



Backup and Recovery for Microsoft SQL Server on AWS FSx for ONTAP

NetApp Solutions

NetApp
October 20, 2023

Table of Contents

- TR-4951: Backup and Recovery for Microsoft SQL Server on AWS FSx for ONTAP 1
 - SnapCenter Configuration 1
 - SnapCenter newly installed user interface 1
 - Configure a backup policy 10
 - Configure and protect MSSQL Server database 17
 - SnapCenter backup operations 19
 - Monitor backup job 20
 - Backup operation for multiple databases 21
 - Configure and protect multiple SQL Server databases 30
 - Trigger on-demand backup for multiple SQL Server databases 33
 - Monitor multiple-database backup jobs 35
 - Transaction log backup for multiple database backup 36
 - Configure and protect multiple MSSQL Server databases 42
 - Triggering an on-demand transaction log backup for mutiple SQL Server databases 45
 - Monitoring 47
 - Restore and recovery 47
 - Restoring deleted tables on a SQL Server database to a point in time 48
 - Monitoring the restore progress 53
 - Where to find additional information 55

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

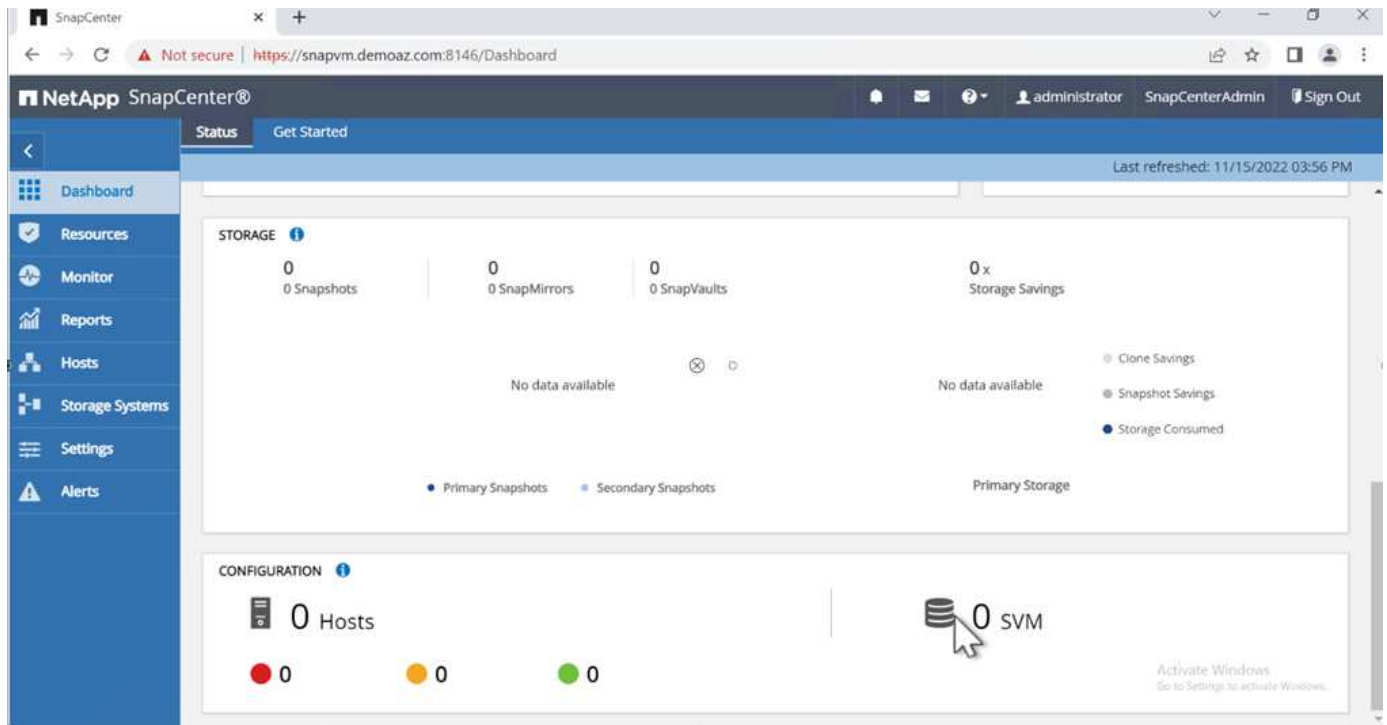
SnapCenter Configuration

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.

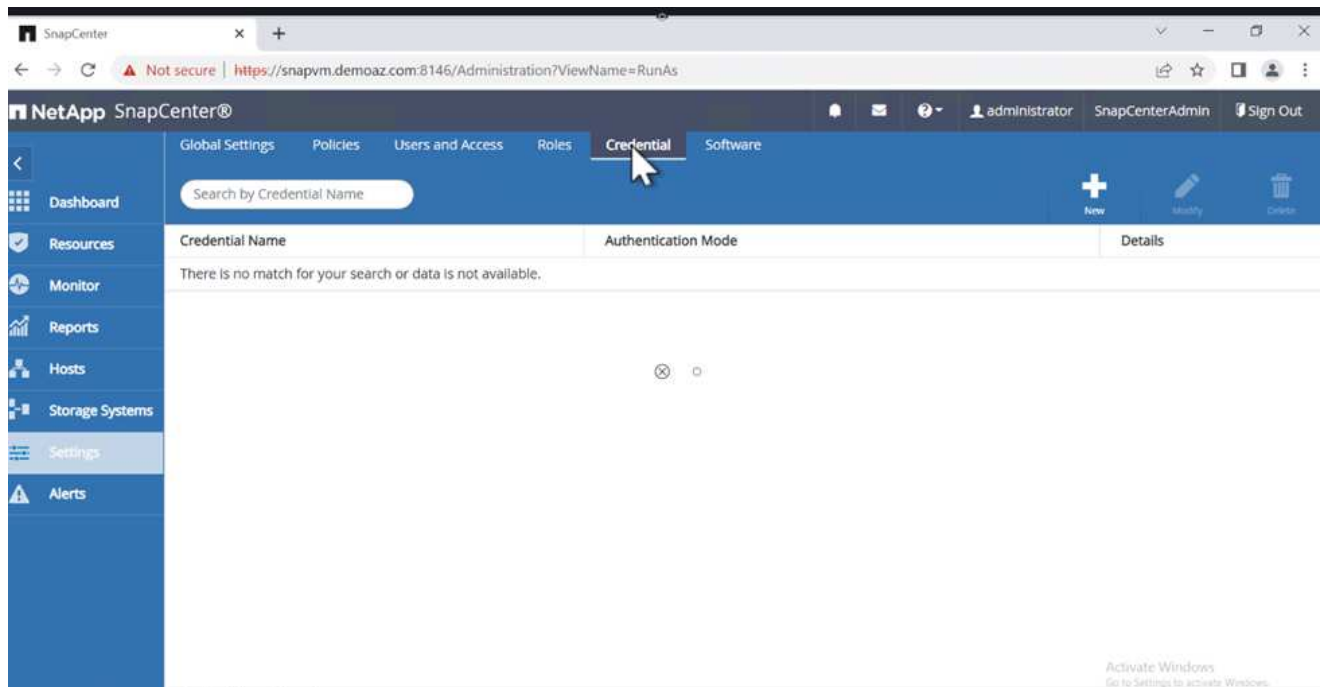


NetApp recommends using role-based access control (RBAC) to delegate data protection and management capabilities to individual users across the SnapCenter and window hosts. The user must have access to the SQL Server hosting the database. For multiple hosts, the username and password must be the same 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 (+).



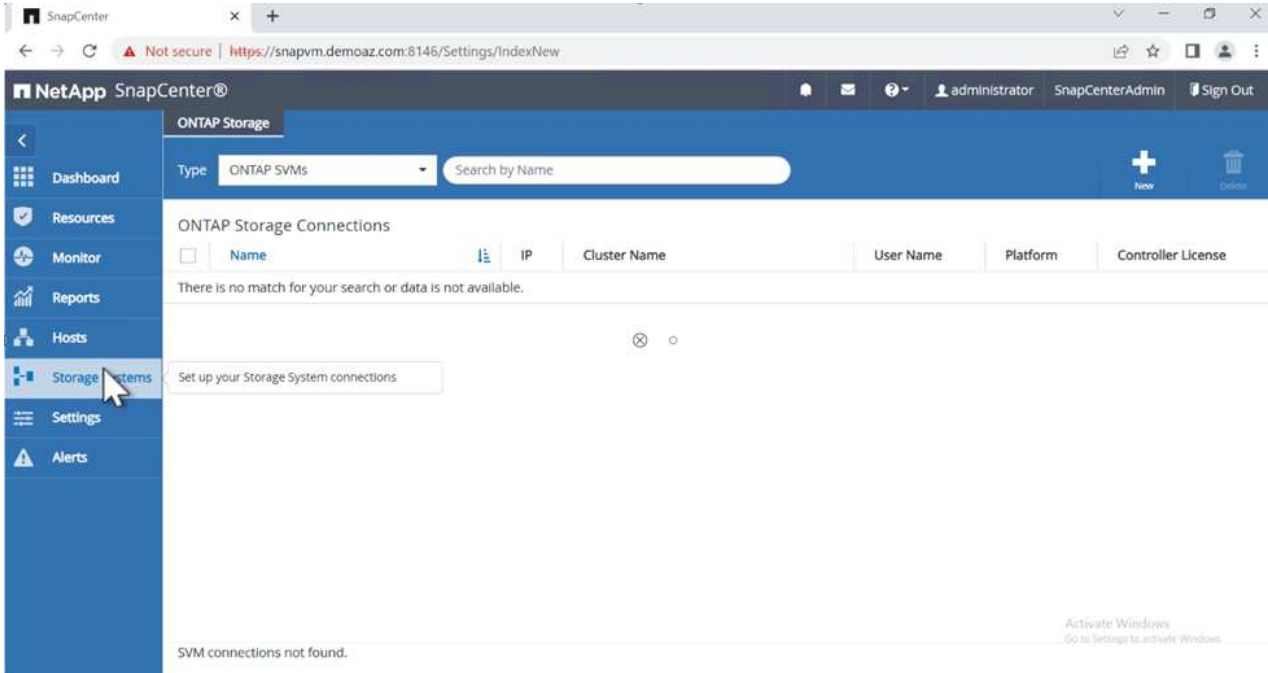
The new user must have administrator rights on the SQL Server host.

A screenshot of the 'Credential' dialog box. It has a title bar 'Credential' with a close button. The form contains four fields: 'Credential Name' with the value 'Demoaz', 'Authentication Mode' with a dropdown menu showing 'Windows', 'Username' with the value 'demoaz\clusteradmin', and 'Password' with masked characters '.....'. There is an information icon (i) to the right of the Username field. At the bottom, there is a progress indicator 'Setting credential...' with a circular arrow icon, and two buttons: 'Cancel' and 'OK'.

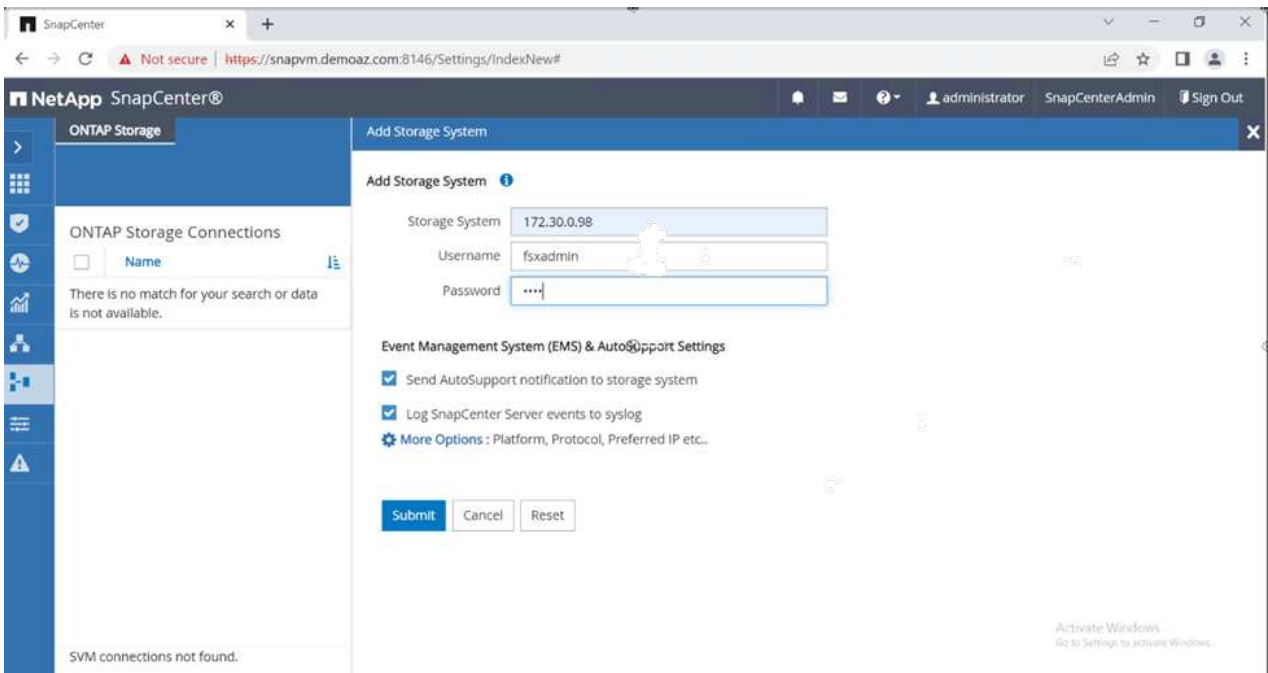
Configure storage

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.

NetApp SnapCenter®

ONTAP Storage

Type: Search by Name

ONTAP Storage Connections

	Name	IP	Cluster Name	User Name	Platform	Controller License
<input type="checkbox"/>	FSXSYMTST005		rdsfsxTest01		FSx	Not applicable

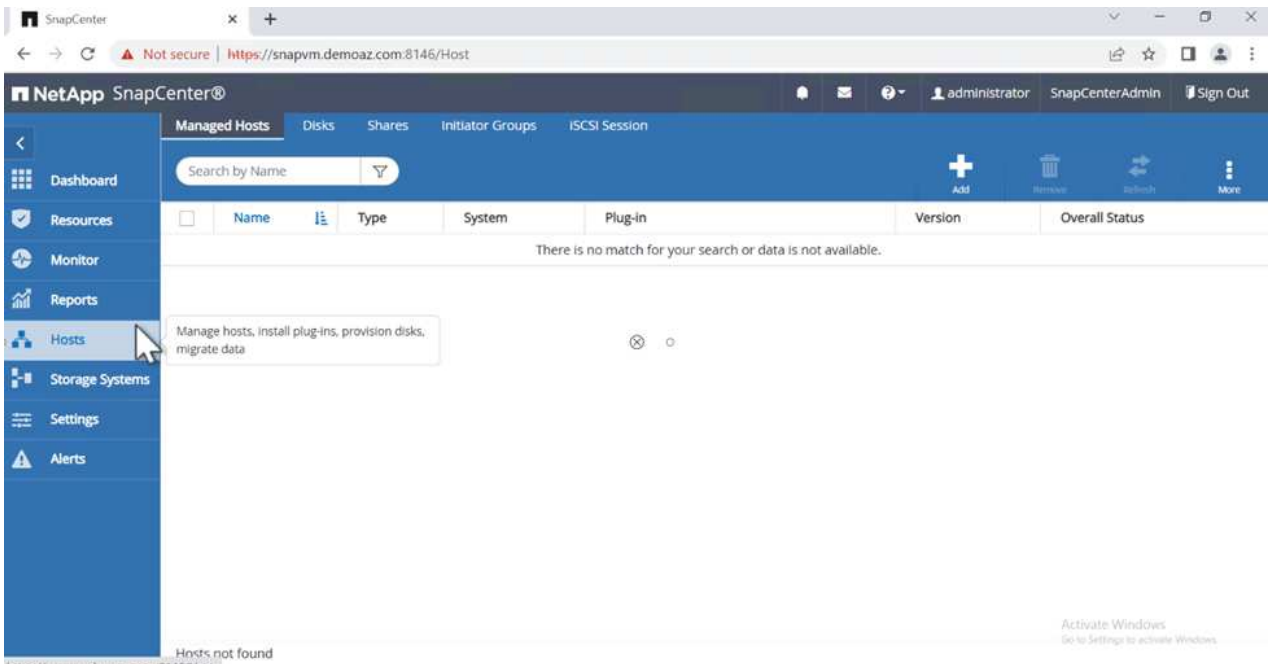
Total 1

Activate Windows
Go to Settings to activate Windows.

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.

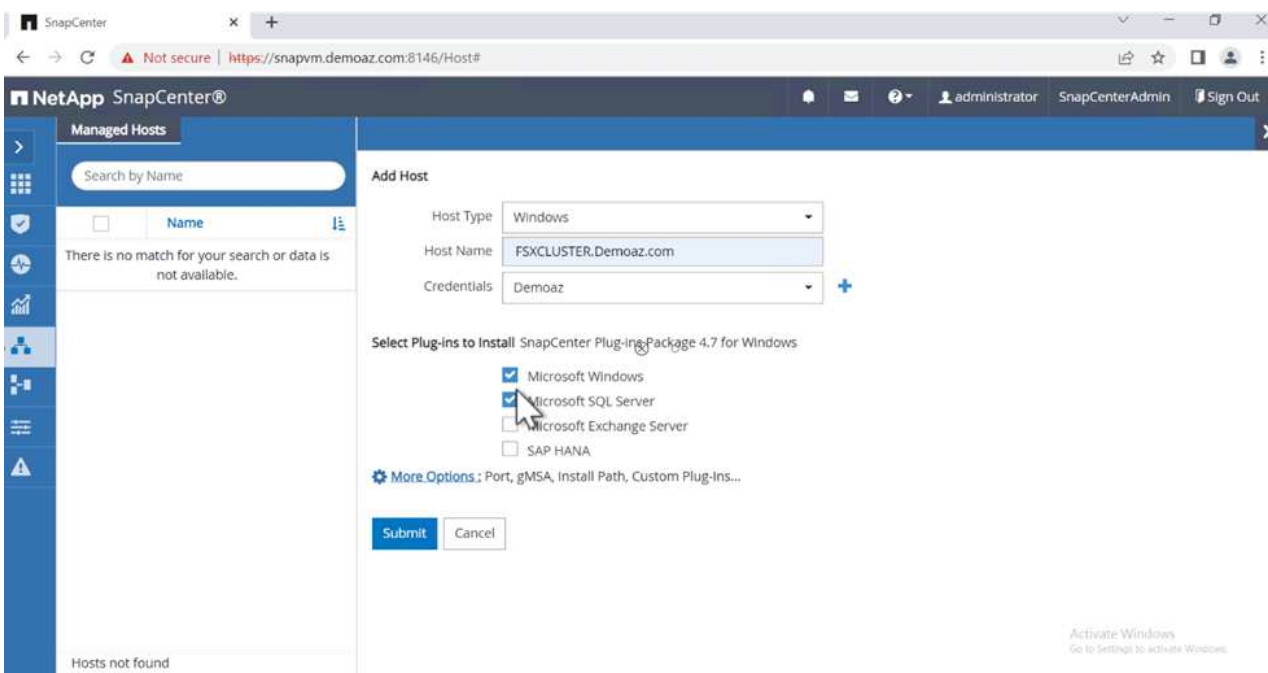


2. Provide the fully qualified domain name (FQDN) or IP address of the remote host.



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.

NetApp SnapCenter®

Managed Hosts | Disks | Shares | Initiator Groups | iSCSI Session

Search by Name

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

Total 1

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

NetApp SnapCenter®

File Systems

View Path

Name	Host	Storage Layout	Resource Groups	Policies	Last Backup	Overall Status
D:\	FSXCLUSTER.Demoaz.com	FSXSVMTSTRDS/...FCIDATA/FCIDATA				Not protected
E:\	FSXCLUSTER.Demoaz.com	FSXSVMTSTRDS/.../FCILOG/FCILOG				Not protected
F:\	FSXCLUSTER.Demoaz.com	FSXSVMTSTRDS/...ACKUP/FCIBACKUP				Not protected
G:\	FSXCLUSTER.Demoaz.com	FSXSVMTSTRDS/...SNAPLOG/SNAPLOG				Not protected
H:\	FSXCLUSTER.Demoaz.com	FSXSVMTSTRDS/...FCITEMP/FCITEMP				Not protected
K:\	FSXCLUSTER.Demoaz.com	FSXSVMTSTRDS/...UORUM/FCIQUORUM				Not protected

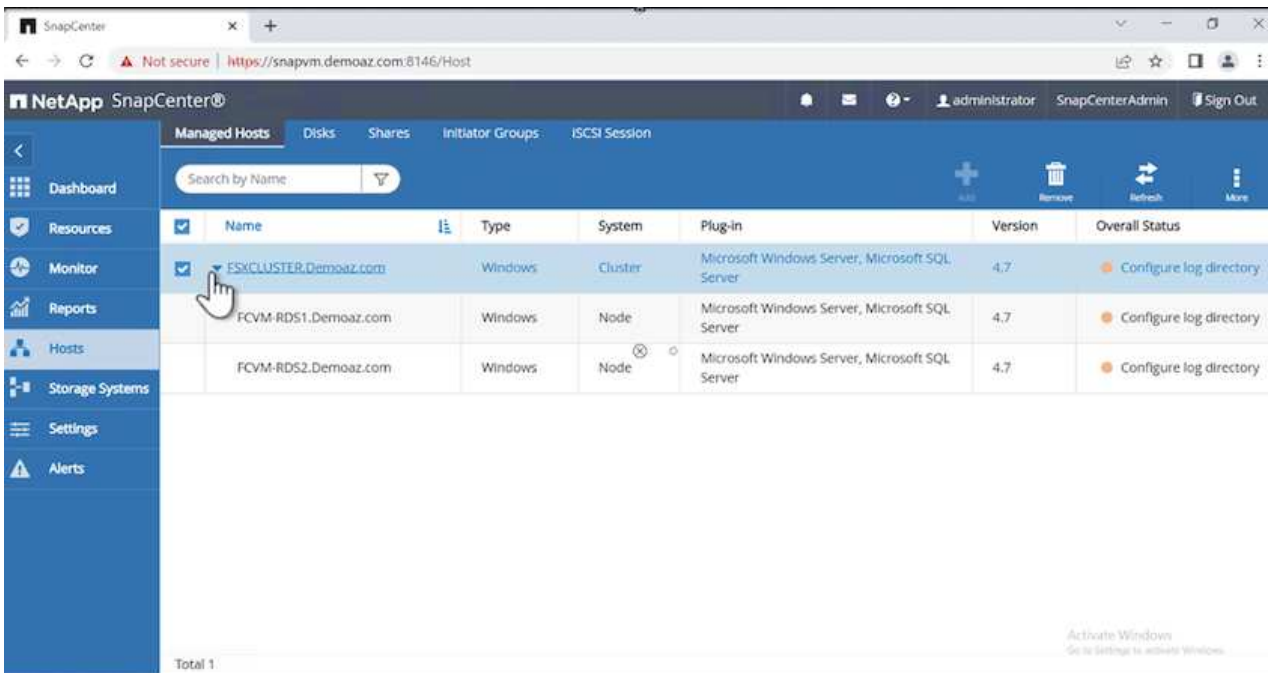
Total 6

Activity | The 5 most recent jobs are displayed | 0 Completed | 0 Warnings | 0 Failed | 0 Canceled | 0 Running | 0 Queued

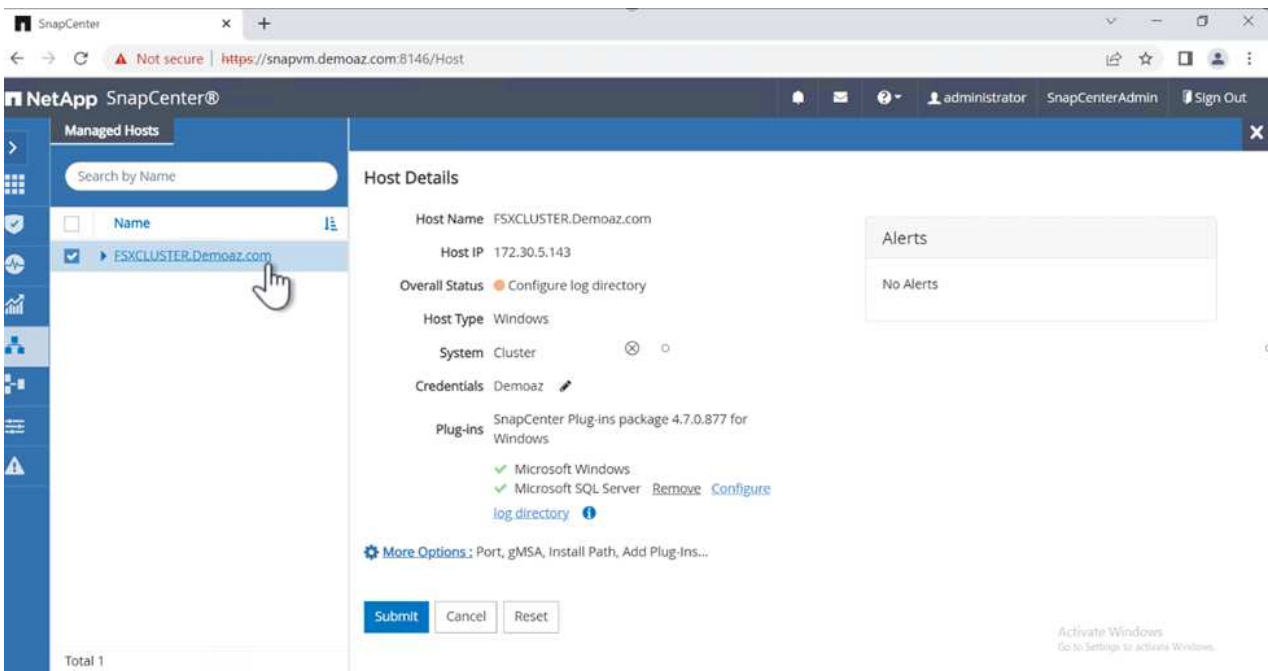
Configure log directory

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

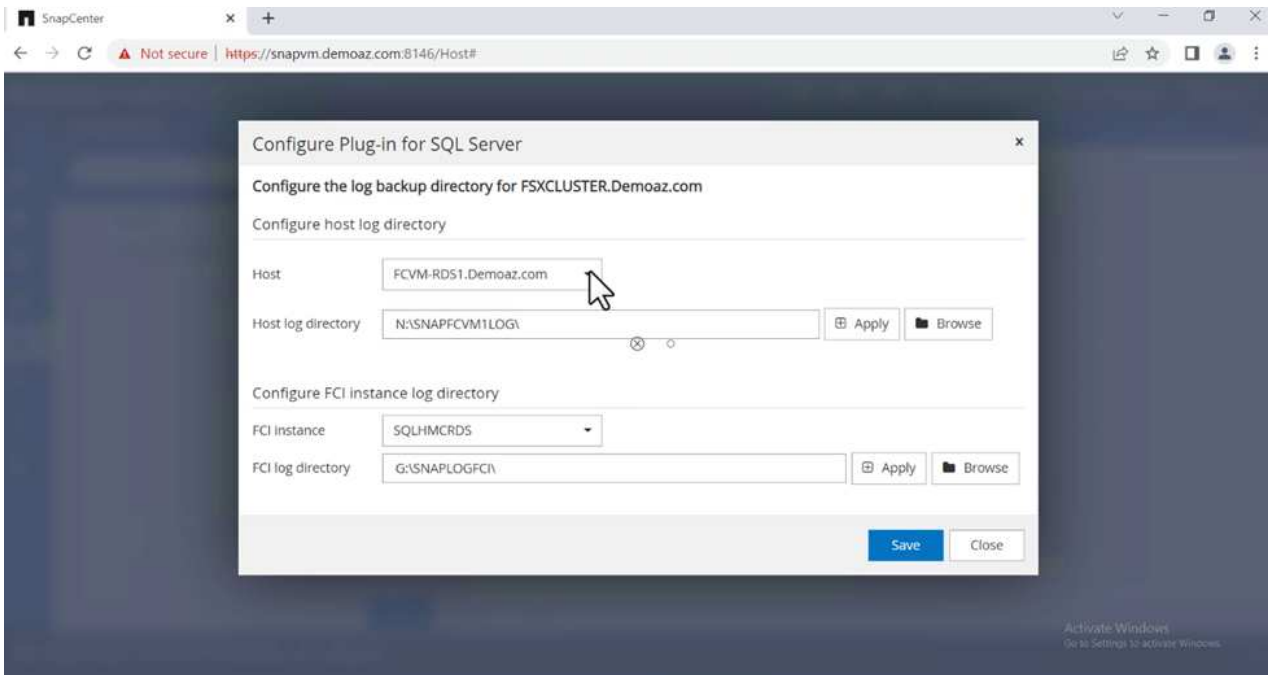
1. Click the check box. A new tab opens.



