



SnapCenter® Software 4.2

Administration Guide

August 2019 | 215-14388_A0
doctrcomments@netapp.com

 **NetApp®**

Contents

Deciding whether to read the SnapCenter Administration information	5
Using role-based access control	6
SnapCenter role-based access control	6
Adding a user or group and assigning role and assets	6
Creating a new role	8
Modifying a role	8
Modifying SnapCenter users or groups	9
Application-level role-based access control	9
Using the Dashboard	10
Viewing Dashboard information	10
Information provided in the Dashboard	10
Requesting Jobs status reports from the Dashboard	14
Requesting Protection status reports from the Dashboard	14
Using SnapCenter reporting capabilities	16
Accessing SnapCenter reports	16
Types of reports	16
Filtering your report data	17
Exporting or printing reports	17
Setting the SMTP server for email notifications using Global Settings	18
Configuring the option to email reports	18
Monitoring jobs, schedules, events, and logs	20
Monitoring SnapCenter jobs	20
Monitoring SnapCenter schedules	20
Monitoring SnapCenter events	20
Monitoring SnapCenter logs	21
Removing jobs and logs from SnapCenter	22
Managing the SnapCenter Server repository	23
Prerequisites for protecting the SnapCenter repository	23
Backing up the SnapCenter repository	23
Viewing backups of the SnapCenter repository	24
Restoring a SnapCenter database repository	24
Migrating the SnapCenter repository	25
Resetting the SnapCenter repository password	25
Managing hosts	27
Refreshing virtual machine information	27
Starting and restarting plug-in services	28
Suspending schedules on hosts to place them in maintenance mode	28
Managing resources of untrusted domains	30
Registering untrusted Active Directory domains	30
Modifying untrusted domains	31

Unregistering untrusted Active Directory domains	32
Configuring secured MySQL connections with SnapCenter Server	33
Configuring secured MySQL connections for standalone SnapCenter Server configurations	33
Configuring secured MySQL connections for NLB configurations	35
Managing the storage system	39
Modifying storage system configuration	39
Deleting the storage system	40
Viewing SnapManager Suite storage controller license installation status using the SnapCenter GUI	40
Provisioning storage on Windows hosts	42
Configuring LUN storage	42
Establishing an iSCSI session	42
Disconnecting an iSCSI session	43
Creating and managing igroups	44
Creating and managing disks	45
Creating and managing SMB shares	51
Creating an SMB share	51
Deleting an SMB share	52
Reclaiming space on the storage system	52
Using PowerShell cmdlets to provision storage	53
Provisioning storage in VMware environments	54
Supported VMware guest OS platforms	54
VMware ESXi server-related limitations	54
Minimum vCenter privileges required for SnapCenter RDM operations	54
Using FC RDM LUNs in a Microsoft cluster	55
Requirements for using FC RDM LUNs in a Microsoft cluster	55
Microsoft cluster support limitations when using FC/iSCSI RDM LUNs	56
Creating a shared FC RDM LUN	56
Troubleshooting RDM LUN creation	56
Managing EMS data collection	58
Stopping EMS data collection	58
Starting EMS data collection	58
Changing EMS data collection schedule and target SVM	59
Monitoring EMS data collection status	59
Using REST APIs	60
Accessing REST APIs using the Swagger API web page	60
Plug-in support for REST APIs	61
Troubleshooting SnapCenter REST APIs	61
Copyright	62
Trademark	63
How to send comments about documentation and receive update notifications	64
Index	65

Deciding whether to read the SnapCenter Administration information

This information describes how to manage SnapCenter by managing your hosts, the SnapCenter Server repository, EMS data collection, and untrusted domains, and how to provision storage on Windows hosts, maintain role-based access control (RBAC), use the Dashboard, and generate reports.

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

- Use Application Request Routing and Network Load Balancing
- Provision storage on Windows hosts or reclaim storage space
- Create and manage SMB shares on Windows hosts
- Modify hosts and plug-ins or remove a host
- Start or restart plug-in services
- Suspend or restart schedules on hosts
- Configure, backup, or restore the SnapCenter repository
- Register, modify, or unregister hosts in untrusted domains
- Configure, export, or print reports
- Monitor jobs, schedules, events, and logs
- Stop, start, modify, and monitor EMS data collection
- Use SnapCenter REST APIs

You should have already performed the following tasks:

- Read the SnapCenter Software Release Notes

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
- Information about the SnapCenter Plug-in for VMware vSphere provided by the NetApp Data Broker virtual appliance
[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](#)
- SnapCenter PowerShell cmdlets or Linux commands
[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)
[SnapCenter Software 4.2 Linux Command Reference Guide](#)

Using role-based access control

SnapCenter provides centralized control and oversight for SnapCenter administrators, while empowering individual application administrators to manage backup, restore, and cloning functions through the use of roles and their access permissions.

SnapCenter role-based access control

SnapCenter role-based access control (RBAC) enables you to manage or create roles, assign permissions to those roles, and add domain-created and operating system-created users or groups to these roles, to centrally manage SnapCenter access.

For more information about SnapCenter role-based access control (RBAC), see the SnapCenter concepts documentation.

Concepts

For information about the additional vCenter RBAC that is provided by the SnapCenter Plug-in for VMware vSphere, see the NetApp Data Broker, SnapCenter Plug-in for VMware vSphere, documentation.

[Data Protection Guide for VMs, Datastores, and VMDKs using the SnapCenter Plug-in for VMware vSphere](#)

Adding a user or group and assigning role and assets

To configure role-based access control for SnapCenter users, you can add users or groups and assign role. The role determines the options that SnapCenter users can access.

Before you begin

- You must have logged in as the “SnapCenterAdmin” role.
- You must have created the user or group accounts in Active Directory in the operating system or database. You cannot use SnapCenter to create these accounts.

Note: The group names should not include `^[] ;|, +*?< >'` characters.

About this task

- SnapCenter includes several predefined roles.
You can either assign these roles to the user or create new roles.
- After you assign a role to a user or group that contains the appropriate permissions, you must assign the user access to SnapCenter assets, such as hosts and storage connections.
This enables users to perform the actions for which they have permissions on the assets that are assigned to them.
- You should assign a role to the user or group at some point to take advantage of RBAC permissions and efficiencies.
- You can assign assets like host, resource groups, policy, storage connection, plug-in, and credential to the user while creating the user or group.
- When a new node is added to a Windows cluster or a DAG (Exchange Server Database Availability Group) asset and if this new node is assigned to a user, you must reassign the asset to the user or group to include the new node to the user or group.

You should reassign the RBAC user or group to the cluster or DAG to include the new node to the RBAC user or group. For example, you have a two-node cluster and you have assigned an RBAC user or group to the cluster. When you add another node to the cluster, you should reassign the RBAC user or group to the cluster to include the new node for the RBAC user or group.


- If you are planning to replicate Snapshot copies, you must assign the storage connection for both the source and destination volume to the user performing the operation.
You should add assets before assigning access to the users.

Attention: If you are using the NetApp Data Broker, SnapCenter Plug-in for VMware vSphere functions, to protect VMs, VMDKs, or datastores, you use the VMware vSphere GUI to add a vCenter user to a SnapCenter Plug-in for VMware vSphere role. The vCenter documentation contains information about adding a user to a role in vCenter

The SnapCenter concepts documentation contains more information about SnapCenter role-based access control (RBAC).

