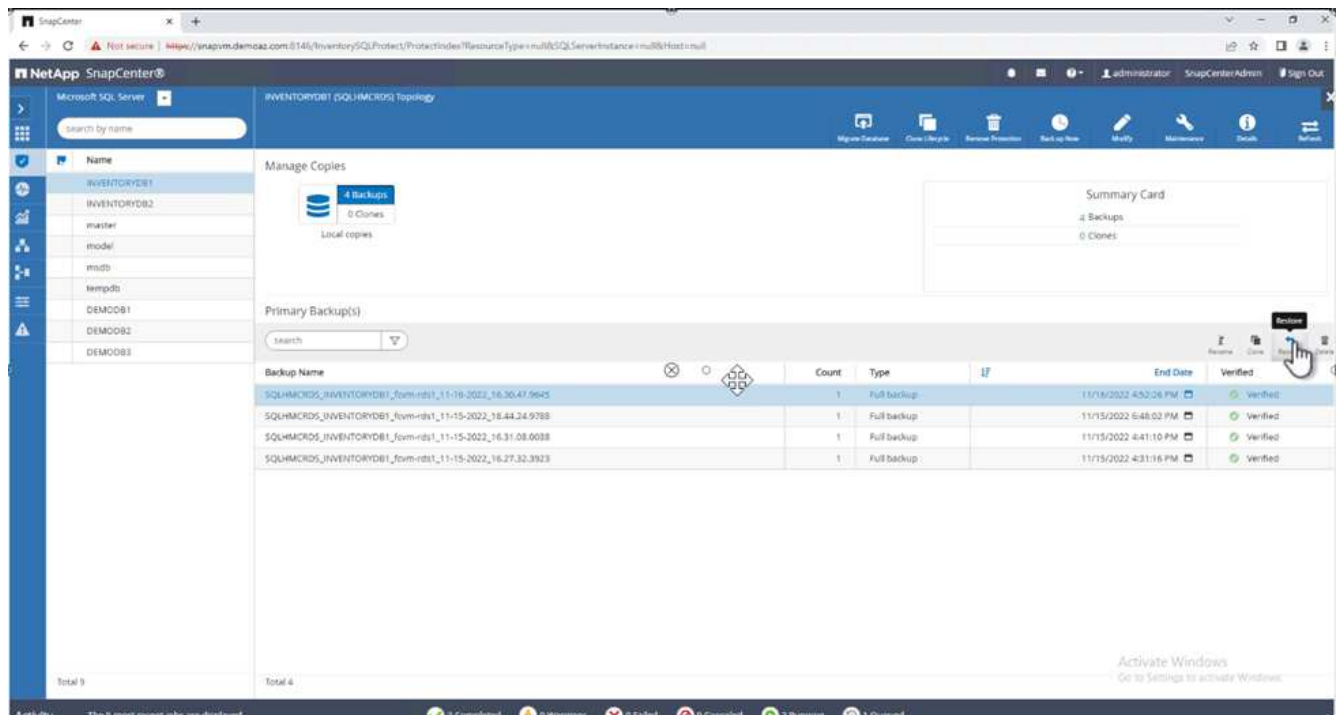


2. SnapCenter サーバにログインします。[リソース]タブで、データベースを選択します。

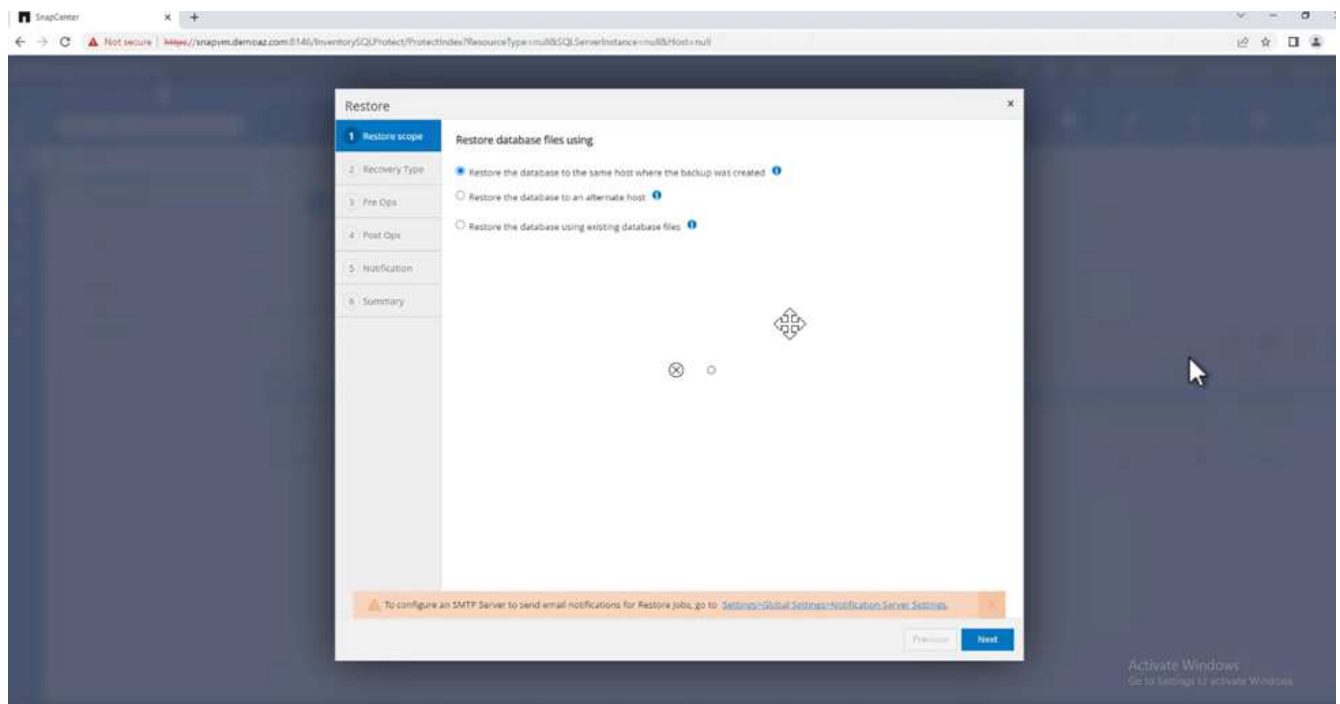


3. 最新のバックアップを選択します。

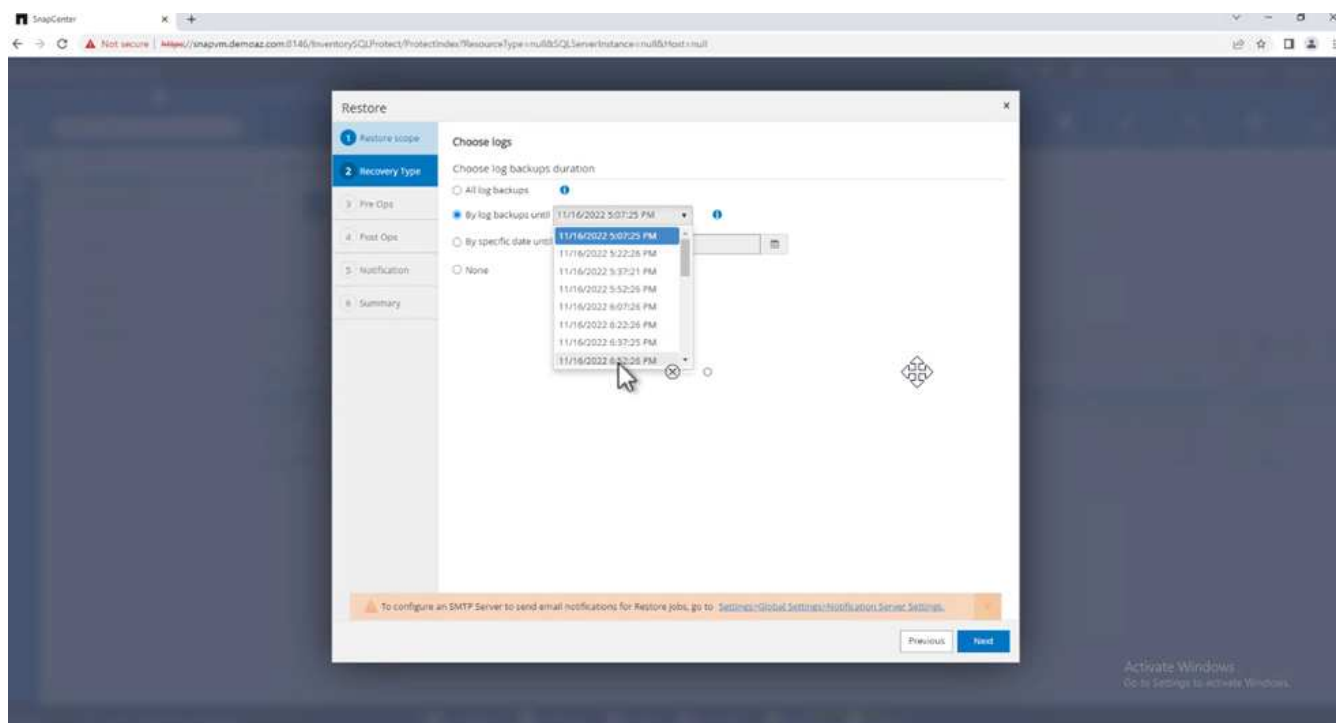
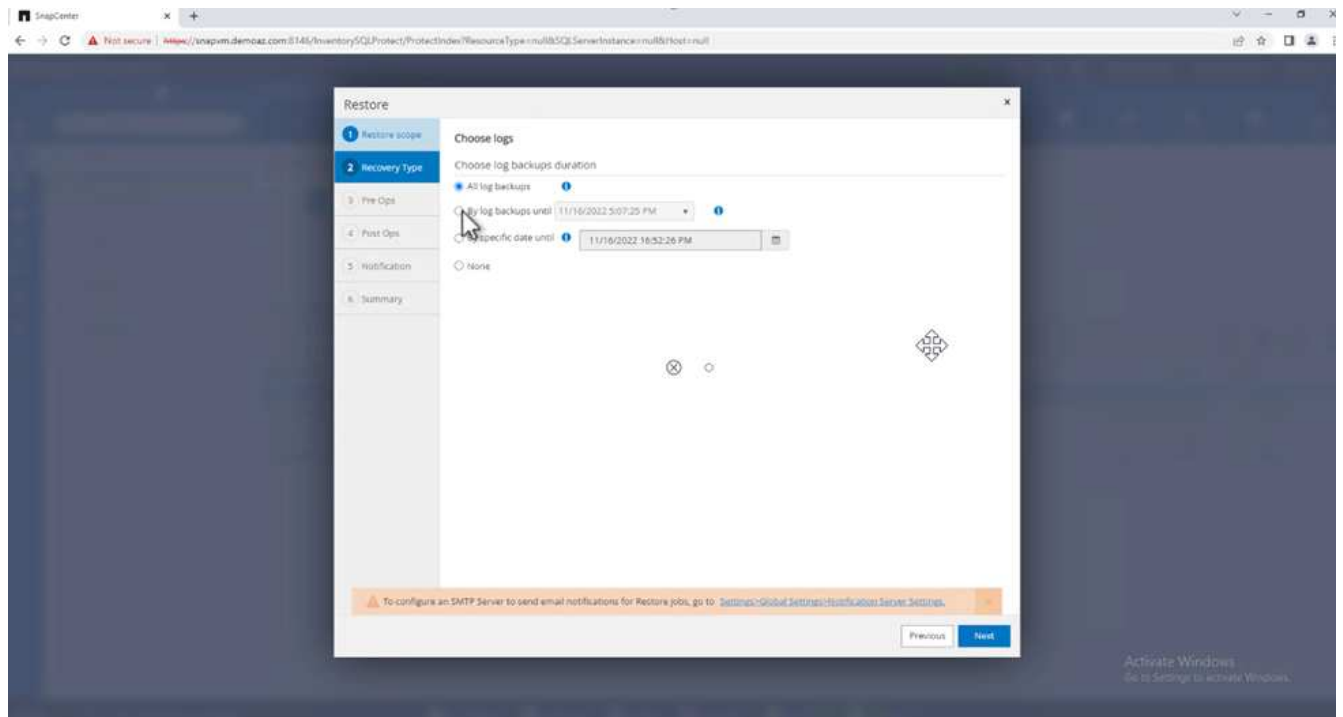
4. 右側で、\*[リストア]\*を選択します。



5. 新しいウィンドウが表示されます。[リストア]\*オプションを選択します。
6. 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します。「\*次へ\*」をクリックします。

