Back up Exchange resources

SnapCenter Software 4.7

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/us-en/snapcenter-47/protect-sce/concept_back_up_exchange_resources.html on September 26, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Back up Exchange resources . . . 1
- Backup workflow . . . 1
- Exchange database and backup verification . . . 1
- Determine whether Exchange resources are available for backup . . . 2
- Create backup policies for Exchange Server databases . . . 3
- Create resource groups and attach policies for Exchange Servers . . . 9
- Back up Exchange databases . . . 12
- Back up Exchange resources groups . . . 14
- Create a storage system connection and a credential using PowerShell cmdlets for Exchange Server . . . 15
- Back up Exchange resources using PowerShell cmdlets . . . 16
- Monitor backup operations . . . 18
  - Monitor operations in the Activity pane . . . 19
- Cancel backup operations for Exchange database . . . 19
- Remove Exchange backups using PowerShell cmdlets . . . 20
- View Exchange backups in the Topology page . . . 21

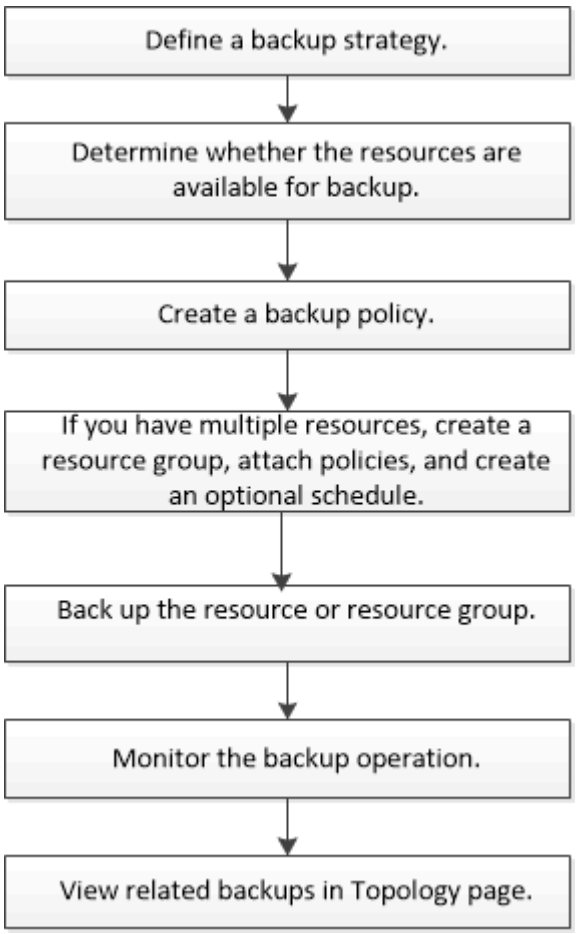
Back up Exchange resources

Backup workflow

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

You can schedule multiple backups to run across servers simultaneously. Backup and restore operations cannot be performed simultaneously on the same resource. Active and passive backup copies on the same volume are not supported.

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



Exchange database and backup verification

SnapCenter Plug-in for Microsoft Exchange Server does not provide backup verification; however, you can use the Eseutil tool provided with Exchange to verify Exchange databases and backups.

The Microsoft Exchange Eseutil tool is a command line utility that is included with your Exchange server. The utility enables you to perform consistency checks to verify the integrity of Exchange databases and backups.

Best Practice: It is not necessary to perform consistency checks on databases that are part of a Database Availability Group (DAG) configuration with at least two replicas.

For additional information, see Microsoft Exchange Server documentation.

Determine whether Exchange resources are available for backup

Resources are the databases, Exchange Database Availability Groups 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.

What you will need

- You must have already completed tasks such as installing SnapCenter Server, adding hosts, creating storage system connections, adding credentials, and installing Plug-in for Exchange.
- To take advantage of Single Mailbox Recovery software features, you must have located your active database on the Exchange Server where Single Mailbox Recovery software is installed.
- If databases reside on VMware RDM LUNs, you must deploy the SnapCenter Plug-in for VMware vSphere and register the plug-in with SnapCenter. The SnapCenter Plug-in for VMware vSphere documentation has more information.

