SnapCenter® Software 4.2

Data Protection Guide

For Microsoft® Exchange Server

October 2019 | 215-14391_2019-10_en-us
doccomments@netapp.com

Updated for 4.2.1

NetApp®

Contents

Deciding whether to read the SnapCenter Data Protection Guide for Microsoft Exchange Server

This information describes how to use SnapCenter to perform backup and restore operations on Microsoft Exchange Server resources.

You should read this information if you want to use SnapCenter in the following ways:

- You want to create data protection policies and resource groups for Exchange Server resources
- You want to perform backup, or restore operations on Exchange Server resources using the graphical user interface (GUI)
- You want to perform backup or restore operations on Exchange Server resources using Windows cmdlets

You should have already performed the following tasks:

- Installed SnapCenter Server and the SnapCenter Plug-in for Microsoft Exchange Server
- Configured role-based access control (RBAC), storage system connections, and credentials
- Deployed the NetApp Data Broker virtual appliance, enabled the SnapCenter Plug-in for VMware vSphere, and registered the plug-in with SnapCenter, if you want to protect Exchange Server data on virtual machines. The NetApp Data Broker, SnapCenter Plug-in for VMware vSphere, documentation has more information.
  Deployment Guide for SnapCenter Plug-in for VMware vSphere
- Set up SnapMirror and SnapVault relationships, if you want backup replication

You can also use the following information to help accomplish your data protection goals:

- SnapCenter Server and plug-in installation and setup
  Installing and setting up SnapCenter
  Getting Started
- SnapCenter concepts, including architecture, features, and benefits
  Concepts
- Other SnapCenter Data Protection Guides for specific types of resources, such as Microsoft SQL Server, Oracle, Windows file systems, and custom plug-ins
- SnapCenter PowerShell cmdlets
  SnapCenter Software 4.2 Windows Cmdlet Reference Guide
- SnapCenter administration, including dashboards, reporting capabilities, and REST APIs, and managing licenses, storage connections, and the SnapCenter Server repository
  Performing administrative tasks
- The SnapCenter 4.1.1 documentation has information on protecting virtualized databases and file systems using the SnapCenter 4.1.1 Plug-in for VMware vSphere. The NetApp Data Broker, SnapCenter Plug-in for VMware vSphere, documentation has information on protecting virtualized databases and file systems using the Linux-based NetApp Data Broker virtual appliance (Open Virtual Appliance format) for SnapCenter 4.2.
  Data Protection Guide for VMs, Datastores, and VMDKs using the SnapCenter Plug-in for VMware vSphere

SnapCenter Plug-in for Microsoft Exchange Server overview

The SnapCenter Plug-in for Microsoft Exchange Server is a host-side component of the NetApp SnapCenter Software that enables application-aware data protection management of Exchange databases. The Plug-in for Exchange automates the backup and restore of Exchange databases in your SnapCenter environment.

When the Plug-in for Exchange is installed, you can use SnapCenter with NetApp SnapMirror technology to create mirror copies of backup sets on another volume and with NetApp SnapVault technology to perform disk-to-disk backup replication for standards compliance or archival purposes.

The Data Protection Guide for your plug-in has information about data protection operations.

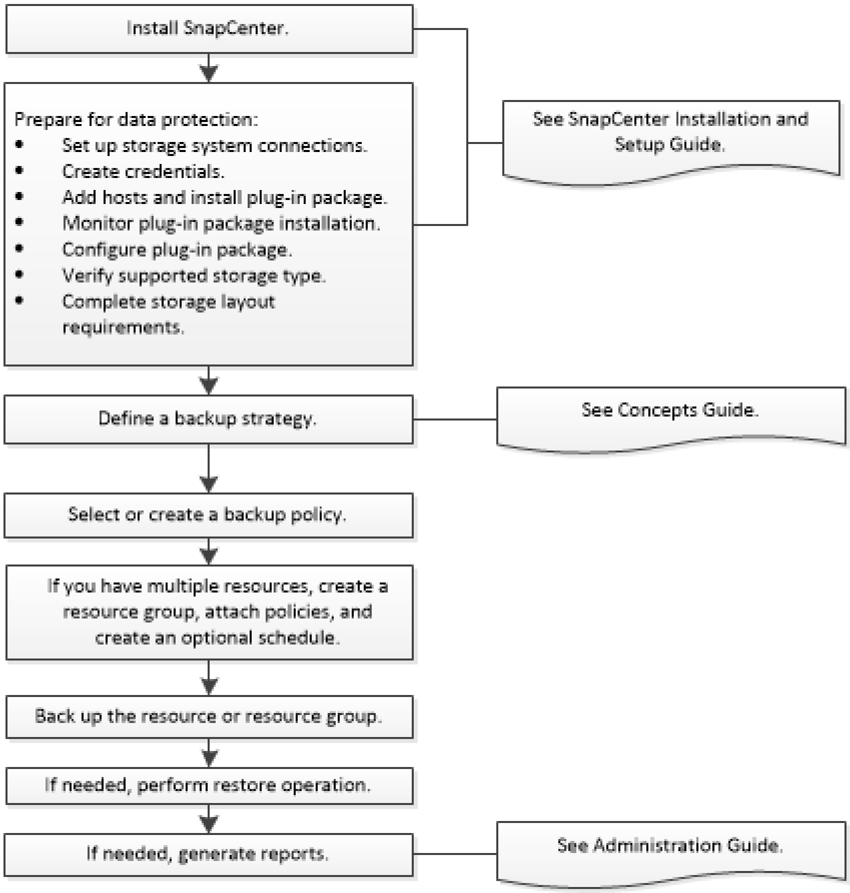
The SnapCenter concepts documentation has information about the SnapCenter architecture, features, and benefits.

Related information

Concepts
Installing and setting up SnapCenter

Data protection workflow for Microsoft Exchange Server

The data protection workflow lists the tasks that you must perform for data protection.