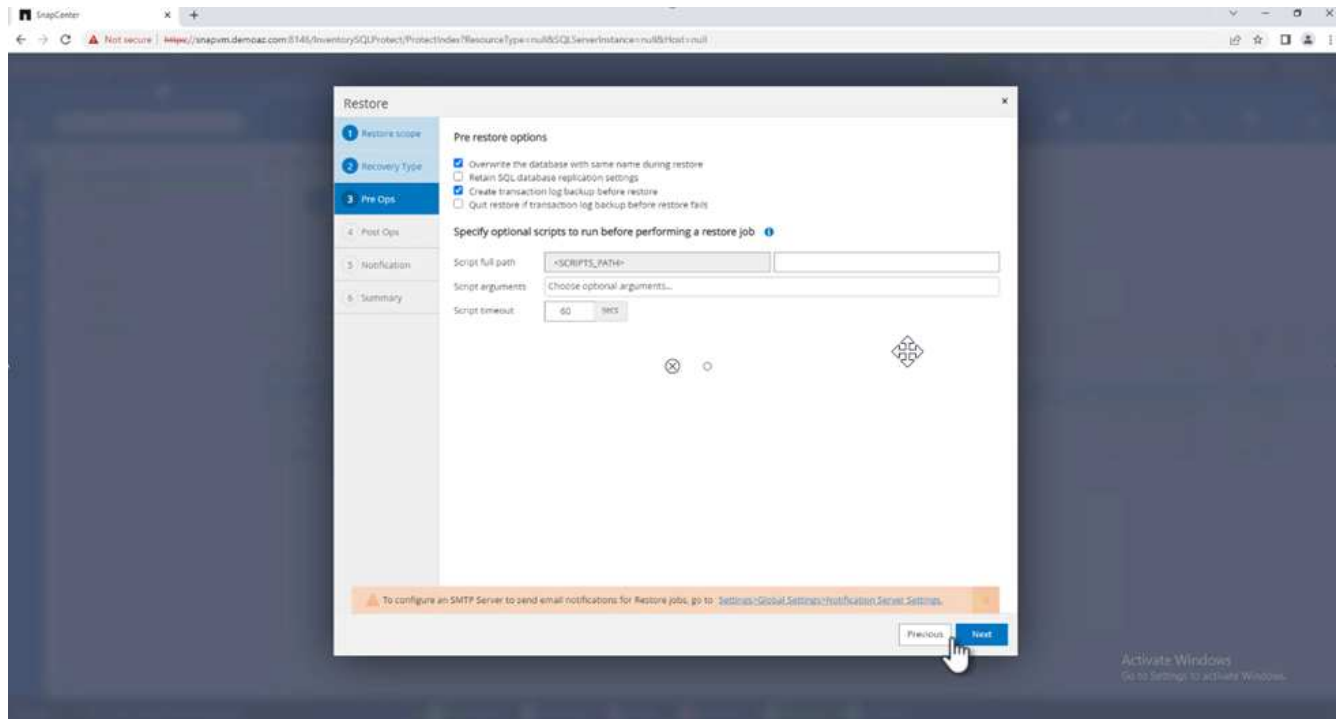


7. で、[すべてのログバックアップ]\*を選択します。「\*次へ\*」をクリックします。



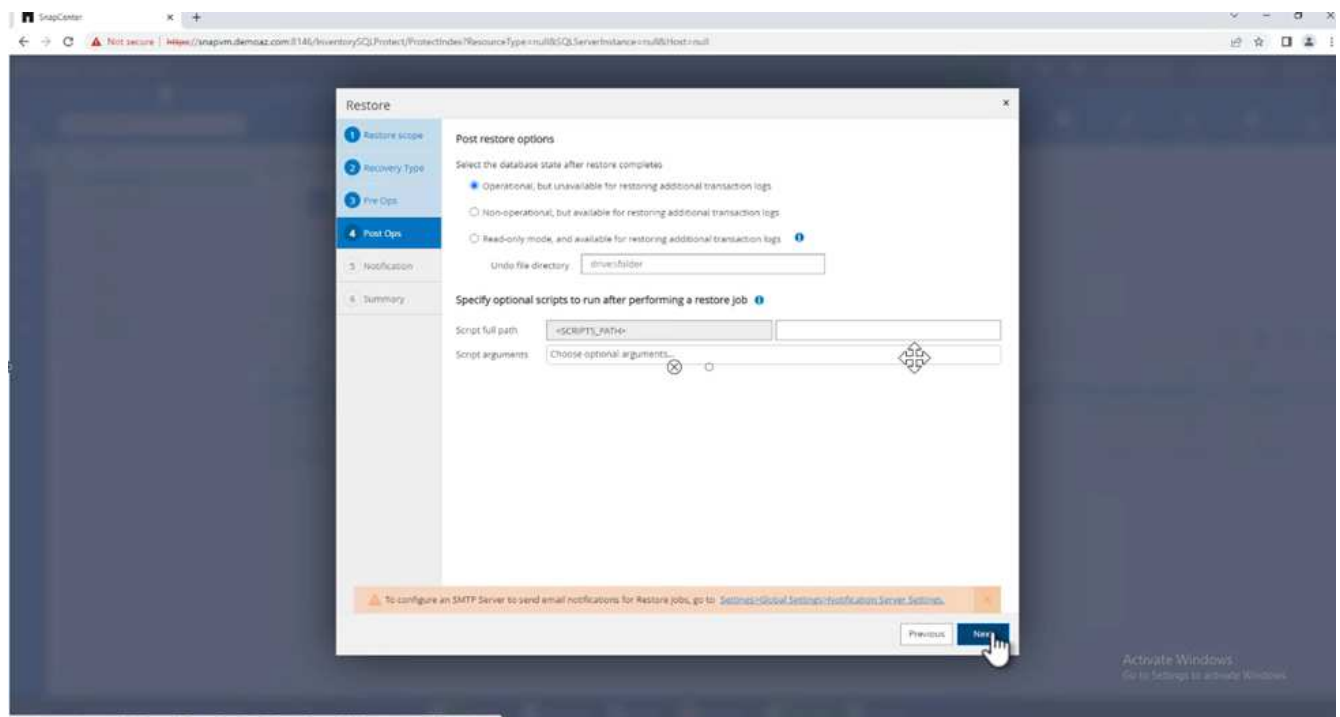
リストア前のオプション：

1. [リストア時に同じ名前データベースを上書きする]オプションを選択します。「\*次へ\*」をクリックします。

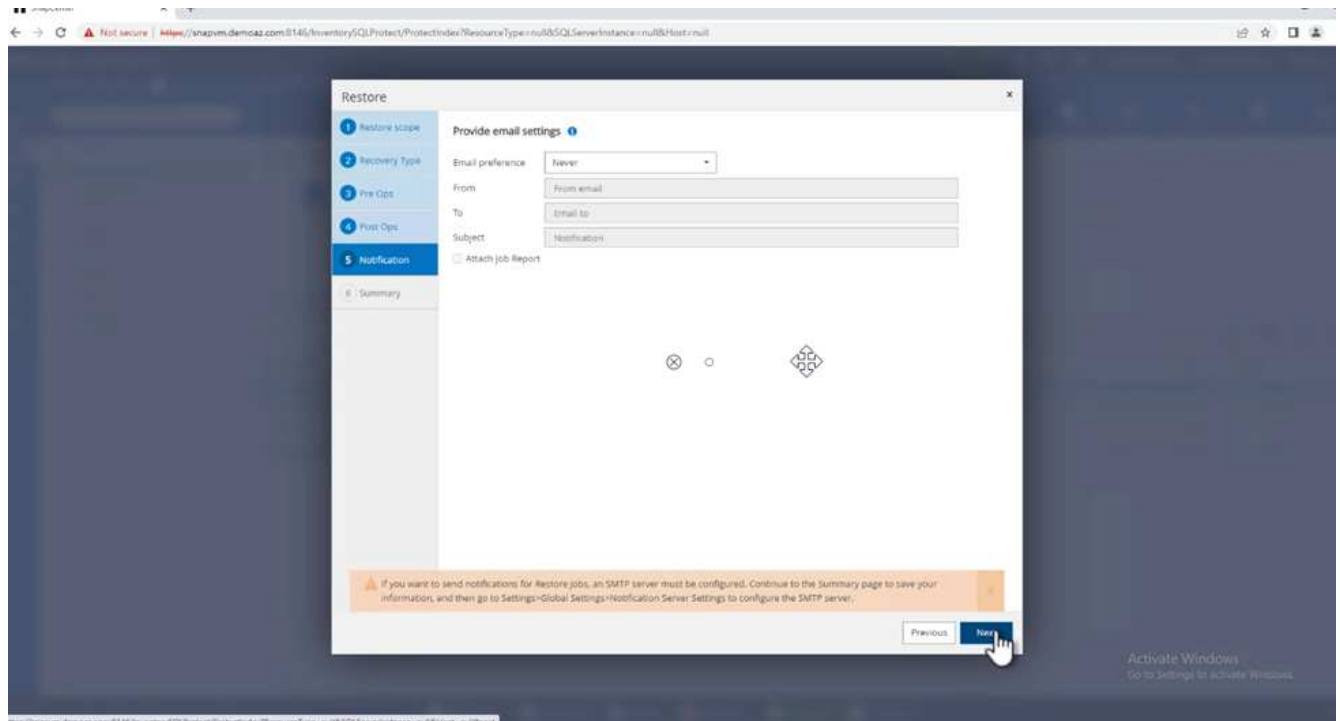


リストア後のオプション：

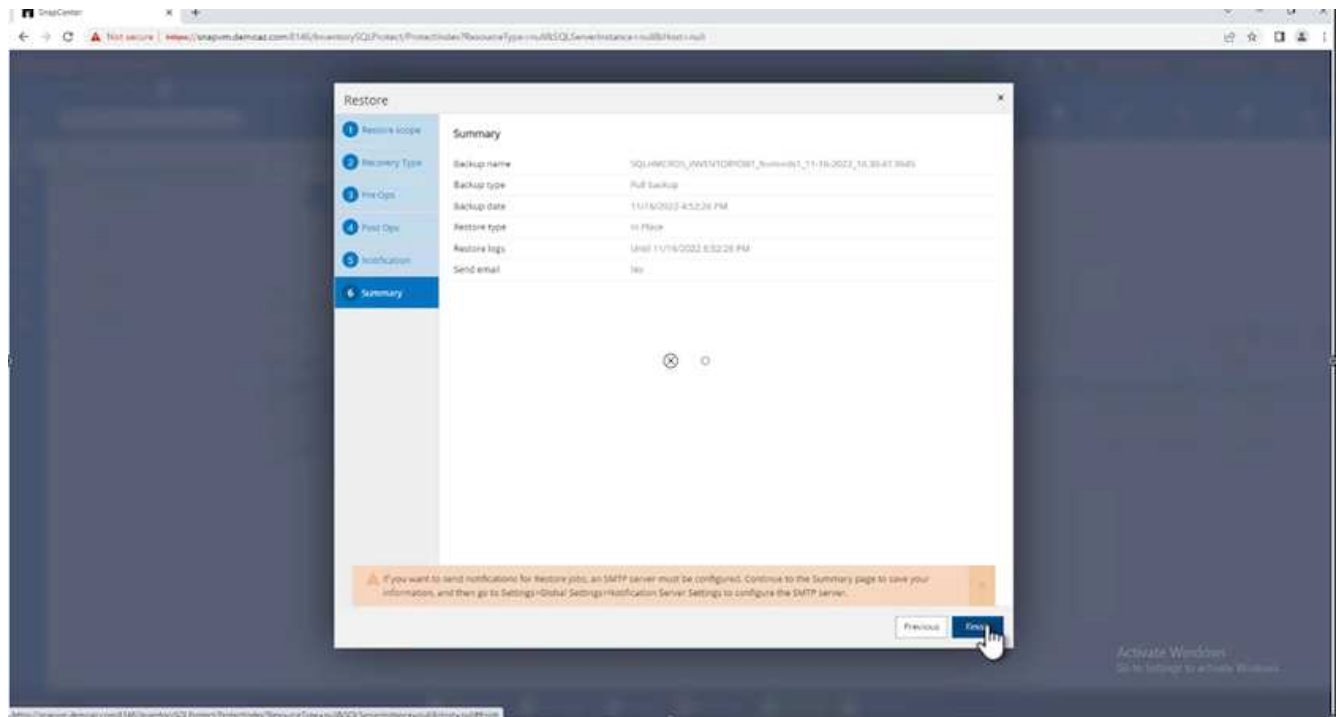
1. オプション\***[Operational, but unavailable for restoring additional transaction logs]**\*を選択します。「\* 次へ \*」をクリックします。



2. Eメール設定を指定します。「\* 次へ \*」をクリックします。



3. [概要]ページで、\*[完了]\*をクリックします。



リストアの進行状況を監視しています

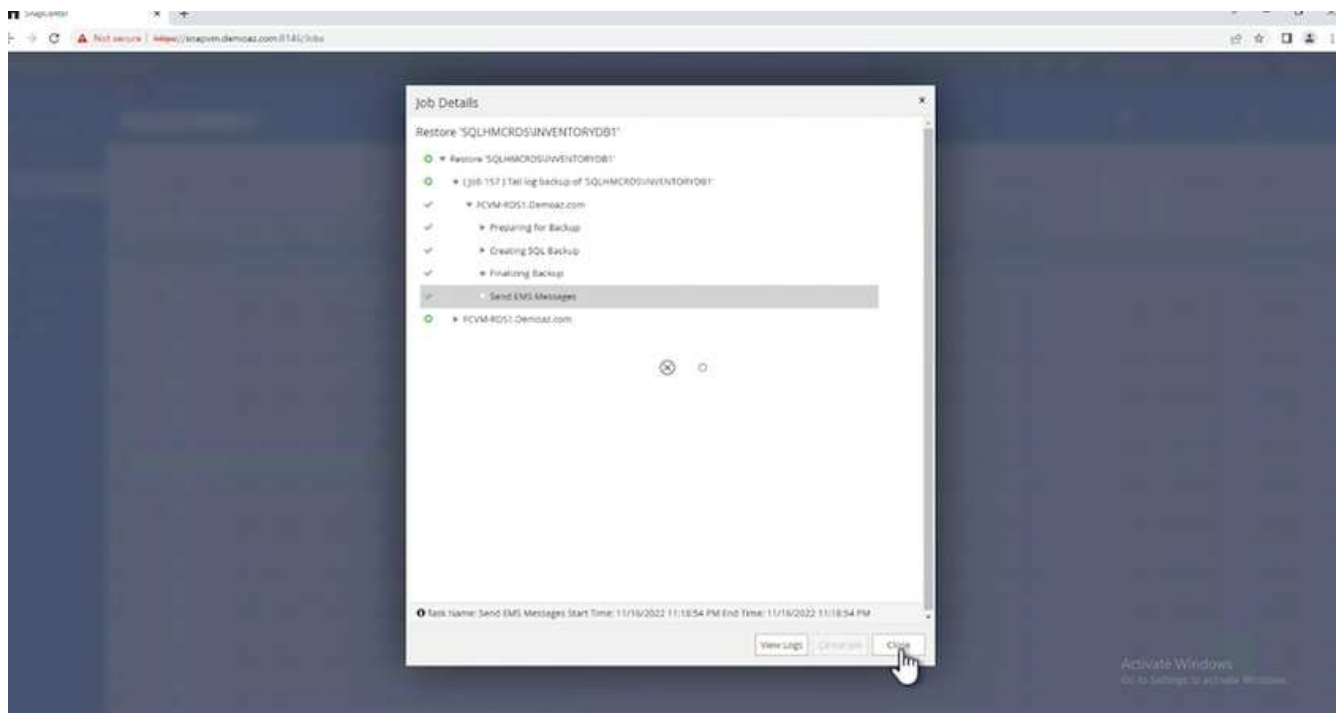
1. [監視]\*タブで、リストアジョブの詳細をクリックして、リストアジョブの進捗状況を表示します。



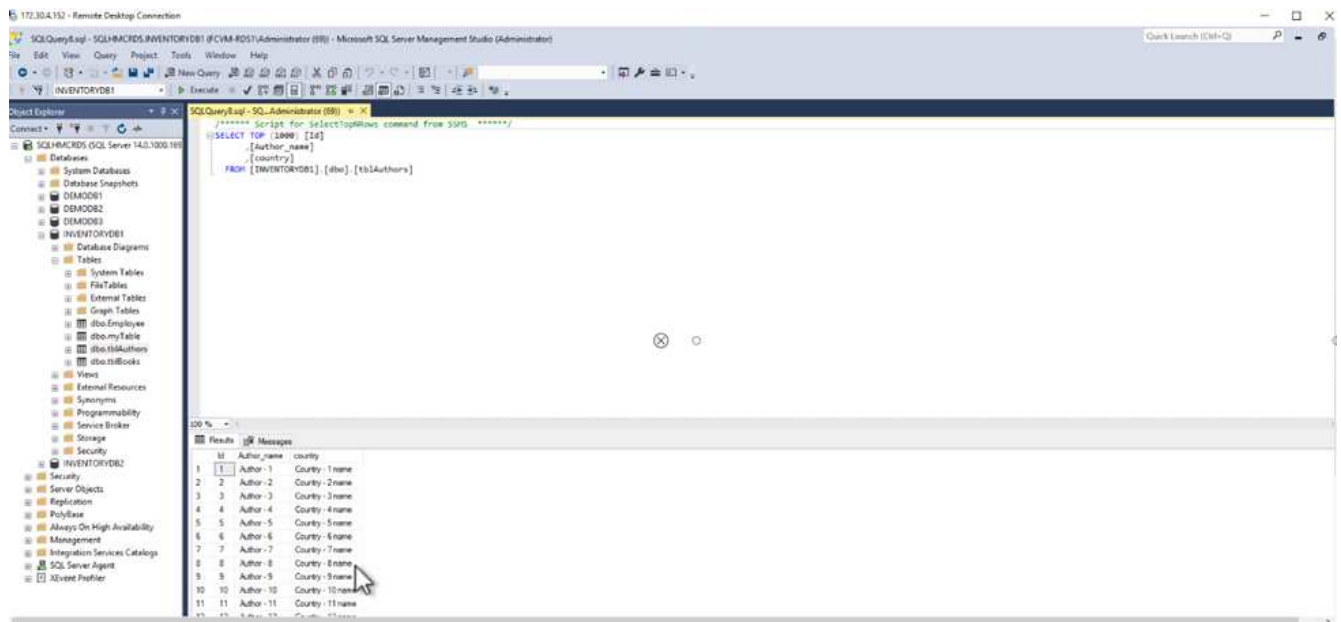
The screenshot shows the NetApp SnapCenter interface with a list of jobs. The table has columns for ID, Status, Name, Start date, End date, and Owner. A mouse cursor is pointing at the 'Send EMS Messages' step in the job details for job ID 137.

ID	Status	Name	Start date	End date	Owner
134	✓	Restore 'SQLMCRD5\INVENTORYDB1'	11/16/2022 11:11:03 PM		Administrator
135	✓	Backup of Resource Group 'SQLMCRD5\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 11:00:01 PM		Administrator
134	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 10:59:02 PM	11/16/2022 11:10:54 PM	Administrator
133	✓	Backup of Resource Group 'SQLMCRD5\INVENTORYDB2' with policy 'InventoryDB2_fullbackup'	11/16/2022 10:55:01 PM	11/16/2022 10:58:50 PM	Administrator
132	✓	Backup of Resource Group 'SQLMCRD5\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 10:45:01 PM	11/16/2022 11:10:54 PM	Administrator
131	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 10:44:02 PM	11/16/2022 10:55:53 PM	Administrator
130	✓	Backup of Resource Group 'SQLMCRD5\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 10:30:01 PM	11/16/2022 10:55:54 PM	Administrator
148	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 10:29:02 PM	11/16/2022 10:40:53 PM	Administrator
148	✓	Backup of Resource Group 'SQLMCRD5\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 10:15:01 PM	11/16/2022 10:40:53 PM	Administrator
147	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 10:14:02 PM	11/16/2022 10:25:53 PM	Administrator
146	✓	Backup of Resource Group 'SQLMCRD5\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 10:00:01 PM	11/16/2022 10:25:53 PM	Administrator
145	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 9:58:02 PM	11/16/2022 10:10:53 PM	Administrator
144	✓	Backup of Resource Group 'SQLMCRD5\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 9:45:01 PM	11/16/2022 10:10:53 PM	Administrator
143	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 9:44:02 PM	11/16/2022 9:55:54 PM	Administrator
142	✓	Backup of Resource Group 'SQLMCRD5\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 9:30:01 PM	11/16/2022 9:55:54 PM	Administrator
141	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 9:29:02 PM	11/16/2022 9:40:53 PM	Administrator
140	✓	Backup of Resource Group 'SQLMCRD5\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 9:15:01 PM	11/16/2022 9:40:53 PM	Administrator
139	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 9:14:02 PM	11/16/2022 9:25:54 PM	Administrator
138	✓	Backup of Resource Group 'SQLMCRD5\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 9:00:01 PM	11/16/2022 9:25:54 PM	Administrator
137	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 8:59:02 PM	11/16/2022 9:10:53 PM	Administrator
136	✓	Backup of Resource Group 'SQLMCRD5\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 8:45:01 PM	11/16/2022 9:10:53 PM	Administrator
135	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 8:44:02 PM	11/16/2022 8:55:54 PM	Administrator
134	✓	Backup of Resource Group 'SQLMCRD5\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 8:30:01 PM	11/16/2022 8:55:54 PM	Administrator
133	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 8:29:02 PM	11/16/2022 8:40:53 PM	Administrator

2. ジョブの詳細をリストアします。



3. SQL Serverホスト> database > table are presentに戻ります。



## 詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを参照してください。

- "TR-4714 : 『Best Practices Guide for Microsoft SQL Server using NetApp SnapCenter 』 "

<https://www.netapp.com/pdf.html?item=/media/12400-tr4714pdf.pdf>

- "データベースをリストアする際の要件"

"[https://docs.netapp.com/us-en/snapcenter-45/protect-scsql/concept\\_requirements\\_for\\_restoring\\_a\\_database.html](https://docs.netapp.com/us-en/snapcenter-45/protect-scsql/concept_requirements_for_restoring_a_database.html)"

- クローンデータベースのライフサイクルについて

"<https://library.netapp.com/ecmdocs/ECMP1217281/html/GUID-4631AFF4-64FE-4190-931E-690FCADA5963.html>"

## TR-4923 : 『SQL Server on AWS EC2 using Amazon FSx ONTAP』

このソリューションには、Amazon FSx ONTAPを使用したAWS EC2へのSQL Serverの導入が含まれています。

執筆者 : Pat Sinthusan and Niyaz Mohamed、NetApp

### はじめに

オンプレミスのストレージシステムとクラウドストレージサービスの機能の違いによって、アプリケーションをオンプレミスからクラウドに移行したいと考えている企業は少なくありません。このギャップが解消された

ことで、Microsoft SQL Serverなどのエンタープライズアプリケーションの移行で問題が生じていました。特に、堅牢なスナップショット、Storage Efficiency機能、高可用性、信頼性、一貫性のあるパフォーマンスなどのエンタープライズアプリケーションを実行するために必要なサービスが不足しているため、設計のトレードオフやアプリケーションの移行が必要になりました。FSx ONTAPを使用すれば、妥協する必要がなくなります。FSx ONTAPは、AWSが販売、サポート、請求、フルマネージドのネイティブ（ファーストパーティ）AWSサービスです。NetApp ONTAPの機能を活用して、エンタープライズクラスのストレージとデータ管理機能を提供します。ネットアップは、AWSで30年にわたってマネージドサービスとしてオンプレミスで提供してきたのと同じ機能を提供します。

EC2インスタンス上のSQL Serverを使用すると、データベース管理者は、自身のデータベース環境と基盤となるオペレーティングシステムにアクセスしてカスタマイズできます。SQL Server on EC2インスタンスを組み合わせ ["AWS FSX ONTAP の略"](#)でデータベースファイルを格納することで、パフォーマンスの向上、データ管理、ブロックレベルのレプリケーションを使用したシンプルで簡単な移行パスを実現できます。そのため、AWS VPC上で複雑なデータベースを簡単に移行して、クリック回数を減らすことができ、スキーマの変換も不要です。

## Amazon FSx ONTAPとSQL Serverを併用するメリット

Amazon FSx ONTAPは、AWSにSQL Serverを導入するための理想的なファイルストレージです。次のようなメリットがあります。

- 一貫した高パフォーマンスとスループットを低レイテンシで実現
- NVMeキャッシュによるインテリジェントなキャッシングでパフォーマンスを向上
- 容量、スループット、IOPSをオンザフライで柔軟にサイジングできます
- オンプレミスからAWSへの効率的なブロックレプリケーション
- データベース環境での一般的なプロトコルであるiSCSIの使用
- シンプロビジョニングやゼロフットプリントのクローンなどのStorage Efficiency機能を備えています
- バックアップにかかる時間が数時間から数分に短縮され、RTOが短縮されます
- わかりやすいNetApp SnapCenter UIで、SQLデータベースのバックアップとリカバリをきめ細かく実行できます
- 実際の移行前に複数のテスト移行を実行できること
- 移行中のダウンタイムを短縮し、ファイルレベルまたはI/Oレベルのコピーによって移行の課題を克服できます
- メジャーリリースまたはパッチの更新後にルート原因を検出することで、MTTRを短縮できます