Concepts

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Users and Access** > .
3. In the **Add Users/Groups from Active Directory or Workgroup** page:

For this field...	Do this...
Access Type	Select either Domain or workgroup For Domain authentication type, you should specify the domain name of the user or group to which you want to add the user to a role. By default, it is pre-populated with the logged in domain name. Note: You must register the untrusted domain in the Settings > Global Settings > Domain Settings page.
Type	Select either User or Group Note: SnapCenter supports only security group and not the distribution group.
User Name	<ol style="list-style-type: none"> a. Type the partial user name, and then click Add. Note: The user name is case-sensitive. b. Select the user name from the search list. Note: When you add users from a different domain or an untrusted domain, you should type the user name fully because there is no search list for cross domain users. Repeat this step to add additional users or groups to the selected role.
Roles	Select the role to which you want to add the user.


4. Click **Assign**, and then in the **Assign Assets** page:
 - a. Select the type of asset from the **Asset** drop-down list.

- b. In the Asset table, select the asset.
The assets are listed only if the user has added the assets to SnapCenter.
 - c. Repeat this procedure for all of the required assets.
 - d. Click **Save**.
5. Click **Submit**.

Creating a new role

In addition to using the existing SnapCenter roles, you can create your own roles and customize the permissions.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Roles**.
3. Click .
4. In the **Add Role** page, specify a name and description for the new role.
5. Select **All members of this role can see other members' objects** to enable other members of the role to see resources such as volumes and hosts after they refresh the resources list.
You should deselect this option if you do not want members of this role to see objects to which other members are assigned.
Note: When this option is enabled, assigning users access to objects or resources is not required if users belong to the same role as the user who created the objects or resources.
6. In the **Permissions** page, select the permissions that you want to assign to the role, or click **Select All** to grant all permissions to the role.
7. Click **Submit**.

Modifying a role

You can modify a SnapCenter role to remove users or groups and change the permissions associated with the role. It is especially useful to modify roles when you want to change or eliminate the permissions used by an entire role.

About this task

You cannot modify or remove permissions for the SnapCenterAdmin role.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Roles**.
3. From the Role name field, click the role you want to modify.
4. In the **Role Details** page alter the permissions or unassign the members as needed.
5. Select **All members of this role can see other members' objects** to enable other members of the role to see resources such as volumes and hosts after they refresh the resources list. Deselect this option if you do not want members of this role to see objects to which other members are assigned.

Note: When this option is enabled, assigning users access to objects or resources is not required if users belong to the same role as the user who created the objects or resources.

6. Click **Submit**.

Modifying SnapCenter users or groups

You can modify SnapCenter users or groups to alter their roles and assets.

Before you begin

You must be logged in as the SnapCenter administrator.

Steps

1. In the left navigation pane, click **Settings**.
2. On the **Settings** page, click **Users and Access**.
3. From the User or Group name list, click the user or group that you want to modify.
4. On the User or Group details page, alter roles and assets.
5. Click **Submit**.

Application-level role-based access control

Application-level role-based access control (RBAC) enables SnapCenter users to provide credentials for access to applications such as SQL Server or Oracle databases.

For information on how to set up credentials, see the data protection documentation for the specific plug-in.

[NetApp SnapCenter Software Resources](#)

Using the Dashboard

From the SnapCenter left navigation pane, the Dashboard gives you a first glance into the health of your system, including recent job activity, alerts, protection summary, storage efficiency and usage, status of SnapCenter jobs (Backup, Clone, Restore), configuration status for standalone and Windows cluster hosts, number of Storage Virtual Machines (SVMs) managed by SnapCenter, and license capacity.

Viewing Dashboard information

From the SnapCenter left navigation pane, you can view various Dashboard tiles, or displays, along with associated system details. The number of displays available in the Dashboard is fixed and cannot be changed. The content provided within each display is dependent on role-based access control (RBAC).

Steps

1. In the left navigation pane, click **Dashboard**.
2. Click the active areas on each display to obtain additional information.

For example, clicking a donut chart in the Jobs display redirects you to the Monitor page for more information about your selection. Clicking a donut chart in the Protection Summary display redirects you to the Reports page, which can provide more information about your selection.

Information provided in the Dashboard

The Dashboard gives you a first glance into the health of your system through a series of fixed tiles, or displays. These displays cover job activities, alerts, resource protection status, primary and secondary storage usage, host configuration, licensing status, jobs that cover backup, restore and clone operations, and SVMs registered with SnapCenter. Understanding what information is provided in the SnapCenter Dashboard can be helpful in monitoring SnapCenter activity and managing data protection services.

Information displayed in the Dashboard view depends on the role assigned to the user that is currently logged in to SnapCenter. Some content might not be displayed if the user does not have permission to view that information.

In many cases, you can view more information about a display by hovering on **i**. In some cases, information in dashboard displays is linked to detailed source information in SnapCenter GUI pages such as Resources, Monitor, and Reports.

Recent Job Activities

The Recent Job Activities tile displays the latest job activity from any Backup, Restore, and Clone jobs that you have access to. Jobs in this display have one of the following states: Completed, Warning, Failed, Running, Queued, and Canceled.

Hovering over a job provides more information. You can view additional job information by clicking a specific job number, which redirects you to the Monitor page. From there, you can get job details or log information, and generate a report specific to that job.

Click **See All** to view a history of all SnapCenter jobs.

Alerts

The Alerts tile displays the latest unresolved Critical and Warning alerts for the hosts and SnapCenter Server.

The total count of Critical and Warning category alerts is shown at the top of the display. Clicking the Critical or Warning totals redirects you to the Alerts page with the specific filter applied in the Alerts page.

Clicking a specific alert redirects you to the Alerts page for details about that alert.

Clicking **See All** at the bottom of the display redirects you to the Alerts page for a list of all alerts.

Latest Protection Summary

The Latest Protection Summary tile gives you the protection status for all entities that you have access to. By default, the display is set to provide the status for all plug-ins. Status information is provided for resources backed up to primary storage as Snapshot copies, and to secondary storage using SnapMirror and SnapVault technologies. The availability of protection status information for secondary storage is based on the selected plug-in type.

Note: If you are using a mirror-vault protection policy, the counters for the protection summary are displayed in the SnapVault summary chart and not in the SnapMirror chart.

Protection status for individual plug-ins is available by selecting a plug-in from the drop-down menu. A donut chart shows the percentage of protected resources for the selected plug-in. Clicking a donut slice redirects you to the **Reports > Plug-in** page, which provides a detailed report of all primary and secondary storage activity for the specified plug-in.

Note: Reports about secondary storage apply to SnapVault only; SnapMirror reports are not supported.

Note: SAP HANA provides protection status information for primary and secondary storage for Snapshot copies. Only primary storage protection status is available for file-based backups.

Primary and secondary storage resource protection states	
Failed	Primary: Count of entities that are part of a Resource Group, where the Resource Group has run a backup, but the backup failed.
	Secondary: Count of entities with backups that have failed to transfer to a Secondary destination.
Successful	Primary: Count of entities in a resource group, where the Resource Group has been successfully backed up.
	Secondary: Count of entities with backups that have been successfully transferred to a Secondary destination.
Not configured	Primary: Count of entities that are not part of any Resource Group and have not been backed up.
	Secondary: Count of entities that are part of one or more Resource Groups that are not configured for backups to be transferred to a Secondary destination.
Not initiated	Primary: Count of entities that are part of a Resource Group, but no backup has been run.
	Secondary: Not applicable.

Note: If you use SnapCenter Server 4.2 and an earlier version of the plug-in (earlier than 4.2) to create backups, the Latest Protection Summary tile does not display the SnapMirror protection status of these backups.

Jobs

The Jobs tile provides you with a summary of backup, restore, and clone jobs that you have access to. You can customize the time frame for any report by using the drop-down menu. Time frame options are fixed at last 24 hours, last 7 days, and last 30 days. The default report shows data protection jobs run during the last 7 days.

Backup, restore, and clone job information is displayed in donut charts. Clicking a donut slice redirects you to the Monitor page with job filters pre-applied to the selection.