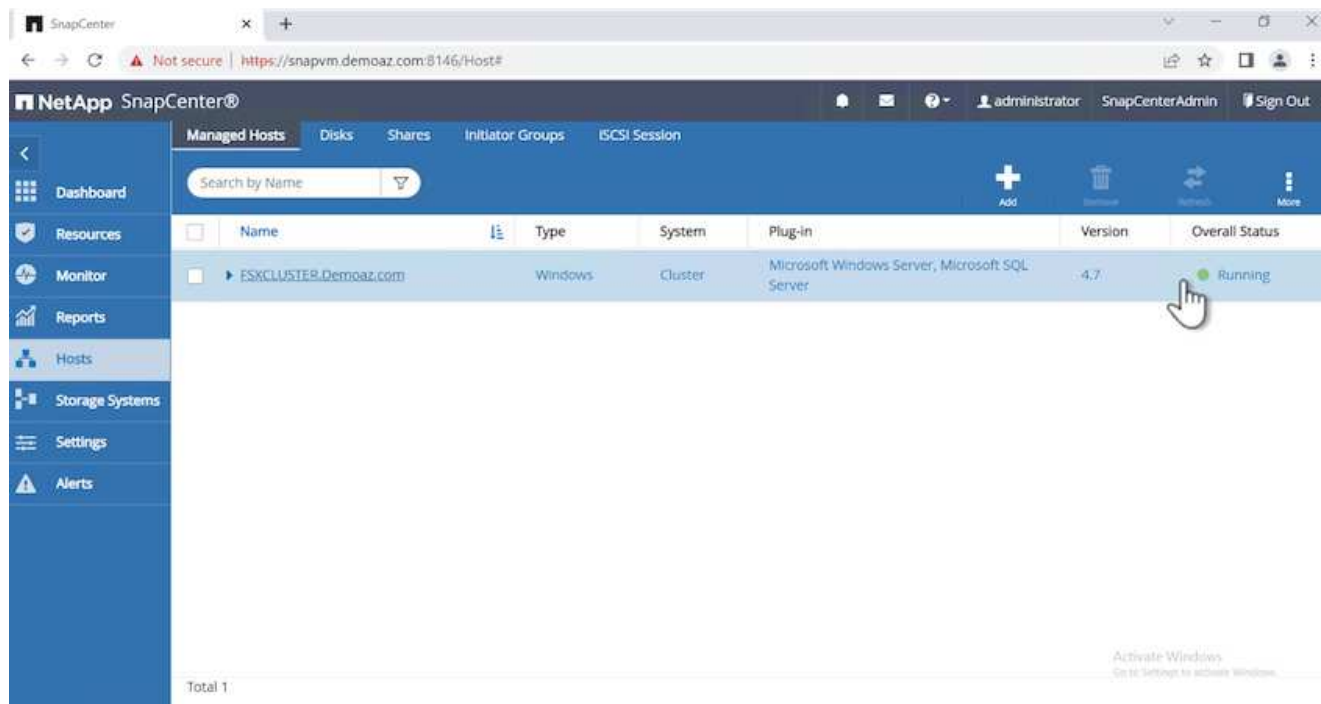
2. Click the **configure log directory** link.



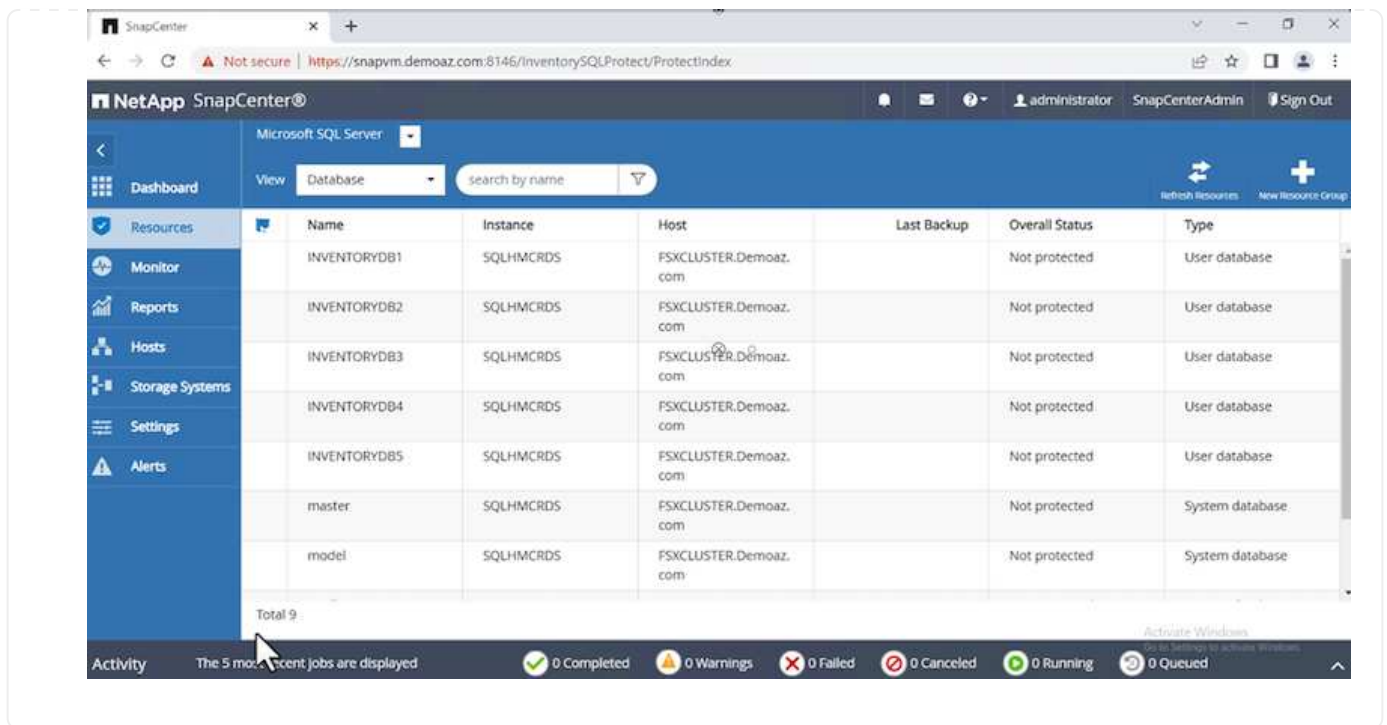
3. Select the drive for the host log directory and the FCI instance log directory. Click **Save**. Repeat the same process for the second node in the cluster. Close the window.



The host is now in a running state.



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



Configure a backup policy

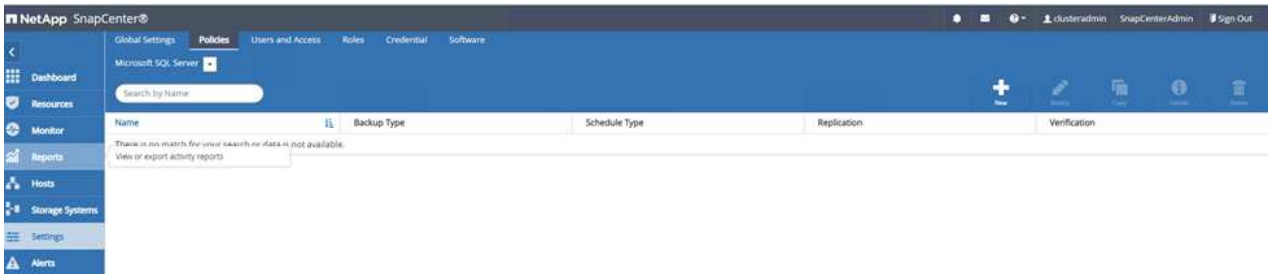
A backup policy is a set of rules that govern how to manage, schedule, and retain backup. It helps with the backup type and frequency based on your company's SLA.

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

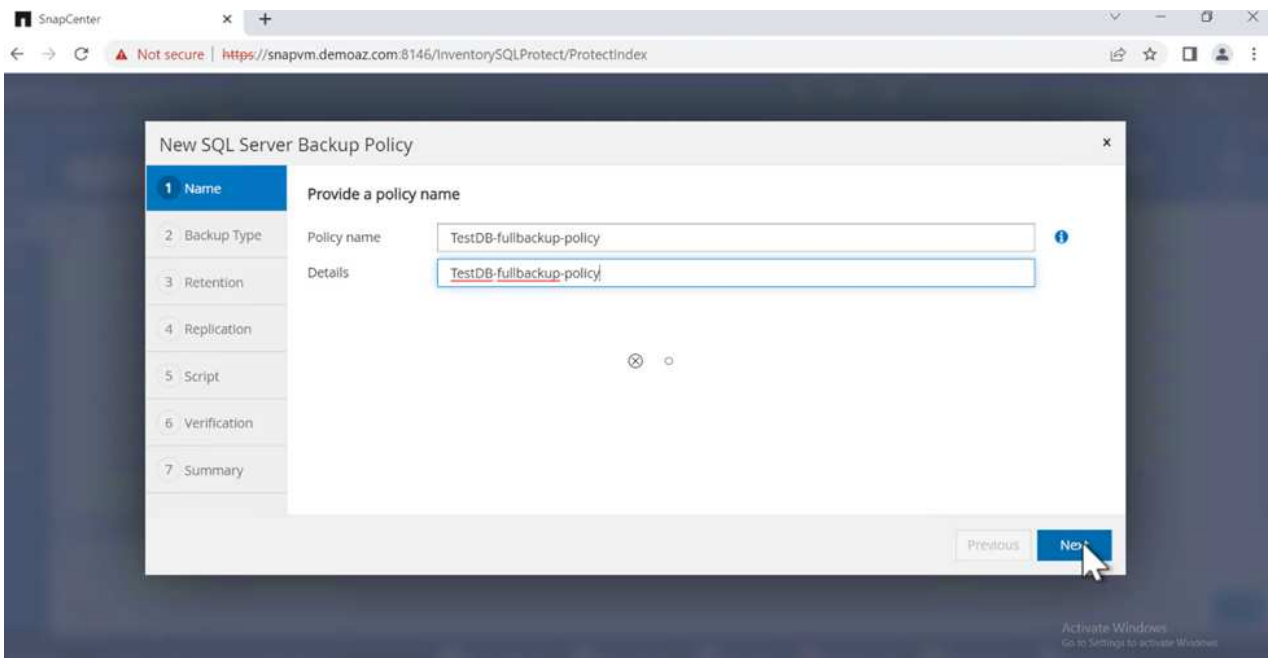
Configure back-up operation for an FCI database

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

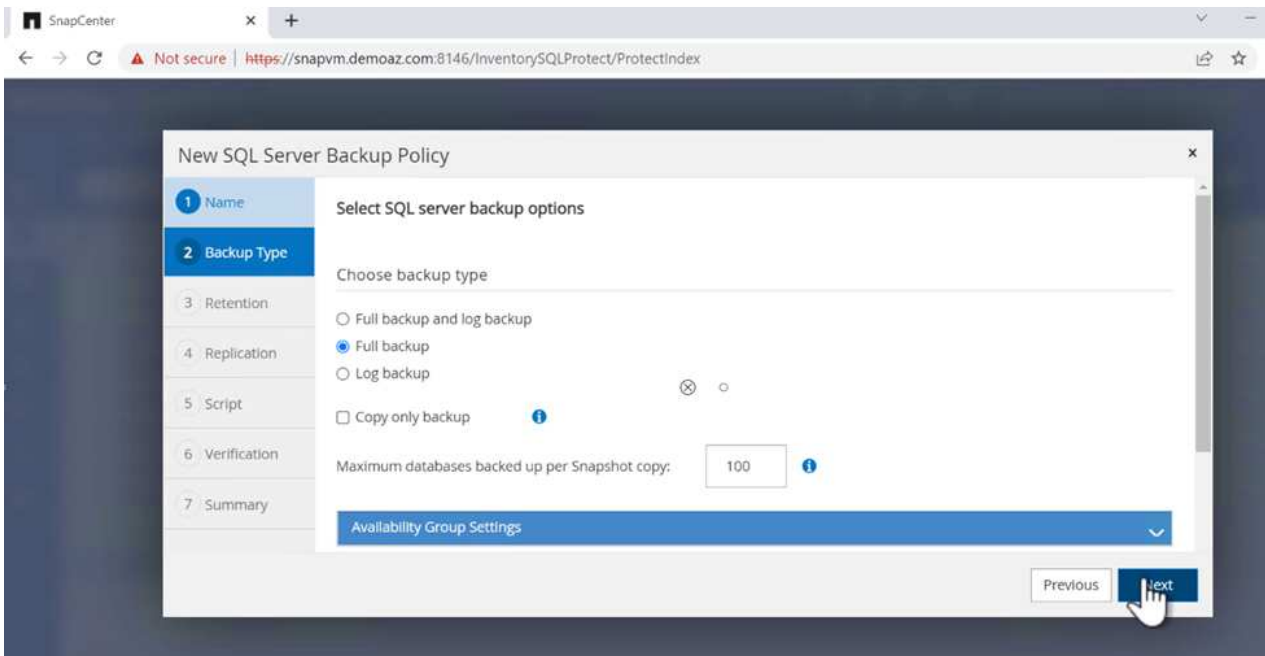
1. Go to **Settings** and select **Policies** on the top left. Then click **New**.



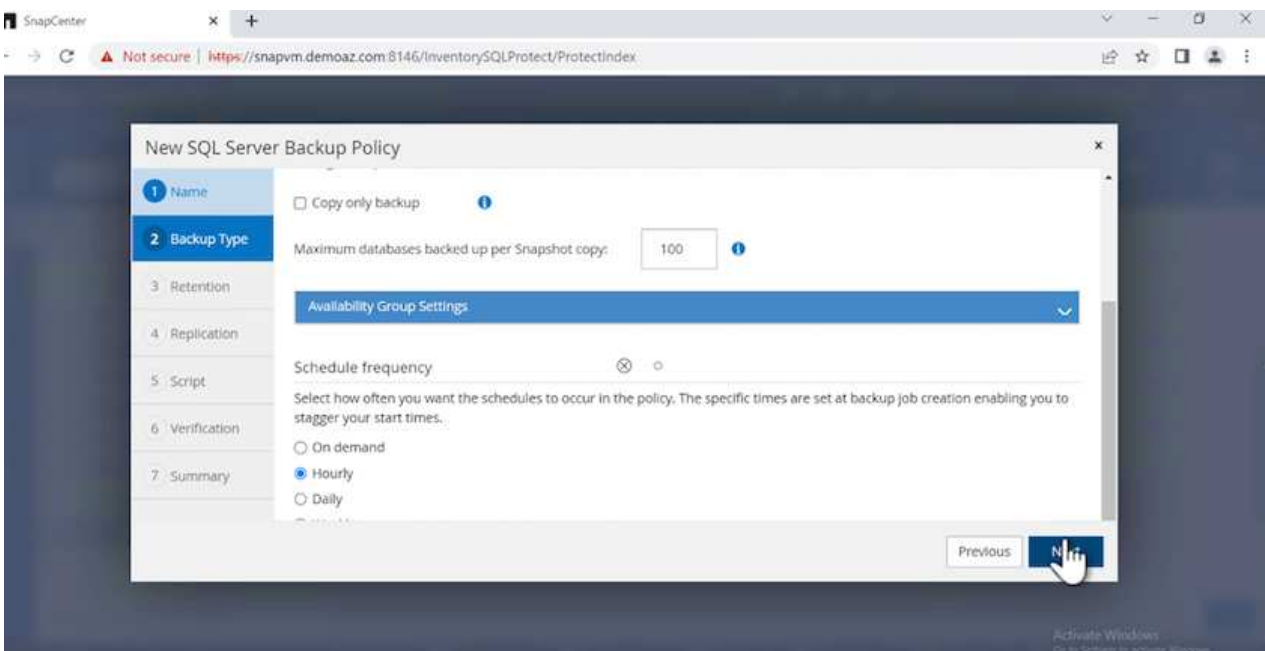
2. Enter the policy name and a description. Click **Next**.



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.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

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

☒ Keep log backups applicable to last

7

full backups

☐ Keep log backups applicable to last

14

days

Full backup retention settings ⓘ

Weekly

☒ Total Snapshot copies to keep

7

☐ Keep Snapshot copies for

14

days

Previous

Next

6. Configure the replication options.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☐ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Choose

Error retry count

3

Previous

Next

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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Script timeout

Previous

Next

8. Run verification based on the backup schedule.

New SQL Server Backup Policy

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

Select the options to run backup verification

Run verifications for the following backup schedules

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

☒ Weekly

Database consistency checks options

☒ Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)

☒ Suppress all information message (NO_INFOMSGS)

☐ Display all reported error messages per object (ALL_ERRORMSG)

☐ Do not check non-clustered indexes (NOINDEX)

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

Verification script settings

Script timeout: 60 secs

Prescript full path:

Prescript arguments: Choose optional arguments...

Postscript full path:

Postscript arguments: Choose optional arguments...

Previous
Next

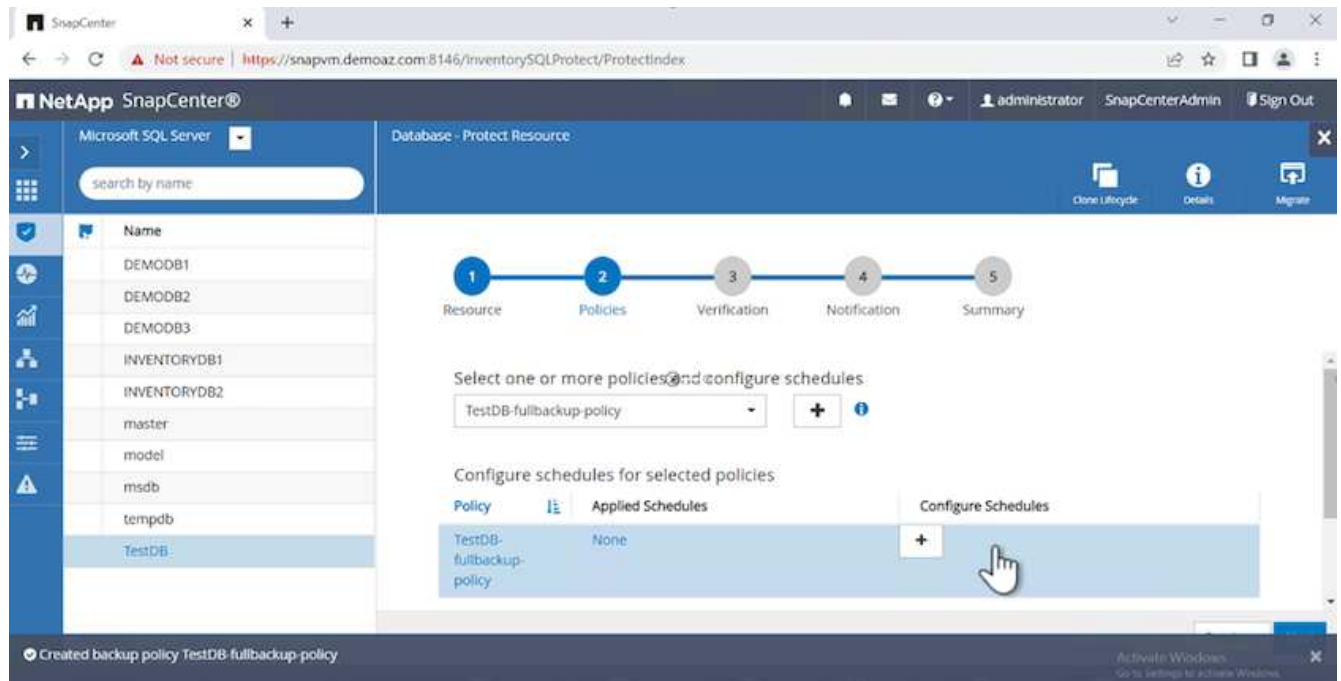
9. The **Summary** page provides details of the backup policy. Any errors can be corrected here.

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

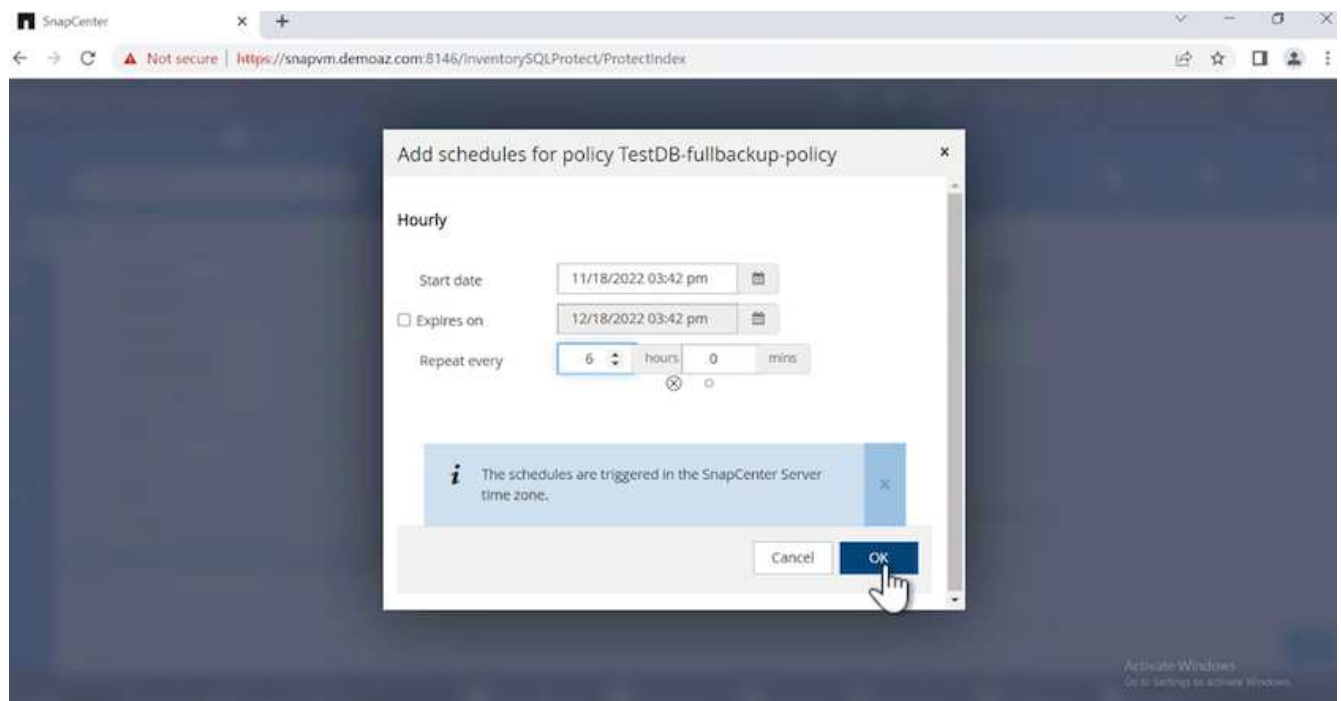
Previous
Finish

Configure and protect MSSQL Server database

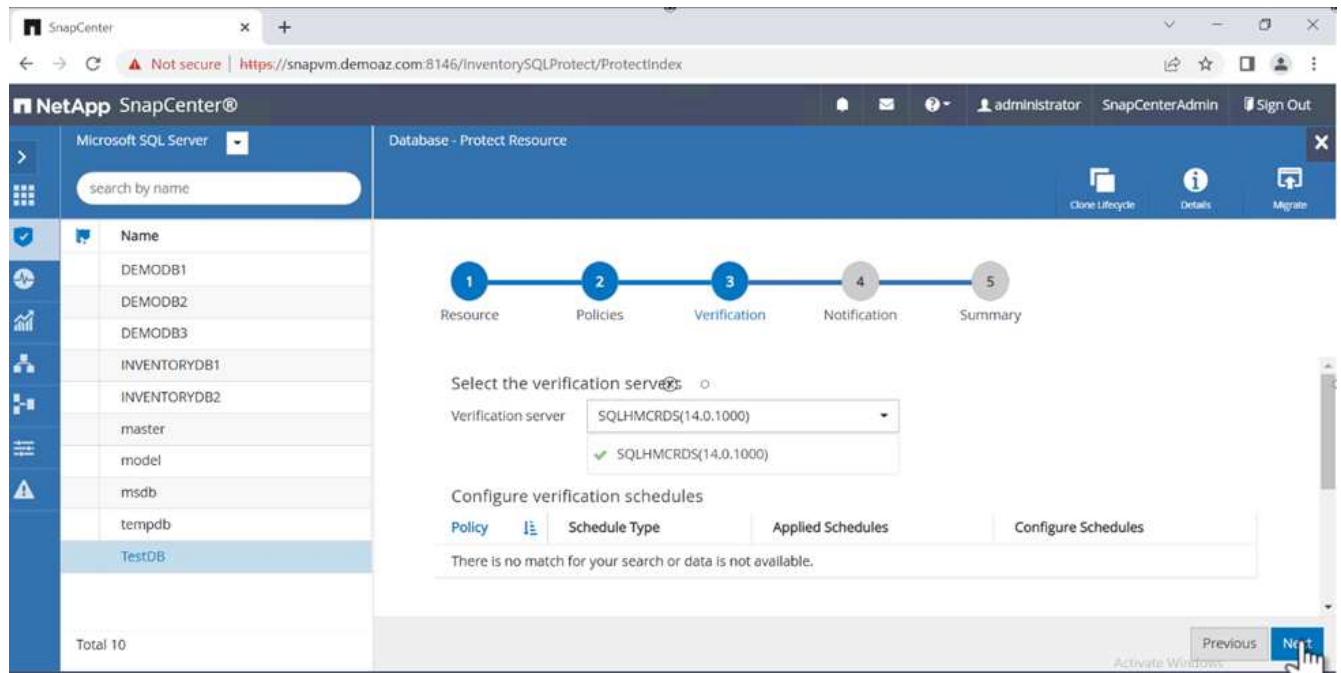
1. Set up the starting date and expiration date of the backup policy.