一般的にオンプレミスで使用されているように、FSX ONTAPにSQL Serverデータベースを導入すると、優れたパフォーマンス、ストレージ効率、データ管理機能を備えた理想的なデータベースストレージ環境が実現します。ワークセットサイズが5%であると仮定して複数のiSCSIセッションを使用した場合、Flash Cacheを配置すると、FSX ONTAP サービスでは10万IOPSを超えることがあります。この構成では、非常に要件の厳しいアプリケーションのパフォーマンスを完全に制御できます。FSx ONTAPに接続された小規模なEC2インスタンスで実行されるSQL Serverは、はるかに大規模なEC2インスタンスで実行されるSQL Serverと同じパフォーマンスを発揮します。これは、FSx ONTAPにはネットワーク帯域幅の制限のみが適用されるためです。インスタンスのサイズを縮小することでコンピューティングコストも削減され、TCOを最適化して導入できます。iSCSIを使用するSQLと、FSx ONTAP上のマルチチャネルの継続的可用性共有を組み合わせたSMB3.0は、SQLワークロードに大きなメリットをもたらします。

## 開始する前に

Amazon FSx ONTAPとSQL Server on EC2インスタンスを組み合わせることで、今日の最も厳しいアプリケーション要件を満たすエンタープライズレベルのデータベースストレージ設計を作成できます。両方のテクノロジーを最適化するには、SQL ServerのI/Oパターンと特性を理解することが重要です。SQL Serverデータベース用の適切に設計されたストレージレイアウトは、SQL ServerのパフォーマンスとSQL Serverインフラの管理をサポートします。また、ストレージレイアウトを適切に設定すれば、初期導入を成功させ、ビジネスの成長に合わせて環境をスムーズに拡張できます。

### 前提条件

本ドキュメントの手順を完了する前に、次の前提条件を満たしている必要があります。

- AWSアカウント
- EC2とFSx ONTAPをプロビジョニングするための適切なIAMロール
- EC2上のWindows Active Directoryドメイン
- すべてのSQL Serverノードが相互に通信する必要があります
- DNS解決が機能し、ホスト名を解決できることを確認します。この条件を満たしていない場合は、ホストファイルエントリを使用します
- SQL Serverのインストールに関する一般的な知識

また、ネットアップのSQL Server環境向けベストプラクティスを参照して、ストレージ構成が最適であることを確認してください。

FSX ONTAP では、ストレージの調達が最も簡単な作業であり、ファイルシステムを更新することで実行できます。このシンプルなプロセスにより、必要に応じてコストとパフォーマンスを動的に最適化し、SQLワークロードのバランスを取ることができます。また、シンプロビジョニングも有効になります。FSX ONTAP シンプロビジョニングは、ファイルシステムでプロビジョニングされているものよりも、SQL Serverを実行しているEC2インスタンスに、より多くの論理ストレージを提供するように設計されています。スペースを事前に割り当てるのではなく、データの書き込み時にストレージスペースが動的に各ボリュームまたはLUNに割り当てられます。ほとんどの構成では、ボリュームまたはLUN内のデータが削除される（Snapshotコピーに保持されていない）と、空きスペースも解放されます。次の表に、ストレージを動的に割り当てるための設定を示します。

設定	構成
ボリュームギャランティ	なし（デフォルトで設定）
LUNリザーベーション	有効
fractional_reserve	0%（デフォルトで設定）
スナップリザーブ	0%
自動削除	ボリューム/古い順に選択します
オートサイズ	オン
最初に試す	自動拡張
ボリューム階層化ポリシー	Snapshotのみ
Snapshotポリシー	なし

この構成では、ボリュームの合計サイズは、ファイルシステムで実際に使用可能なストレージよりも大きくなる可能性があります。LUNまたはSnapshotコピーがボリューム内の使用可能なスペースよりも多くのスペースを必要とする場合、ボリュームは、包含ファイルシステムからより多くのスペースを取得して自動的に拡張します。自動拡張では、FSX ONTAP によって、ボリュームのサイズが事前に決めた最大サイズまで自動的に拡張されます。ボリュームの自動拡張をサポートするには、使用可能なスペースを包含ファイルシステムに確保する必要があります。そのため、自動拡張を有効にした状態でファイルシステムの空きスペースを監視し、必要に応じてファイルシステムを更新してください。

さらに、ボリュームのスペースが不足してボリューム内のLUNが書き込みを受け付けられなくなったときにFSx ONTAPからEC2ホストに通知されるように、LUNのオプションをenabledに設定し ["space-alloc のようになります"](#)ます。また、このオプションを選択すると、EC2ホスト上のSQL Serverがデータを削除したときにFSx ONTAPで自動的にスペースが再生されます。space-allocationオプションは、デフォルトでdisabledに設定されています。



ギャランティがnoneのボリュームにスペースリザーブLUNを作成する場合の動作は、スペースリザーブなしのLUNと同じです。ギャランティがnoneのボリュームは、ボリューム自体、書き込み時に初めてスペースが割り当てられるため、LUNに割り当てられるスペースはありません。

この構成では、通常、FSX ONTAP 管理者はボリュームのサイズを設定して、ホスト側とファイルシステム内のLUNの使用済みスペースを管理および監視する必要があります。



SQL Serverのワークロードには別のファイルシステムを使用することを推奨します。ファイルシステムが複数のアプリケーションに使用されている場合は、ファイルシステムとファイルシステム内のボリュームの両方のスペース使用量を監視して、ボリューム間でスペースの競合が発生していないことを確認します。



FlexCloneボリュームの作成に使用されるSnapshotコピーは、自動削除オプションでは削除されません。



ストレージのオーバーコミットメントは、最小限のシステム停止でも許容できないSQL Serverなどのミッションクリティカルなアプリケーションに対して慎重に検討し、管理する必要があります。このような場合は、ストレージ消費の傾向を監視して、オーバーコミットメントが許容される量を判断することを推奨します。

#### ベストプラクティス

1. ストレージパフォーマンスを最適化するには、ファイルシステムの容量をデータベース全体の1.35倍にプロビジョニングします。
2. シンプロビジョニングを使用してアプリケーションのダウンタイムを回避するには、適切な監視と効果的なアクションプランが必要です。
3. Cloudwatchやその他の監視ツールのアラートを設定して、ストレージがいっぱいになったときに対応できるように十分な時間をユーザーに連絡するようにしてください。

## SQL Server用のストレージを設定し、バックアップ、リストア、クローニングの各処理にSnapCenterを導入します

SnapCenterでSQL Serverの処理を実行するには、まずSQL Server用のボリュームとLUNを作成する必要があります。



## SQL Server用のボリュームとLUNを作成します

SQL Server用のボリュームとLUNを作成するには、次の手順を実行します。

1. Amazon FSxコンソールを開きます。 <https://console.aws.amazon.com/fsx/>
2. CreationメソッドのStandard Createオプションを使用して、NetApp ONTAP ファイルシステムのAmazon FSXを作成します。これにより、FSxadminとvsadminの資格情報を定義できます。

**Creation method**

Quick create  
Use recommended best-practice configurations. Most configuration options can be changed after the file system is created.

Standard create  
You set all of the configuration options, including specifying performance, networking, security, backups, and maintenance.

3. fsxadminのパスワードを指定します。

### File system administrative password

Password for this file system's "fsxadmin" user, which you can use to access the ONTAP CLI or REST API.

- Don't specify a password  
 Specify a password

Password

Confirm password

4. SVMのパスワードを指定します。

### SVM administrative password

Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.

- Don't specify a password  
 Specify a password

Password

Confirm password

5. の手順に従ってボリュームを作成します "FSx ONTAPでのボリュームの作成".

ベストプラクティス

- ストレージの Snapshot コピーのスケジュールと保持ポリシーを無効にします。代わりに、NetApp SnapCenter を使用して、SQL ServerのデータボリュームとログボリュームのSnapshotコピーを調整します。
- 高速できめ細かなリストア機能を利用するために、別々のボリューム上の個々のLUNにデータベースを設定します。
- ランダムな読み取り/書き込みワークロードであるため、ユーザデータファイル (.mdf) を別々のボリュームに配置します。トランザクションログバックアップは、データベースバックアップよりも頻繁に作成するのが一般的です。このため、トランザクションログファイル (.ldf) をデータファイルとは別のボリュームに配置して、それぞれに個別のバックアップスケジュールを作成できるようにします。また、この分離により、ログファイルのシーケンシャルライトI/Oとデータファイルのランダムリード/ライトI/Oが分離され、SQL Serverのパフォーマンスが大幅に向上します。
- tempdbは、Microsoft SQL Serverで一時的なワークスペースとして使用されるシステムデータベースです。特に、I/Oを大量に消費するDBCC CHECKDB操作に使用されます。したがって、このデータベースは専用ボリュームに配置してください。ボリューム数が課題となる大規模な環境では、慎重に計画したあとで、tempdbを少数のボリュームに統合し、他のシステムデータベースと同じボリュームに格納できます。tempdbのデータ保護は、Microsoft SQL Serverを再起動するたびに、このデータベースが再作成されるため、優先度が高くありません。

6. 次のSSHコマンドを使用してボリュームを作成します。

```
vol create -vserver svm001 -volume vol_awssqlprod01_data -aggregate
aggr1 -size 800GB -state online -tiering-policy snapshot-only
-percent-snapshot-space 0 -autosize-mode grow -snapshot-policy none
-security-style ntfs
volume modify -vserver svm001 -volume vol_awssqlprod01_data
-fractional-reserve 0
volume modify -vserver svm001 -volume vol_awssqlprod01_data -space
-mgmt-try-first vol_grow
volume snapshot autodelete modify -vserver svm001 -volume
vol_awssqlprod01_data -delete-order oldest_first
```

7. Windows Serverの管理者権限を使用して、PowerShellでiSCSIサービスを開始します。

```
Start-service -Name msiscsi
Set-Service -Name msiscsi -StartupType Automatic
```

8. Windows Serverの管理者権限を使用して、PowerShellでMultipath IOをインストールします。

```
Install-WindowsFeature -name Multipath-IO -Restart
```

9. Windows Serverの管理者権限を使用して、PowerShellでWindowsイニシエータ名を検索します。

```
Get-InitiatorPort | select NodeAddress
```



```
PS C:\Users\administrator.CONTOSO> Get-InitiatorPort | select NodeAddress
NodeAddress
-----
iqn.1991-05.com.microsoft:ws2019-sql1.contoso.net
```

10. puttyを使用してStorage Virtual Machine (SVM) に接続し、igroupを作成します。

```
igroup create -igroup igrp_ws2019sql1 -protocol iscsi -ostype
windows -initiator iqn.1991-05.com.microsoft:ws2019-sql1.contoso.net
```

11. LUNを作成するには、次のSSHコマンドを使用します。

```
lun create -path /vol/vol_awssqlprod01_data/lun_awssqlprod01_data
-size 700GB -ostype windows_2008 -space-allocation enabled lun
create -path /vol/vol_awssqlprod01_log/lun_awssqlprod01_log -size
100GB -ostype windows_2008 -space-allocation enabled
```

```
svmsql:> lun create -path /vol/vol_awssqlprod01_data/lun_awssqlprod01_data -size 700GB -ostype windows_2008
Created a LUN of size 700g (751619276800)
svmsql:> lun create -path /vol/vol_awssqlprod01_log/lun_awssqlprod01_log -size 100GB -ostype windows_2008
Created a LUN of size 100g (107374182400)
svmsql:> lun show
Vserver      Path
-----
svmsql      /vol/vol_awssqlprod01_data/lun_awssqlprod01_data
              online unmapped windows_2008
              700GB
svmsql      /vol/vol_awssqlprod01_log/lun_awssqlprod01_log
              online unmapped windows_2008
              100GB
2 entries were displayed.
```

12. OSのパーティショニングスキームを使用してI/Oアライメントを実行するには、推奨されるLUNタイプとしてwindows\_2008を使用してください。詳細については、[を参照してください"ここをクリック"](#)。
13. 次のSSHコマンドを使用して、作成したLUNにigroupをマッピングします。

```
lun show
lun map -path /vol/vol_awssqlprod01_data/lun_awssqlprod01_data
-igroup igrp_awssqlprod01
lun map -path
/vol/vol_awssqlprod01_log/lun_awssqlprod01_log -igroup
igrp_awssqlprod01
```

```

svmsql::> lun show
Vserver  Path                                          State  Mapped  Type      Size
-----
svmsql   /vol/vol_awssqlprod01_data/lun_awssqlprod01_data
                                         online unmapped windows_2008
                                         700GB
svmsql   /vol/vol_awssqlprod01_log/lun_awssqlprod01_log
                                         online unmapped windows_2008
                                         100GB
2 entries were displayed.

svmsql::> lun map -path /vol/vol_awssqlprod01_data/lun_awssqlprod01_data -igroup igrp_awssqlprod01
svmsql::> lun map -path /vol/vol_awssqlprod01_log/lun_awssqlprod01_log -igroup igrp_awssqlprod01

svmsql::>
svmsql::> lun show
Vserver  Path                                          State  Mapped  Type      Size
-----
svmsql   /vol/vol_awssqlprod01_data/lun_awssqlprod01_data
                                         online mapped   windows_2008
                                         700GB
svmsql   /vol/vol_awssqlprod01_log/lun_awssqlprod01_log
                                         online mapped   windows_2008
                                         100GB
2 entries were displayed.

```

- Windowsフェイルオーバークラスタを使用する共有ディスクの場合は、SSHコマンドを実行して、Windowsフェイルオーバークラスタに参加しているすべてのサーバに属するigroupに同じLUNをマッピングします。
- iSCSIターゲットを使用してWindows ServerをSVMに接続する。AWSポータルでターゲットのIPアドレスを検索します。

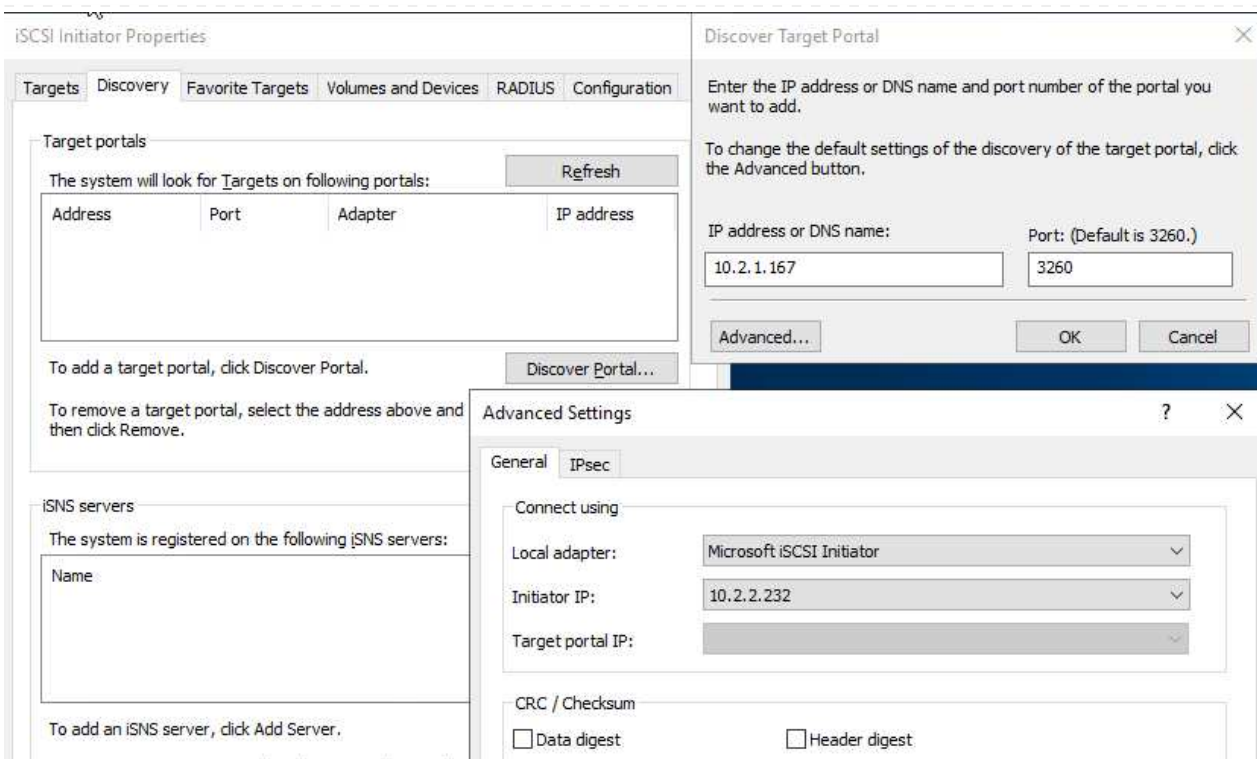
#### svmsql (svm-09e98ab33a31b724a)

Summary	
SVM ID svm-09e98ab33a31b724a	Creation time 2021-09-21T13:19:34-07:00
SVM name svmsql	Lifecycle state Created
UUID ea00ea2d-1b1d-11ec-9de1-6f9cef731025	Subtype DEFAULT
File system ID fs-0ab4b447ebd6082aa	
Resource ARN arn:aws:fs:us-west-2:139763910815:storage-virtual-machine/fs-0ab4b447ebd6082aa/svm-09e98ab33a31b724a	

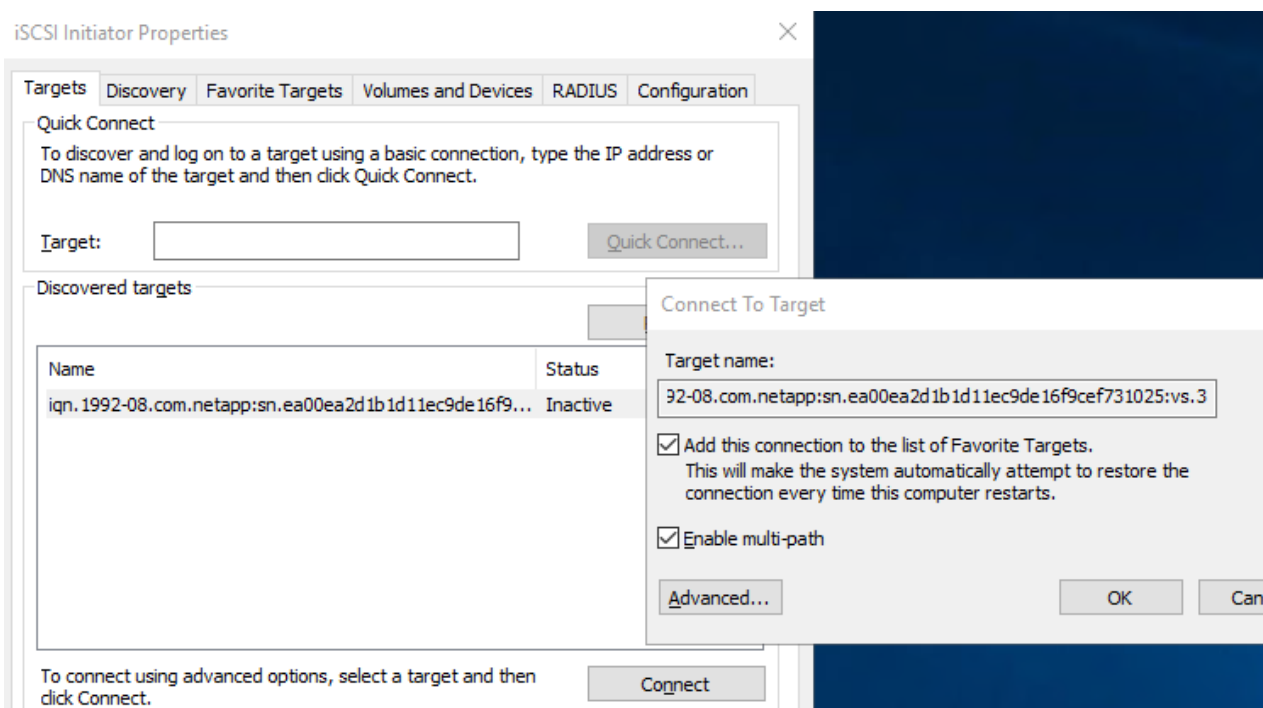
Endpoints	
Management DNS name svm-09e98ab33a31b724a.fs-0ab4b447ebd6082aa.fsx.us-west-2.amazonaws.com	Management IP address 198.19.255.153
NFS DNS name svm-09e98ab33a31b724a.fs-0ab4b447ebd6082aa.fsx.us-west-2.amazonaws.com	NFS IP address 198.19.255.153
iSCSI DNS name iscsi.svm-09e98ab33a31b724a.fs-0ab4b447ebd6082aa.fsx.us-west-2.amazonaws.com	iSCSI IP addresses 10.2.1.167, 10.2.2.12

