



# **Microsoft SQL Server**

## NetApp Solutions

NetApp  
August 03, 2023

# Table of Contents

Microsoft SQL Server .....	1
TR-4897: SQL Server on Azure NetApp Files - Real Deployment View .....	1
TR-4923: SQL Server on AWS EC2 using Amazon FSx for NetApp ONTAP .....	13
TR-4951: Backup and Recovery for Microsoft SQL Server on AWS FSx for ONTAP .....	41
TR-4467: SAP with Microsoft SQL Server on Windows - Best practices using NetApp Clustered Data ONTAP and SnapCenter .....	96
Modernizing your Microsoft SQL Server environment .....	97
TR-4764: Best practices for Microsoft SQL Server with NetApp EF-Series .....	97

# Microsoft SQL Server

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

Niyaz Mohamed, NetApp

IT organizations face constant change. Gartner reports nearly 75% of all databases will require cloud-based storage by 2022. As a leading relational database management system (RDBMS), Microsoft SQL Server is the go-to choice for Windows platform-designed applications and organizations that rely on SQL Server for everything from enterprise resource planning (ERP) to analytics to content management. SQL Server has helped to revolutionize the way enterprises manage massive data sets and power their applications to meet the schema and query performance demands.

Most IT organizations follow a cloud-first approach. Customers in a transformation phase evaluate their current IT landscape and then migrate their database workloads to the cloud based on an assessment and discovery exercise. Some factors driving customers toward cloud migration include elasticity/burst, data center exit, data center consolidation, end-of-life scenarios, mergers, acquisitions, and so on. The reason for migration can vary based on each organization and their respective business priorities. When moving to the cloud, choosing the right cloud storage is very important in order to unleash the power of SQL Server database cloud deployment.

### Use case

Moving the SQL Server estate to Azure and integrating SQL Server with Azure's vast array of platform-as-a-service (PaaS) features such as Azure Data Factory, Azure IoT Hub, and Azure Machine Learning creates tremendous business value to support digital transformation. Adopting the cloud also enables the respective business unit to focus on productivity and delivering new features and enhancements faster (Dev/Test use case) than relying on the CAPEX model or traditional private cloud models. This document covers a real-time deployment of SQL Server Always On availability group (AOAG) on Azure NetApp Files leveraging Azure Virtual Machines.

Azure NetApp Files provides enterprise-grade storage with continuously available file shares. Continuously available shares are required by SQL Server production databases on SMB file share to make sure that the node always has access to the database storage, including during disruptive scenarios such as controller upgrades or failures. Continuously available file shares eliminate the need to replicate data between storage nodes. Azure NetApp Files uses SMB 3.0 scale-out, persistent handles, and transparent failover to support nondisruptive operations (NDOs) for planned and unplanned downtime events, including many administrative tasks.

When planning cloud migrations, you should always evaluate the best approach to use. The most common and easiest approach for application migration is rehosting (also known as lift and shift). The example scenario provided in this document uses the rehosting method. SQL Server on Azure virtual machines with Azure NetApp Files allows you to use full versions of SQL Server in the cloud without having to manage on-premises hardware. SQL Server virtual machines (VMs) also simplify licensing costs when you pay as you go and provides elasticity and bursting capabilities for development, test, and estate refresh scenarios.

### Factors to consider

#### VM performance

Selecting the right VM size is important for optimal performance of a relational database in a public cloud. Microsoft recommends that you continue using the same database performance-tuning options that are

applicable to SQL Server in on-premises server environments. Use [memory-optimized](#) VM sizes for the best performance of SQL Server workloads. Collect the performance data of existing deployment to identify the RAM and CPU utilization while choosing the right instances. Most deployments choose between the D, E, or M series.

## Notes:

- For the best performance of SQL Server workloads, use memory-optimized VM sizes.
- NetApp and Microsoft recommend that you identify the storage performance requirements before choosing the instance type with the appropriate memory-to-vCore ratio. This also helps select a lower-instance type with the right network bandwidth to overcome storage throughput limits of the VM.

## VM redundancy

To increase redundancy and high availability, SQL Server VMs should either be in the same [availability set](#) or different [availability zones](#). When creating Azure VMs, you must choose between configuring availability sets versus availability zones; an Azure VM cannot participate in both.

## High availability

For high availability, configuring SQL Server AOAG or Always On Failover Cluster Instance (FCI) is the best option. For AOAG, this involves multiple instances of SQL Server on Azure Virtual Machines in a virtual network. If high availability is required at the database level, consider configuring SQL Server availability groups.

## Storage configuration

Microsoft SQL Server can be deployed with an SMB file share as the storage option. Starting with SQL Server 2012, system databases (master, model, msdb, or tempdb), and user databases can be installed with Server Message Block (SMB) file server as a storage option. This applies to both SQL Server stand-alone and SQL Server FCI.



File share storage for SQL Server databases should support continuously available property. This provides uninterrupted access to the file-share data.

Azure NetApp Files provides high performing file storage to meet any demanding workload, and it reduces SQL Server TCO as compared to block storage solutions. With block storage, VMs have imposed limits on I/O and bandwidth for disk operations; network bandwidth limits alone are applied against Azure NetApp Files. In other words, no VM-level I/O limits are applied to Azure NetApp Files. Without these I/O limits, SQL Server running on smaller VMs connected to Azure NetApp Files can perform as well as SQL Server running on much larger VMs. Azure NetApp Files reduce SQL Server deployment costs by reducing compute and software licensing costs. For detailed cost analysis and performance benefits of using Azure NetApp Files for SQL Server deployment, see the [Benefits of using Azure NetApp Files for SQL Server deployment](#).

## Benefits

The benefits of using Azure NetApp Files for SQL Server include the following:

- Using Azure NetApp Files allows you to use smaller instances, thus reducing compute cost.
- Azure NetApp Files also reduces software licensing costs, which reduce the overall TCO.
- Volume reshaping and dynamic service level capability optimizes cost by sizing for steady-state workloads and avoiding overprovisioning.

#### **Notes:**

- To increase redundancy and high availability, SQL Server VMs should either be in the same [availability set](#) or in different [availability zones](#). Consider file path requirements if user-defined data files are required; in which case, select SQL FCI over SQL AOAG.
- The following UNC path is supported: `\ANFSMB-b4ca.anf.test\SQLDB` and `\ANFSMB-b4ca.anf.test\SQLDB\`.
- The loopback UNC path is not supported.
- For sizing, use historic data from your on-premises environment. For OLTP workloads, match the target IOPS with performance requirements using workloads at average and peak times along with the disk reads/sec and disk writes/sec performance counters. For data warehouse and reporting workloads, match the target throughput using workloads at average and peak times and the disk read bytes/sec and disk write bytes/sec. Average values can be used in conjunction with volume reshaping capabilities.

#### **Create continuously available shares**

Create continuously available shares with the Azure portal or Azure CLI. In the portal, select the Enable Continuous Availability property option. for the Azure CLI, specify the share as a continuously available share by using the `az netappfiles volume create` with the `smb-continuously-avl` option set to `$True`. To learn more about creating a new, continuous availability-enabled volume, see [Creating a Continuously Available Share](#).

#### **Notes:**

- Enable continuous availability for the SMB volume as shown in the following image.
- If a non-administrator domain account is used, make sure the account has the required security privilege assigned.
- Set the appropriate permissions at the share level and proper file-level permissions.
- A continuously available property cannot be enabled on existing SMB volumes. To convert an existing volume to use a continuously available share, use NetApp Snapshot technology. For more information, see [Convert existing SMB volumes to use Continuous Availability](#).

# Create a volume

X

Basics    **Protocol**    Tags    Review + create

Configure access to your volume.

## Access

Protocol type  NFS  SMB  Dual-protocol (NFSv3 and SMB)

## Configuration

Active Directory \*  10.0.0.100 - anf.test/join

Share name \*  SQLDB

Enable Continuous Availability

**Review + create**

< Previous

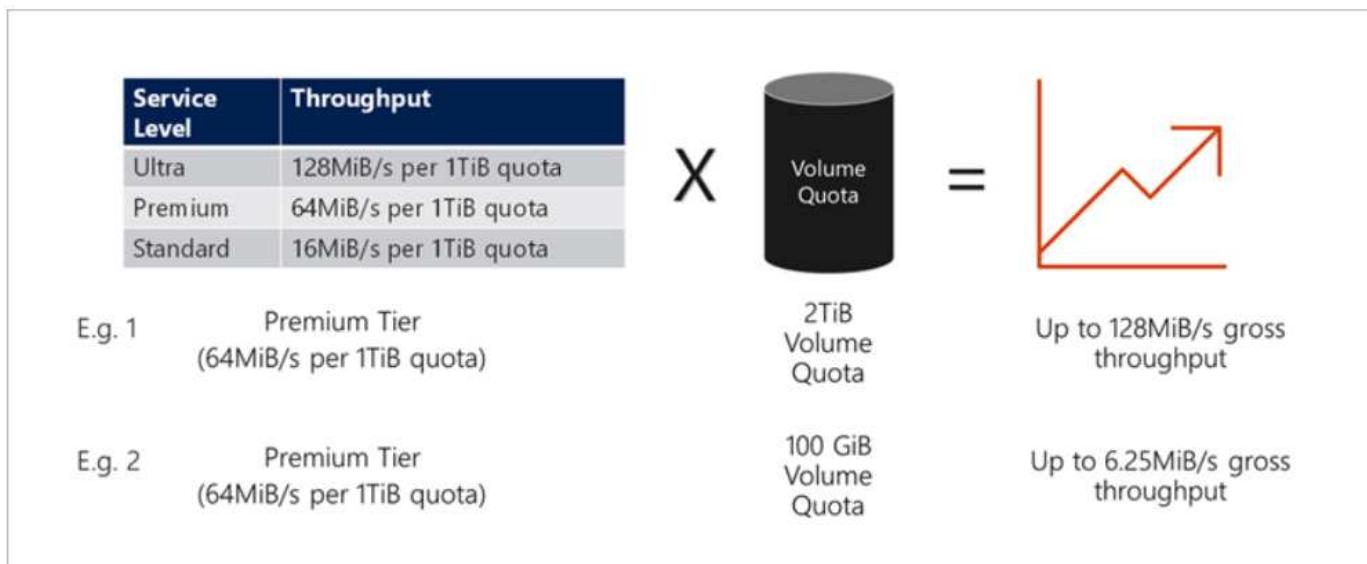
Next : Tags >

## Performance

Azure NetApp Files supports three service levels: Standard (16MBps per terabyte), Premium (64MBps per terabyte), and Ultra (128MBps per terabyte). Provisioning the right volume size is important for optimal performance of the database workload. With Azure NetApp Files, volume performance and the throughput limit are based on a combination of the following factors:

- The service level of the capacity pool to which the volume belongs
- The quota assigned to the volume
- The quality of service (QoS) type (auto or manual) of the capacity pool

For more information, see [Service levels for Azure NetApp Files](#).



## Performance validation

As with any deployment, testing the VM and storage is critical. For storage validation, tools such as HammerDB, Apploader, the [SQL Server storage benchmark \(SB\) tool](#), or any custom script or FIO with the appropriate read/write mix should be used. Keep in mind however that most SQL Server workloads, even busy OLTP workloads, are closer to 80%–90% read and 10%–20% write.

To showcase performance, a quick test was performed against a volume using premium service levels. In this test, the volume size was increased from 100GB to 2TB on the fly without any disruption to application access and zero data migration.



Here is another example of real time performance testing with HammerDB performed for the deployment covered in this paper. For this testing, we used a small instance with eight vCPUs, a 500GB Premium SSD, and a 500GB SMB Azure NetApp Files volume. HammerDB was configured with 80 warehouses and eight

users.

The following chart shows that Azure NetApp Files was able to deliver 2.6x the number of transactions per minute at 4x lower latency when using a comparable sized volume (500GB).

An additional test was performed by resizing to a larger instance with 32x vCPUs and a 16TB Azure NetApp Files volume. There was a significant increase in transactions per minute with consistent 1ms latency. HammerDB was configured with 80 warehouses and 64 users for this test.



## Cost optimization

Azure NetApp Files allows nondisruptive, transparent volume resizing and the ability to change the service levels with zero downtime and no effect on applications. This is a unique capability allowing dynamic cost management that avoids the need to perform database sizing with peak metrics. Rather, you can use steady state workloads, which avoids upfront costs. The volume reshaping and dynamic service-level change allows you to adjust the bandwidth and service level of Azure NetApp Files volumes on demand almost instantaneously without pausing I/O, while retaining data access.

Azure PaaS offerings such as LogicApp or Functions can be used to easily resize the volume based on a specific webhook or alert rule trigger to meet the workload demands while dynamically handling the cost.

For example, consider a database that needs 250MBps for steady state operation; however, it also requires a peak throughput of 400MBps. In this case, the deployment should be performed with a 4TB volume within the Premium service level to meet the steady-state performance requirements. To handle the peak workload, increase the volume size using Azure functions to 7TB for that specific period, and then downsize the volume to make the deployment cost effective. This configuration avoids overprovisioning of the storage.

## Real-time, high-level reference design

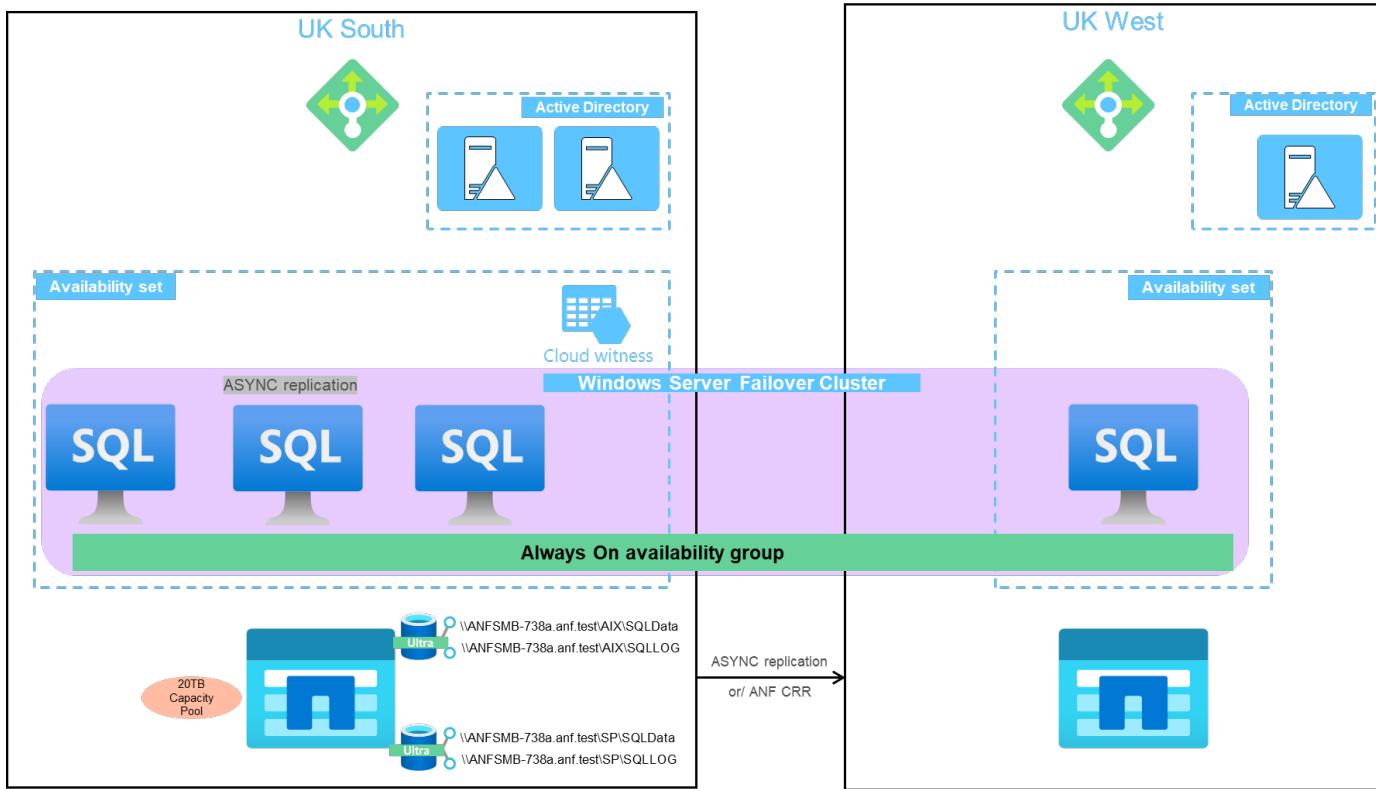
This section covers a real-time deployment of a SQL database estate in an AOAG configuration using an Azure NetApp Files SMB volume.

- Number of nodes: 4
- Number of databases: 21
- Number of availability groups: 4

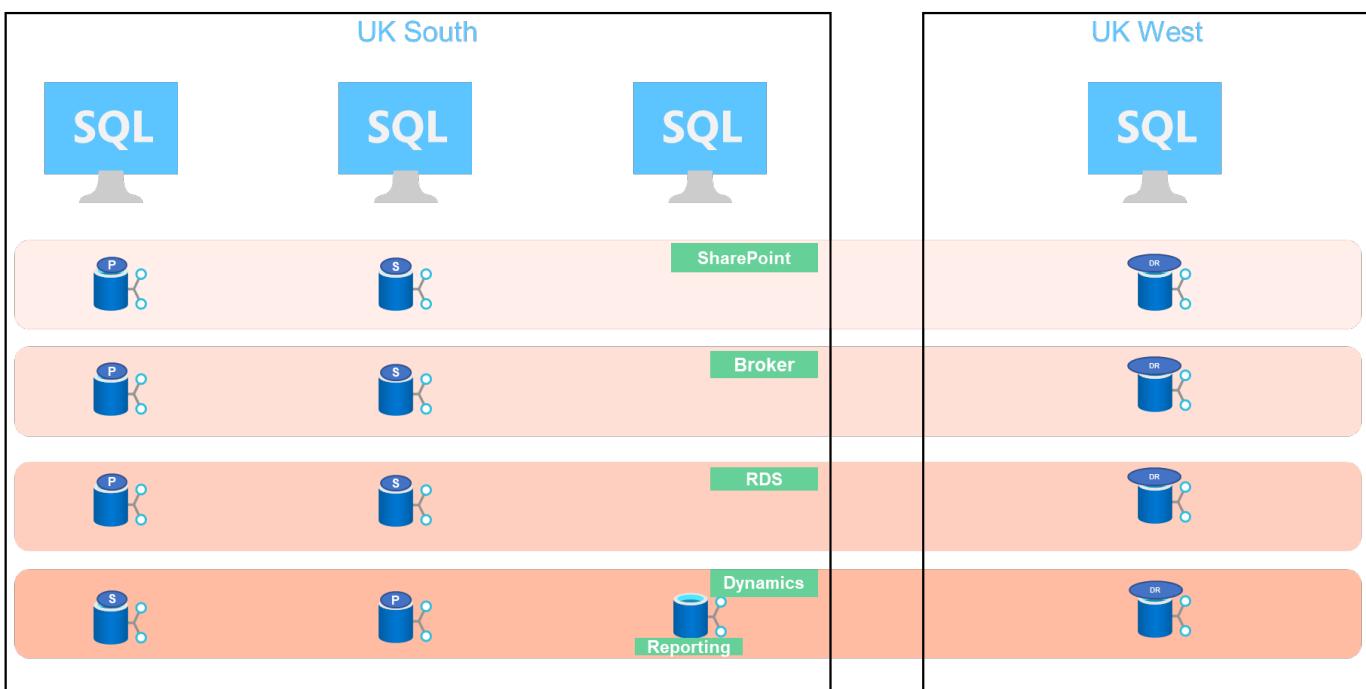
- Backup retention: 7 days
- Backup archive: 365 days



Deploying FCI with SQL Server on Azure virtual machines with an Azure NetApp Files share provides a cost-efficient model with a single copy of the data. This solution can prevent add-file operation issues if the file path differs from the secondary replica.



The following image shows the databases within AOAG spread across the nodes.



## Data layout

The user database files (.mdf) and user database transaction log files (.ldf) along with tempDB are stored on the same volume. The service level is Ultra.

The configuration consists of four nodes and four AGs. All 21 databases (part of Dynamic AX, SharePoint, RDS connection broker, and indexing services) are stored on the Azure NetApp Files volumes. The databases are balanced between the AOAG nodes to use the resources on the nodes effectively. Four D32 v3 instances are added in the WSFC, which participates in the AOAG configuration. These four nodes are provisioned in the Azure virtual network and are not migrated from on-premises.

## Notes:

- If the logs require more performance and throughput depending on the nature of the application and the queries executed, the database files can be placed on the Premium service level, and the logs can be stored at the Ultra service level.
- If the tempdb files have been placed on Azure NetApp Files, then the Azure NetApp Files volume should be separated from the user database files. Here is an example distribution of the database files in AOAG.

## Notes:

- To retain the benefits of Snapshot copy-based data protection, NetApp recommends not combining data and log data into the same volume.
- An add-file operation performed on the primary replica might fail on the secondary databases if the file path of a secondary database differs from the path of the corresponding primary database. This can happen if the share path is different on primary and secondary nodes (due to different computer accounts). This failure could cause the secondary databases to be suspended. If the growth or performance pattern cannot be predicted and the plan is to add files later, a SQL Server failover cluster with Azure NetApp Files is an acceptable solution. For most deployments, Azure NetApp Files meets the performance requirements.

## Migration

There are several ways to migrate an on-premises SQL Server user database to SQL Server in an Azure virtual machine. The migration can be either online or offline. The options chosen depend on the SQL Server version, business requirements, and the SLAs defined within the organization. To minimize downtime during the database migration process, NetApp recommends using either the AlwaysOn option or the transactional replication option. If it is not possible to use these methods, you can migrate the database manually.

The simplest and most thoroughly tested approach for moving databases across machines is backup and restore. Typically, you can start with a database backup followed by a copy of the database backup into Azure. You can then restore the database. For the best data transfer performance, migrate the database files into the Azure VM using a compressed backup file. The high-level design referenced in this document uses the backup approach to Azure file storage with Azure file sync and then restore to Azure NetApp files.



Azure Migrate can be used to discover, assess, and migrate SQL Server workloads.

To perform a migration, complete the following high-level steps:

1. Based on your requirements, set up connectivity.
2. Perform a full database backup to an on-premises file-share location.
3. Copy the backup files to an Azure file share with Azure file sync.
4. Provision the VM with the desired version of SQL Server.
5. Copy the backup files to the VM by using the `copy` command from a command prompt.
6. Restore the full databases to SQL Server on Azure virtual machines.



To restore 21 databases, it took approximately nine hours. This approach is specific to this scenario. However, other migration techniques listed below can be used based on your situation and requirements.

Other migration options to move data from an on-premises SQL Server to Azure NetApp Files include the following:

- Detach the data and log files, copy them to Azure Blob storage, and then attach them to SQL Server in the Azure VM with an ANF file share mounted from the URL.
- If you are using Always On availability group deployment on-premises, use the [Add Azure Replica Wizard](#) to create a replica in Azure and then perform failover.
- Use SQL Server [transactional replication](#) to configure the Azure SQL Server instance as a subscriber, disable replication, and point users to the Azure database instance.
- Ship the hard drive using the Windows Import/Export Service.

## Backup and recovery

Backup and recovery are an important aspect of any SQL Server deployment. It is mandatory to have the appropriate safety net to quickly recover from various data failure and loss scenarios in conjunction with high availability solutions such as AOAG. SQL Server Database Quiesce Tool, Azure Backup (streaming), or any third-party backup tool such as Commvault can be used to perform an application-consistent backup of the databases,

Azure NetApp Files Snapshot technology allows you to easily create a point-in-time (PiT) copy of the user databases without affecting performance or network utilization. This technology also allows you to restore a

Snapshot copy to a new volume or quickly revert the affected volume to the state it was in when that Snapshot copy was created by using the revert volume function. The Azure NetApp Files snapshot process is very quick and efficient, which allows for multiple daily backups, unlike the streaming backup offered by Azure backup. With multiple Snapshot copies possible in a given day, the RPO and RTO times can be significantly reduced. To add application consistency so that data is intact and properly flushed to the disk before the Snapshot copy is taken, use the SQL Server database quiesce tool ([SCSQLAPI tool](#); access to this link requires NetApp SSO login credentials). This tool can be executed from within PowerShell, which quiesces the SQL Server database and in turn can take the application-consistent storage Snapshot copy for backups.

\*Notes: \*

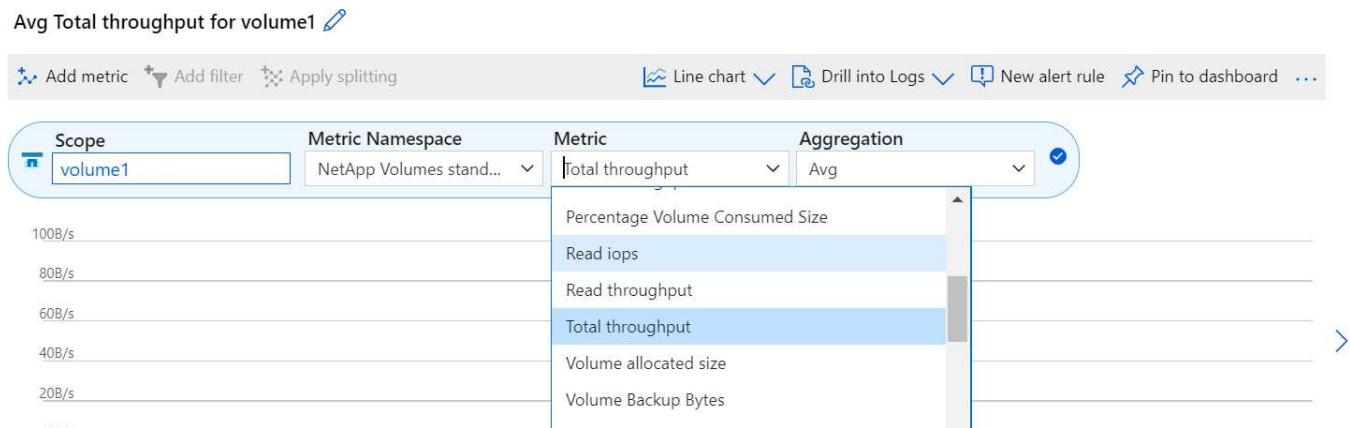
- The SCSSQLAPI tool only supports the 2016 and 2017 versions of SQL Server.
- The SCSSQLAPI tool only works with one database at a time.
- Isolate the files from each database by placing them onto a separate Azure NetApp Files volume.

Because of SCSSQL API's vast limitations, [Azure Backup](#) was used for data protection in order to meet the SLA requirements. It offers a stream-based backup of SQL Server running in Azure Virtual Machines and Azure NetApp Files. Azure Backup allows a 15-minute RPO with frequent log backups and PiT recovery up to one second.

## Monitoring

Azure NetApp Files is integrated with Azure Monitor for the time series data and provides metrics on allocated storage, actual storage usage, volume IOPS, throughput, disk read bytes/sec, disk write bytes/sec, disk reads/sec and disk writes/sec, and associated latency. This data can be used to identify bottlenecks with alerting and to perform health checks to verify that your SQL Server deployment is running in an optimal configuration.

In this HLD, ScienceLogic is used to monitor Azure NetApp Files by exposing the metrics using the appropriate service principal. The following image is an example of the Azure NetApp Files Metric option.



## Dev/Test using thick clones

With Azure NetApp Files, you can create instantaneous copies of databases to test functionality that should be implemented by using the current database structure and content during the application development cycles, to use the data extraction and manipulation tools when populating data warehouses, or to even recover data that was mistakenly deleted or changed. This process does not involve copying data from Azure Blob containers, which makes it very efficient. After the volume is restored, it can be used for read/write operations, which significantly reduces validation and time to market. This needs to be used in conjunction with SCSSQLAPI for application consistency. This approach provides yet another continuous cost optimization technique along with Azure NetApp Files leveraging the Restore to New volume option.

## **Notes:**

- The volume created from the Snapshot copy using the Restore New Volume option consumes capacity from the capacity pool.
- You can delete the cloned volumes by using REST or Azure CLI to avoid additional costs (in case the capacity pool must be increased).

## **Hybrid storage options**

Although NetApp recommends using the same storage for all the nodes in SQL Server availability groups, there are scenarios in which multiple storage options can be used. This scenario is possible for Azure NetApp Files in which a node in AOAG is connected with an Azure NetApp Files SMB file share and the second node is connected with an Azure Premium disk. In these instances, make sure that the Azure NetApp Files SMB share is holding the primary copy of the user databases and the Premium disk is used as the secondary copy.

## **Notes:**

- In such deployments, to avoid any failover issues, make sure that continuous availability is enabled on the SMB volume. With no continuously available attribute, the database can fail if there is any background maintenance at the storage layer.
- Keep the primary copy of the database on the Azure NetApp Files SMB file share.

## **Business continuity**

Disaster recovery is generally an afterthought in any deployment. However, disaster recovery must be addressed during the initial design and deployment phase to avoid any impact to your business. With Azure NetApp Files, the cross-region replication (CRR) functionality can be used to replicate the volume data at the block level to the paired region to handle any unexpected regional outage. The CRR-enabled destination volume can be used for read operations, which makes it an ideal candidate for disaster recovery simulations. In addition, the CRR destination can be assigned with the lowest service level (for instance, Standard) to reduce the overall TCO. In the event of a failover, replication can be broken, which makes the respective volume read/write capable. Also, the service level of the volume can be changed by using the dynamic service level functionality to significantly reduce disaster recovery cost. This is another unique feature of Azure NetApp Files with block replication within Azure.

## **Long-term Snapshot copy archive**

Many organizations must perform long-term retention of snapshot data from database files as a mandatory compliance requirement. Although this process is not used in this HLD, it can be easily accomplished by using a simple batch script using [AzCopy](#) to copy the snapshot directory to the Azure Blob container. The batch script can be triggered based on a specific schedule by using scheduled tasks. The process is straightforward—it includes the following steps:

1. Download the AzCopy V10 executable file. There is nothing to install because it is an exe file.
2. Authorize AzCopy by using a SAS token at the container level with the appropriate permissions.
3. After AzCopy is authorized, the data transfer begins.

## **Notes:**

- In batch files, make sure to escape the % characters that appear in SAS tokens. This can be done by adding an additional % character next to existing % characters in the SAS token string.
- The [Secure Transfer Required](#) setting of a storage account determines whether the connection to a storage account is secured with Transport Layer Security (TLS). This setting is enabled by default. The

following batch script example recursively copies data from the Snapshot copy directory to a designated Blob container:

```
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=ZxRUJwF1LXgHS8As7HzXJOadXXVJ7PxxIX3ACpx56XY%%3D"
echo %dest%
```

The following example cmd is executed in PowerShell:

```
-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
```

## Notes:

- A similar backup feature for long-term retention will soon be available in Azure NetApp Files.
- The batch script can be used in any scenario that requires data to copied to Blob container of any region.

## Cost optimization

With volume reshaping and dynamic service level change, which is completely transparent to the database, Azure NetApp Files allows continuous cost optimizations in Azure. This capability is used in this HLD extensively to avoid overprovisioning of additional storage to handle workload spikes.

Resizing the volume can be easily accomplished by creating an Azure function in conjunction with the Azure alert logs.

## Conclusion

Whether you are targeting an all-cloud or hybrid cloud with stretch databases, Azure NetApp Files provides excellent options to deploy and manage the database workloads while reducing your TCO by making data requirements seamless to the application layer.

This document covers recommendations for planning, designing, optimizing, and scaling Microsoft SQL Server deployments with Azure NetApp Files, which can vary greatly between implementations. The right solution depends on both the technical details of the implementation and the business requirements driving the project.

## Takeaways

The key points of this document include:

- You can now use Azure NetApp Files to host the database and file share witness for SQL Server cluster.
- You can boost the application response times and deliver 99.9999% availability to provide access to SQL Server data when and where it is needed.
- You can simplify the overall complexity of the SQL Server deployment and ongoing management, such as raid striping, with simple and instant resizing.
- You can rely on intelligent operations features to help you deploy SQL Server databases in minutes and speed development cycles.
- If Azure Cloud is the destination, Azure NetApp Files is the right storage solution for optimized deployment.

## Where to find additional information

To learn more about the information described in this document, refer to the following website links:

- Solution architectures using Azure NetApp Files

<https://docs.microsoft.com/en-us/azure/azure-netapp-files/azure-netapp-files-solution-architectures>

- Benefits of using Azure NetApp Files for SQL Server deployment

<https://docs.microsoft.com/en-us/azure/azure-netapp-files/solutions-benefits-azure-netapp-files-sql-server>

- SQL Server on Azure Deployment Guide Using Azure NetApp Files

<https://www.netapp.com/pdf.html?item=/media/27154-tr-4888.pdf>

- Fault tolerance, high availability, and resilience with Azure NetApp Files

<https://cloud.netapp.com/blog/azure-anf-blr-fault-tolerance-high-availability-and-resilience-with-azure-netapp-files>

## TR-4923: SQL Server on AWS EC2 using Amazon FSx for NetApp ONTAP

Authors: Pat Sinthusan and Niyaz Mohamed, NetApp

## Introduction

Many companies that would like to migrate applications from on-premises to the cloud find that the effort is hindered by the differences in capabilities offered by on-premises storage systems and cloud storage services. That gap has made migrating enterprise applications such as Microsoft SQL Server much more problematic. In particular, gaps in the services needed to run an enterprise application such as robust snapshots, storage efficiency capabilities, high availability, reliability, and consistent performance have forced customers to make design tradeoffs or forgo application migration. With FSx for NetApp ONTAP, customers no longer need to compromise. FSx for NetApp ONTAP is a native (1st party) AWS service sold, supported, billed, and fully managed by AWS. It uses the power of NetApp ONTAP to provide the same enterprise grade storage and data management capabilities NetApp has provided on-premises for three decades in AWS as a managed service.