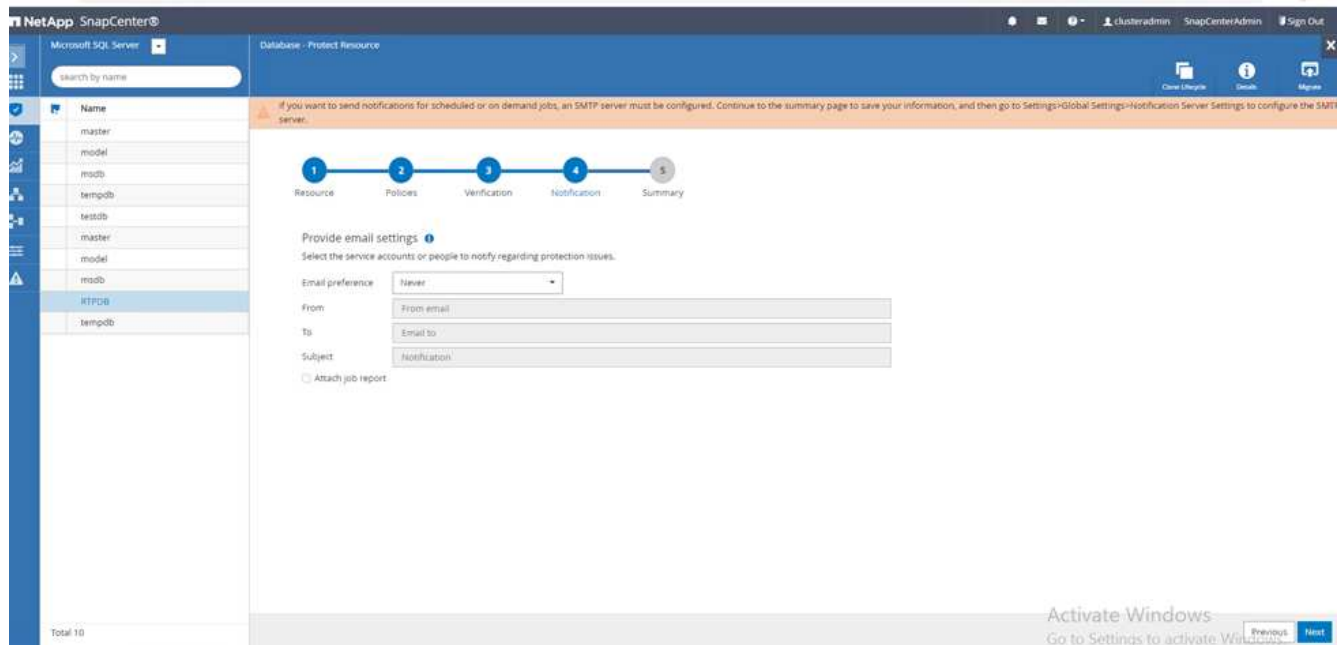
2. Define the schedule for the backup. To do that, click (+) to configure a schedule. Enter the **Start date** and **Expires on** date. Set the time based on the company's SLA.



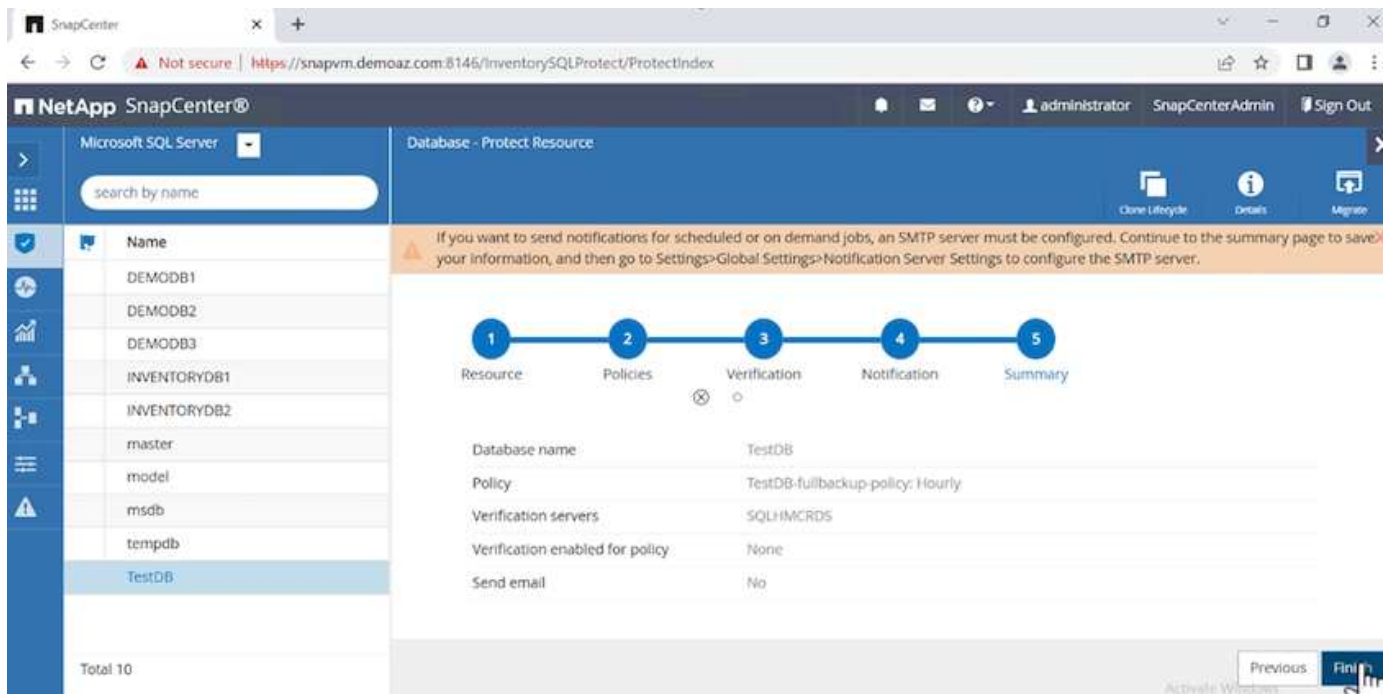
3. Configure the verification server. From the drop- down menu, select the server.



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



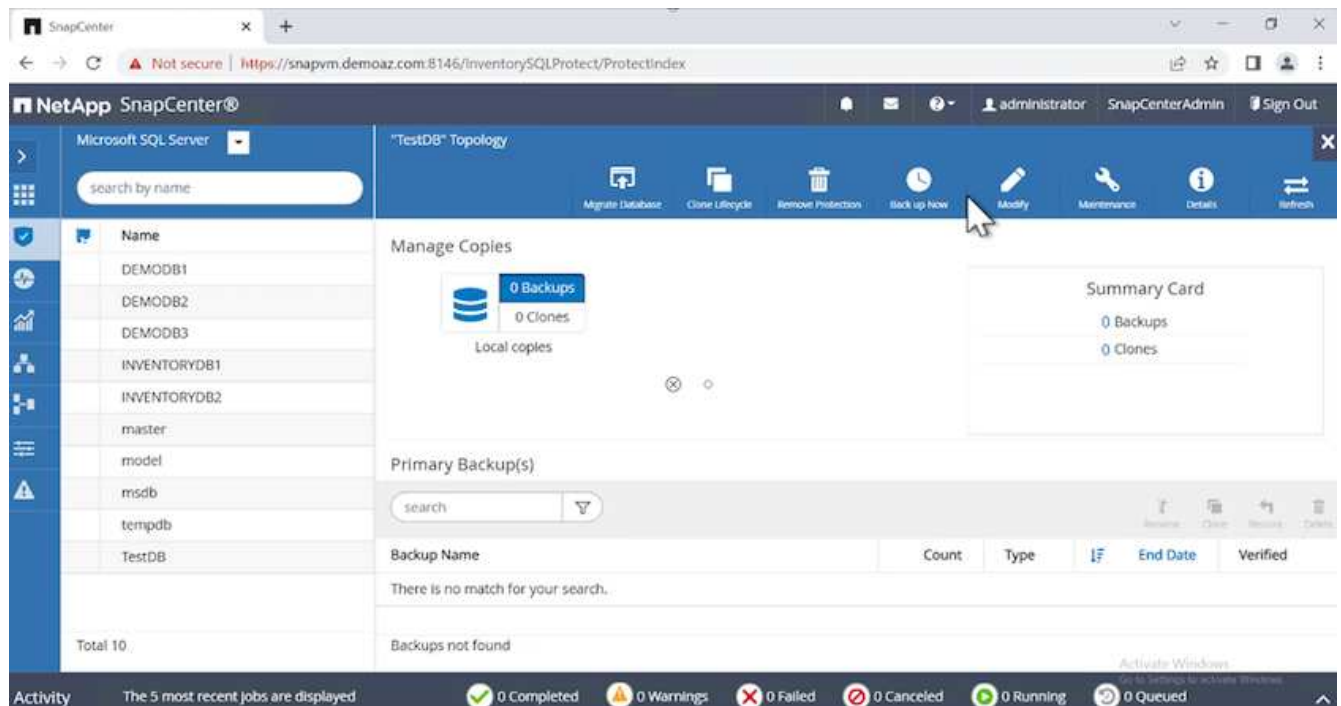
The summary of the backup policy for SQL Server database is now configured.



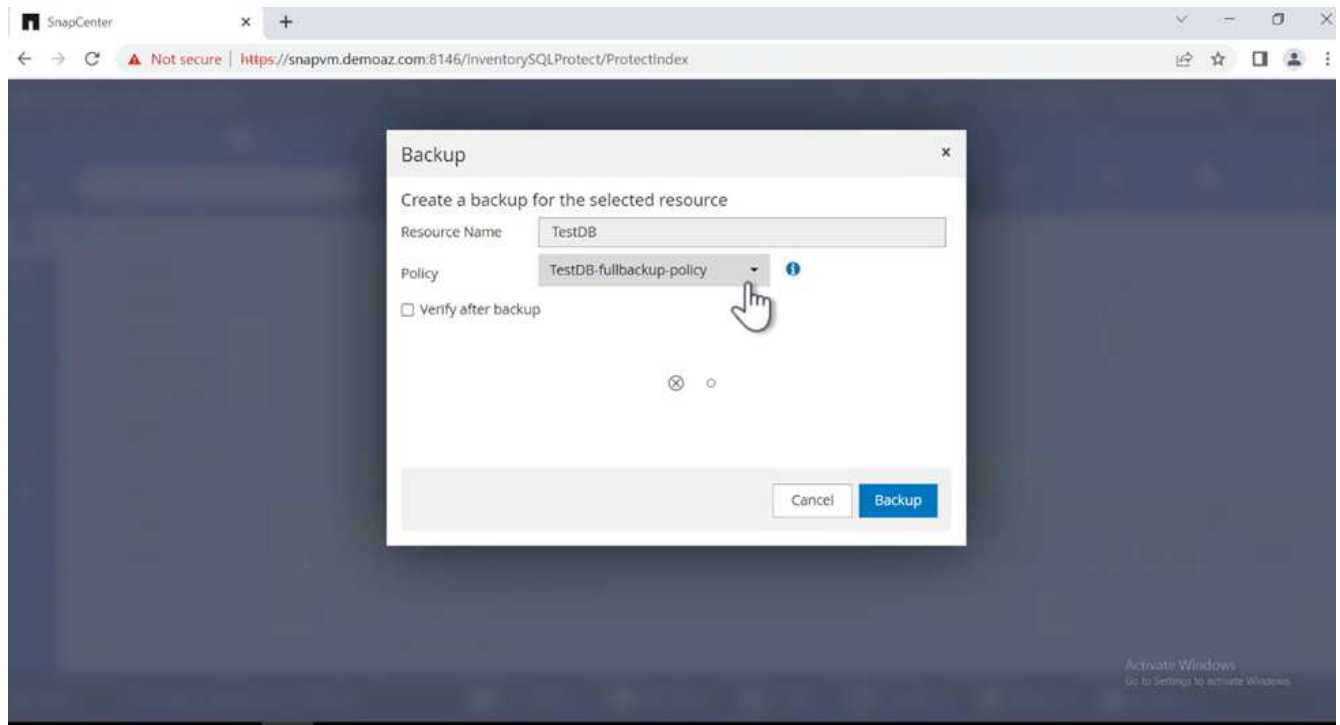
SnapCenter backup operations

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

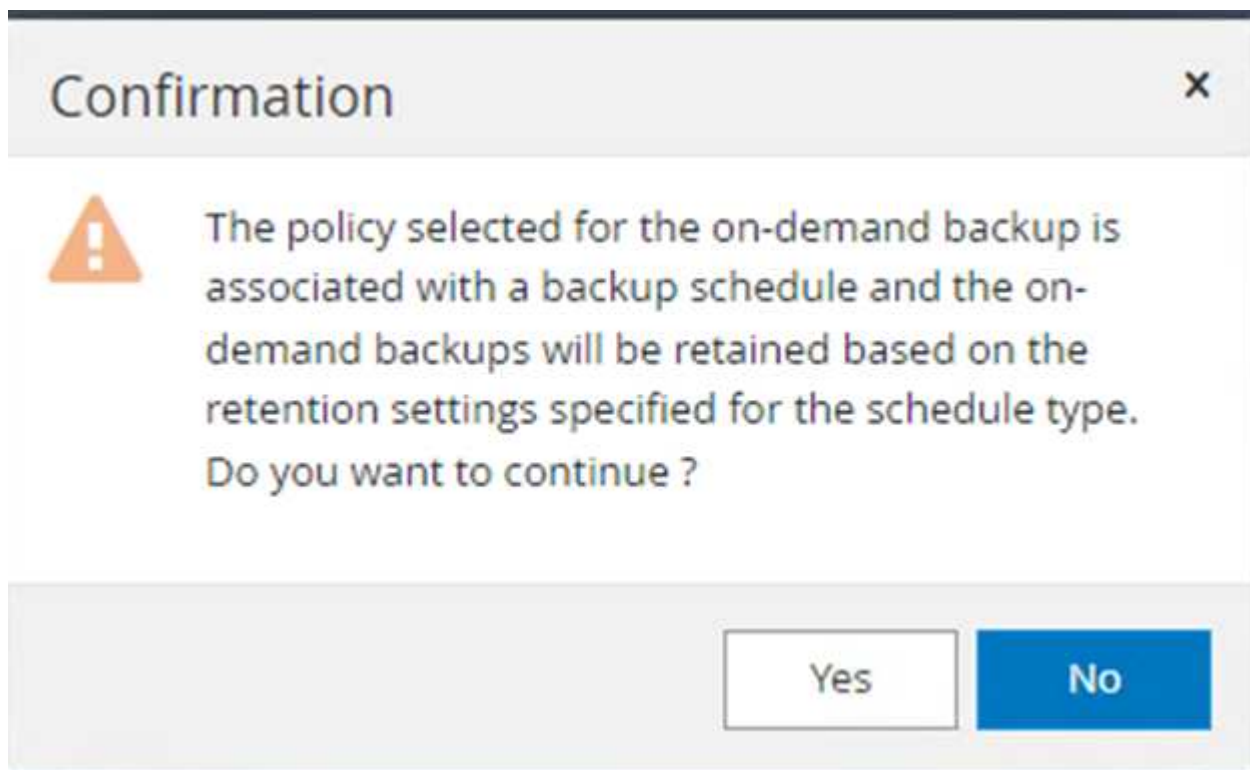
1. From the **Resource** view, select the resource and select **Backup now**.



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

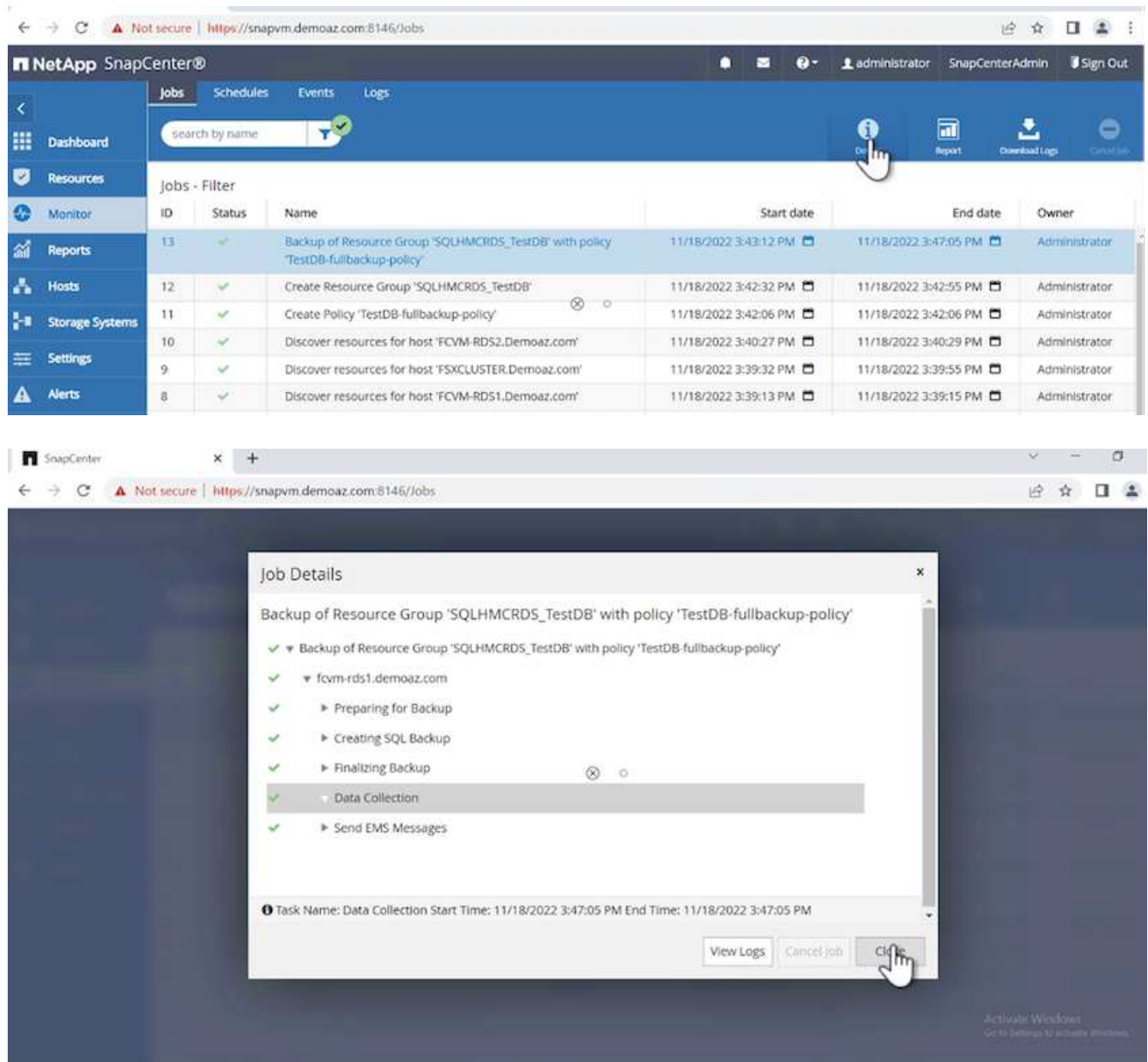


3. A confirmation screen is displayed. Click **Yes** to confirm.



Monitor backup job

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

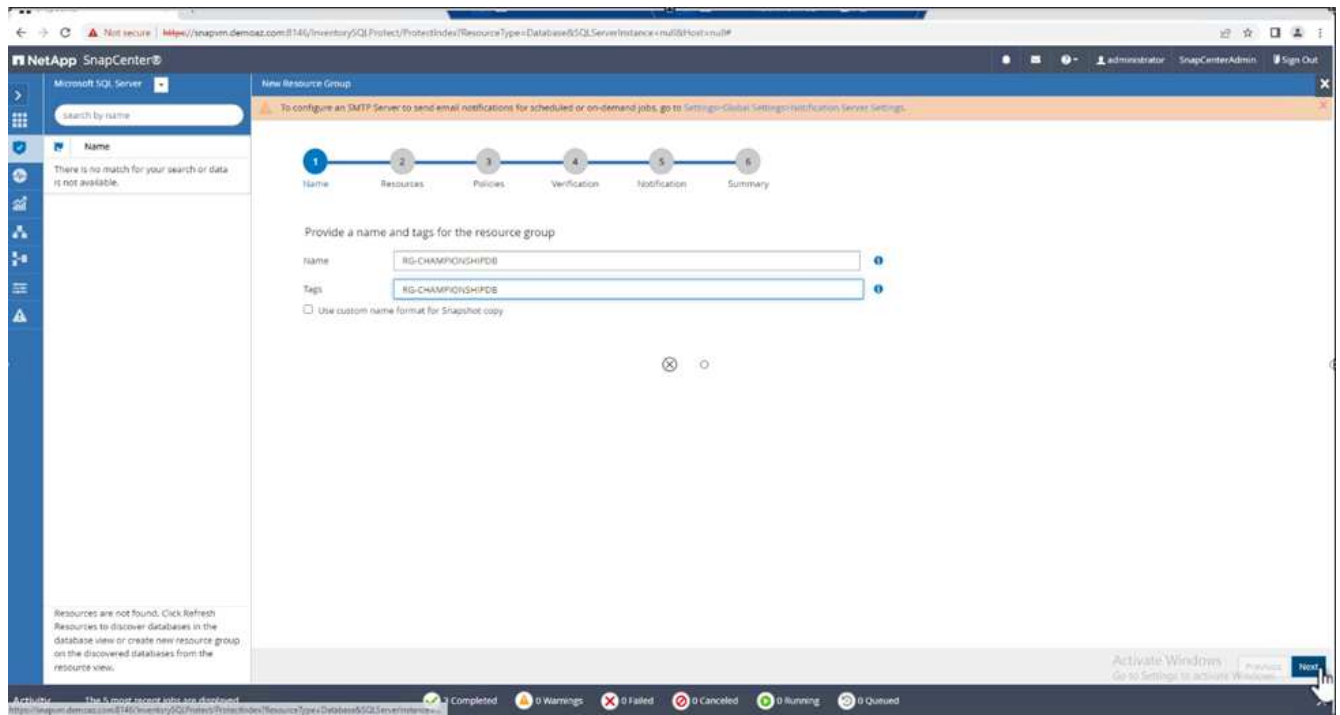


When the backup is completed, a new entry is shown in the Topology view.