- Server ManagerおよびToolsメニューから、iSCSI Initiatorを選択します。[Discovery]タブを選択し、[Discover Portal]を選択します。前の手順で確認したiSCSI IPアドレスを入力し、Advanced (詳細設定)を選択します。[ローカルアダプタ]から[Microsoft iSCSIイニシエータ]を選択します。イニシエータIPから、サーバのIPを選択します。[OK]を選択して、すべてのウィンドウを閉じます。



17. SVMの2つ目のiSCSI IPについて手順12を繰り返します。

18. [\* Targets (ターゲット)]タブを選択し、[\* Connect (接続)]を選択して、[\* Enable multi-path (マルチパスを有効にする)]



19. パフォーマンスを最大限に高めるには、セッションをさらに追加します。5つのiSCSIセッションを作成することを推奨します。プロパティ>\*セッションの追加\*>\*詳細設定\*を選択し、ステップ12を繰り返します。

```
$TargetPortals = ('10.2.1.167', '10.2.2.12')
foreach ($TargetPortal in $TargetPortals) {New-IscsiTargetPortal
-TargetPortalAddress $TargetPortal}
```

```
$TargetPortals = ('10.2.1.167', '10.2.2.12')
foreach ($TargetPortal in $TargetPortals) {New-IscsiTargetPortal -TargetPortalAddress $TargetPortal}

InitiatorInstanceName :
InitiatorPortalAddress :
IsDataDigest           : False
IsHeaderDigest         : False
TargetPortalAddress    : 10.2.1.167
TargetPortalPortNumber : 3260
PSComputerName         :

InitiatorInstanceName :
InitiatorPortalAddress :
IsDataDigest           : False
IsHeaderDigest         : False
TargetPortalAddress    : 10.2.2.12
TargetPortalPortNumber : 3260
PSComputerName         :
```

## ベストプラクティス

- パフォーマンスを最適化するために、ターゲットインターフェイスごとに5つのiSCSIセッションを設定します。
- 全体的なiSCSIパフォーマンスが最大になるようにラウンドロビンポリシーを設定します。
- LUNをフォーマットするときは、パーティションの割り当て単位のサイズが64Kに設定されていることを確認します
  - 次のPowerShellコマンドを実行して、iSCSIセッションが保持されていることを確認します。

```
$targets = Get-IscsiTarget
foreach ($target in $targets)
{
Connect-IscsiTarget -IsMultipathEnabled $true -NodeAddress
$target.NodeAddress -IsPersistent $true
}
```

```
PS C:\windows\system32> Connect-IscsiTarget -NodeAddress (Get-IscsiTarget | select -ExpandProperty NodeAddress)

AuthenticationType : NONE
InitiatorInstanceName : ROOT\ISCSIPT\0000_0
InitiatorNodeAddress : iqn.1991-05.com.microsoft:awssqlprod01.cloudheroes.dom
InitiatorPortalAddress : 0.0.0.0
InitiatorSideIdentifier : 400001370000
IsConnected          : True
IsDataDigest         : False
IsDiscovered         : True
IsHeaderDigest       : False
IsPersistent         : True
NumberOfConnections  : 1
SessionIdentifier    : ffff9988350ff010-4000013700000012
TargetNodeAddress    : iqn.1992-08.com.netapp:sn.ea00ea2d1b1d11ec9de16f9cef731025:vs.3
TargetSideIdentifier : 0200
PSComputerName       :
```

- 次のPowerShellコマンドを使用してディスクを初期化します。

```
$disks = Get-Disk | where PartitionStyle -eq raw
foreach ($disk in $disks) {Initialize-Disk $disk.Number}
```

```
PS C:\Windows\system32> $disks = Get-Disk | where PartitionStyle -eq raw
foreach ($disk in $disks) {Initialize-Disk $disk.Number}
PS C:\Windows\system32> Get-Disk
```

Number	Friendly Name	Serial Number	HealthStatus	OperationalStatus	Total Size	Partition Style
0	AWS PVDISK	vo105d1c31fcb4c790ab	Healthy	Online	30 GB	MBR
1	NETAPP LUN C-Mode	1wB0p7RmR2s2	Healthy	Online	700 GB	GPT
2	NETAPP LUN C-Mode	1wB0p7RmR2s3	Healthy	Online	100 GB	GPT

c. PowerShellを使用して、Create PartitionコマンドとFormat Diskコマンドを実行します。

```
New-Partition -DiskNumber 1 -DriveLetter F -UseMaximumSize
Format-Volume -DriveLetter F -FileSystem NTFS -AllocationUnitSize
65536
New-Partition -DiskNumber 2 -DriveLetter G -UseMaximumSize
Format-Volume -DriveLetter G -FileSystem NTFS -AllocationUnitSize
65536
```

付録BのPowerShellスクリプトを使用して、ボリュームおよびLUNの作成を自動化できます。LUNは、SnapCenterを使用して作成することもできます。

ボリュームとLUNを定義したら、SnapCenterを設定してデータベース処理を実行できるようにする必要があります。

### SnapCenterの概要

NetApp SnapCenterは、ティア1エンタープライズアプリケーション向けの次世代データ保護ソフトウェアです。SnapCenterは、一元管理インターフェイスを備えているため、複数のデータベースやその他のアプリケーションワークロードのバックアップ、リカバリ、クローニングに関連する、複雑で時間のかかる手動プロセスを自動化して簡易化できます。SnapCenterは、ネットアップのSnapshot、NetApp SnapMirror、SnapRestore、NetApp FlexCloneなどのネットアップテクノロジーを活用しています。この統合により、IT部門は、ストレージインフラを拡張し、厳しいSLAコミットメントを満たし、企業全体の管理者の生産性を向上させることができます。

## SnapCenter サーバの要件

次の表に、Microsoft Windows ServerにSnapCenter Serverとプラグインをインストールするための最小要件を示します。

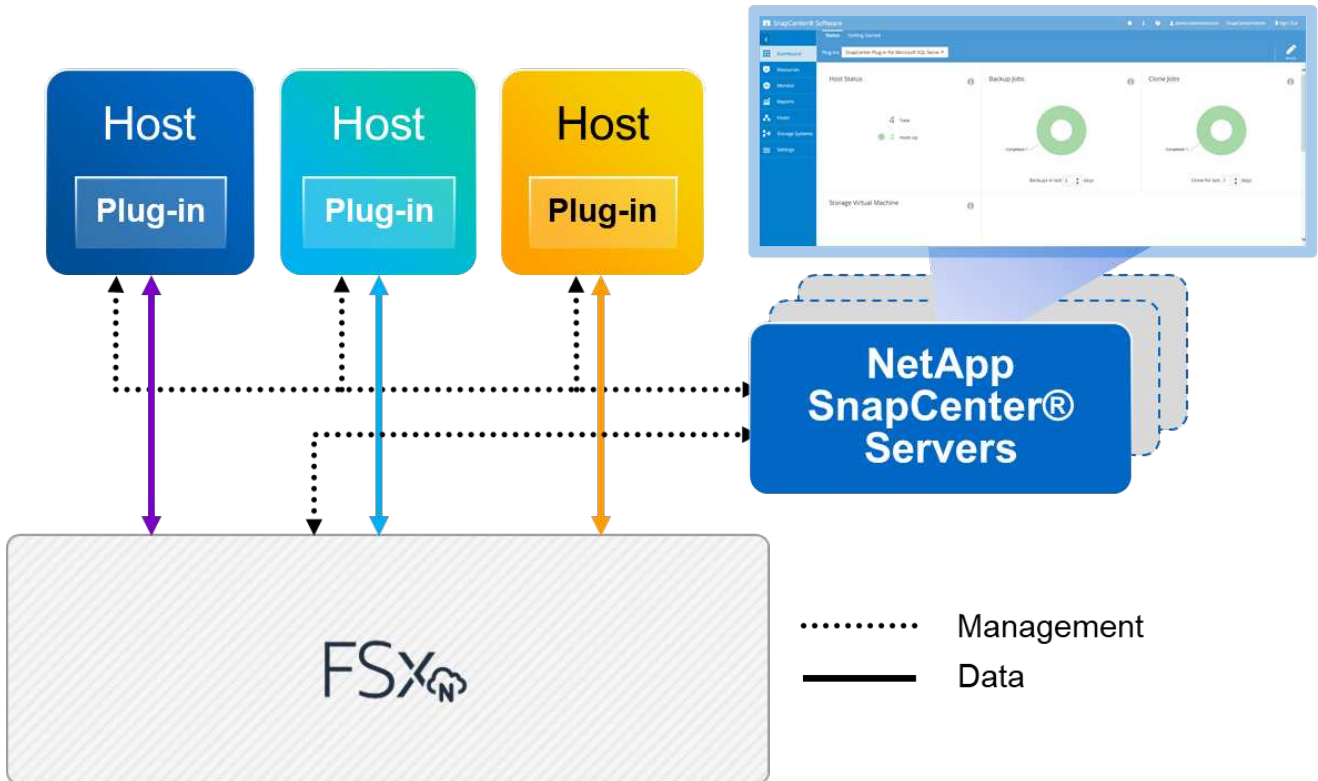
コンポーネント	要件
最小CPU数	4つのコア/vCPU
メモリ	最小構成：8GB推奨：32GB
ストレージスペース	インストール用の最小スペース：リポジトリ用に10GB以上のスペース：10GB
サポートされているオペレーティングシステム	<ul style="list-style-type: none"><li>• Windows Server 2012</li><li>• Windows Server 2012 R2</li><li>• Windows Server 2016</li><li>• Windows Server 2019</li></ul>
ソフトウェアパッケージ	<ul style="list-style-type: none"><li>• .NET 4.5.2以降</li><li>• Windows Management Framework (WMF) 4.0以降</li><li>• PowerShell 4.0以降</li></ul>

詳細については、を参照してください"[スペースとサイジングの要件](#)"。

バージョンの互換性については、を参照してください "[NetApp Interoperability Matrix Tool](#)"。



次の図に、SnapCenter でバックアップする場合のMicrosoft SQL Serverデータベースストレージレイアウトの作成に関する考慮事項を示します。



### ベストプラクティス

1. I/O負荷の高いクエリやサイズの大きいデータベース（500GBなど）を別のボリュームに配置すると、リカバリ時間が短縮されます。このボリュームは、別のジョブでバックアップすることも必要です。
2. 重要度が低い、またはI/O要件が低い中小規模のデータベースを1つのボリュームに統合します。多数のデータベースを同じボリュームにバックアップすると、保持する必要があるSnapshotコピー数が少なくなります。また、Microsoft SQL Serverインスタンスを統合して、同じボリュームを使用して作成するバックアップSnapshotコピーの数を制御することを推奨します。
3. テキスト関連のファイルとファイルストリーミング関連のファイルをすべて格納するために、別々のLUNを作成します。
4. Microsoft SQL Serverのログバックアップを保存する場合は、ホストごとに個別のLUNを割り当てます。
5. データベースサーバのメタデータ設定とジョブの詳細を格納するシステムデータベースが頻繁に更新されない。システムデータベースやtempdbは、別のドライブまたはLUNに配置してください。システムデータベースをユーザデータベースと同じボリュームに配置しないでください。ユーザデータベースのバックアップポリシーが異なり、システムデータベースのユーザデータベースのバックアップ頻度も同じではありません。
6. Microsoft SQL Server可用性グループの設定の場合は、レプリカのデータファイルとログファイルをすべてのノードの同一フォルダ構造に配置します。

ユーザデータベースレイアウトを別々のボリュームに分離することでパフォーマンスが向上するだけで

なく、バックアップとリストアに要する時間にも大きく影響します。データファイルとログファイルに別々のボリュームを配置すると、複数のユーザデータファイルをホストするボリュームに比べて、リストア時間が大幅に短縮されます。同様に、I/O負荷の高いアプリケーションを使用するユーザデータベースは、バックアップ時間が長くなる傾向があります。バックアップとリストアの方法については、本ドキュメントで後述します。



SQL Server 2012 (11.x) 以降、システムデータベース（マスター、モデル、MSDB、tempdb）、およびDatabase Engineユーザデータベースは、ストレージオプションとしてSMBファイルサーバとともにインストールできます。この環境は、スタンドアロンのSQL ServerとSQL Serverフェイルオーバークラスタのどちらのインストールでも使用できます。これにより、FSx ONTAPは、ボリューム容量、パフォーマンスの拡張性、データ保護機能など、パフォーマンスとデータ管理のすべての機能で使用でき、SQL Serverはこれらの機能を活用できます。アプリケーションサーバが使用する共有には、継続的可用性が設定されている必要があります。また、ボリュームはNTFSセキュリティ形式で作成する必要があります。NetApp SnapCenterは、FSx ONTAPからSMB共有に配置されたデータベースでは使用できません。



SnapCenter を使用してバックアップを実行しないSQL Serverデータベースについては、データファイルとログファイルを別々のドライブに配置することを推奨します。データを同時に更新して要求するアプリケーションでは、ログファイルに書き込み負荷がかかり、（アプリケーションによっては）データファイルの読み取り/書き込み負荷が高くなります。データを取得する場合、ログファイルは必要ありません。そのため、データの要求は、そのドライブに配置されたデータファイルから満たすことができます。



新しいデータベースを作成するときは、データとログ用に別々のドライブを指定することを推奨します。データベース作成後にファイルを移動するには、データベースをオフラインにする必要があります。Microsoftのその他の推奨事項については、「データファイルとログファイルを別々のドライブに配置する」をご覧ください。

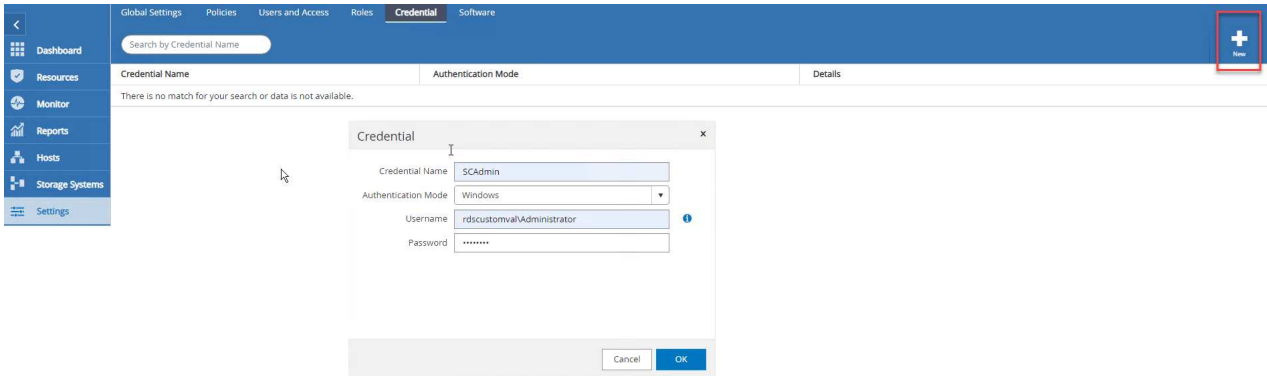


## SnapCenter のインストールとセットアップ

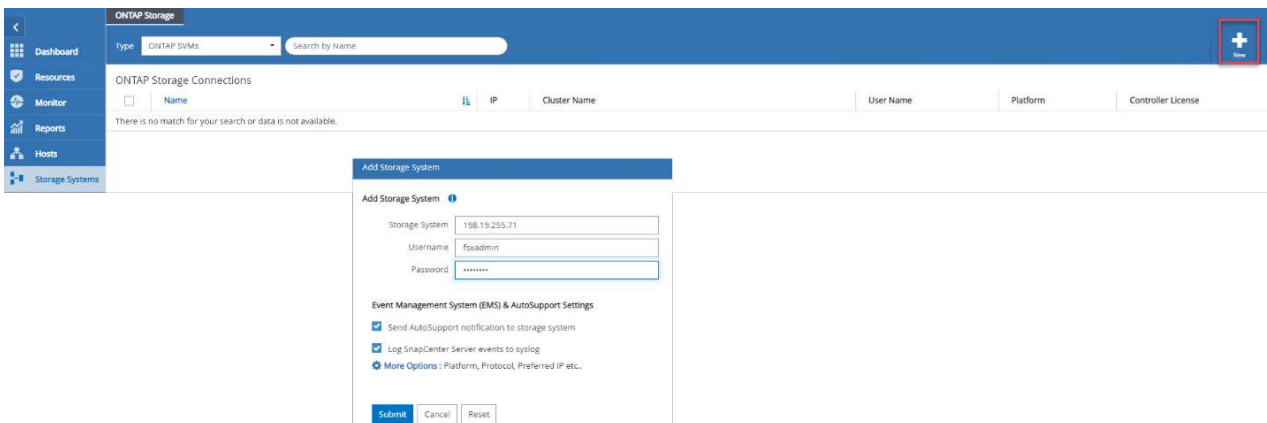
と "SnapCenter Plug-in for Microsoft SQL Serverをインストールしています"に従って、 "SnapCenterサーバのインストール"SnapCenterをインストールしてセットアップします。

