Back up SQL Server database, or instance, or availability group

SnapCenter Software 5.0

NetApp
July 18, 2024

Table of Contents

Back up SQL Server database, or instance, or availability group

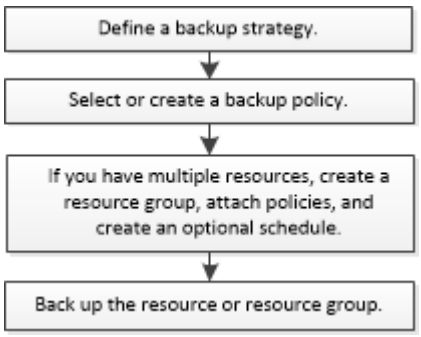
Backup workflow

When you install the SnapCenter Plug-in for Microsoft SQL Server in your environment, you can use SnapCenter to back up the SQL Server resources.

You can schedule multiple backups to run across servers simultaneously.

Backup and restore operations cannot be performed simultaneously on the same resource.

The following workflow shows the sequence in which you must perform the backup operations:



The Backup Now, Restore, Manage Backups, and Clone options on the Resources page are disabled if you select a non-NetApp LUN, a database that is corrupted, or a database that is being restored.

You can also use PowerShell cmdlets manually or in scripts to perform backup, restore, recovery, verify, and clone operations. For detailed information about PowerShell cmdlets, use the SnapCenter cmdlet help or see the SnapCenter Software Cmdlet Reference Guide

How SnapCenter backs up databases

SnapCenter uses Snapshot technology to back up the SQL Server databases that reside on LUNs or VMDKs. SnapCenter creates the backup by creating Snapshots of the databases.

When you select a database for a full database backup from the Resources page, SnapCenter automatically selects all the other databases that reside on the same storage volume. If the LUN or VMDK stores only a single database, you can clear or reselect the database individually. If the LUN or VMDK houses multiple databases, you must clear or reselect the databases as a group.

All the databases that reside on a single volume are backed up concurrently using Snapshots. If the maximum number of concurrent backup databases is 35, and if more than 35 databases reside in a storage volume, then the total number of Snapshots that are created equals the number of databases divided by 35.

You can configure the maximum number of databases for each Snapshot in the backup policy.

When SnapCenter creates a Snapshot, the entire storage system volume is captured in the Snapshot. However, the backup is valid only for the SQL host server for which the backup was created.

If data from other SQL host servers resides on the same volume, this data cannot be restored from the Snapshot.

Find more information

Back up resources using PowerShell cmdlets

Quiesce or grouping resources operations fail

Determine whether resources are available for backup

Resources are the databases, application instances, Availability Groups, and similar components that are maintained by the plug-ins you have installed. You can add those resources to resource groups so that you can perform data protection jobs, but first you must identify which resources you have available. Determining available resources also verifies that the plug-in installation has completed successfully.

Before you begin

- You must have already completed tasks such as installing SnapCenter Server, adding hosts, creating storage system connections, and adding credentials.
- To discover the Microsoft SQL databases, one of the following conditions should be met.
  - The user that was used to add the plug-in host to SnapCenter Server should have the required permissions (sysadmin) on the Microsoft SQL Server.
  - If the above condition is not met, in the SnapCenter Server you should configure the user that has the required permissions (sysadmin) on the Microsoft SQL Server. The user should be configured at the Microsoft SQL Server instance level and the user can be a SQL or Windows user.
- To discover the Microsoft SQL databases in a Windows cluster, you must unblock the Failover Cluster Instance (FCI) TCP/IP port.
- If databases reside on VMware RDM LUNs or VMDKs, you must deploy the SnapCenter Plug-in for VMware vSphere and register the plug-in with SnapCenter.

  For more information, see Deploy SnapCenter Plug-in for VMware vSphere
- If the host is added with gMSA and if the gMSA has login and system admin privileges, the gMSA will be used to connect to the SQL instance.

About this task

You cannot back up databases when the **Overall Status** option in the Details page is set to Not available for backup. The **Overall Status** option is set to Not available for backup when any of the following is true:

- Databases are not on a NetApp LUN.
- Databases are not in normal state.

  Databases are not in normal state when they are offline, restoring, recovery pending, suspect, and so on.
- Databases have insufficient privileges.

  For example, if a user has only view access to the database, files and properties of the database cannot be identified and hence cannot be backed up.

SnapCenter can backup only the primary database if you have a availability group configuration on SQL Server Standard Edition.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page select **Database**, or **Instance**, or **Availability Group**, from the **View** drop-down list.

   Click and select the host name and the SQL Server Instance to filter the resources. You can then click to close the filter pane.

3. Click **Refresh Resources**.

   The newly added, renamed, or deleted resources are updated to the SnapCenter Server inventory.

   You must refresh the resources if the databases are renamed outside of SnapCenter.

   The resources are displayed along with information such as resource type, host or cluster name, associated resource groups, backup type, policies and overall status.

   - If the database is on a non NetApp storage, `Not available for backup` is displayed in the **Overall Status** column.

     You cannot perform data protection operations on a database that is on a non NetApp storage.

   - If the database is on a NetApp storage and not protected, `Not protected` is displayed in the **Overall Status** column.
   - If the database is on a NetApp storage system and protected, the user interface displays `Backup not run` message in the **Overall Status** column.
   - If the database is on a NetApp storage system and protected and if the backup is triggered for the database, the user interface displays `Backup succeeded` message in the **Overall Status** column.