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 in mount, unmount, reseed, or recovery pending state.
- If you have a Database Availability Group (DAG), you can back up all databases in the group by running the backup job from the DAG.

Steps

1. In the left navigation pane, click **Resources**, and then select **Microsoft Exchange Server** from the plug-ins drop-down list located in the upper left corner of the Resources page.
2. In the Resources page select **Database**, or **Database Availability Group**, or **Resource Group**, from the **View** drop-down list.

   All the databases and DAGs are displayed with their DAG or hostnames in FQDN format, so you can distinguish between multiple databases.

   Click and select the host name and the Exchange Server 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 name, Database Availability Group name, server in which the database is currently active, server with copies, time of last backup, and overall status.

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

     In a DAG, if the active database copy is on non-NetApp storage and if at least one passive database copy is on NetApp storage, Not protected is displayed in the **Overall Status** column.

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

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

Create backup policies for Exchange Server databases

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

What you will need

- You must have defined your data protection strategy.

  For details, see the information about defining a data protection strategy for Exchange databases.

- 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 refreshed (discovered) the Exchange Server resources.
- If you are replicating Snapshot copies 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.
- 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

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 script settings. Specifying options in a policy saves time when you want to reuse the policy for another resource group.
- Full backup retention is specific to a given policy. A database or resource using policy A with a full backup retention of 4 retains 4 full backups and has no effect on policy B for the same database or resource, which might have a retention of 3 to retain 3 full backups.
- Log backup retention is effective across policies, and applies to all log backups for a database or resource. Therefore, when a full backup is performed using policy B, the log retention setting affects log backups created by policy A on the same database or resource. Similarly, the log retention setting for policy A affects log backups created by policy B on the same database.
- 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.

Best Practice: It's best that you configure the secondary retention policy based on the number of full and log backups, overall, that you want to retain. When you configure secondary retention policies, keep in mind that when databases and logs that are in different volumes, each backup can have three Snapshot copies, and when databases and logs are in the same volume, each backup can have two Snapshot copies.

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 Backup Type page, perform the following steps:
   a. Choose backup type:

If you want to…	Do this…
Back up the database files and the required transaction logs	Select **Full backup and Log backup**. Databases are backed up with log truncation, and all logs are backed up, including the truncated logs. This is the recommended backup type.

If you want to…	Do this…
Back up the database files and the uncommitted transaction logs	Select **Full backup**. Databases are backed up with log truncation, and truncated logs are not backed up.
Back up all the transaction logs	Select **Log backup**. All transaction logs on the active file system are backed up, and there is no log truncation. A *scebackupinfo* directory is created on the same disk as the live log. This directory contains the pointer to the incremental changes for the Exchange database and it is not equivalent to the complete log files.
Back up all database files and transaction logs without truncating the transaction log files	Select **Copy Backup**. All databases and all logs are backed up, and there is no log truncation. You typically use this backup type for reseeding a replica or for testing or diagnosing a problem.

ⓘ You should define the space required for log backups based on the full backup retention and not based on Up-to-the-minute (UTM) retention.

ⓘ Create separate vault policies for logs and databases when dealing with Exchange volumes (LUNs), and set the keep (retention) for the log policy to twice the number for each label as the database policy, using the same labels. For more information see, SnapCenter for Exchange Backups only keep half the Snapshots on the Vault destination log volume.

b. In the Database Availability Group Settings section, select an action:

For this field…	Do this…
Back up active copies	Select this option to back up only the active copies of the selected database. For database availability groups (DAGs), this option backs up only active copies of all databases in the DAG. Passive copies are not backed up.

For this field…	Do this…
Back up copies on servers to be selected at backup job creation time	Select this option to back up any copies of the databases on the selected servers, both active and passive. For DAGs, this option backs up both active and passive copies of all databases on the selected servers.

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 cluster changes, the backups of the previous owner node will be retained. The retention is applicable only at the node level.

c. In the Schedule frequency section, select one or more of the frequency types: **On demand**, **Hourly**, **Daily**, **Weekly**, and **Monthly**.

You can specify the schedule (start date, end date) for backup operations 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).

6. In the Retention page, configure the retention settings.

The options displayed depend upon the backup type and frequency type you previously selected.

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.