SnapCenter をインストールしたら、次の手順を実行してセットアップします。

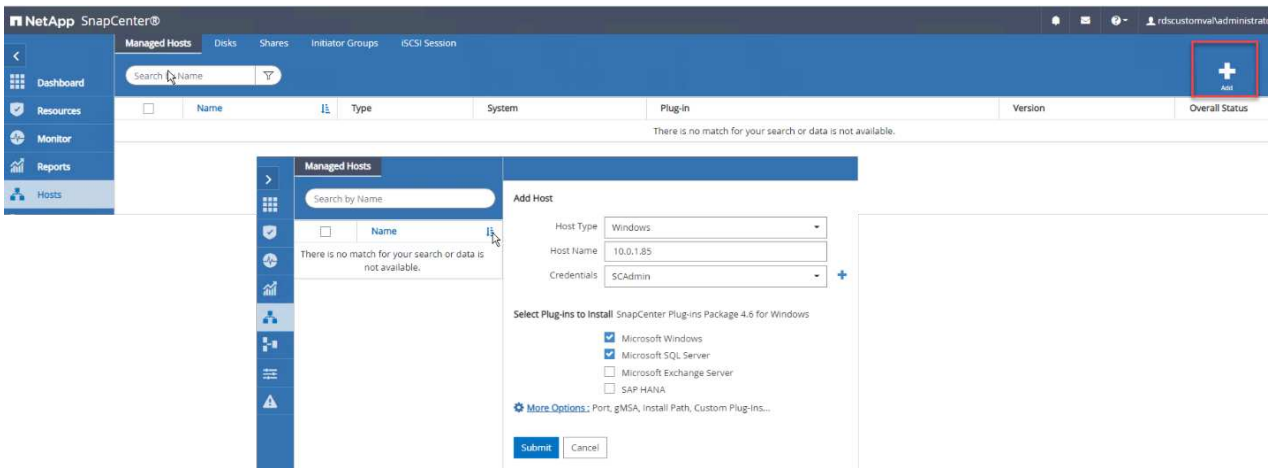
1. クレデンシャルを設定するには、\* Settings > New \*を選択し、クレデンシャル情報を入力します。



2. [Storage Systems]>[New]を選択してストレージシステムを追加し、でFSx ONTAPの適切なストレージ情報を入力します。



3. [Hosts>\*Add\*]を選択してホストを追加し、ホスト情報を入力します。SnapCenterは、WindowsおよびSQL Serverプラグインを自動的にインストールします。このプロセスには時間がかかることがあります。



すべてのプラグインをインストールしたら、ログディレクトリを設定する必要があります。トランザクションログバックアップが格納された場所を指定します。ホストを選択してログディレクトリを設定し、[ログディレクトリを設定]を選択します。



SnapCenterは、ホストログディレクトリを使用してトランザクションログバックアップデータを格納します。これはホストおよびインスタンスレベルです。SnapCenterで使用する各SQL Serverホストには、ログバックアップを実行するように設定されたホストログディレクトリが必要です。SnapCenterにはデータベースリポジトリがあるため、バックアップ、リストア、クローニングの処理に関連するメタデータは中央のデータベースリポジトリに格納されます。

ホストログディレクトリのサイズは、次のように計算します。

ホストログディレクトリのサイズ = (システムデータベースサイズ + (最大DB LDFサイズ × 日次ログ変更率%)) × (Snapshotコピー保持率) ÷ (1 - LUNオーバーヘッドスペース%)

ホストログディレクトリのサイジングの計算式では、次のことを前提としています。

- tempdbデータベースを含まないシステムデータベースのバックアップ
- 10%のLUNオーバーヘッド・スペースホスト・ログ・ディレクトリを専用のボリュームまたはLUNに配置します。ホストログディレクトリのデータ量は、バックアップのサイズとバックアップを保持する日数によって異なります。

**Managed Hosts**

Search by Name

<input type="checkbox"/>	Name
<input checked="" type="checkbox"/>	RDSAMAZ-FFIDFMR.rdscustomval.com

**Host Details**

Host Name RDSAMAZ-FFIDFMR.rdscustomval.com

Host IP 10.0.1.56

Overall Status ● Configure log directory

Host Type Windows

System Stand-alone

Credentials SCAdmin

Plug-ins SnapCenter Plug-ins package 4.6.0.6965 for Windows

- ✓ Microsoft Windows
- ✓ Microsoft SQL Server [Remove](#) [Configure log directory](#)

[More Options](#) : Port, gMSA, Install Path, Add Plug-Ins...

[Submit](#) [Cancel](#) [Reset](#)

LUNがすでにプロビジョニングされている場合は、ホストログディレクトリを表すマウントポイントを選択できます。

**Configure Plug-in for SQL Server** ×

Configure the log backup directory for RDSAMAZ-FFIDFMR.rdscustomval.com

Configure host log directory

Host log directory  [Browse](#)

Choose directory on NetApp Storage

- RDSAMAZ-FFIDFMR.rdscustomval.com
  - D:\FSxN\Data\
  - D:\FSxN\HLD\
  - D:\FSxN\Log\'

[Save](#) [Close](#)

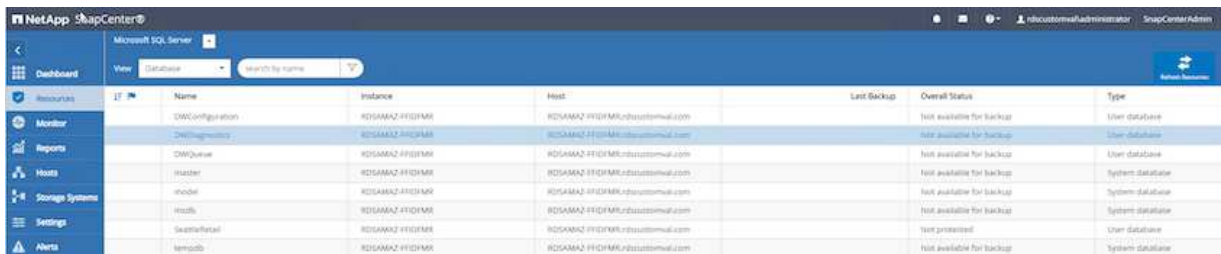
これで、SQL Serverのバックアップ、リストア、クローニングの処理を実行する準備ができました。

## SnapCenter を使用してデータベースをバックアップする

データベースとログファイルをFSX ONTAP LUNに配置したら、SnapCenter を使用してデータベースをバックアップできます。フルバックアップを作成するには、次のプロセスを使用します。

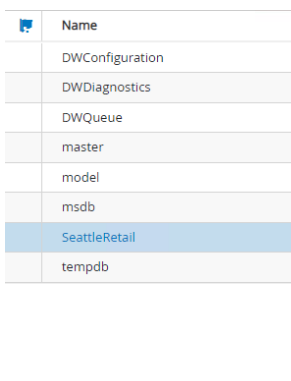
### ベストプラクティス

- SnapCenter では、バックアップをスケジュールする頻度など、RPOをバックアップ頻度として指定し、データ損失を最大数分まで削減できます。SnapCenter では、バックアップを5分ごとの頻度で実行するようにスケジュールを設定できます。ただし、場合によっては、ピークトランザクション時間内や、データ変更率が所定の時間内に高くない時間帯に、バックアップが5分以内に完了しないことがあります。フルバックアップではなくトランザクションログを頻繁にバックアップするようにスケジュールを設定することを推奨します。
- RPOとRTOには、数多くのアプローチがあります。このバックアップ方法に代わるもう1つの方法は、間隔の異なるデータとログのバックアップポリシーを用意することです。たとえば、SnapCenter では、ログバックアップを15分間隔で、データバックアップを6時間間隔で実行するようにスケジュールします。
- Snapshotを最適化するためのバックアップ設定および管理するジョブの数には、リソースグループを使用します。
  - a. [リソース]を選択し、左上のドロップダウン・メニューから[Microsoft SQL Server]を選択します。[\*リソースを更新]を選択します。



IT	Name	Instance	Host	Last Backup	Overall Status	Type
	DWCconfiguration	RDSAMAZ-F1DFMR	RDSAMAZ-F1DFMR.uscustom1.com		Not available for backup	User database
	DWDiagnostics	RDSAMAZ-F1DFMR	RDSAMAZ-F1DFMR.uscustom1.com		Not available for backup	User database
	DWQueue	RDSAMAZ-F1DFMR	RDSAMAZ-F1DFMR.uscustom1.com		Not available for backup	User database
	master	RDSAMAZ-F1DFMR	RDSAMAZ-F1DFMR.uscustom1.com		Not available for backup	System database
	model	RDSAMAZ-F1DFMR	RDSAMAZ-F1DFMR.uscustom1.com		Not available for backup	System database
	msdb	RDSAMAZ-F1DFMR	RDSAMAZ-F1DFMR.uscustom1.com		Not available for backup	System database
	SeattleRetail	RDSAMAZ-F1DFMR	RDSAMAZ-F1DFMR.uscustom1.com		Not prepared	User database
	tempdb	RDSAMAZ-F1DFMR	RDSAMAZ-F1DFMR.uscustom1.com		Not available for backup	System database

- b. バックアップするデータベースを選択し、\* Next および (\*) を選択してポリシーを追加します（作成していない場合）。新しいポリシーを作成するには、「\*新しいSQL Serverバックアップポリシー」に従います。



Name
DWCconfiguration
DWDiagnostics
DWQueue
master
model
msdb
SeattleRetail
tempdb



Select one or more policies and configure schedules

Full Backup  ⓘ

Configure schedules for selected policies

Policy ⓘ	Applied Schedules	Configure Schedules
Full Backup	None	To schedule operations select a policy that has the appropriate schedule associated, or modify the selected policy to allow schedules.

- c. 必要に応じて、検証サーバを選択します。このサーバは、フルバックアップの作成後にSnapCenterでDBCC CHECKDBを実行するサーバです。[次へ\*]をクリックして通知を確認し、[概要]を選択します。確認したら、[完了]をクリックします。

Name
DWConfiguration
DWDiagnostics
DWQueue
master
model
msdb
SeattleRetail
tempdb

1 Resource    2 Policies    3 Verification    4 Notification    5 Summary

Select the verification servers

Verification server:

Configure verification schedules

Policy	Schedule Type	Applied Schedules	Configure Schedules
There is no match for your search or data is not available.			

- d. [今すぐバックアップする]をクリックして、バックアップをテストします。ポップアップ・ウィンドウで、\*バックアップ\*を選択します。

### Backup

Create a backup for the selected resource

Resource Name:

Policy:  ⓘ

Verify after backup

- e. バックアップが完了したことを確認するには、\* Monitor \*を選択します。

ID	Status	Name	Start date	End date	Owner
18	✓	Backup of Resource Group 'RDSMAAZ-FIDMR_SeattleRetail' with policy 'Full Backup'	03/29/2022 1:47:30 AM	03/29/2022 1:48:41 AM	RDS\CUSTOMER\Administrator
19	✓	Create Resource Group 'RDSMAAZ-FIDMR_SeattleRetail'	03/29/2022 1:45:04 AM	03/29/2022 1:45:26 AM	RDS\CUSTOMER\Administrator
20	✓	Create Policy 'Full Backup'	03/29/2022 1:41:37 AM	03/29/2022 1:41:48 AM	RDS\CUSTOMER\Administrator
21	✓	Discover resources for all hosts	03/29/2022 1:38:12 AM	03/29/2022 1:38:17 AM	RDS\CUSTOMER\Administrator

## ベストプラクティス

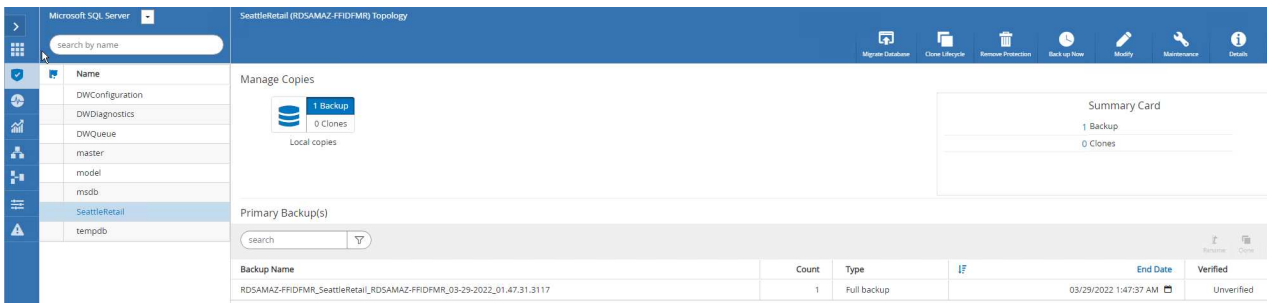
- リストア・プロセス中にSnapCenter がすべてのバックアップ・ファイルを読み取って自動的に順序どおりにリストアできるように、SnapCenter からトランザクション・ログ・バックアップをバックアップします。
- サードパーティ製品をバックアップに使用する場合は、ログシーケンスの問題を回避するためにSnapCenter でバックアップをコピーを選択し、本番環境にロールアップする前にリストア機能をテストします。

## SnapCenter を使用してデータベースをリストアします

FSX ONTAP をEC2上のSQL Serverとともに使用する主な利点の1つは各データベース・レベルで迅速かつ詳細なリストアを実行できることです

個々のデータベースを特定の時点またはSnapCenter で最新の状態にリストアするには、次の手順を実行します。

1. Resources (リソース) を選択し、リストアするデータベースを選択します。



2. データベースのリストアに使用するバックアップ名を選択し、リストアを選択します。
3. 「\* Restore \*」ポップアップ・ウィンドウに従って、データベースを復元します。
4. 「\* Monitor \*」を選択して、リストア・プロセスが正常に完了したことを確認します。



SnapCenter では、リソースグループ内のインスタンスまたはインスタンスのグループに含まれる、サイズの大きなデータベースをバックアップできます。データベースのサイズは、バックアップ時間の主要な要因ではありません。バックアップの所要時間は、ボリュームあたりのLUN数、Microsoft SQL Server の負荷、インスタンスあたりのデータベースの総数、および具体的にはI/O帯域幅と使用量によって異なります。インスタンスまたはリソースグループからデータベースをバックアップするようにポリシーを設定する際には、Snapshotコピーごとにバックアップするデータベースの最大数をホストあたり100に制限することを推奨します。Snapshotコピーの総数が、1、023個のコピー制限を超えないようにしてください。

また、各データベースまたはインスタンスに対して複数のジョブを作成するのではなく、データベース数をグループ化して、バックアップジョブを並行して実行するように制限することを推奨します。バックアップ期間のパフォーマンスを最適化するには、一度にバックアップできるデータベース数を100個以下にするようにバックアップジョブの数を減らします。

前述したように、バックアッププロセスではI/O使用率が重要な要素です。データベースのI/O処理がすべて完了するまで、バックアッププロセスを休止する必要があります。大量のI/O処理が発生しているデータベースは、別のバックアップ時間に保留するか、バックアップ対象の同じリソースグループ内の他のリソースへの影響を避けるために、他のバックアップジョブから分離する必要があります。

インスタンスあたり200のデータベースをホストするMicrosoft SQL Serverホストが6つある環境では、ホストごとに4つのLUNとボリュームごとに1つのLUNが作成されていると仮定した場合、Snapshotコピーごとにバックアップできるデータベースの最大数を100に設定したフルバックアップポリシーを設定します。各インスタンスに200個のデータベースがあると、200個のデータファイルが2つのLUNに均等に分散され、200個のログファイルがボリュームあたり100個のLUNに均等に分散されます。

3つのリソースグループを作成して3つのバックアップジョブをスケジュールします。各グループには合計400個のデータベースが含まれます。

3つのバックアップジョブをすべて同時に実行すると、1、200個のデータベースがバックアップされます。サーバの負荷とI/O使用状況によっては、各インスタンスの開始時間と終了時間が異なる場合があります。この場合、合計24個のSnapshotコピーが作成されます。

ネットアップでは、フルバックアップに加えて、重要なデータベースに対してトランザクションログバックアップを設定することを推奨しています。データベースプロパティが完全復旧モデルに設定されていることを確認します。

#### ベストプラクティス

1. tempdbデータベースは一時的なデータを含んでいるため、バックアップには含めないでください。tempdbは、Snapshotコピーを作成しないストレージシステムボリュームにあるLUNまたはSMB共有に配置します。
2. I/O負荷の高いアプリケーションを使用するMicrosoft SQL Serverインスタンスは、別のバックアップジョブに分離して、他のリソースの全体的なバックアップ時間を短縮する必要があります。
3. 同時にバックアップするデータベースセットは、最大で約100個に制限し、残りのデータベースバックアップセットはずらして配置することで、同時にバックアップ処理が行われないようにします。
4. Microsoft SQL Serverインスタンスで新規データベースが作成されるたびに、SnapCenter は自動的に新規データベースをバックアップ対象と見なします。そのため、リソースグループでは、複数のデータベースではなくMicrosoft SQL Serverインスタンス名を使用します。
5. データベースリカバリモデルをフルリカバリモデルに変更するなど、データベース設定を変更した場

合は、すぐにバックアップを実行して最新の状態へのリストア処理を実行してください。

6. SnapCenter では、SnapCenter の外部で作成されたトランザクションログバックアップをリストアできません。
7. FlexVol ボリュームをクローニングするときは、クローンメタデータ用の十分なスペースがあることを確認してください。
8. データベースをリストアするときは、ボリュームに十分なスペースがあることを確認してください。
9. 少なくとも週に1回は、システムデータベースの管理とバックアップを行うための個別のポリシーを作成します。



## SnapCenter を使用して、データベースをクローニングする

開発/テスト環境の別の場所にデータベースをリストアしたり、ビジネス分析目的でコピーを作成したりする場合、ネットアップのベストプラクティスは、クローニング方法論を利用して同じインスタンスまたは代替インスタンス上にデータベースのコピーを作成することです。

FSx ONTAP環境でホストされたiSCSIディスクに500GBのデータベースをクローニングする場合、通常は5分未満で完了します。クローニングが完了したら、クローニングしたデータベースに対して必要なすべての読み取り/書き込み処理を実行できます。ほとんどの時間はディスクスキャン (diskpart) に費やされています。ネットアップのクローニング手順は、データベースのサイズに関係なく、通常は2分未満で完了します。

データベースのクローニングは、デュアル方式で実行できます。最新のバックアップからクローンを作成することも、セカンダリインスタンスで最新のコピーを利用できるクローンライフサイクル管理を使用することもできます。

SnapCenter を使用すると、必要なディスクにクローンコピーをマウントして、セカンダリインスタンスのフォルダ構造の形式を維持し、引き続きバックアップジョブのスケジュールを設定できます。

同じインスタンス内の新しいデータベース名でデータベースをクローニングします

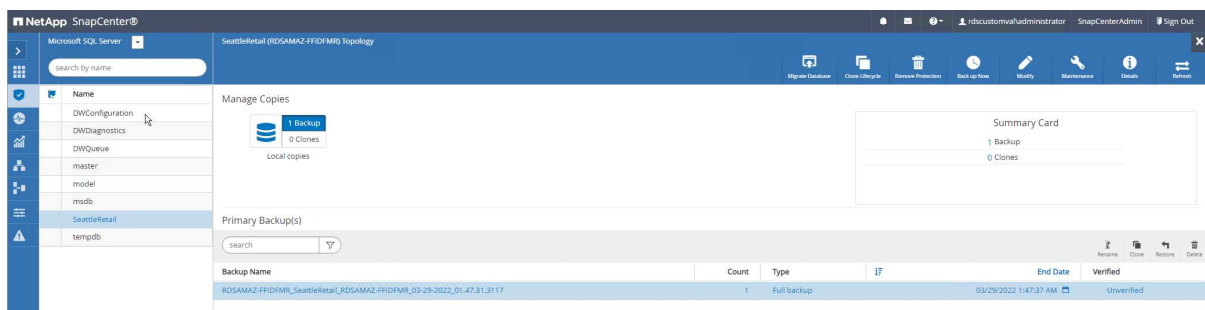
EC2で実行されている同じSQL Serverインスタンス内の新しいデータベース名にデータベースをクローニングするには、次の手順を実行します。