   If you have enabled an SQL authentication while setting up the credentials, the discovered instance or database is shown with a red padlock icon. If the padlock icon appears, you must specify the instance or database credentials for successfully adding the instance or database to a resource group.

4. After the SnapCenter administrator assigns the resources to a RBAC user, the RBAC user must log in and click **Refresh Resources** to see the latest **Overall Status** of the resources.

Migrate resources to NetApp storage system

After you have provisioned your NetApp storage system using SnapCenter Plug-in for Microsoft Windows, you can migrate your resources to the NetApp storage system or from one NetApp LUN to another NetApp LUN using either the SnapCenter graphical user interface (GUI) or using the PowerShell cmdlets.

Before you begin

- You must have added storage systems to SnapCenter Server.
- You must have refreshed (discovered) the SQL Server resources.

Most of the fields on these wizard pages are self-explanatory. The following information describes some of the fields for which you might require guidance.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, select **Database** or **Instance** from the **View** drop-down list.
3. Select either the database or the instance from the list and click **Migrate**.
4. In the Resources page, perform the following actions:

For this field…	Do this…
Database Name (optional)	If you have selected an instance for migration, you must select the databases of that instance from the **Databases** drop-down list.
Choose Destinations	Select the target location for data and log files. The data and log files are moved to Data and Log folder respectively under the selected NetApp drive. If any folder in the folder structure is not present, then a folder is created, and the resource is migrated.
Show database file details (optional)	Select this option when you want to migrate multiple files of a single database. This option is not displayed when you select the **Instance** resource.
Options	Select **Delete copy of Migrated Database at Original Location** to delete copy of database from the source. Optional: **RUN UPDATE STATISTICS on tables before detaching the database**.

5. In the Verify page, perform the following actions:

For this field…	Do this…
Database Consistency Check Options	Select **Run before** to check the integrity of the database before migration. Select **Run after** to check the integrity of the database after migration.

For this field…	Do this…
DBCC CHECKDB options	• Select **PHYSICAL_ONLY** option to limit the integrity check to the physical structure of the database and to detect torn pages, checksum failures, and common hardware failures that impact the database. • Select **NO_INFOMSGS** option to suppress all of the informational messages. • Select **ALL_ERRORMSGS** option to display all of the reported errors per object. • Select **NOINDEX** option if you do not want to check nonclustered indexes. The SQL Server database uses Microsoft SQL Server Database Consistency Checker (DBCC) to check the logical and physical integrity of the objects in the database. You might want to select this option to decrease the execution time. • Select **TABLOCK** option to limit the checks and obtain locks instead of using an internal database Snapshot.

6. Review the summary, and then click **Finish**.

Create backup policies for SQL Server databases

You can create a backup policy for the resource or the resource group before you use SnapCenter to back up SQL Server resources, or you can create a backup policy at the time you create a resource group or backup a single resource.

Before you begin

- You must have defined your data protection strategy.
- You must have prepared for data protection by completing tasks such as installing SnapCenter, adding hosts, identifying resources, and creating storage system connections.
- You must have configured the host log directory for log backup.
- You must have refreshed (discovered) the SQL Server resources.
- If you are replicating Snapshots to a mirror or vault, the SnapCenter administrator must have assigned the storage virtual machines (SVMs) for both the source volumes and destination volumes to you.

  For information about how administrators assign resources to users, see the SnapCenter installation information.

- If you want to run the PowerShell scripts in prescripts and postscripts, you should set the value of the

usePowershellProcessforScripts parameter to true in the web.config file.

The default value is false.

- For SnapMirror Business Continuity (SM-BC), for more information on prerequisites and limitations refer Object limits for SnapMirror Business Continuity.

About this task

- A backup policy is a set of rules that governs how you manage and retain backups, and how frequently the resource or resource group is backed up. Additionally, you can specify replication and script settings. Specifying options in a policy saves time when you want to reuse the policy for another resource group.

  The SCRIPTS_PATH is defined using the PredefinedWindowsScriptsDirectory key located in the SMCoreServiceHost.exe.Config file of the plug-in host.

  If needed, you can change this path and restart SMcore service. It is recommended that you use the default path for security.

  The value of the key can be displayed from swagger through the API: API /4.7/configsettings

  You can use the GET API to display the value of the key. SET API is not supported.

- SnapLock
  - If 'Retain the backup copies for a specific number of days' option is selected, then the SnapLock retention period must be lesser than or equal to the mentioned retention days.

    Specifying a Snapshot locking period prevents deletion of the Snapshots until the retention period expires. This could lead to retaining a larger number of Snapshots than the count specified in the policy.

    For ONTAP 9.12.1 and below version, the clones created from the SnapLock Vault Snapshots as part of restore will inherit the SnapLock Vault expiry time. Storage admin should manually cleanup the clones post the SnapLock expiry time.

    Primary SnapLock settings are managed in SnapCenter backup policy and the secondary SnapLock settings are managed by ONTAP.

Step 1: Create Policy Name

1. In the left navigation pane, select **Settings**.
2. In the Settings page, select **Policies**.
3. Select **New**.
4. In the **Name** page, enter the policy name and description.