Backup, restore, and clone job status	
Failed	Count of jobs that have failed.
Warning	Count of jobs that have experienced an error.
Successful	Count of jobs that have completed successfully.
Running	Count of jobs that are currently running.

Storage

The Storage tile displays the primary and secondary storage consumed by protection jobs over a 90-day period, graphically depicts consumption trends, and calculates primary storage savings. Storage information is updated once every 24 hours at 12 a.m.

The day's consumption total, which comprises the total number of backups that are available in SnapCenter and size occupied by these backups, will be displayed at the top of the display. A backup could have multiple Snapshot copies associated with it and the count will reflect the same. This is applicable to both primary and secondary Snapshot copies. For example, you have created 10 backups, out of which 2 are deleted due to policy-based backup retention and 1 backup is explicitly deleted by you. Thus, a count of 7 backups will be displayed along with the size occupied by these 7 backups.

The Storage Savings factor for primary storage is the ratio of logical capacity (clone and Snapshot copy savings plus storage consumed) to the physical capacity of primary storage. A bar chart illustrates the storage savings.

The line graph separately plots primary and secondary storage consumption on a day-by-day basis over a rolling 90-day period. Hovering over the charts provides detailed day-by-day results.

Note: If you use SnapCenter Server 4.2 and an earlier version of the plug-in (earlier than 4.2) to create backups, the Storage tile does not display the number of backups, the storage consumed by these backups, the Snapshot savings, the clone savings, and the Snapshot size.

Configuration

The Configuration tile provides consolidated status information for all active stand-alone and Windows cluster hosts that SnapCenter is managing, and that you have access to. This includes the plug-in status information associated with those hosts.

Clicking the number adjacent to Hosts redirects you to the Managed Hosts section in the Hosts page. From there, you can obtain detailed information for a selected host.

Additionally, this display shows the sum of Standalone ONTAP SVMs and Cluster ONTAP SVMs that SnapCenter is managing and that you have access to. Clicking the number adjacent to SVM redirects you to the Storage Systems page. From there, you can obtain detailed information for a selected SVM.

The Host configuration state is presented as red (critical), yellow (warning), and green (active), along with the number of hosts in each state. Status messages are provided for each state.

Host configuration status	
Upgrade mandatory	Count of hosts that are running unsupported plug-ins and need an upgrade. An unsupported plug-in is not compatible with this version of SnapCenter.
Migration mandatory	Count of hosts that are running unsupported plug-ins and need migration. An unsupported plug-in is not compatible with this version of SnapCenter.
No plug-ins installed	Count of hosts that are added successfully but the plug-ins need to be installed, or the plug-ins installation has failed.
Suspended	Count of hosts whose schedules are suspended and are under maintenance.
Stopped	Count of hosts that are up, but the plug-in services are not running.
Host down	Count of hosts that are down or not reachable.
Upgrade available (optional)	Count of hosts where a newer version of the plug-in package is available for upgrade.
Migration available (optional)	Count of hosts where a newer version of the plug-in is available for migration.
Configure log directory	Count of hosts where the log directory has to be configured for SCSQL to take transaction log backup.
Configure VMware plug-ins	Count of hosts where the VMware virtual machines' SCV host needs to be added.
Unknown	Count of hosts that have been registered but the installation is not yet triggered.
Running	Count of hosts that are up and plug-ins are running. And in the case of SCSQL plug-ins, log directory and hypervisor are configured.
Installing\Uninstalling plug-ins	Count of hosts where plug-in installation or uninstallation in progress.

Licensed Capacity

The Licensed Capacity tile displays information about total licensed capacity, used capacity, capacity threshold alerts, and license expiration alerts for SnapCenter Standard capacity-based licenses.

Note: This display appears only if you are using SnapCenter Standard capacity-based licenses on Cloud Volumes ONTAP or ONTAP Select platforms. For FAS or AFF platforms, the SnapCenter license is controller-based and licensed for unlimited capacity, and no capacity license is required.

Licensed Capacity	
In use	Amount of capacity currently in use.
Notify	Capacity threshold at which notifications are displayed on the Dashboard, and, if configured, when email notifications are sent.
Licensed	Amount of licensed capacity.
Over	Amount of capacity that has exceeded the licensed capacity.

Requesting Jobs status reports from the Dashboard

You can request reports about backup, restore, and clone jobs from the Dashboard page. This is useful if you want to identify the total number of successful or failed jobs in your SnapCenter environment.

Steps

1. In the left navigation pane, click **Dashboard**
2. Locate the **Jobs** tile in the **Dashboard**, and then select **Backup, Restore, or Clone**.
3. Using the pull-down menu, select the time frame for which you want Jobs information: 24 hours, 7 days, or 30 days.
The systems display a donut chart covering the data.
4. Click the donut slice representing the job information for which you want a report.
When you click the donut chart, you are redirected from the Dashboard page to the Monitor page. The Monitor page displays the jobs with the status you selected from the donut chart.
5. From the **Monitor** page list, click on a specific job to select it.
6. At the top of the **Monitor** page, click **Reports**.

Result

The report displays information only for the job you selected. You can review the report or download it to your local system.

Requesting Protection status reports from the Dashboard

You can request protection details for resources managed by specific plug-ins using the Dashboard.

About this task

Only data backups are considered for data protection summary.

Steps

1. In the left navigation pane, click **Dashboard**.
2. Locate the **Latest Protection Summary** tile in the Dashboard and use the pull-down menu to select a plug-in.

The Dashboard displays a donut chart for resources backed up to Primary storage and, if applicable to the plug-in, a donut chart for resources backed up to secondary storage.

Note: Data protection reports are available only for specific plug-ins types. Specifying “All Plug-ins” is not supported.

3. Click the donut slice representing the status for which you want a report.

Note: Redirection to the Reports page for SnapMirror donut chart is not supported.

Note: Redirection to the Reports page for File-based SAP HANA backup is not supported.

Result

When you click the donut chart, you are redirected from Dashboard page to the Reports, and then to the Plug-inpage. The report displays only status for the plug-in you selected. You can review the report or download it to your local system.

Using SnapCenter reporting capabilities

SnapCenter provides a variety of reporting options that enable you to monitor and manage your system health and operation success.

Accessing SnapCenter reports

You can use the SnapCenter Dashboard to get a quick overview of the health of your system. From the Dashboard you can drill into more details. Alternatively, you can access the detailed reports directly.

Step

1. Access reports by one of the following methods:
 - In the left navigation pane, click **Dashboard**, and then click **Last Protection Summary** pie chart to see more details in the Reports page.
 - In the left navigation pane, click **Reports**.

Types of reports

SnapCenter provides customizable report options that provide you with details about your data protection jobs and plug-in resource status.

Report type	Description
Backup Report	The Backup Report provides overall data about backup trends for your SnapCenter environment, the backup success rate, and some information about each backup performed during the specified time. If a backup is deleted, the report does not display any status information for the deleted backup. The Backup Detail Report provides detailed information about a specified backup job and lists the resources successfully backed up and any that have failed.
Clone Report	The Clone Report provides overall data about clone trends for your SnapCenter environment, the clone success rate, and some information about each clone job performed during the specified time. If a clone is deleted, the report does not display any status information for the deleted clone. The Clone Detail Report provides details about the specified clone, including policy, resource group, clone host, and clone job task status. If a task fails, the Clone Detail Report displays information about the failure.
Restore Report	The Restore Report provides overall information about restore jobs. The Restore Detail Report provides details about a specified restore job, including host name, backup name, job start and duration, and the status of individual job tasks. If a task fails, the Restore Detail Report displays information about the failure.