Backup operation for multiple databases

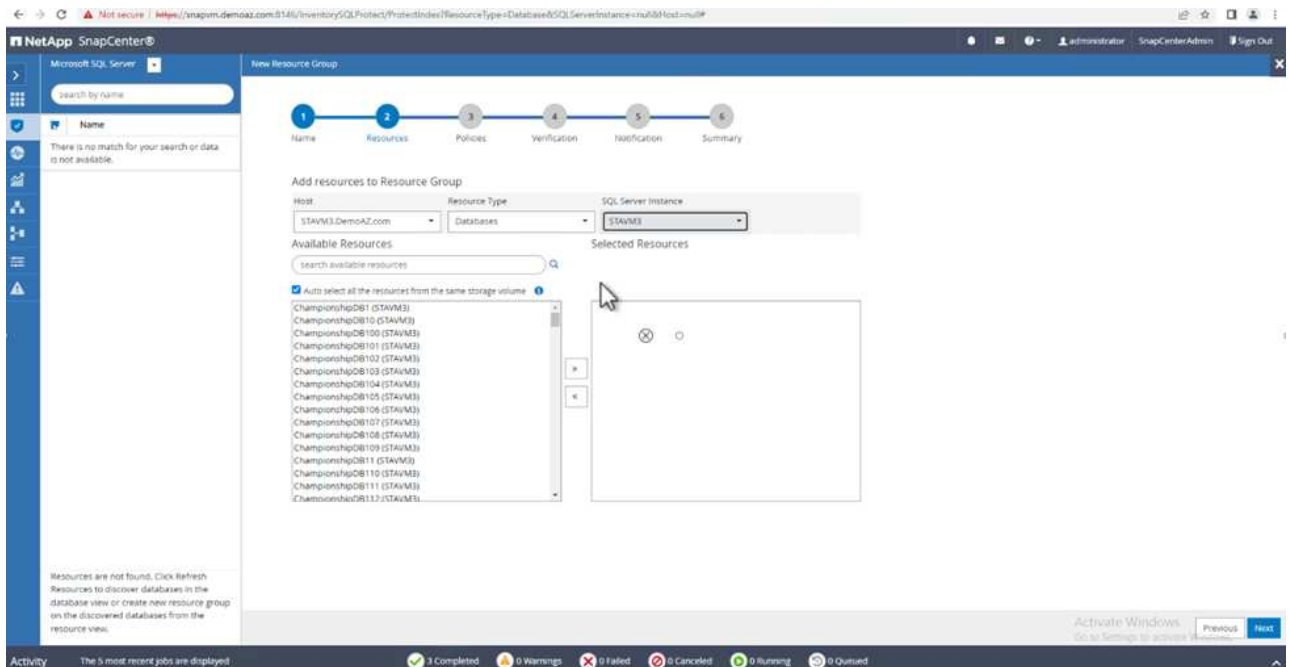
To configure a backup policy for multiple SQL Server databases, create resource group policies by completing the following steps:

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

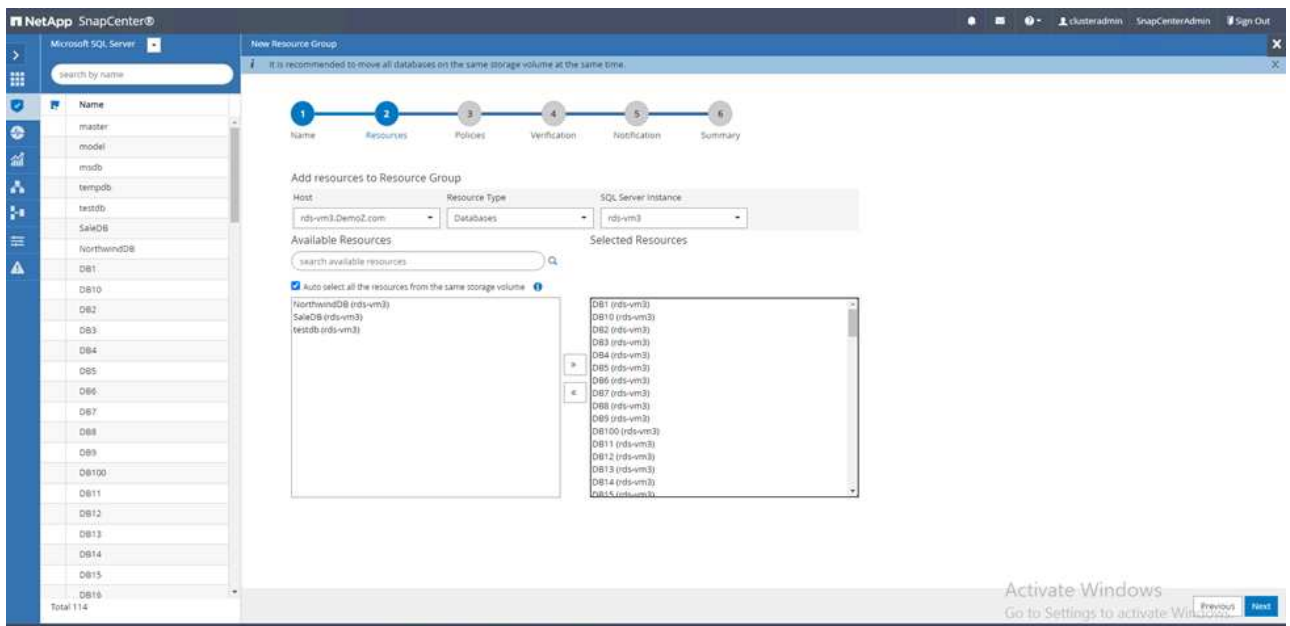


4. Add resources to the resource group:

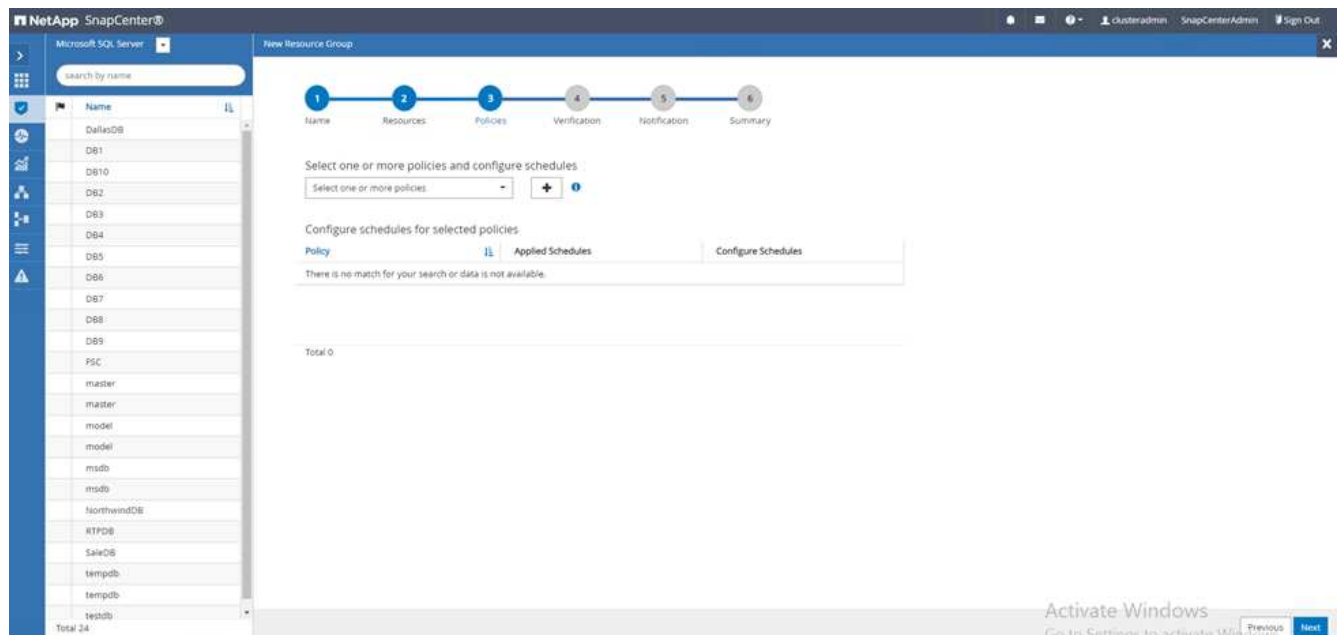
- **Host.** Select the server from the drop-down menu hosting the database.
- **Resource type.** From the drop-down menu, select **Database**.
- **SQL Server instance.** Select the server.



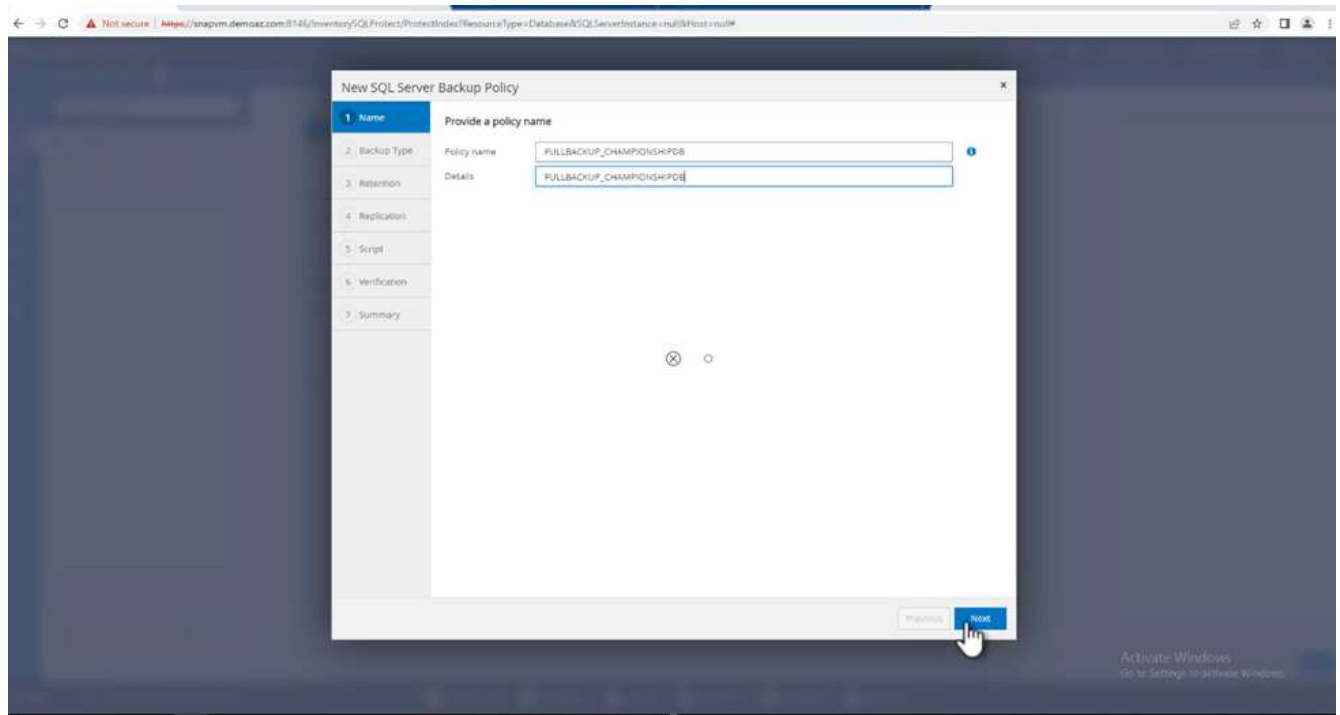
The **option** Auto Selects All the Resources from the Same Storage Volume* is selected by default. Clear the option and select only the databases you need to add to the resource group, Click the arrow to add and click **Next**.



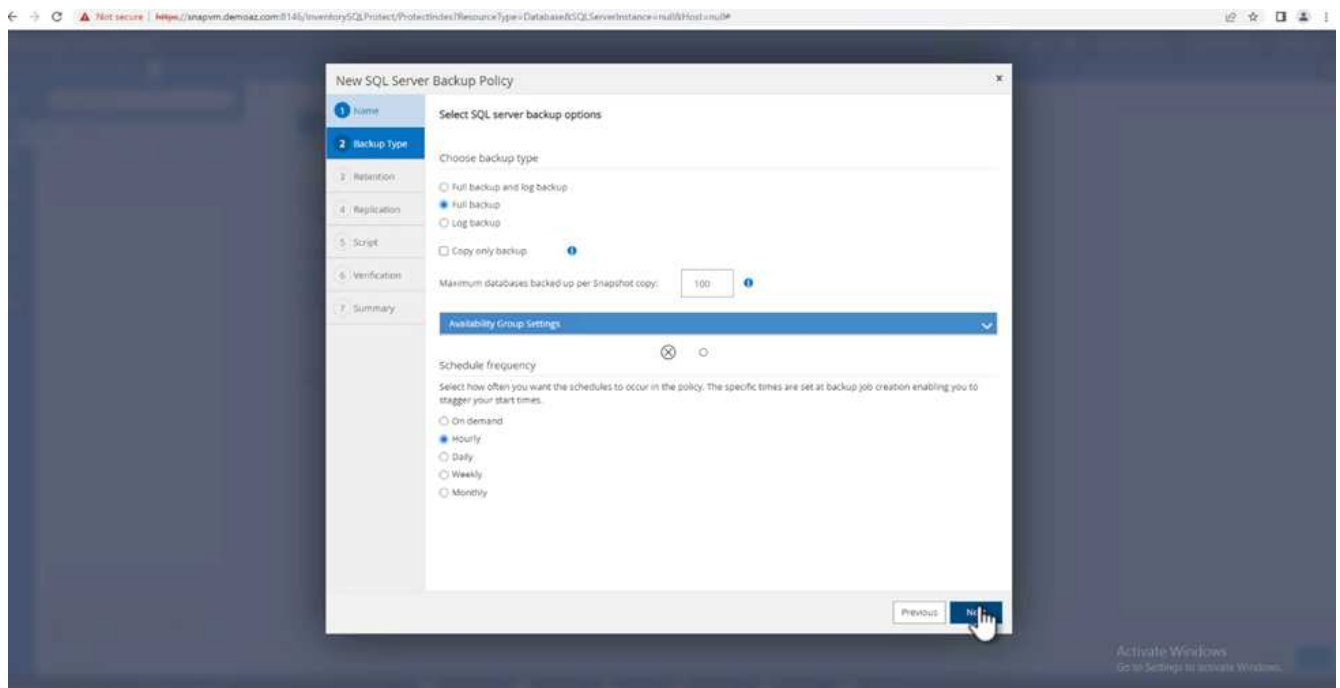
5. On the policies, click (+).



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.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

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

☒ Keep log backups applicable to last

7

full backups

☐ Keep log backups applicable to last

14

days

Full backup retention settings ⓘ

Weekly

☒ Total Snapshot copies to keep

7

☐ Keep Snapshot copies for

14

days

Previous

Next

9. Configure the replication options.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☐ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Choose

Error retry count

3

Previous

Next

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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Choose optional arguments...

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Choose optional arguments...

Script timeout

60

secs

Previous

Next

11. Confirm the verification for the following backup schedules.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run verifications for the following backup schedules

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

☐ Hourly

Database consistency checks options

☒ Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)
☒ Suppress all information message (NO_INFOMSGS)
☐ Display all reported error messages per object (ALL_ERRORMSG5)
☐ Do not check non-clustered indexes (NOINDEX)
☐ Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)

Verification script settings

Script timeout

60secs

Prescript full path

<SCRIPTS_PATH>

Prescript arguments

Choose optional arguments...

Postscript full path

<SCRIPTS_PATH>

Postscript arguments

Choose optional arguments...

Previous

Next

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

New SQL Server Backup Policy

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

Summary

Policy name	FULLBACKUP_CHAMPIONSHIPDB
Details	FULLBACKUP_CHAMPIONSHIPDB
Backup type	Full backup
Availability group settings	Backup only on preferred backup replica
Schedule Type	Hourly
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:
Backup postscript settings	undefined <input checked="" type="radio"/> <input type="radio"/> Postscript arguments:
Verification for backup schedule type	Hourly
Verification prescript settings	undefined Prescript arguments:
Verification postscript settings	undefined Postscript arguments:

Previous
Finish

Configure and protect multiple SQL Server databases

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

NetApp SnapCenter

Microsoft SQL Server

Search by name

Name

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

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

FULLBACKUP_CHAMPIONSHIPDB +

Configure schedules for selected policies

Policy	Applied Schedules	Configuration Schedules
FULLBACKUP_CHAMPIONSHIPDB	None	+ <input checked="" type="radio"/> <input type="radio"/>

Total 1

☐ Use Microsoft SQL Server scheduler

2. Set the time.

Add schedules for policy FULLBACKUP_CHAMPIONSHIPDB



Hourly

Start date

11/11/2022 05:30 pm



☐ Expires on

12/11/2022 05:27 pm



Repeat every

8



hours

0

mins



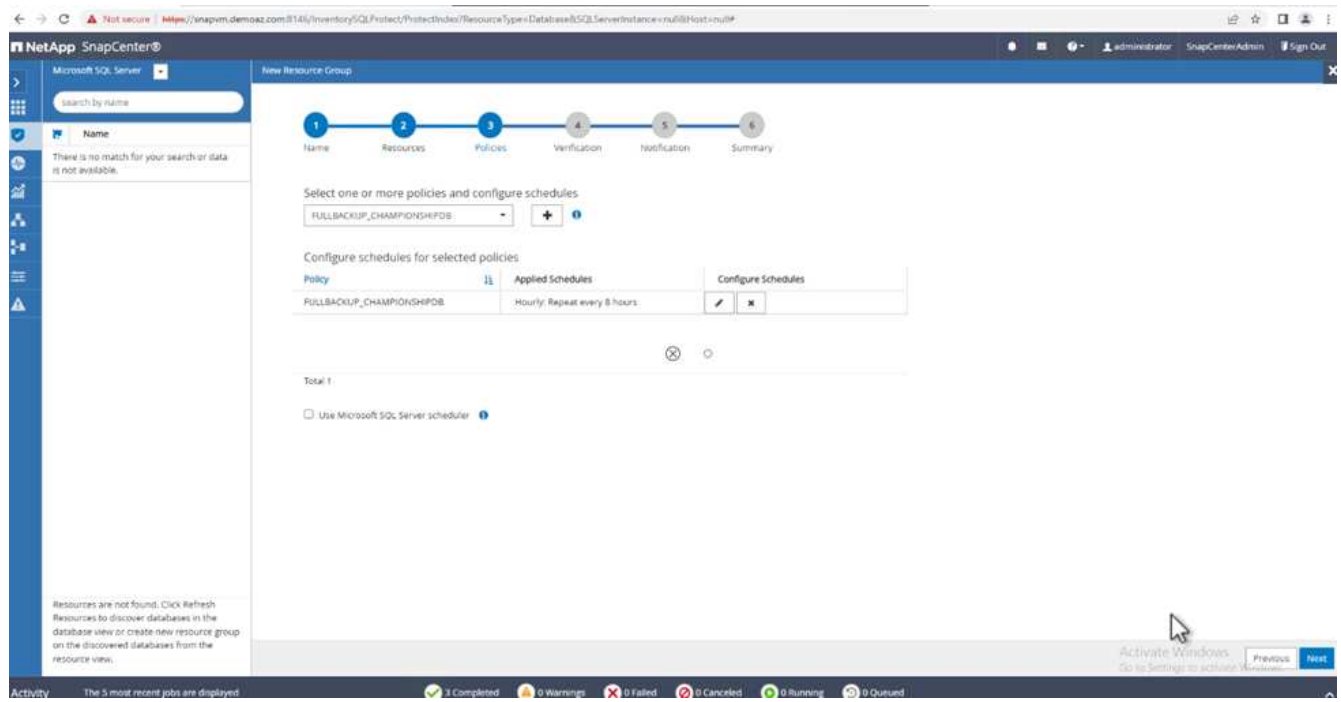
The schedules are triggered in the SnapCenter Server time zone.



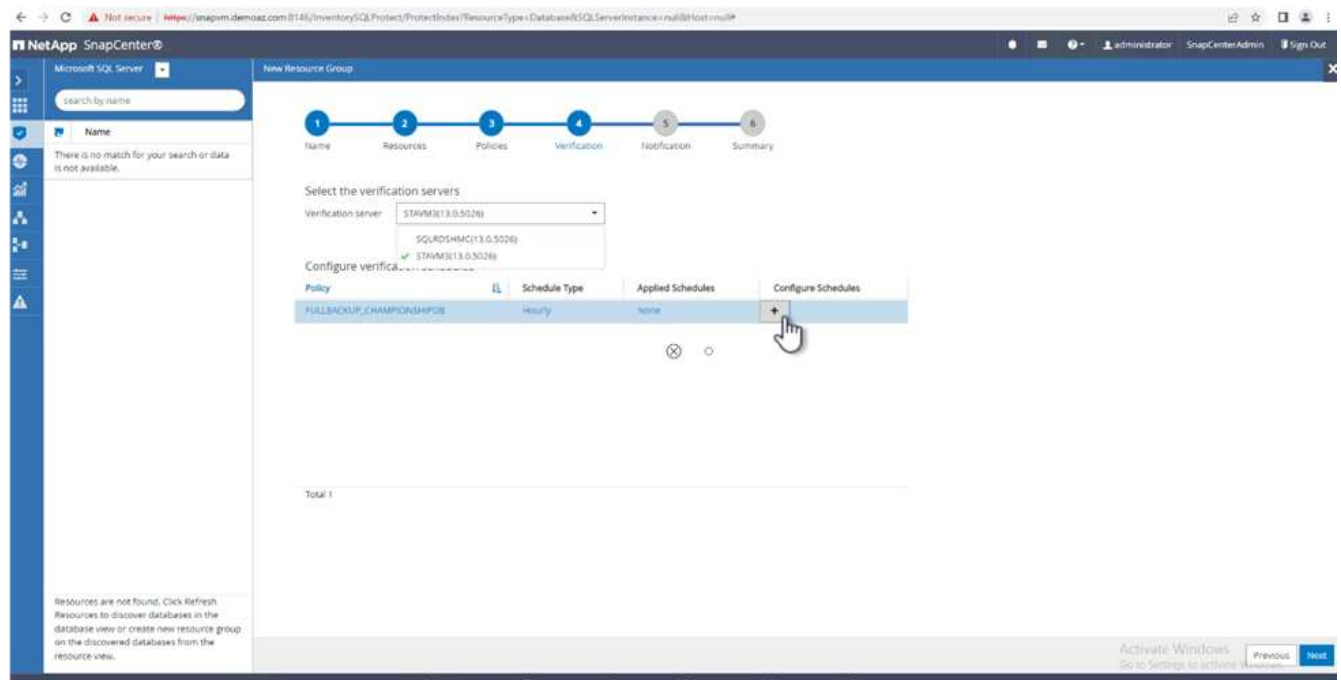
Cancel

OK

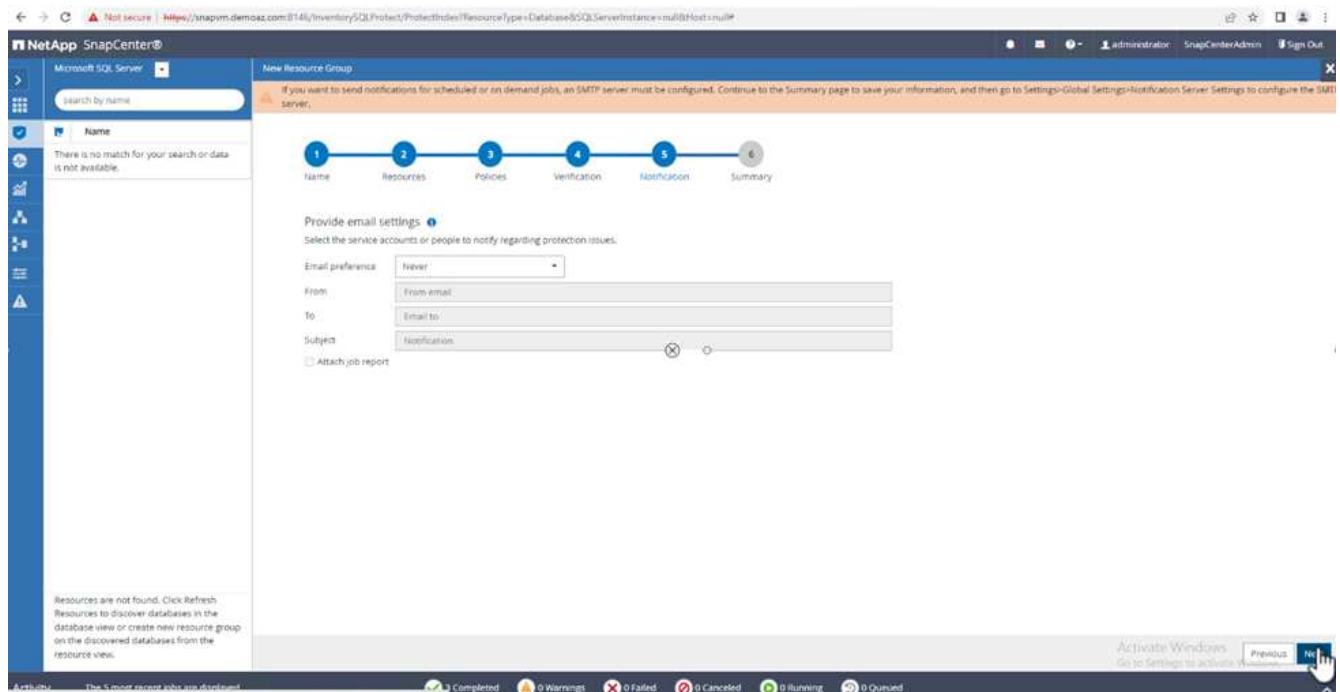




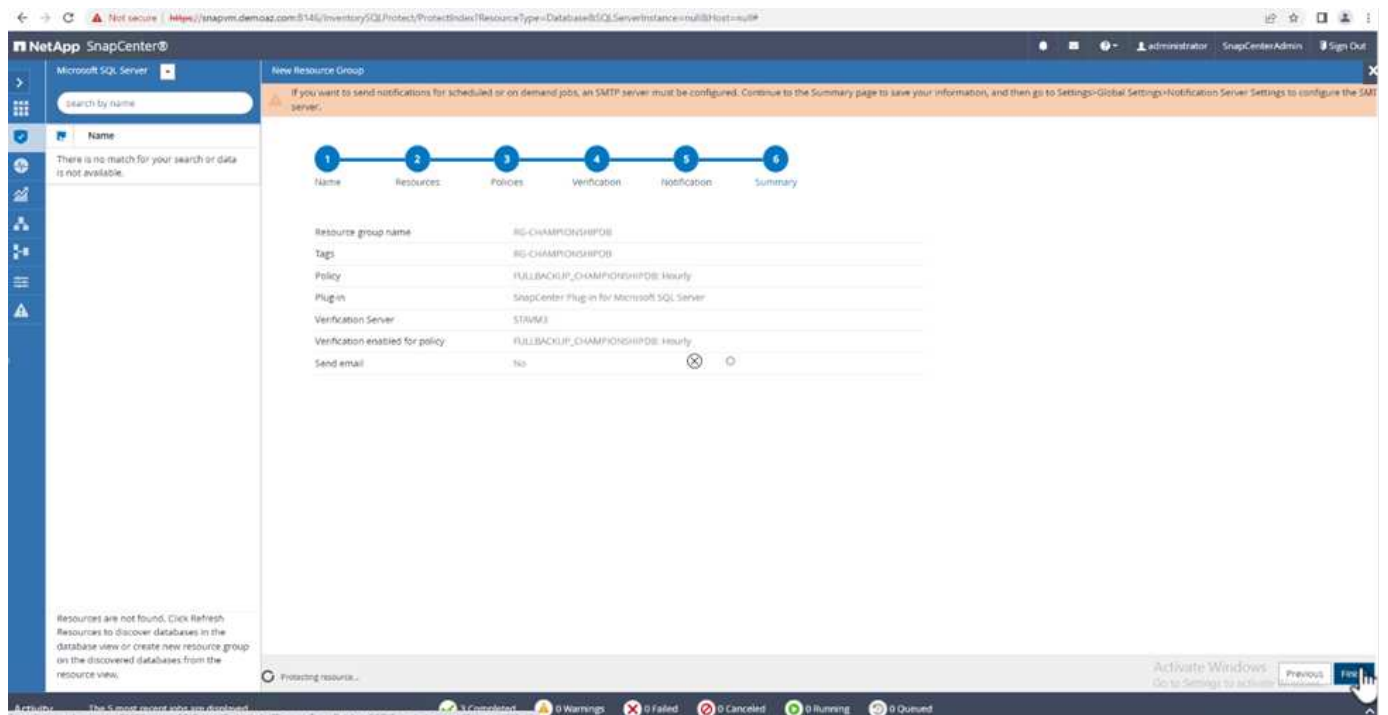
3. From the **Verification** tab, select the server, configure the schedule, and click **Next**.



