NetApp

Protect Microsoft SQL Server databases

SnapCenter software

NetApp
August 29, 2025

Table of Contents

Protect Microsoft SQL Server databases

Add hosts and install SnapCenter plug-in for SQL Server database

SnapCenter supports data protection of SQL instances on SMB shares on Azure NetApp Files. The standalone and availability group (AG) configurations are supported.

You must use the SnapCenter Add Host page to add hosts, and then install the plug-ins package. The plug-ins are automatically installed on the remote hosts.

Before you begin

- You must be a user that is assigned to a role that has the plug-in install and uninstall permissions, such as the SnapCenter Admin role.
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in, or if the user belongs to a local workgroup user, you must disable UAC on the host.

Steps

1. In the left navigation pane, select **Hosts**.
2. Verify that the **Managed Hosts** tab is selected at the top.
3. Select **Add**.
4. In the Hosts page do the following:
    a. In the Host Type field, select the host type.
    b. In the Host name field, enter the fully qualified domain name (FQDN) or the IP address of the host.
    c. In the Credentials field, enter the credential that you created.
5. In the **Select Plug-ins to Install** section, select the plug-ins to install.
6. (Optional) Click **More Options** and specify the details.
7. Select **Submit**.
8. Select **Configure log directory** and in the Configure host log directory page, enter the SMB path of the host log directory, and click **Save**.
9. Click **Submit** and monitor the installation progress.

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.

Steps

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

5. In the Policy type page, perform the following steps:

    a. Select **Azure NetApp Files** as the storage type.

    b. Select the backup type.

        i. Select **Full Backup and Log Backup** if you want to back up database files and transaction logs.

        ii. Select **Full Backup** if you want to back up only the database files.

        iii. Select **Log Backup** if you want to back up only the transaction logs.

        iv. Select **Copy Only Backup** if you want to back up your resources by using another application.

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

        i. Select Backup on preferred backup replica if you want to back up only on the replica.

        ii. Select primary AG replica or the secondary AG replica for the backup.

        iii. Select the backup priority.

6. In the Snapshot and backup page, perform the following steps:

    a. Select the frequency of the scheduled backup.

    b. Specify the retention settings depending on the backup type selected.

    c. If you want to enable Azure NetApp Files backup, select **Enable backup** and specify the retention settings.

7. In the Verification page, perform the following steps:

    a. In the Run verification for following backup schedules section, select the schedule frequency.

    b. In the Database consistency check options section, perform the following actions:

        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.

        ii. Select **Suppress all information messages (NO_INFOMSGS)** to suppress all informational messages.

        Selected by default.

        iii. Select **Display all reported error messages per object (ALL_ERRORMSGS)** to display all the reported errors per object.

        iv. 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.

        v. 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.

    c. In the **Log Backup** section, select **Verify log backup upon completion** to verify the log backup upon completion.

    d. 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.

8. Review the summary and click **Finish**.

Create resource groups and attach SQL backup policies

A resource group is the container to which you must add resources that you want to back up and protect.

A resource group enables you to back up all 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.

Steps

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

2. In the Resources page, click **New Resource Group**.

3. In the Name page, perform the following actions:

For this field…	Do this…
Name	Enter a name for the resource group.
Tags	Enter one or more labels that will help you later search for the resource group.
Use custom name format for Snapshot copy	Select this check box, and enter a custom name format that you want to use for the Snapshot name.

4. In the Resources page, select a host name from the **Host** drop-down list and resource type from the **Resource Type** drop-down list.

5. 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.

    b. In the Configure Schedules column, click ➕ for the policy you want to configure.

    c. In the Add schedules for policy *policy_name* dialog box, configure the schedule, and then click **OK**.

    d. Select the Microsoft SQL Server scheduler.

7. In the Verification page, perform the following steps:

    a. Select the verification server.

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

    c. Either select **Run verification after backup** or **Run scheduled verification**.

    d. Click **OK**.

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

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

Back up SQL Server databases running on Azure NetApp Files

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

Before you begin

You should create a load balancer, if the Azure Windows Failover Cluster does not have a cluster IP assigned or if it is not reachable from SnapCenter. The load balancer's IP should be configured and reachable from the SnapCenter Server.

Steps

1. In the left navigation pane, select **Resources**, and then select the appropriate plug-in from the list.

2. In the Resource page, select **Database**, **Instance**, or **Availability Group** from the View drop-down list.

3. In the Resource page, select **Use custom name format for Snapshot copy**, and then enter a custom name format that you want to use for the Snapshot name.

4. In the Policies page, perform the following steps:

   a. Select one or more policies from the drop-down list.

   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**.

      policy_name is the name of the policy that you selected.

   d. Select **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.

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

   c. Either select **Run verification after backup** or **Run scheduled verification**.

   d. Click OK.

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

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

8. Select **Back up Now**.

9. In the Backup page, perform the following steps:

   a. If multiple policies are associated with the resource, from the **Policy** drop-down list, select the policy that you want to use for backup.

   b. Select **Verify after backup**.

   c. Select **Backup**.

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

Back up SQL Server resource groups

You can back up the resource groups that consist of multiple resources. A backup operation on the resource group is performed on all resources defined in the resource group.