1. [リソース]を選択し、次にクローンを作成する必要があるデータベースを選択します。
2. クローンを作成するバックアップ名を選択し、Cloneを選択します。
3. バックアップ・ウィンドウに表示されるクローンの手順に従って、クローン・プロセスを完了します。
4. Monitorを選択して、クローニングが完了したことを確認します。

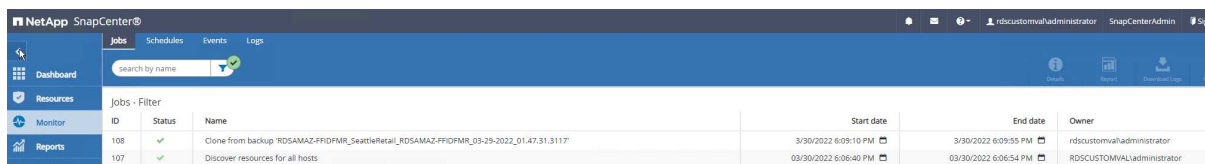
## EC2で実行されている新しいSQL Serverインスタンスにデータベースをクローニングします

EC2で実行する新しいSQL Serverインスタンスにデータベースをクローニングするには、次の手順を実行します。

1. 同じVPC内のEC2に新しいSQL Serverを作成します。
2. iSCSIプロトコルとMPIOを有効にし、セクション「SQL Server用のボリュームとLUNの作成」の手順3と4に従ってFSx ONTAPへのiSCSI接続をセットアップします。
3. 「SnapCenter のインストールとセットアップ」セクションの手順3に従って、EC2上の新しいSQL ServerをSnapCenter に追加します。
4. リソース／インスタンスを表示を選択し、リソースを更新を選択します。
5. [リソース]を選択し、次にクローンを作成するデータベースを選択します。
6. クローンを作成するバックアップ名を選択し、Cloneを選択します。



7. バックアップからのクローン作成の手順に従い、EC2に新しいSQL Serverインスタンスを指定し、インスタンス名を指定してクローンプロセスを終了します。
8. Monitorを選択して、クローニングが完了したことを確認します。



このプロセスの詳細については、次のビデオをご覧ください。

[EC2で実行されている新しいSQL Serverインスタンスにデータベースをクローニングします](#)

付録

## 付録A：クラウド形成テンプレートで使用するYAMLファイル

AWSコンソールのクラウド形成テンプレートでは、次の.yamlファイルを使用できます。

- "<https://github.com/NetApp/fsxn-iscsisetup-cft>"

PowerShellを使用してiSCSI LUNの作成とNetApp SnapCenterのインストールを自動化するには、からリポジトリのクローンを作成 "[このGitHubリンク](#)"します。

次のスクリプトを使用して、ボリュームとLUNをプロビジョニングし、上記の手順に基づいてiSCSIをセットアップします。PowerShellスクリプトには次の2つがあります。

- `_EnableMPIO.ps1`

```
Function Install_MPIO_ssh {
    $hostname = $env:COMPUTERNAME
    $hostname = $hostname.Replace('-', '_')

    #Add schedule action for the next step
    $path = Get-Location
    $path = $path.Path + '\2_CreateDisks.ps1'
    $arg = '-NoProfile -WindowStyle Hidden -File ' + $path
    $schAction = New-ScheduledTaskAction -Execute "Powershell.exe"
    -Argument $arg
    $schTrigger = New-ScheduledTaskTrigger -AtStartup
    $schPrincipal = New-ScheduledTaskPrincipal -UserId "NT AUTHORITY
\SYSTEM" -LogonType ServiceAccount -RunLevel Highest
    $return = Register-ScheduledTask -Action $schAction -Trigger
    $schTrigger -TaskName "Create Vols and LUNs" -Description "Scheduled
Task to run configuration Script At Startup" -Principal $schPrincipal
    #Install -Module PosH-SSH
    Write-host 'Enable MPIO and SSH for PowerShell' -ForegroundColor
Yellow
    $return = Find-PackageProvider -Name 'Nuget' -ForceBootstrap
    -IncludeDependencies
    $return = Find-Module PoSH-SSH | Install-Module -Force
    #Install Multipath-IO with PowerShell using elevated privileges in
Windows Servers
    Write-host 'Enable MPIO' -ForegroundColor Yellow
    $return = Install-WindowsFeature -name Multipath-IO -Restart
}
Install_MPIO_ssh
Remove-Item -Path $MyInvocation.MyCommand.Source
```

- `_CreateDisks.ps1`

```
....
#Enable MPIO and Start iSCSI Service
Function PrepISCSI {
    $return = Enable-MSDSMAutomaticClaim -BusType iSCSI
    #Start iSCSI service with PowerShell using elevated privileges in
Windows Servers
```

```

$return = Start-service -Name msiscsi
$return = Set-Service -Name msiscsi -StartupType Automatic
}
Function Create_igroup_vols_luns ($fsxN){
    $hostname = $env:COMPUTERNAME
    $hostname = $hostname.Replace('-', '_')
    $volsluns = @()
    for ($i = 1;$i -lt 10;$i++){
        if ($i -eq 9){
            $volsluns
+=(@{volname=('v_'+$hostname+'_log');volsize=$fsxN.logvolsize;lunname=('l_'+$hostname+'_log');lunsize=$fsxN.loglunsize})
        } else {
            $volsluns
+=(@{volname=('v_'+$hostname+'_data'+[string]$i);volsize=$fsxN.datavolsize;lunname=('l_'+$hostname+'_data'+[string]$i);lunsize=$fsxN.datalunsize})
        }
    }
    $secStringPassword = ConvertTo-SecureString $fsxN.password
-AsPlainText -Force
    $credObject = New-Object System.Management.Automation.PSCredential
($fsxN.login, $secStringPassword)
    $igroup = 'igrp_'+$hostname
    #Connect to FSx N filesystem
    $session = New-SSHSession -ComputerName $fsxN.svmip -Credential
$credObject -AcceptKey:$true
    #Create igroup
Write-host 'Creating igroup' -ForegroundColor Yellow
    #Find Windows initiator Name with PowerShell using elevated
privileges in Windows Servers
    $initport = Get-InitiatorPort | select -ExpandProperty NodeAddress
    $sshcmd = 'igroup create -igroup ' + $igroup + ' -protocol iscsi
-ostype windows -initiator ' + $initport
    $ret = Invoke-SSHCommand -Command $sshcmd -SSHSession $session
    #Create vols
Write-host 'Creating Volumes' -ForegroundColor Yellow
    foreach ($vollun in $volsluns){
        $sshcmd = 'vol create ' + $vollun.volname + ' -aggregate agr1
-size ' + $vollun.volsize #+ ' -vserver ' + $vserver
        $return = Invoke-SSHCommand -Command $sshcmd -SSHSession
$session
    }
    #Create LUNs and mapped LUN to igroup
Write-host 'Creating LUNs and map to igroup' -ForegroundColor
Yellow

```

```

    foreach ($vollun in $volsluns){
        $ssshcmd = "lun create -path /vol/" + $vollun.volname + "/" +
$vollun.lunname + " -size " + $vollun.lunsize + " -ostype Windows_2008
" #-vserver " +$vserver
        $return = Invoke-SSHCommand -Command $ssshcmd -SSHSession
$session
        #map all luns to igroup
        $ssshcmd = "lun map -path /vol/" + $vollun.volname + "/" +
$vollun.lunname + " -igroup " + $igroup
        $return = Invoke-SSHCommand -Command $ssshcmd -SSHSession
$session
    }
}
Function Connect_iSCSI_to_SVM ($TargetPortals){
    Write-host 'Online, Initialize and format disks' -ForegroundColor
Yellow
    #Connect Windows Server to svm with iSCSI target.
    foreach ($TargetPortal in $TargetPortals) {
        New-IscsiTargetPortal -TargetPortalAddress $TargetPortal
        for ($i = 1; $i -lt 5; $i++){
            $return = Connect-IscsiTarget -IsMultipathEnabled $true
-IsPersistent $true -NodeAddress (Get-iscsiTarget | select
-ExpandProperty NodeAddress)
        }
    }
}
Function Create_Partition_Format_Disks{

    #Create Partion and format disk
    $disks = Get-Disk | where PartitionStyle -eq raw
    foreach ($disk in $disks) {
        $return = Initialize-Disk $disk.Number
        $partition = New-Partition -DiskNumber $disk.Number
-AssignDriveLetter -UseMaximumSize | Format-Volume -FileSystem NTFS
-AllocationUnitSize 65536 -Confirm:$false -Force
        # $return = Format-Volume -DriveLetter $partition.DriveLetter
-FileSystem NTFS -AllocationUnitSize 65536
    }
}
Function UnregisterTask {
    Unregister-ScheduledTask -TaskName "Create Vols and LUNs"
-Confirm:$false
}
Start-Sleep -s 30
$fsxN = @{svmip ='198.19.255.153';login =
'vsadmin';password='net@pp11';datavolsize='10GB';datalunsize='8GB';logv

```

```
olsize='8GB';loglunsize='6GB'}
$TargetPortals = ('10.2.1.167', '10.2.2.12')
PrepISCSI
Create_igroup_vols_luns $fsxN
Connect_iSCSI_to_SVM $TargetPortals
Create_Partition_Format_Disks
UnregisterTask
Remove-Item -Path $MyInvocation.MyCommand.Source
.....
```

ファイルを最初に実行する `EnableMPIO.ps1` と、サーバのリブート後に2番目のスクリプトが自動的に実行されます。これらのPowerShellスクリプトは、SVMのクレデンシャルアクセスが原因で実行されたあとで削除できます。

## 詳細情報の入手方法

- Amazon FSx ONTAP

["https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html"](https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html)

- FSx ONTAP入門

["https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/getting-started.html"](https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/getting-started.html)

- SnapCenter インターフェイスの概要

<https://www.youtube.com/watch?v=IVEBF4kV6Ag&t=0s>

- SnapCenter ナビゲーションペインのオプションを確認します

[https://www.youtube.com/watch?v=\\_IDKt-koySQ](https://www.youtube.com/watch?v=_IDKt-koySQ)

- SnapCenter 4.0 for SQL Serverプラグインをセットアップします

<https://www.youtube.com/watch?v=MopbUFSdHKE>

- SnapCenter とSQL Serverプラグインを使用したデータベースのバックアップおよびリストア方法

[https://www.youtube.com/watch?v=K343qPD5\\_Ys](https://www.youtube.com/watch?v=K343qPD5_Ys)

- SnapCenter とSQL Serverプラグインを使用してデータベースをクローニングする方法

<https://www.youtube.com/watch?v=ogEc4DkGv1E>

## Azure NetApp Files 上の SQL Server

TR-4897 : 『SQL Server on Azure NetApp Files - Real Deployment View』

このドキュメントでは、Azure NetApp Files で Azure 仮想マシンを利用して SQL

## Server Always On 可用性グループ（AOAG）をリアルタイムで導入する方法について説明します。

ネットアップ、Niyaz Mohamed

IT 組織は絶えず変化しています。Gartner のレポートでは、すべてのデータベースのほぼ 75% が 2022 年までにクラウドベースストレージが必要になると報告されています。Microsoft SQL Server は、業界をリードするリレーショナルデータベース管理システム（RDBMS）として、Windows プラットフォームで設計されたアプリケーションや組織に最適です。エンタープライズリソースプランニング（ERP）から分析、コンテンツ管理まで、SQL Server に依存します。SQL Server は、大規模なデータセットを管理する方法を変革し、アプリケーションを強化して、スキーマやクエリのパフォーマンスの要求に対応できるようにしました。

ほとんどの IT 組織は、クラウドファーストのアプローチを採用しています。変革フェーズにあるお客様は、現在の IT 環境を評価し、評価と調査の演習に基づいてデータベースワークロードをクラウドに移行します。柔軟性 / バースト性、データセンターの終了、データセンターの統合、サポート終了シナリオ、合併、合併など、お客様をクラウドへ移行させる要因には次のものがあります。買収など。移行の理由は、組織ごとの優先事項と、それぞれのビジネスの優先事項によって異なります。クラウドに移行する際には、SQL Server データベースクラウドの導入を有効に活用するために、適切なクラウドストレージを選択することが非常に重要です。

### ユースケース

SQL Server 環境を Azure に移行し、SQL Server を Azure の膨大なプラットフォームサービス（PaaS）機能（Azure Data Factory、Azure IoT Hub、Azure Machine Learning など）と統合することで、デジタル変革をサポートするための大きなビジネス価値が生まれます。また、クラウドを採用することで、各事業部門は、CAPEX モデルや従来のプライベートクラウドモデルに頼らずに、生産性に重点を置き、新機能や拡張機能（DevTest ユースケース）をより迅速に提供することができます。このドキュメントでは、Azure NetApp Files で Azure 仮想マシンを利用して SQL Server Always On 可用性グループ（AOAG）をリアルタイムで導入する方法について説明します。

Azure NetApp Files は、継続的な可用性が確保されたファイル共有を備えたエンタープライズクラスのストレージを提供します。SQL Server の本番用データベースの SMB ファイル共有には、継続的な可用性を備えた共有が必要です。これにより、コントローラのアップグレードや障害などのシステム停止を伴うシナリオにおいて、ノードは常にデータベースストレージにアクセスできます。継続的な可用性が確保されたファイル共有により、ストレージノード間でデータをレプリケートする必要がなくなります。Azure NetApp Files は、SMB 3.0 のスケールアウト、永続的ハンドル、透過的なフェイルオーバー機能を使用して、計画的停止と計画外停止の間のノンストップオペレーション（NDO）をサポートします。これには、多くの管理タスクが含まれます。

クラウドへの移行を計画する場合は、常に最適な使用方法を評価する必要があります。アプリケーション移行で最も一般的かつ簡単なアプローチはリホスト（リフトアンドシフトとも呼ばれます）です。このドキュメントの例では、リホスト方法を使用しています。Azure NetApp Files を使用した Azure 仮想マシン上の SQL Server では、オンプレミスのハードウェアを管理しなくても、クラウド上で SQL Server のフルバージョンを使用できます。SQL Server 仮想マシン（VM）は、従量課金制でもライセンスコストを簡易化し、開発、テスト、環境の更新シナリオ向けに柔軟性とバースト性の高い機能を提供します。

### 考慮すべき要因

このセクションでは、クラウドで Azure NetApp Files を SQL Server に使用する場合に考慮する必要があるさまざまな問題について説明します。



## VMパフォーマンス

パブリッククラウドのリレーショナルデータベースのパフォーマンスを最適化するには、適切な VM サイズを選択することが重要です。Microsoft では、オンプレミスサーバ環境の SQL Server と同じデータベースパフォーマンス調整オプションを引き続き使用することを推奨しています。SQL Serverワークロードのパフォーマンスを最適化するには、VMサイズを使用します **"メモリの最適化"**。既存の導入環境のパフォーマンスデータを収集し、適切なインスタンスを選択しながら RAM と CPU の利用率を確認します。ほとんどの導入環境では、D、E、または M シリーズのいずれかを選択できます。

- 注：\*
- SQL Server ワークロードのパフォーマンスを最大限に高めるには、メモリに最適化された VM サイズを使用します。
- ネットアップと Microsoft は、適切なメモリと VCORE の比率に基づいてインスタンスタイプを選択する前に、ストレージのパフォーマンス要件を特定することを推奨しています。これは、適切なネットワーク帯域幅を備えた低いインスタンスタイプを選択して、VM のストレージスループットの制限に克服するのにも役立ちます。

## VM の冗長性

冗長性と高可用性を高めるには、SQL Server VMを同一または異なる **"可用性ゾーン"**VMに配置する必要があります **"可用性セット"**。Azure VM を作成する場合は、アベイラビリティセットとアベイラビリティゾンのどちらかを設定する必要があります。Azure VM を両方に含めることはできません。

## 高可用性

高可用性を実現するには、SQL Server AOAG または Always On フェイルオーバークラスティンスタンス（FCI）を構成することを推奨します。AOAG の場合、これには仮想ネットワーク内の Azure Virtual Machine 上の SQL Server の複数のインスタンスが含まれます。データベースレベルで高可用性が必要な場合は、SQL Server 可用性グループを設定することを検討してください。

## ストレージ構成

Microsoft SQL Server では、ストレージオプションとして SMB ファイル共有を導入できます。SQL Server 2012 以降、システムデータベース（マスター、モデル、msdb、または tempdb）、およびユーザーデータベースは、ストレージオプションとして Server Message Block（SMB；サーバメッセージブロック）ファイルサーバとともにインストールできます。この環境は、SQL Server のスタンドアロンと SQL Server FCI の両方に対応しています。



SQL Server データベース用のファイル共有ストレージでは、継続的可用性がサポートされている必要があります。これにより、ファイル共有データに中断なくアクセスできます。

Azure NetApp Files は、あらゆる要求の厳しいワークロードに対応できる高性能なファイルストレージを提供し、ブロックストレージソリューションに比べて SQL Server の TCO を削減します。ブロックストレージでは、VM の I/O およびディスク処理の帯域幅に制限があり、ネットワーク帯域幅の制限だけが Azure NetApp Files に適用されます。つまり、Azure NetApp Files には VM レベルの I/O 制限は適用されません。これらの I/O 制限がない場合、Azure NetApp Files に接続された小規模な VM で SQL Server を実行することも、はるかに大規模な VM で SQL Server を実行することもできます。Azure NetApp Files は、コンピューティングとソフトウェアのライセンスコストを削減することで、SQL Server の導入コストを削減します。Azure NetApp Filesを使用してSQL Serverを導入する場合の詳細なコスト分析とパフォーマンス上のメリットについては、[を参照して "Azure NetApp Files for SQL Server の導入のメリット"](#)ください。

Azure NetApp Files for SQL Server を使用する利点は次のとおりです。

- Azure NetApp Files を使用すると、インスタンスを小さくしてコンピューティングコストを削減できます。
- また、Azure NetApp Files はソフトウェアライセンスコストを削減し、全体的な TCO を削減します。
- ボリュームを再構築して動的なサービスレベル機能を利用すると、安定状態のワークロードのサイジングを行い、オーバープロビジョニングを回避することでコストを最適化できます。
- 注： \*
- 冗長性と高可用性を高めるには、SQL Server VMを同一または異なるVM "可用性ゾーン"に配置する必要があります "可用性セット"。ユーザ定義のデータファイルが必要な場合は、ファイルパスの要件を考慮してください。その場合は、SQL FCI over SQLAOAG を選択します。
- 次のUNCパスがサポートされています。 "[\\ANFSMB-b4ca.anf.test\sqldb](#) および [\\ANFSMB-b4ca.anf.test\sqldb\](#)"
- ループバック UNC パスはサポートされていません。
- サイジングには、オンプレミス環境の履歴データを使用します。OLTP ワークロードの場合は、ワークロードの平均時間とピーク時間、ディスク読み取り回数 / 秒、ディスク書き込み回数 / 秒のパフォーマンスカウンタを使用して、ターゲット IOPS とパフォーマンス要件を一致させます。Data Warehouse および Reporting のワークロードの場合は、ワークロードの平均時間とピーク時間、およびディスクの読み取りバイト数 / 秒とディスクの書き込みバイト数 / 秒を使用して、ターゲットのスループットを調整します平均値は、ボリュームの形状変更機能と組み合わせて使用できます。

#### 継続的可用性を備えた共有を作成

Azure ポータルまたは Azure CLI を使用して、継続的可用性を備えた共有を作成する。ポータルで、[Enable Continuous Availability]プロパティオプションを選択します。Azure CLIの場合、に設定されたオプションを `$True`` 使用して、共有を継続的可用性を備えた共有として指定します ``az netappfiles volume create with the smb-continuously-avl`。継続的可用性が有効な新しいボリュームの作成の詳細については、を参照してください "[継続的可用性を備えた共有を作成しています](#)"。

- 注： \*
- 次の図に示すように、SMB ボリュームの継続的可用性を有効にします。
- 管理者以外のドメインアカウントを使用する場合は、そのアカウントに必要なセキュリティ権限が割り当てられていることを確認してください。
- 共有レベルで適切な権限を設定し、適切なファイルレベルの権限を設定します。
- 既存の SMB ボリュームでは継続的可用性プロパティを有効にできません。既存のボリュームを変換して継続的な可用性が確保された共有を使用するには、NetApp Snapshot テクノロジーを使用します。詳細については、を参照してください "[既存の SMB ボリュームを継続的可用性を使用するように変換します](#)"。

Basics **Protocol** Tags Review + create

Configure access to your volume.