4. Configure notifications to send an email.

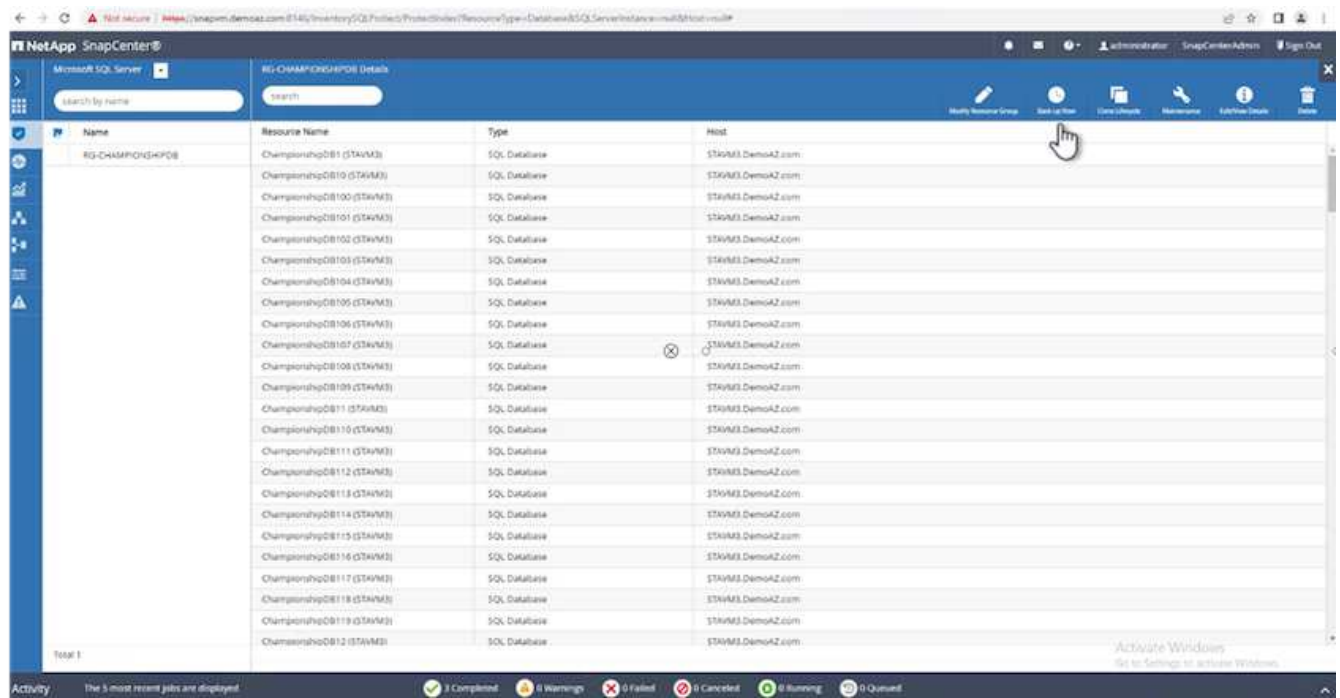


The policy is now configured for backing up multiple SQL Server databases.

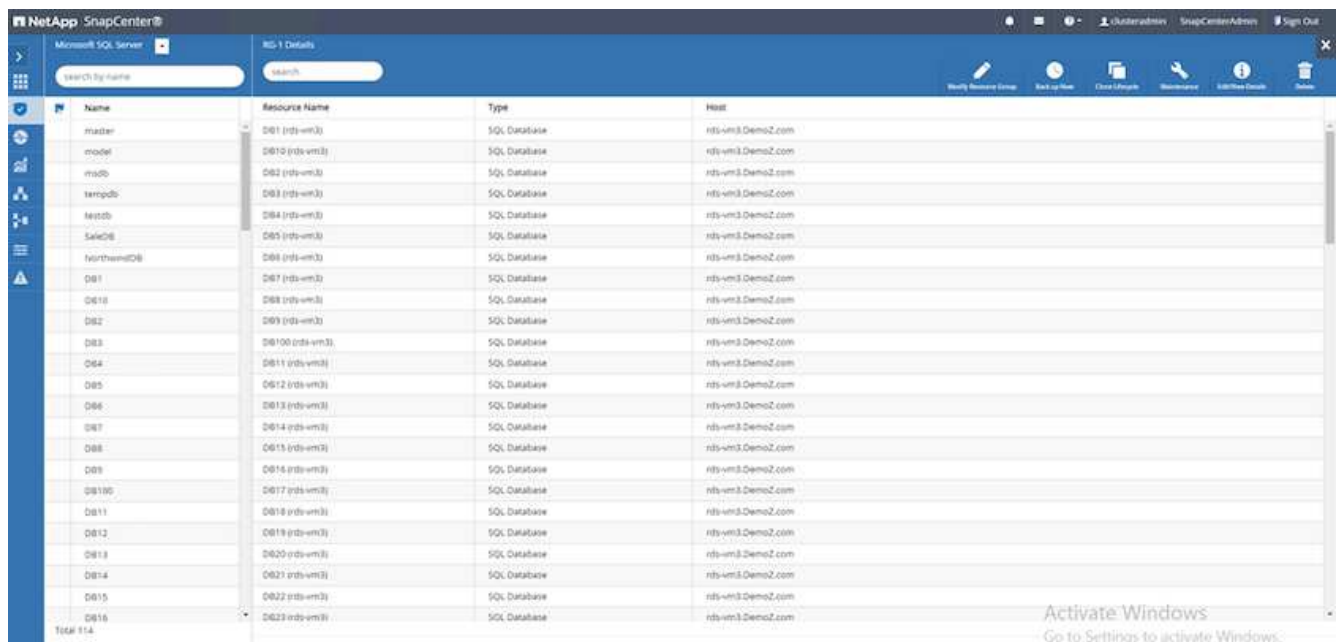


Trigger on-demand backup for multiple SQL Server databases

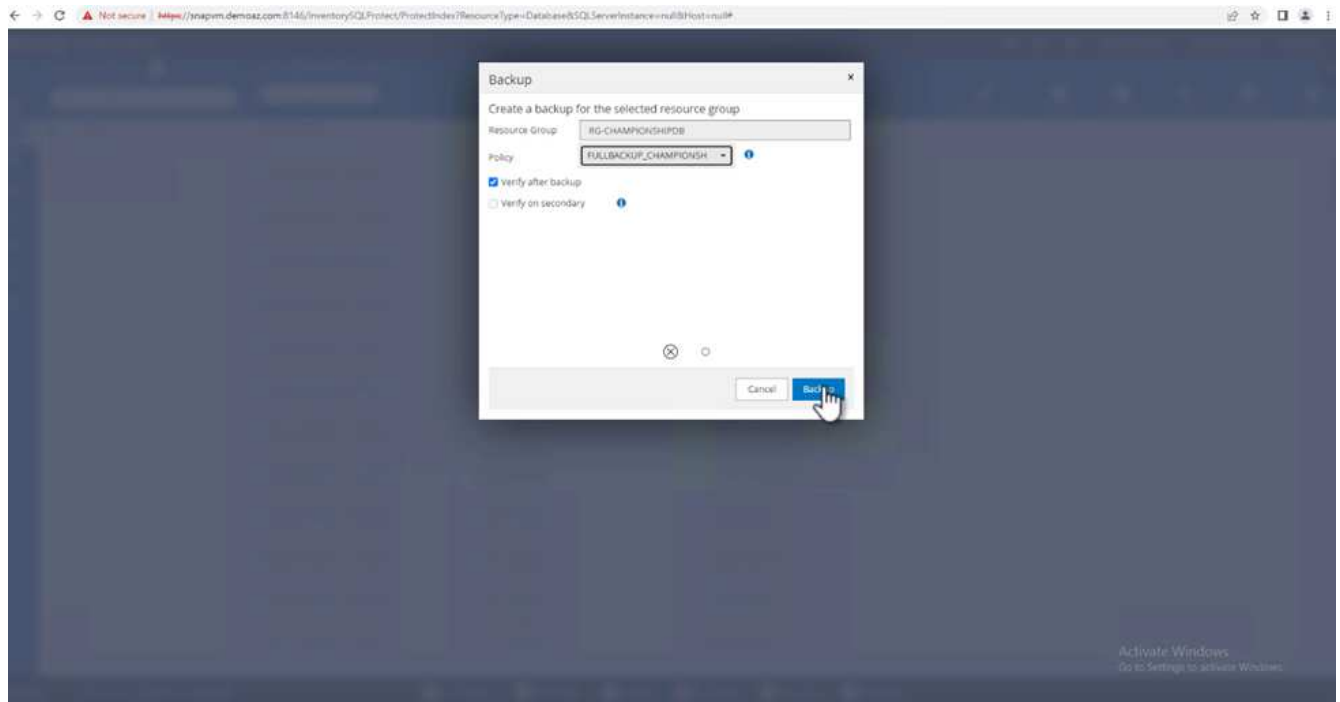
1. From the **Resource** tab, select view. From the drop-down menu, select **Resource Group**.



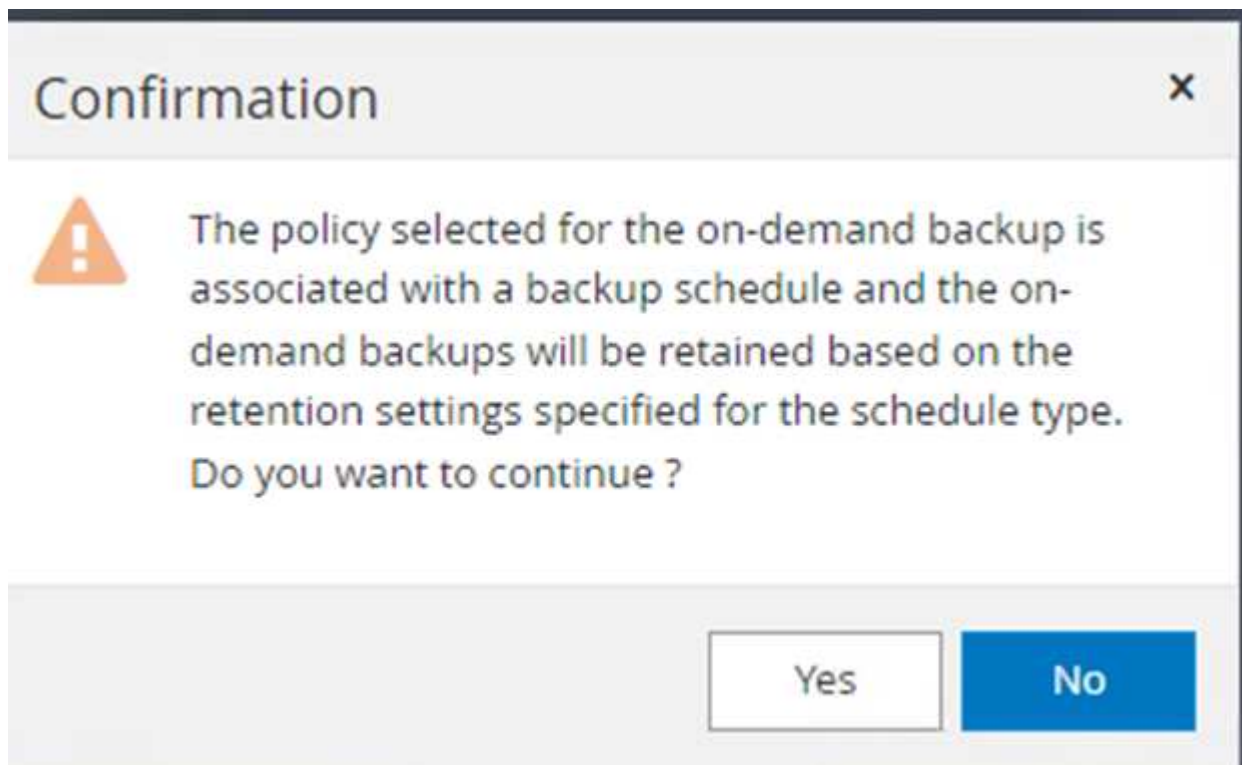
2. Select the resource group name.
3. Click **Backup now** in the upper right.



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



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

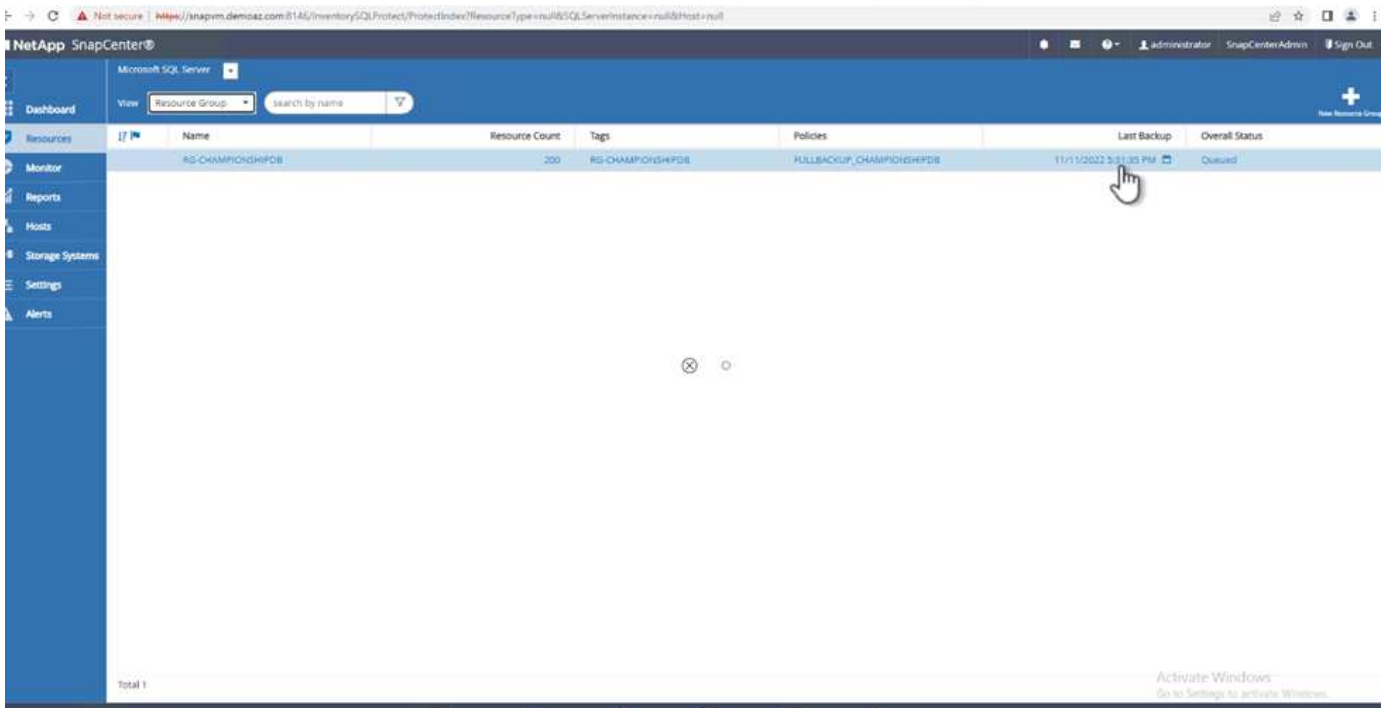


Monitor multiple-database backup jobs

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.

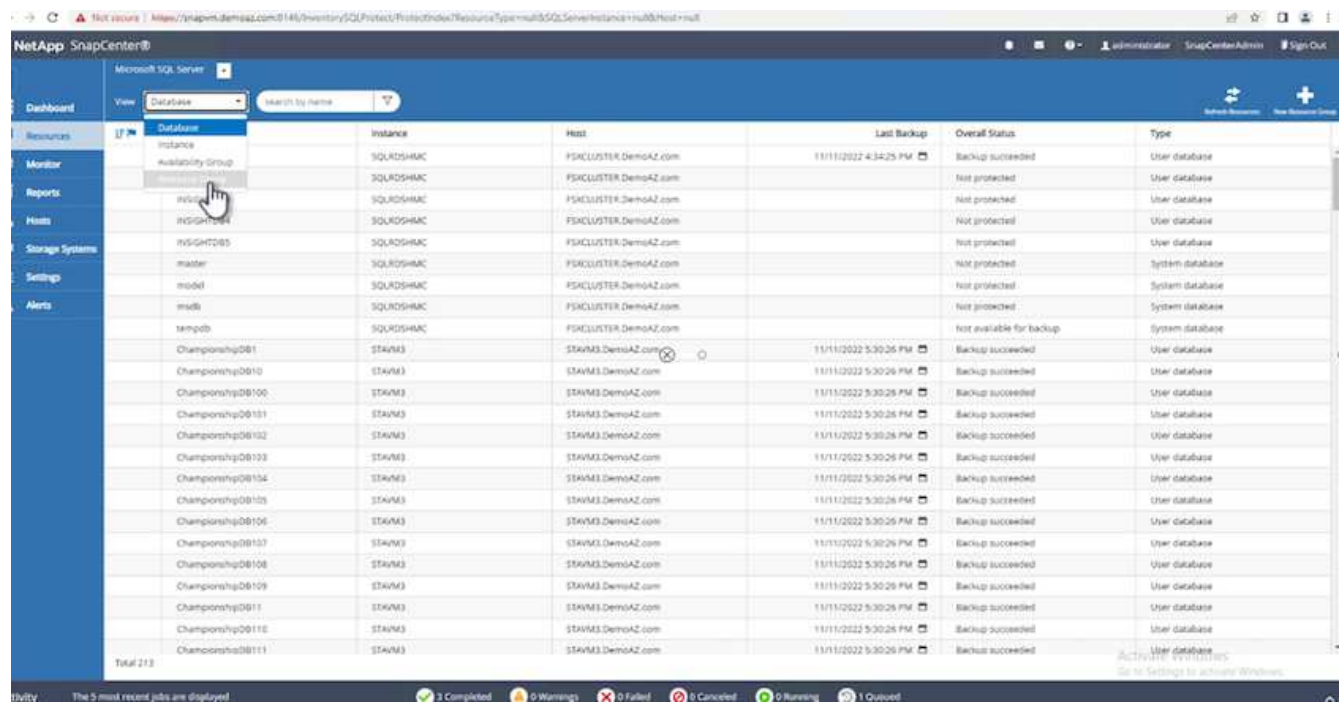


Transaction log backup for multiple database backup

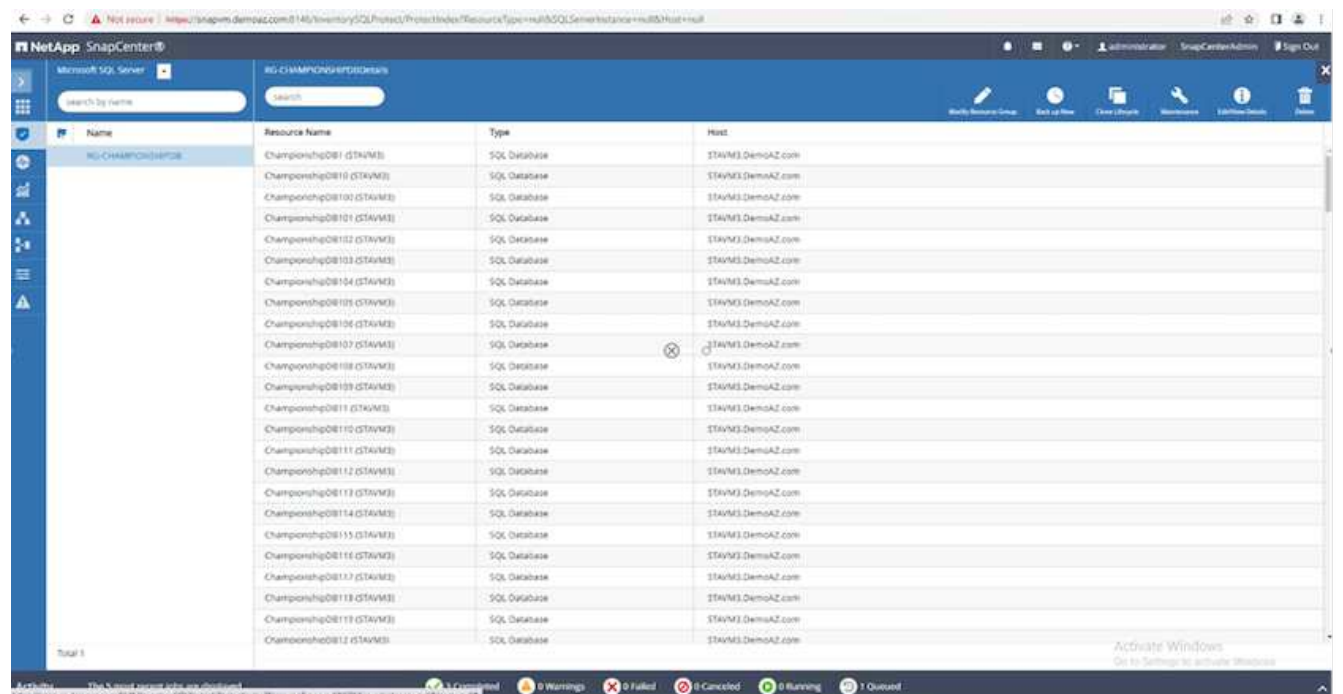
SnapCenter supports the full, bulked logged, and simple recovery models. The simple recovery mode does not support transactional log backup.

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

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

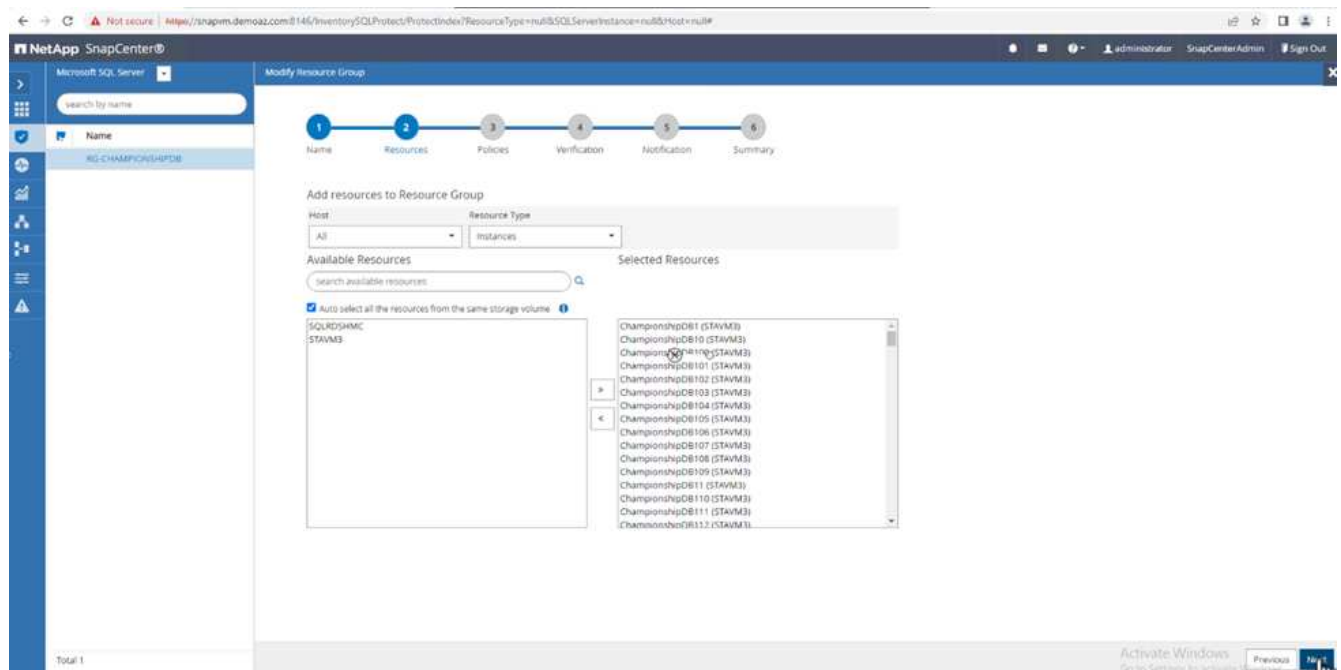


2. Select the resource group backup policy created.
3. Select **Modify Resource Group** in the upper right.

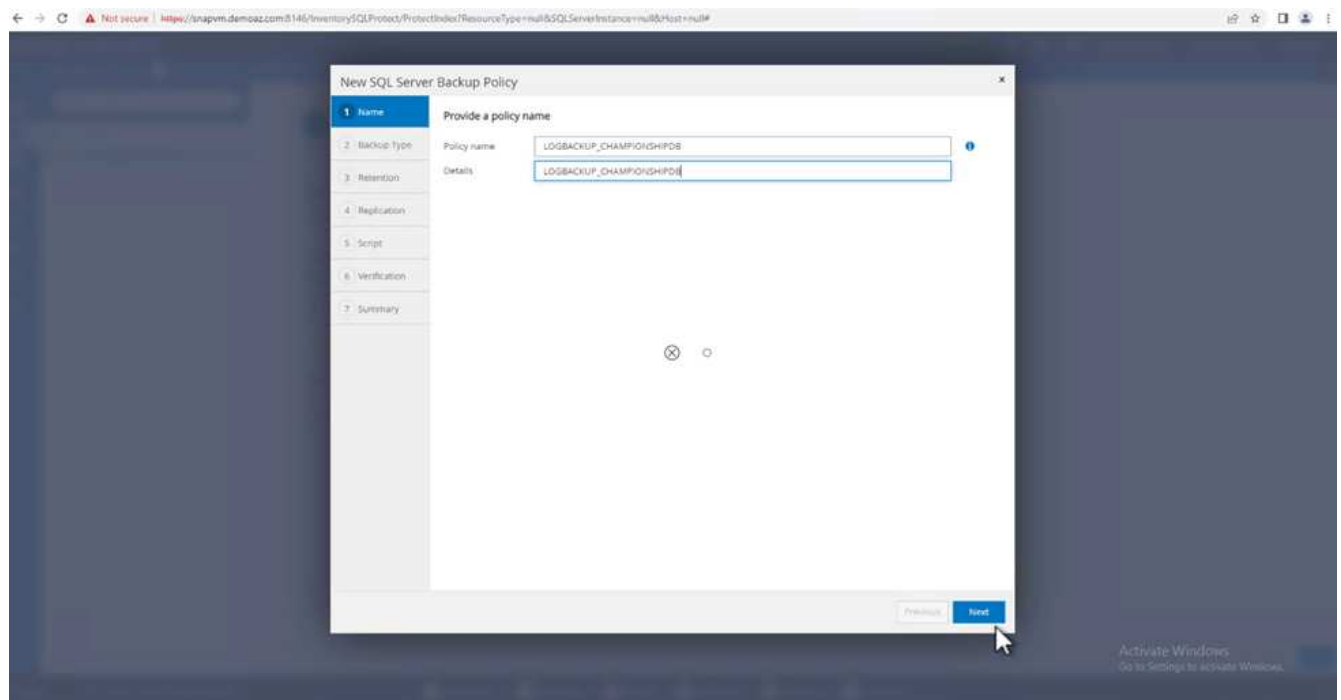


4. The **Name** section defaults to the backup policy name and tag. Click **Next**.

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



5. Enter the policy name.



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

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

☐ Full backup and log backup

☐ Full backup

☒ Log backup

☐ Copy only backup

Maximum databases backed up per Snapshot copy:

100

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 ✕

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

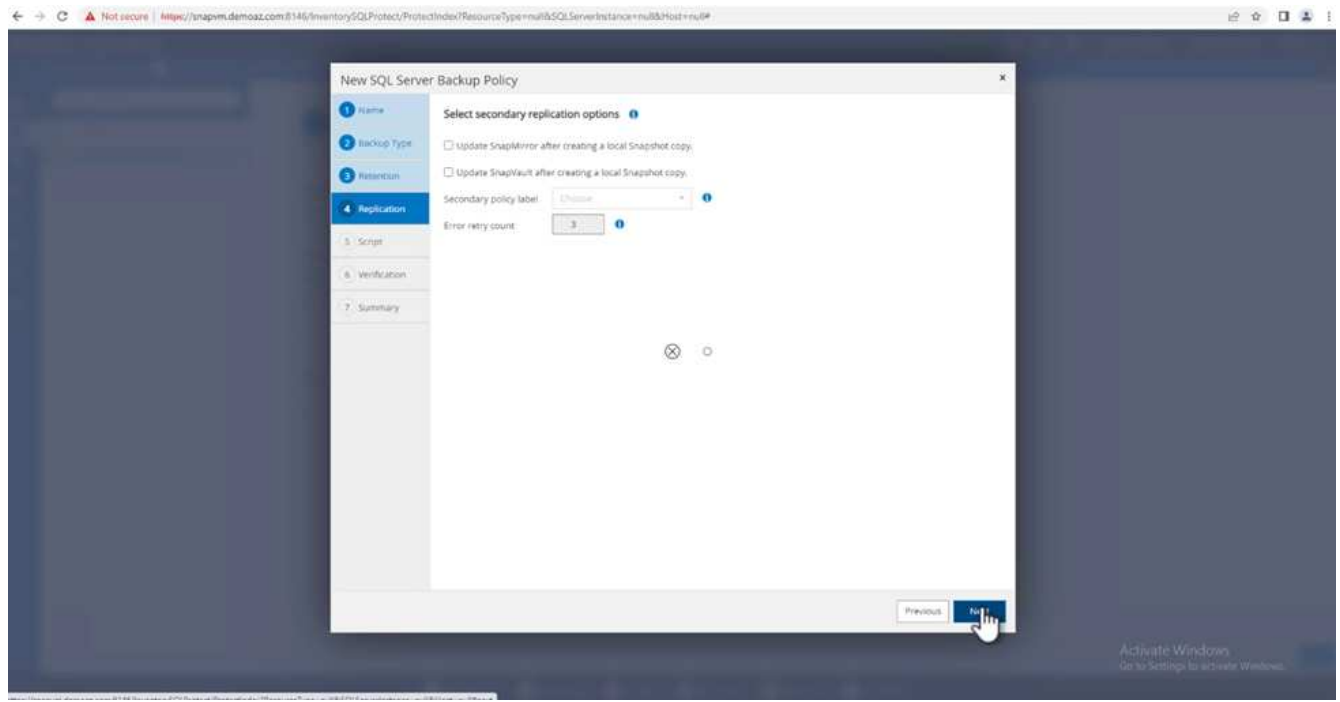
Log backup retention settings

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.