Report type	Description
Plug-in Report	These reports provide protection details for resources managed by all SnapCenter plug-in instances. You can see an overview, details about databases outside of resource groups (unprotected), databases that have not been backed up during this report period, databases that belong to a resource group for which backups have failed, and database SnapVault status.

Filtering your report data

You might want to filter your report data according to a range of parameters, depending on the level of detail and time span of information you require.

Steps

1. In the left navigation pane, click **Reports**.
2. If the **Parameter** view is not displayed, click the **Toggle Parameters Area** icon from the report toolbar.
3. Specify the time range for which you want to run your report.
If you omit the end date, you retrieve all available information.
4. Filter your report information based on any of the following criteria:
 - Resource group
 - Host
 - Policy
 - Resource
 - Status
5. Click **Apply**.

Exporting or printing reports

Exporting SnapCenter reports enables you to view the report in a variety of alternative formats. You can also print reports.

Steps

1. In the left navigation pane, click **Reports**.
2. From the reports toolbar:

If you want to...	Do this...
Preview a printable report	Click the Toggle Print Preview icon.

If you want to...	Do this...
Export a report to an alternate format	Choose a format from the Export icon drop-down list: <ul style="list-style-type: none"> • CSV • Excel • PDF • Rich Text Format • TIFF • Web Archive

3. To print a report, click the **Print** icon.
4. To view a specific report summary, scroll to the appropriate section of the report.

Setting the SMTP server for email notifications using Global Settings

You can specify the SMTP server to use for sending data protection job reports to yourself or to others. You can also send a test email to verify the configuration. The settings are applied globally for any SnapCenter job for which you configure email notification.

About this task

This option configures the SMTP server for sending all data protection job reports. However, if you want to have regular SnapCenter data protection job updates for a particular resource sent to yourself or to others so that you can monitor the status of those updates, you can configure the option to email the SnapCenter reports when you are creating a resource group.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Global Settings**.
3. Enter the SMTP server and click **Save**.
4. To send a test email, enter the email address from and to which you will send the email, enter the subject, and click **Send**.

Configuring the option to email reports

If you want to have regular SnapCenter data protection job updates sent to yourself or to others so that you can monitor the status of those updates, you can configure the option to email the SnapCenter reports when you are creating a resource group.

Before you begin

You must have configured your SMTP server on the Global Settings page under Settings.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. Select the type of resource you want to view and click **New Resource Group**, or select an existing resource group and click **Modify** to configure email reports for an existing resource group.

3. In the **Notification** panel of the **New Resource Group** wizard, select from the pull-down menu whether you want to receive reports always, on failure, or on failure or warning.
4. Enter the address the email is sent from, the address the email is sent to, and the subject of the email.

Monitoring jobs, schedules, events, and logs

You can monitor the progress of your jobs, get information about scheduled jobs, and review events and logs from the Monitor page.

Monitoring SnapCenter jobs

You can view information about SnapCenter backup, clone, restore, and verification jobs. You can filter this view based on start and end date, type of job, resource group, policy, or SnapCenter plugin. You can also get additional details and log files for specified jobs.

You can also monitor jobs related to SnapMirror and SnapVault operations.

You can monitor only the jobs that you created and that are relevant to you unless you are assigned SnapCenter Admin or another super user role.

You can perform the following tasks related to monitoring jobs:

- Monitor backup, clone, restore, and verification operations.
- View job details and reports.
- Stop a scheduled job.

Monitoring SnapCenter schedules

You might want to view current schedules to determine when the operation starts, when it was last run, and when it runs next. You can also determine the host on which the operation runs, along with the operation's resource group and policy information.

Steps

1. In the left navigation pane, click **Monitor**.
2. In the Monitor page, click **Schedules**.
3. Select the resource group and the schedule type.
4. View the list of scheduled operations.

Monitoring SnapCenter events

You can view a list of SnapCenter events in the system, such as when a user creates a resource group or when the system initiates activities, such as creating a scheduled backup. You might want to view events to determine if an operation such as a backup or a restore operation is currently in progress.

About this task

All job information appears in the Events page. For example, when a backup job starts, a “backup start” event appears. When the backup completes, a “backup complete” event appears.

Steps

1. In the left navigation pane, click **Monitor**.
2. In the Monitor page, click **Events**.

3. Optional. In the Filter box, enter the start or end date, category of event (such as backup, resource group, or policy) and severity level, and click **Apply**. Alternatively, enter characters in the Search box.
4. View the list of events.

Monitoring SnapCenter logs

You can view and download SnapCenter server logs, SnapCenter host agent logs, and plug-in logs. You might want to view the logs to help with troubleshooting.

You can filter the logs to show only a specific log severity level:

- Debug
- Info
- Warn
- Error
- Fatal

You can also obtain job level logs: for example, logs that help you troubleshoot the reason for a backup job failure. For job level logs, use the **Monitor > Jobs** option.

Steps

1. In the left navigation pane, click **Monitor**.
2. In the Monitor page, click **Logs**.
3. Select the log type, host, and instance.
If you select a log type of **plugin**, you can select a host or SnapCenter plug-in. You cannot do this if the log type is **server**.
4. To filter the logs by a specific source, message, or log level, click the filter icon at the top of the column heading.
To show all logs, choose “Greater than or equal to” as the “Debug” level.
5. Click **Refresh**.
6. View the list of logs.

In large configurations for optimum performance, you should set the log settings for SnapCenter to minimal level by using the PowerShell cmdlet.

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10 -
JobLogsMaxFileSize 10MB -Server
```

The information regarding the parameters that can be used with the command and their descriptions can be obtained by running `help command_name`. Alternatively, you can also refer to the *Command Reference Guide*.

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

Removing jobs and logs from SnapCenter

You can remove backup, restore, clone, and verification jobs and logs from SnapCenter. SnapCenter stores successful and failed job logs indefinitely unless you remove them. You might want to remove them to replenish storage.

Before you begin

There must be no jobs currently in operation.

About this task

You can remove a specific job by providing a Job ID or you can remove jobs within a specified period.

You do not need to place the host in maintenance mode to remove jobs.

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. Launch PowerShell.
2. From the command prompt, enter:

```
Open-SMConnection
```

3. From the command prompt, enter:

```
Remove-SmJobs
```

4. In the left navigation pane, click **Monitor**.
5. In the **Monitor** page, click **Jobs**.
6. In the **Jobs** page, review the status of the job.

Managing the SnapCenter Server repository

Information related to various operations performed from SnapCenter is stored in the SnapCenter Server database repository. You must create backups of the repository to protect the SnapCenter Server from data loss.

You can perform the following tasks to protect the SnapCenter Server repository:

- Set the configuration that is required to create repository backups.
- Obtain the SnapCenter repository backups that were backed up on schedule.
- Restore the SnapCenter repository when required.
- Migrate the SnapCenter repository to a different disk.

The SnapCenter Server repository is sometimes referred to as the NSM database.

Prerequisites for protecting the SnapCenter repository

Your environment must meet certain prerequisites to protect the SnapCenter repository.

- Managing storage virtual machine (SVM) connections
You must configure the storage credentials.
- Provisioning hosts
At least one NetApp storage disk should be present on the SnapCenter repository host. If a NetApp disk is not present on the SnapCenter repository host, you must create one.
For details about adding hosts, setting up SVM connections, and provisioning hosts, see the installation instructions.
- Provisioning iSCSI LUN or VMDK
For a network load balance balancing (NLB) configuration, you can provision either a iSCSI LUN or a VMDK in one of the SnapCenter Servers.

Related concepts

[Provisioning storage on Windows hosts](#) on page 42

Backing up the SnapCenter repository

Backing up the SnapCenter Server repository helps protect it from data loss. You can back up the repository by running the `Protect-SmRepository` cmdlet.

About this task

The `Protect-SmRepository` cmdlet accomplishes the following tasks:

- Creates a resource group and a policy
- Creates a backup schedule for the SnapCenter repository

Steps

1. Launch PowerShell.

2. On the SnapCenter Server host, establish a session using the `Open-SmConnection` cmdlet, and then enter your credentials.
3. Back up the repository using the `Protect-SmRepository` cmdlet and the required parameters.

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](#)

Viewing backups of the SnapCenter repository

You can display a list of SnapCenter Server database repository backups by running the `Get-SmRepositoryBackups` cmdlet.

About this task

The repository backups are created according to the schedule specified in the `Protect-SmRepository` cmdlet. You can also create repository backups from the SnapCenter GUI.

Steps

1. Launch PowerShell.
2. From the command prompt, enter the following cmdlet, and then provide credentials to connect to the SnapCenter Server:

```
Open-SMConnection
```

3. List all available SnapCenter database backups using the `Get-SmRepositoryBackups` cmdlet.
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](#)

Restoring a SnapCenter database repository

You can restore the SnapCenter repository by running the `Restore-SmRepositoryBackup` cmdlet.

About this task

When you are restoring the SnapCenter repository, other SnapCenter operations that are running will be impacted because during the restore operation the repository database is not accessible.

Steps

1. Launch PowerShell.
2. From the command prompt, enter the following cmdlet, and then provide credentials to connect to the SnapCenter Server:

```
Open-SMConnection
```

3. Restore the repository backup using the `Restore-SmRepositoryBackup` cmdlet.

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

The following cmdlet restores the SnapCenter MySQL database repository from the backups existing on either iSCSI LUN or VMDK:

```
C:\PS>Restore-SmRepositoryBackup -BackupName
MySQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445
```

The following cmdlet restores the SnapCenter MySQL database when backup files are deleted accidentally in the iSCSI LUN. For VMDK manually restore the backup from ONTAP Snapshot copies.

```
C:\PS>Restore-SmRepositoryBackup -BackupName
MySQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445 -
RestoreFileSystem
```

Migrating the SnapCenter repository

You can migrate the SnapCenter Server database repository from the default location to another disk. You might migrate the repository when you want to relocate it to a disk with more space.

Steps

1. Stop the MYSQL57 service in Windows.
2. Locate the MySQL data directory.
You can usually find the data directory at C:\ProgramData\MySQL\MySQL Server 5.7\Data.
3. Copy the MySQL data directory to the new location, for example, E:\Data\nsm.
4. Right click on the new directory, and then select **Properties > Security** to add the Network Service local server account to the new directory, and then assign the account full control.
5. Rename the original database directory, for example, nsm_copy.
6. From a Windows command prompt, create a symbolic directory link by using the mklink command.

Example

```
"mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
```

7. Start the MYSQL57 service in Windows.
8. Verify that the database location change is successful by logging in to SnapCenter and checking repository entries, or by logging in to the MySQL utility and connecting to the new repository.
9. Delete the original, renamed, database repository directory (nsm_copy).

Resetting the SnapCenter repository password

The MySQL Server repository database password is automatically generated during SnapCenter Server installation from SnapCenter 4.2. This automatically generated password is not known to

SnapCenter user at any point. If you want to access the repository database, you should reset the password.

Before you begin

You should have the SnapCenter administrator privileges to reset the password.

Steps

1. Launch PowerShell.
2. From the command prompt, enter the following command, and then provide the credentials to connect to the SnapCenter Server:

```
Open-SMConnection
```

3. Reset the repository password:

```
Set-SmRepositoryPassword
```

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](#)

The following command resets the repository password:

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: *****
ConfirmPassword: *****
Successfully updated the MySQL server password.
```

Managing hosts

You can add hosts and install SnapCenter plug-in packages, add a verification server, remove hosts, migrate SnapCenter Plug-in for Microsoft SQL Server backup jobs, and update host to upgrade plug-in packages or add new plug-in packages.

You can perform these tasks...	By using the SnapCenter Plug-in for...					
	Microsoft Exchange Server	Microsoft SQL Server	Microsoft Windows	Oracle Database	SAP HANA Database	Custom Plug-ins
Add hosts and install plug-in package See installation documentation.	✓	✓	✓	✓	✓	✓
Update ESXi information for a host		✓				
Suspend schedules and place hosts in maintenance mode	✓	✓	✓	✓	✓	✓
Modify hosts by adding, upgrading, or removing plug-ins	✓	✓	✓	✓	✓	✓
Remove hosts from SnapCenter	✓	✓	✓	✓	✓	✓
Start plug-in services	✓	✓	✓	✓	✓	✓
Import backup jobs from Microsoft SQL Server, SnapManager for SQL Server, SnapManager for Oracle, or SnapManager for SAP. See installation documentation.		✓		✓		

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](#)

Related information

[Installing and setting up SnapCenter](#)

Refreshing virtual machine information

You must refresh your virtual machine information when VMware vCenter credentials change or the database or file system host restarts.

About this task

Refreshing your virtual machine information in SnapCenter initiates communication with the VMware vSphere vCenter and obtains vCenter credentials.

RDM-based disks are managed by the SnapCenter Plug-in for Microsoft Windows, which is installed on the database host. To manage RDMs, the SnapCenter Plug-in for Microsoft Windows communicates with the vCenter server that manages the database host.


Steps

1. In the SnapCenter left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Managed Hosts**.
3. In the **Managed Hosts** page, select the host you want to update.
4. Click **Refresh VM**.

Starting and restarting plug-in services

Starting SnapCenter plug-in services enables you start services if they are not running or restart them if they are running. You might want to restart services after maintenance has been performed.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Managed Hosts**.
3. In the **Managed Hosts** page, select the host you want to start.
4. Click  icon and click **Start Service** or **Restart Service**.

You can start or restart service of multiple hosts simultaneously.


Suspending schedules on hosts to place them in maintenance mode

When you want to prevent the host from running any SnapCenter scheduled jobs, you can place your host in maintenance mode. You must do this before you upgrade the plug-ins. You might want to do this if you are performing maintenance tasks on hosts.

About this task

You cannot suspend the schedules on a host that is down because SnapCenter cannot communicate with that host.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Managed Hosts**.
3. In the **Managed Hosts** page, select the host that you want to suspend.
4. Click the  icon, and then click **Suspend Schedule** to place the host for this plug-in in maintenance mode.

You can suspend the schedule of multiple hosts simultaneously.

Note: You do not have to stop the plug-in service first. The plug-in service can be in a running or stopped state.

After you suspend the schedules on the host, the Managed Hosts page shows “Suspended” in the Overall status field for the host.

After you finish

After you complete host maintenance, bring the host out of maintenance mode by clicking **Activate Schedule**.

You can activate the schedule of multiple hosts simultaneously.

Managing resources of untrusted domains

In addition to managing hosts in Active Directory (AD) trusted domains, SnapCenter also manages hosts in multiple AD untrusted domains. The untrusted AD domains must be registered with the SnapCenter Server. SnapCenter supports users and groups of multiple untrusted AD domains.

You can install the SnapCenter Server on a machine that is in either a domain or a workgroup. To install the SnapCenter Server, you should specify the domain credentials if the machine is in a domain or the local administrator credentials if the machine is in a workgroup.

Active Directory (AD) groups that belong to domains not registered with the SnapCenter Server are not supported. Although you can create SnapCenter roles with these AD groups, logging in to SnapCenter Server fails with the following error message: The user you are trying to login does not belong to any roles. Please contact your administrator.

Registering untrusted Active Directory domains

You must register the Active Directory with SnapCenter Server to register and manage hosts, users, and groups from multiple untrusted Active Directory domains.