**Access**Protocol type  NFS  SMB  Dual-protocol (NFSv3 and SMB)**Configuration**Active Directory \* ⓘ  ▼Share name \* ⓘ Enable Continuous Availability ⓘ **Review + create**

&lt; Previous

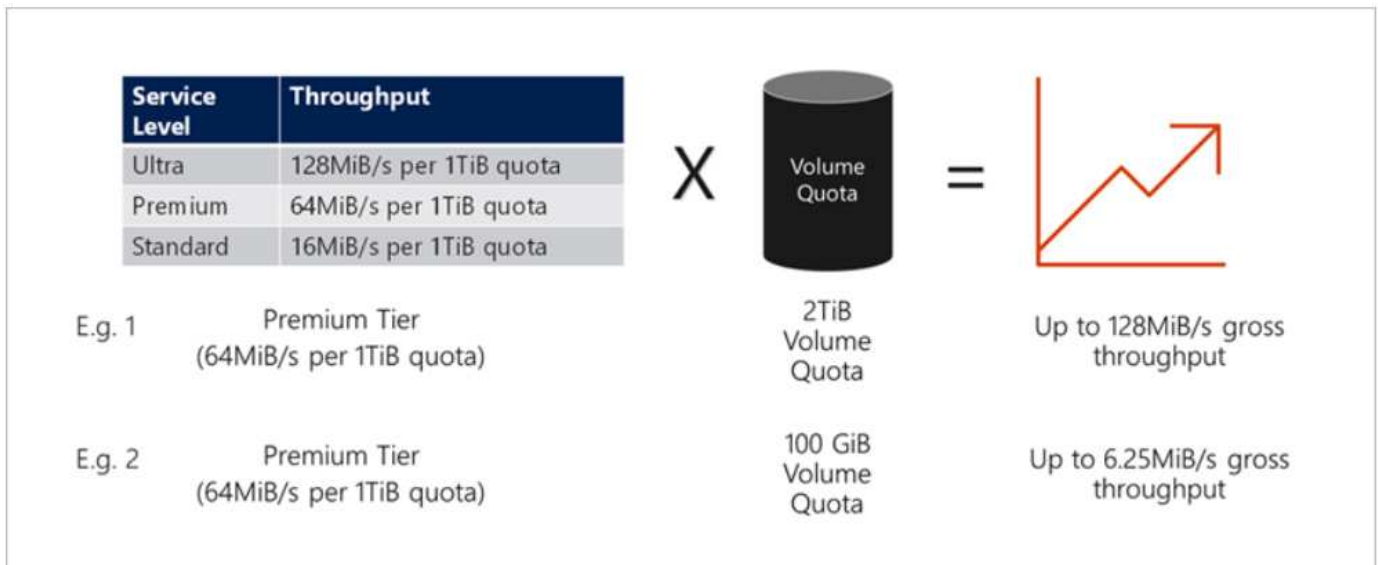
Next : Tags &gt;

## パフォーマンス

Azure NetApp Files は、Standard（テラバイトあたり 16Mbps）、Premium（テラバイトあたり 64MBps）、Ultra（テラバイトあたり 128MBps）の 3 つのサービスレベルをサポートします。データベースワークロードのパフォーマンスを最適化するには、適切なボリュームサイズをプロビジョニングすることが重要です。Azure NetApp Files では、ボリュームのパフォーマンスとスループット制限は次の要素の組み合わせに基づいて決まります。

- ボリュームが属する容量プールのサービスレベル
- ボリュームに割り当てられているクォータ
- 容量プールのサービス品質（QoS）タイプ（auto または manual）

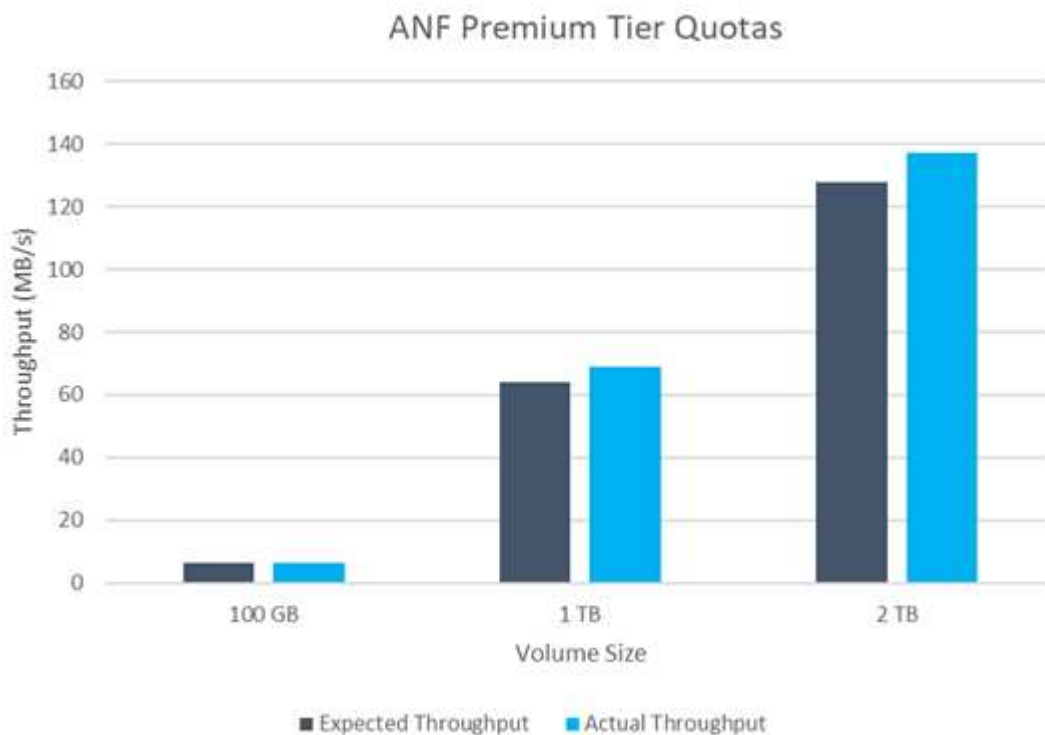
詳細については、を参照してください ["Azure NetApp Files のサービスレベル"](#)。



### パフォーマンスの検証

あらゆる導入同様、VM とストレージをテストすることが重要です。ストレージの検証には、HammerDB、Apploader、、、または適切な読み取り/書き込みの組み合わせを持つ任意のカスタムスクリプトまたは fio などのツールを "SQL Server Storage Benchmark (SB) ツール" 使用する必要があります。ただし、SQL Server のワークロードのほとんどは、ビジー状態の OLTP ワークロードでも、読み取りが 80~90%、書き込みが 10~20% 近くになることに注意してください。

パフォーマンスを確認するために、Premium サービスレベルを使用してボリュームに対してクイックテストを実行しました。このテストでは、ボリュームサイズを 100GB から 2TB にオンザフライで拡張しました。アプリケーションへのアクセスを中断することなく、データの移行もゼロでした。



ここでは、HammerDB を使用して導入した、リアルタイムのパフォーマンステストの別の例を示します。こ

のテストでは、vCPU 8 個、500GB Premium SSD、500GB SMB Azure NetApp Files ボリュームを含む小規模インスタンスを使用しました。HammerDB は、80 のウェアハウスと 8 人のユーザで構成されています。

次のグラフから、Azure NetApp Files では、1 分あたりのトランザクション数が 2.6x で、同等のサイズのボリューム（500GB）を使用した場合のレイテンシが 4 分の 1 に削減されたことがわかります。

さらに、vCPU が 32 個、Azure NetApp Files が 16TB の大容量インスタンスへのサイズ変更によって、テストを実施しました。1 分あたりのトランザクション数は大幅に増加し、レイテンシは常に 1 ミリ秒に抑えられました。HammerDB は、このテストで 80 個のウェアハウスと 64 人のユーザで構成されました。



## コストの最適化

Azure NetApp Files を使用すると、ボリュームのサイズを透過的に無停止で変更でき、ダウンタイムやアプリケーションへの影響なしでサービスレベルを変更できます。これは、動的なコスト管理が可能な独自の機能で、ピーク時の指標を使用してデータベースのサイジングを行う必要を回避できます。安定した状態のワークロードを利用できるため、初期投資が不要になります。ボリュームの形状変更とサービスレベルの動的変更を使用すると、データアクセスを維持しながら、I/O を一時停止することなく、Azure NetApp Files ボリュームの帯域幅とサービスレベルをほぼ瞬時にオンデマンドで調整できます。

LogicApp や関数などの Azure PaaS ソリューションを使用すると、特定の webhook または alert ルールトリガーに基づいてボリュームのサイズを簡単に変更し、ワークロードの要件を満たしながらコストを動的に処理できます。

たとえば、安定した動作に 250Mbps のデータを必要とするデータベースがありますが、400Mbps のピークスループットも必要とします。この場合、安定したパフォーマンスの要件を満たすために、Premium サービスレベルに 4TB ボリュームを追加して導入する必要があります。ピーク時のワークロードに対処するには、Azure の機能を使用して特定の期間でボリュームサイズを 7TB に増やしてから、導入コストを抑えるためにボリュームのサイズを縮小します。この構成では、ストレージのオーバプロビジョニングを回避できます。

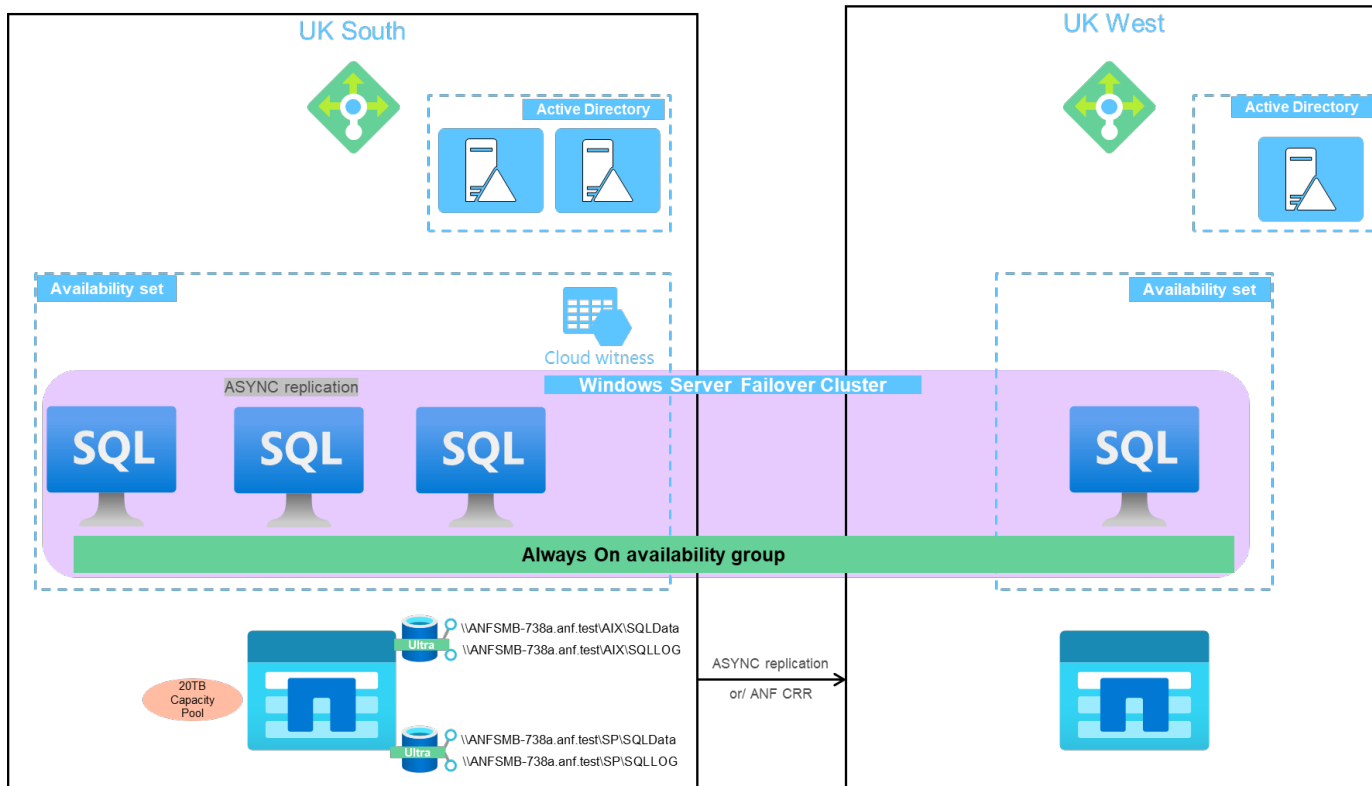
## リアルタイムの高レベル・リファレンス・デザイン

このセクションでは、Azure NetApp Files SMB ボリュームを使用して AOAG 構成に SQL データベース資産をリアルタイムで導入する方法について説明します。

- ノード数： 4.
- データベース数： 21
- 可用性グループの数： 4.
- バックアップの保持： 7 日
- バックアップアーカイブ： 365 日

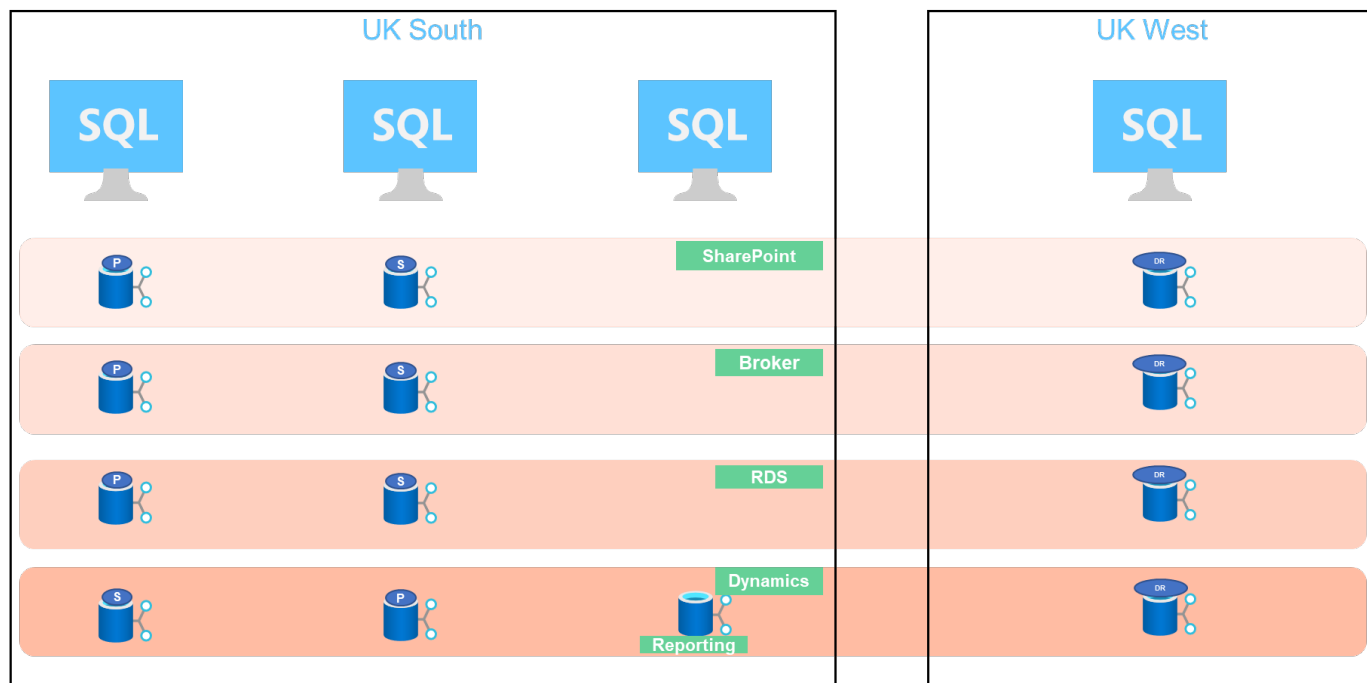


Azure NetApp Files 共有を使用して Azure 仮想マシンに SQL Server と FCI を導入すると、コスト効率に優れたモデルでデータのコピーを 1 つ作成できます。この解決策では、ファイルパスがセカンダリレプリカと異なる場合に、追加ファイル操作の問題を回避できます。



次の図は、AOAG 内のデータベースがノード全体に分散していることを示しています。





## データレイアウト

ユーザデータベースファイル（.mdf）とユーザデータベーストランザクションログファイル（.ldf）は、tempdb とともに同じボリュームに格納されます。サービスレベルは Ultra です。

構成は 4 つのノードと 4 つの AGS で構成されます。21 個のデータベース（Dynamic AX、SharePoint、RDS コネクションブローカー、インデックスサービスの一部）はすべて Azure NetApp Files ボリュームに格納されます。ノード上のリソースを効果的に使用するために、AOAG ノード間でデータベースが分散されます。WSFC には、AOAG 構成に属する 4 つの D32 v3 インスタンスが追加されています。これらの 4 つのノードは Azure Virtual Network でプロビジョニングされ、オンプレミスから移行されることはありません。