Install SnapCenter.
Prepare for data protection:
• Set up storage system connections.
• Create credentials.
• Add hosts and install plug-in package.
• Monitor plug-in package installation.
• Configure plug-in package.
• Verify supported storage type.
• Complete storage layout requirements.
See SnapCenter Installation and Setup Guide.
Define a backup strategy.
See Concepts Guide.
Select or create a backup policy.
If you have multiple resources, create a resource group, attach policies, and create an optional schedule.
Back up the resource or resource group.
If needed, perform restore operation.
If needed, generate reports.
See Administration Guide.

Related concepts

Backing up Exchange resources on page 14

Related references

Restoring Exchange resources on page 28

Related information

Installing and setting up SnapCenter
Concepts
Performing administrative tasks

Preparing for data protection

Before performing any data protection operation such as backup or restore operations, you must define your strategy and set up the environment. You can also set up the SnapCenter Server to use SnapMirror and SnapVault technology.

To take advantage of SnapVault and SnapMirror technology, you must configure and initialize a data protection relationship between the source and destination volumes on the storage device. You can use ONTAP System Manager or you can use the storage console command line to perform these tasks.

Related references

Prerequisites for using the SnapCenter Plug-in for Microsoft Exchange Server on page 8

Exchange Server privileges required on page 9

Storage types supported by SnapCenter Plug-in for Microsoft Windows and for Microsoft Exchange Server on page 10

Prerequisites for using the SnapCenter Plug-in for Microsoft Exchange Server

Before you use the Plug-in for Exchange, the SnapCenter administrator must install and configure the SnapCenter Server and perform the prerequisite tasks.

- Install and configure SnapCenter Server.
- Log in to SnapCenter.
- Configure the SnapCenter environment by adding or assigning storage system connections and creating a credential.

  Note: SnapCenter does not support multiple SVMs with the same name on different clusters. Each SVM supported by SnapCenter must have a unique name.
- Add hosts, install the SnapCenter Plug-in for Microsoft Windows and the SnapCenter Plug-in for Microsoft Exchange Server, and discover (refresh) the resources.
- Perform host-side storage provisioning using the SnapCenter Plug-in for Microsoft Windows.
- If you are using SnapCenter Server to protect Exchange databases that reside on VMware RDM LUNs, you must have deployed the NetApp Data Broker virtual appliance, enabled the SnapCenter Plug-in for VMware vSphere, and registered the plug-in with SnapCenter. See the NetApp Data Broker, SnapCenter Plug-in for VMware vSphere, documentation.

  Note: VMDKs are not supported.
- Move an existing Microsoft Exchange Server database from a local disk to supported storage using Microsoft Exchange tools.
- Set up SnapMirror and SnapVault relationships, if you want backup replication.

The SnapCenter 4.1.1 documentation has information on protecting virtualized databases and file systems using the SnapCenter 4.1.1 Plug-in for VMware vSphere. The NetApp Data Broker, SnapCenter Plug-in for VMware vSphere, documentation has information on protecting virtualized databases and file systems using the Linux-based NetApp Data Broker virtual appliance (Open Virtual Appliance format) for SnapCenter 4.2.

Deployment Guide for SnapCenter Plug-in for VMware vSphere

Data Protection Guide for VMs, Datastores, and VMDKs using the SnapCenter Plug-in for VMware vSphere

Exchange Server privileges required

To enable SnapCenter to add Exchange Server or DAG, and to install SnapCenter Plug-in for Microsoft Exchange Server on a host or DAG, you must configure SnapCenter with credentials for a user with a minimum set of privileges and permissions.

You must have a domain user with local administrator privileges, and with local login permissions on the remote Exchange host, as well as administrative permissions on all the nodes in the DAG. The domain user requires the following minimum permissions:

- Add-MailboxDatabaseCopy
- Dismount-Database
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- Move-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly:$true
- Mount-Database
- New-MailboxDatabase
- New-PublicFolderDatabase
- Remove-MailboxDatabase
- Remove-MailboxDatabaseCopy
- Remove-PublicFolderDatabase
- Resume-MailboxDatabaseCopy
- Set-AdServerSettings
- Set-MailboxDatabase -allowfilerestore:$true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

Storage types supported by SnapCenter Plug-in for Microsoft Windows and for Microsoft Exchange Server

SnapCenter supports a wide range of storage types on both physical machines and virtual machines. You must verify whether support is available for your storage type before installing the package for your host.

SnapCenter provisioning and data protection support is available on Windows Server. For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT).

NetApp Interoperability Matrix Tool

Machine	Storage type	Provision using	Support notes
Physical server	FC-connected LUNs	SnapCenter graphical user interface (GUI) or PowerShell cmdlets	
	iSCSI-connected LUNs	SnapCenter GUI or PowerShell cmdlets	
VMware VM	RDM LUNs connected by an FC or iSCSI HBA	PowerShell cmdlets	Physical compatibility only
	iSCSI LUNs connected directly to the guest system by the iSCSI initiator	SnapCenter GUI or PowerShell cmdlets	
	Note: VMDKs are not supported.		
Hyper-V VM	Virtual FC (vFC) LUNs connected by a virtual Fibre Channel Switch	SnapCenter GUI or PowerShell cmdlets	You must use Hyper-V Manager to provision Virtual FC (vFC) LUNs connected by a virtual Fibre Channel Switch.
	iSCSI LUNs connected directly to the guest system by the iSCSI initiator	SnapCenter GUI or PowerShell cmdlets	
	Note: Hyper-V pass through disks and backing up databases on VHD(x) that are provisioned on NetApp storage are not supported.		

How resources, resource groups, and policies are used for protecting Exchange Server

Before you use SnapCenter, it is helpful to understand basic concepts related to the backup and restore operations you want to perform. You interact with resources, resource groups, and policies for different operations.