Step 2: Configure backup options

1. Choose your backup type

Full Backup and Log Backup

Back up the database files and transaction logs and to truncate the transaction logs.

1. Select **Full backup and Log backup**.
2. Enter the maximum number of databases that should be backed up for each Snapshot.

> You must increase this value if you want to run multiple backup operations concurrently.

Full Backup

Back up the database files.

1. Select **Full backup**.
2. Enter the maximum number of databases that should be backed up for each Snapshot. Default value is 100

> You must increase this value if you want to run multiple backup operations concurrently.

Log Backup

Back up the transaction logs. . Select **Log backup**.

Copy Only Backup

1. If you are backing up your resources by using another backup application, select **Copy only backup**.

Keeping the transaction logs intact allows any backup application to restore the databases. You typically should not use the copy only option in any other circumstance.

> Microsoft SQL does not support the **Copy only backup** option together with the **Full backup and Log backup** option for secondary storage.

2. In the Availability Group Settings section, perform the following actions:

   a. Backup on preferred backup replica only.

      Select this option to backup only on preferred backup replica. The preferred backup replica is decided by the backup preferences configured for the AG in the SQL Server.

   b. Select replicas for backup.

      Choose the primary AG replica or the secondary AG replica for the backup.

   c. Select Backup priority (Minimum and Maximum backup priority)

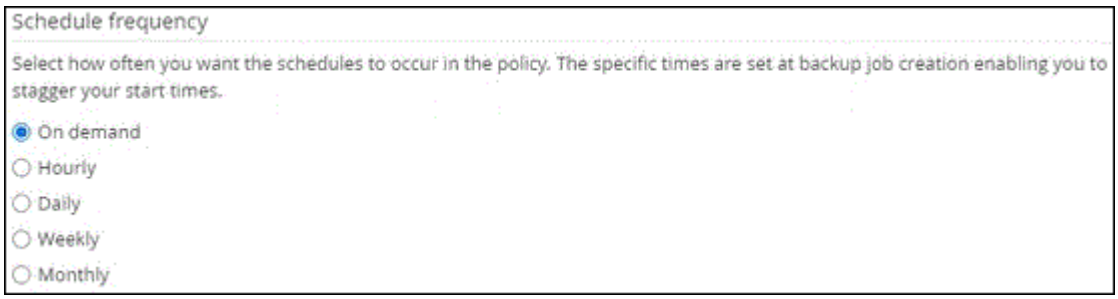
      Specify a minimum backup priority number, and a maximum backup priority number that decide the AG replica for backup. For example, you can have a minimum priority of 10 and a maximum priority of 50. In this case, all the AG replicas with a priority more than 10 and less than 50 are considered for backup.

By default, the minimum priority is 1 and maximum priority is 100.

> In cluster configurations, the backups are retained at each node of the cluster according to the retention settings set in the policy. If the owner node of the AG changes, the backups are taken according to the retention settings and the backups of the previous owner node will be retained. The retention for AG is applicable only at the node level.

3. Schedule the backup frequency for this policy. Specify the schedule type by selecting either **On demand**, **Hourly**, **Daily**, **Weekly**, or **Monthly**.

   You can only select one schedule type for a policy.



> You can specify the schedule (start date, end date, and frequency) for backup operation while creating a resource group. This enables you to create resource groups that share the same policy and backup frequency, but lets you assign different backup schedules to each policy.

> If you have scheduled for 2:00 a.m., the schedule will not be triggered during daylight saving time (DST).

Step 3: Configure retention settings

In the Retention page, depending on the backup type selected in the backup type page, perform one or more of the following actions:

1. In the Retention settings for the up-to-the-minute restore operation section, perform one of the following actions:

Specific number of copies

Retain only a specific number of Snapshots.

1. Select the **Keep log backups applicable to last <number> days** option, and specify the number of days to be retained. If you near this limit, you might want to delete older copies.

Specific number of days

Retain the backup copies for a specific number of days.

1. Select the **Keep log backups applicable to last <number> days of full backups** option, and specify the number of days to keep the log backup copies.

2. In the **Full backup retentions settings** section for the On Demand retention settings, perform the

following actions:

a. Specify total number of Snapshots to keep

   i. To specify the number of Snapshots to keep, select **Total Snapshot copies to keep**.

   ii. If the number of Snapshots exceeds the specified number, the Snapshots are deleted with the oldest copies deleted first.

> By default, the value of retention count is set to 2. If you set the retention count to 1, the retention operation might fail because the first Snapshot is the reference Snapshot for the SnapVault relationship until a newer Snapshot is replicated to the target.

> The maximum retention value is 1018 for resources on ONTAP 9.4 or later, and 254 for resources on ONTAP 9.3 or earlier. Backups will fail if retention is set to a value higher than what the underlying ONTAP version supports.

b. Length of time to keep Snapshots

   i. If you want to specify the number of days for which you want to keep the Snapshots before deleting them, select **Keep Snapshot copies for**.

c. If you want to specify the Snapshot locking period, select **Snapshot copy locking period** and select days, months, or years.

   Snaplock retention period should be less than 100 years.

3. In the **Full backup retentions settings** section for the Hourly, Daily, Weekly and Monthly retention settings, specify the retention settings for the schedule type selected in Backup Type page.

   a. Specify total number of Snapshots to keep

      i. To specify the number of Snapshots to keep, select **Total Snapshot copies to keep**. If the number of Snapshots exceeds the specified number, the Snapshots are deleted with the oldest copies deleted first.