With SQL Server on EC2 instances, database administrators can access and customize their database environment and the underlying operating system. A SQL Server on EC2 instance in combination with [AWS FSx ONTAP](#) to store the database files, enables high performance, data management, and a simple and easy migration path using block-level replication. Therefore, you can run your complex database on AWS VPC with an easy lift-and-shift approach, fewer clicks, and no schema conversions.

## Benefits of using Amazon FSx for NetApp ONTAP with SQL Server

Amazon FSx for NetApp ONTAP is the ideal file storage for SQL Server deployments in AWS. Benefits include the following:

- Consistent high performance and throughput with low latency
- Intelligent caching with NVMe cache to improve performance
- Flexible sizing so that you can increase or shrink capacity, throughput, and IOPs on the fly
- Efficient on-premises-to-AWS block replication
- The use of iSCSI, a well-known protocol for the database environment
- Storage efficiency features like thin provisioning and zero-footprint clones
- Backup time reduction from hours to mins, thereby reducing the RTO
- Granular backup and recovery of SQL databases with the intuitive NetApp SnapCenter UI
- The ability to perform multiple test migrations before actual migration
- Shorter downtime during migration and overcoming migration challenges with file-level or I/O-level copy
- Reducing MTTR by finding the root cause after a major release or patch update

Deploying SQL Server databases on FSx ONTAP with the iSCSI protocol, as is commonly used on-premises, provides an ideal database storage environment with superior performance, storage efficiency, and data-management capabilities. Using multiple iSCSI sessions, assuming a 5% working set size, fitting a Flash Cache delivers over 100K IOPs with the FSx ONTAP service. This configuration provides complete control over performance for the most demanding applications. SQL Server running on smaller EC2 instances connected to FSx for ONTAP can perform the same as SQL Server running on a much larger EC2 instance, because only network bandwidth limits are applied against FSx for ONTAP. Reducing the size of instances also reduces the compute cost, which provides a TCO-optimised deployment. The combination of SQL using iSCSI, SMB3.0 with multichannel, continuous availability shares on FSx for ONTAP provides great advantages for SQL workloads.

## Before you begin

The combination of Amazon FSx for NetApp ONTAP and SQL Server on EC2 instance enables the creation of enterprise-level database storage designs that can meet todays most demanding application requirements. To

optimize both technologies, it is vital to understand SQL Server I/O patterns and characteristics. A well-designed storage layout for a SQL Server database supports the performance of SQL Server and the management of the SQL Server infrastructure. A good storage layout also allows the initial deployment to be successful and the environment to grow smoothly over time as your business grows.

## Prerequisites

Before you complete the steps in this document, you should have the following prerequisites:

- An AWS account
- Appropriate IAM roles to provision EC2 and FSx for ONTAP
- A Windows Active Directory domain on EC2
- All SQL Server nodes must be able to communicate with each other
- Make sure DNS resolution works and host names can be resolved. If not, use host file entry.
- General knowledge of SQL Server installation

Also, please refer to the NetApp Best Practices for SQL Server environments to ensure the best storage configuration.

## Best practice configurations for SQL Server environments on EC2

With FSx ONTAP, procuring storage is the easiest task and can be performed by updating the file system. This simple process enables dynamic cost and performance optimization as needed, it helps to balance the SQL workload, and it is also a great enabler for thin provisioning. FSx ONTAP thin provisioning is designed to present more logical storage to EC2 instances running SQL Server than what is provisioned in the file system. Instead of allocating space upfront, storage space is dynamically allocated to each volume or LUN as data is written. In most configurations, free space is also released back when data in the volume or LUN is deleted (and is not being held by any Snapshot copies). The following table provides configuration settings for dynamically allocating storage.

Setting	Configuration
Volume guarantee	None (set by default)
LUN reservation	Enabled
fractional_reserve	0% (set by default)
snap_reserve	0%
Autodelete	volume / oldest_first
Autosize	On
try_first	Autogrow
Volume tiering policy	Snapshot only
Snapshot policy	None

With this configuration, the total size of the volumes can be greater than the actual storage available in the file system. If the LUNs or Snapshot copies require more space than is available in the volume, the volumes automatically grow, taking more space from the containing file system. Autogrow allows FSx ONTAP to automatically increase the size of the volume up to a maximum size that you predetermine. There must be space available in the containing file system to support the automatic growth of the volume. Therefore, with autogrow enabled, you should monitor the free space in the containing filesystem and update the file system when needed.

Along with this, set the [space-allocation](#) option on LUN to enabled so that FSx ONTAP notifies the EC2 host when the volume has run out of space and the LUN in the volume cannot accept writes. Also, this option enables FSx for ONTAP to reclaim space automatically when the SQL Server on EC2 host deletes data. The space-allocation option is set to disabled by default.



If a space-reserved LUN is created in a none-guaranteed volume, then the LUN behaves the same as a non-space-reserved LUN. This is because a none-guaranteed volume has no space to allocate to the LUN; the volume itself can only allocate space as it is written to due to its none guarantee.

With this configuration, FSx ONTAP administrators can generally size the volume so that they must manage and monitor the used space in the LUN on the host side and in the file system.



NetApp recommends using a separate file system for SQL server workloads. If the file system is used for multiple applications, monitor the space usage of both the file system and volumes within the file system to make sure that volumes are not competing for available space.



Snapshot copies used to create FlexClone volumes are not deleted by the autodelete option.



Overcommitment of storage must be carefully considered and managed for a mission-critical application such as SQL server for which even a minimal outage cannot be tolerated. In such a case, it is best to monitor storage consumption trends to determine how much, if any, overcommitment is acceptable.

## Best Practices

1. For optimal storage performance, provision file-system capacity to 1.35x times the size of total database usage.
2. Appropriate monitoring accompanied by an effective action plan is required when using thin provisioning to avoid application downtime.
3. Make sure to set Cloudwatch and other monitoring tool alerts so that people are contacted with enough time to react as storage is filled.

## Configure Storage for SQL Server and deploy Snapcenter for Backup, Restore and clone operations

In order to perform SQL server operations with SnapCenter, you must first create volumes and LUNs for SQL server.

## Create volumes and LUNs for SQL Server

To create volumes and LUNs for SQL Server, complete the following steps:

1. Open the Amazon FSx console at <https://console.aws.amazon.com/fsx/>
2. Create an Amazon FSx for the NetApp ONTAP file system using the Standard Create option under Creation Method. This allows you to define FSxadmin and vsadmin credentials.

**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.

1. Specify the password for fsxadmin.

### 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

1. Specify the password for SVMs.

### 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

1. Create volumes by following the step listed in [Creating a volume on FSx for NetApp ONTAP](#).

### Best practices

- Disable storage Snapshot copy schedules and retention policies. Instead, use NetApp SnapCenter to coordinate Snapshot copies of the SQL Server data and log volumes.
- Configure databases on individual LUNs on separate volumes to leverage fast and granular restore functionality.
- Place user data files (.mdf) on separate volumes because they are random read/write workloads. It is common to create transaction log backups more frequently than database backups. For this reason, place transaction log files (.ldf) on a separate volume from the data files so that independent backup schedules can be created for each. This separation also isolates the sequential write I/O of the log files from the random read/write I/O of data files and significantly improves SQL Server performance.
- Tempdb is a system database used by Microsoft SQL Server as a temporary workspace, especially for I/O intensive DBCC CHECKDB operations. Therefore, place this database on a dedicated volume. In large environments in which volume count is a challenge, you can consolidate tempdb into fewer volumes and store it in the same volume as other system databases after careful planning. Data protection for tempdb is not a high priority because this database is recreated every time Microsoft SQL Server is restarted.

2. Use the following SSH command to create volumes:

```
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 -aggregate aggr1
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
```

1. Start the iSCSI service with PowerShell using elevated privileges in Windows Servers.

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

1. Install Multipath-IO with PowerShell using elevated privileges in Windows Servers.

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

1. Find the Windows initiator Name with PowerShell using elevated privileges in Windows Servers.

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

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

1. Connect to Storage virtual machines (SVM) using putty and create an iGroup.

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

1. Use the following SSH command to create LUNs:

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

1. To achieve I/O alignment with the OS partitioning scheme, use windows\_2008 as the recommended LUN type. Refer [here](#) for additional information.
2. Use the following SSH command to map igroup to the LUNs that you just created.

```
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.

```

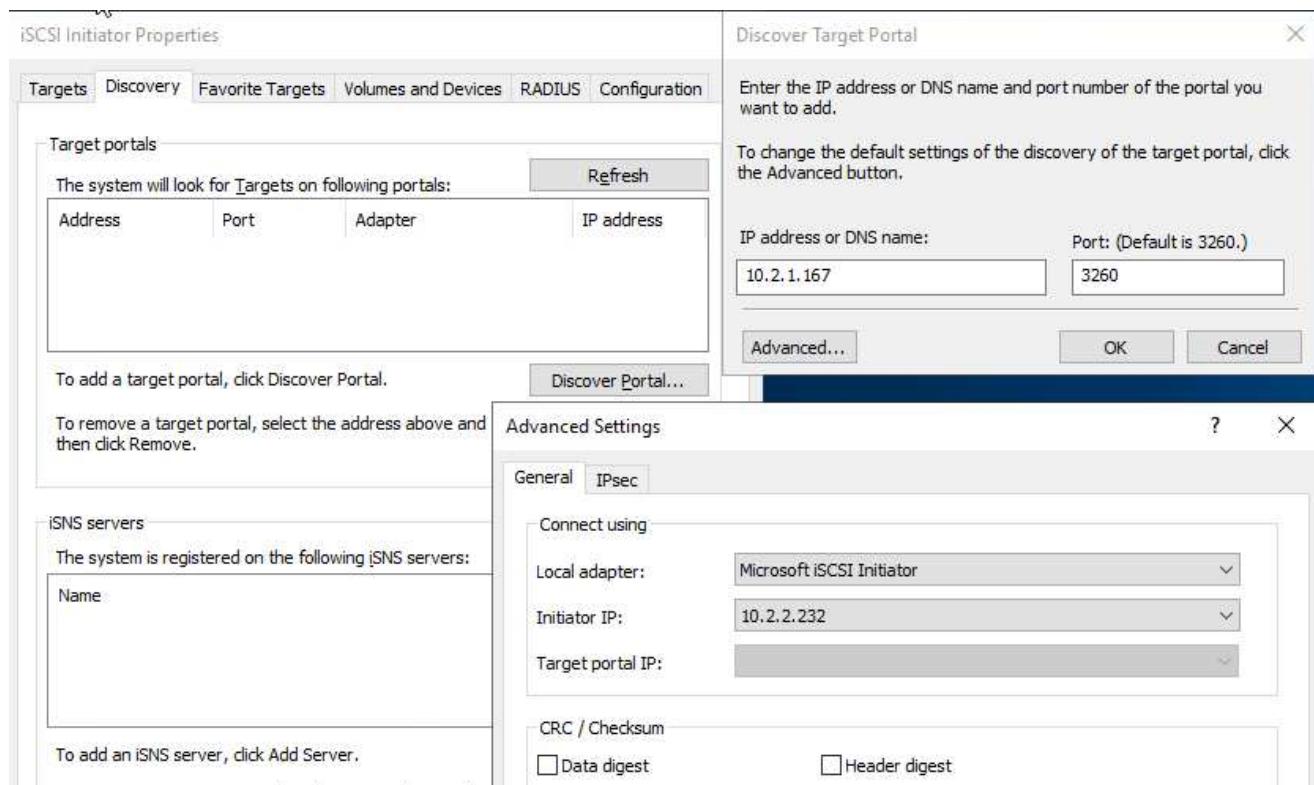
1. For a shared disk that uses the Windows Failover Cluster, run an SSH command to map the same LUN to the igroup that belong to all servers that participate in the Windows Failover Cluster.
2. Connect Windows Server to an SVM with an iSCSI target. Find the target IP address from AWS Portal.

#### svmsql (svm-09e98ab33a31b724a)

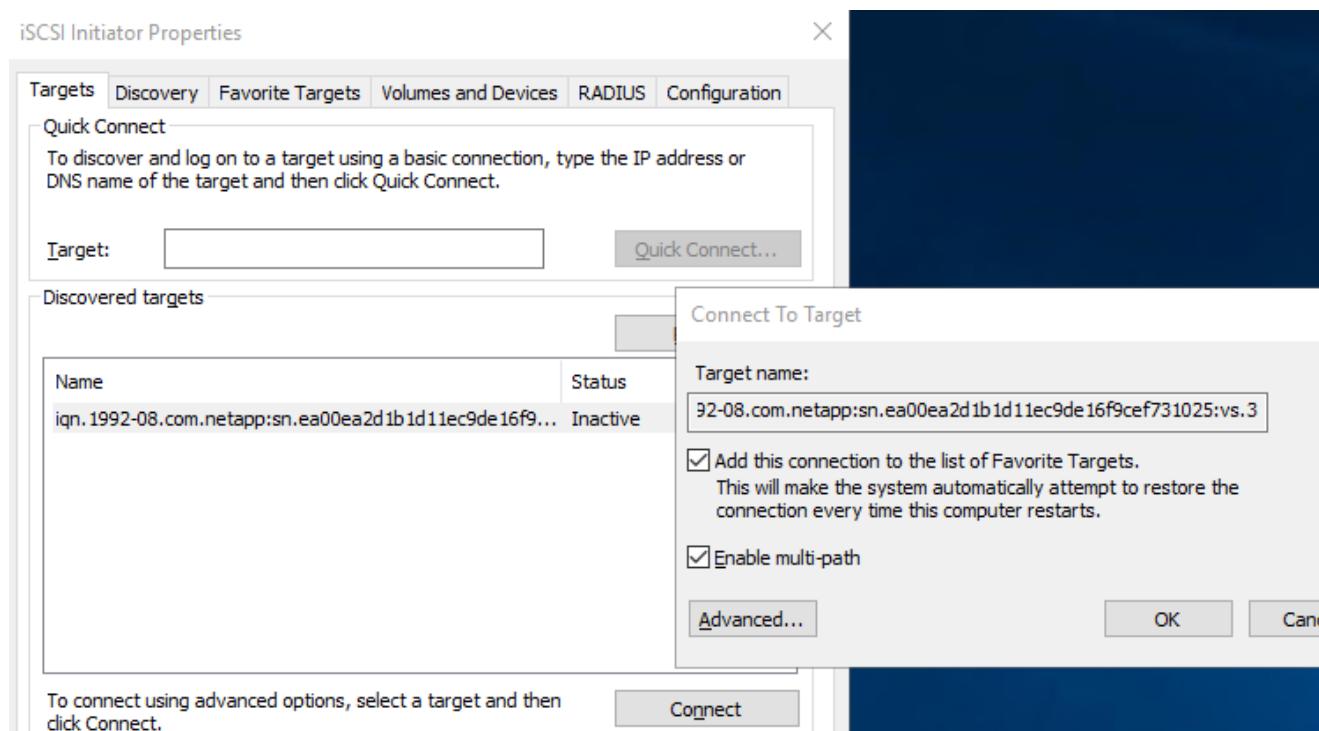
Summary	
SVM ID	Creation time
svm-09e98ab33a31b724a <a href="#">Copy</a>	2021-09-21T13:19:34-07:00
SVM name	Lifecycle state
svmsql <a href="#">Copy</a>	<span style="color: green;">✓</span> Created
UUID	Subtype
ea00ea2d-1b1d-11ec-9de1-6f9cef731025	DEFAULT
File system ID	
fs-0ab4b447ebd6082aa <a href="#">Copy</a>	
Resource ARN	
arn:aws:fsx:us-west-2:139763910815:storage-virtual-machine/fs-0ab4b447ebd6082aa/svm-09e98ab33a31b724a <a href="#">Copy</a>	
Endpoints	
Management DNS name	Management IP address
svm-09e98ab33a31b724a.fs-0ab4b447ebd6082aa.us-west-2.amazonaws.com <a href="#">Copy</a>	198.19.255.153 <a href="#">Copy</a>
NFS DNS name	NFS IP address
svm-09e98ab33a31b724a.fs-0ab4b447ebd6082aa.us-west-2.amazonaws.com <a href="#">Copy</a>	198.19.255.153 <a href="#">Copy</a>
iSCSI DNS name	iSCSI IP addresses
iscsi.svm-09e98ab33a31b724a.fs-0ab4b447ebd6082aa.us-west-2.amazonaws.com <a href="#">Copy</a>	10.2.1.167, 10.2.2.12 <a href="#">Copy</a>

1. From Server Manager and the Tools menu, select the iSCSI Initiator. Select the Discovery tab and then select Discover Portal. Supply the iSCSI IP address from previous step and select Advanced. From Local Adapter, select Microsoft iSCSI Initiator. From Initiator IP, select the IP of the server. Then

select OK to close all windows.



1. Repeat step 12 for the second iSCSI IP from the SVM.
2. Select the **Targets** tab, select **Connect**, and select **Enable multi-path**.



1. For best performance, add more sessions; NetApp recommends creating five iSCSI sessions. Select **Properties** > \***Add session** > \***Advanced** and repeat step 12.

```
$TargetPortals = ('10.2.1.167', '10.2.2.12')
foreach ($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   :
```

+

## Best practices

+

- \* Configure five iSCSI sessions per target interface for optimal performance.
- \* Configure a round-robin policy for the best overall iSCSI performance.
- \* Make sure that the allocation unit size is set to 64K for partitions when formatting the LUNs

1. Run the following PowerShell command to make sure that the iSCSI session is persisted.

```
$targets = Get-IscsiTarget
foreach ($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\ISCSIPRT\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       : fffff9988350ff010-4000013700000012
TargetNodeAddress        : iqn.1992-08.com.netapp:sn.ea00ea2d1b1d11ec9de16f9cef731025:vs.3
TargetSideIdentifier    : 0200
PSComputerName          :
```

1. Initialize disks with the following PowerShell command.

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

Number Friendly Name		Serial Number	HealthStatus	OperationalStatus	Total Size	Partition Style
0	AWS PVIDISK	vo105d1c31fcbb4c790ab	Healthy	online	30 GB	MBR
1	NETAPP LUN C-Mode	1wB0p?RmR2s2	Healthy	online	700 GB	GPT
2	NETAPP LUN C-Mode	1wB0p?RmR2s3	Healthy	online	100 GB	GPT

### 1. Run the Create Partition and Format Disk commands with PowerShell.

```
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
```

You can automate volume and LUN creation using the PowerShell script from Appendix B. LUNs can also be created using SnapCenter.

Once the volumes and LUNs are defined, you need to set up SnapCenter to be able to perform the database operations.

### SnapCenter overview

NetApp SnapCenter is next-generation data protection software for tier-1 enterprise applications. SnapCenter, with its single-pane-of-glass management interface, automates and simplifies the manual, complex, and time-consuming processes associated with the backup, recovery, and cloning of multiple databases and other application workloads. SnapCenter leverages NetApp technologies, including NetApp Snapshots, NetApp SnapMirror, SnapRestore, and NetApp FlexClone. This integration allows IT organizations to scale their storage infrastructure, meet increasingly stringent SLA commitments, and improve the productivity of administrators across the enterprise.

## SnapCenter Server requirements

The following table lists the minimum requirements for installing the SnapCenter Server and plug-in on Microsoft Windows Server.

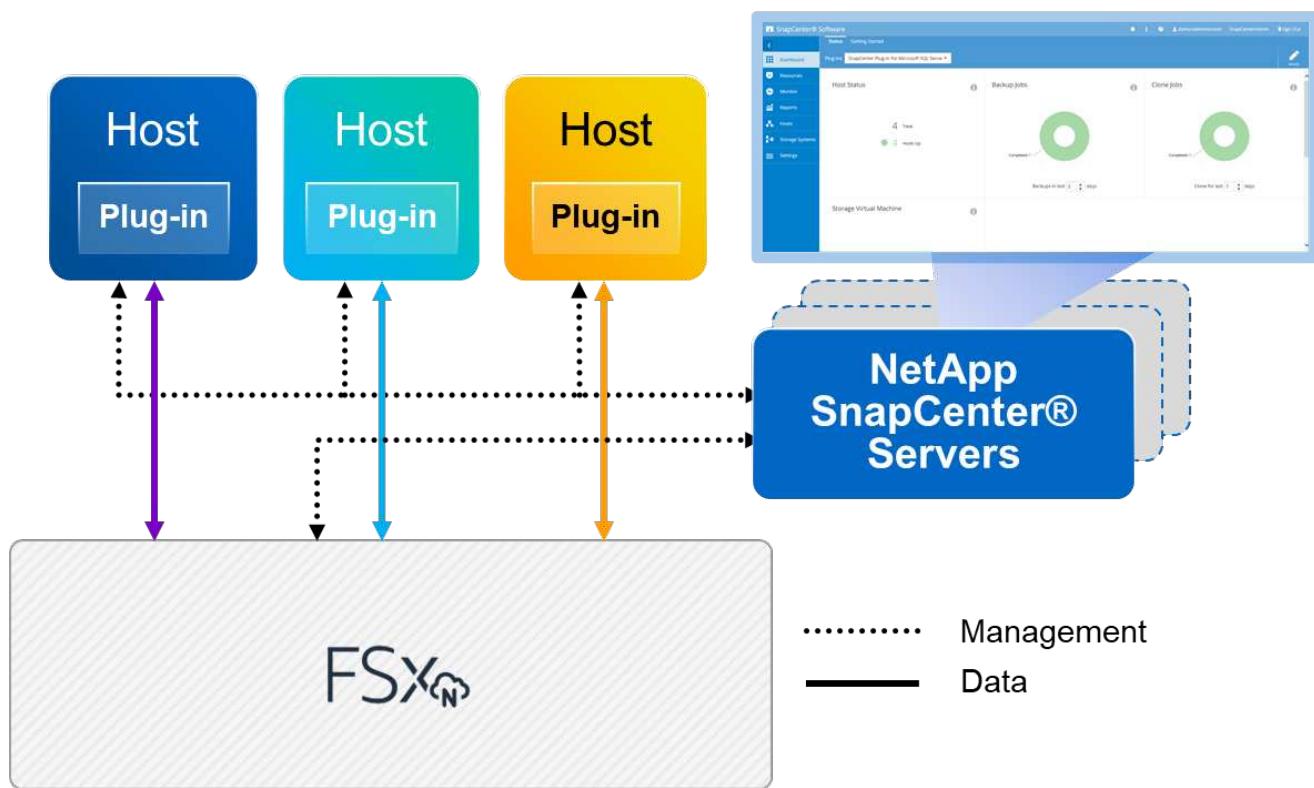
Components	Requirement
Minimum CPU count	Four cores/vCPUs
Memory	Minimum: 8GB Recommended: 32GB
Storage space	Minimum space for installation: 10GB Minimum space for repository: 10GB
Supported operating system	<ul style="list-style-type: none"><li>Windows Server 2012</li><li>Windows Server 2012 R2</li><li>Windows Server 2016</li><li>Windows Server 2019</li></ul>
Software packages	<ul style="list-style-type: none"><li>.NET 4.5.2 or later</li><li>Windows Management Framework (WMF) 4.0 or later</li><li>PowerShell 4.0 or later</li></ul>

For detailed information, refer to [space and sizing requirements](#).

For version compatibility, see the [NetApp Interoperability Matrix Tool](#).

## Database storage layout

The following figure depicts some considerations for creating the Microsoft SQL Server database storage layout when backing up with SnapCenter.



## Best practices

1. Place databases with I/O-intensive queries or with large database size (say 500GB or more) on a separate volume for faster recovery. This volume should also be backed up by separate jobs.
2. Consolidate small-to-medium size databases that are less critical or have fewer I/O requirements to a single volume. Backing up a large number of databases residing in the same volume leads to fewer Snapshot copies that need to be maintained. It is also a best practice to consolidate Microsoft SQL Server instances to use the same volumes to control the number of backup Snapshot copies taken.
3. Create separate LUNs to store full text-related files and file-streaming related files.
4. Assign separate LUNs per host to store Microsoft SQL Server log backups.
5. System databases that store database server metadata configuration and job details are not updated frequently. Place system databases/tempdb in separate drives or LUNs. Do not place system databases in the same volume as the user databases. User databases have a different backup policy, and the frequency of user database backup is not same for system databases.
6. For Microsoft SQL Server Availability Group setup, place the data and log files for replicas in an identical folder structure on all nodes.

In addition to the performance benefit of segregating the user database layout into different volumes, the database also significantly affects the time required to back up and restore. Having separate volumes for data and log files significantly improves the restore time as compared to a volume hosting multiple user data files. Similarly, user databases with a high I/O intensive application are prone to an increase in the backup time. A more detailed explanation about backup and restore practices is provided later in this document.

 Starting with SQL Server 2012 (11.x), system databases (Master, Model, MSDB, and TempDB), and Database Engine user databases can be installed with an SMB file server as a storage option. This applies to both stand-alone SQL Server and SQL Server failover cluster installations. This enables you to use FSx for ONTAP with all its performance and data management capabilities, including volume capacity, performance scalability, and data protection features, which SQL Server can take advantage of. Shares used by the application servers must be configured with the continuously available property set and the volume should be created with NTFS security style. NetApp Snapcenter cannot be used with databases placed on SMB shares from FSx for ONTAP.

 For SQL Server databases that do not use SnapCenter to perform backups, Microsoft recommends placing the data and log files on separate drives. For applications that simultaneously update and request data, the log file is write intensive, and the data file (depending on your application) is read/write intensive. For data retrieval, the log file is not needed. Therefore, requests for data can be satisfied from the data file placed on its own drive.

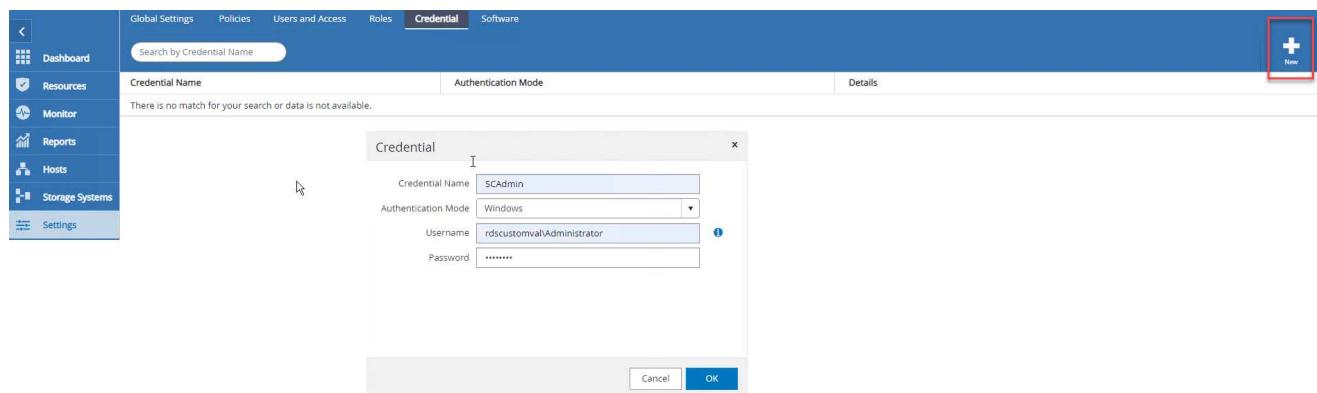
 When you create a new database, Microsoft recommends specifying separate drives for the data and logs. To move files after the database is created, the database must be taken offline. For more Microsoft recommendations, see Place Data and Log Files on Separate Drives.

## Installation and setup for SnapCenter

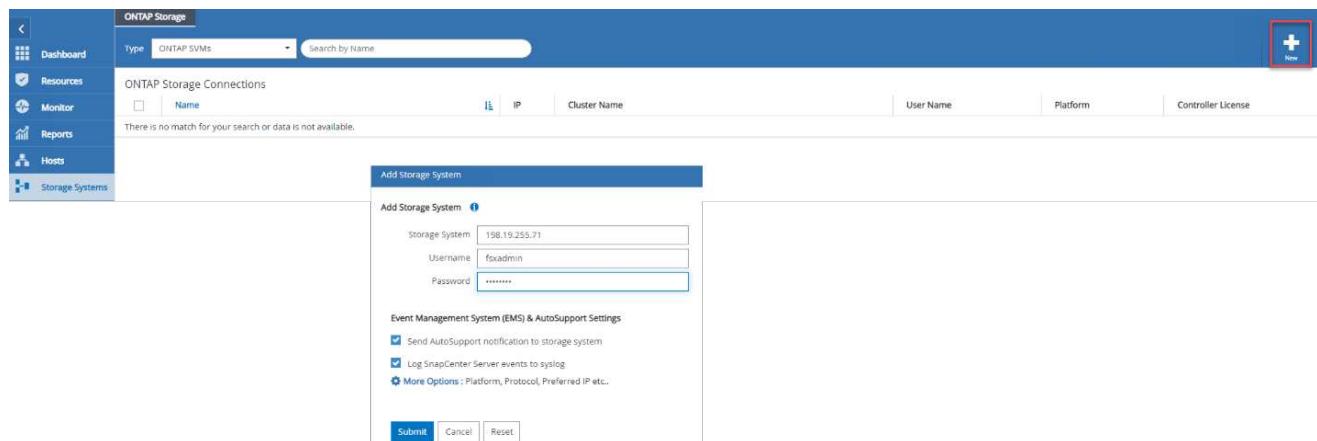
Follow the [Install the SnapCenter Server](#) and [Installing SnapCenter Plug-in for Microsoft SQL Server](#) to install and setup SnapCenter.

After Installing SnapCenter, complete the following steps to set it up.

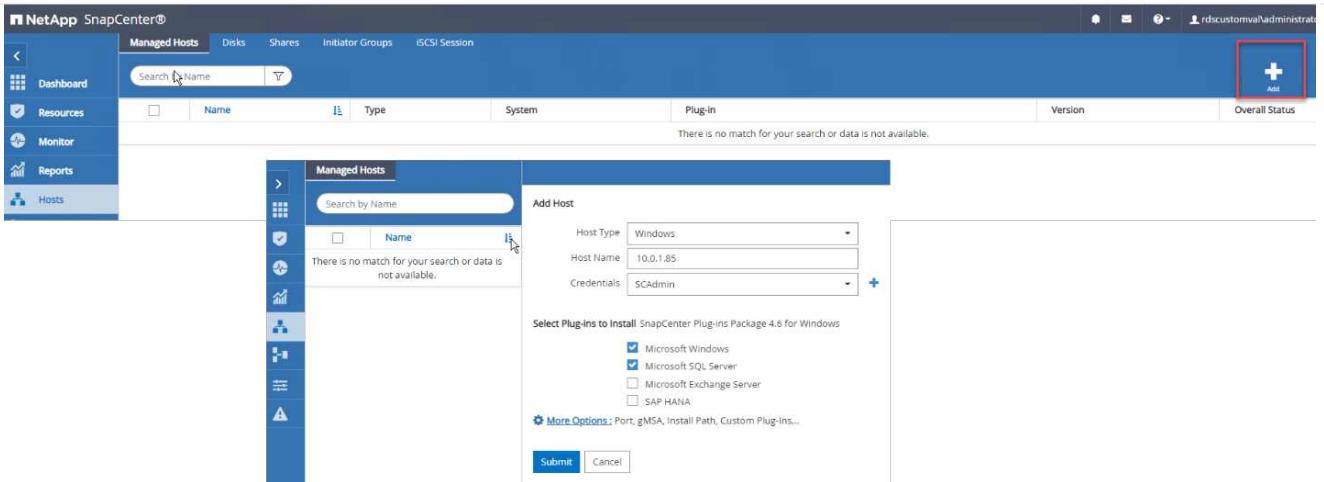
1. To set up credentials, select **Settings > New** and then enter the credential information.



1. Add the storage system by selecting **Storage Systems > New** and the provide the appropriate FSx for ONTAP storage information.



1. Add hosts by selecting **Hosts > Add**, and then provide the host information. SnapCenter automatically installs the Windows and SQL Server plug-in. This process might take some time.



After all Plug-ins are installed, you must configure the log directory. This is the location where the transaction log backup resides. You can configure the log directory by selecting the host and then select configure the log directory.



SnapCenter uses a host log directory to store transaction log backup data. This is at the host and instance level. Each SQL Server host used by SnapCenter must have a host log directory configured to perform log backups. SnapCenter has a database repository, so metadata related to backup, restore, or cloning operations is stored in a central database repository.

The size of the host log directory is calculated as follows:

$$\text{Size of host log directory} = \text{system database size} + (\text{maximum DB LDF size} \times \text{daily log change rate \%} \times (\text{Snapshot copy retention}) \div (1 - \text{LUN overhead space \%}))$$

The host log directory sizing formula assumes the following:

- A system database backup that does not include the tempdb database
- A 10% LUN overhead spacePlace the host log directory on a dedicated volume or LUN. The amount of data in the host log directory depends on the size of the backups and the number of days that backups are retained.