- *Resources* are typically mailbox databases or Microsoft Exchange Database Availability Group (DAG) that you back up with SnapCenter.

- A SnapCenter *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.

  When you perform an operation on a resource group, you perform that operation on the *resources* defined in the resource group according to the schedule you specify for the resource group.

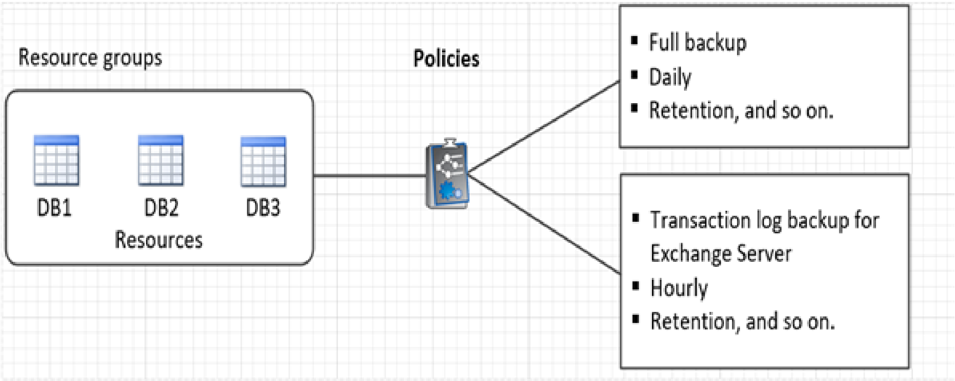
  You can back up on demand a single resource or a resource group. You also can perform scheduled backups for single resources and resource groups.

  The resource groups were formerly known as *datasets*.

- The *policies* specify the backup frequency, copy retention, scripts, and other characteristics of data protection operations.

  When you create a resource group, you select one or more policies for that group. You can also select one or more policies when you perform a backup on demand for a single resource.

Think of a resource group as defining *what* you want to protect and when you want to protect it in terms of day and time. Think of a policy as defining *how* you want to protect it. If you are backing up all databases of a host, for example, you might create a resource group that includes all the databases in the host. You could then attach two policies to the resource group: a daily policy and an hourly policy. When you create the resource group and attach the policies, you might configure the resource group to perform a full backup daily and another schedule that performs log backups hourly. The following image illustrates the relationship between resources, resource groups, and policies for databases:



Logging in to SnapCenter

SnapCenter supports role-based access control (RBAC). SnapCenter admin assigns roles and resources through SnapCenter RBAC to either a user in workgroup or active directory, or to groups in active directory. The RBAC user can now log in to SnapCenter with the assigned roles.

Before you begin

- You should enable Windows Process Activation Service (WAS) in Windows Server Manager.
- If you want to use Internet Explorer as the browser to log in to the SnapCenter Server, you should ensure that the Protected Mode in Internet Explorer is disabled.

About this task

During installation, the SnapCenter Server Install wizard creates a shortcut and places it on the desktop and in the Start menu of the host where SnapCenter is installed. Additionally, at the end of the installation, the Install wizard displays the SnapCenter URL based on the information that you provided during installation, which you can copy if you want to log in from a remote system.

> **Attention:** If you have multiple tabs open in your web browser, closing just the SnapCenter browser tab does not log you out of SnapCenter. To end your connection with SnapCenter, you must log out of SnapCenter either by clicking the **Sign out** button, or by closing the entire web browser.

> **Best Practice:** For security reasons, it is recommended that you do not enable your browser to save your SnapCenter password.

The default GUI URL is a secure connection to the default port 8146 on the server where the SnapCenter Server is installed (`https://server:8146`). If you provided a different server port during the SnapCenter installation, that port is used instead.

For Network Load Balance (NLB) deployment, you must access SnapCenter using the NLB cluster IP (`https://NLB_Cluster_IP:8146`). If you do not see the SnapCenter UI when you navigate to `https://NLB_Cluster_IP:8146` in Internet Explorer (IE), you must add the NLB IP address as a trusted site in IE on each plug-in host, or you must disable IE Enhanced Security on each plug-in host.

NetApp KB Article 2025082: SnapCenter in an HA configuration with Application Request Routing enabled.

In addition to using the SnapCenter GUI, you can use PowerShell cmdlets to create scripts to perform configuration, backup, and restore operations. Some cmdlets might have changed with each SnapCenter release. The SnapCenter cmdlet or SnapCenter CLI documentation has the details.

> **Note:** If you are logging in to SnapCenter for the first time, you must log in using the credentials that you provided during the install process.

Steps

1. Launch SnapCenter from the shortcut located on your local host desktop, or from the URL provided at the end of the installation, or from the URL provided by your SnapCenter administrator.
2. Enter user credentials.

To specify the following...	Use one of these formats...
Domain administrator	***NetBIOS\UserName*** ***UserName@UPN suffix*** For example, username@netapp.com ***Domain FQDN\UserName***
Local administrator	***UserName***

3. If you are assigned more than one role, from the **Role** box, select the role that you want to use for this login session.

   Your current user and associated role are shown in the upper right of SnapCenter after you are logged in.

Result

If you are using SnapCenter for the first time, the Storage Systems page is displayed, and the Get Started pane is expanded.

If the logging fails with the error that site cannot be reached, you should map the SSL certificate to SnapCenter.

After logging to SnapCenter Server for the first time, the SnapCenter Server Configuration Checker schedule is created. The default values are Weekly and Every Sunday at 11:59 pm. To modify the schedule or run the SnapCenter Server schedule, click **Settings > Scheduled Configuration Checker**.

After you finish

If you have untrusted Active Directory domains that you want SnapCenter to support, you must register those domains with SnapCenter before configuring the roles for the users on untrusted domains. The administration documentation has more details.