Before you begin

- The fully qualified domain name (FQDN) should be reachable from SnapCenter Server.
- If the FQDN is not resolvable, the domain controller IP addresses that are provided should be resolvable from SnapCenter Server.
- You must have enabled bidirectional communication between the plug-in hosts and the SnapCenter Server.
- DNS resolution must have been set up from the SnapCenter Server to the plug-in hosts and vice-versa.

About this task

- To register an untrusted domain, you can use either the SnapCenter user interface or PowerShell cmdlets.
- You can register an untrusted domain with the FQDN. If the FQDN is not resolvable from the SnapCenter Server, you can register with an IP address.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Global Settings**.
3. In the **Global Settings** page, click **Domain Settings**.
4. Click  to register a new domain.
5. In the **Register New Domain** page, specify the information that is required for registering the untrusted domain:

For this field...	Do this...
Domain Name	Specify the NetBIOS name for the domain.

For this field...	Do this...
Domain FQDN	Specify the FQDN and click Resolve .
Domain controller IP addresses	If the domain FQDN is not resolvable from the SnapCenter Server, specify one or more domain controller IP addresses. <i>NetApp Knowledgebase Answer 1087234: SnapCenter does not allow to add Domain Controller IP for untrusted domain from GUI</i>

6. Click **OK**.

After you finish

After you finish registering the host of this domain, you should perform the following tasks:

- Add hosts
- Add users or groups to this domain
- Assign roles to the users or groups of this domain

Related tasks

Adding a user or group and assigning role and assets on page 6

Related information

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

Modifying untrusted domains

You can modify an untrusted domain when you want to update the domain controller IP addresses or the fully qualified domain name (FQDN).


About this task

After you modify the FQDN, the associated assets (hosts, users, and groups) might not function as expected.

To modify an untrusted domain, you can use either the SnapCenter user interface or PowerShell cmdlets.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Global Settings**.
3. In the **Global Settings** page, click **Domain Settings**.

4. Click  , and then provide the following details:

For this field...	Do this...
Domain FQDN	Specify the FQDN, and click Resolve .

For this field...	Do this...
Domain controller IP addresses	If the domain FQDN is not resolvable, specify one or more domain controller IP addresses.

5. Click **OK**.

Related information

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

Unregistering untrusted Active Directory domains

You can unregister an untrusted Active Directory domain if you do not want to use the assets that are associated with that domain.


Before you begin

You must have removed the hosts, users, groups, and credentials that are associated with the untrusted domain.

About this task

- After the domain is unregistered from SnapCenter Server, users of that domain cannot access SnapCenter Server.
- If there are associated assets (hosts, users, and groups), after unregistering the domain, the assets will be non-operational.
- To unregister an untrusted domain, you can use either the SnapCenter user interface or PowerShell cmdlets.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Global Settings**.
3. In the **Global Settings** page, click **Domain Settings**.
4. From the list of domains, select the domain that you want to unregister.
5. Click , and then click **OK**.

Related information

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

Configuring secured MySQL connections with SnapCenter Server

You can generate Secure Sockets Layer (SSL) certificates and key files if you want to secure the communication between SnapCenter Server and MySQL Server in standalone configurations or Network Load Balancing (NLB) configurations.

Configuring secured MySQL connections for standalone SnapCenter Server configurations

You can generate Secure Sockets Layer (SSL) certificates and key files, if you want to secure the communication between SnapCenter Server and MySQL Server. You must configure the certificates and key files in the MySQL Server and SnapCenter Server.

Before you begin

SnapCenter Server must be installed.

About this task

The following certificates are generated:

- CA certificate
- Server public certificate and private key file
- Client public certificate and private key file

Steps

1. Set up the SSL certificates and key files for MySQL servers and clients on Windows by using the `openssl` command.

MySQL Version 5.7: Creating SSL Certificates and Keys Using openssl

Note: The common name value that is used for the server certificate, client certificate, and key files must each differ from the common name value that is used for the CA certificate. If the common name values are the same, the certificate and key files fail for servers that are compiled by using OpenSSL.

Best Practice: You should use the server fully qualified domain name (FQDN) as the common name for the server certificate.

2. Copy the SSL certificates and key files to the MySQL Data folder.
The default MySQL Data folder path is `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.
3. Update the CA certificate, server public certificate, client public certificate, server private key, and client private key paths in the MySQL server configuration file (`my.ini`).
The default MySQL server configuration file (`my.ini`) path is `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.

Note: You must specify the CA certificate, server public certificate, and server private key paths in the `[mysqld]` section of the MySQL server configuration file (`my.ini`).

You must specify the CA certificate, client public certificate, and client private key paths in the [client] section of the MySQL server configuration file (`my.ini`).

Example

The following example shows the certificates and key files copied to the [mysqld] section of the `my.ini` file in the default folder `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

The following example shows the paths updated in the [client] section of the `my.ini` file.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. Stop the SnapCenter Server web application in the Internet Information Server (IIS).
5. Restart the MySQL service.
6. Update the value of the `MySQLProtocol` key in the `web.config` file.

Example

The following example shows the value of the `MySQLProtocol` key updated in the `web.config` file.

```
<add key="MySQLProtocol" value="SSL" />
```

7. Update the `web.config` file with the paths that were provided in the [client] section of the `my.ini` file.

Example

The following example shows the paths updated in the [client] section of the `my.ini` file.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem" />
```

8. Start the SnapCenter Server web application in the IIS.

Configuring secured MySQL connections for NLB configurations

You can generate Secure Sockets Layer (SSL) certificates and key files for both the Network Load Balancing (NLB) nodes if you want to secure the communication between SnapCenter Server and MySQL servers. You must configure the certificates and key files in the MySQL servers and on the NLB nodes.

Before you begin

SnapCenter Server must be installed.

About this task

The following certificates are generated:

- CA certificate
A CA certificate is generated on one of the NLB nodes, and this CA certificate is copied to the other NLB node.
- Server public certificate and server private key files for both the NLB nodes
- Client public certificate and client private key files for both the NLB nodes

Steps

1. For the first NLB node, set up the SSL certificates and key files for MySQL servers and clients on Windows by using the `openssl` command.

MySQL Version 5.7: Creating SSL Certificates and Keys Using openssl

Note: The common name value that is used for the server certificate, client certificate, and key files must each differ from the common name value that is used for the CA certificate. If the common name values are the same, the certificate and key files fail for servers that are compiled by using OpenSSL.

Best Practice: You should use the server fully qualified domain name (FQDN) as the common name for the server certificate.

- a. Copy the SSL certificates and key files to the MySQL Data folder.

The default MySQL Data folder path is `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.

- b. Update the CA certificate, server public certificate, client public certificate, server private key, and client private key paths in the MySQL server configuration file (`my.ini`).

The default MySQL server configuration file (`my.ini`) path is `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.

Note: You must specify CA certificate, server public certificate, and server private key paths in the `[mysqld]` section of the MySQL server configuration file (`my.ini`).

You must specify CA certificate, client public certificate, and client private key paths in the `[client]` section of the MySQL server configuration file (`my.ini`).

Example

The following example shows the certificates and key files copied to the `[mysqld]` section of the `my.ini` file in the default folder `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

The following example shows the paths updated in the `[client]` section of the `my.ini` file.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

2. For the second NLB node, copy the CA certificate and generate server public certificate, server private key files, client public certificate, and client private key files. perform the following steps:

- a. Copy the CA certificate generated on the first NLB node to the MySQL Data folder of the second NLB node.

The default MySQL Data folder path is `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.

Note: You must not create a CA certificate again. You should create only the server public certificate, client public certificate, server private key file, and client private key file.

- b. For the first NLB node, set up the SSL certificates and key files for MySQL servers and clients on Windows by using the `openssl` command.

MySQL Version 5.7: Creating SSL Certificates and Keys Using openssl

Note: The common name value that is used for the server certificate, client certificate, and key files must each differ from the common name value that is used for the CA certificate. If the common name values are the same, the certificate and key files fail for servers that are compiled by using OpenSSL.

It is recommended to use the server FQDN as the common name for the server certificate.

- c. Copy the SSL certificates and key files to the MySQL Data folder.
- d. Update the CA certificate, server public certificate, client public certificate, server private key, and client private key paths in the MySQL server configuration file (`my.ini`).

Note: You must specify the CA certificate, server public certificate, and server private key paths in the `[mysqld]` section of the MySQL server configuration file (`my.ini`).

You must specify the CA certificate, client public certificate, and client private key paths in the `[client]` section of the MySQL server configuration file (`my.ini`).

Example

The following example shows the certificates and key files copied to the `[mysqld]` section of the `my.ini` file in the default folder `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/Data`.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

The following example shows the paths updated in the `[client]` section of the `my.ini` file.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

3. Stop the SnapCenter Server web application in the Internet Information Server (IIS) on both the NLB nodes.
4. Restart the MySQL service on both the NLB nodes.
5. Update the value of the `MySQLProtocol` key in the `web.config` file for both the NLB nodes.

Example

The following example shows the value of `MySQLProtocol` key updated in the `web.config` file.