**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...

If the LUNs have already been provisioned, you can select the mount point to represent the host log directory.

Configure Plug-in for SQL Server x

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

Configure host log directory

Host log directory

Choose directory on NetApp Storage

RDSAMAZ-FFIDFMR.rdscustomval.com

D:\FSxN\Data\  
D:\FSxN\HLD\  
D:\FSxN\Log\

Now you are ready to perform backup, restore and clone operations for SQL Server.

## Backup database with SnapCenter

After placing the database and log files on the FSx ONTAP LUNs, SnapCenter can be used to back up the databases. The following processes are used to create a full backup.

### Best Practices

- In SnapCenter terms, RPO can be identified as the backup frequency, for example, how frequently you want to schedule the backup so that you can reduce the loss of data to up to few minutes. SnapCenter allows you to schedule backups as frequently as every five minutes. However, there might be a few instances in which a backup might not complete within five minutes during peak transaction times or when the rate of change of data is more in the given time. A best practice is to schedule frequent transaction log backups instead of full backups.
- There are numerous approaches to handle the RPO and RTO. One alternative to this backup approach is to have separate backup policies for data and logs with different intervals. For example, from SnapCenter, schedule log backups in 15-minute intervals and data backups in 6-hour intervals.
- Use a resource group for a backup configuration for Snapshot optimization and the number of jobs to be managed.

1. Select **Resources**, and then select **Microsoft SQL Server** \*on the drop-down menu on the top left. Select \*Refresh Resources.

The screenshot shows the NetApp SnapCenter interface. On the left, a sidebar navigation includes Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area has a dropdown menu set to "Microsoft SQL Server". Below it, a search bar says "search by name". A table lists databases: DWConfiguration, DWDiagnostic, DWQueue, master, model, msdb, SeattleRetail, and tempdb. Columns include Name, Instance, Host, Last Backup, Overall Status, and Type. Most databases are listed as "Not available for backup".

1. Select the database to be backed up, then select **Next** and (\*) to add the policy if one has not been created. Follow the \*New SQL Server Backup Policy to create a new policy.

The screenshot shows the "Policies" step of the backup wizard. It features a numbered progress bar (1-5) where step 1 is "Resource" (highlighted in blue), step 2 is "Policies" (highlighted in blue), step 3 is "Verification", step 4 is "Notification", and step 5 is "Summary". Below the progress bar, a message says "Select one or more policies and configure schedules". A dropdown menu shows "Full Backup". To the right, there's a "Configure Schedules for selected policies" section with tabs for "Policy", "Applied Schedules", and "Configure Schedules". Under "Policy", "Full Backup" is selected. Under "Applied Schedules", "None" is listed. A note below says "To schedule operations select a policy that has the appropriate schedule associated, or modify the selected policy to allow schedules." A cursor arrow points to the "Configure Schedules" tab.

1. Select the verification server if necessary. This server is the server that SnapCenter runs DBCC CHECKDB after a full backup has been created. Click **Next** for notification, and then select **Summary** to review. After reviewing, click **Finish**.

1. Click **Back up Now** to test the backup. In the pop-up windows, select **Backup**.

### Backup

Create a backup for the selected resource

Resource Name	SeattleRetail
Policy	Full Backup
<input type="checkbox"/> Verify after backup	

**Cancel** **Backup**

1. Select **Monitor** to verify that the backup has been completed.

Jobs						
ID		Status	Name	Start date	End date	Owner
94	✓	Backup of Resource Group 'RDSAMAZ-FFIDFMR_SeattleRetail' with policy 'Full Backup'		03/29/2022 1:47:30 AM	03/29/2022 1:47:41 AM	RDSCUSTOMVAL\administrator
93	✓	Create Resource Group 'RDSAMAZ-FFIDFMR_SeattleRetail'		03/29/2022 1:45:24 AM	03/29/2022 1:45:26 AM	RDSCUSTOMVAL\administrator
92	✓	Create Policy 'Full Backup'		03/29/2022 1:41:37 AM	03/29/2022 1:41:40 AM	RDSCUSTOMVAL\administrator
91	✓	Discover resources for all hosts		03/29/2022 1:38:12 AM	03/29/2022 1:38:17 AM	RDSCUSTOMVAL\administrator

## Best Practices

- Backup the transaction log backup from SnapCenter so that during the restoration process, SnapCenter can read all the backup files and restore in sequence automatically.
- If third party products are used for backup, select Copy backup in SnapCenter to avoid log sequence issues, and test the restore functionality before rolling into production.

## Restore database with SnapCenter

One of the major benefits of using FSx ONTAP with SQL Server on EC2 is its ability to perform fast and granular restore at each database level.

Complete the following steps to restore an individual database to a specific point in time or up to the minute with SnapCenter.

1. Select Resources and then select the database that you would like to restore.

1. Select the backup name that the database needs to be restored from and then select restore.
2. Follow the **Restore** pop-up windows to restore the database.
3. Select **Monitor** to verify that the restore process is successful.

ID	Status	Name	Start date	End date	Owner
96	✓	Restore 'RDSAMAZ-FFIDFMRSeattleRetail'	03/29/2022 1:54:31 AM	03/29/2022 1:56:26 AM	ROSCUSTOMVAL\administrator
94	✓	Backup of Resource Group 'RDSAMAZ-FFIDFMR_SeattleRetail' with policy 'Full Backup'	03/29/2022 1:47:30 AM	03/29/2022 1:47:41 AM	ROSCUSTOMVAL\administrator
93	✓	Create Resource Group 'RDSAMAZ-FFIDFMR_SeattleRetail'	03/29/2022 1:45:24 AM	03/29/2022 1:45:28 AM	ROSCUSTOMVAL\administrator
92	✓	Create Policy 'Full Backup'	03/29/2022 1:41:37 AM	03/29/2022 1:41:40 AM	ROSCUSTOMVAL\administrator
91	✓	Discover resources for all hosts	03/29/2022 1:38:12 AM	03/29/2022 1:38:17 AM	ROSCUSTOMVAL\administrator
88	✓	Discover resources for host 'RDSAMAZ-FFIDFMR.rdscustomval.com'	03/28/2022 10:55:17 PM	03/28/2022 10:55:18 PM	ROSCUSTOMVAL\administrator
87	✓	Discover resources for host 'RDSAMAZ-FFIDFMR.rdscustomval.com'	03/28/2022 10:41:18 PM	03/28/2022 10:41:19 PM	ROSCUSTOMVAL\administrator

## Considerations for an instance with a large number of small-to-large size databases

SnapCenter can back up a large number of sizeable databases in an instance or group of instances within a resource group. The size of a database is not the major factor in backup time. The duration of a backup can vary depending on number of LUNs per volume, the load on Microsoft SQL Server, the total number of databases per instance, and, specifically, the I/O bandwidth and usage. While configuring the policy to back up databases from an instance or resource group, NetApp recommends that you restrict the maximum database backed up per Snapshot copy to 100 per host. Make sure the total number of Snapshot copies does not exceed the 1,023-copy limit.

NetApp also recommends that you limit the backup jobs running in parallel by grouping the number of databases instead of creating multiple jobs for each database or instance. For optimal performance of the backup duration, reduce the number of backup jobs to a number that can back up around 100 or fewer databases at a time.

As previously mentioned, I/O usage is an important factor in the backup process. The backup process must wait to quiesce until all the I/O operations on a database are complete. Databases with highly intensive I/O operations should be deferred to another backup time or should be isolated from other backup jobs to avoid affecting other resources within the same resource group that are to be backed up.

For an environment that has six Microsoft SQL Server hosts hosting 200 databases per instance, assuming four LUNs per host and one LUN per volume created, set the full backup policy with the maximum databases backed up per Snapshot copy to 100. Two hundred databases on each instance are laid out as 200 data files distributed equally on two LUNs, and 200 log files are distributed equally on two LUNs, which is 100 files per LUN per volume.

Schedule three backup jobs by creating three resource groups, each grouping two instances that include a total of 400 databases.

Running all three backup jobs in parallel backs up 1,200 databases simultaneously. Depending on the load on the server and I/O usage, the start and end time on each instance can vary. In this instance, a total of 24 Snapshot copies are created.

In addition to the full backup, NetApp recommends that you configure a transaction log backup for critical databases. Make sure that the database property is set to full recovery model.

### Best practices

1. Do not include the tempdb database in a backup because the data it contains is temporary. Place tempdb on a LUN or an SMB share that is in a storage system volume in which Snapshot copies will not be created.
2. A Microsoft SQL Server instance with a high I/O intensive application should be isolated in a different backup job to reduce the overall backup time for other resources.
3. Limit the set of databases to be simultaneously backed up to approximately 100 and stagger the remaining set of database backups to avoid a simultaneous process.
4. Use the Microsoft SQL Server instance name in the resource group instead of multiple databases because whenever new databases are created in Microsoft SQL Server instance, SnapCenter automatically considers a new database for backup.
5. If you change the database configuration, such as changing the database recovery model to the full recovery model, perform a backup immediately to allow up-to-the-minute restore operations.
6. SnapCenter cannot restore transaction log backups created outside of SnapCenter.
7. When cloning FlexVol volumes, make sure that you have sufficient space for the clone metadata.

8. When restoring databases, make sure that sufficient space is available on the volume.
9. Create a separate policy to manage and back up system databases at least once a week.

## Cloning databases with SnapCenter

To restore a database onto another location on a dev or test environment or to create a copy for business analysis purposes, the NetApp best practice is to leverage the cloning methodology to create a copy of the database on the same instance or an alternate instance.

The cloning of databases that are 500GB on an iSCSI disk hosted on a FSx for ONTAP environment typically takes less than five minutes. After cloning is complete, the user can then perform all the required read/write operation on the cloned database. Most of the time is consumed for disk scanning (diskpart). The NetApp cloning procedure typically take less than 2 minutes regardless of the size of the databases.

The cloning of a database can be performed with the dual method: you can create a clone from the latest backup or you can use clone life-cycle management through which the latest copy can be made available on the secondary instance.

SnapCenter allows you to mount the clone copy on the required disk to maintain the format of the folder structure on the secondary instance and continue to schedule backup jobs.

### Clone databases to the new database name in the same instance

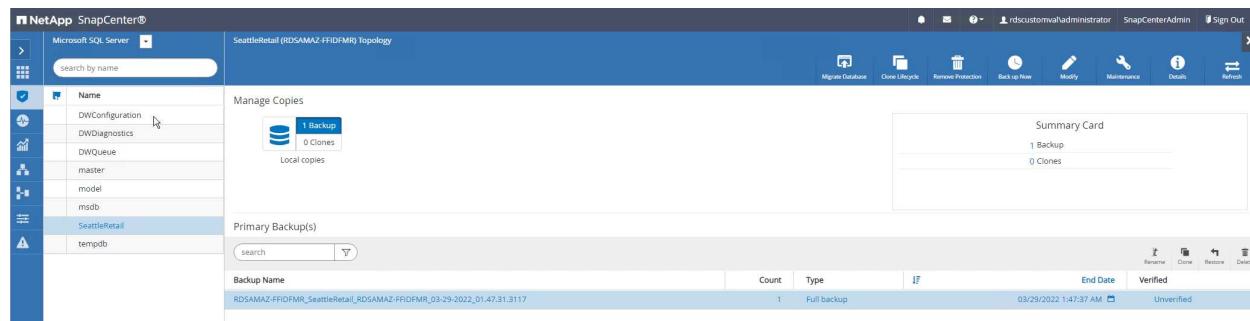
The following steps can be used to clone databases to the new database name in the same SQL server instance running on EC2:

1. Select Resources and then the database that need to be cloned.
2. Select the backup name that you would like to clone and select Clone.
3. Follow the clone instructions from the backup windows to finish the clone process.
4. Select Monitor to make sure that cloning is completed.

## Clone databases into the new SQL Server instance running on EC2

The following step are used to clone databases to the new SQL server instance running on EC2:

1. Create a new SQL Server on EC2 in the same VPC.
2. Enable the iSCSI protocol and MPIO, and then setup the iSCSI connection to FSx for ONTAP by following step 3 and 4 in the section “Create volumes and LUNs for SQL Server.”
3. Add a new SQL Server on EC2 into SnapCenter by follow step 3 in the section “Installing and setup for SnapCenter.”
4. Select Resource > View Instance, and then select Refresh Resource.
5. Select Resources, and then the database that you would like to clone.
6. Select the backup name that you would like to clone, and then select Clone.



The screenshot shows the NetApp SnapCenter interface. On the left sidebar, under 'Resources', 'SeattleRetail' is selected. In the main pane, 'Manage Copies' shows '1 Backup' and '0 Clones'. Below it, 'Primary Backup(s)' lists a single backup named 'RDSAMAZ-FFIDFMR\_SeattleRetail\_RDSAMAZ-FFIDFMR\_03-29-2022\_01.47.31.3117'. A summary card on the right indicates '1 Backup' and '0 Clones'.

1. Follow the Clone from Backup instructions by providing the new SQL Server instance on EC2 and instance name to finish the clone process.
2. Select Monitor to make sure that cloning is completed.



The screenshot shows the NetApp SnapCenter interface with the 'Jobs' tab selected. It displays a table of tasks:

ID	Status	Name	Start date	End date	Owner
108	✓	Clone from backup 'RDSAMAZ-FFIDFMR_SeattleRetail_RDSAMAZ-FFIDFMR_03-29-2022_01.47.31.3117'	3/30/2022 6:09:10 PM	3/30/2022 6:09:55 PM	rdscustomvaladministrator
107	✓	Discover resources for all hosts	03/30/2022 6:06:40 PM	03/30/2022 6:06:54 PM	RDSCUSTOMVALAdministrator

To learn more about this process, watch the following video:

[Clone databases into the new SQL Server instance running on EC2](#)

## Appendices

### Appendix A: YAML file for use in Cloud Formation Template

The following .yaml file can be used with the Cloud Formation Template in AWS Console.

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

To automate ISCSI LUN creation and NetApp SnapCenter installation with PowerShell, clone the repo from [this GitHub link](#).

## Appendix B: Powershell scripts for provisioning volumes and LUNs

The following script is used to provision volumes and LUNs and also to set up iSCSI based on the instruction provided above. There are two PowerShell scripts:

- `_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=(

'1_'+$hostname+'_log');lunsize=$fsxN.loglunsize})
    } else {
        $volsluns
    }
    +=(@{volname=('v_'+$hostname+'_data'+[string]$i);volsize=$fsxN.datavols
ize;lunname=('1_'+$hostname+'_data'+[string]$i);lunsize=$fsxN.datalunsi
ze})
}
}