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 copy is the reference Snapshot copy for the SnapVault relationship until a newer Snapshot copy is replicated to the target.

a. In the Log backups retention settings section, select one of the following:

If you want to…	Do this…
Retain only a specific number of log backups	Select **Number of full backups for which logs are retained**, and specify the number of full backups for which you want up-to-the-minute restorability. Up-to-the-minute (UTM) retention applies to log backup created via full or log backup. 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. The log folders created as part of full and log backups are automatically deleted as part of UTM. You cannot delete the log folders manually. For example, if the retention setting of full or full and log backup is set for 1 month and UTM retention is set to 10 Days, then the log folder created as part of these backups will be deleted as per UTM. As a result, only 10 days log folders will be there and all other backups are marked for point-in-time restore. You can set UTM retention value as 0, if you do not want to perform up-to-the-minute restore. This will enable point-in-time restore operation. **Best Practice:** It's best that the setting must be equal to the setting for Total Snapshot copies (full backups) in the Full backup retention settings section. This ensures that log files are retained for each full backup.
Retain the backup copies for a specific number of days	Select the **Keep log backups for last** option, and specify the number of days to keep the log backup copies. The log backups up to the number of days of full backups are retained.

If you selected **Log backup** as the backup type, log backups are retained as part of the up-to-the-minute retention settings for full backups.

b. In the Full backup retention settings section, select one of the following for on-demand backups, and then select one for full backups:

For this field…	Do this…
Retain only a specific number of Snapshot copies	If you want to specify the number of full backups to keep, select the **Total Snapshot copies to keep** option, and specify the number of Snapshot copies (full backups) to retain. If the number of full backups exceeds the specified number, the full backups that exceed the specified number are deleted, with the oldest copies deleted first.
Retain full backups for a specific number of days	Select the **Keep Snapshot copies for** option, and specify the number of days to keep Snapshot copies (full backups).

If you have a database with only log backups and no full backups on a host in a DAG configuration, the log backups are retained in the following ways:

- By default, SnapCenter finds the oldest full backup for this database in all the other hosts in the DAG, and deletes all log backups on this host that were taken before the full backup.
- You can override the above default retention behavior for a database on a host in a DAG with only log backups by adding the key **MaxLogBackupOnlyCountWithoutFullBackup** in the *C:\Program Files\NetApp\SnapCenter WebApp\web.config* file.

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

In the example, the value 10 means you keep up to 10 log backups on the host.

7. In the Replication page, select one or both of the following secondary replication options:

For this field…	Do this…
Update SnapMirror after creating a local Snapshot copy	Select this option to keep mirror copies of backup sets on another volume (SnapMirror).
Update SnapVault after creating a local Snapshot copy	Select this option to perform disk-to-disk backup replication.

For this field…	Do this…
Secondary policy label	Select a Snapshot label. Depending on the Snapshot copy label that you select, ONTAP applies the secondary Snapshot copy 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	Enter the number of replication attempts that should occur before the process halts.

You should configure SnapMirror retention policy in ONTAP for the secondary storage to avoid reaching the maximum limit of Snapshot copies on the secondary storage.

8. 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.
   - Prescript backup arguments include “$Database” and “$ServerInstance”.
   - Postscript backup arguments include “$Database”, “$ServerInstance”, “$BackupName”, “$LogDirectory”, and “$LogSnapshot”.

     You can run a script to update SNMP traps, automate alerts, send logs, and so on.

     The prescripts or postscripts path should not include drives or shares. The path should be relative to the SCRIPTS_PATH.
9. Review the summary, and then click **Finish**.

Create resource groups and attach policies for Exchange Servers

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 and the protection schedule.

About this task

- 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.

Steps

1. In the left navigation pane, click **Resources**, and then select the Microsoft Exchange Server 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 copy name and format. For example, *customtext_resourcegroup_policy_hostname* or *resourcegroup_hostname*. By default, a timestamp is appended to the Snapshot copy name.

5. In the Resources page, perform the following steps:

   a. Select the resource type and the Database Availability Group from drop-down lists to filter the list of available resources.

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

   In the Available Resources and Selected Resources sections, the database name is displayed with the FQDN of the host. This FQDN only indicates that the database is active on that specific host and might not take backup on this host. You should select one or more backup servers from the Server selection option,

where you want to take backup in case you have selected the **Back up copies on servers to be selected at backup job creation time** option in the policy.

a. Type the name of the resource in the search text box, or scroll to locate a resource.