> You must set the retention count to 2 or higher if you plan to enable SnapVault replication. If you set the retention count to 1, the retention operation might fail because the first Snapshot is the reference Snapshot for the SnapVault relationship until a newer Snapshot is replicated to the target.

   b. Length of time to keep Snapshots

      a. To specify the number of days for which you want to keep the Snapshots before deleting them, select **Keep Snapshot copies for**.

   c. If you want to specify the Snapshot locking period, select **Snapshot copy locking period** and select days, months, or years.

      SnapLock retention period should be less than 100 years.

      The log Snapshot retention is set to 7 days by default. Use Set-SmPolicy cmdlet to change the log Snapshot retention.

This example sets the log Snapshot retention to 2:

Example 1. Show Example

```
Set-SmPolicy -PolicyName 'newpol' -PolicyType 'Backup' -PluginPolicyType 'SCSQL' -sqlbackuptype
'FullBackupAndLogBackup' -RetentionSettings
@{BackupType='DATA';ScheduleType='Hourly';RetentionCount=2},@{BackupType='LOG_SNAPSHOT';
ScheduleType='None';RetentionCount=2},@{BackupType='LOG';ScheduleType='Hourly';RetentionCount
=2} -scheduletype 'Hourly'
```

SnapCenter retains Snapshot copies of the database

Step 4: Configure replication settings

1. In the Replication page, specify replication to the secondary storage system:

Update SnapMirror

Update SnapMirror after creating a local Snapshot copy.

1. Select this option to create mirror copies of backup sets on another volume (SnapMirror).

   This option should be enabled for SnapMirror Business Continuity (SM-BC) or for SnapMirror Sync (SM-S).

   During secondary replication, the SnapLock expiry time loads the primary SnapLock expiry time. Clicking the **Refresh** button in the Topology page refreshes the secondary and primary SnapLock expiry time that are retrieved from ONTAP.

   See View SQL Server backups and clones in the Topology page.

Update SnapVault

Update SnapVault after creating a Snapshot copy.

1. Select this option to perform disk-to-disk backup replication.

   During secondary replication, the SnapLock expiry time loads the primary SnapLock expiry time. Clicking the **Refresh** button in the Topology page refreshes the secondary and primary SnapLock expiry time that are retrieved from ONTAP.

   When SnapLock is configured only on the secondary from ONTAP known as SnapLock Vault, clicking the **Refresh** button in the Topology page refreshes the locking period on the secondary that is retrieved from ONTAP.

   For more information on SnapLock Vault see Commit Snapshot copies to WORM on a vault destination

   See View SQL Server backups and clones in the Topology page.

Secondary Policy Label

1. Select a Snapshot label.

Depending on the Snapshot label that you select, ONTAP applies the secondary Snapshot retention policy that matches the label.

> If you have selected **Update SnapMirror after creating a local Snapshot copy**, you can optionally specify the secondary policy label. However, if you have selected **Update SnapVault after creating a local Snapshot copy**, you should specify the secondary policy label.

Error Retry Count

1. Enter the number of replication attempts that should occur before the process halts.

Step 5: Configure script settings

1. In the Script page, enter the path and the arguments of the prescript or postscript that should be run before or after the backup operation, respectively.

For example, you can run a script to update SNMP traps, automate alerts, and send logs.

> The prescripts or postscripts path should not include drives or shares. The path should be relative to the SCRIPTS_PATH.

> You must configure the SnapMirror retention policy in ONTAP so that the secondary storage does not reach the maximum limit of Snapshots.

Step 6: Configure verification settings

In the Verification page, perform the following steps:

1. In the Run verification for following backup schedules section, select the schedule frequency.
2. In the Database consistency check options section, perform the following actions:
   a. Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)
      i. Select **Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)** to limit the integrity check to the physical structure of the database and to detect torn pages, checksum failures, and common hardware failures that impact the database.
   b. Suppress all information messages (NO INFOMSGS)
      i. Select **Supress all information messages (NO_INFOMSGS)** to suppress all informational messages. Selected by default.
   c. Display all reported error messages per object (ALL_ERRORMSGS)
      i. Select **Display all reported error messages per object (ALL_ERRORMSGS)** to display all the reported errors per object.
   d. Do not check nonclustered indexes (NOINDEX)
      i. Select **Do not check nonclustered indexes (NOINDEX)** if you do not want to check nonclustered indexes. The SQL Server database uses Microsoft SQL Server Database Consistency Checker (DBCC) to check the logical and physical integrity of the objects in the database.
   e. Limit the checks and obtain the locks instead of using an internal database Snapshot (TABLOCK)
      i. Select **Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)** to limit the checks and obtain locks instead of using an internal database Snapshot.
3. In the **Log Backup** section, select **Verify log backup upon completion** to verify the log backup upon completion.
4. In the **Verification script settings** section, enter the path and the arguments of the prescript or postscript that should be run before or after the verification operation, respectively.

> The prescripts or postscripts path should not include drives or shares. The path should be relative to the SCRIPTS_PATH.