$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.svmpip -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 aggr1
-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){
    $sshcmd = "lun create -path /vol/" + $vollun.volname + "/" +
    $vollun.lunname + " -size " + $vollun.lunsize + " -ostype Windows_2008
    "#-vserver " +$vserver
    $return = Invoke-SSHCommand -Command $sshcmd -SSHSession
    $session
        #map all luns to igroup
        $sshcmd = "lun map -path /vol/" + $vollun.volname + "/" +
    $vollun.lunname + " -igroup " + $igroup
        $return = Invoke-SSHCommand -Command $sshcmd -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 Partition 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 =
'vesadmin';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
....
```

Run the file EnableMPIO.ps1 first and the second script executes automatically after the server has been rebooted. These PowerShell scripts can be removed after they have been executed due to credential access to the SVM.

## Where to find additional information

- Amazon FSx for NetApp ONTAP

<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html>

- Getting Started with FSx for NetApp ONTAP

<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/getting-started.html>

- Overview of the SnapCenter interface

<https://www.youtube.com/watch?v=lVEBF4kV6Ag&t=0s>

- Tour through SnapCenter navigation pane options

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

- Setup SnapCenter 4.0 for SQL Server plug-in

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

- How to back up and restore databases using SnapCenter with SQL Server plug-in

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

- How to clone a database using SnapCenter with SQL Server plug-in

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

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

Author(s): Niyaz Mohammed, Carine Ngwekwe - NetApp Solutions Engineering

This document covers the steps necessary to perform backup and recovery for Microsoft SQL Server on AWS

FSx for ONTAP with SnapCenter. This includes the following information:

- NetApp SnapCenter configuration
- SnapCenter backup operations
- Backup operation for an FCI database
- Backup operation for multiple databases
- Restore and recovery

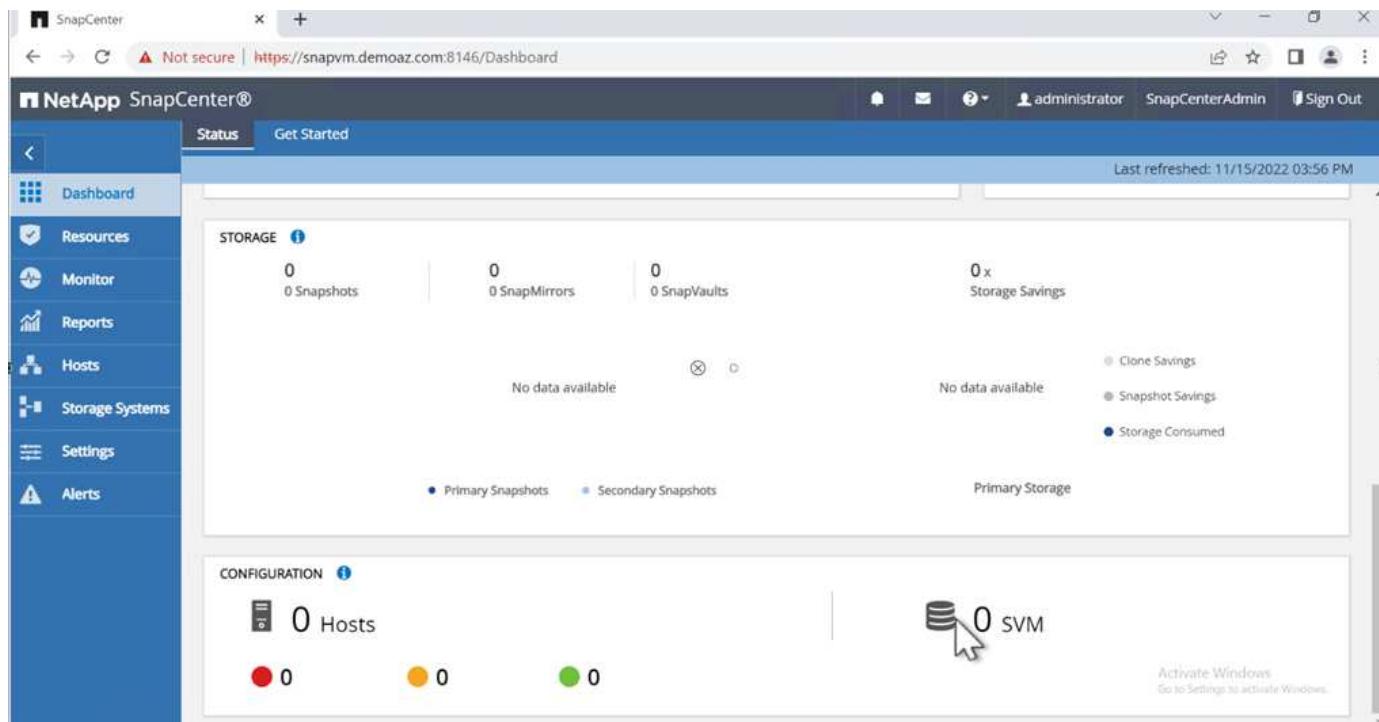
## SnapCenter Configuration

The following steps must be performed for SnapCenter configuration and the protection of Microsoft SQL Server resources. Each of the following steps is detailed in the following sections.

1. Configure sysadmin credentials for the SQL Server backup and restore user.
2. Configure storage settings. Provide Amazon Web Services (AWS) management credential to access the Amazon FSx for NetApp ONTAP storage virtual machines (SVMs) from SnapCenter.
3. Add a SQL Server host to SnapCenter. Deploy and install the required SnapCenter Plug-ins.
4. Configure policies. Define the backup operation type, retention, and optional Snapshot backup replication.
5. Configure and protect the Microsoft SQL Server database.

## SnapCenter newly installed user interface

Configure credentials for SQL Server backup and restore the user with sysadmin rights.



NetApp recommends using role-based access control (RBAC) to delegate data protection and management capabilities to individual users across the SnapCenter and window hosts. The user must have access to the SQL Server hosting the database. For multiple hosts, the username and password must be the same across the various hosts. Furthermore, to enable SnapCenter to deploy the required plug-in on SQL Server hosts, you must register the domain information for SnapCenter to validate your credentials and hosts.

Expand the following sections to see the detailed instructions on how to complete each step.

## Add the credentials

Go to **Settings**, select **Credentials**, and click (+).

The screenshot shows the NetApp SnapCenter web interface. The top navigation bar includes links for Global Settings, Policies, Users and Access, Roles, Credential (which is highlighted in blue), and Software. Below the navigation is a search bar labeled "Search by Credential Name". A main table displays columns for "Credential Name" and "Authentication Mode". A message at the bottom of the table states, "There is no match for your search or data is not available." On the left side, there is a vertical sidebar with icons for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings (which is also highlighted in blue), and Alerts.

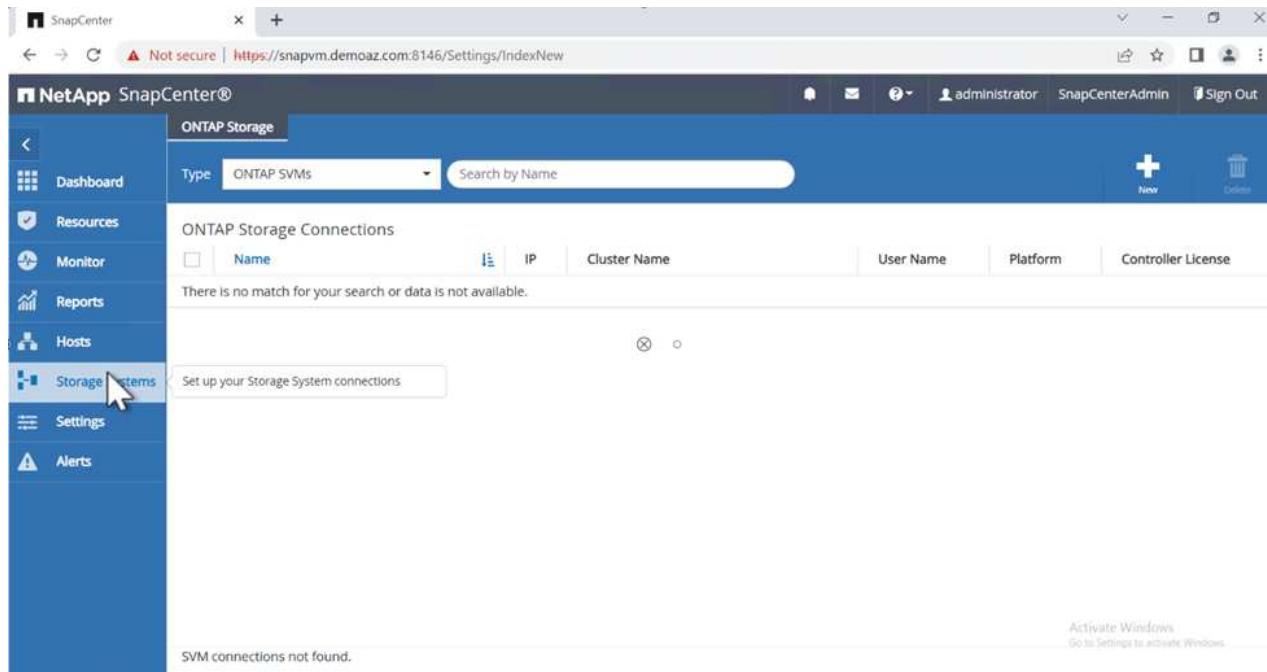
The new user must have administrator rights on the SQL Server host.

This screenshot shows a modal dialog titled "Credential" for creating a new credential. The form contains four fields: "Credential Name" (set to "Demoaz"), "Authentication Mode" (set to "Windows"), "Username" (set to "demoaz\clusteradmin"), and "Password" (represented by a series of dots). Below the form is a status message "Setting credential..." with a progress bar. At the bottom right are "Cancel" and "OK" buttons.

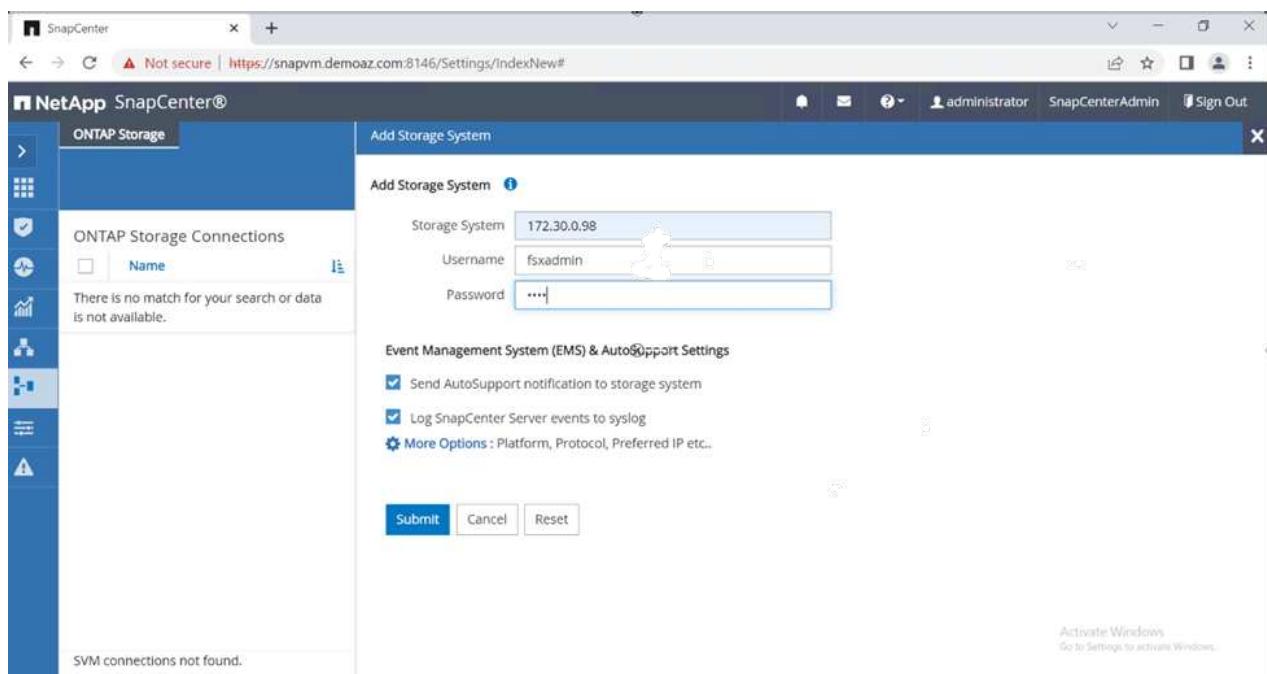
## Configure storage

To configure storage in SnapCenter, complete the following steps:

1. In the SnapCenter UI, select **Storage Systems**. There are two storage types, **ONTAP SVM** and **ONTAP Cluster**. By default, the storage type is **ONTAP SVM**.
2. Click (+) to add the storage system information.



3. Provide the **FSx for ONTAP management endpoint**.



4. The SVM is now configured in SnapCenter.

SnapCenter

Not secure | https://snapvm.demoaz.com:8146/Settings/IndexNew#

NetApp SnapCenter®

ONTAP Storage

Type: ONTAP SVMs Search by Name

ONTAP Storage Connections

Name	IP	Cluster Name	User Name	Platform	Controller License
ESXSVMTESRDS		rdsfsxTest01		PSX	Not applicable

Total 1

Activate Windows  
Go to Settings to activate Windows.

The screenshot shows the NetApp SnapCenter web interface. The left sidebar contains navigation links: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area is titled 'ONTAP Storage' and shows 'ONTAP Storage Connections'. A table lists one connection: 'ESXSVMTESRDS' with 'rdsfsxTest01' as the Cluster Name, 'PSX' as the Platform, and 'Not applicable' as the Controller License. The top right corner shows user information: administrator, SnapCenterAdmin, and Sign Out. A browser header at the top indicates the URL is https://snapvm.demoaz.com:8146/Settings/IndexNew#, and a note says 'Not secure'.

## Add a SQL Server host to SnapCenter

To add a SQL Server host, complete the following steps:

1. From the Host tab, click (+) to add the Microsoft SQL Server host.

2. Provide the fully qualified domain name (FQDN) or IP address of the remote host.



The credentials are populated by default.

3. Select the option for Microsoft windows and Microsoft SQL Server and then submit.

The SQL Server packages are installed.

The screenshot shows the NetApp SnapCenter interface. The left sidebar has tabs for Dashboard, Resources, Monitor, Reports, Hosts (which is selected), Storage Systems, Settings, and Alerts. The main content area is titled "Managed Hosts" and shows a table with one row:

Name	Type	System	Plug-in	Version	Overall Status
FSXCLUSTER.Demoaz.com	Windows	Cluster			Installing plug-in

Total 1 hosts are managed.

1. After the installation is complete, go to the **Resource** tab to verify whether all FSx for ONTAP iSCSI volumes are present.

The screenshot shows the NetApp SnapCenter interface. The left sidebar has tabs for Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area is titled "File Systems" and shows a table with six rows:

Name	Host	Storage Layout	Resource Groups	Policies	Last Backup	Overall Status
D:\	FSXCLUSTER.Demo...STER.Demoaz.com	FSXSVMTESRDS:/..._FCIDATA/FCIDATA				Not protected
E:\	FSXCLUSTER.Demo...STER.Demoaz.com	FSXSVMTESRDS:/..._L/FCILOG/FCILOG				Not protected
F:\	FSXCLUSTER.Demo...STER.Demoaz.com	FSXSVMTESRDS:/..._ACKUP/FCIBACKUP				Not protected
G:\	FSXCLUSTER.Demo...STER.Demoaz.com	FSXSVMTESRDS:/..._SNAPLOG/SNAPLOG				Not protected
H:\	FSXCLUSTER.Demo...STER.Demoaz.com	FSXSVMTESRDS:/..._FCITEMP/FCITEMP				Not protected
K:\	FSXCLUSTER.Demo...STER.Demoaz.com	FSXSVMTESRDS:/..._UORUM/FCIQUORUM				Not protected

Total 6 file systems are listed. A hand cursor icon is pointing at the first row (D:\). The bottom navigation bar shows "Activity" and "The 5 most recent jobs are displayed".

## Configure log directory

To configure a host log directory, complete the following steps:

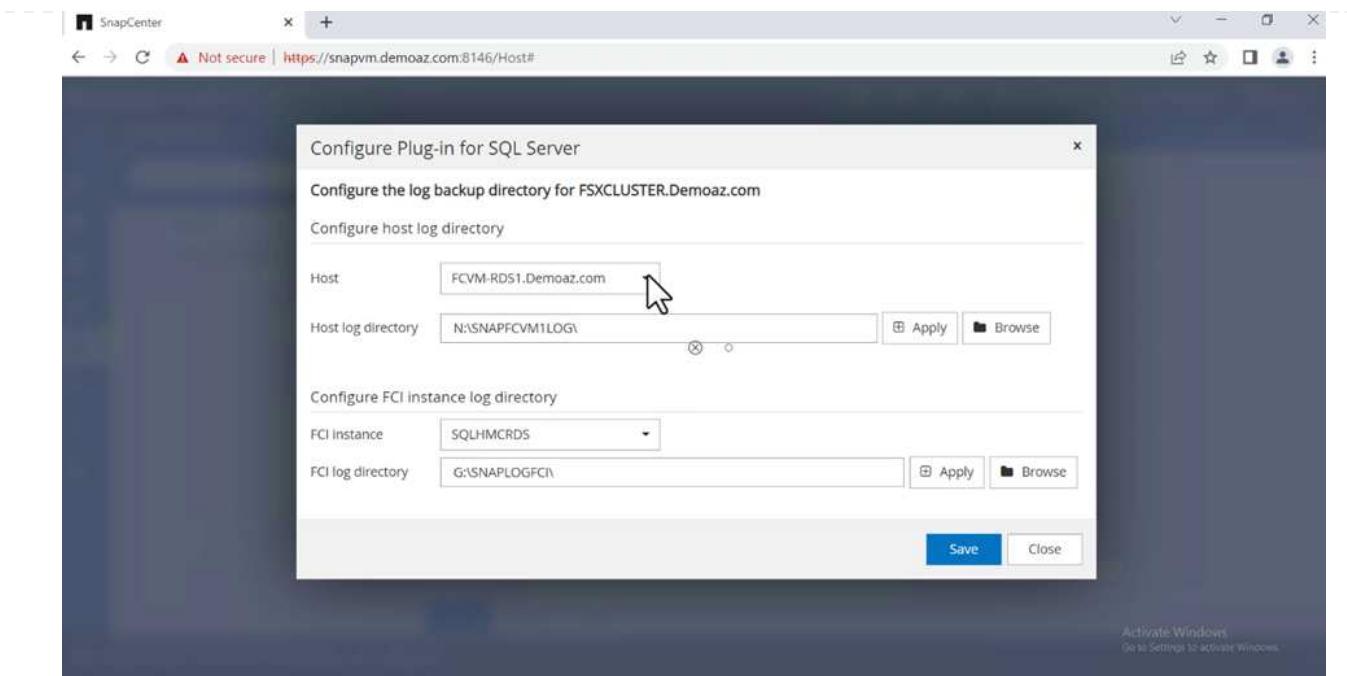
1. Click the check box. A new tab opens.

The screenshot shows the NetApp SnapCenter web interface. On the left, there's a sidebar with icons for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area is titled "Managed Hosts" and contains a table with three rows. The first row has a checked checkbox and is highlighted in blue. The second and third rows have unchecked checkboxes. The columns are: Name, Type, System, Plug-in, Version, and Overall Status. The first host listed is "FSXCLUSTER.Demoaz.com". The overall status for all hosts is "Configure log directory". At the bottom right of the interface, there's a message: "Activate Windows Go to Settings to activate Windows".

2. Click the **configure log directory** link.

This screenshot shows the "Host Details" page for the host "FSXCLUSTER.Demoaz.com". The left sidebar shows the "Managed Hosts" list with the same three hosts as the previous screen. The main panel displays the host's name, IP address, overall status (which now includes "Configure log directory"), host type (Windows), system (Cluster), credentials (Demoaz), and plug-ins (SnapCenter Plug-ins package 4.7.0.877 for Windows). Under the plug-ins section, there are links for "Microsoft Windows" and "Microsoft SQL Server" with options to "Remove" or "Configure log directory". At the bottom of the panel are "Submit", "Cancel", and "Reset" buttons. The overall status for the host is "Configure log directory".

3. Select the drive for the host log directory and the FCI instance log directory. Click **Save**. Repeat the same process for the second node in the cluster. Close the window.



The host is now in a running state.

The screenshot shows the NetApp SnapCenter interface with the 'Managed Hosts' tab selected. The left sidebar includes 'Dashboard', 'Resources', 'Monitor', 'Reports', 'Hosts' (which is selected), 'Storage Systems', 'Settings', and 'Alerts'. The main area displays a table of managed hosts:

Name	Type	System	Plug-in	Version	Overall Status
FSXCLUSTER.Demoaz.com	Windows	Cluster	Microsoft Windows Server, Microsoft SQL Server	4.7	<span>Running</span>

A hand cursor is hovering over the 'Running' status indicator for the host entry. The status bar at the bottom right says 'Activate Windows Go to Settings to activate Windows.'

1. From the **Resources** tab, we have all the servers and databases.

The screenshot shows the NetApp SnapCenter interface for a Microsoft SQL Server instance. The left sidebar has a blue background with icons for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area has a white background with a header bar containing the title 'NetApp SnapCenter®' and a dropdown menu set to 'Microsoft SQL Server'. Below the header is a toolbar with buttons for 'View' (set to 'Database'), 'refresh', and 'New Resource Group'. A search bar says 'search by name'. To the right of the search bar are two buttons: 'Refresh Resources' and a plus sign for 'New Resource Group'. The main content area is a table with the following columns: Name, Instance, Host, Last Backup, Overall Status, and Type. The table lists nine databases:

Name	Instance	Host	Last Backup	Overall Status	Type
INVENTORYDB1	SQLHMCARDS	FSXCLUSTER.Demoaz.com		Not protected	User database
INVENTORYDB2	SQLHMCARDS	FSXCLUSTER.Demoaz.com		Not protected	User database
INVENTORYDB3	SQLHMCARDS	FSXCLUSTER.Demoaz.com		Not protected	User database
INVENTORYDB4	SQLHMCARDS	FSXCLUSTER.Demoaz.com		Not protected	User database
INVENTORYDB5	SQLHMCARDS	FSXCLUSTER.Demoaz.com		Not protected	User database
master	SQLHMCARDS	FSXCLUSTER.Demoaz.com		Not protected	System database
model	SQLHMCARDS	FSXCLUSTER.Demoaz.com		Not protected	System database
Total 9					

At the bottom of the interface, there is a footer bar with the following information: 'Activity' (with a tooltip 'The 5 most recent jobs are displayed'), job status counts (0 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, 0 Queued), and links to 'Activate Windows' and 'Go to Settings to activate Windows'.

## Configure a backup policy

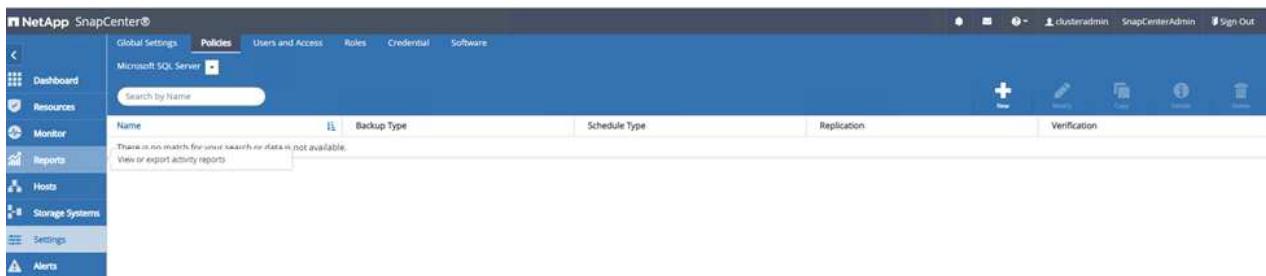
A backup policy is a set of rules that govern how to manage, schedule, and retain backup. It helps with the backup type and frequency based on your company's SLA.

Expand the following sections to see the detailed instructions on how to complete each step.

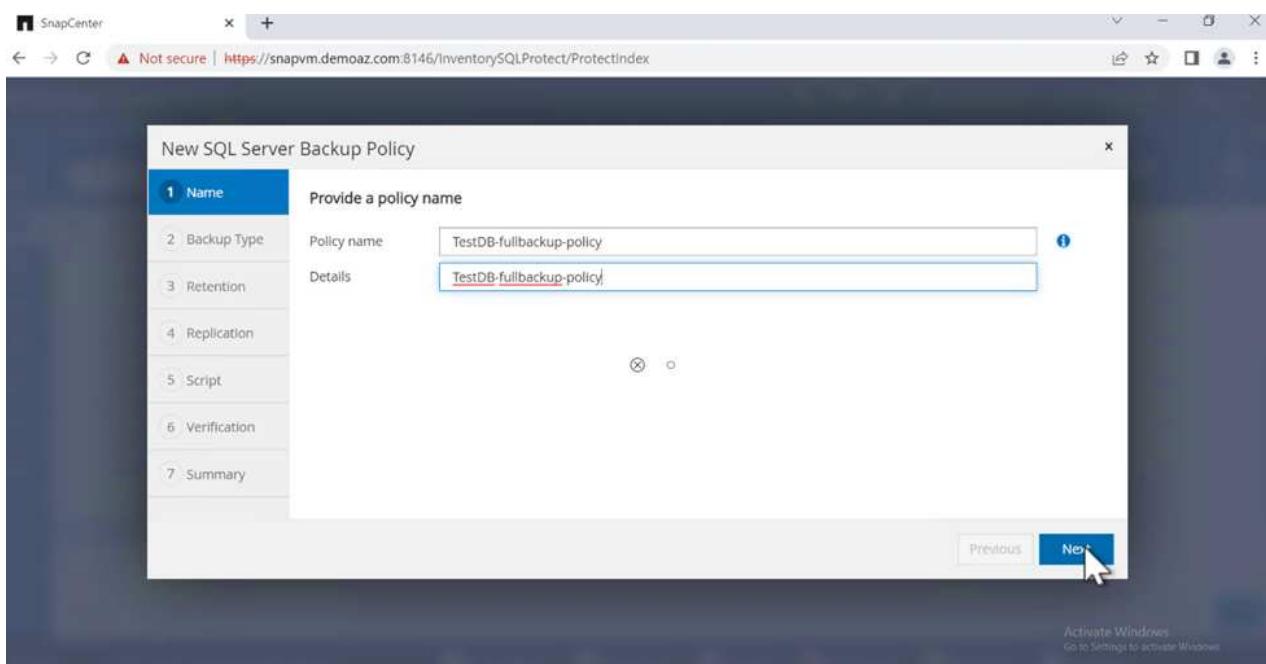
## Configure back-up operation for an FCI database

To configure a backup policy for an FCI database, complete the following steps:

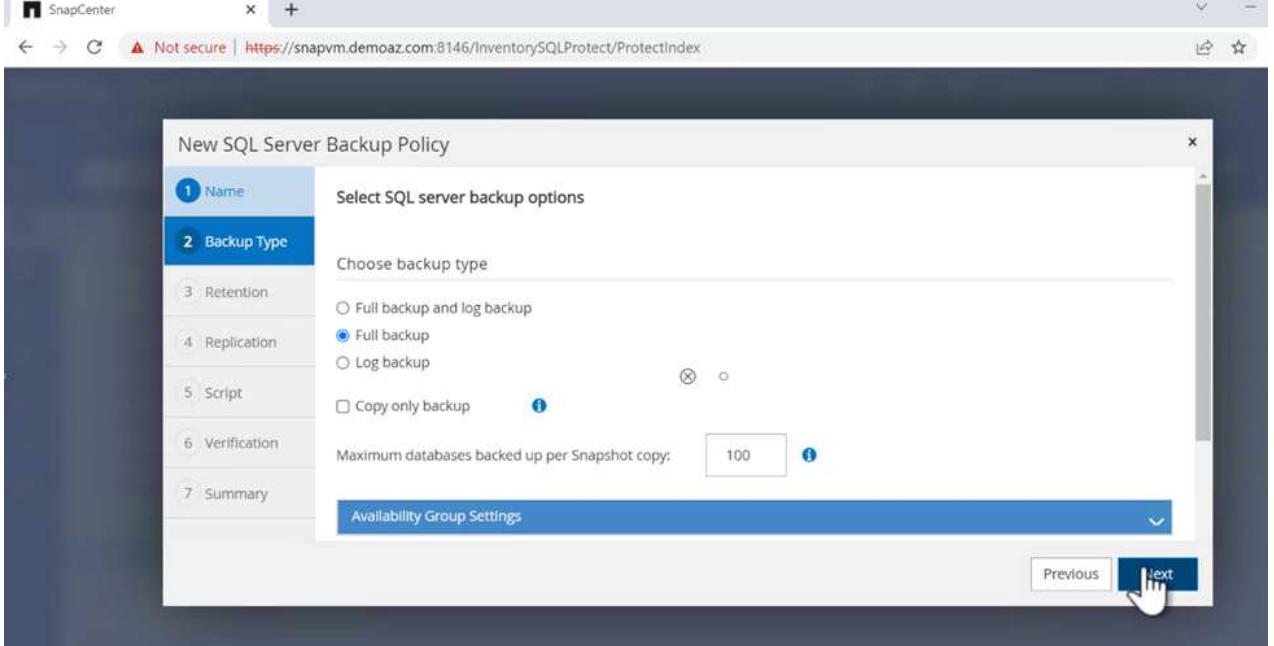
1. Go to **Settings** and select **Policies** on the top left. Then click **New**.



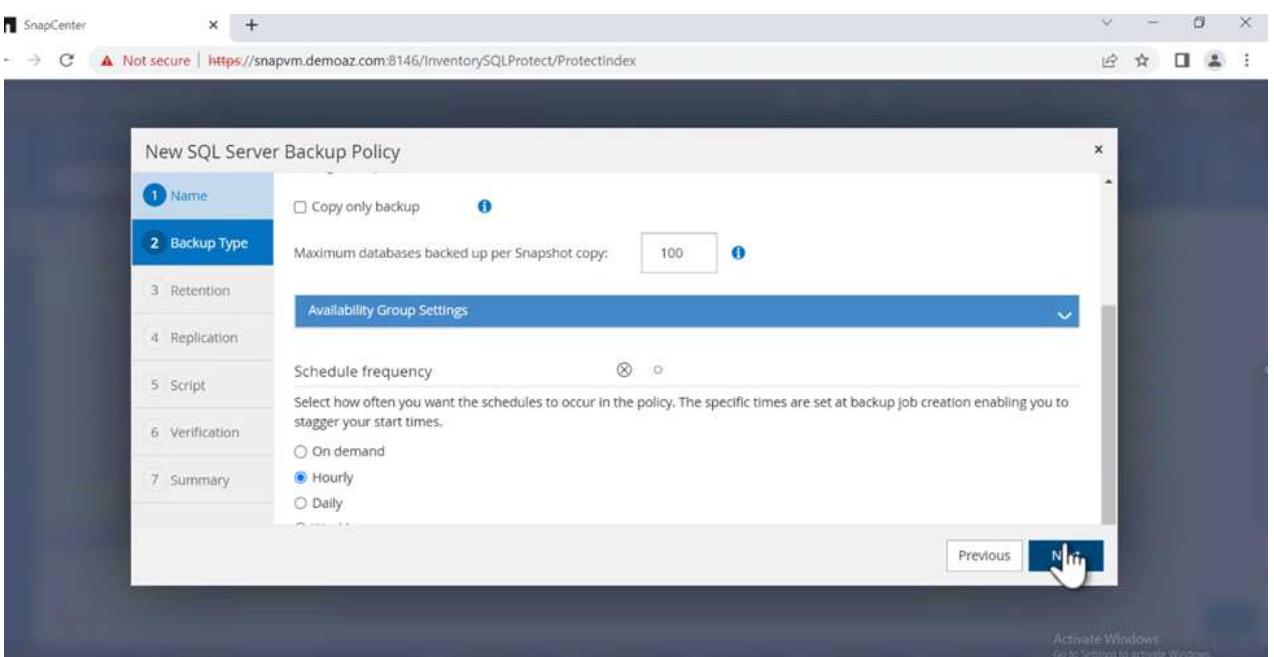
2. Enter the policy name and a description. Click **Next**.



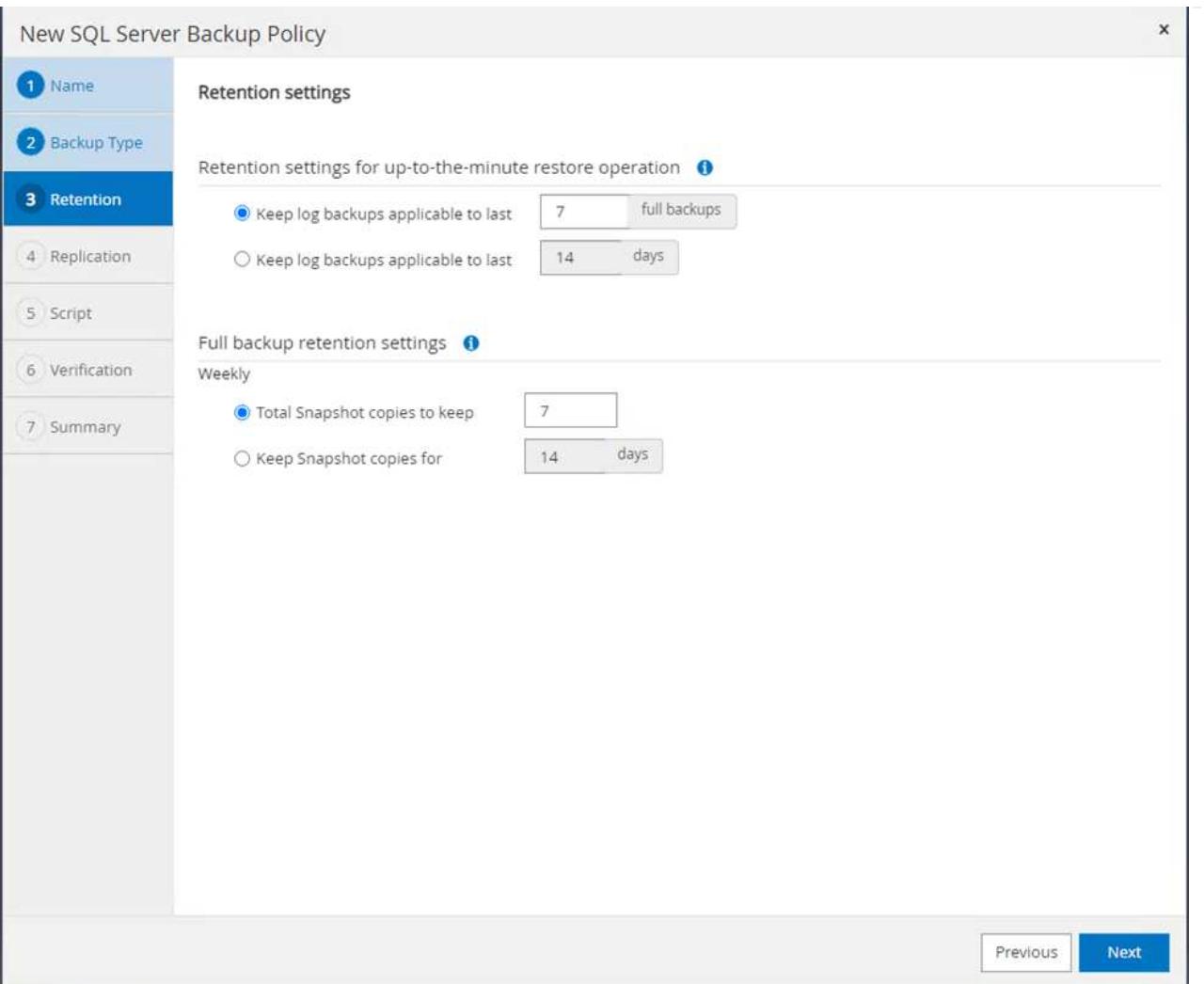
3. Select **Full backup** as the backup type.



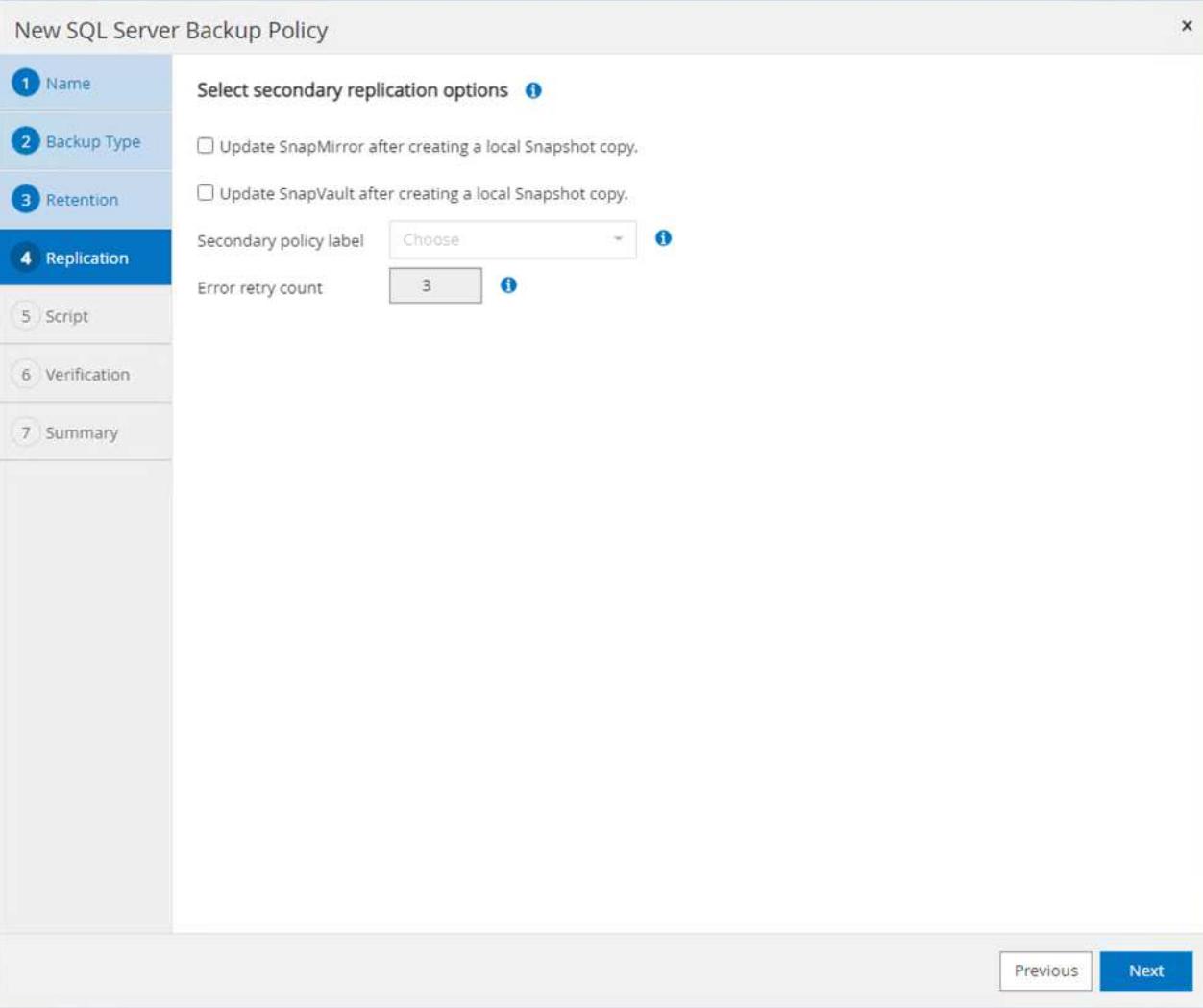
4. Select the schedule frequency (this is based on the company SLA). Click **Next**.



5. Configure the retention settings for the backup.



6. Configure the replication options.



7. Specify a run script to run before and after a backup job is run (if any).

New SQL Server Backup Policy

x

1 Name

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments  Choose optional arguments...

2 Backup Type

3 Retention

4 Replication

5 Script

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments  Choose optional arguments...

6 Verification

7 Summary

Script timeout  60 secs

Previous

The screenshot shows the 'New SQL Server Backup Policy' configuration dialog. The 'Script' tab is active. It contains sections for 'Prescript' and 'Postscript' with their respective full path and argument input fields. A 'Script timeout' field is set to 60 seconds. Navigation buttons 'Previous' and 'Next' are visible at the bottom.

- Run verification based on the backup schedule.

New SQL Server Backup Policy

**1 Name**

Select the options to run backup verification

**2 Backup Type**

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

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

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. The **Summary** page provides details of the backup policy. Any errors can be corrected here.

SnapCenter

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

New SQL Server Backup Policy

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

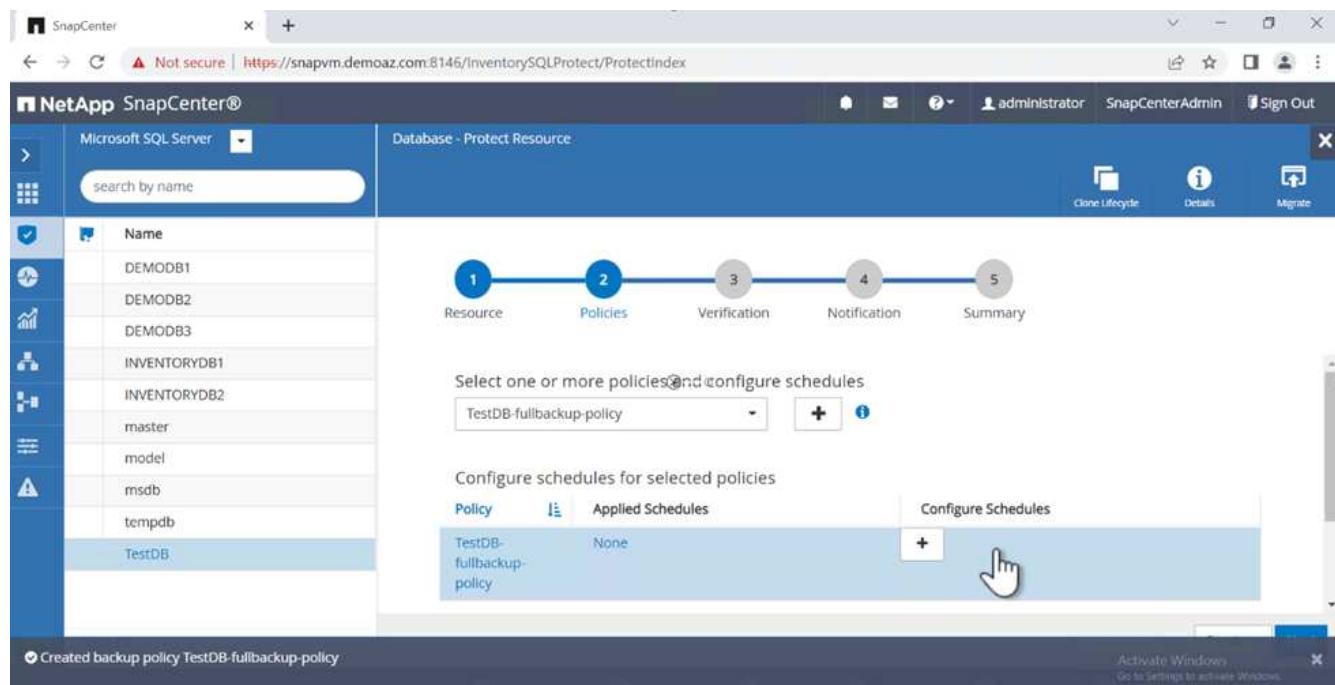
**7 Summary**

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"/>
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:

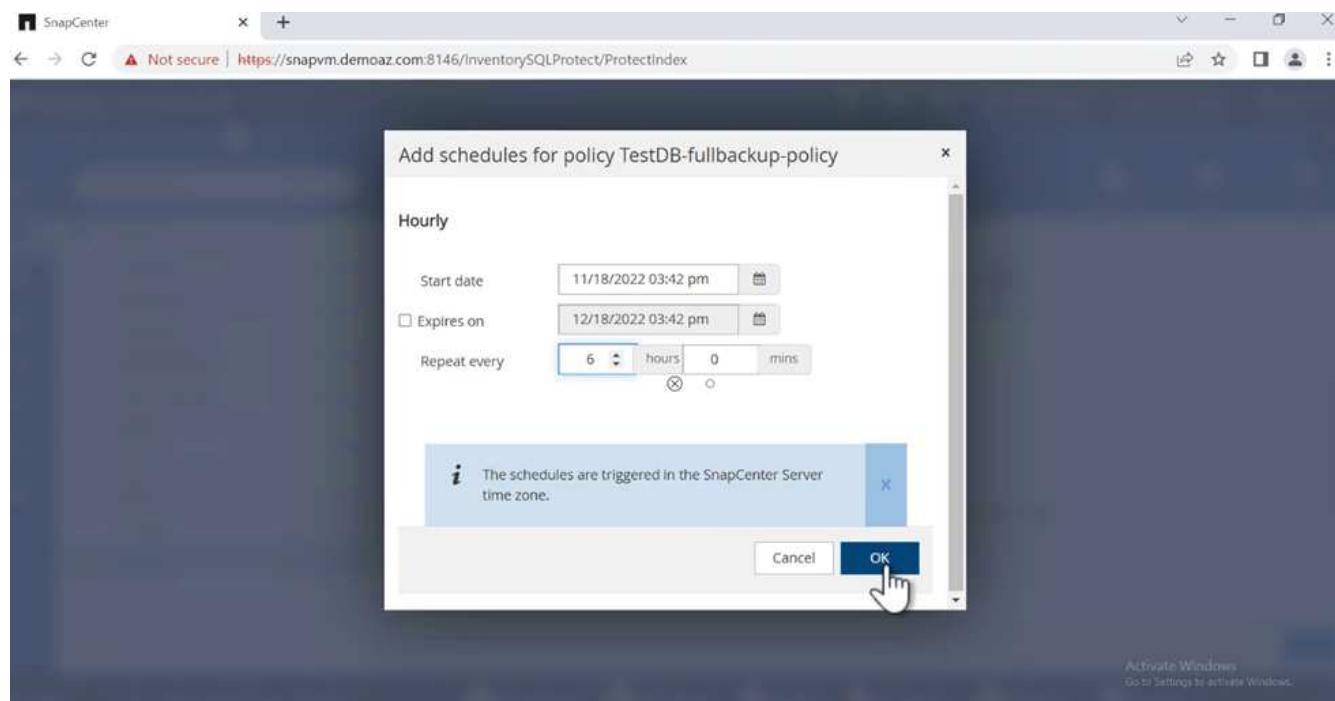
**Previous** **Finish**

## Configure and protect MSSQL Server database

1. Set up the starting date and expiration date of the backup policy.



2. Define the schedule for the backup. To do that, click (+) to configure a schedule. Enter the **Start date** and **Expires on** date. Set the time based on the company's SLA.



3. Configure the verification server. From the drop-down menu, select the server.

The screenshot shows the 'Database - Protect Resource' page in NetApp SnapCenter. On the left, a sidebar lists databases: DEMODB1, DEMODB2, DEMODB3, INVENTORYDB1, INVENTORYDB2, master, model, msdb, tempdb, and TestDB (which is selected). A search bar at the top says 'search by name'. The main area has a progress bar with five steps: 1. Resource (blue), 2. Policies (blue), 3. Verification (blue), 4. Notification (gray), and 5. Summary (gray). Step 3 is highlighted. A dropdown 'Verification server' is set to 'SQLHMCRD(14.0.1000)' with a checked option below it. Below the server selection, there's a section for 'Configure verification schedules' with tabs for 'Policy' (selected), 'Schedule Type', 'Applied Schedules', and 'Configure Schedules'. A message states 'There is no match for your search or data is not available.' At the bottom right are 'Previous' and 'Next' buttons.

4. Confirm the configured schedule by clicking the plus sign and confirm.
5. Provide information for email notification. Click **Next**.

The screenshot shows the 'Database - Protect Resource' page in NetApp SnapCenter. The sidebar lists databases: master, model, msdb, tempdb, testdb, master, model, msdb, KTFDB (which is selected), and tempdb. A message at the top right says: 'If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.' The main area has a progress bar with five steps: 1. Resource (blue), 2. Policies (blue), 3. Verification (blue), 4. Notifications (blue), and 5. Summary (gray). Step 4 is highlighted. A section titled 'Provide email settings' asks to 'Select the service accounts or people to notify regarding protection issues.' It includes fields for 'Email preference' (set to 'Never'), 'From' (From email), 'To' (Email to), 'Subject' (Notification), and a checkbox for 'Attach job report'. At the bottom right are 'Previous' and 'Next' buttons.

The summary of the backup policy for SQL Server database is now configured.

The screenshot shows the "Database - Protect Resource" page in the NetApp SnapCenter interface. On the left, a sidebar lists various databases: DEMODB1, DEMODB2, DEMODB3, INVENTORYDB1, INVENTORYDB2, master, model, msdb, tempdb, and TestDB, which is selected. The main pane displays the following information:

- Database name:** TestDB
- Policy:** TestDB-fullbackup-policy: Hourly
- Verification servers:** SQLHIMCRDS
- Verification enabled for policy:** None
- Send email:** No

A progress bar at the top indicates the steps: 1. Resource (highlighted), 2. Policies, 3. Verification, 4. Notification, 5. Summary. A note at the top right says: "If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server."

## SnapCenter backup operations

To create on-demand SQL Server backups, complete the following steps:

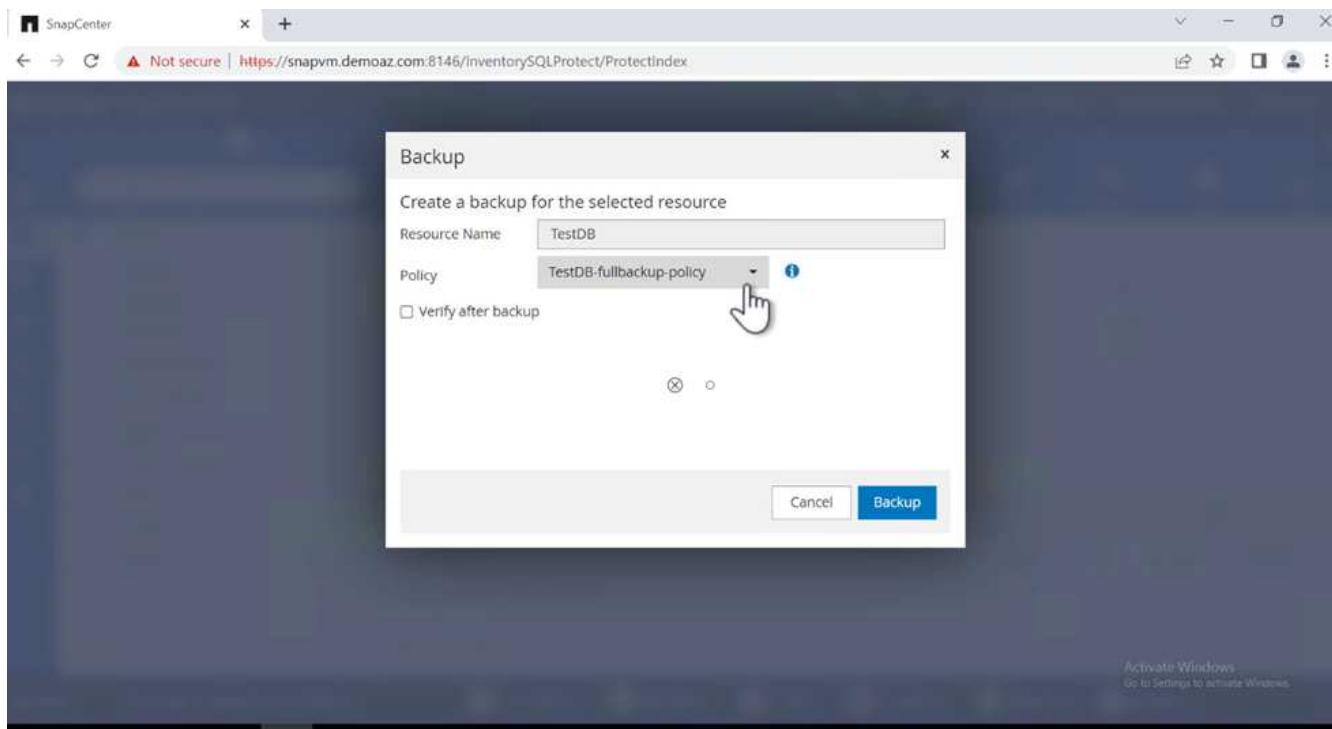
1. From the **Resource** view, select the resource and select **Backup now**.

The screenshot shows the "Resource" view in the NetApp SnapCenter interface. The toolbar includes buttons for Migrate Database, Clone Lifecycle, Remove Protection, Back up now (which has a cursor over it), Modify, Maintenance, Details, and Refresh. The main pane displays the following information:

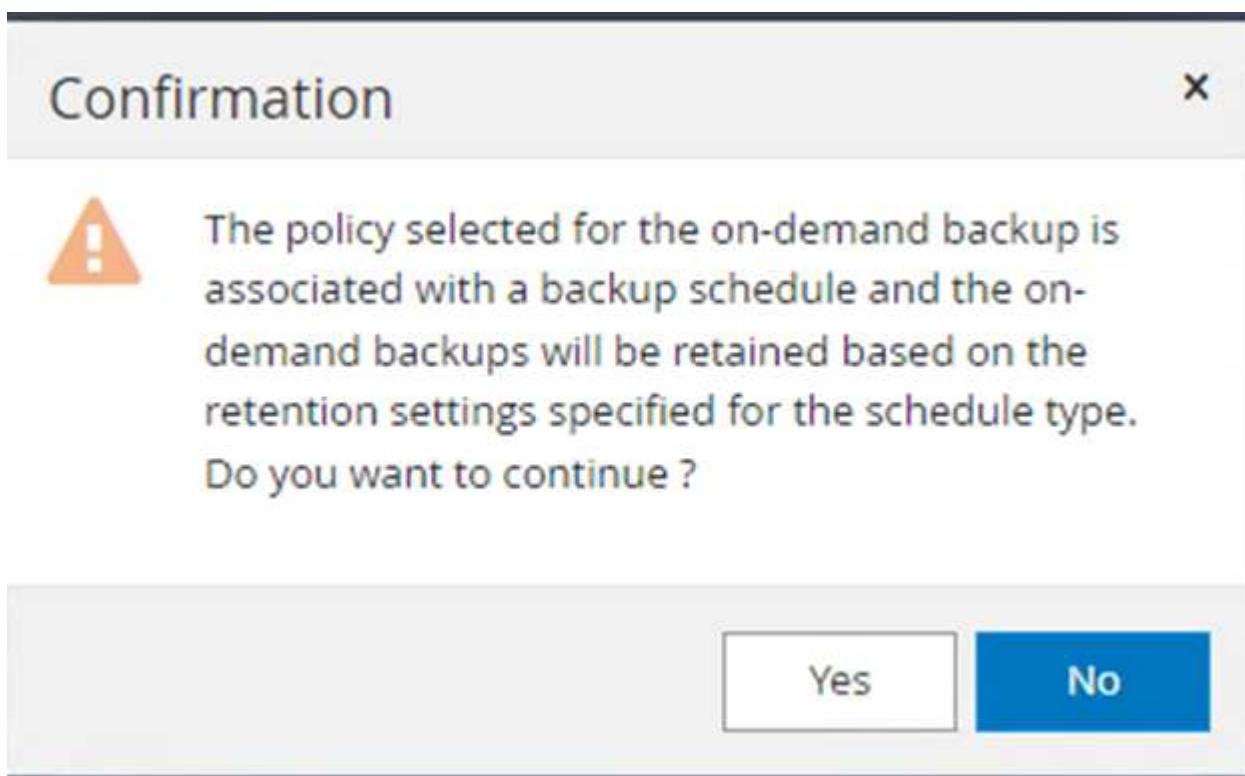
- Topology:** "TestDB" Topology
- Manage Copies:** 0 Backups, 0 Clones
- Primary Backup(s):** There is no match for your search.
- Summary Card:** 0 Backups, 0 Clones.

The sidebar on the left lists the same database names as the previous screenshot: DEMODB1, DEMODB2, DEMODB3, INVENTORYDB1, INVENTORYDB2, master, model, msdb, tempdb, and TestDB. The total count is 10.

2. In the **Backup** dialog box, click **Backup**.



3. A confirmation screen is displayed. Click **Yes** to confirm.



## Monitor backup job

1. From the **Monitor** tab, click the job and select **Details** on the right to view the jobs.

The screenshot shows the NetApp SnapCenter interface. The top navigation bar includes tabs for 'Jobs', 'Schedules', 'Events', and 'Logs'. A search bar is present above the main content area. The left sidebar has sections for 'Dashboard', 'Resources' (which is selected), 'Monitor', 'Reports', 'Hosts', 'Storage Systems', 'Settings', and 'Alerts'. The main content area displays a table titled 'Jobs - Filter' with columns for 'ID', 'Status', 'Name', 'Start date', 'End date', and 'Owner'. One row is highlighted, representing a 'Backup of Resource Group 'SQLHMCRD5\_TestDB'' job with ID 13, status '✓', name 'Backup of Resource Group 'SQLHMCRD5\_TestDB'' with policy 'TestDB-fullbackup-policy'', start date 11/18/2022 3:43:12 PM, end date 11/18/2022 3:47:05 PM, and owner 'Administrator'. A hand cursor is hovering over the 'Details' icon (an info sign) in the top right corner of the table row.

This screenshot shows a 'Job Details' modal window. The title is 'Job Details' and the sub-section is 'Backup of Resource Group 'SQLHMCRD5\_TestDB'' with policy 'TestDB-fullbackup-policy''. The modal lists the steps of the backup process: 'Preparing for Backup', 'Creating SQL Backup', 'Finalizing Backup', 'Data Collection' (which is currently in progress, indicated by a grey background), and 'Send EMS Messages'. At the bottom of the modal, there is a message: 'Task Name: Data Collection Start Time: 11/18/2022 3:47:05 PM End Time: 11/18/2022 3:47:05 PM'. Below the message are three buttons: 'View Logs', 'Cancel Job', and 'Close'. A hand cursor is hovering over the 'Close' button. The background of the modal is dark, matching the overall theme of the application.

When the backup is completed, a new entry is shown in the Topology view.

## Backup operation for multiple databases

To configure a backup policy for multiple SQL Server databases, create resource group policies by completing the following steps:

1. In the **Resources** tab from the **View** menu, change to a resource group using the drop-down menu.

The screenshot shows the NetApp SnapCenter interface for Microsoft SQL Server. The left sidebar has 'Resources' selected. The main area displays a table of databases:

	Instance	Host	Last Backup	Overall Status	Type
INSIGHTDB3	SQLRDSHMC	FSXCLUSTER.DemoAZ.com	11/11/2022 4:34:25 PM	Backup succeeded	User database
INSIGHTDB4	SQLRDSHMC	FSXCLUSTER.DemoAZ.com		Not protected	User database
	SQLRDSHMC	FSXCLUSTER.DemoAZ.com		Not protected	User database
	SQLRDSHMC	FSXCLUSTER.DemoAZ.com		Not protected	User database
	SQLRDSHMC	FSXCLUSTER.DemoAZ.com		Not protected	User database
	master	SQLRDSHMC	FSXCLUSTER.DemoAZ.com	Not protected	System database
	model	SQLRDSHMC	FSXCLUSTER.DemoAZ.com	Not protected	System database
	msdb	SQLRDSHMC	FSXCLUSTER.DemoAZ.com	Not protected	System database
	tempdb	SQLRDSHMC	FSXCLUSTER.DemoAZ.com	Not available for backup	System database
	ChampionshipDB1	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB10	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB100	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB101	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB102	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB103	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB104	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB105	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB106	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB107	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB108	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB109	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB111	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB110	STAVM3	STAVM3.DemoAZ.com	Not protected	User database