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.

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 multiple policies are associated with the resource group, from the **Policy** drop-down list, select the policy that you want to use for backup.

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

   c. Select **Backup**.

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

Restore and recover SQL Server databases

You can use SnapCenter to restore backed-up SQL Server databases. Database restoration is a multiphase process that copies all the data and log pages from a specified SQL Server backup to a specified database.

About this task

You should ensure that the target instance for restore is configured with an active directory user who belongs to the SMB ADactive directory domain and has permissions to set the file permissions appropriately. You should configure the credentials in SnapCenter at instance level.

The SQL authentication for target instance will not be supported for SMB configurations. The target instance should be configured in SnapCenter with the active directory user having the required permissions.

If the SnapCenter Plug-in services service account is not an active directory user then while performing restore to alternate host, the user who have the full control over the source volumes is required so that it can be impersonated and perform the required operation.

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 either **Database** or **Resource Group** from the View list.

3. Select the database or the resource group from the list.

4. From the Manage Copies view, select **Backups** from storage system.

5. Select the backup from the table, and then click the icon.

6. In the Restore Scope page, select one of the following options:

   a. Select **Restore the database to the same host where the backup was created** if you want to restore the database to the same SQL server where the backups are taken.

b. Select **Restore the database to an alternate host** if you want the database to be restored to a different SQL server in the same or different host where backups are taken.

7. In the Recovery Scope page, select one of the following options:

    a. Select **None** when you need to restore only the full backup without any logs.

    b. Select **All log backups** up-to-the-minute backup restore operation to restore all the available log backups after the full backup.

    c. Select **By log backups** to perform a point-in-time restore operation, which restores the database based on backup logs until the backup log with the selected date.

    d. Select **By specific date until** to specify the date and time after which transaction logs are not applied to the restored database.

    e. If you have selected **All log backups**, **By log backups**, or **By specific date until** and the logs are located at a custom location, select **Use custom log directory**, and then specify the log location.

8. In the Pre-Ops and Post Ops page, specify the required details.

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

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

11. Monitor the restore process by using the **Monitor** > **Jobs** page.

Clone SQL Server database backup

You can use SnapCenter to clone a SQL database using the backup of the database. The clones created are thick clones and are created on the parent capacity pool.

About this task

You should ensure that the target instance for clone is configured with an active directory user who belongs to the SMB ADactive directory domain and has permissions to set the file permissions appropriately. You should configure the credentials in SnapCenter at instance level.

The SQL authentication for target instance will not be supported for SMB configurations. The target instance should be configured in SnapCenter with the active directory user having the required permissions.

If the SnapCenter Plug-in services service account is not an active directory user then while performing clone, the user who have the full control over the source volumes is required so that it can be impersonated and perform the required operation.

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 either **Database** or **Resource Group** from the **View** list.

3. Select the database or resource group.

4. From the **Manage Copies** view page, select the backup from primary storage system.

5. Select the backup, and then select .

6. In the **Clone Options** page, provide all the required details.

7. In the Location page, select a storage location to create a clone.

    If the SQL Server database ANF volumes are configured in a manual QOS capacity pool, specify the QOS

for the cloned volumes.

If QOS for the cloned volumes is not specified, the QOS of the source volume will be used. If the automatic QOS capacity pool is used, the QOS value specified will be ignored.

8. In the Logs page, select one of the following options:

    a. Select **None** if you want to clone only the full back up without any logs.

    b. Select **All log backups** if you want to clone all the available log backups dated after the full backup.

    c. Select **By log backups until** if you want to clone the database based on the backup logs that were created up to the backup log with the selected date.

    d. Select **By specific date until** if you do not want to apply the transaction logs after the specified date and time.

9. In the **Script** page, enter the script timeout, path, and the arguments of the prescript or postscript that should be run before or after the clone operation, respectively.

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

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

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

Perform Clone Lifecycle

Using SnapCenter, you can create clones from a resource group or database. You can either perform on-demand clone or you can schedule recurring clone operations of a resource group or database. If you clone a backup periodically, you can use the clone to develop applications, populate data, or recover data.

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 either **Database** or **Resource Group** from the **View** list.

3. Select the database or resource group.

4. From the **Manage Copies** view page, select the backup from primary storage system.

5. Select the backup, and then select .

6. In the **Clone Options** page, provide all the required details.

7. In the Location page, select a storage location to create a clone.

    If the SQL Server database ANF volumes are configured in a manual QOS capacity pool, specify the QOS for the cloned volumes.

    If QOS for the cloned volumes is not specified, the QOS of the source volume will be used. If the automatic QOS capacity pool is used, the QOS value specified will be ignored.

8. In the **Script** page, enter the script timeout, path, and the arguments of the prescript or postscript that should be run before or after the clone operation, respectively.

9. In the Schedule page, perform one of the following actions:

    ◦ Select **Run now** if you want to execute the clone job immediately.

    ◦ Select **Configure schedule** when you want to determine how frequently the clone operation should occur, when the clone schedule should start, on which day the clone operation should occur, when the

schedule should expire, and whether the clones must be deleted after the schedule expires.

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

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

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