- 注： \*
- アプリケーションの性質と実行するクエリに応じて、ログのパフォーマンスとスループットが向上する必要がある場合は、データベースファイルを Premium サービスレベルに配置し、Ultra サービスレベルでログを格納できます。
- tempdb ファイルが Azure NetApp Files に配置されている場合は、Azure NetApp Files ボリュームをユーザのデータベースファイルから分離する必要があります。AOAG でのデータベースファイルの配布例を次に示します。
- 注： \*
- Snapshot コピーベースのデータ保護のメリットを維持するために、データとログのデータを同じボリュームに統合しないことを推奨します。
- セカンダリデータベースのファイルパスが対応するプライマリデータベースのパスと異なる場合、プライマリレプリカで実行されるアドオンファイル処理がセカンダリデータベースで失敗する可能性があります。この状況は、プライマリノードとセカンダリノードで共有パスが異なる場合（コンピュータアカウントが異なることが原因）に発生することがあります。この障害が発生すると、セカンダリデータベースが原因によって中断される可能性があります。拡張またはパフォーマンスのパターンを予測できず、あとでファイルを追加する予定の場合は、Azure NetApp Files を使用した SQL Server フェイルオーバークラス

タも許容される解決策です。ほとんどの環境では、Azure NetApp Files がパフォーマンス要件を満たしています。

## 移行

オンプレミスの SQL Server ユーザーデータベースを Azure 仮想マシンの SQL Server に移行するには、いくつかの方法があります。移行はオンラインとオフラインのどちらでも実行できます。選択するオプションは、SQL Server のバージョン、ビジネス要件、および組織内で定義されている SLA によって異なります。データベース移行プロセス中のダウンタイムを最小限に抑えるために、AlwaysOn オプションまたはトランザクションレプリケーションオプションのどちらかを使用することを推奨します。これらの方法を使用できない場合は、データベースを手動で移行できます。

マシン間でデータベースを移動するための最もシンプルで徹底的にテストされたアプローチは、バックアップとリストアです。通常は、データベースバックアップのあとにデータベースバックアップのコピーを Azure に作成します。そのあとでデータベースをリストアできます。最適なデータ転送パフォーマンスを実現するには、圧縮されたバックアップファイルを使用してデータベースファイルを Azure VM に移行します。本ドキュメントで紹介している高度な設計では、Azure ファイルストレージのバックアップ方法と Azure ファイルの同期を使用し、Azure NetApp Files にリストアするアプローチを採用しています。



Azure Migrate は、SQL Server ワークロードの検出、評価、移行に使用できます。

移行を実行するには、次の手順を実行します。

1. 要件に基づいて、接続をセットアップします。
2. オンプレミスのファイル共有場所へのフルデータベースバックアップを実行
3. Azure ファイル同期を使用して、バックアップファイルを Azure ファイル共有にコピーします。
4. 目的のバージョンの SQL Server で VM をプロビジョニングします。
5. コマンドプロンプトからコマンドを使用して、バックアップファイルを VM にコピーし `copy` ます。
6. フルデータベースを Azure 仮想マシン上の SQL Server にリストアします。



21 のデータベースをリストアするには、約 9 時間かかりました。この方法はこのシナリオに特有です。ただし、状況や要件に応じて、以下に示すその他の移行方法を使用できます。

オンプレミスの SQL Server から Azure NetApp Files にデータを移動するためのその他の移行オプションには、次のものがあります。

- データファイルとログファイルを切り離し、Azure Blob Storage にコピーして、URL からマウントされた ANF ファイル共有を使用して Azure VM 内の SQL Server に接続します。
- オンプレミスで Always On 可用性グループデプロイメントを使用している場合は、を使用して "[Azure レプリカの追加ウィザード](#)" Azure でレプリカを作成し、フェイルオーバーを実行します。
- SQL Server を使用して "[トランザクションレプリケーション](#)"、Azure SQL Server インスタンスをサブスクライバとして設定し、レプリケーションを無効にして、ユーザーに Azure データベースインスタンスを指定します。
- Windows インポート / エクスポートサービスを使用して、ハードドライブを出荷します。

## バックアップとリカバリ

バックアップとリカバリは、SQL Server 環境にとって重要な要素です。AOAG などの高可用性ソリューション



ンと組み合わせて、さまざまなデータ障害および損失シナリオから迅速にリカバリするための適切な安全ネットを用意する必要があります。CommVault などのサードパーティ製バックアップツールでは、SQL Server データベースの休止ツール、Azure バックアップ（ストリーミング）、またはアプリケーションと整合性のあるデータベースバックアップを実行できます。

Azure NetApp Files の Snapshot テクノロジーを使用すると、パフォーマンスやネットワーク利用率に影響を与えることなく、ユーザデータベースのポイントインタイム（PiT）コピーを簡単に作成できます。また、このテクノロジーを使用すると、新しいボリュームに Snapshot コピーをリストアしたり、ボリュームの状態を、ボリュームリポート機能を使用して Snapshot コピーが作成された時点の状態にすばやくリポートしたりできます。Azure NetApp Files スナップショットプロセスは非常に高速で効率的で、Azure バックアップのストリーミングバックアップとは異なり、毎日のバックアップを複数作成できます。1日に複数の Snapshot コピーを作成できるため、RPO と RTO が大幅に短縮されます。アプリケーションの整合性を追加して、Snapshot コピーを作成する前にデータに影響を与えずにディスクに適切にフラッシュするには、SQL Server データベースの休止ツールを使用し("SCSQLAPI ツール"ます。このリンクにアクセスするには、NetApp SSOログインクレデンシャルが必要です)。このツールは PowerShell から実行できます。PowerShell では、SQL Server データベースを休止し、アプリケーションと整合性のあるバックアップ用ストレージ Snapshot コピーを作成できます。

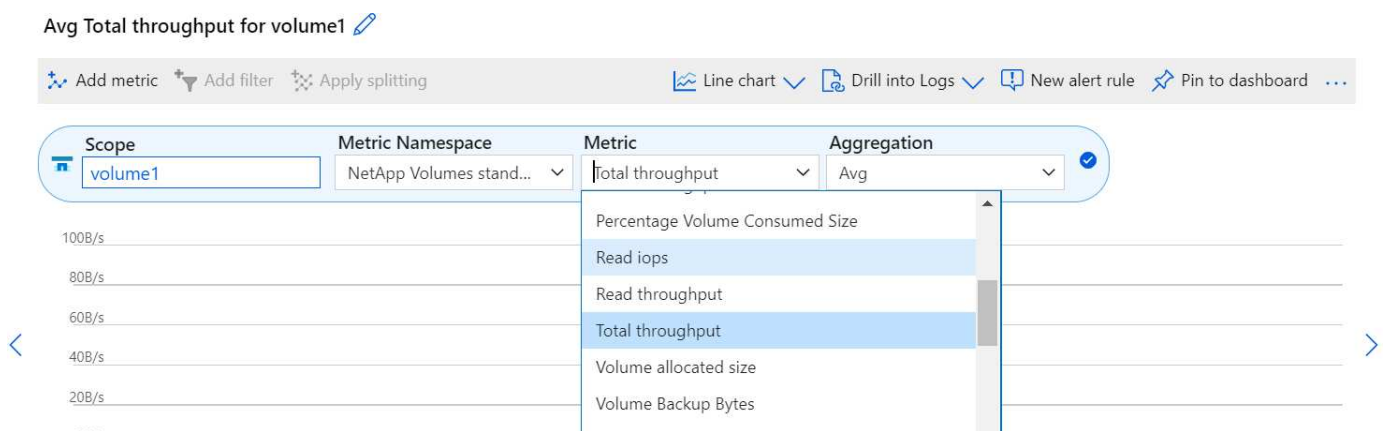
- 注：\*
- SCSQLAPI ツールは、2016 および 2017 バージョンの SQL Server のみをサポートします。
- SCSQLAPI ツールは、一度に 1 つのデータベースでのみ動作します。
- 各データベースのファイルを別々の Azure NetApp Files ボリュームに配置して、それらのファイルを分離します。

SCSQL APIには膨大な制限があるため "Azure バックアップ"、はSLA要件を満たすためにデータ保護に使用されてきました。Azure Virtual Machine と Azure NetApp Files で実行される SQL Server のストリームベースのバックアップを提供します。Azure Backup では、15 分の RPO を実現し、ログバックアップと PIT リカバリを最大 1 秒まで頻繁に実行できます。

## 監視

Azure NetApp Files は、時系列データ用の Azure Monitor と統合されており、割り当てられたストレージ、実際のストレージ使用量、ボリューム IOPS、スループット、ディスク読み取りバイト / 秒に関する指標を提供します。ディスク書き込みバイト / 秒、ディスク読み取り / 秒、ディスク書き込み / 秒、および関連するレイテンシ。このデータを使用して、アラート生成によるボトルネックを特定し、健全性チェックを実行して、SQL Server 環境が最適な構成で実行されていることを確認できます。

この HLD では、ScienceLogic を使用して、適切なサービスプリンシパルを使用してメトリックを公開することで Azure NetApp Files を監視します。次の図は、Azure NetApp Files Metric オプションの例です。



## シッククローンを使用した DevTest

Azure NetApp Files を使用すると、アプリケーション開発サイクル中に現在のデータベースの構造とコンテンツを使用して実装が必要な機能をテストするためのデータベースのコピーを瞬時に作成でき、データの抽出と操作を行うツールを使用してデータウェアハウスにデータを取り込むことができます。また、誤って削除または変更されたデータをリカバリすることもできます。このプロセスでは Azure Blob コンテナからデータをコピーする必要がないため、非常に効率的です。ボリュームのリストア後は読み取り / 書き込み処理に使用できるため、検証と製品化までの時間が大幅に短縮されます。この機能は、SCSQLAPI と併用してアプリケーションの整合性を保つ必要があります。このアプローチでは、別の継続的なコスト最適化手法に加えて、Restore to New volume オプションを活用する Azure NetApp Files も提供されます。

- 注： \*
- Snapshot コピーから作成されたボリュームに Restore New Volume オプションを使用すると、容量プールの容量が使用されます。
- REST または Azure CLI を使用してクローンボリュームを削除すると、追加のコストを回避できます（容量プールの拡張が必要になった場合）。

## ハイブリッドストレージの選択肢

ネットアップでは、SQL Server 可用性グループのすべてのノードに同じストレージを使用することを推奨していますが、場合によっては複数のストレージオプションを使用できます。このシナリオは、Azure NetApp Files で、AOAG のノードが Azure NetApp Files SMB ファイル共有に接続され、2 つ目のノードが Azure Premium ディスクに接続されている場合に発生します。このような場合は、Azure NetApp Files SMB 共有にユーザデータベースのプライマリコピーが保持され、Premium ディスクがセカンダリコピーとして使用されていることを確認してください。

- 注： \*
- このような環境でフェイルオーバーの問題を回避するには、SMB ボリュームで継続的可用性が有効になっていることを確認してください。継続的可用性属性を持たないストレージレイヤでバックグラウンドでメンテナンスを実施すると、データベースで障害が発生する可能性があります。
- データベースのプライマリコピーは Azure NetApp Files SMB ファイル共有に保持します。

## ビジネス継続性

ディザスタリカバリは、一般にあらゆる導入で後回しになっています。ただし、ビジネスへの影響を回避するために、設計および導入の初期段階でディザスタリカバリに対処する必要があります。Azure NetApp Files では、クロスリージョンレプリケーション（CRR）機能を使用して、予期しないリージョンの停止を処理するためにブロックレベルでボリュームデータをペアリングされたリージョンにレプリケートできます。CRR 対応のデスティネーション・ボリュームは読み取り処理に使用できるため、災害復旧シミュレーションに最適です。さらに 'CRR デスティネーションを最小のサービス・レベル（Standard など）で割り当てることにより' 全体的な TCO を削減できますフェイルオーバーが発生した場合はレプリケーションを解除することで対応するボリュームを読み取り / 書き込み可能にすることができます。また、動的なサービスレベル機能を使用してディザスタリカバリコストを大幅に削減することで、ボリュームのサービスレベルを変更することもできます。これは Azure NetApp Files 独自の機能で、Azure 内でブロックレプリケーションを実行します。

## 長期的な Snapshot コピーのアーカイブ

多くの組織では、Snapshot データをデータベースファイルから長期的に保持することが必須のコンプライアンス要件として求められています。このHLDではこのプロセスを使用しませんが、を使用してSnapshotディレクトリをAzure Blobコンテナにコピーする簡単なバッチスクリプトを使用することで簡単に実行できます **"AzCopy"**。スケジュールされたタスクを使用して、特定のスケジュールに基づいてバッチスクリプトを実行できます。このプロセスは簡単で、次の手順で構成されます。

1. AzCopy V10 実行ファイルをダウンロードします。ファイルであるため、インストールする必要はありません。exe
2. コンテナレベルで適切な権限を持つ SAS トークンを使用して 'AzCopy を承認します
3. AzCopy が承認されると、データ転送が開始されます。
  - 注： \*
  - バッチファイルでは、SAS トークンに表示される % 文字をエスケープする必要があります。そのためには、SAS トークン文字列で既存の % 文字の横に % 文字を追加します。
  - "セキュアな転送が必要です"ストレージアカウントの設定によって、ストレージアカウントへの接続をTransport Layer Security (TLS) で保護するかどうかが決まります。この設定はデフォルトで有効になっています。次のバッチスクリプト例は、Snapshot コピーディレクトリから指定された BLOB コンテナにデータを再帰的にコピーします。

```
SET source="Z:\~snapshot"  
echo %source%  
SET  
dest="https://testanfacct.blob.core.windows.net/azcoptst?sp=racwdl&st=2020-10-21T18:41:35Z&se=2021-10-22T18:41:00Z&sv=2019-12-12&sr=c&sig=ZxRUJwFlLXgHS8As7HzXJOaDXXVJ7PxxIX3ACpx56XY%%3D"  
echo %dest%
```

PowerShell で次のコマンドが実行されます。

```
-recursive
```

```
INFO: Scanning...
INFO: Any empty folders will not be processed, because source and/or
destination doesn't have full folder support
Job b3731dd8-da61-9441-7281-17a4db09ce30 has started
Log file is located at: C:\Users\niyaz\.azcopy\b3731dd8-da61-9441-7281-
17a4db09ce30.log
0.0 %, 0 Done, 0 Failed, 2 Pending, 0 Skipped, 2 Total,
INFO: azcopy.exe: A newer version 10.10.0 is available to download
0.0 %, 0 Done, 0 Failed, 2 Pending, 0 Skipped, 2 Total,
Job b3731dd8-da61-9441-7281-17a4db09ce30 summary
Elapsed Time (Minutes): 0.0333
Number of File Transfers: 2
Number of Folder Property Transfers: 0
Total Number of Transfers: 2
Number of Transfers Completed: 2
Number of Transfers Failed: 0
Number of Transfers Skipped: 0
TotalBytesTransferred: 5
Final Job Status: Completed
```

- 注： \*
- 長期保持用の同様のバックアップ機能も、近日中に Azure NetApp Files で使用可能になります。
- バッチスクリプトは、任意のリージョンの BLOB コンテナにデータをコピーする必要がある場合に使用できません。

#### コストの最適化

ボリュームの形状変更とサービスレベルの動的変更をデータベースに対して完全に透過的に行うことで、Azure NetApp Files は Azure で継続的なコスト最適化を実現します。この HLD では、この機能を使用して、ワークロードの急増に対処するためにストレージを追加でオーバープロビジョニングすることを回避しています。

ボリュームのサイズ変更は、Azure 機能と Azure アラートログを組み合わせて作成すると簡単に実行できます。

#### まとめ

オールクラウドにも、ストレッチデータベースを使用したハイブリッドクラウドにも、Azure NetApp Files は、データベースワークロードの導入と管理に最適なオプションを提供します。データ要件はアプリケーションレイヤとシームレスに連携し、TCO を削減します。

このドキュメントでは、Azure NetApp Files を使用した Microsoft SQL Server 環境の計画、設計、最適化、拡張に関する推奨事項について説明します。この推奨事項は、実装によって大きく異なる場合があります。適切な解決策は、導入の技術的な詳細と、プロジェクトの背景にあるビジネス要件の両方によって異なります。

## 重要なポイント

本ドキュメントの主な内容は次のとおりです。

- Azure NetApp Files を使用して、SQL Server クラスターのデータベースおよびファイル共有監視をホストできるようになりました。
- アプリケーションの応答時間を短縮し、99.9999% の可用性を実現して、必要なときに必要な場所で SQL Server データにアクセスできるようにします。
- シンプルで瞬時のサイズ変更により、SQL Server の導入と、RAID ストライピングなどの継続的な管理の全体的な複雑さを緩和できます。
- インテリジェントな運用機能を利用すれば、SQL Server データベースを数分で導入し、開発サイクルを短縮できます。
- Azure クラウドが移行先である場合、最適化された導入に最適なストレージ解決策は Azure NetApp Files です。

## 詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、次の Web サイトのリンクを参照してください。

- Azure NetApp Files を使用した解決策アーキテクチャ  
["https://docs.microsoft.com/en-us/azure/azure-netapp-files/azure-netapp-files-solution-architectures"](https://docs.microsoft.com/en-us/azure/azure-netapp-files/azure-netapp-files-solution-architectures)
- Azure NetApp Files for SQL Server の導入のメリット  
["https://docs.microsoft.com/en-us/azure/azure-netapp-files/solutions-benefits-azure-netapp-files-sql-server"](https://docs.microsoft.com/en-us/azure/azure-netapp-files/solutions-benefits-azure-netapp-files-sql-server)
- 耐障害性、高可用性、Azure NetApp Files との耐障害性を備えています  
["https://cloud.netapp.com/blog/azure-anf-blg-fault-tolerance-high-availability-and-resilience-with-azure-netapp-files"](https://cloud.netapp.com/blog/azure-anf-blg-fault-tolerance-high-availability-and-resilience-with-azure-netapp-files)

## TR-4467 : 『SAP with Microsoft SQL Server on Windows』 - 『Best Practices Using NetApp Clustered Data ONTAP and SnapCenter 』

Marco Schoen、ネットアップ

TR-4467では、Windows環境でMicrosoft SQL Serverを実行するSAP Business Suiteソリューションをサポートする、clustered Data ONTAP の導入に関するベストプラクティスをお客様やパートナー様に紹介しています。

["TR-4467 : 『SAP with Microsoft SQL Server on Windows』 - 『Best Practices Using NetApp Clustered Data ONTAP and SnapCenter 』 "](#)

## Microsoft SQL Server環境の刷新

運用を最適化し、オンプレミスでもクラウドでも、データを最大限に活用できます。

["Microsoft SQL Server環境の刷新"](#)

## TR-4590 : 『Best Practice Guide for Microsoft SQL Server with ONTAP』

Manohar KulkarniとPat Sinthusan、NetApp

このドキュメントでは、効果的かつ効率的なストレージ導入とエンドツーエンドのデータ保護および保持計画を実現するために、NetApp ONTAP®ソフトウェアを実行するNetAppストレージシステムにSQL Serverを導入する際のベストプラクティスと設計上の考慮事項について説明します。

["TR-4590 : 『Best Practices Guide for Microsoft SQL Server with ONTAP』 "](#)

## TR-4764 : 『Best Practices for Microsoft SQL Server with NetApp EF Series』

ミッチ・ブラックバーン、パット・シントウサン、NetApp

このベストプラクティスガイドは、ストレージ管理者およびデータベース管理者がMicrosoft SQL ServerをNetApp EFシリーズストレージに正常に導入できるようにすることを目的としています。

["TR-4764 : 『Best Practices for Microsoft SQL Server with NetApp EF Series』 "](#)



## 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。