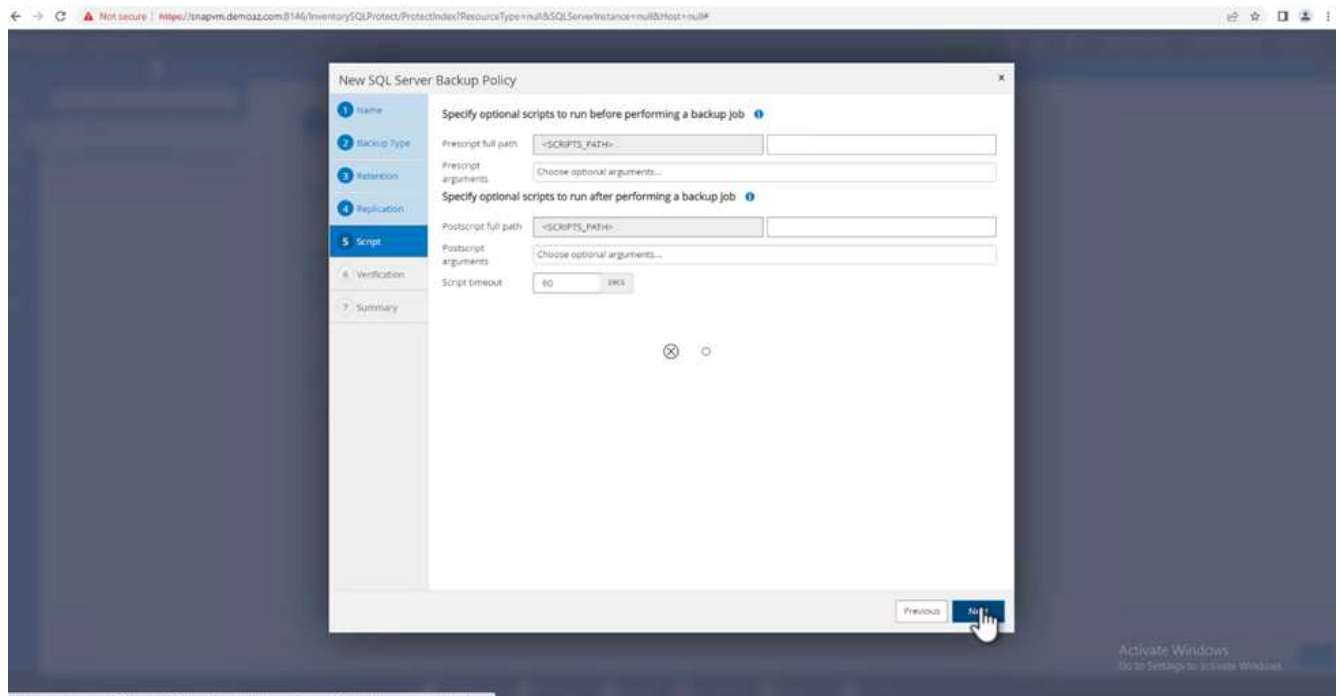
Previous

Next

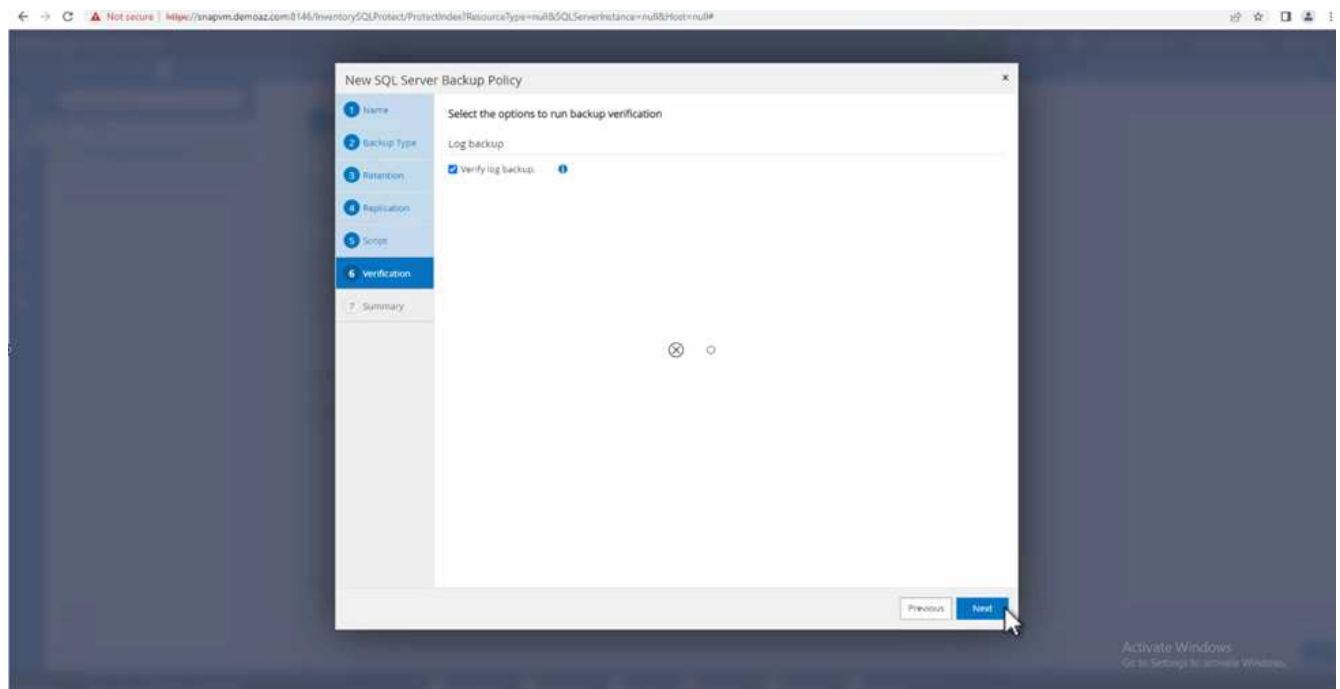
10. (Optional) Configure the replication options.



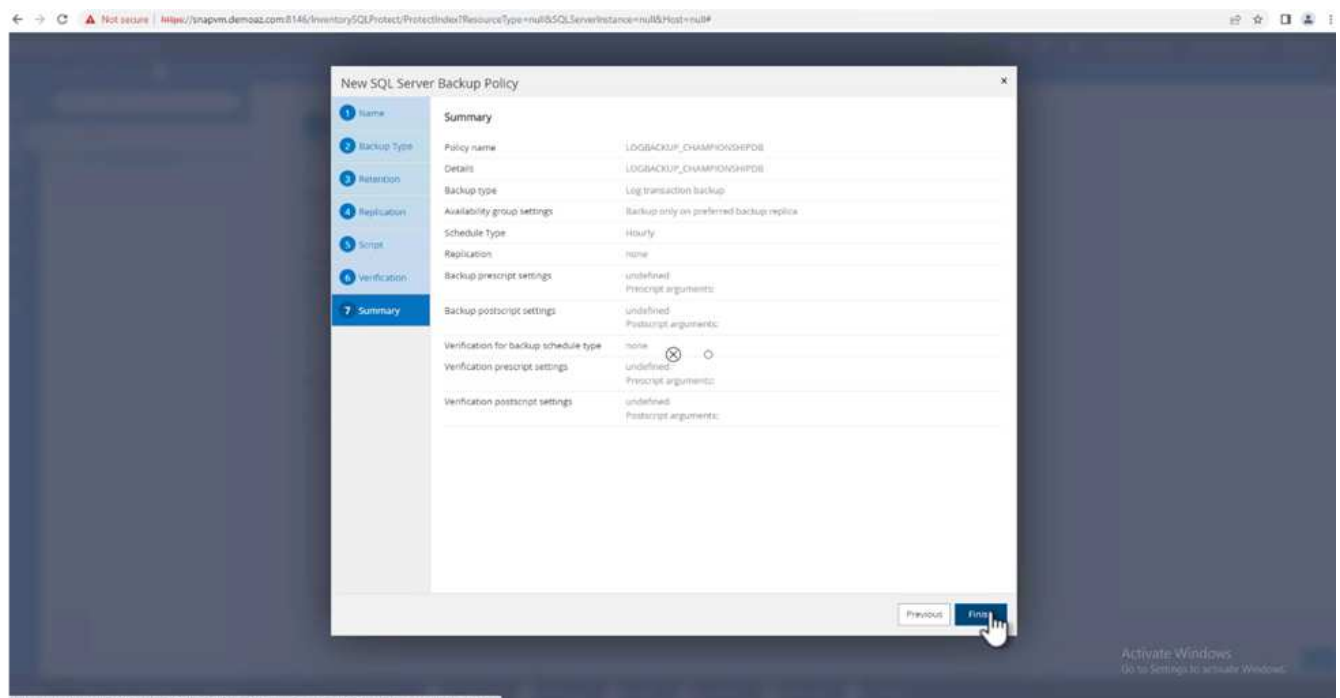
11. (Optional) Configure any scripts to run before performing a backup job.



12. (Optional) Configure backup verification.

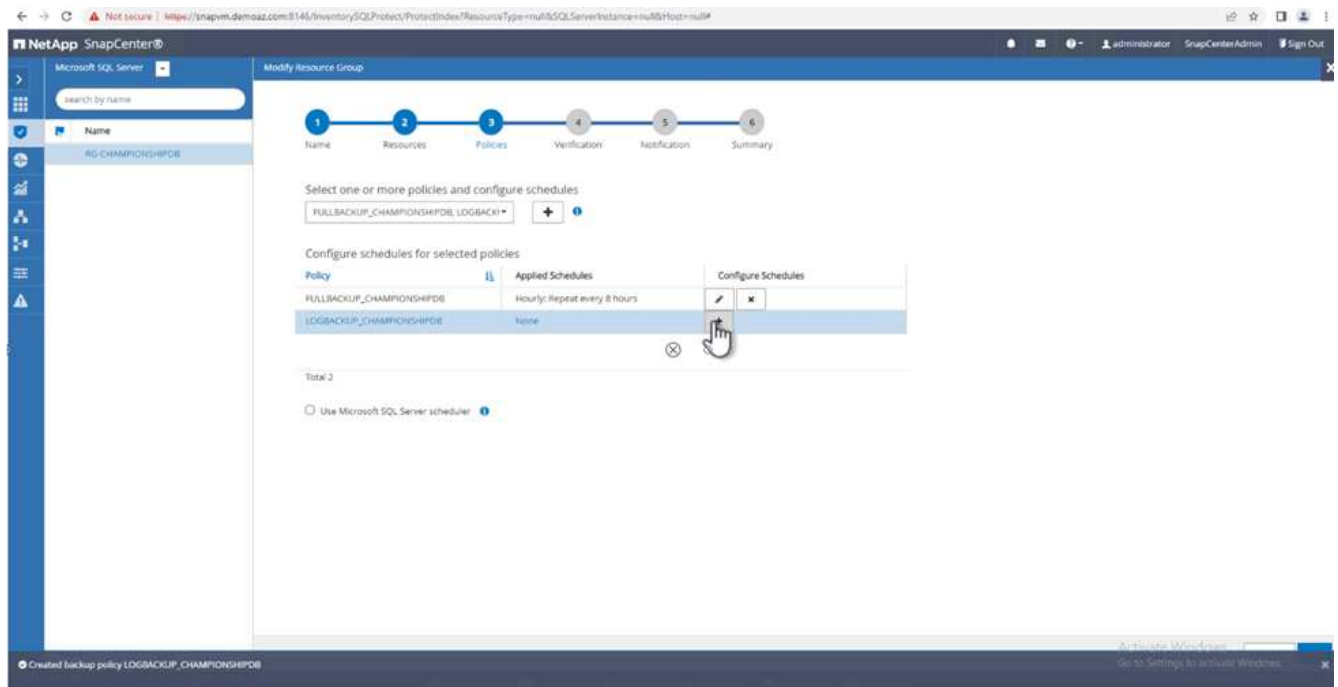


13. On the **Summary** page, click **Finish**.

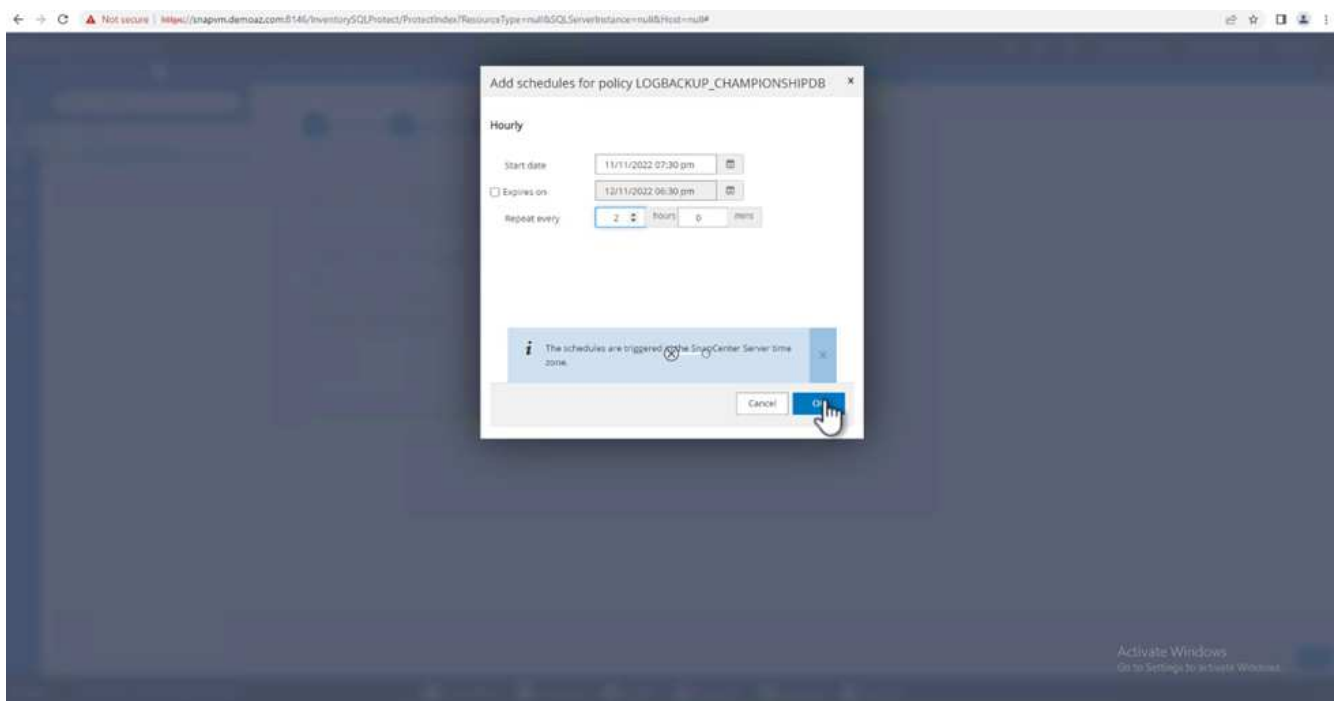


Configure and protect multiple MSSQL Server databases

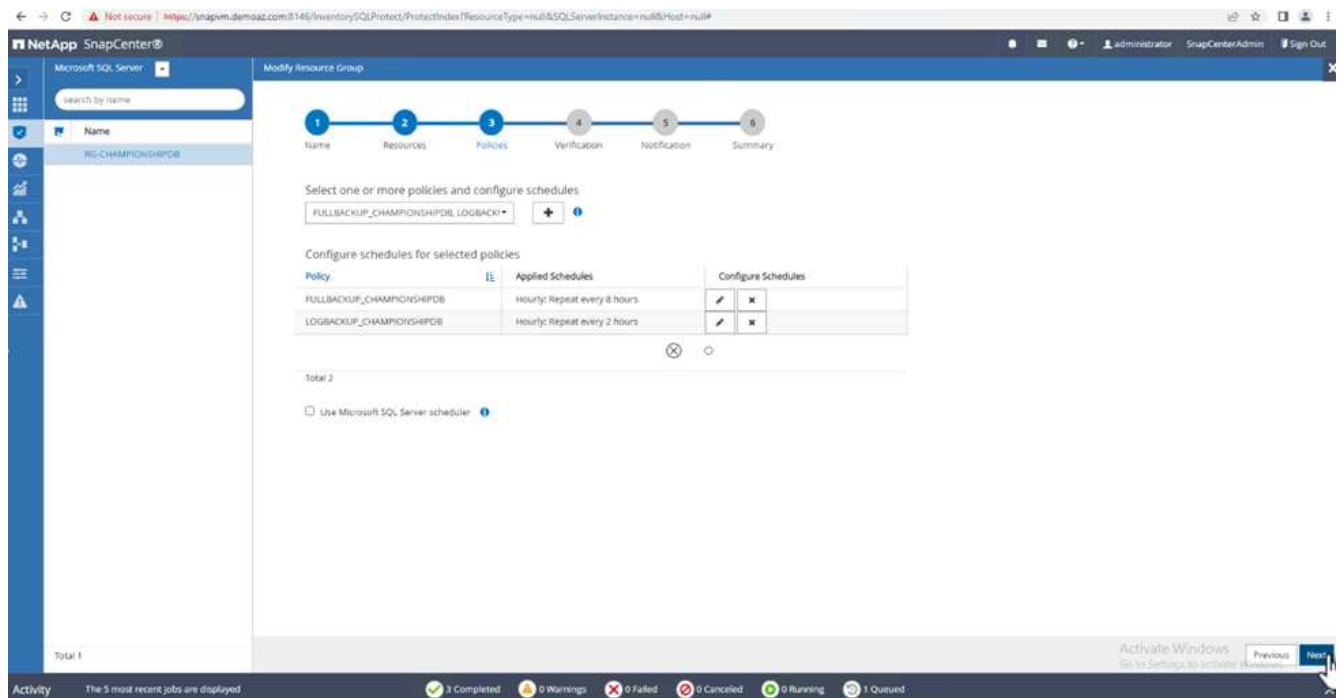
1. Click the newly created transaction log backup policy.



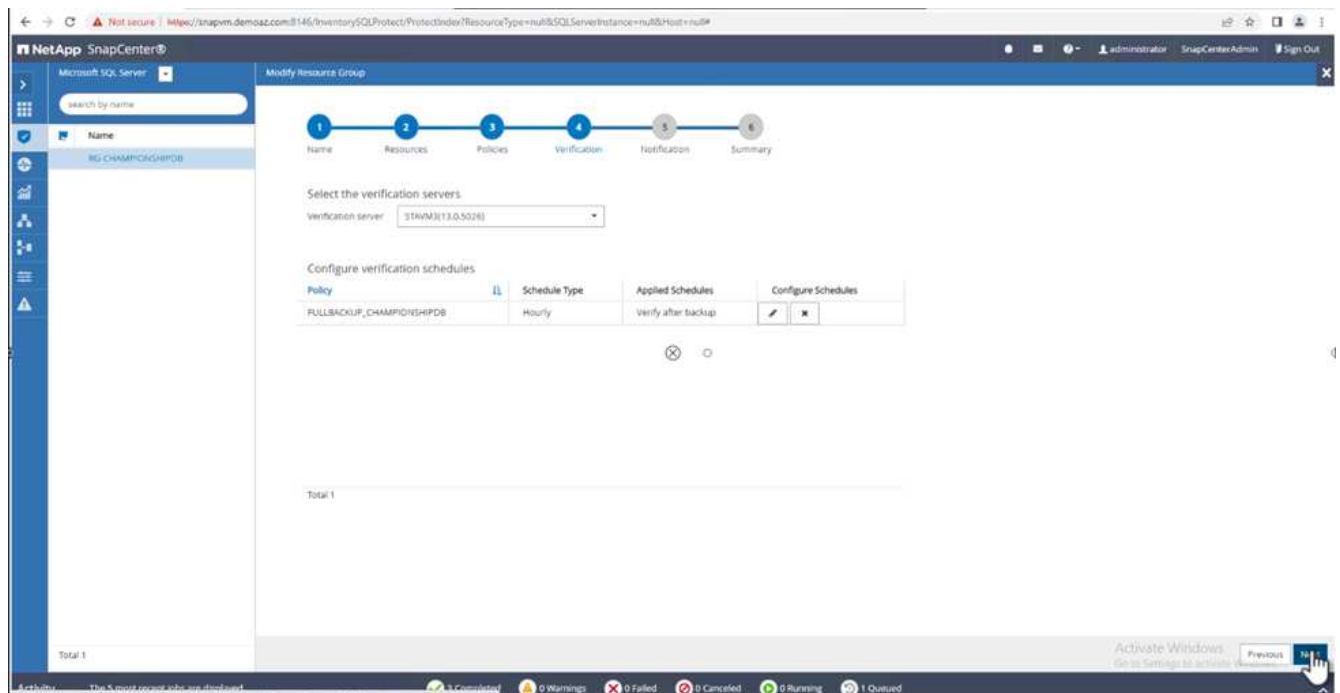
2. Set the **Start date** and **Expires on** date.
3. Enter the frequency of the log backup policy depending on the SLA, RTP, and RPO. Click OK.



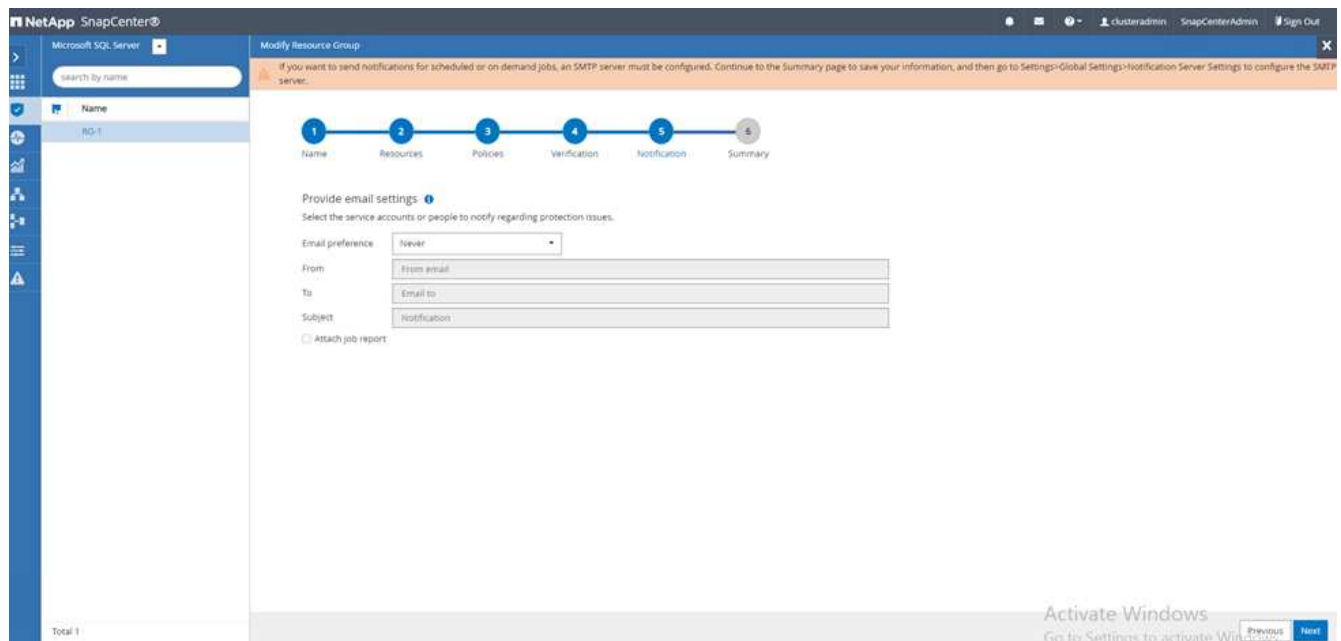
4. You can see both policies. Click **Next**.