```
<add key="MySQLProtocol" value="SSL" />
```

6. Update the `web.config` file with the paths that you specified in the `[client]` section of the `my.ini` file for both the NLB nodes.

Example

The following example shows the paths updated in the [client] section of the my.ini files.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem" />
```

7. Start the SnapCenter Server web application in the IIS on both the NLB nodes.
8. Use the `Set-SmRepositoryConfig -RebuildSlave -Force` PowerShell cmdlet with the `-Force` option on one of the NLB nodes to establish secured MySQL replication on both the NLB nodes.

Even if the replication status is healthy, the `-Force` option allows you to rebuild the slave repository.

Managing the storage system

After adding the storage system, you can modify the storage system configuration or delete the storage system. You can also view whether a SnapManager Suite license is installed on a FAS or All Flash FAS on primary storage system.

Modifying storage system configuration

You can use SnapCenter to modify your storage system configuration if you want to change the user name, password, platform, port, protocol, timeout period, preferred IP address, or messaging options.

About this task

You can modify storage connections for an individual user or for a group. If you belong to one or more groups with permission to the same storage system, the storage connection name is displayed multiple times in the storage connection list, once for each group with permission to the storage system.

Steps

1. In the left navigation pane, click **Storage Systems**.
2. In the **Storage Systems** page, from the **Type** drop-down perform one of the following actions:

Select...	Steps...
ONTAP SVMs	<p>To view all the SVMs that were added and to modify the required SVM configuration.</p> <ol style="list-style-type: none"> a. In the Storage Connections page, click the SVM name. b. Perform one of the following actions: <ul style="list-style-type: none"> • If the SVM is not part of any cluster, in the Modify Storage System page, modify the configurations such as user name, password, EMS and AutoSupport settings, platform, protocol, port, timeout, and preferred IP. • If the SVM is part of a cluster, in the Modify Storage System page, select Manage SVM Independently and modify the configurations such as user name, password, EMS and AutoSupport settings, platform, protocol, port, timeout, and preferred IP. <p>After modifying the SVM to be managed independently, later if you decide to manage it through cluster, you should delete the SVM and click Rediscover. The SVM will be added to the ONTAP cluster.</p>

Select...	Steps...
ONTAP Clusters	<p>To view all the clusters that were added and modify the required cluster configuration.</p> <ol style="list-style-type: none"> a. In the Storage Connections page, click the cluster name. b. In the Modify Storage System page, click the edit icon next to Username and modify the user name and password. c. Select or clear the EMS and AutoSupport settings. d. Click More Options and modify other configurations such as platform, protocol, port, timeout, and preferred IP.

3. Click **Submit**.

Deleting the storage system

You can use SnapCenter to delete any unused storage system.

About this task

You can delete storage connections for an individual user or for a group. If you belong to one or more groups with permission to the same storage system, the storage system name is displayed multiple times in the storage connection list, once for each group with permission to the storage system.

Attention: When you are deleting a storage system, all operations that are being performed on that storage system will fail.

Steps

1. In the left navigation pane, click **Storage Systems**.
2. In the **Storage Systems** page, from the **Type** drop-down, select either **ONTAP SVMs** or **ONTAP Clusters**.
3. In the **Storage Connections** page, either select the check box next to the SVM, or the cluster that you want to delete.

Note: You cannot select the SVM that is part of a cluster.

4. Click **Delete**.
5. In the **Delete Storage System Connection Settings** page, click **OK**.

Note: If an SVM is deleted from ONTAP cluster using ONTAP GUI, in the SnapCenter GUI click **Rediscover** to update the SVM list.

Viewing SnapManager Suite storage controller license installation status using the SnapCenter GUI



You can use the SnapCenter GUI to view whether a SnapManager Suite license is installed on FAS or AFF primary storage systems, and to identify which storage systems might require SnapManager

Suite licenses. SnapManager Suite licenses apply only to FAS and AFF SVMs or clusters on primary storage systems.

Steps

1. In the left navigation pane, click **Storage Systems**.
2. In the **Storage Systems** page, from the **Type** drop-down, select whether to view all the SVMs or clusters that were added:
 - To view all of the SVMs that were added, select **ONTAP SVMs**.
 - To view all of the clusters that were added, select **ONTAP Clusters**.
When you click the cluster name, all of the SVMs that are part of the cluster are displayed in the Storage Virtual Machines section.
3. In the **Storage Connections** list, locate the **Controller License** column.

The Controller License column displays the following statuses:

	Indicates that a SnapManager Suite license is installed on a FAS or AFF primary storage system.
	Indicates that a SnapManager Suite license is not installed on a FAS or AFF primary storage system.
Not applicable	Indicates that a SnapManager Suite license is not applicable for this controller. This message is displayed for the following platforms: <ul style="list-style-type: none"> • Cloud Volumes ONTAP • ONTAP Select • Secondary storage

Provisioning storage on Windows hosts

You can use SnapCenter to assign NetApp storage to supported Windows Server hosts. Provisioning Windows hosts with SnapCenter ensures that the backups you create are application consistent. You must have installed and configured the SnapCenter Plug-ins Package for Windows.

If you are coming to SnapCenter from a NetApp SnapManager product and are satisfied with how your hosts are provisioned, you can skip this provisioning information.

As part of provisioning storage, you can perform the following tasks:

- Configure an FC-connected or iSCSI-connected LUN
 - Establish an iSCSI session to connect to a LUN
 - Create igroups to specify which hosts can access a given LUN on the storage system
 - Create, resize, and connect to a disk
- Create an SMB share on a storage virtual machine (SVM)

For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT).

[NetApp Interoperability Matrix Tool](#)

Related concepts

[Provisioning storage in VMware environments](#) on page 54

Configuring LUN storage

You can use SnapCenter to configure an FC-connected or iSCSI-connected LUN. You can also use SnapCenter to connect an existing LUN to a Windows host.

LUNs are the basic unit of storage in a SAN configuration. The Windows host sees LUNs on your system as virtual disks. For more information, see the information on ONTAP 9 SAN configuration.

[ONTAP 9 SAN Configuration Guide](#)

Establishing an iSCSI session

If you are using iSCSI to connect to a LUN, you must establish an iSCSI session before you create the LUN to enable communication.

Before you begin

- You must have defined the storage system node as an iSCSI target.
- You must have started the iSCSI service on the storage system.

[ONTAP 9 SAN Administration Guide](#)

About this task

You can establish an iSCSI session only between the same IP versions: either IPv6 to IPv6 or IPv4 to IPv4.