	ChampionshipDB111	STAVM3	STAVM3.DemoAZ.com	Not protected	User database

Total 213

Activate Windows  
Go to Settings to activate Windows.

Activity: The 5 most recent jobs are displayed. Status icons: 3 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, 0 Queued.

2. Click (+) for a new resource group.

The screenshot shows the NetApp SnapCenter interface for creating a new resource group. The left sidebar has 'Resources' selected. The main area displays a table with one row:

Name	Resource Count	Tags	Policies	Last Backup	Overall Status

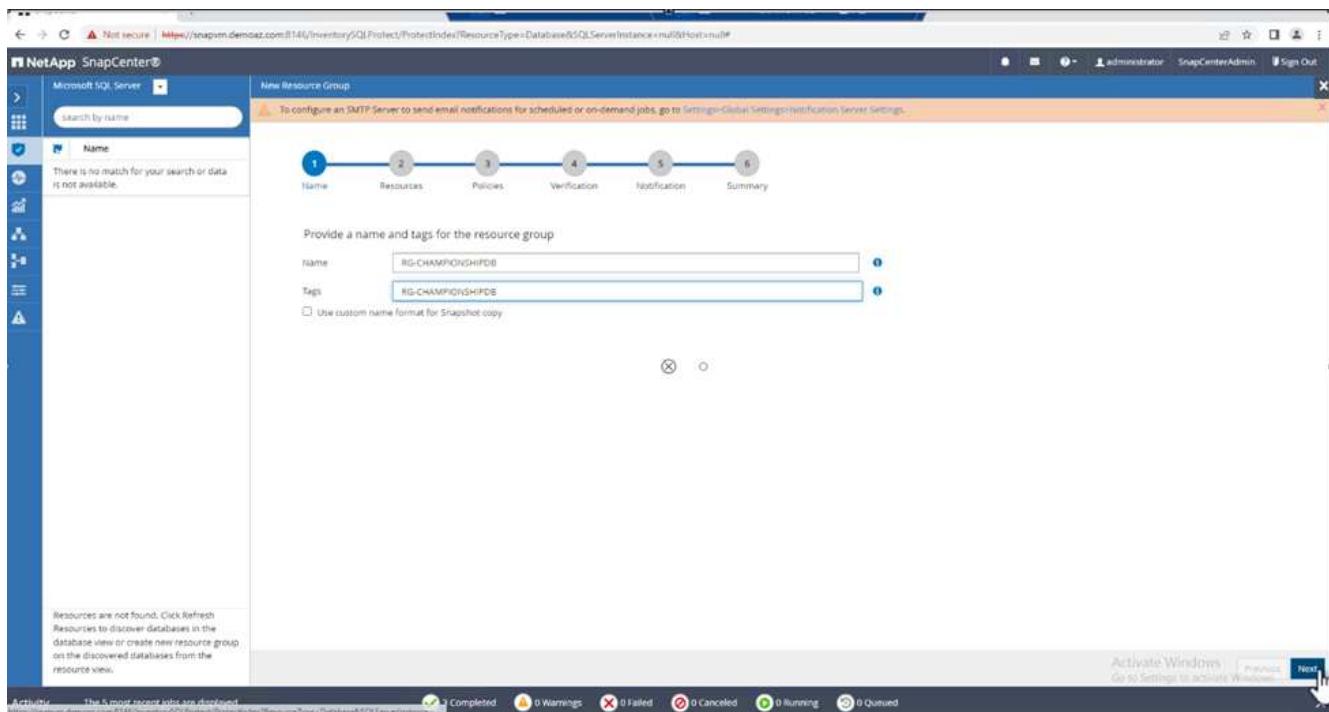
There is no match for your search or data is not available.

Resources are not found. Click Refresh Resources to discover databases in the database view or create new resource group on the discovered databases from the resource view.

Activate Windows  
Go to Settings to activate Windows.

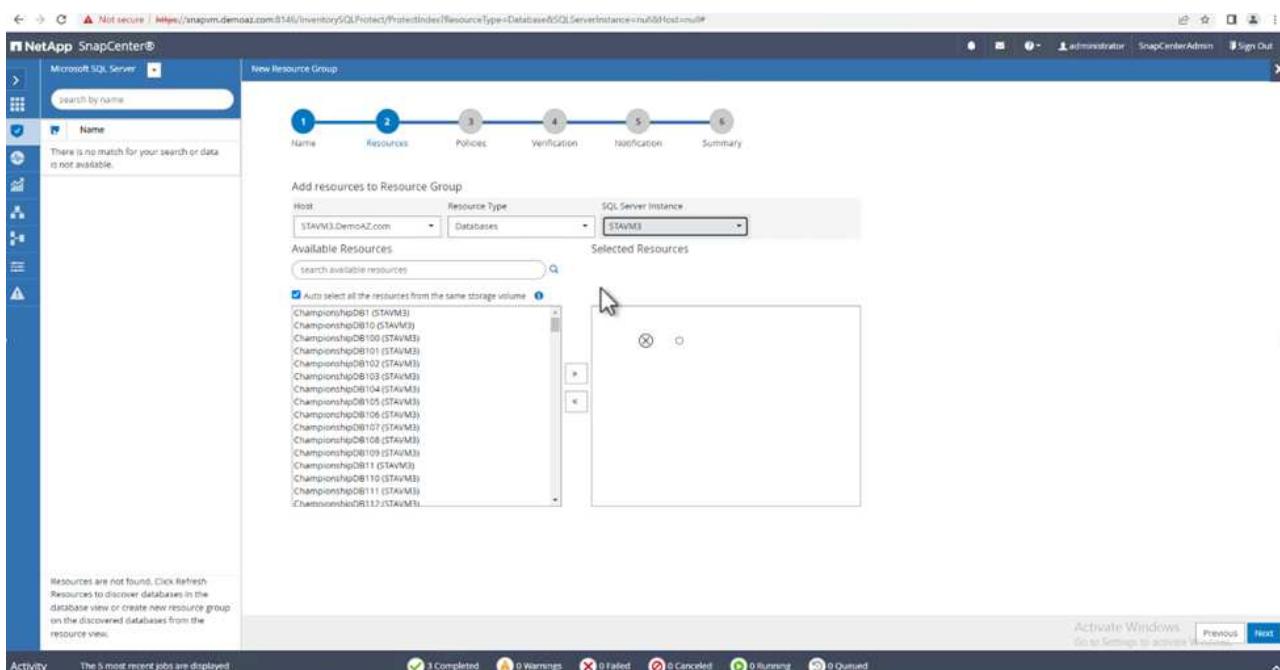
Activity: The 5 most recent jobs are displayed. Status icons: 3 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, 0 Queued.

3. Provide a name and tag. Click Next.

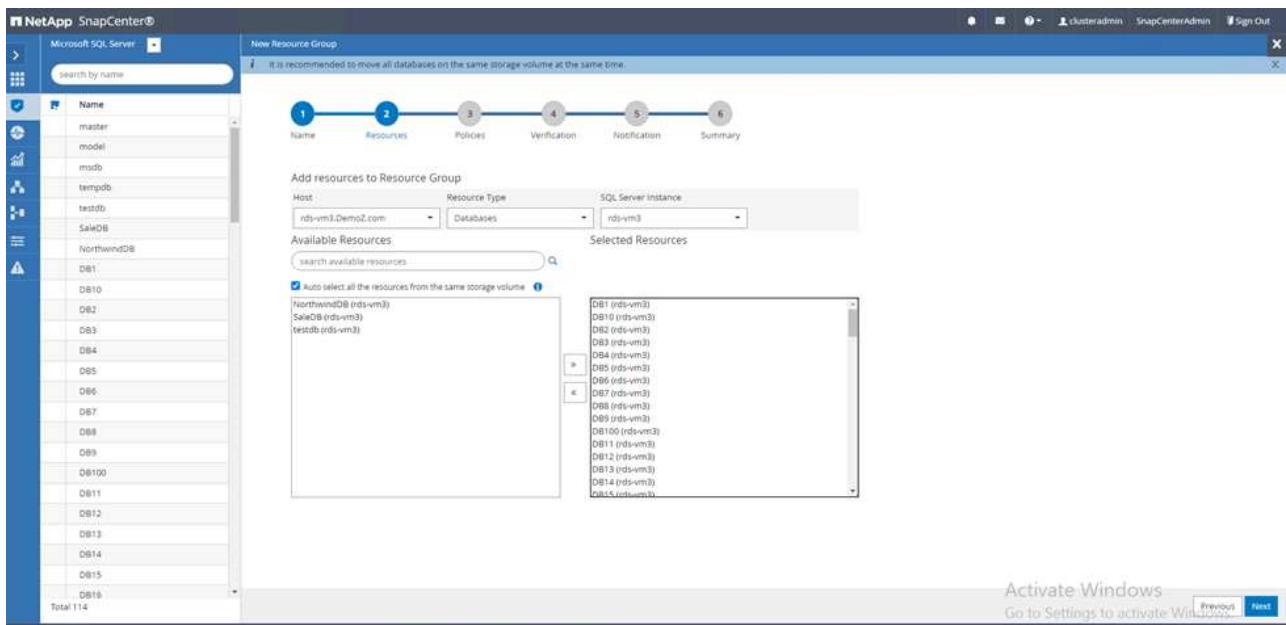


#### 4. Add resources to the resource group:

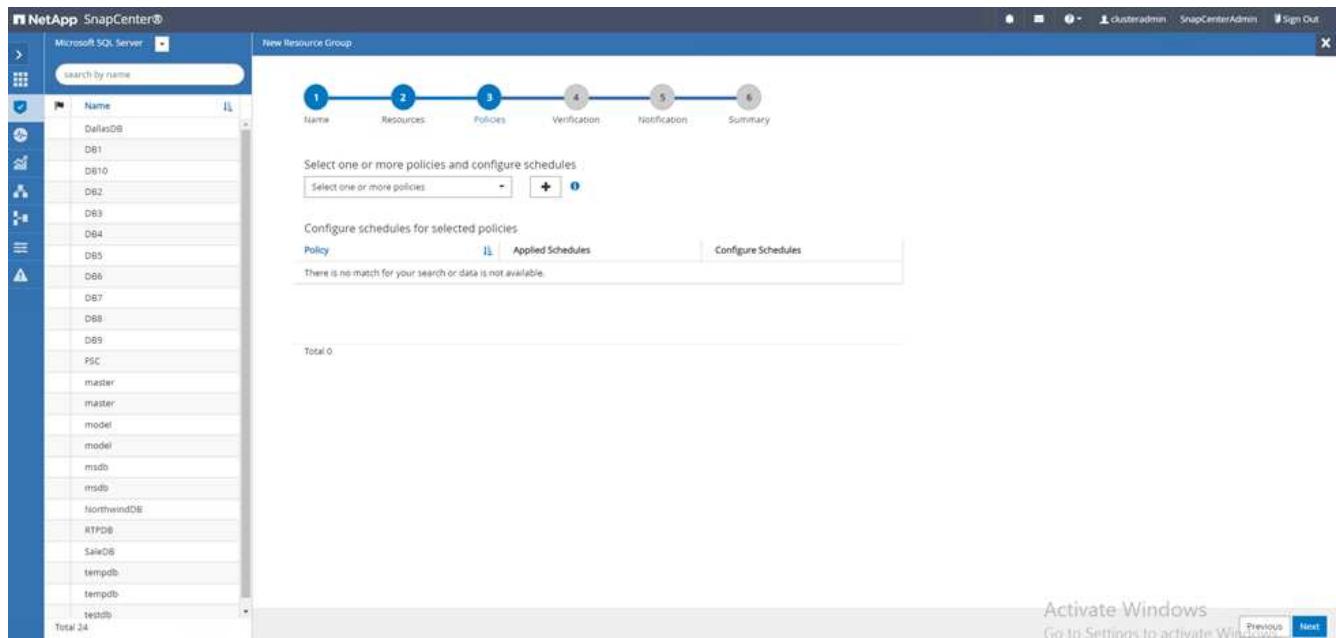
- **Host.** Select the server from the drop-down menu hosting the database.
- **Resource type.** From the drop-down menu, select **Database**.
- **SQL Server instance.** Select the server.



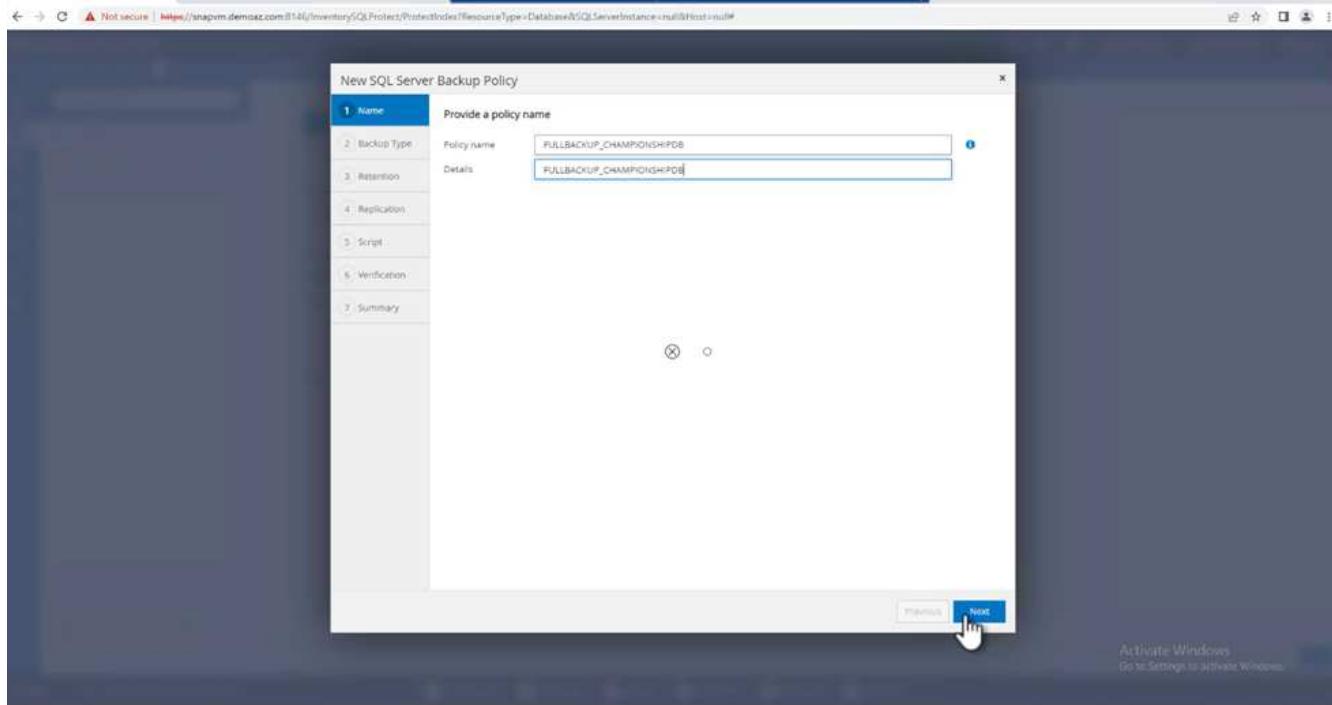
The **option Auto Selects All the Resources from the Same Storage Volume\*** is selected by default. Clear the option and select only the databases you need to add to the resource group, Click the arrow to add and click **Next**.



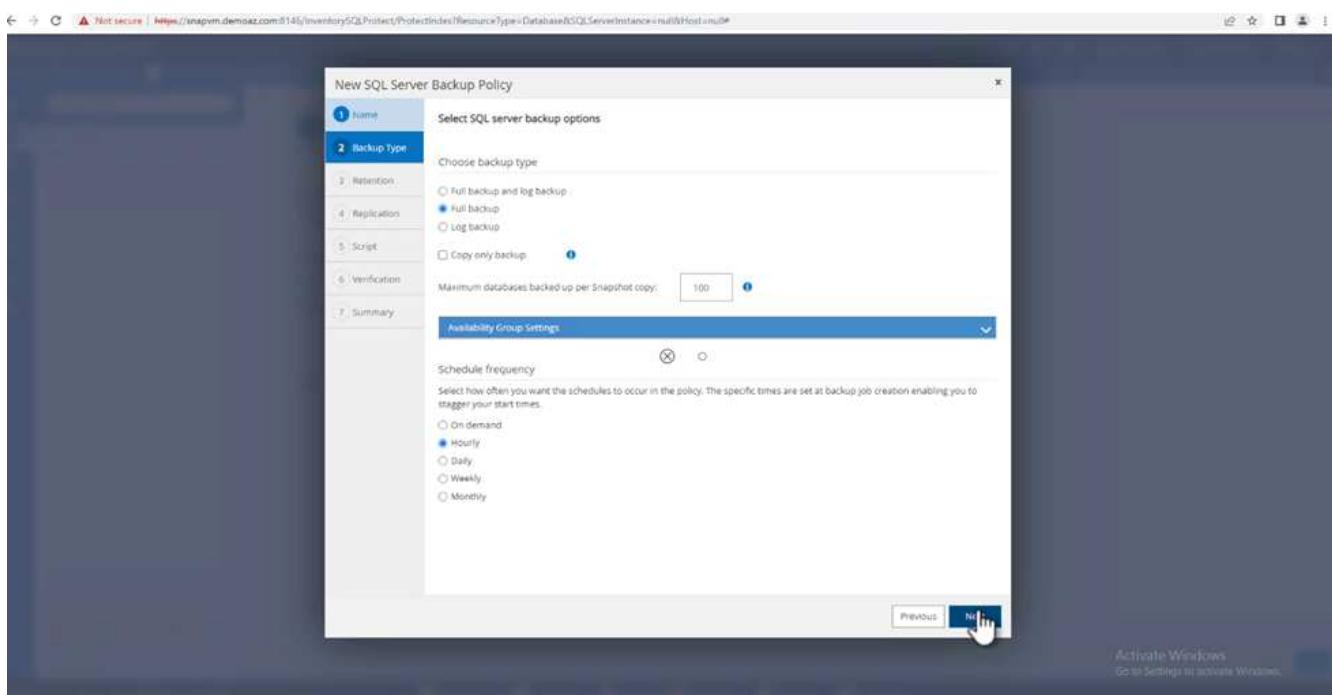
5. On the policies, click (+).



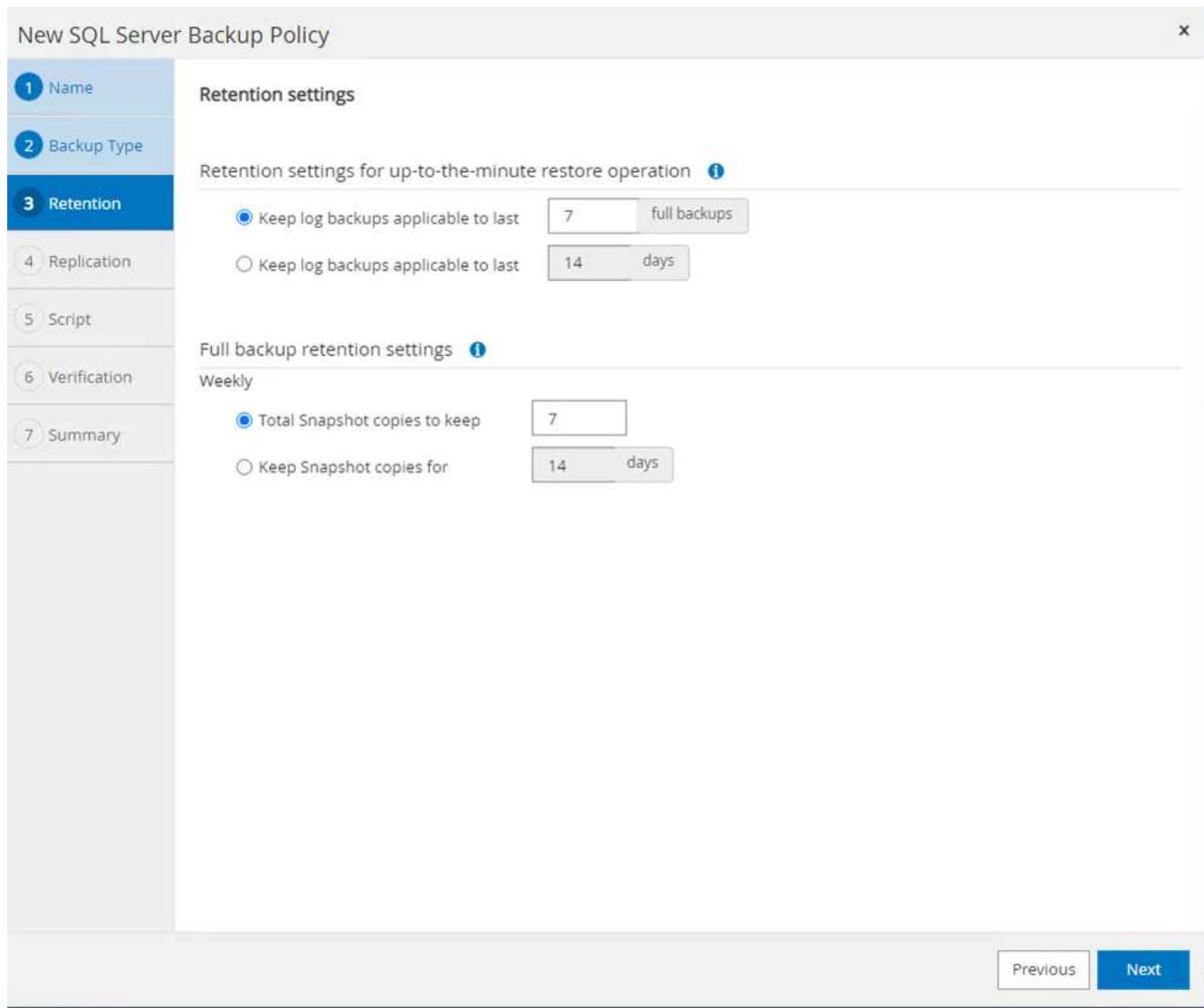
6. Enter the resource group policy name.



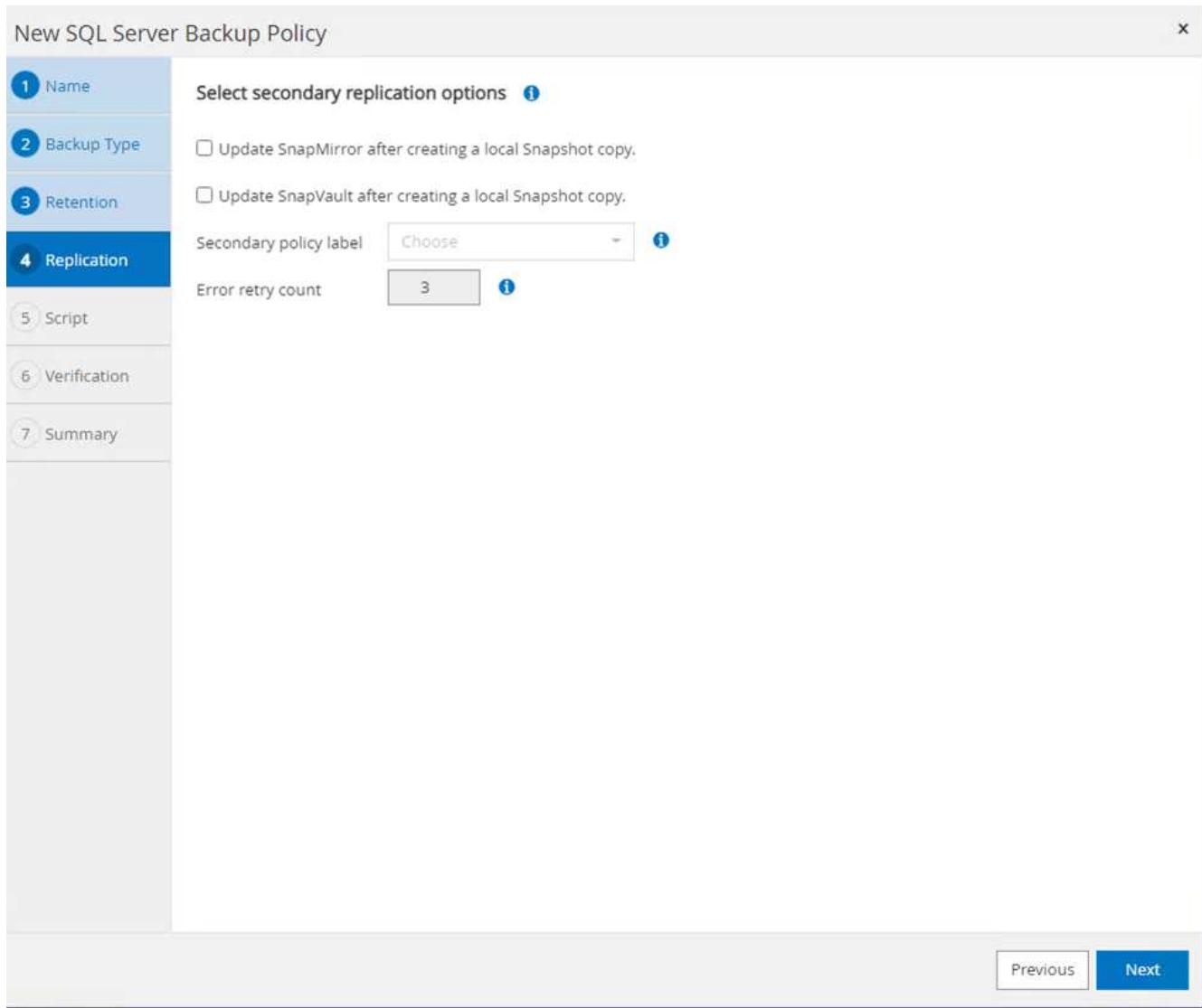
7. Select **Full backup** and the schedule frequency depending on your company's SLA.



8. Configure the retention settings.



9. Configure the replication options.



10. Configure the scripts to run before performing a backup. Click **Next**.

New SQL Server Backup Policy X

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

Prescript full path

Prescript arguments  Choose optional arguments...

**2 Backup Type** Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments  Choose optional arguments...

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Script timeout  60 secs

Previous Next

11. Confirm the verification for the following backup schedules.

New SQL Server Backup Policy

**1 Name**

Select the options to run backup verification

**2 Backup Type**

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

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

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)

**7 Summary**

Verification script settings ?

Script timeout  secs

Prescript full path

Prescript arguments

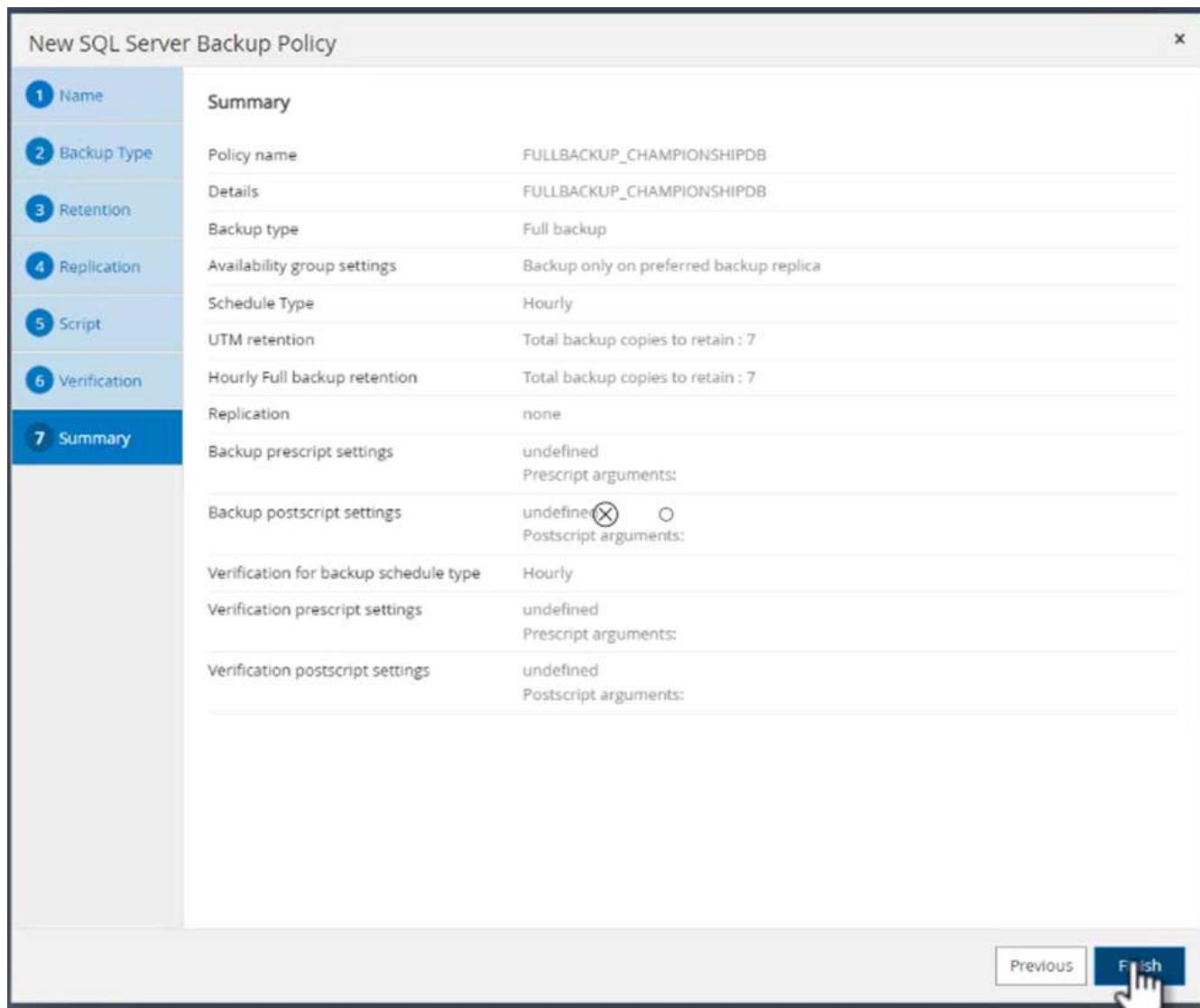
Postscript full path

Postscript arguments

**Previous** **Next**

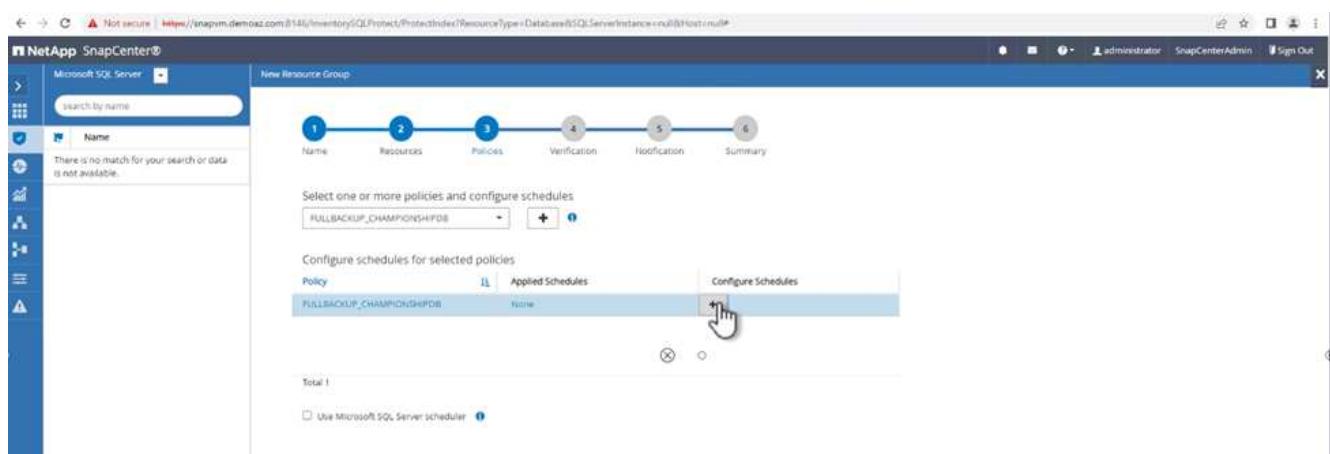
The screenshot shows the 'Verification' step of the 'New SQL Server Backup Policy' wizard. The left sidebar lists steps 1 through 7. Step 6, 'Verification', is selected and highlighted in blue. The main area contains several configuration sections: 'Select the options to run backup verification' (with 'Hourly' checked), 'Database consistency checks options' (with 'Limit the integrity structure to physical structure of the database (PHYSICAL\_ONLY)' and 'Suppress all information message (NO\_INFOMSGS)' checked), and 'Verification script settings' (with fields for 'Script timeout' (60), 'Prescript full path' (<SCRIPTS\_PATH>), 'Prescript arguments' (Choose optional arguments...), 'Postscript full path' (<SCRIPTS\_PATH>), and 'Postscript arguments' (Choose optional arguments...)). At the bottom right are 'Previous' and 'Next' buttons.

12. On the **Summary** page, verify the information, and click **Finish**.



## Configure and protect multiple SQL Server databases

1. Click the (+) sign to configure the start date and the expire- on date.



2. Set the time.

## Add schedules for policy FULLBACKUP\_CHAMPIONSHIPDB

X

### Hourly

Start date

11/11/2022 05:30 pm



Expires on

12/11/2022 05:27 pm



Repeat every

8



hours

0

mins



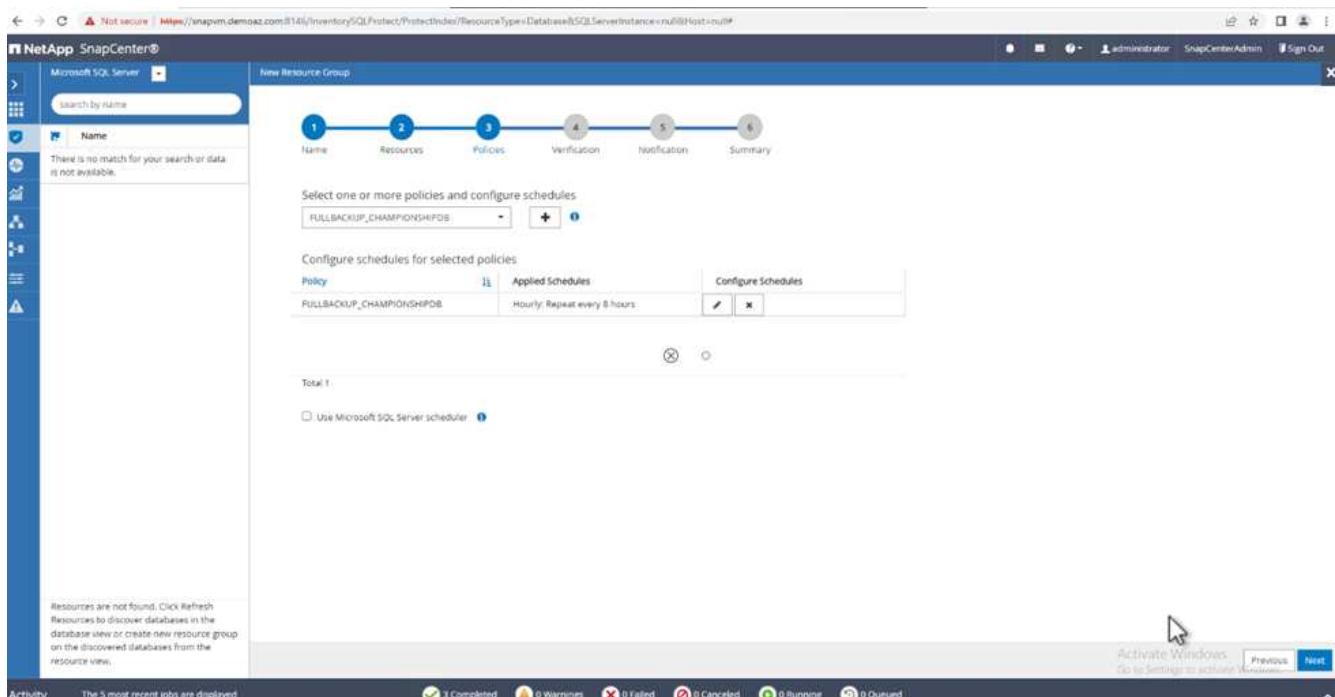
The schedules are triggered in the SnapCenter Server time zone.



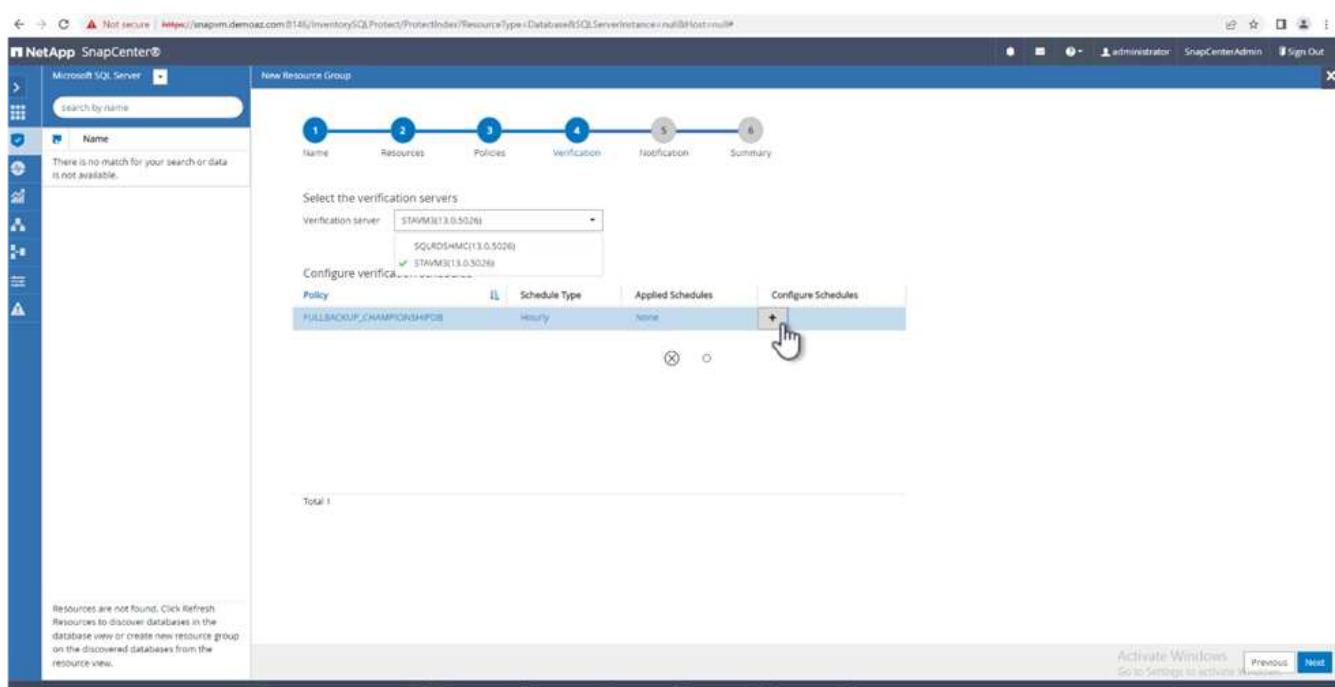
Cancel

OK

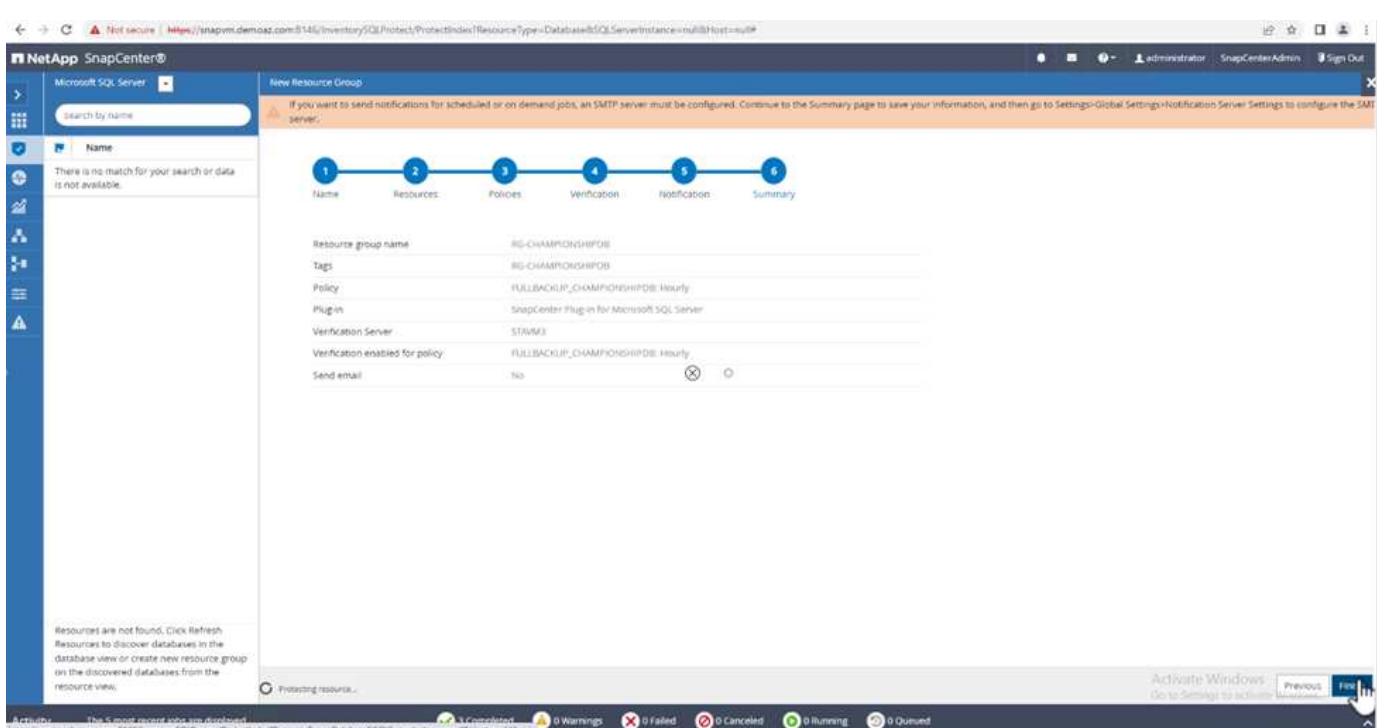
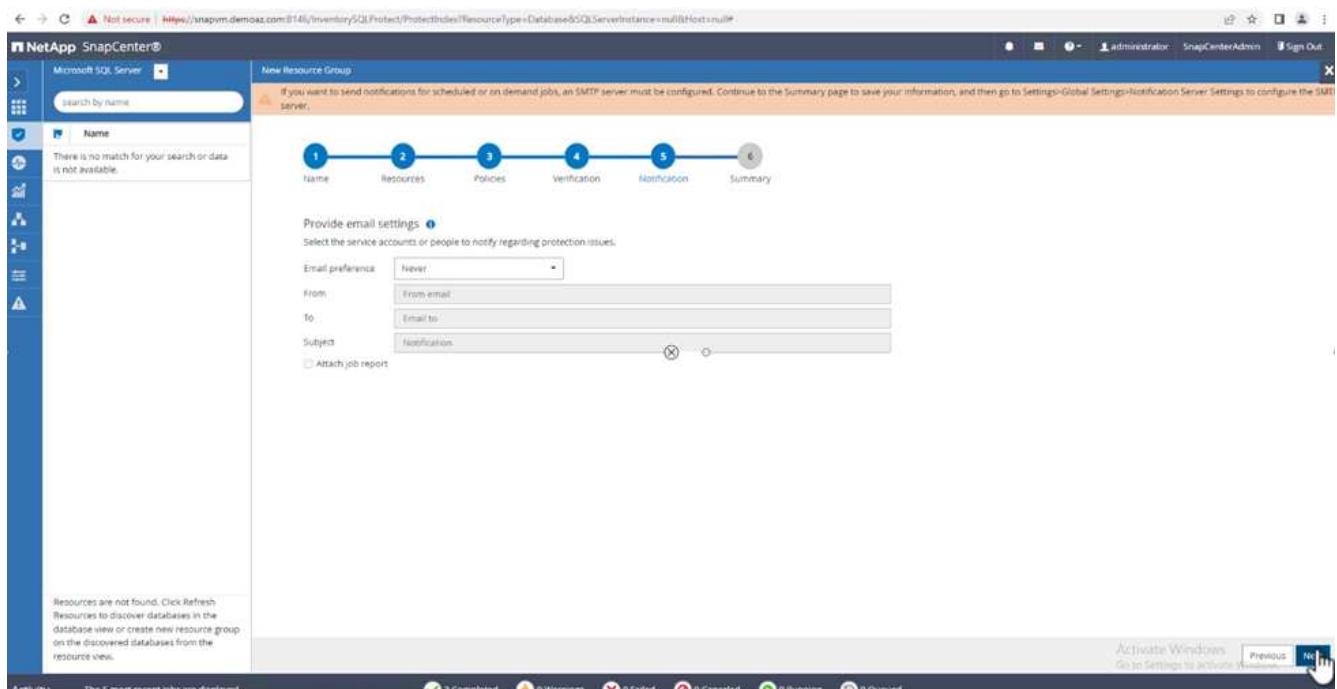




- From the **Verification** tab, select the server, configure the schedule, and click **Next**.



- Configure notifications to send an email.



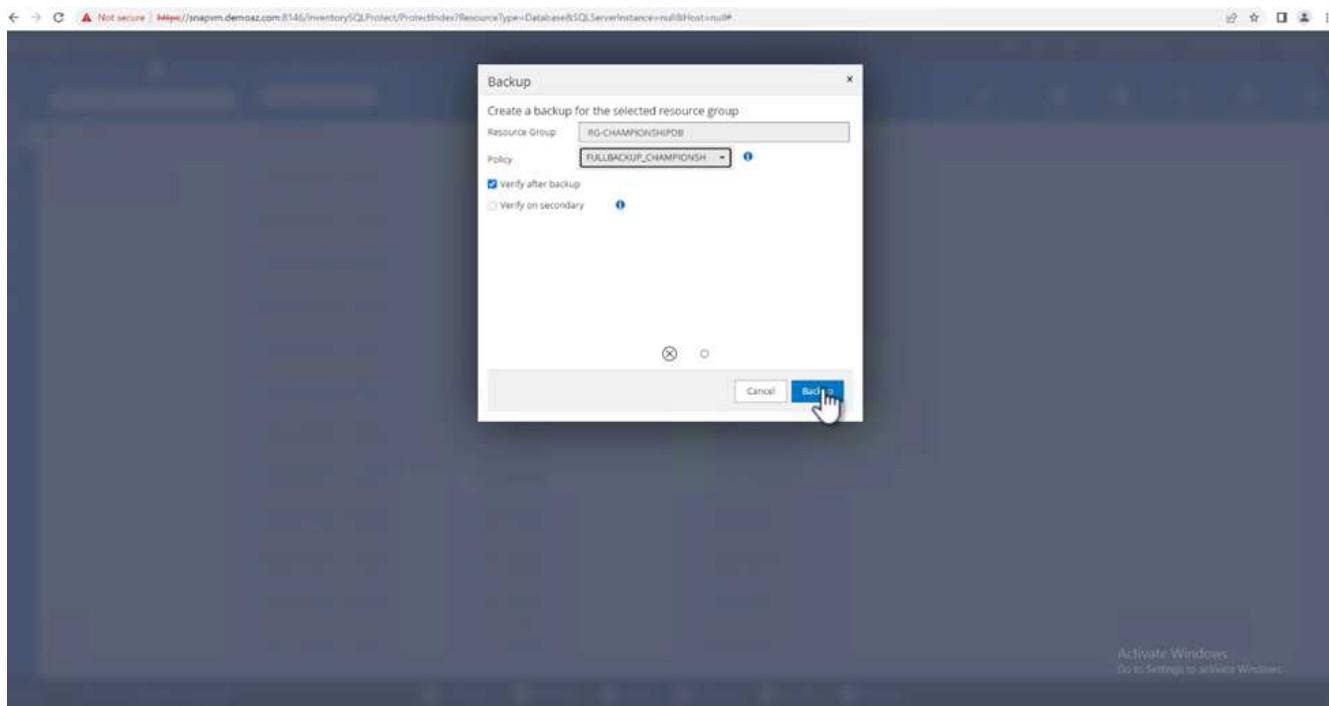
1. From the **Resource** tab, select view. From the drop-down menu, select **Resource Group**.

The screenshot shows the NetApp SnapCenter interface for a Microsoft SQL Server resource group named "RG-O-MAMP-OSHE/DB". The main pane displays a list of 33 SQL databases, each with its name, type (SQL Database), and host (STAVM3.DemoAZ.com). At the top right of the interface, there is a toolbar with icons for "Modify Resource Group", "Backup now", "Done Lifecycle", "Maintenance", "Edit/View Details", and "Delete". A cursor is hovering over the "Backup now" button.

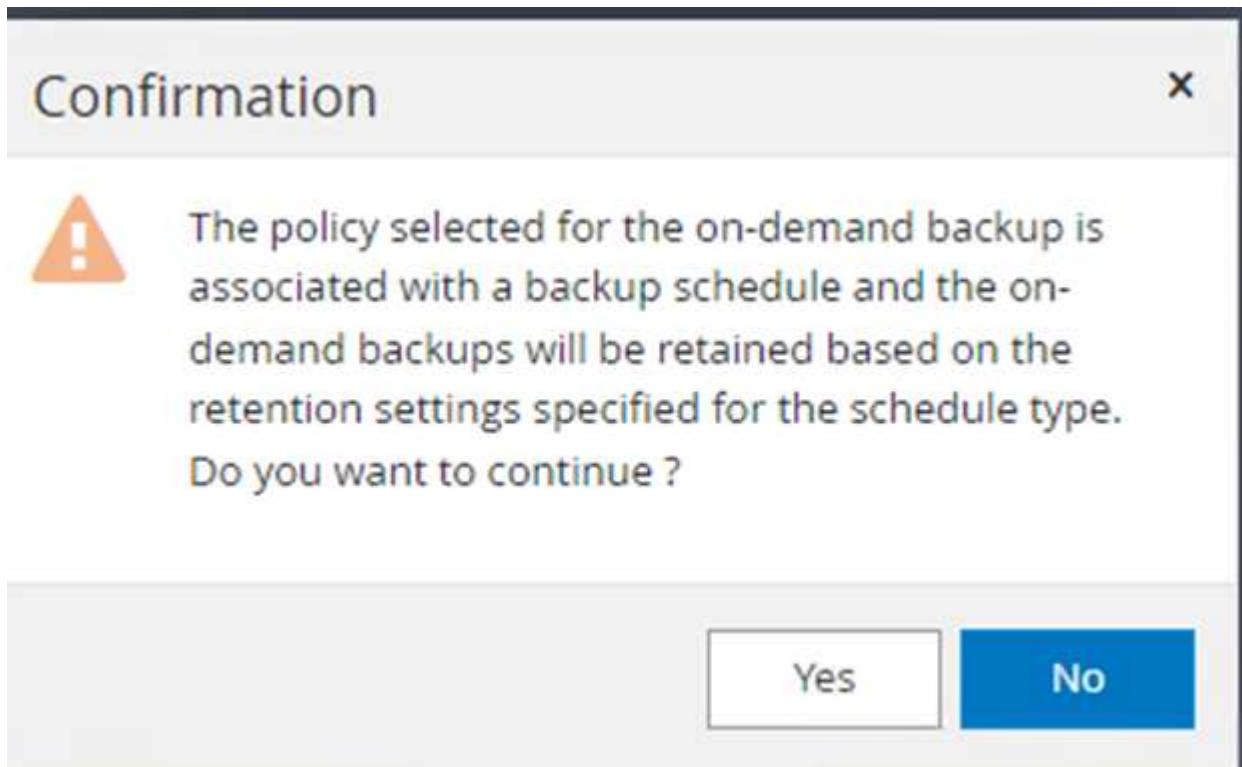
2. Select the resource group name.
3. Click **Backup now** in the upper right.

The screenshot shows the NetApp SnapCenter interface for a Microsoft SQL Server resource group named "RG-1". The main pane displays a list of 23 SQL databases, each with its name, type (SQL Database), and host (rds-vm3.Demo2.com). At the top right of the interface, there is a toolbar with icons for "Modify Resource Group", "Backup now", "Done Lifecycle", "Maintenance", "Edit/View Details", and "Delete". A cursor is hovering over the "Verify after backup" checkbox in a modal dialog box that has appeared over the interface.

4. A new window opens. Click the **Verify after backup** checkbox and then click backup.

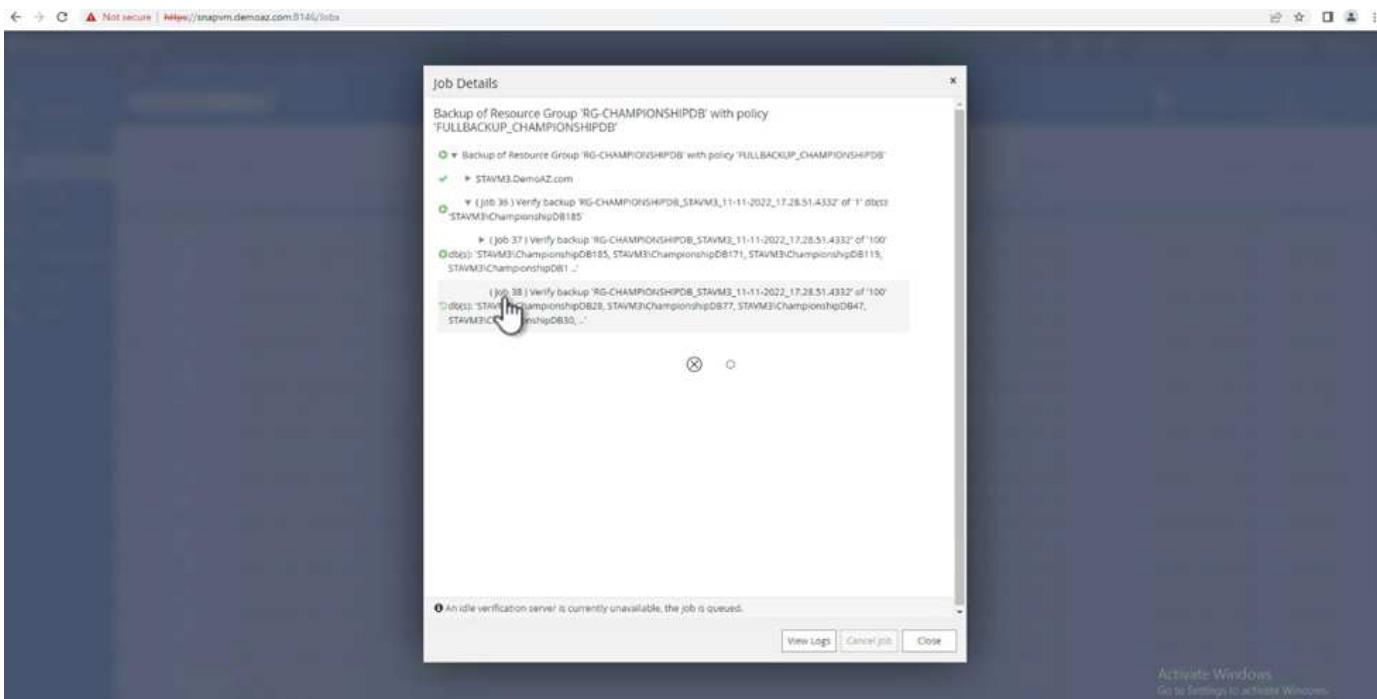


5. A confirmation message is displayed. Click **Yes**.



## Monitor multiple-database backup jobs

From the left navigation bar, click **Monitor**, select the backup job, and click **Details** to view job progress.



Click the **Resource** tab to see the time it takes for the backup to be completed.

The screenshot shows the 'Resources' tab in NetApp SnapCenter. It lists a single resource group named 'RG-CHAMPIONSHIPDB'. The table includes columns for Name, Resource Count, Tags, Policies, Last Backup, and Overall Status. The 'Overall Status' for the resource group is 'Queued'. A hand cursor is hovering over the 'Overall Status' cell for the 'RG-CHAMPIONSHIPDB' row.

## Transaction log backup for multiple database backup

SnapCenter supports the full, bulked logged, and simple recovery models. The simple recovery mode does not support transactional log backup.

To perform a transaction log backup, complete the following steps:

1. From the **Resources** tab, change the view menu from **Database** to **Resource group**.

The screenshot shows the NetApp SnapCenter interface for Microsoft SQL Server. The left sidebar includes tabs for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area displays a table of database information with columns for Instance, Host, Last Backup, Overall Status, and Type. The table lists numerous databases, including master, model, msdb, tempdb, and multiple ChampionshipDB entries. A total of 213 databases are shown. At the bottom, there are status indicators for completed, warnings, failed, canceled, running, and queued jobs.

2. Select the resource group backup policy created.
3. Select **Modify Resource Group** in the upper right.

The screenshot shows the NetApp SnapCenter interface for the 'RG-CHAMPIONSHIPDB' resource group. The left sidebar shows the 'Resources' tab is selected. The main area displays a table of resource group details, with the 'Name' column highlighted. The table lists 213 entries, each corresponding to a database within the resource group. At the bottom, there are status indicators for completed, warnings, failed, canceled, running, and queued jobs.

4. The **Name** section defaults to the backup policy name and tag. Click **Next**.

The **Resources** tab highlights the bases to which the transaction backup policy is to be configured.

The screenshot shows the 'Modify Resource Group' wizard in NetApp SnapCenter. The current step is 'Resources'. On the left, there's a sidebar with icons for Home, Overview, Protection, and more. The main area has tabs: Name, Resources (which is selected), Policies, Verification, Notification, and Summary. Below the tabs, it says 'Add resources to Resource Group'. It shows a dropdown for 'Host' set to 'All' and 'Resource Type' set to 'Instances'. Under 'Available Resources', there's a search bar and a list of resources from 'SQLRD34MC' (STAVM3). An unchecked checkbox 'Auto select all the resources from the same storage volume' is present. On the right, a larger list of resources is shown, including 'ChampionshipDB1 (STAVM3)', 'ChampionshipDB10 (STAVM3)', 'ChampionshipDB11 (STAVM3)', 'ChampionshipDB12 (STAVM3)', 'ChampionshipDB13 (STAVM3)', 'ChampionshipDB14 (STAVM3)', 'ChampionshipDB15 (STAVM3)', 'ChampionshipDB16 (STAVM3)', 'ChampionshipDB17 (STAVM3)', 'ChampionshipDB18 (STAVM3)', 'ChampionshipDB19 (STAVM3)', 'ChampionshipDB20 (STAVM3)', 'ChampionshipDB21 (STAVM3)', 'ChampionshipDB22 (STAVM3)'. At the bottom, there's a note 'Activate Windows Go to Settings to activate Windows.' and a 'Next' button.

5. Enter the policy name.

The screenshot shows the 'New SQL Server Backup Policy' dialog box. The current step is 'Name'. On the left, a vertical navigation pane lists steps: 1. Name (selected), 2. Backup Type, 3. Retention, 4. Replication, 5. Script, 6. Verification, 7. Summary. The main area has a section 'Provide a policy name' with a 'Policy name' input field containing 'LOGBACKUP\_CHAMPIONSHIPDB'. Below it is a 'Details' input field also containing 'LOGBACKUP\_CHAMPIONSHIPDB'. At the bottom right, there are 'Previous' and 'Next' buttons, with 'Next' being highlighted. A note 'Activate Windows Go to Settings to activate Windows.' is at the bottom right of the dialog.

6. Select the SQL Server backup options.
7. Select log backup.
8. Set the schedule frequency based on your company's RTO. Click **Next**.

New SQL Server Backup Policy X

**1 Name** Select SQL server backup options

**2 Backup Type** Choose backup type

Full backup and log backup  
 Full backup  
 Log backup  
 Copy only backup i

Maximum databases backed up per Snapshot copy: 100 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

Previous Next

9. Configure the log backup retention settings. Click **Next**.

New SQL Server Backup Policy

X

1 Name

2 Backup Type

**3 Retention**

4 Replication

5 Script

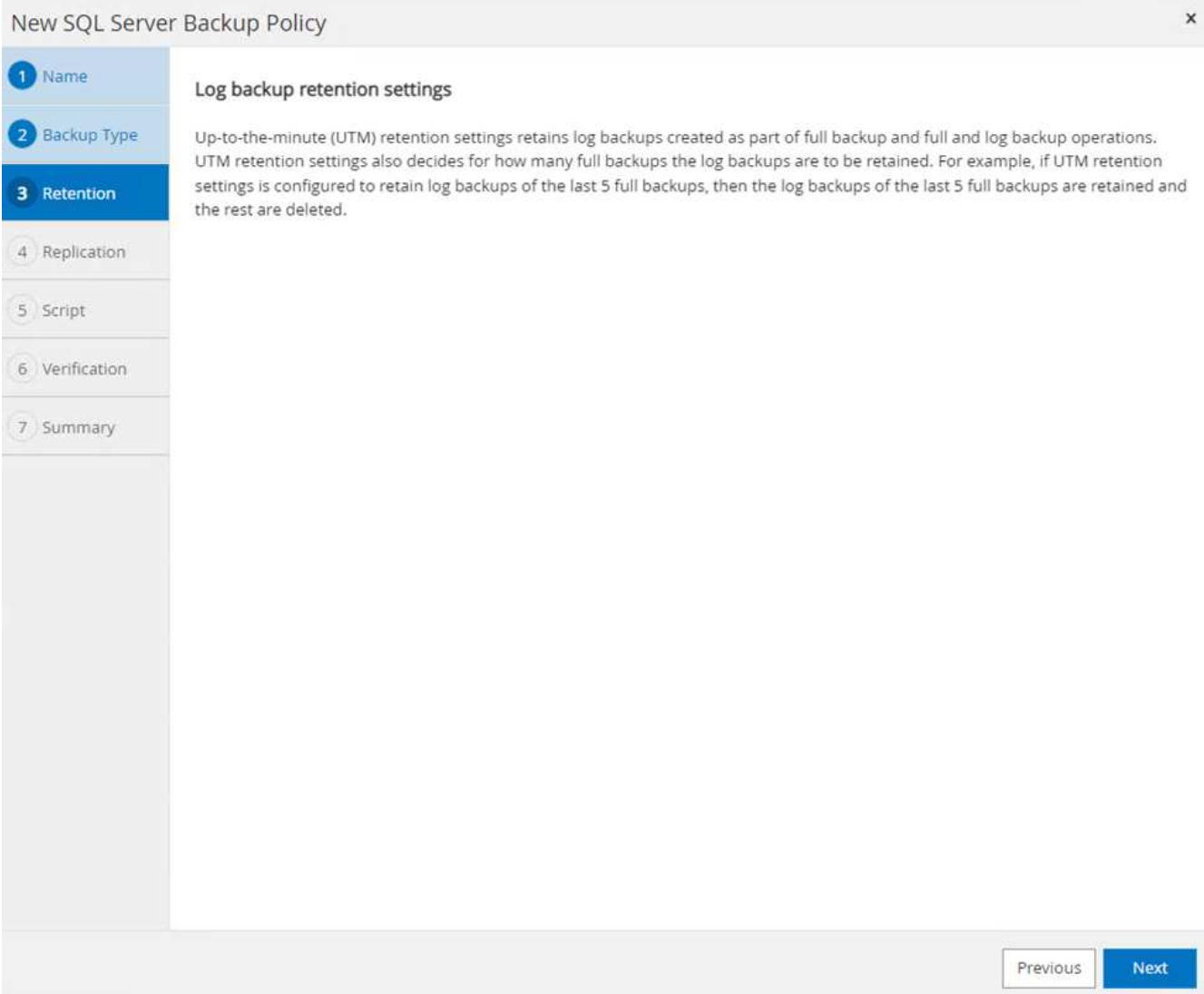
6 Verification

7 Summary

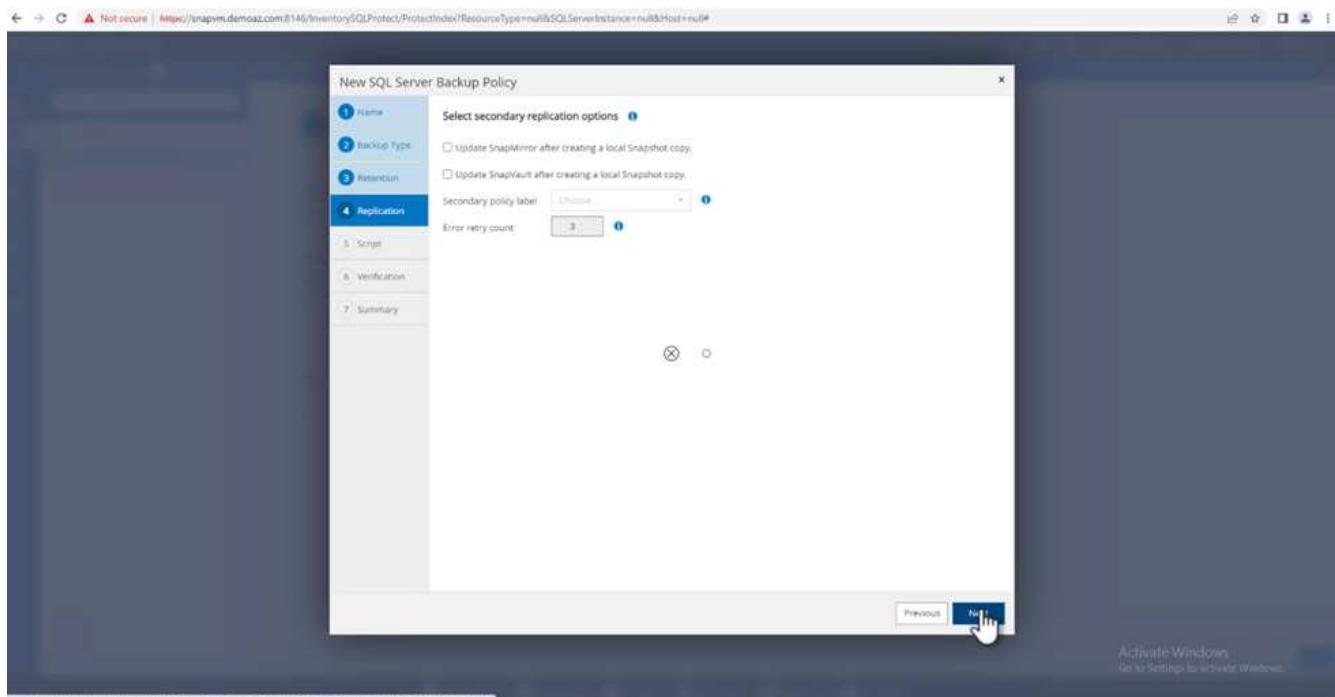
**Log backup retention settings**

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.

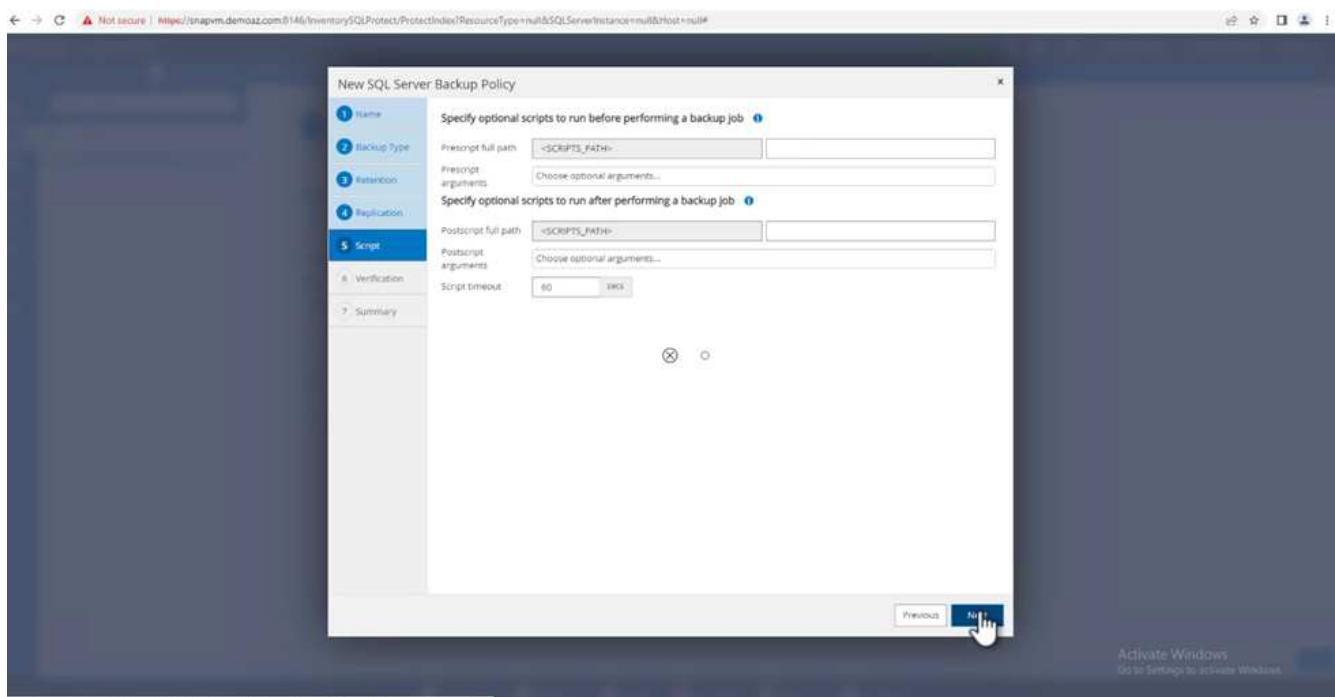
Previous Next