Performing administrative tasks

Related information

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

Backing up Exchange resources

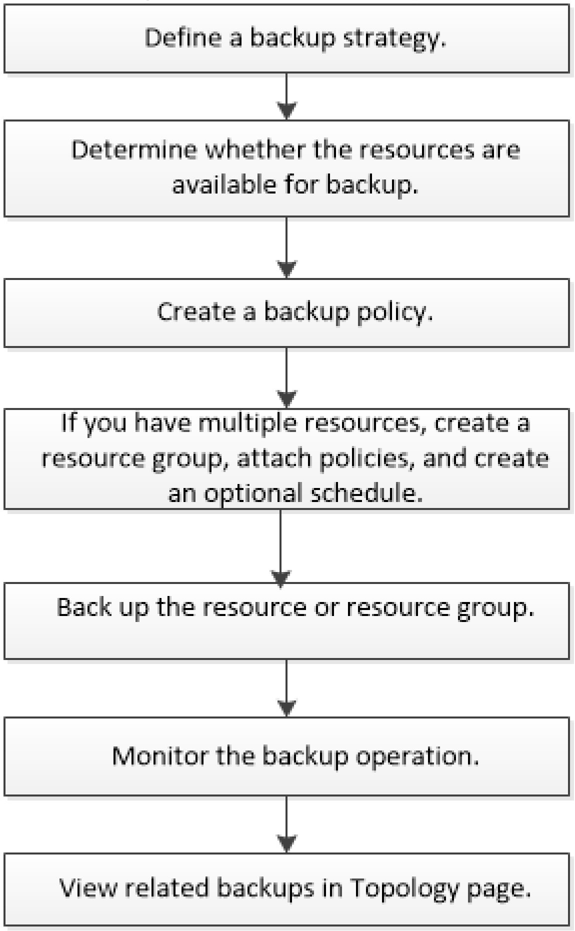
When you install the SnapCenter Plug-in for Microsoft Exchange Server in your environment, you can use SnapCenter to back up Exchange resources.

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 of backup operations:


Define a backup strategy.
Determine whether the resources are available for backup.
Create a backup policy.
If you have multiple resources, create a resource group, attach policies, and create an optional schedule.
Back up the resource or resource group.
Monitor the backup operation.
View related backups in Topology page.

Related tasks

Creating backup policies for Exchange Server databases on page 16
Monitoring backup operations on page 24

Related information

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

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 your Microsoft Exchange Server documentation.

Determining whether 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.

Before you begin

- 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 have deployed the NetApp Data Broker virtual appliance, enabled the SnapCenter Plug-in for VMware vSphere, and registered the plug-in with SnapCenter. See the NetApp Data Broker, SnapCenter Plug-in for VMware vSphere, documentation.
  Deployment Guide for SnapCenter Plug-in for VMware vSphere

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, suspend, and so on.
- 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.
  You cannot back up at the DAG level if there are nodes in the DAG that use non-NetApp storage. You must back up the databases from each DAG member host instead.

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.

   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.

Result

The resources are displayed along with information such as resource name, Database Availability Group name, 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.
  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.

Creating backup policies for Exchange Server databases

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

Before you begin

- You must have defined your data protection strategy.
  For details, see the information about defining a data protection strategy for Exchange databases.
  Concepts
- 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 SVMs for both the source volumes and destination volumes to you.
  Refer the *Administration Guide* for information about how administrators assign resources to users.
  Performing administrative tasks

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.

> **Best Practice:** NetApp recommends 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.

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 **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. **Note:** This is the recommended backup type.
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.
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.

    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 DAGs, this option backs up only active copies of all databases in the DAG. Passive copies are not backed up.
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.

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

   Note: 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.

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

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

Note: 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.

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 the **Number of full backups for which logs are retained** option, and specify the number of full backups for which you want up-to-the-minute restorability. For up-to-the-minute (UTM) restore operations, the retention setting is the number of full backups for which the log backups are retained. If you configure UTM retention (the number of full backups for which logs are retained) to 5, the log backups up to the most recent 5 full backups for this database are retained, and the rest are deleted. **Note:** The setting must be equal to the setting for Total Snapshot copies (full backups) in theFull 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 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).