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.

  Resource groups of SnapCenter for Microsoft Exchange Server cannot have more than 30 databases per Snapshot copy. If there are more than 30 databases in one resource group, a second Snapshot copy is created for the additional databases. Therefore, 2 sub jobs are created under the main backup job. For backups having secondary replication, while SnapMirror or SnapVault update is in progress, there could be scenarios where the update for both the sub-jobs overlap. The main backup job keeps on running forever even if the logs indicate that the job is completed.

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 + .

If a policy contains the **Back up copies on servers to be selected at backup job creation time** option, a server selection option is displayed to select one or more servers. The server selection option will list only the server where the selected database is on NetApp storage.

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.

Third party backup schedules are not supported when they overlap with SnapCenter backup schedules.

7. 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`.

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.

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

Back up Exchange databases

If a database is not part of any resource group, you can back up the database or Database Availability Group from the Resources page.

What you will need

- You must have created a backup policy.
- You must have assigned the aggregate that is being used by the backup operation to the SVM used by the database.
- If you want to back up a resource that has a SnapMirror relationship with a secondary storage, the 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.
- If you want to perform backup of a Database or a Database Availability Group which has active/passive database copy on a NetApp and non-NetApp storage, and you have selected **Back up active copies** or **Back up copies on servers to be selected during backup job creation time** option in the policy, then the backup jobs will go in to warning state. The backup will succeed for active/passive database copy on NetApp storage and backup will fail for active/passive database copy on non-NetApp storage.

Best Practice: Do not run backups of active and passive databases at the same time. A race condition can occur and one of the backups might fail.

Steps

1. In the left navigation pane, click **Resources**, and then select the **Microsoft Exchange Server plug-in** from the list.
2. In the Resources page, select either **Database**, or **Database Availability Group** from the **View** list.

   In the Resources page, the icon indicates that the database is on non-NetApp storage.

   In a DAG, If an active database copy is on a non-NetApp storage and at least one passive database copy resides on a NetApp storage, then you can protect the database.

   Click , and then select the host name and the database type to filter the resources. You can then click to close the filter pane.

   - If you want to back up a database, click on the database name.
     i. If the Topology view is displayed, click **Protect**.
     ii. If the Database - Protect Resource wizard is displayed, continue to Step 3.
   - If you want to back up a Database Availability Group, click on the Database Availability Group name.
3. If you want to specify a custom Snapshot copy name, in the Resources page, select the **Use custom name format for Snapshot copy** check box, and then enter a custom name format that you want to use

for the Snapshot copy name.

For example, *customtext_policy_hostname* or *resource_hostname*. By default, a timestamp is appended to the Snapshot copy name.

4. 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 + .

   If a policy contains the **Back up copies on servers to be selected at backup job creation time** option, a server selection option is displayed to select one or more servers. The server selection option will list only the server where the selected database is on a NetApp storage.

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

   a. Click + in the Configure Schedules column for the policy for which you want to configure a schedule.

   b. In the Add schedules for policy *policy_name* window, configure the schedule, and then click **OK**.

      Where, *policy_name* is the name of the policy that you have selected.

      The configured schedules are listed in the Applied Schedules column.

5. 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 backup operation performed on the resource, select **Attach Job Report**.

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

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

   The database topology page is displayed.

7. Click **Back up Now**.

8. 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. Click **Backup**.

9. Monitor the backup's progress by double-clicking the job in the Activity pane at the bottom of the page to display the Job Details page.

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

  For information, see: 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*

Back up Exchange resources groups

A resource group is a collection of resources on a host or Exchange DAG, and the resource group can include either a whole DAG or individual databases. You can backup the resources groups from the Resources page.