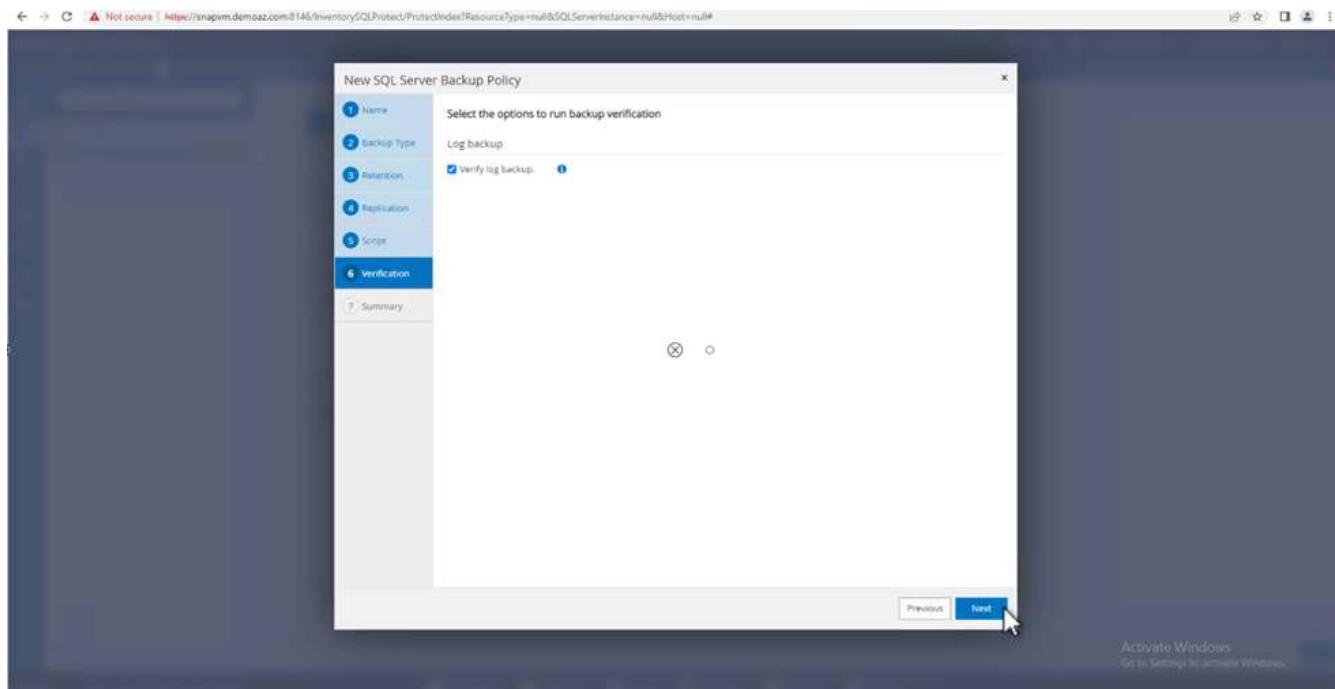
10. (Optional) Configure the replication options.



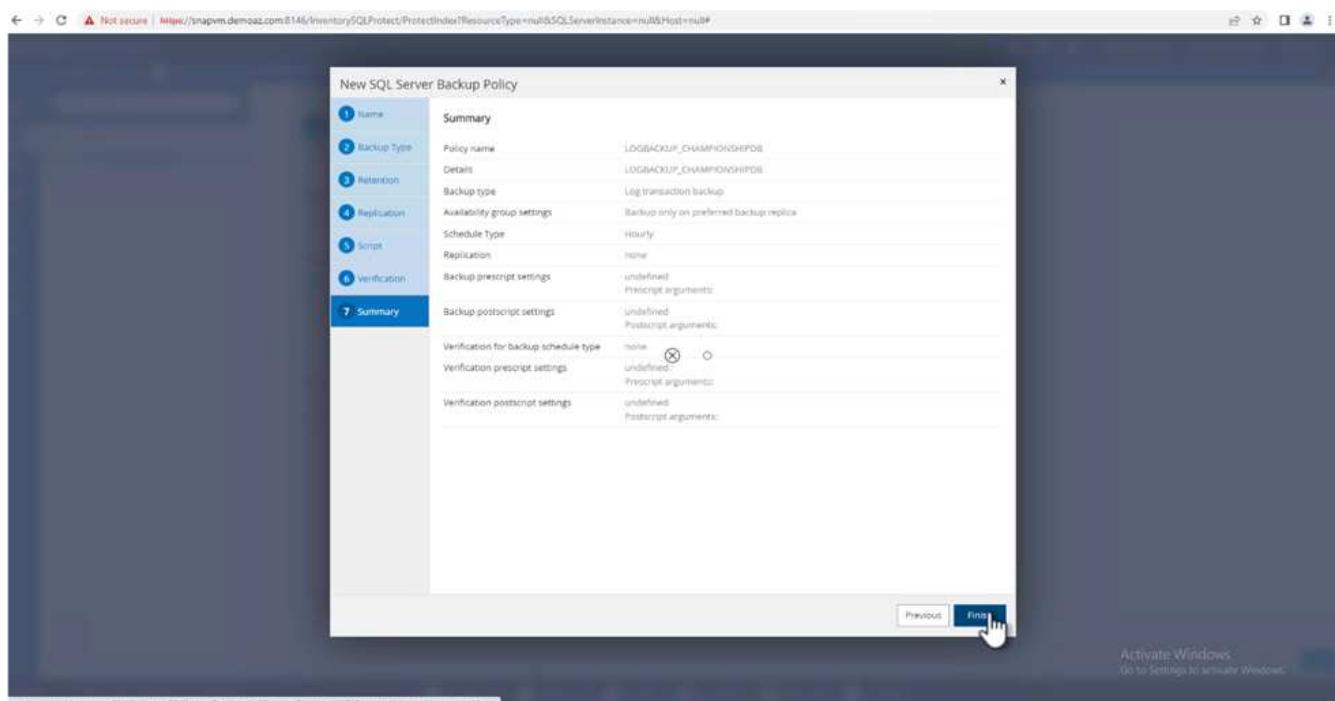
11. (Optional) Configure any scripts to run before performing a backup job.



12. (Optional) Configure backup verification.



13. On the **Summary** page, click **Finish**.



## Configure and protect multiple MSSQL Server databases

1. Click the newly created transaction log backup policy.

NetApp SnapCenter®

Microsoft SQL Server

Modify Resource Group

Name: RG-CHAMPIONSHIPDB

Select one or more policies and configure schedules:

FULLBACKUP\_CHAMPIONSHIPDB +

Configure schedules for selected policies:

Policy	Applied Schedules	Configure Schedules
FULLBACKUP_CHAMPIONSHIPDB	Hourly: Repeat every 8 hours	<input type="button" value="Edit"/> <input type="button" value="X"/>
LOGBACKUP_CHAMPIONSHIPDB	None	<input type="button" value="Edit"/> <input type="button" value="X"/>

Total 2

Use Microsoft SQL Server scheduler ?

Created backup policy LOGBACKUP\_CHAMPIONSHIPDB

Activate Windows Go to Settings to activate Windows

2. Set the **Start date** and **Expires on** date.
3. Enter the frequency of the log backup policy depending on the SLA, RTP, and RPO. Click OK.

Add schedules for policy LOGBACKUP\_CHAMPIONSHIPDB

Hourly

Start date: 11/11/2022 07:30 pm

Expires on: 12/11/2022 06:30 pm

Repeat every: 2 hours 0 mins

The schedules are triggered by the SnapCenter Server time zone.

Cancel

Activate Windows Go to Settings to activate Windows

4. You can see both policies. Click **Next**.

**Policies Step:**

Policy	Applied Schedules	Configure Schedules
FULLBACKUP_CHAMPIONSHIPDB	Hourly: Repeat every 8 hours	<input checked="" type="checkbox"/> <input type="checkbox"/>
LOGBACKUP_CHAMPIONSHIPDB	Hourly: Repeat every 2 hours	<input checked="" type="checkbox"/> <input type="checkbox"/>

Total 2

Use Microsoft SQL Server scheduler

## 5. Configure the verification server.

**Verification Step:**

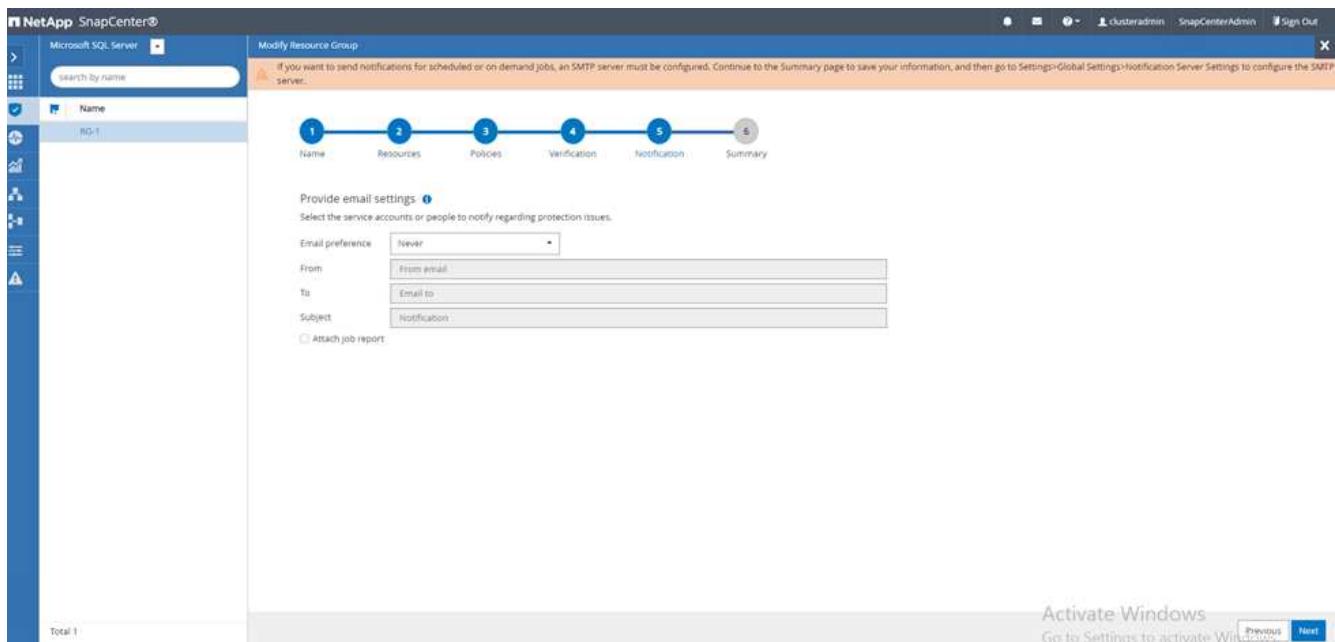
Select the verification servers:

Verification server: STAVM3(13.0.5026)

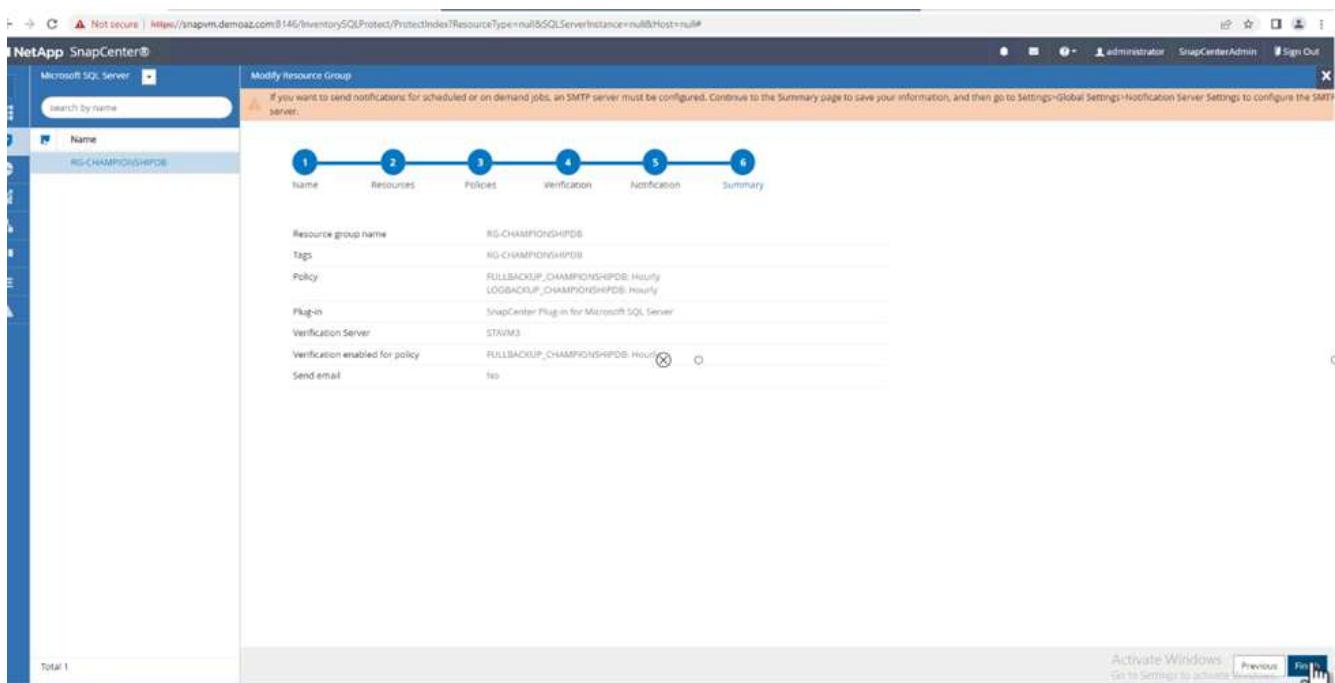
Policy	Schedule Type	Applied Schedules	Configure Schedules
FULLBACKUP_CHAMPIONSHIPDB	Hourly	Verify after backup	<input checked="" type="checkbox"/> <input type="checkbox"/>

Total 1

## 6. Configure email notification.



7. On the **Summary** page, click **Finish**.



## Triggering an on-demand transaction log backup for multiple SQL Server databases

To trigger an on-demand backup of the transactional log for multiple SQL server databases, complete the following steps:

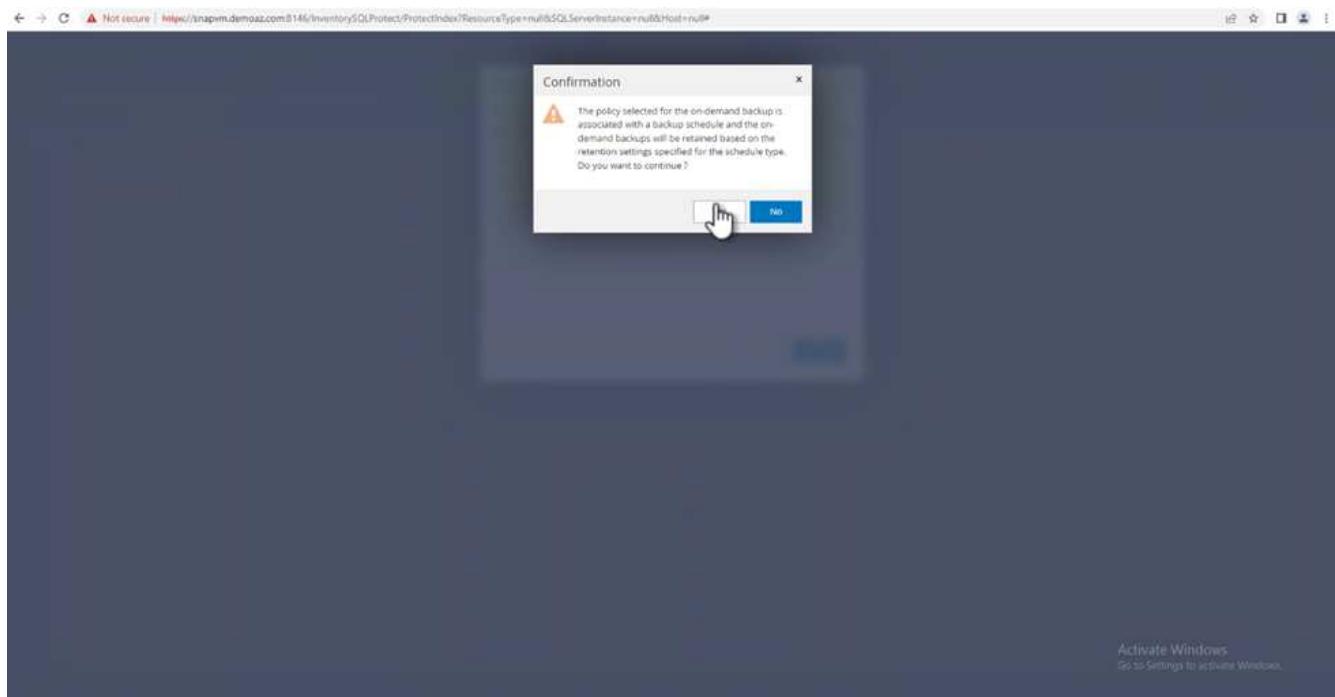
1. On the newly created policy page, select **Backup now** at the upper right of the page.

The screenshot shows the NetApp SnapCenter interface for managing Microsoft SQL Server resources. A specific resource group, RG-CHAMPIONSHIPDB, is selected. The interface displays a table of 24 SQL databases, each with its name, type (SQL Database), and host information (STAV/M3.DemoAZ.com). A callout box on the left provides instructions for setting up policies, global settings, roles, permissions, and load balancing. At the top right, there are several action buttons: 'Modify Resource Group', 'Backup Now' (which is being pointed to by a mouse cursor), 'Delete', 'Edit/View Details', 'Maintenance', 'Metrics', and 'Logs'. A message at the bottom right encourages activating Windows.

- From the pop-up on the **Policy** tab, select the drop-down menu, select the backup policy, and configure the transaction log backup.

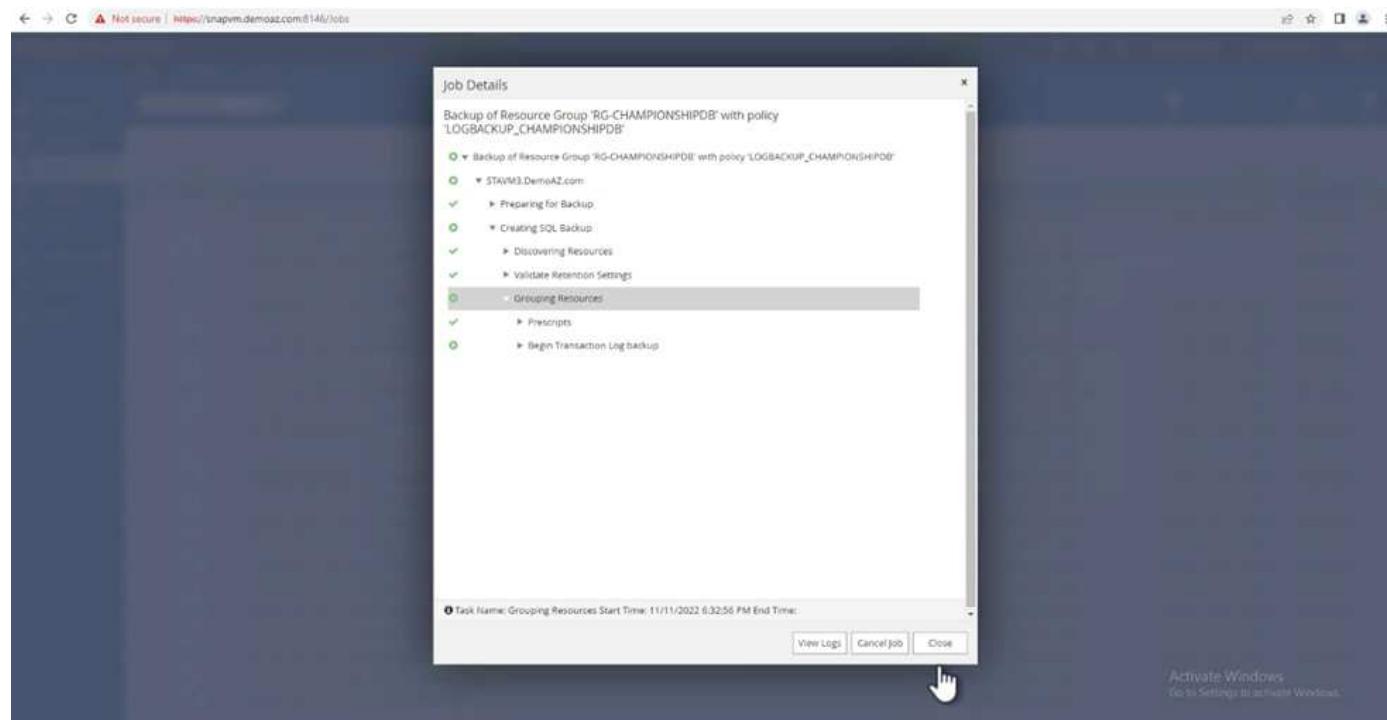
This screenshot shows a 'Backup' dialog box overlaid on the previous interface. It prompts the user to create a backup for the selected resource group, RG-CHAMPIONSHIPDB. The 'Policy' dropdown menu is open, showing two options: 'FULLBACKUP\_CHAMPIONSHIPDB' (selected) and 'LOGBACKUP\_CHAMPIONSHIPDB'. A checkbox for 'Verify after backup' is present but unchecked. At the bottom of the dialog are 'Cancel' and 'Backup' buttons, with the latter being highlighted by a mouse cursor.

- Click **Backup**. A new window is displayed.
- Click **Yes** to confirm the backup policy.



## Monitoring

Move to the **Monitoring** tab and monitor the progress of the backup job.



## Restore and recovery

See the following prerequisites necessary for restoring a SQL Server database in SnapCenter.

- The target instance must be online and running before a restore job completes.
- SnapCenter operations that are scheduled to run against the SQL Server database must be disabled,

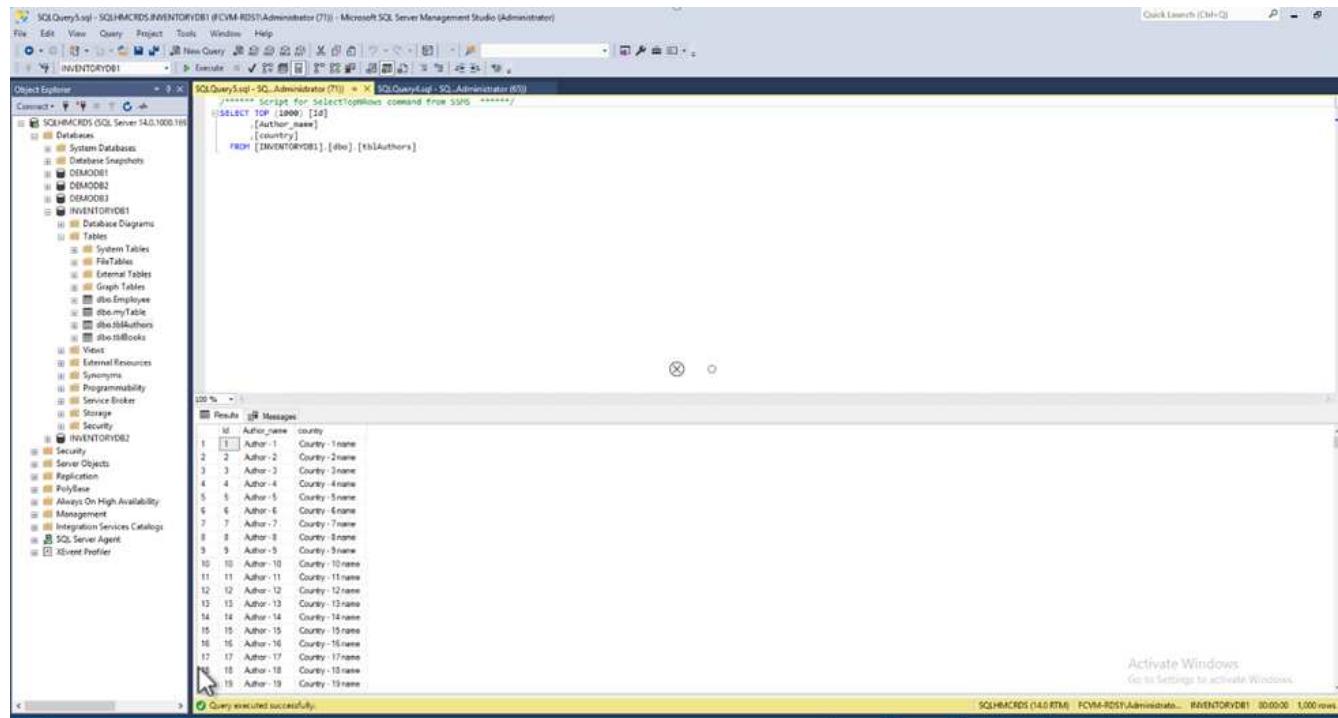
including any jobs scheduled on remote management or remote verification servers.

- If you are restoring custom log directory backups to an alternate host, the SnapCenter server and the plugin host must have the same SnapCenter version installed.
- You can restore the system database to an alternate host.
- SnapCenter can restore a database in a Windows cluster without taking the SQL Server cluster group offline.

## Restoring deleted tables on a SQL Server database to a point in time

To restore a SQL Server database to a point in time, complete the following steps:

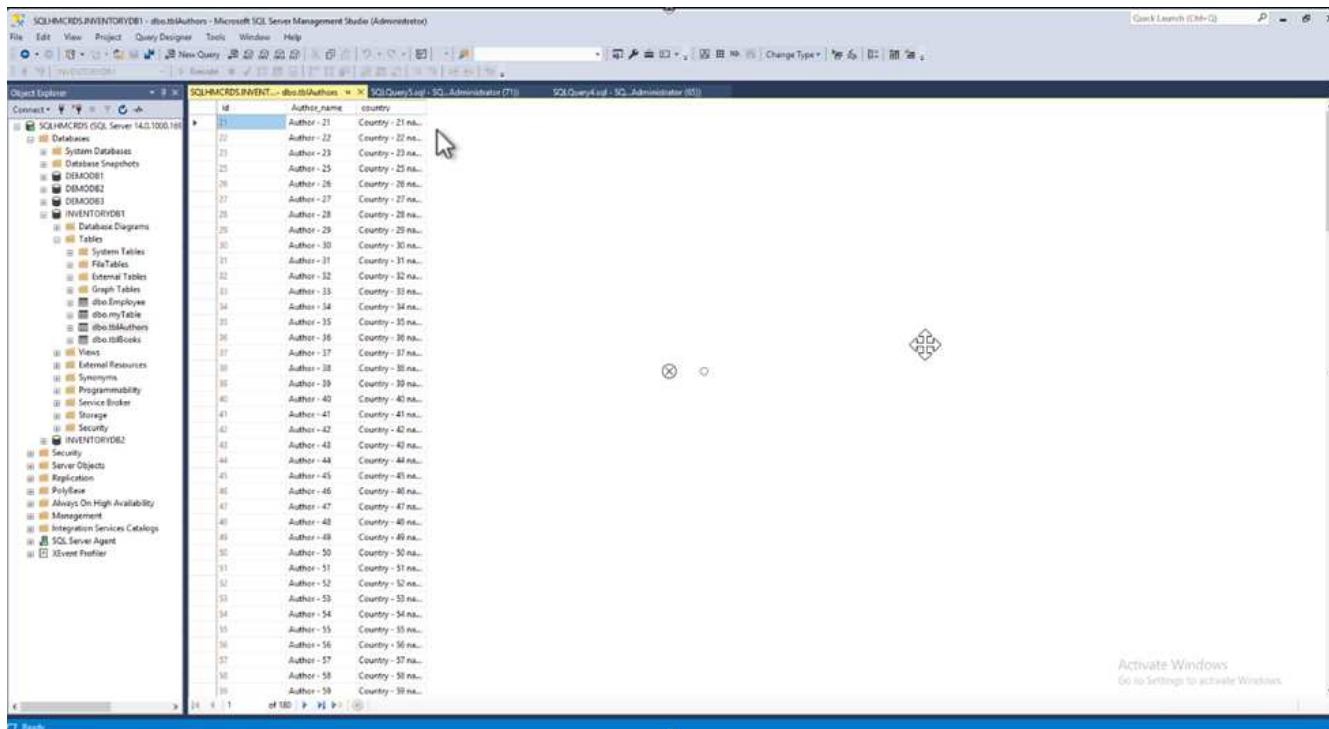
1. The following screenshot shows the initial state of the SQL Server database before the deleted tables.



The screenshot shows a Microsoft SQL Server Management Studio (SSMS) interface. On the left, the Object Explorer tree view shows the database structure, including the INVENTORYDB1 database which contains several tables like Authors, Books, and Titles. In the center, a query results grid displays 20 rows of data from the Authors table, with columns for Id, Author\_name, and country. The data shows various authors from different countries. At the bottom of the results grid, a message says "Query executed successfully." To the right of the results grid, there is a watermark for "Activate Windows" and a status bar at the bottom of the window.

Id	Author_name	country
1	Author - 1	Country - 1 name
2	Author - 2	Country - 2 name
3	Author - 3	Country - 3 name
4	Author - 4	Country - 4 name
5	Author - 5	Country - 5 name
6	Author - 6	Country - 6 name
7	Author - 7	Country - 7 name
8	Author - 8	Country - 8 name
9	Author - 9	Country - 9 name
10	Author - 10	Country - 10 name
11	Author - 11	Country - 11 name
12	Author - 12	Country - 12 name
13	Author - 13	Country - 13 name
14	Author - 14	Country - 14 name
15	Author - 15	Country - 15 name
16	Author - 16	Country - 16 name
17	Author - 17	Country - 17 name
18	Author - 18	Country - 18 name
19	Author - 19	Country - 19 name

The screenshot shows that 20 rows were deleted from the table.



## 2. Log into SnapCenter Server. From the **Resources** tab, select the database.

The screenshot shows the SnapCenter interface with the following details:

- Left Sidebar:** Includes 'Dashboard', 'Monitor', 'Reports', 'Hosts', 'Storage Systems', 'Settings', and 'Alerts'.
- Top Bar:** 'NetApp SnapCenter®', 'Microsoft SQL Server', 'View: Database', 'Search by name'.
- Table:** Shows the following data for a Microsoft SQL Server instance:
 

Name	Instance	Host	Last Backup	Overall Status	Type
INVENTORYDB1	SQLHMCRODS	PSXCLUSTER.Demoaz.com	11/16/2022 10:52:44 PM	Backup succeeded	User database
INVENTORYDB2	SQLHMCRODS	PSXCLUSTER.Demoaz.com	11/16/2022 10:59:49 PM	Backup succeeded	User database
master	SQLHMCRODS	PSXCLUSTER.Demoaz.com		Not protected	System database
model	SQLHMCRODS	PSXCLUSTER.Demoaz.com		Not protected	System database
msdb	SQLHMCRODS	PSXCLUSTER.Demoaz.com		Not protected	System database
tempdb	SQLHMCRODS	PSXCLUSTER.Demoaz.com		Not available for backup	System database
DEMOOB1	SQLHMCRODS	PSXCLUSTER.Demoaz.com	11/16/2022 11:03:57 PM	Backup succeeded	User database
DEMOOB2	SQLHMCRODS	PSXCLUSTER.Demoaz.com	11/16/2022 11:03:57 PM	Backup succeeded	User database
DEMOOB3	SQLHMCRODS	PSXCLUSTER.Demoaz.com	11/16/2022 11:03:57 PM	Backup succeeded	User database
- Bottom Status Bar:** 'Activate Windows' and 'Go to Settings to activate Windows.'

## 3. Select the most recent backup.

## 4. On the right, select **Restore**.

The screenshot shows the NetApp SnapCenter interface for managing Microsoft SQL Server databases. The left sidebar lists databases: INVENTORYDB1, INVENTORYDB2, master, model, msdb, tempdb, DEMO0B1, DEMO0B2, and DEMO0B3. The main area displays the 'INVENTORYDB1 (SQL.HMCROSS) Topology'. A summary card indicates 4 Backups and 0 Clones. Below this, a table shows Primary Backup(s) with columns: Backup Name, Count, Type, LF, End Date, and Verified. The table lists four full backups from 11/15/2022 at various times, all marked as verified.

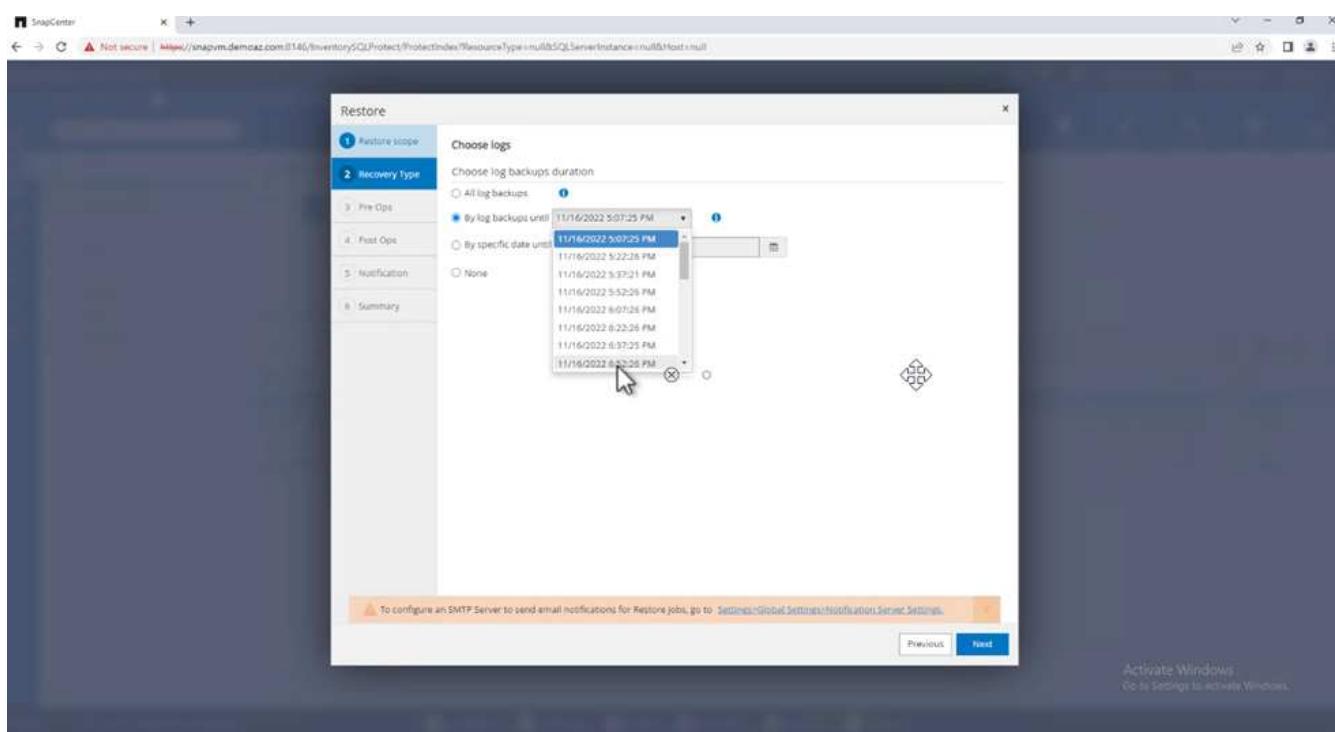
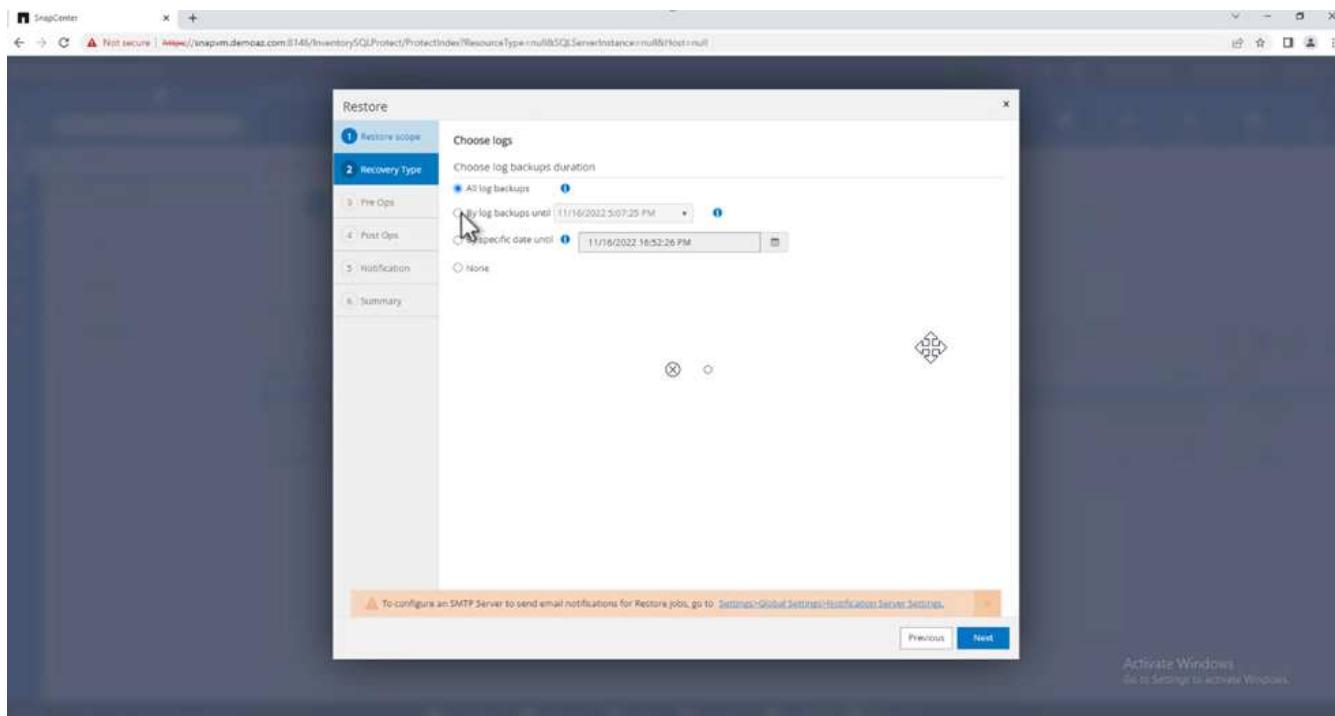
5. A new window is displayed. Select the **Restore** option.
6. Restore the database to the same host where the backup was created. Click **Next**.

The screenshot shows the 'Restore' dialog box. The 'Scope' tab is active, displaying options for restoring database files. The 'Recovery Type' section contains three radio buttons:

- Restore the database to the same host where the backup was created
- Restore the database to an alternate host
- Restore the database using existing database files

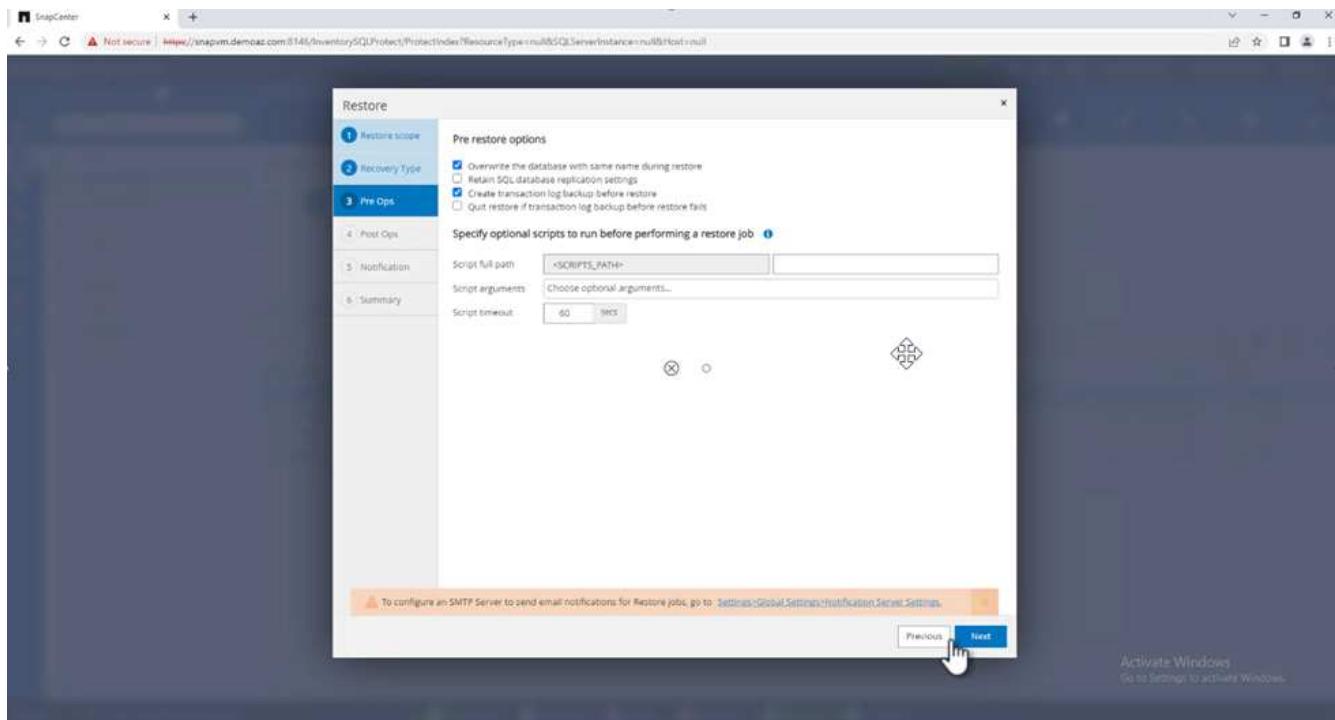
A note at the bottom states: "To configure an SMTP Server to send email notifications for Restore jobs, go to [Settings>Global Settings>Notification Server Settings](#)". At the bottom right, there are 'Previous' and 'Next' buttons.

7. For the **Recovery type**, select **All log backups**. Click **Next**.



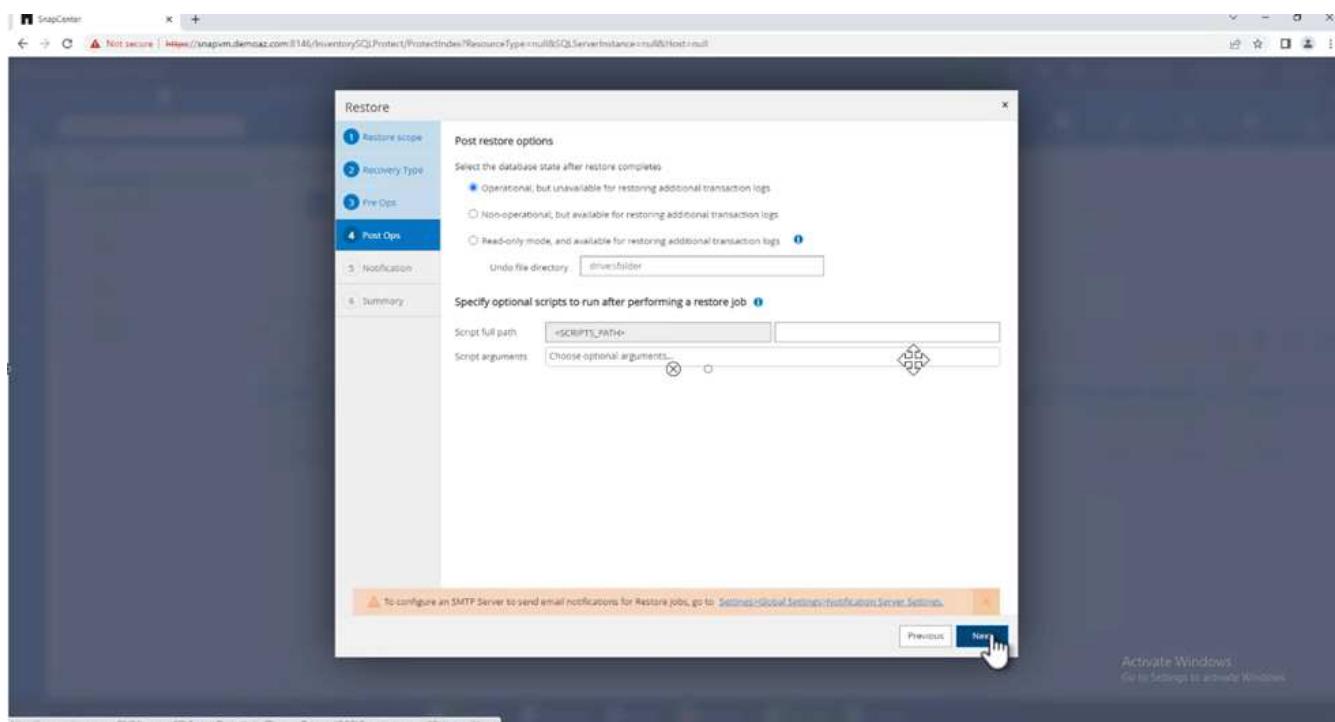
### Pre- restore options:

1. Select the option **Overwrite the database with same name during restore**. Click **Next**.

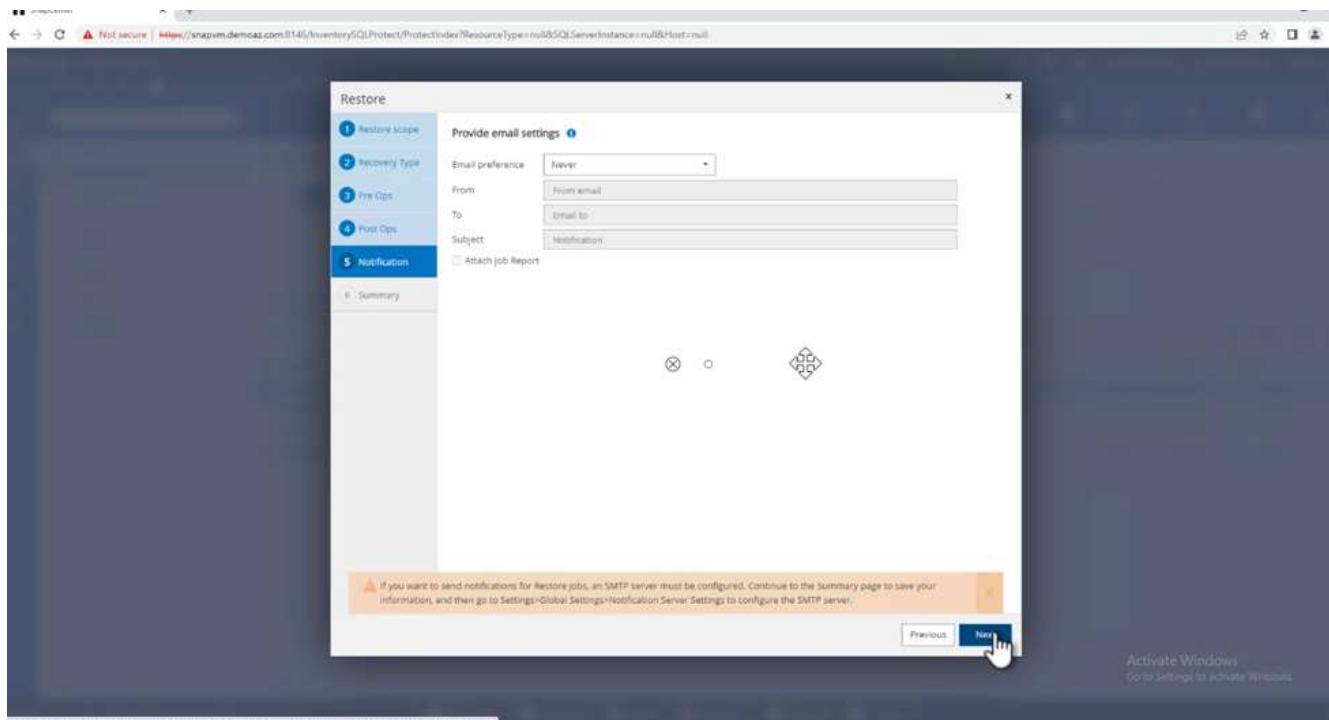


### Post- restore options:

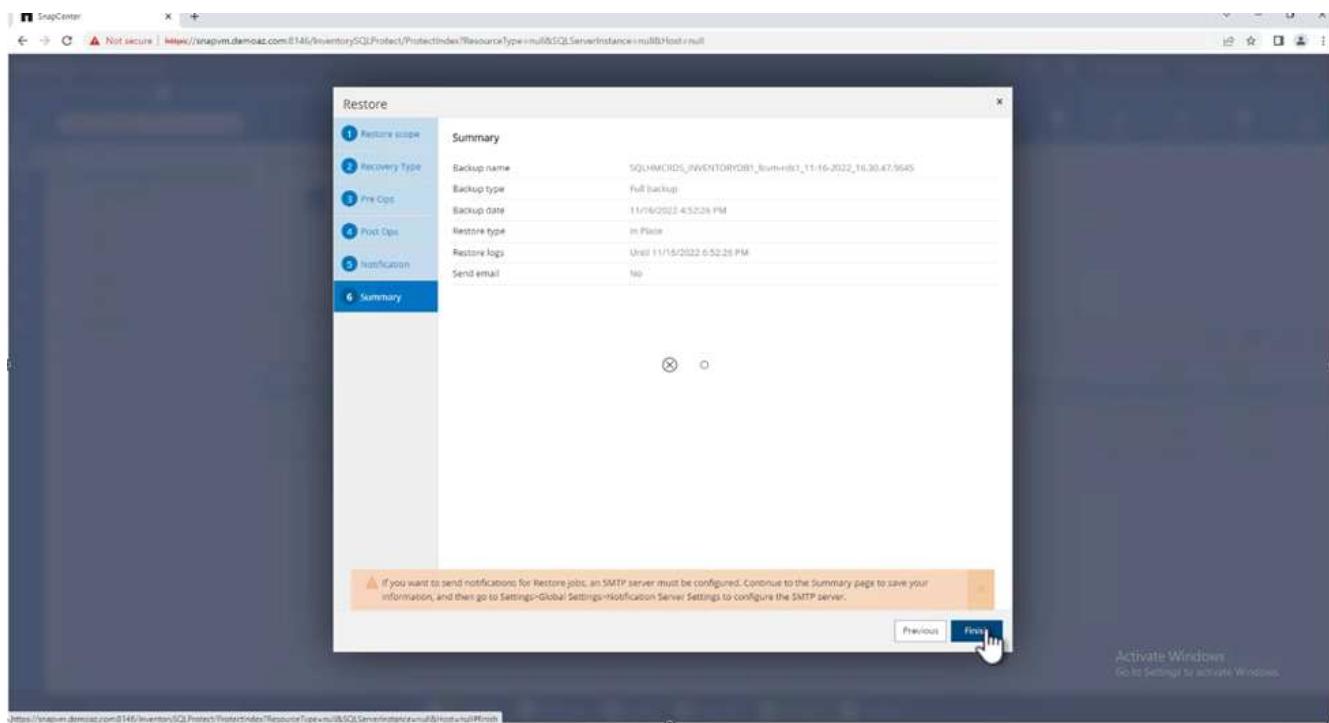
1. Select the option **Operational, but unavailable for restoring additional transaction logs**. Click **Next**.



2. Provide the email settings. Click **Next**.



3. On the **Summary** page, click **Finish**.



## Monitoring the restore progress

1. From the **Monitoring** tab, click the restore job details to view the progress of the restore job.

Screenshot of the NetApp SnapCenter interface. The left sidebar shows navigation options: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area is titled 'Jobs - Filter' and lists 133 backup jobs. The columns include ID, Status, Name, Start date, End date, and Owner. Most jobs are labeled 'Backup of Resource Group' or 'Restore' with various policy names like 'demoDB-logbackup\_policy'. The 'Owner' column consistently shows 'Administrator'. A search bar at the top is set to 'search by name'.

## 2. Restore the job details.

The screenshot shows the 'Job Details' dialog for job 157. The dialog title is 'Job Details' and the sub-task title is 'Restore 'SQLHMCRD\$INVENTORYDB''. The tree view shows the following steps:

- Restore 'SQLHMCRD\$INVENTORYDB'
- (job 157) Tail log backup of 'SQLHMCRD\$INVENTORYDB'
- FCM-RDS1.Demoaz.com
  - Preparing for Backup
  - Creating SQL Backup
  - Finalizing Backup
  - Send EMS Messages
- FCM-RDS1.Demoaz.com

A tooltip at the bottom indicates the task name is 'Send EMS Messages' with a start time of 11/16/2022 11:18:54 PM and an end time of 11/16/2022 11:18:54 PM. Buttons at the bottom are 'View Logs', 'Cancel job', and 'Close'.

## 3. Return to SQL Server host > database > table are present.