Note: 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. For example,

  ```
  <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.
Secondary policy label	Depending on the Snapshot copy label that you select, ONTAP applies the secondary Snapshot copy retention policy that matches the label.
Error retry count	Enter the number of replication attempts that should occur before the process halts.

8. Optional: 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.

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

Related concepts

Preparing for data protection on page 8

Creating resource groups and attaching policies for Exchange Servers

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 and the protection schedule.

About this task

You can back up a database or Database Availabililty Group (DAG) individually, on demand, without creating a new resource group.

A resource group cannot contain more than one DAG.

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.

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

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

For this field…	Do this…
Name	Enter the resource group name.
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.

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

   b. Type the name of the resource in the search text box, or scroll to locate a resource.
   c. To move resources from the **Available Resources** section to the **Selected Resources** section, perform one of the following steps:
6. In the **Policies** page, perform the following steps:
   a. Select one or more policies from the drop-down list.

> **Note:** You can also create a policy by clicking + .

> **Note:** 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.

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.

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 *Cmdlet Reference Guide*.

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

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

Backing 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.

Before you begin

- 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.

About this task

> **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 appropriate plug-in from the list.

2. On the **Resources** page, select either **Database**, or **Database Availability Group** from the **View** list.

   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.
     - **a.** If the Topology view is displayed, click **Protect**.
     - **b.** 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, on 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.

   Example

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

4. On the **Policies** page, perform the following steps:

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

      Note: You can also create a policy by clicking + .

      Note: 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.

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

   b. Click + 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`* 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**.

   Note: 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.
   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.

Backing 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.

Before you begin

- 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 SVM used by the database.
- If you want to back up a resource that has a SnapMirror relationshipwith 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.

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 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 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.
   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.

Monitoring backup operations

You can monitor the progress of different backup operations by using the SnapCenter Jobs 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 state of the operation:

- ▶ 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. Optional: 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.

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

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

Monitoring 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.

About this task

The Activity pane displays information regarding backup, restore, 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.

Canceling the backup operations

You can cancel backup operations that are queued.

Before you begin

- You must be logged in as the SnapCenter Admin or job owner to cancel operations.

About this task

- You can cancel a backup operation from either the Monitor page or the Activity pane.
- 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.

Step

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 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**.

Result

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

Related information

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

Viewing 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 storage.

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 primary backups that are available on the storage.

- ⛁ 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 either database, the resource, or 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** 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.

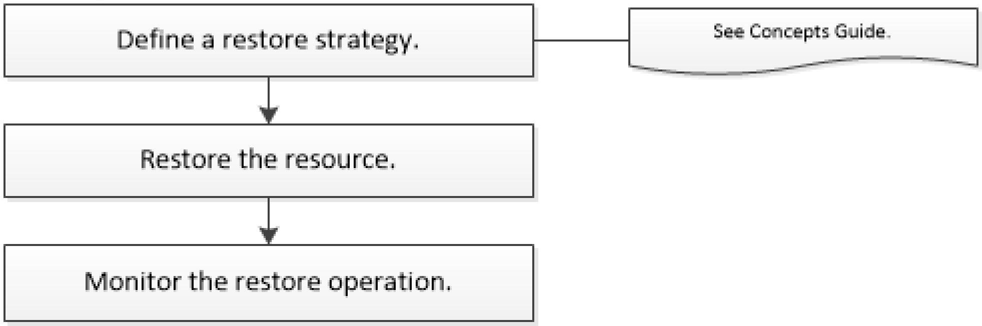
6. Select the backup from the table, and then click the data protection icons to perform restore, rename, and delete operations.

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

Restoring Exchange resources

You can use SnapCenter to restore Exchange databases by restoring one or more backups to your active file system.

The following workflow shows the sequence in which you must perform the Exchange database restore operations:



You can also use PowerShell cmdlets manually or in scripts to perform backup and restore operations. For detailed information about PowerShell cmdlets, use the SnapCenter cmdlet help or see the cmdlet reference information.

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

Related information

SnapCenter Software 4.2 Windows Cmdlet Reference Guide
Concepts

Requirements for restoring a database

Before you restore a Exchange Server database from a SnapCenter Plug-in for Microsoft Exchange Server backup, you must ensure that several requirements are met.

- The Exchange Server must be online and running before you can restore a database.
- The databases must exist on the Exchange Server.

  Note: Restoring deleted databases is not supported.
- SnapCenter schedules for the database must be suspended.
- The SnapCenter Server and the SnapCenter Plug-in for Microsoft Exchange Server host must be connected to the primary and secondary storage that contains the backups you want to restore.

Restoring Exchange databases

You can use SnapCenter to restore backed-up Exchange databases.

Before you begin

- You must have backed up the resource groups, database, or Database Availability Groups (DAGs).
- If you are replicating Snapshot copies to a mirror or vault, the SnapCenter administrator must have assigned you the SVMs for both the source volumes and destination volumes.

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

About this task

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

Note: DAG-level backups must be restored from individual databases.

Steps

1. In the left navigation pane, click **Resources**, and in the upper left corner of the **Resource** page, select the Exchange Server plug-in from the drop-down list.
2. In the **Resources** page, select **Database** from the **View** list.
3. Select the database from the list.

   The topology page is displayed.
4. From the **Manage Copies** view, select **Backups**, from the **Primary Backups** table, and then click ↰.
5. In the **Options** page, select one of the following log backup options:

Option	Description
All log backups	Choose **All log backups** to perform up-to-the-minute backup restore operation to restore all of the available log backups after the full backup.
By log backups until	Choose **By log backups until** to perform a point-in-time restore operation, which restores the database based on log backups until the selected log.
By specific date until	Choose **By specific date until** to specify the date and time up to which transaction logs are applied to the restored database. This point-in-time restore operation restores transaction log entries that were recorded until the last backup on the specified date and time.
None	Choose **None** when you need to restore only the full backup without any log backups.

   You can also select the following actions:

   - **Recover and mount database after restore**
     Select this if you want SnapCenter to recover and mount the database after the restore operation.
   - **Do not verify the integrity of transaction logs in the backup before restore**
     By default, SnapCenter verifies the integrity of transaction logs in a backup before performing a restore operation.

     Best Practice: Selecting this option is not recommended.
6. At the bottom of the **Options** page, select **Recover and mount the database after the restore** if you want SnapCenter to perform this task.
7. Optional: In the **Script** page, enter the path and the arguments of the prescript or postscript that should be run before or after the restore operation, respectively.

   Restore prescript arguments include $Database and $ServerInstance.

Restore postscript arguments include $Database, $ServerInstance, $BackupName, $LogDirectory, and $TargetServerInstance.

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

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.

9. Review the summary, and then click **Finish**.
10. You can view the status of the restore job by expanding the **Activity** panel at the bottom of the page.

After you finish

You should monitor the restore process using the **Monitor** > **Jobs** page.

Related information

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

Restoring an Exchange Server database from secondary storage

You can restore a backed up Exchange Server database from secondary storage (mirror or vault).

Before you begin

You must have replicated the Snapshot copies from primary storage to a secondary storage.

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 **Resource Group** from the **View** drop-down list.
3. Select the database or the resource group.

   The database or resource group topology page is displayed.

4. In the **Manage Copies** section, select **Backups** from the secondary storage system (mirror or vault).
5. Select the backup from the list, and then click ↰.
6. On the **Location** page, choose the destination volume for restoring the selected resource.
7. Complete the **Restore** wizard, review the summary, and then click **Finish**.

Reseeding a passive Exchange node replica

If you need to restore a replica copy, for instance when a copy is corrupt, you can restore to the latest backup using the reseed feature in SnapCenter.

Before you begin

- You must be using SnapCenter Server 4.1 or later, and Plug-in for Exchange 4.1 or later.

Reseeding a replica is not supported in SnapCenter versions earlier than 4.1.

- You must have created a backup of the database you want to reseed.

About this task

Best Practice: To avoid lagging between nodes, we recommend that you either create a new backup before you perform a reseed operation, or choose the host with the latest backup.

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 appropriate option from the **View** list:

Option	Description
To reseed a single database	Select **Database** from the View list.
To reseed databases in a DAG	Select **Database Availability Group** from the View list.

3. Select the resource you want to restore.
4. On the **Manage Copies** page, click **Reseed**.
5. From the list of unhealthy databases copies in the **Reseed** wizard, select the one you want to reseed, and then click **Next**.
6. In the **Host** window, select the host with the backup from which you want to reseed, and then click **Next**.
7. Optional: In the **Script** page, enter the path and the arguments of the prescript or postscript that should be run before or after the restore operation, respectively.

   For example, you can run a script to update SNMP traps, automate alerts, send logs, and so on.
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.
9. Review the summary, and then click **Finish**.
10. You can view the status of the job by expanding the **Activity** panel at the bottom of the page.

Monitoring restore operations

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

About this task

Post-restore states describe the conditions of the resource after a restore operation and any further restore actions that you can take.

The following icons appear on the Jobs page, and indicate the state of the operation:

- ● 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. Optional: In the **Jobs** page, perform the following steps:
    a. Click ▼ to filter the list so that only restore operations are listed.
    b. Optional: Specify the start and end dates.
    c. From the **Type** drop-down list, select **Restore**.
    d. From the **Status** drop-down list, select the restore status.
    e. Click **Apply** to view the operations that are completed successfully.
4. Select the restore job, and then click **Details** to view the job details.
5. Optional: In the **Job Details** page, click **View logs**.

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

Canceling restore operations

You can cancel restore jobs that are queued.

Before you begin

- You must be logged in as the SnapCenter Admin or job owner to cancel restore operations.

About this task

- You can cancel a restore operation from either the Monitor page or the Activity pane.
- You cannot cancel a running restore operation.
- You can use the SnapCenter GUI, PowerShell cmdlets, or CLI commands to cancel the restore operations.
- The **Cancel Job** button is disabled for restore 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.

Step

1. Perform one of the following actions:

From the…	Action
Monitor page	**a.** In the left navigation pane, click **Monitor** > **Jobs**. **b.** Select the job and click **Cancel Job**.
Activity pane	**a.** After initiating the restore 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**.

Related information

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

Backing up, restoring, and removing backups using PowerShell cmdlets

The SnapCenter Plug-in for Microsoft Exchange Server includes PowerShell cmdlets for scripting of backup and restore operations.

The following are common tasks you might perform using PowerShell cmdlets:

- Preparing the PowerShell environment
- Creating a storage system connection and a credential
- Backing up Exchange Server databases
- Restoring Exchange Server databases
- Removing backups

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 *Cmdlet Reference Guide*.

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

Creating 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 back up and restore.

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 data LIF IP address.

About this task

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 *Cmdlet Reference Guide*.

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

Steps

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

   Example

   This example opens a PowerShell session:

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

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

   Example

   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.

   Example

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

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

Backing up 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.

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.

About this task

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 *Cmdlet Reference Guide*.

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

> **Note:** 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.

Example