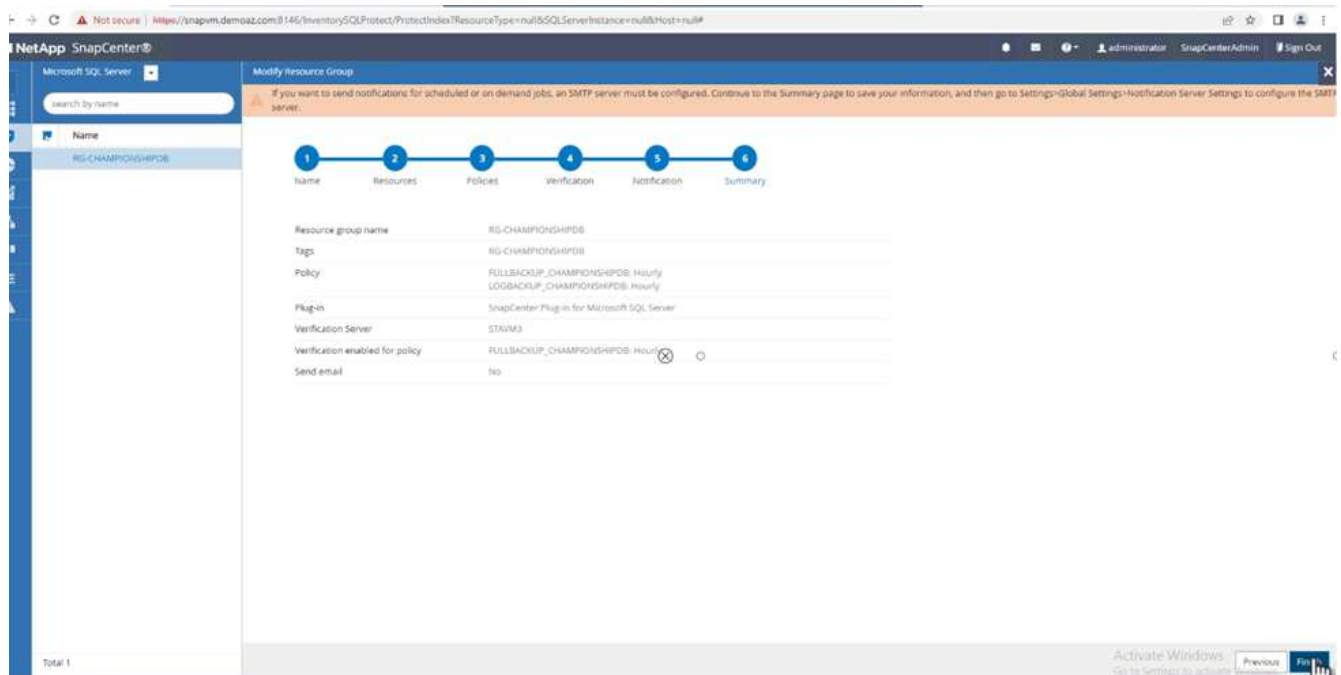
5. Configure the verification server.



6. Configure email notification.



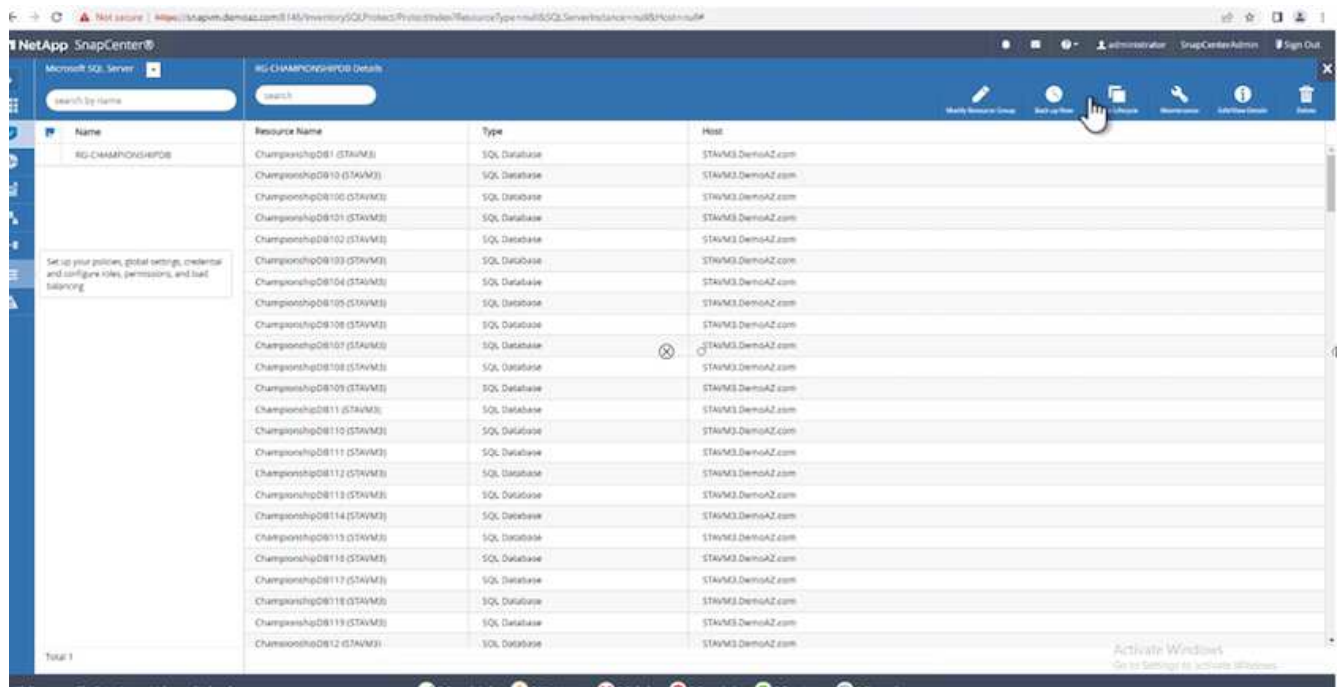
7. On the **Summary** page, click **Finish**.



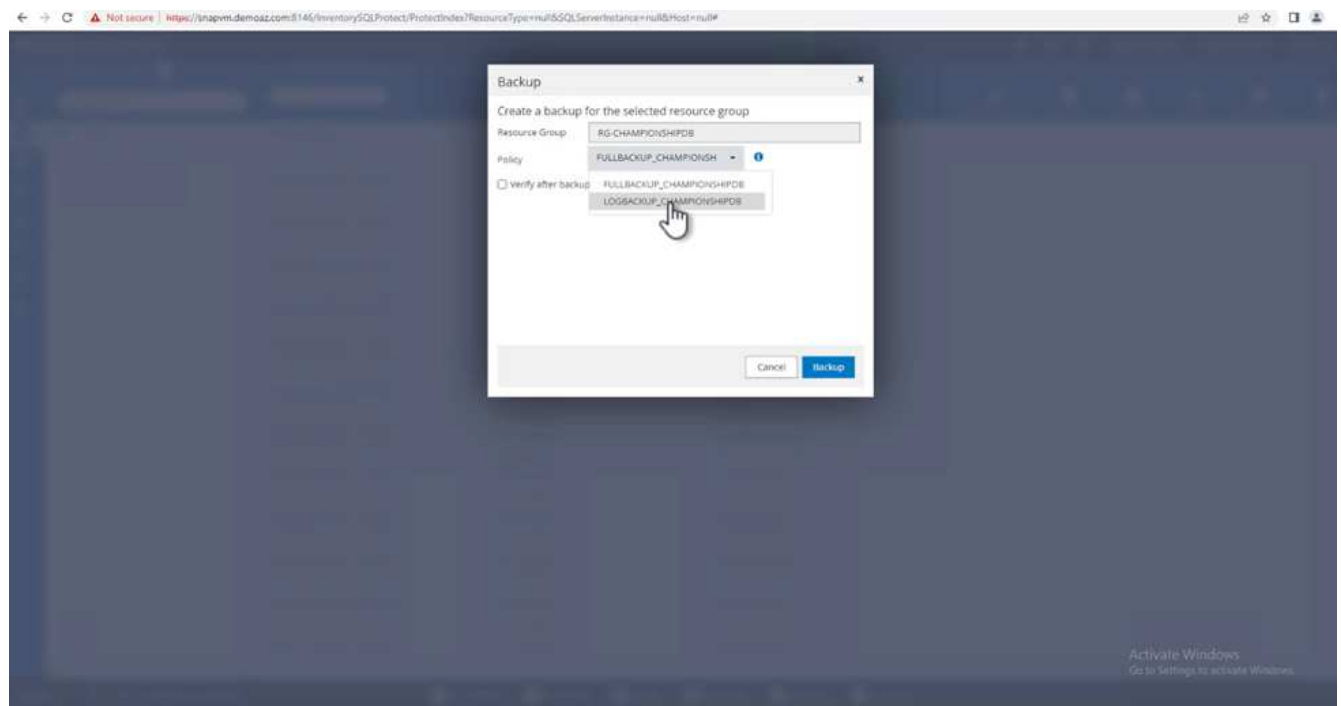
Triggering an on-demand transaction log backup for mutiple SQL Server databases

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

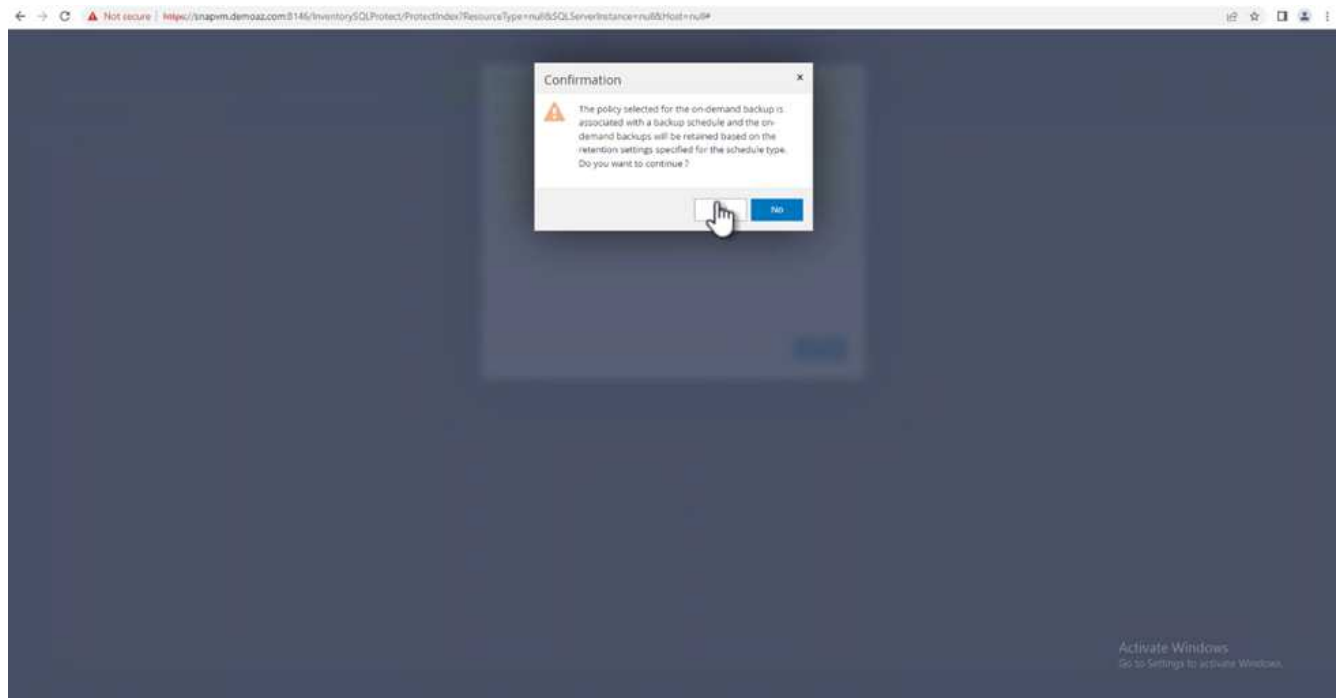
1. On the newly created policy page, select **Backup now** at the upper right of the page.



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



- 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.

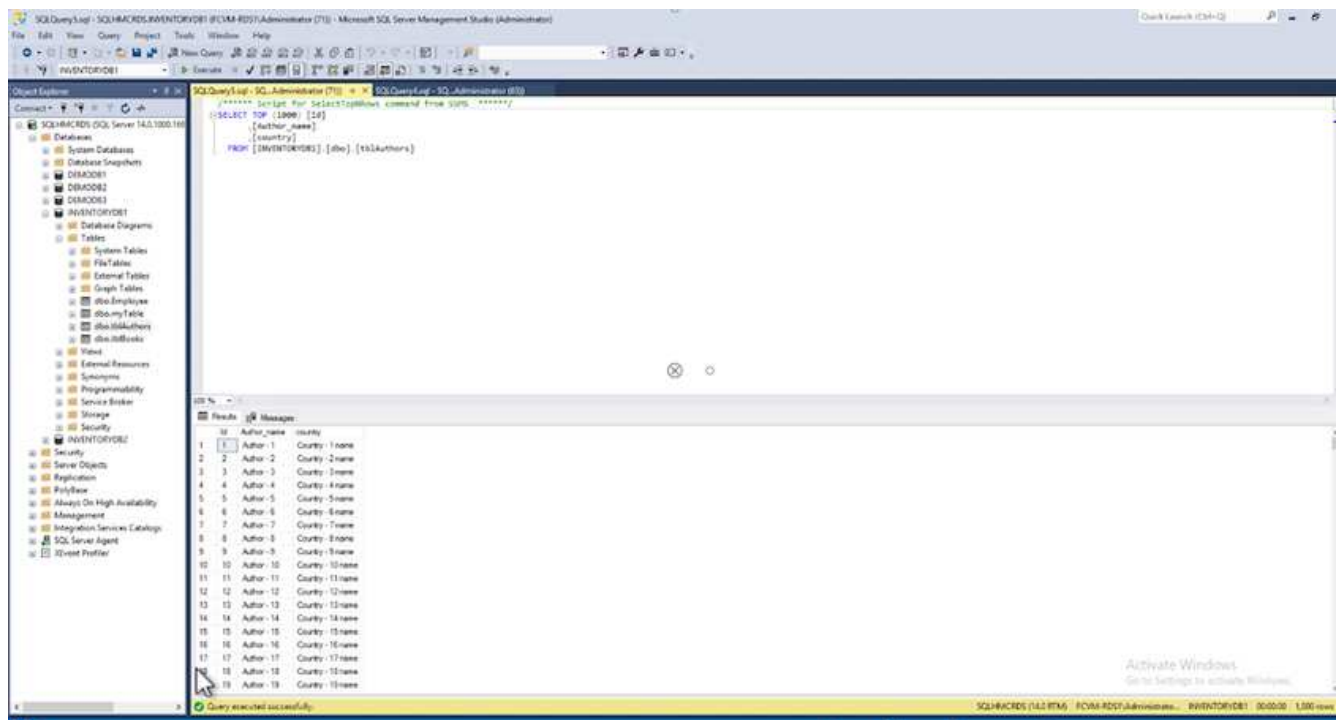
- The target instance must be online and running before a restore job completes.

- 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.

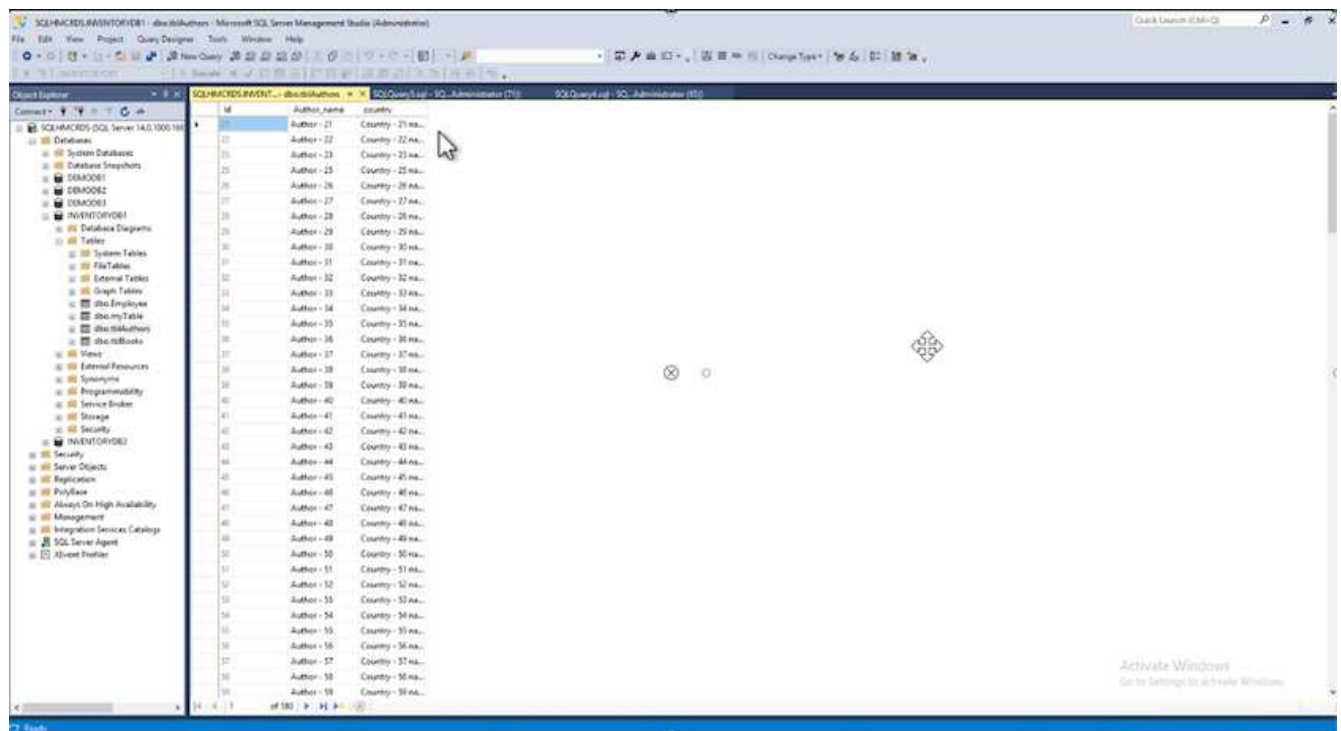
Restoring deleted tables on a SQL Server database to a point in time

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

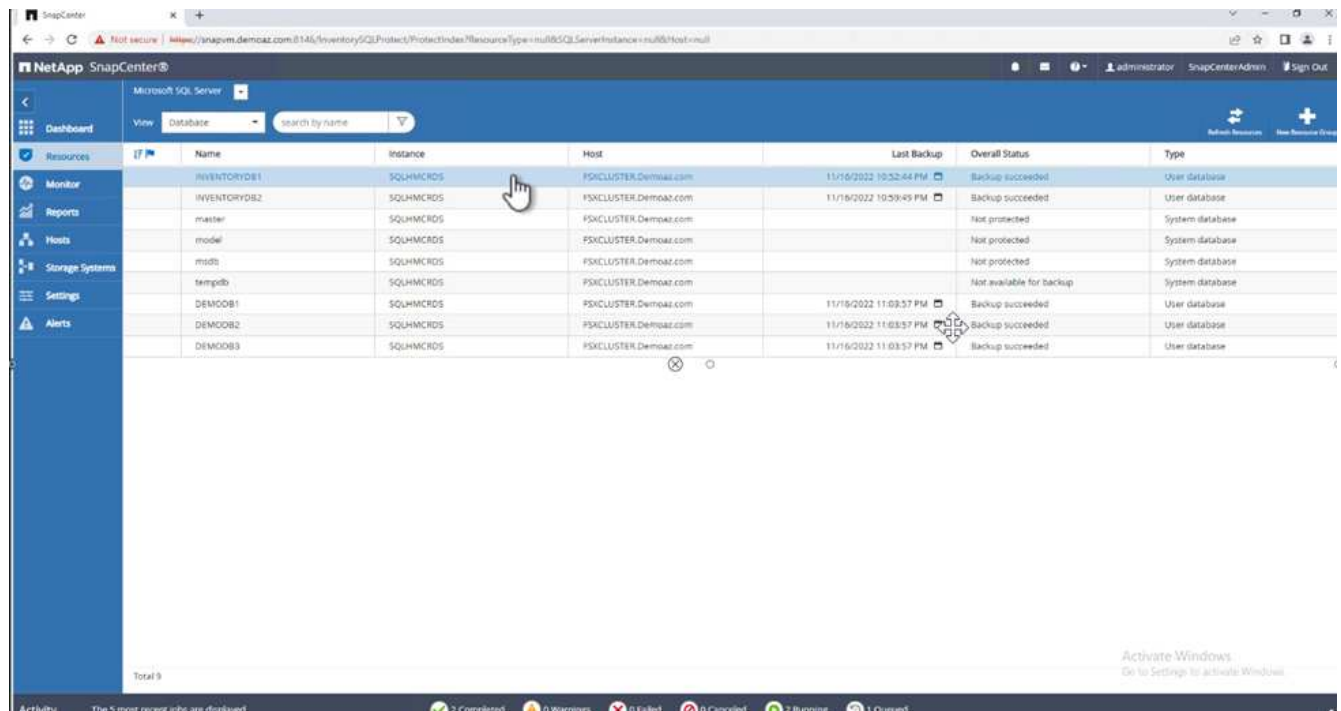
1. The following screenshot shows the initial state of the SQL Server database before the deleted tables.