Step 7: Review summary

1. Review the summary, and then select **Finish**.

Create resource groups and attach policies for SQL Server

A resource group is a container to which you add resources that you want to back up and protect together. A resource group enables you to back up all of the data that is associated with a given application simultaneously. A resource group is required for any data protection job. You must also attach one or more policies to the resource group to define the type of data protection job that you want to perform.

You can protect resources individually without creating a new resource group. You can take backups on the protected resource.

About this task

- For ONTAP 9.12.1 and below version, the clones created from the SnapLock Vault Snapshots as part of restore will inherit the SnapLock Vault expiry time. Storage admin should manually cleanup the clones post the SnapLock expiry time.
- Adding new databases without SM-BC to an existing resource group which contains resources with SM-BC is not supported.
- Adding new databases to an existing resource group in failover mode of SM-BC is not supported. You can add resources to the resource group only in regular or fail-back state.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, select **Database** from the **View** list.

   If you have recently added a resource to SnapCenter, click **Refresh Resources** to view the newly added resource.

3. Click **New Resource Group**.
4. In the Name page, perform the following actions:

For this field…	Do this…
Name	Enter the resource group name. The resource group name should not exceed 250 characters.
Tags	Enter one or more labels that will help you later search for the resource group. For example, if you add HR as a tag to multiple resource groups, you can later find all resource groups associated with the HR tag.
Use custom name format for Snapshot copy	Optional: Enter a custom Snapshot name and format. For example, customtext_resourcegroup_policy_hostname or resourcegroup_hostname. By default, a timestamp is appended to the Snapshot name.

5. In the Resources page, perform the following steps:
   a. Select the host name, resource type, and the SQL Server instance from drop-down lists to filter the list of resources.

      If you have recently added resources, they will appear on the list of Available Resources only after you refresh your resource list.

   b. To move resources from the **Available Resources** section to the Selected Resources section, perform one of the following steps:
      - Select **Autoselect all resources on same storage volume** to move all of the resources on the same volume to the Selected Resources section.
      - Select the resources from the **Available Resources** section and then click the right arrow to move them to the **Selected Resources** section.
6. In the Policies page, perform the following steps:
   a. Select one or more policies from the drop-down list.

      You can also create a policy by clicking + .

      In the Configure schedules for selected policies section, the selected policies are listed.

   b. In the Configure schedules for selected policies section, click + in the Configure Schedules column for the policy for which you want to configure the schedule.
   c. In the Add schedules for policy *policy_name* dialog box, configure the schedule by specifying the start date, expiration date, and frequency, and then click **OK**.

      You must do this for each frequency listed in the policy. The configured schedules are listed in the Applied Schedules column in the **Configure schedules for selected policies** section.

   d. Select the Microsoft SQL Server scheduler.

      You must also select a scheduler instance to associate with the scheduling policy.

      If you do not select Microsoft SQL Server scheduler, the default is Microsoft Windows scheduler.

   Third party backup schedules are not supported when they overlap with SnapCenter backup schedules. You should not modify the schedules and rename the backup job created in Windows scheduler or SQL Server agent.
7. In the Verification page, perform the following steps:
   a. Select the verification server from the **Verification server** drop-down list.

      The list includes all the SQL Servers added in SnapCenter. You can select multiple verification servers (local host or remote host).

      The verification server version should match the version and edition of the SQL server that is hosting the primary database.

   b. Click **Load locators** to load the SnapMirror and SnapVault volumes to perform verification on

secondary storage.

c. Select the policy for which you want to configure your verification schedule, and then click .

d. In the Add Verification Schedules policy_name dialog box, perform the following actions:

If you want to…	Do this…
Run verification after backup	Select **Run verification after backup**.
Schedule a verification	Select **Run scheduled verification**.

e. Click **OK**.

The configured schedules are listed in the Applied Schedules column. You can review and then edit by clicking  or delete by clicking .

8. In the Notification page, from the **Email preference** drop-down list, select the scenarios in which you want to send the emails.

You must also specify the sender and receiver email addresses, and the subject of the email. If you want to attach the report of the operation performed on the resource group, select **Attach Job Report**.

For email notification, you must have specified the SMTP server details either using the GUI or PowerShell command Set-SmSmtpServer.

9. Review the summary, and then click **Finish**.

Related information

Create backup policies for SQL Server databases

Requirements for backing up SQL resources

Before you backup a SQL resource, you must ensure that several requirements are met.

- You must have migrated a resource from a non-NetApp storage system to a NetApp storage system.
- You must have created a backup policy.
- If you want to back up a resource that has a SnapMirror relationship to a secondary storage, the ONTAP role assigned to the storage user should include the “snapmirror all” privilege. However, if you are using the “vsadmin” role, then the “snapmirror all” privilege is not required.
- The backup operation initiated by an active directory (AD) user fails if the SQL instance credential is not assigned to the AD user or group. You must assign the SQL instance credential to AD user or group from the **Settings** > **User Access** page.
- You must have created a resource group with a policy attached.
- If a resource group has multiple databases from different hosts, the backup operation on some hosts might be triggered late because of network issues. You should configure the value of FMaxRetryForUninitializedHosts in web.config by using the Set-SmConfigSettings PS cmdlet.

Back up SQL resources

If a resource is not yet part of any resource group, you can back up the resource from the Resources page.