```
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.

Example

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
```

Example

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'}
```

Example

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.

Example

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.

Example

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_
bkp_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'}
```

Example

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_
bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database
Availability Group";"Names"="DAGSCE0102"}
```

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

Example

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

Example

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.

Example

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?
```

Example

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

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

Restoring resources using PowerShell cmdlets

Restoring an Exchange database includes initiating a connection session with the SnapCenter Server, listing the backups and retrieving backup information, and restoring a backup.

Before you begin

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

About this task

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 *Cmdlet Reference Guide*.

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

Steps

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

   Example

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

2. Retrieve the information about the one or more backups that you want to restore by using the `Get-SmBackup` cmdlet.

   Example

   This example displays information about all available backups:

   ```
   PS C:\> Get-SmBackup

   BackupId                      BackupName
   BackupTime                    BackupType
   --------                      ----------
   ----------                    ----------
   341                           ResourceGroup_36304978_UTM... 12/8/2017
   4:13:24 PM          Full Backup
   342                           ResourceGroup_36304978_UTM... 12/8/2017
   4:16:23 PM          Full Backup
   355                           ResourceGroup_06140588_UTM... 12/8/2017
   6:32:36 PM          Log Backup
   356                           ResourceGroup_06140588_UTM... 12/8/2017
   6:36:20 PM          Full Backup
   ```

3. Restore data from the backup by using the `Restore-SmBackup` cmdlet.

   Example

   This example restores an up-to-the-minute backup:

   ```
   C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
   exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341
   ```

   Example

   This example restores a point-in-time backup:

   ```
   C:\ PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
   exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341 -LogRestoreType
   ByTransactionLogs -LogCount 2
   ```

   Example

   This example restores a backup on secondary storage to primary story:

   ```
   C:\ PS> Restore-SmBackup -PluginCode 'SCE' -AppObjectId 'DB2' -
   BackupId 81 -Confirm:$false
   -archive @{Primary="paw_vs:vol1";Secondary="paw_vs:vol1_mirror"} -
   logrestoretype All
   ```

   The `-archive` parameter enables you to specify the primary and secondary volumes you want to use for the restore.

Reseeding a replica using PowerShell cmdlets

You can use PowerShell cmdlets to restore an unhealthy replica by using either the most recent copy on the same host or the most recent copy from an alternate host.

About this task

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 *Cmdlet Reference Guide*.

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

Steps

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

   Example

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

2. Reseed the database by using the `reseed-SmDagReplicaCopy` cmdlet.

   Example

   This example reseeds the failed copy of the database called execdb on the host "mva-rx200.netapp.com" using the latest backup on that host.

   ```
   reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
   execdb
   ```

   Example

   This example reseeds the failed copy of the database called execdb using the latest backup of the database (production/copy) on an alternate host "mva-rx201.netapp.com."

   ```
   reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -
   Database  execdb -BackupHost "mva-rx201.netapp.com"
   ```

Removing 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.

Before you begin

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

About this task

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 *Cmdlet Reference Guide*.

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

Steps

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

   Example

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

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

   Example

   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"):
   ```