```
SELECT TOP (1000) [Id]
      ,[Author_name]
      ,[country]
  FROM [INVENTORYDB1].[dbo].[tb1Authors]
```

	Author_name	country
1	Author -1	Country -1name
2	Author -2	Country -2name
3	Author -3	Country -3name
4	Author -4	Country -4name
5	Author -5	Country -5name
6	Author -6	Country -6name
7	Author -7	Country -7name
8	Author -8	Country -8name
9	Author -9	Country -9name
10	Author -10	Country -10name
11	Author -11	Country -11name
12	Author -12	Country -12name

## Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

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

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

- Requirements for restoring a database

[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)

- Understanding cloned database lifecycles

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

# TR-4467: SAP with Microsoft SQL Server on Windows - Best practices using NetApp Clustered Data ONTAP and SnapCenter

Marco Schoen, NetApp

TR-4467 provides customers and partners with best practices for deploying clustered NetApp Data ONTAP in support of SAP Business Suite solutions running in a Microsoft SQL Server on Windows environment.

[TR-4467: SAP with Microsoft SQL Server on Windows - Best practices using NetApp Clustered Data ONTAP and SnapCenter](#)

# **Modernizing your Microsoft SQL Server environment**

Optimize operations and unleash the power of your data - on the premises or in the cloud.

[Modernizing your Microsoft SQL Server environment](#)

## **TR-4764: Best practices for Microsoft SQL Server with NetApp EF-Series**

Mitch Blackburn, Pat Sinthusan, NetApp

This best practices guide is intended to help storage administrators and database administrators successfully deploy Microsoft SQL Server on NetApp EF-Series storage.

[TR-4764: Best practices for Microsoft SQL Server with NetApp EF-Series](#)

## **Copyright information**

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—with prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## **Trademark information**

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.