About this task

- For Windows credentials authentication, you must set up your credential before installing the plug-ins.
- For SQL Server instance authentication, you must add the credential after installing the plug-ins.
- For gMSA authentication, you must setup gMSA while registering the host with SnapCenter in the **Add Host** or **Modify Host** page to enable and use the gMSA.
- If the host is added with gMSA and if the gMSA has login and system admin privileges, the gMSA will be used to connect to the SQL instance.

Steps

1. In the left navigation pane, select **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, select **Database** ,or **Instance**, or **Availability Group** from the **View** drop-down list.
   a. Select the database, or instance, or availability group that you want to back up.

      When you take a backup of an instance, the information about the last backup status or the timestamp of that instance will not be available in the resources page.

      In the topology view, you cannot differentiate whether the backup status, timestamp, or backup is for an instance or a database.
3. In the Resources page, select the **custom name format for Snapshot copy** check box, and then enter a custom name format that you want to use for the Snapshot name.

   For example, customtext_policy_hostname or resource_hostname. By default, a timestamp is appended to the Snapshot name.
4. In the Policies page, perform the following tasks:
   a. In the Policies section, select one or more policies from the drop-down list.

      You can create a policy by selecting  to start the policy wizard.

      In the **Configure schedules for selected policies** section, the selected policies are listed.

   b. Select  in the Configure Schedules column for the policy for which you want to configure a schedule.
   c. In the **Add schedules for policy** `policy_name` dialog box, configure the schedule, and then select **OK**.

      Here `policy_name` is the name of the policy that you have selected.

      The configured schedules are listed in the **Applied Schedules** column.

   d. Select the **Use Microsoft SQL Server scheduler**, and then select the scheduler instance from the **Scheduler Instance** drop-down list that is associated with the scheduling policy.

5. In the Verification page, perform the following steps:
   a. Select the verification server from the **Verification server** drop-down list.

      You can select multiple verification servers (local host or remote host).

      The verification server version should be equal or above the version of the edition of the SQL server that is hosting the primary database.

   b. Select **Load secondary locators to verify backups on secondary** to verify your backups on secondary storage system.

   c. Select the policy for which you want to configure your verification schedule, and then select +.

   d. In the Add Verification Schedules *policy_name* dialog box, perform the following actions:

If you want to…	Do this…
Run verification after backup	Select **Run Verification after Backup**.
Schedule a verification	Select **Run scheduled verification**.

      If the verification server does not have a storage connection, the verification operation fails with error: Failed to mount disk.

   e. Select **OK**.

      The configured schedules are listed in the Applied Schedules column.

6. In the Notification page, from the **Email preference** drop-down list, select the scenarios in which you want to send the emails.

   You must also specify the sender and receiver email addresses, and the subject of the email. If you want to attach the report of the operation performed on the resource group, select **Attach Job Report**.

   For email notification, you must have specified the SMTP server details either using the GUI or PowerShell command Set-SmSmtpServer.

7. Review the summary, and then select **Finish**.

   The database topology page is displayed.

8. Select **Back up Now**.
9. In the Backup page, perform the following steps:
   a. If you have applied multiple policies to the resource, from the **Policy** drop-down list, select the policy that you want to use for backup.

      If the policy selected for the on-demand backup is associated with a backup schedule, the on-demand backups will be retained based on the retention settings specified for the schedule type.

   b. Select **Verify after backup** to verify your backup.

c. Select **Backup**.

> You should not rename the backup job created in Windows scheduler or SQL Server agent.

If the policy selected for the on-demand backup is associated with a backup schedule, the on-demand backups will be retained based on the retention settings specified for the schedule type.

An implicit resource group is created. You can view this by selecting respective user or group from the User Access page. The implicit resource group type is “Resource”.

10. Monitor the operation progress by selecting **Monitor** > **Jobs**.

After you finish

- In MetroCluster configurations, SnapCenter might not be able to detect a protection relationship after a failover.

  Unable to detect SnapMirror or SnapVault relationship after MetroCluster failover

- If you are backing up application data on VMDKs and the Java heap size for the SnapCenter Plug-in for VMware vSphere is not large enough, the backup might fail. To increase the Java heap size, locate the script file /opt/netapp/init_scripts/scvservice. In that script, the `do_start method` command starts the SnapCenter VMware plug-in service. Update that command to the following: `Java -jar -Xmx8192M -Xms4096M`.

Related information

Create backup policies for SQL Server databases

Back up resources using PowerShell cmdlets

Backup operations fails with MySQL connection error because of the delay in the TCP_TIMEOUT

Backup fails with Windows scheduler error

Quiesce or grouping resources operations fail

Back up SQL Server resource groups

You can back up a resource group on demand from the Resources page. If a resource group has a policy attached and a schedule configured, then backups occur automatically according to the schedule.

Steps

1. In the left navigation pane, select **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, select **Resource Group** from the **View** list.

   You can search the resource group either by entering the resource group name in the search box, or by selecting **[Filter icon]**, and then selecting the tag. You can then select **[Filter icon]** to close the filter pane.

3. In the Resource Groups page, select the resource group that you want to back up, and then select **Back up Now**.

4. In the Backup page, perform the following steps:
    a. If you have associated multiple policies with the resource group, from the **Policy** drop-down list, select the policy that you want to use for backup.

       If the policy selected for the on-demand backup is associated with a backup schedule, the on-demand backups will be retained based on the retention settings specified for the schedule type.

    b. After backup, select **Verify** to verify the on-demand backup.