Troubleshooting data protection operations

If you encounter unexpected behavior while performing data protection operations, you can use the log files to help identify the cause and to resolve the problem.

The log files are located at `/Program Files/NetApp/SnapCenter/SnapCenter Plug-in for Microsoft Exchange Server/log`. You can also download the log files from the SnapCenter user interface by clicking **Monitor** > **Logs** > **Download**.

Back up operation on some hosts might trigger late

Description

If a resource group has multiple databases from different hosts, the backup operation on some hosts might trigger late because of network issues.

Error message

`Scheduled job is not triggered on host(s) <HOST_NAMES>`

Corrective action

You should configure the key `MaxRetryForUninitializedHosts` value in `web.config` by using the `Set SmConfigSettings PS cmdlet` cmdlet. In the following example, the default value of the retry count is 10:

```
Set-SmConfigSettings -Server -configSettings
@{"MaxRetryForUninitializedHosts"=10}
```

Passive database copy goes into suspended or failed state after restore on active database

Description

When you restore an active database from a backup, the passive database might go into suspended or failed state if there is a lag between the replica and the active database. The state change can occur when the active database's log chain forks and begins a new branch which breaks replication.

Corrective action

Exchange Server will attempt to fix the replica, but if it is unable to do so, after restore, you can create a fresh backup, and then reseed the replica.

Restore fails during database dismount when database is failing over to passive node

Description

The Plug-in for Exchange restore operation fails during Exchange Server database dismount when the database is failing over to the passive node.

Corrective action

Wait for the failover to complete, and then retry the restore operation.

Restore operation times out

Description

During a restore operation that accesses VMs, the vCenter Server timed out while waiting for a response from the SnapCenter server.

This error can occur when VMotion or the actual restore operation exceeds the timeout set for responses from the SnapCenter server.

Error message

`The operation has timed out`

Corrective action

You can increase the SnapCenter server timeout value by including the following REST API in the appsetting section of the `SMCoreServiceHost.exe.Config` file located under SmCore in the SnapCenter Server:

```
<add key="RESTTimeout" value="timeout-value"/>
```

The default timeout value is 10800000 (in milliseconds, which is 3 hours). You can increase that value, in milliseconds, as needed.

Exchange backup fails with VSS event ID 8193

Description

An Exchange backup fails with Volume Shadow Copy Service event ID 8193. The issue might indicate that there is an issue with the disk on which the database is located.

Corrective action

You can create a new database on a new disk, and then move the mailboxes from the old database to the new database.

Backups fail after changing the Exchange plug-in host port in SnapCenter

Description

When you change the Exchange plug-in host port number using the **Hosts** > **Modfy** option in SnapCenter, backups might fail when the plug-in host status indicates it is in suspended mode.

Corrective action

Wait until the Exchange plug-in host status changes to Running, and then try the backup operation.

Backup operation fails if Snapshot copies on the secondary storage reaches maximum limit

Description

When the number of Snapshot copies on the secondary storage (mirror-vault) reaches the maximum limit, the activity to register backup and apply retention in the backup operation fails.

Error message

```
This Snapshot copy is currently used as a reference Snapshot copy by one or
more SnapMirror relationships. Deleting the Snapshot copy can cause future
SnapMirror operations to fail.
```

Corrective action

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

SnapCenter Dashboard backup jobs are not updated when Exchange backups are deleted

Description

When you delete an Exchange backup job in the SnapCenter Topology view, and then view the backup job pie chart in the Dashboard, the deleted job is still included in the total number of backups.

Corrective action

Open Windows Internet Information Services (IIS) Manager on your SnapCenter host, and restart the service.

Back Up Now button in the Topology page is unavailable after a failed backup

Description

After a backup fails, for example, because a volume in a resource group is offline, the **Back Up Now** button in the Topology page is unavailable even after the volume is brought back online, and the resources are refreshed.

Corrective action

Use the **Refresh Resource** button on the main Resources page, and then navigate back to the Topology page. The **Back Up Now** button displays correctly.

Log backups fail when maximum hard links limit per file is reached

Description

You can retain backups up to the ONTAP maximum of 255 copies. If up-to-the-minute backup retention is not working or is not configured correctly, log backup folders might not be deleted and the maximum hard links might be surpassed, which might cause log backups to fail.

Corrective action

Ensure that up-to-the-minute backup retention is configured and working correctly.

Backups created using Plug-in for Exchange might not have Snapshot copies available for restore

Description

By default, autodelete is enabled on the storage volume, and Snapshot copies might be deleted even when the volume is not full, resulting in Snapshot copies of backups being unavailable for restore.

Workaround

Ensure that you have sufficient space on the storage volume or disable autodelete.

Managing policies

You can create, copy, modify, view, and delete backup policies.

About this task

You can perform the following tasks related to policies:

- Create a policy.
- Modify a policy.

  Note: You can change the schedule type for a policy only after you detach the policy. To change the schedule you must modify the resource group.
- Copy a policy by accepting the default name or typing a new name.
- Detach a policy from a resource group.
- Delete a policy.