What you will need

- You must have created a resource group with a policy attached.
- You must have assigned the aggregate that is being used by the backup operation to the storage virtual machine (SVM) used by the database.
- If you want to back up a resource that has a SnapMirror relationship with a secondary storage, the 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.
- If a resource group has multiple databases from different hosts, the backup operation on some of the hosts might start late because of network issues. You should configure the value of `MaxRetryForUninitializedHosts` in `web.config` by using the `Set-SmConfigSettings` PowerShell cmdlet.
- In a resource group, if you include a Database or Database Availability Group which has active/passive database copy on a NetApp and non-NetApp storage, and you have selected **Back up active copies** or **Back up copies on servers to be selected during backup job creation time** option in the policy, then the backup jobs will go into warning state.

  The backup will succeed for active/passive database copy on NetApp storage and backup will fail for active/passive database copy on non-NetApp storage.

About this task

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, click **Resources**, and then select the **Microsoft Exchange Server 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

clicking , and then selecting the tag. You can then click to close the filter pane.

3. In the Resource Groups page, select the resource group that you want to back up, and then click **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. Click **Backup**.
5. Monitor the backup's progress by double-clicking the job in the Activity pane at the bottom of the page to display the Job Details page.

Create a storage system connection and a credential using PowerShell cmdlets for Exchange Server

You must create a storage virtual machine (SVM) connection and a credential before using PowerShell cmdlets to back up and restore.

What you will need

- 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 data 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 -SVM test_vs1 -Protocol Https
-Timeout 60
```

3. Create a new Run As account by using the `Add-Credential` cmdlet.

   This example creates a new Run As account named ExchangeAdmin with Windows credentials:

```
PS C:> Add-SmCredential -Name ExchangeAdmin -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 Exchange resources using PowerShell cmdlets

Backing up an Exchange Server database includes establishing a connection with the SnapCenter Server, discovering the Exchange Server database, adding a policy, creating a backup resource group, backing up, and viewing the backup status.

What you will need

- 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.

Plug-in for Exchange does not support clone operations; therefore, the CloneType parameter for the Add-SmPolicy cmdlet is not supported for Plug-in for Exchange

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 full backup and log backup Exchange backup type:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies
```

This example creates a new backup policy with an hourly full backup and log backup Exchange backup type:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Hourly_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies -ScheduleType Hourly
-RetentionSettings
@{'BackupType'='DATA';'ScheduleType'='Hourly';'RetentionCount'='10'}
```

This example creates a new backup policy to back up only Exchange logs:

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

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

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

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

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

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

```
C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
-Description 'Backup ResourceGroup with Full and Log backup policy'
-PluginCode SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bk
p_Policy -Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange
Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-
w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

   This example creates a new Exchange Database Availability Group (DAG) backup resource group with the specified policy and resources:

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description
'Backup ResourceGroup with Full and Log backup policy' -PluginCode SCE
-Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bk
p_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database Availability
Group";"Names"="DAGSCE0102"}
```

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

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

This example creates a new backup to secondary storage:

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

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:

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

This example displays a job summary report for a specific job ID:

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

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, see SnapCenter Software Cmdlet Reference Guide.

Monitor backup operations

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 operations 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. If you are using Plug-in for SQL Server or Plug-in for Exchange Server, the Activity pane also displays information about the reseed operation.

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.

Cancel backup operations for Exchange database

You can cancel backup operations that are queued.

What you will need

- You must be logged in as the SnapCenter Admin or job owner to cancel operations.
- You can cancel a backup operation from either the **Monitor** page or the **Activity** pane.
- You cannot cancel a running backup operation.
- You can use the SnapCenter GUI, PowerShell cmdlets, or CLI commands to cancel the backup 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

1. Perform one of the following actions:

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

The operation is canceled, and the resource is reverted to the previous state.

Remove Exchange backups using PowerShell cmdlets

You can use the Remove-SmBackup cmdlet to delete Exchange 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"):
```

View Exchange backups in the Topology page

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

About this task

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

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

- displays the number of backups that are available on the primary storage.
- displays the number of backups that are mirrored on the secondary storage using SnapMirror technology.
- displays the number of backups 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.

Best Practice: To ensure the correct number of replicated backups is displayed, we recommend that you refresh the topology.

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 the database, or the resource, or the resource group from the **View** drop-down list.

3. Select the resource either from the database details view or from the resource group details view.

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

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

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

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

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

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

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

   You cannot rename or delete backups that are on the secondary storage. Deleting Snapshot copies is handled by ONTAP retention settings.

Copyright information

Copyright © 2025 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.