       The **Verify** option in the policy applies only to scheduled jobs.

    c. Select **Backup**.
5. Monitor the operation progress by selecting **Monitor** > **Jobs**.

Related information

Create backup policies for SQL Server databases

Create resource groups and attach policies for SQL Server

Back up resources using PowerShell cmdlets

Backup operations fails with MySQL connection error because of the delay in the TCP_TIMEOUT

Backup fails with Windows scheduler error

Monitor backup operations

Monitor SQL resources backup operations in the SnapCenter Jobs page

You can monitor the progress of different backup operations by using the SnapCenterJobs page. You might want to check the progress to determine when it is complete or if there is an issue.

About this task

The following icons appear on the Jobs page and indicate the corresponding state of the operations:

- In progress
- Completed successfully
- Failed
- Completed with warnings or could not start due to warnings
- Queued
- Canceled

Steps

1. In the left navigation pane, click **Monitor**.
2. In the Monitor page, click **Jobs**.
3. In the Jobs page, perform the following steps:

a. Click to filter the list so that only backup operations are listed.
b. Specify the start and end dates.
c. From the **Type** drop-down list, select **Backup**.
d. From the **Status** drop-down, select the backup status.
e. Click **Apply** to view the operations completed successfully.

4. Select a backup job, and then click **Details** to view the job details.

> Though the backup job status displays , when you click on job details you might see that some of the child tasks of the backup operation are still in progress or marked with warning signs.

5. In the Job Details page, click **View logs**.

   The **View logs** button displays the detailed logs for the selected operation.

Monitor data protection operations on SQL resources in the Activity pane

The Activity pane displays the five most recent operations performed. The Activity pane also displays when the operation was initiated and the status of the operation.

The Activity pane displays information regarding backup, restore, clone, and scheduled backup operations.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. Click on the Activity pane to view the five most recent operations.

   When you click one of the operations, the operation details are listed in the **Job Details** page.

Create a storage system connection and a credential using PowerShell cmdlets

You must create a storage virtual machine (SVM) connection and a credential before using PowerShell cmdlets to perform data protection operations.

Before you begin

- You should have prepared the PowerShell environment to execute the PowerShell cmdlets.
- You should have the required permissions in the Infrastructure Admin role to create storage connections.
- You should ensure that the plug-in installations are not in progress.

  Host plug-in installations must not be in progress while adding a storage system connection because the host cache might not be updated and databases status might be displayed in the SnapCenter GUI as “Not available for backup” or “Not on NetApp storage”.

- Storage system names should be unique.

  SnapCenter does not support multiple storage systems with the same name on different clusters. Each storage system that is supported by SnapCenter should have a unique name and a unique management

LIF IP address.

Steps

1. Initiate a PowerShell connection session by using the Open-SmConnection cmdlet.

   This example opens a PowerShell session:

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

2. Create a new connection to the storage system by using the Add-SmStorageConnection cmdlet.

   This example creates a new storage system connection:

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

3. Create a new credential by using the Add-SmCredential cmdlet.

   This example creates a new credential named FinanceAdmin with Windows credentials:

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

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Back up resources using PowerShell cmdlets

You can use the PowerShell cmdlets to backup SQL Server databases or Windows file systems. This would include backing up a SQL Server database or Windows file system includes establishing a connection with the SnapCenter Server, discovering the SQL Server database instances or Windows file systems, adding a policy, creating a backup resource group, backing up, and verifying the backup.

Before you begin

- You must have prepared the PowerShell environment to execute the PowerShell cmdlets.
- You must have added the storage system connection and created a credential.
- You must have added hosts and discovered resources.

Steps

1. Initiate a connection session with the SnapCenter Server for a specified user by using the Open-SmConnection cmdlet.

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

The username and password prompt is displayed.

2. Create a backup policy by using the Add-SmPolicy cmdlet.

   This example creates a new backup policy with a SQL backup type of FullBackup:

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

   This example creates a new backup policy with a Windows file system backup type of CrashConsistent:

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

3. Discover host resources by using the Get-SmResources cmdlet.

   This example discovers the resources for the Microsoft SQL plug-in on the specified host:

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

   This example discovers the resources for Windows file systems on the specified host:

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

4. Add a new resource group to SnapCenter by using the Add-SmResourceGroup cmdlet.

   This example creates a new SQL database backup resource group with the specified policy and resources:

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

   This example creates a new Windows file system backup resource group with the specified policy and resources:

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

5. Initiate a new backup job by using the New-SmBackup cmdlet.

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

6. View the status of the backup job by using the Get-SmBackupReport cmdlet.

   This example displays a job summary report of all jobs that were run on the specified date:

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

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Cancel the SnapCenter Plug-in for Microsoft SQL Server backup operations

You can cancel backup operations that are running, queued, or non-responsive. When you cancel a backup operation, the SnapCenter Server stops the operation and removes all the Snapshots from the storage if the backup created is not registered with SnapCenter Server. If the backup is already registered with SnapCenter Server, it will not roll back the already created Snapshot even after the cancellation is triggered.

Before you begin

- You must be logged in as the SnapCenter Admin or job owner to cancel restore operations.
- You can cancel only the log or full backup operations that are queued or running.
- You cannot cancel the operation after the verification has started.

  If you cancel the operation before verification, the operation is canceled, and the verification operation will not be performed.