Detaching policies

You can detach policies from a resource or resource group any time that you no longer want those policies to govern data protection for the resources. You must detach a policy before you can delete it or before you modify the schedule type.

About this task

Attention: You cannot detach a policy from a resource or resource group if it is the only policy attached.

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 **Resource Group** from the **View** list.
3. Select the resource group, and then click **Modify Resource Group**.
4. In the **Policies** page of the **Modify Resource Group** wizard, from the drop-down list, clear the check mark next to the policies you want to detach.

   Note: You cannot detach the last remaining policy from an individual resource because every resource must have at least one policy attached. Therefore, if you want to delete or modify the only policy attached to a resource, you must perform the following:

   a. Attach a second placeholder policy.

   b. Detach the original policy from the resource.
5. Make any additional modifications to the resource group in the rest of the wizard, and then click **Finish**.

Modifying policies

You can modify policies when you want to change the Snapshot copy retention settings, error retry count, or scripts information while a policy is attached to a resource or resource group. You can also modify the schedule type (frequency), but only after you detach a policy.

About this task

Modifying the schedule type in a policy requires additional steps because the SnapCenter Server registers the schedule type only at the time the policy is attached to a resource or resource group.

Steps

1. Before you modify a policy, you should decide if you want to add a new schedule type, or if you want to change or modify an existing schedule type.

If you want to...	Then...
Add an additional schedule type	Create a new policy and attach it to the necessary resources or resource groups. For example, if a resource group policy specifies only hourly backups and you want to add daily backups also, you can create a policy with a daily schedule type and add it to the resource group. The resource group would then have two policies: hourly and daily.
Remove or change a schedule type	**a.** Detach the policy from every resource and resource group that uses that policy. **b.** Modify the schedule type. **c.** Attach the policy again to all of the resources and resource groups. For example, if a policy specifies hourly backups and you want to change that to daily backups, you must detach the policy first. **Note:** You cannot detach the last remaining policy from an individual resource because every resource must have at least one policy attached. Therefore, if you want to modify the schedule type of the only policy attached to a resource, you must perform the following: **a.** Attach a placeholder policy. **b.** Detach the original policy from every resource and resource group that uses that policy. **c.** Modify the schedule type. **d.** Attach the modified policy again to all of the resources and resource groups. **e.** Detach the placeholder policy.

2. In the left navigation pane, click **Settings**.
3. In the **Settings** page, click **Policies**.
4. Select the policy, and then click **Modify**.
5. Modify the information, and then click **Finish**.

Deleting policies

If you no longer require policies, you might want to delete them.

Before you begin

You must have detached the policy from resource groups if the policy is associated with any resource group.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Policies**.
3. Select the policy, and then click **Delete**.
4. Click **Yes**.

Managing resource groups

You can create, modify, and delete resource groups. You can also stop and start backup operations on resource groups.

About this task

You can perform the following tasks related to resource groups:

- Create a resource group.
- Modify a resource group by selecting the resource group and clicking **Modify Resource Group** to edit the information you provided while creating the resource group.

  Note: You can change the schedule while modifying the resource group. However, to change the schedule type you must modify the policy.

  Note: If you remove resources from a resource group, the backup retention settings defined in the policies currently attached to the resource group will continue to be applied to the removed resources.
- Create a backup of a resource group.
- Prevent scheduled operations on resource groups from starting.
- Delete a resource group.

Stopping and resuming operations on resource groups

You can temporarily disable scheduled operations from starting on a resource group. Later when you want, you can enable those operations.

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 **Resource Group** from the **View** list.
3. Select the resource group and click **Maintenance**.
4. Click **OK**.

After you finish

If you want to resume operations on the resource group that you had put on maintenance mode, select the resource group and click **Production**.

Deleting resource groups

You can delete a resource group if you no longer need to protect the resources in the resource group. You must ensure that resource groups are deleted before you remove plug-ins from SnapCenter.

About this task

You can optionally force the deletion of all backups, metadata, policies, and Snapshot copies associated with the resource group.

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 **Resource Group** from the **View** list.
3. Select the resource group, and then click **Delete**.
4. Optional: Select the **Delete backups and detach policies associated with this Resource Group** check box to remove all backups, metadata, policies, and Snapshot copies associated with the resource group.

   If you do not select this option, and you have policies and backups associated with the resource group, you must manually remove the associated policies and backups or the resource group is not removed.
5. Click **OK**.

Managing backups

You can rename and delete backups. You can also delete multiple backups simultaneously.

Renaming backups

You can rename backups if you want to provide a better name to improve searchability.

Steps

1. In the left navigation pane, click **Resources**, and then select **Microsoft Exchange Server** from the drop-down list located in the upper left corner.
2. In the **Resources** page either select the resource or resource group from the **View** drop-down list.
3. Select the resource or resource group from the list.

   The resource or resource group topology page is displayed. If the resource or resource group is not configured for data protection, the Protect wizard is displayed instead of the topology page.
4. From the **Manage Copies** view, select **Backups** from the primary storage, and then click ✎.

   Note: You cannot rename or delete backups that are on the secondary storage.
5. In the **Rename backup as** field, enter a new name, and then click **OK**.

Deleting backups

You can delete backups if you no longer require the backup for other data protection operations.

Steps

1. In the left navigation pane, click **Resources**, and then select **Microsoft Exchange Server** from the drop-down list located in the upper left corner.
2. In the **Resources** page either select the resource or resource group from the **View** drop-down list.
3. Select the resource or resource group from the list.

   The resource or resource group topology page is displayed.
4. From the **Manage Copies** view, table, select **Backups** from the primary storage, and then click 🗑.

   Note: You cannot rename or delete backups that are on the secondary storage.
5. Click **OK**.

Copyright

Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

http://www.netapp.com/us/legal/netapptmlist.aspx

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277