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

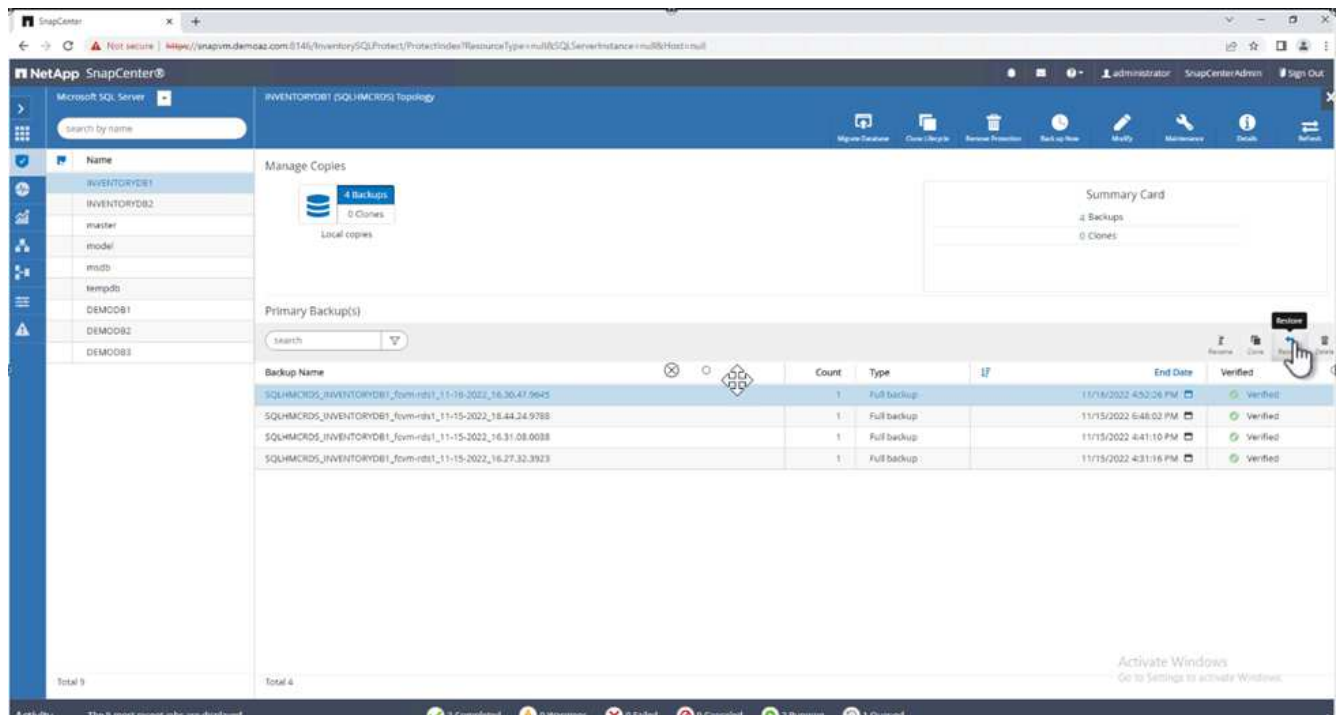


2. Log into SnapCenter Server. From the **Resources** tab, select the database.

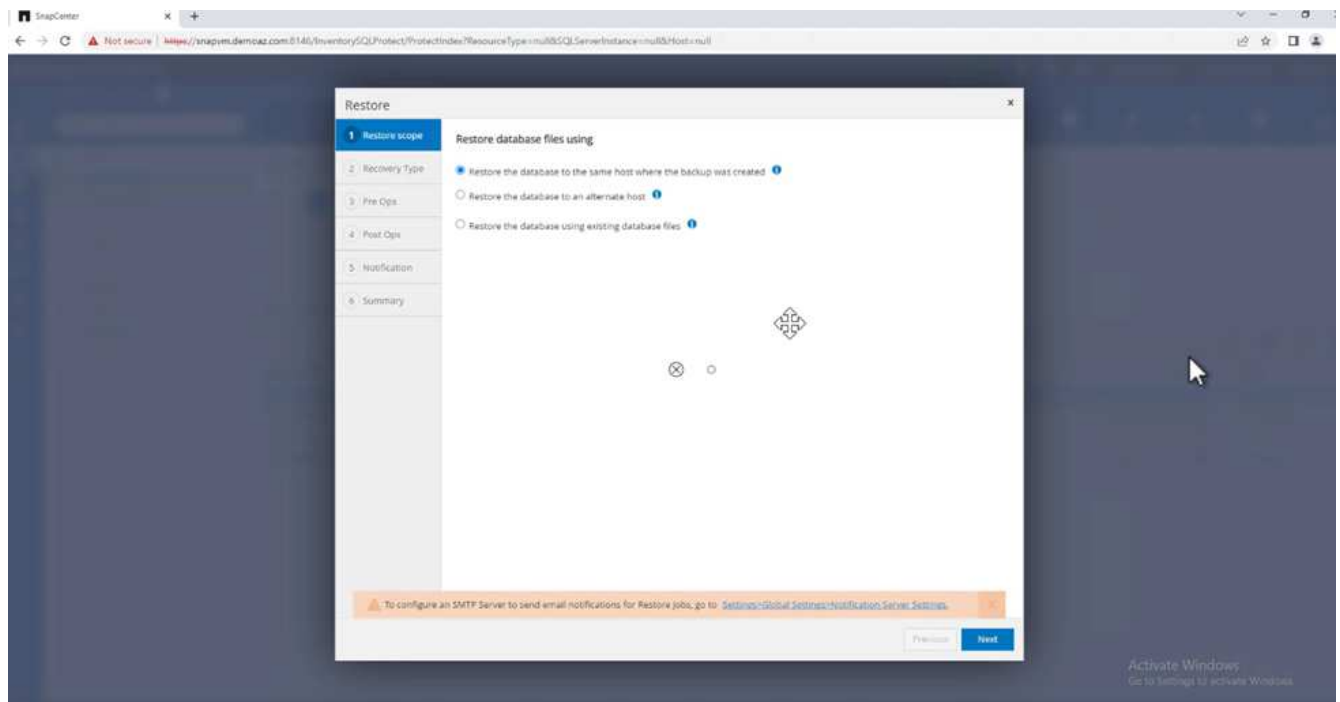


3. Select the most recent backup.

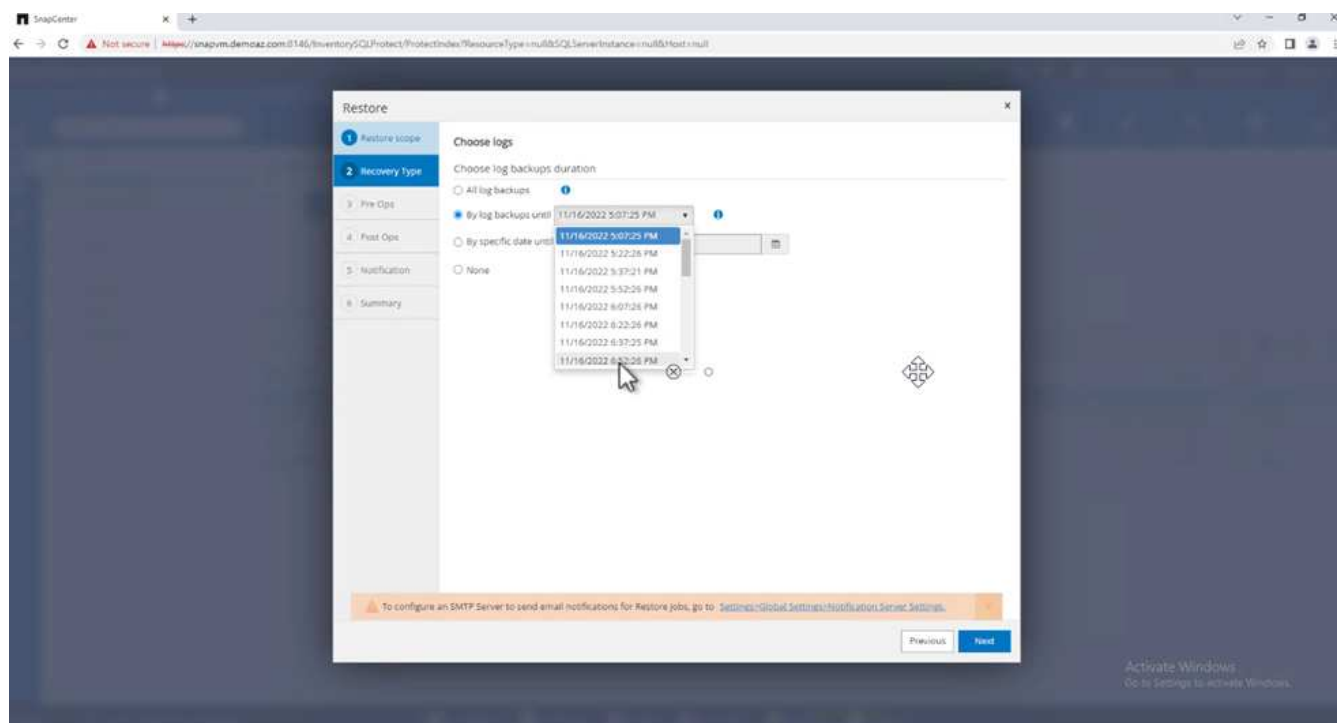
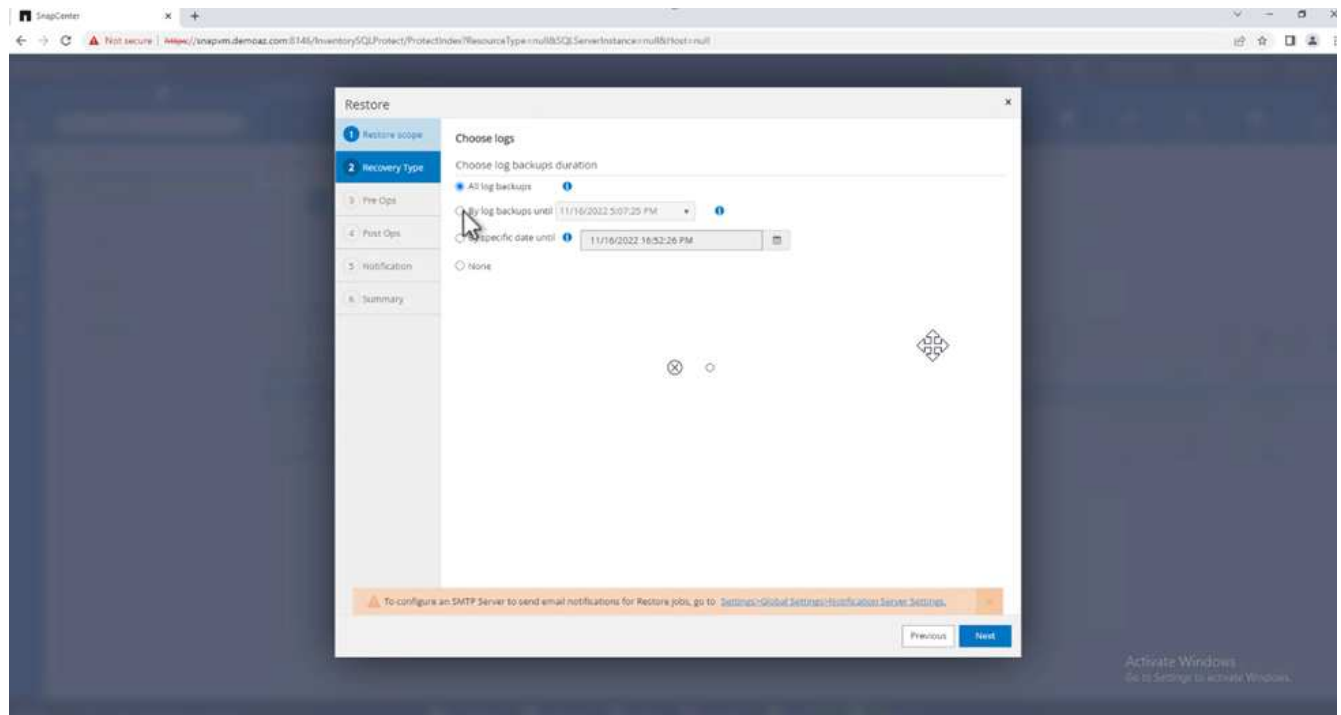
4. On the right, select **Restore**.



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**.

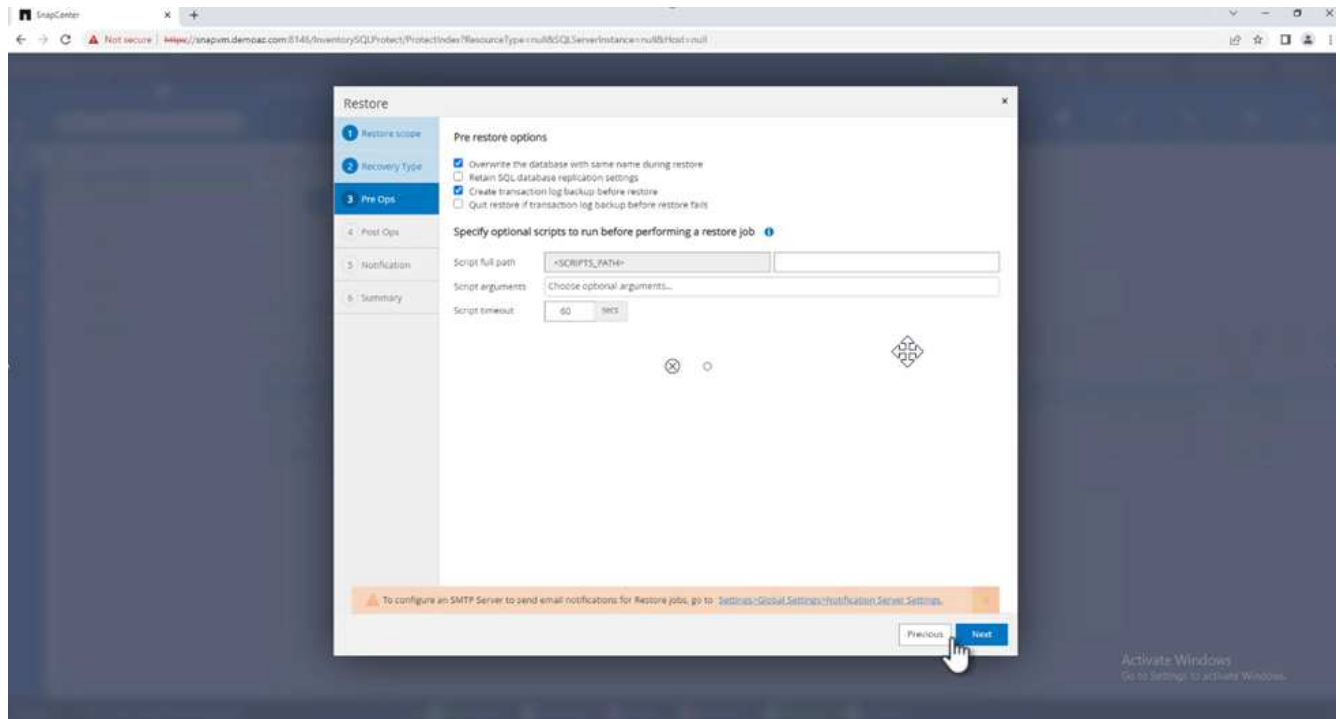


7. For the **Recovery type**, select **All log backups**. Click **Next**.



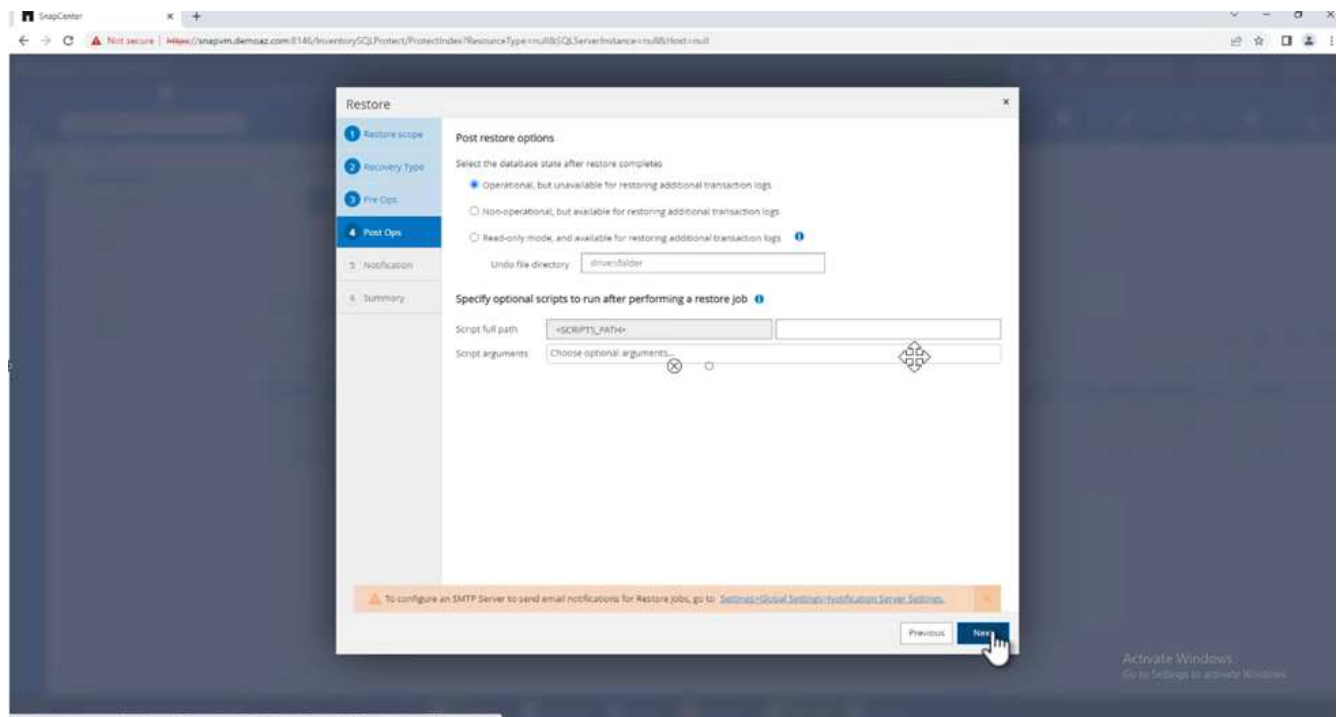
Pre- restore options:

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

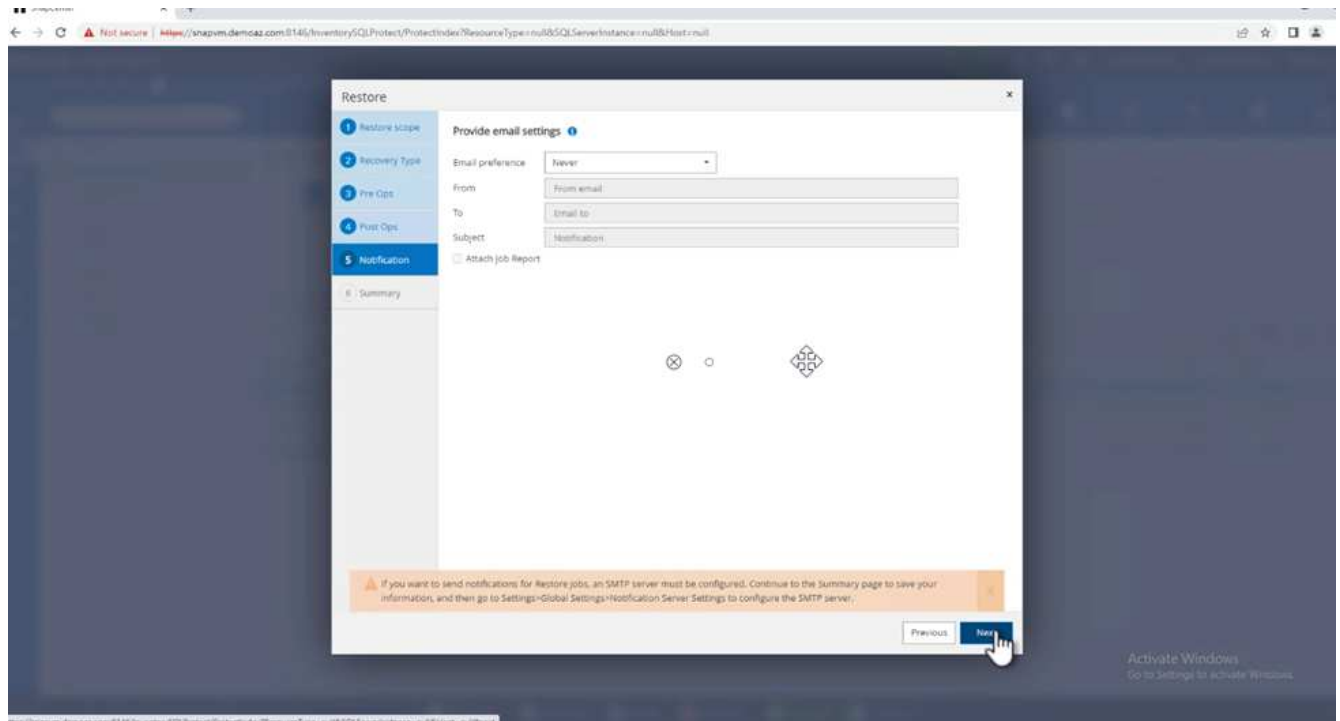


Post- restore options:

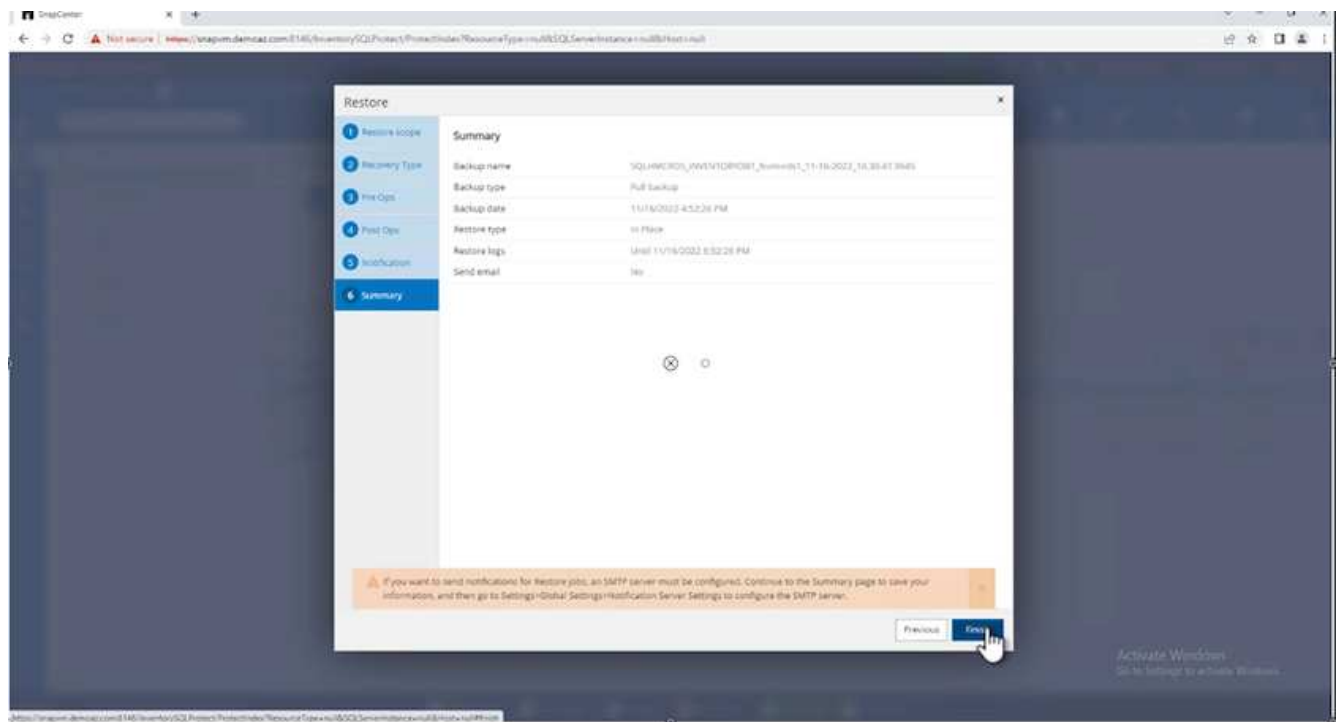
1. Select the option **Operational, but unavailable for restoring additional transaction logs**. Click **Next**.



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



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

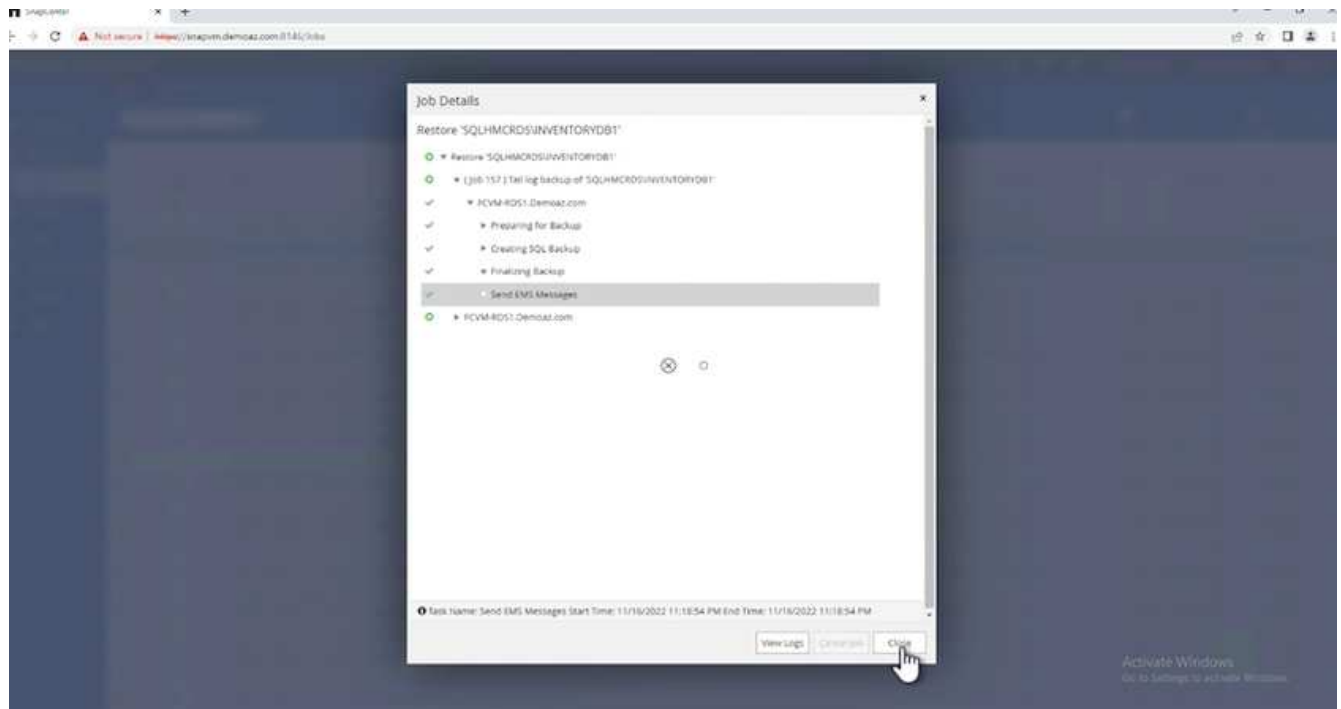


Monitoring the restore progress

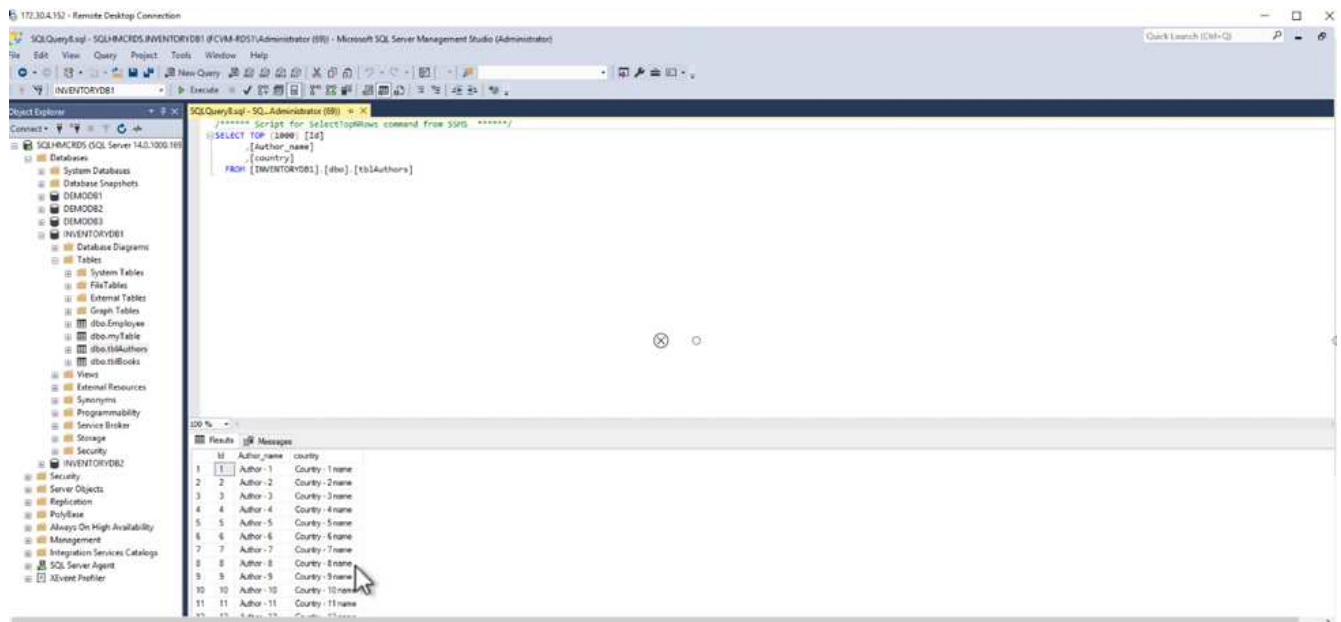
1. From the **Monitoring** tab, click the restore job details to view the progress of the restore job.

ID	Status	Name	Start date	End date	Owner
129	✓	Restore 'SQLMCRDS\INVENTORYDB'	11/16/2022 11:11:18 PM		Administrator
130	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB' with policy 'InventoryDB_logbackup_policy'	11/16/2022 11:00:01 PM		Administrator
134	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 10:59:02 PM	11/16/2022 11:10:54 PM	Administrator
132	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB2' with policy 'InventoryDB2_fullbackup'	11/16/2022 10:55:01 PM	11/16/2022 10:58:50 PM	Administrator
132	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 10:45:01 PM	11/16/2022 11:10:54 PM	Administrator
131	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 10:44:02 PM	11/16/2022 10:55:53 PM	Administrator
150	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 10:30:01 PM	11/16/2022 10:55:54 PM	Administrator
148	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 10:29:02 PM	11/16/2022 10:40:53 PM	Administrator
148	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 10:15:01 PM	11/16/2022 10:40:53 PM	Administrator
147	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 10:14:02 PM	11/16/2022 10:25:53 PM	Administrator
146	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 10:00:01 PM	11/16/2022 10:25:53 PM	Administrator
145	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 9:59:02 PM	11/16/2022 10:10:53 PM	Administrator
144	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 9:45:01 PM	11/16/2022 10:10:53 PM	Administrator
142	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 9:44:02 PM	11/16/2022 9:55:54 PM	Administrator
142	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 9:30:01 PM	11/16/2022 9:55:54 PM	Administrator
141	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 9:29:02 PM	11/16/2022 9:40:53 PM	Administrator
140	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 9:15:01 PM	11/16/2022 9:40:53 PM	Administrator
139	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 9:14:02 PM	11/16/2022 9:25:54 PM	Administrator
138	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 9:00:01 PM	11/16/2022 9:25:54 PM	Administrator
137	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 8:59:02 PM	11/16/2022 9:10:53 PM	Administrator
136	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 8:45:01 PM	11/16/2022 9:10:53 PM	Administrator
135	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 8:44:02 PM	11/16/2022 8:55:54 PM	Administrator
134	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 8:30:01 PM	11/16/2022 8:55:54 PM	Administrator
133	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 8:29:02 PM	11/16/2022 8:40:53 PM	Administrator

2. Restore the job details.



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



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

- [Understanding cloned database lifecycles](#)

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

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—without 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.