- You can cancel a backup operation from either the Monitor page or the Activity pane.
- In addition to using the SnapCenter GUI, you can use PowerShell cmdlets to cancel operations.
- The **Cancel Job** button is disabled for operations that cannot be canceled.
- If you selected **All members of this role can see and operate on other members objects** in Users\Groups page while creating a role, you can cancel the queued backup operations of other members while using that role.

Steps

Perform one of the following actions:

From the…	Action
Monitor page	a. In the left navigation pane, select **Monitor** > **Jobs**. b. Select the job and select **Cancel Job** .
Activity pane	a. After initiating the backup job, select on the Activity pane to view the five most recent operations. b. Select the operation. c. In the Job Details page, select **Cancel Job**.

Result

The operation is canceled, and the resource is reverted to the previous state. If the operation you canceled is non-responsive in the canceling or running state, you should run the `Cancel-SmJob -JobID <int> -Force` cmdlet to forcefully stop the backup operation.

View SQL Server backups and clones in the Topology page

When you are preparing to back up or clone a resource, you might find it helpful to view a graphical representation of all backups and clones on the primary and secondary storage.

About this task

In the Topology page, you can see all of the backups and clones that are available for the selected resource or resource group. You can view the details of those backups and clones, and then select them to perform data protection operations.

You can review the following icons in the **Manage Copies** view to determine whether the backups and clones are available on the primary or secondary storage (Mirror copies or Vault copies).

- displays the number of backups and clones that are available on the primary storage.
- displays the number of backups and clones that are mirrored on the secondary storage using SnapMirror technology.
- displays the number of backups and clones that are replicated on the secondary storage using SnapVault technology.
  - The number of backups displayed includes the backups deleted from the secondary storage.

    For example, if you created 6 backups using a policy to retain only 4 backups, the number of backups displayed is 6.

Clones of a backup of a version-flexible mirror on a mirror-vault type volume are displayed in the topology view, but the mirror backup count in the topology view does not include the version-flexible backup.

If you have secondary relationship as SnapMirror Business Continuity (SM-BC), you can see following additional icons:

-  implies that the replica site is up.
-  implies that the replica site is down.
-  implies that the secondary mirror or vault relationship has not been re-established.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, either select the resource or resource group from the **View** drop-down list.
3. Select the resource either from the resource details view or from the resource group details view.

   If the resource selected is a cloned database, protect the cloned database, source of the clone is displayed in the Topology page. Click **Details** to view the backup used to clone.

   If the resource is protected, the Topology page of the selected resource is displayed.

4. Review the Summary card to see a summary of the number of backups and clones available on the primary and secondary storage.

   The **Summary Card** section displays the total number of backups and clones.

   Clicking the **Refresh** button starts a query of the storage to display an accurate count.

   If SnapLock enabled backup is taken, then clicking the **Refresh** button refreshes the primary and secondary SnapLock expiry time retrieved from ONTAP. A weekly schedule also refreshes the primary and secondary SnapLock expiry time retrieved from ONTAP.

   When the application resource is spread across multiple volumes, the SnapLock expiry time for the backup will be the longest SnapLock expiry time that is set for a Snapshot in a volume. The longest SnapLock expiry time is retrieved from ONTAP.

   For SnapMirror Business Continuity (SM-BC), clicking the **Refresh** button refreshes the SnapCenter backup inventory by querying ONTAP for both primary and replica sites. A weekly schedule also performs this activity for all databases containing SM-BC relationship.

   - For SM-BC, Async Mirror, Vault, or MirrorVault relationships to the new primary destination should be manually configured after failover.
   - After failover, a backup should be created for SnapCenter to be aware of the failover. You can click **Refresh** only after a backup has been created.

5. In the **Manage Copies** view, click **Backups** or **Clones** from the primary or secondary storage to see details of a backup or clone.

   The details of the backups and clones are displayed in a table format.

6. Select the backup from the table, and then click the data protection icons to perform restore, clone, rename, and delete operations.

   You cannot rename or delete backups that are on the secondary storage.

7. Select a clone from the table and click **Clone Split**.
8. If you want to delete a clone, select the clone from the table, and then click .

Remove backups using PowerShell cmdlets

You can use the Remove-SmBackup cmdlet to delete backups if you no longer require them for other data protection operations.

You must have prepared the PowerShell environment to execute the PowerShell cmdlets.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Steps

1. Initiate a connection session with the SnapCenter Server for a specified user by using the Open-SmConnection cmdlet.

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

2. Delete one or more backup using the Remove-SmBackup cmdlet.

   This example deletes two backups using their backup IDs:

```
Remove-SmBackup -BackupIds 3,4
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Clean up the secondary backup count using PowerShell cmdlets

You can use the Remove-SmBackup cmdlet to clean up the backup count for secondary backups that have no Snapshot. You might want to use this cmdlet when the total Snapshots displayed in the Manage Copies topology do not match the secondary storage Snapshot retention setting.

You must have prepared the PowerShell environment to execute the PowerShell cmdlets.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be

obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Steps

1. Initiate a connection session with the SnapCenter Server for a specified user by using the Open-SmConnection cmdlet.

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

2. Clean up secondary backups count using the -CleanupSecondaryBackups parameter.

   This example cleans up the backup count for secondary backups with no Snapshots:

```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Copyright information

Trademark information