You can use a link-local IPv6 address for iSCSI session management and for communication between a host and a target only when both are in the same subnet.

If you change the name of an iSCSI initiator, access to iSCSI targets is affected. After changing the name, you might require to reconfigure the targets accessed by the initiator so that they can recognize the new name. You must ensure to restart the host after changing the name of an iSCSI initiator.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **iSCSI Session**.
3. From the **Storage Virtual Machine** drop-down list, select the storage virtual machine (SVM) for the iSCSI target.
4. From the **Host** drop-down list, select the host for the session.
5. Click **Establish Session**.

The Establish Session wizard is displayed.

6. In the **Establish Session** wizard, identify the target:

In this field...	Enter...
Target node name	The node name of the iSCSI target If there is an existing target node name, the name is displayed in read-only format.
Target portal address	The IP address of the target network portal
Target portal port	The TCP port of the target network portal
Initiator portal address	The IP address of the initiator network portal

7. When you are satisfied with your entries, click **Connect**.
SnapCenter establishes the iSCSI session.
8. Repeat this procedure to establish a session for each target.

Disconnecting an iSCSI session

Occasionally, you might require to disconnect an iSCSI session from a target with which you have multiple sessions.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **iSCSI Session**.
3. From the **Storage Virtual Machine** drop-down list, select the storage virtual machine (SVM) for the iSCSI target.
4. From the **Host** drop-down list, select the host for the session.
5. From the list of iSCSI sessions, select the session that you want to disconnect and click **Disconnect Session**.
6. In the **Disconnect Session** dialog box, click **OK**.
SnapCenter disconnects the iSCSI session.

Creating and managing igroups

You create initiator groups (igroups) to specify which hosts can access a given LUN on the storage system. You can use SnapCenter to create, rename, modify, or delete an igroup on a Windows host.

Creating an igroup

You can use SnapCenter to create an igroup on a Windows host. The igroup will be available in the Create Disk or Connect Disk wizard when you map the igroup to a LUN.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Igroup**.
3. In the **Initiator Groups** page, click **New**.
4. In the **Create Igroup** dialog box, define the igroup:

In this field...	Do this...
Storage System	Select the SVM for the LUN you will map to the igroup.
Host	Select the host on which you want to create the igroup.
Igroup Name	Enter the name of the igroup.
Initiators	Select the initiator.
Type	Select the initiator type, iSCSI, FCP, or mixed (FCP and iSCSI).

5. When you are satisfied with your entries, click **OK**.
SnapCenter creates the igroup on the storage system.

Renaming an igroup

You can use SnapCenter to rename an existing igroup.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Igroup**.
3. In the **Initiator Groups** page, click in the **Storage Virtual Machine** field to display a list of available SVMs, and then select the SVM for the igroup you want to rename.
4. In the list of igroups for the SVM, select the igroup you want to rename and click **Rename**.
5. In the **Rename igroup** dialog box, enter the new name for the igroup and click **Rename**.

Modifying an igroup

You can use SnapCenter to add igroup initiators to an existing igroup. While creating an igroup you can add only one host. If you want to create an igroup for a cluster, you can modify the igroup to add other nodes to that igroup.

Steps

1. In the left navigation pane, click **Hosts**.

2. In the **Hosts** page, click **Igroup**.
3. In the **Initiator Groups** page, click in the **Storage Virtual Machine** field to display a drop-down list of available SVMs, then select the SVM for the igroup you want to modify.
4. In the list of igroups, select an igroup and click **Add Initiator to igroup**.
5. Select a host.
6. Select the initiators and click **OK**.

Deleting an igroup

You can use SnapCenter to delete an igroup when you no longer need it.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Igroup**.
3. In the **Initiator Groups** page, click in the **Storage Virtual Machine** field to display a drop-down list of available SVMs, then select the SVM for the igroup you want to delete.
4. In the list of igroups for the SVM, select the igroup you want to delete and click **Delete**.
5. In the **Delete igroup** dialog box, click **OK**.

SnapCenter deletes the igroup.

Creating and managing disks

The Windows host sees LUNs on your storage system as virtual disks. You can use SnapCenter to create and configure an FC-connected or iSCSI-connected LUN.

About this task

Using SnapCenter, you can perform the following disk-related tasks:

- View the lists of disks on a host.
- Create a disk.
- Resize a disk.
- Connect to a disk.
- Disconnect from a disk.
- Delete a disk.

Note: SnapCenter does not support renaming a disk. If a disk that is managed by SnapCenter is renamed, SnapCenter operations will not succeed.

Viewing the disks on a host

You can view the disks on each Windows host you manage with SnapCenter.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Disks**.

3. Select the host from the **Host** drop-down list.

The disks are listed.

Creating FC-connected or iSCSI-connected LUNs or disks

The Windows host sees LUNs on your storage system as virtual disks. You can use SnapCenter to create and configure an FC-connected or iSCSI-connected LUN.

Before you begin

- You must have created a volume for the LUN on your storage system.
The volume should hold LUNs only, and only LUNs created with SnapCenter.
[ONTAP 9 Logical Storage Management Guide](#)
Note: You cannot create a LUN on a SnapCenter-created clone volume unless the clone has already been split.
- You must have started the FC or iSCSI service on the storage system.
[ONTAP 9 SAN Administration Guide](#)
- If you are using iSCSI, you must have established an iSCSI session with the storage system.
[Starting an iSCSI session](#) on page 42

About this task

- You cannot connect a LUN to more than one host unless the LUN is shared by hosts in a Windows Server failover cluster.
- If a LUN is shared by hosts in a Windows Server failover cluster that uses CSV (Cluster Shared Volumes), you must create the disk on the host that owns the cluster group.
- The SnapCenter Plug-ins Package for Windows must be installed only on the host on which you are creating the disk.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Disks**.
3. Select the host from the **Host** drop-down list.
4. Click **New**.

The Create Disk wizard opens.

5. On the **LUN Name** page, identify the LUN:

In this field...	Do this...
Storage System	Select the SVM for the LUN.
LUN path	Click Browse to select the full path of the folder containing the LUN.
LUN name	Enter the name of the LUN.
Cluster size	Select the LUN block allocation size for the cluster. Cluster size depends upon the operating system and applications.
LUN label	Optionally, enter descriptive text for the LUN.

6. On the **Disk Type** page, select the disk type:

Select...	If...
Dedicated disk	The LUN can be accessed by only one host. Ignore the Resource Group field.
Shared disk	The LUN is shared by hosts in a Windows Server failover cluster. Enter the name of the cluster resource group in the Resource Group field. You need only create the disk on one host in the failover cluster.
Cluster Shared Volume (CSV)	The LUN is shared by hosts in a Windows Server failover cluster that uses CSV. Enter the name of the cluster resource group in the Resource Group field. Make sure that the host on which you are creating the disk is the owner of the cluster group.

7. On the **Drive Properties** page, specify the drive properties:

Property	Description
Auto assign mount point	SnapCenter automatically assigns a volume mount point based on the system drive. For example, if your system drive is C:, auto assign creates a volume mount point under your C: drive (C:\scmntpt\). Auto assign is not supported for shared disks.
Assign drive letter	Mount the disk to the drive you select in the adjoining drop-down list.
Use volume mount point	Mount the disk to the drive path you specify in the adjoining field. The root of the volume mount point must be owned by the host on which you are creating the disk.
Do not assign drive letter or volume mount point	Choose this option if you prefer to mount the disk manually in Windows.
LUN size	Specify the LUN size; 150 MB minimum. Select MB, GB, or TB in the adjoining drop-down list.
Use thin provisioning for the volume hosting this LUN	Thin provision the LUN. Thin provisioning allocates only as much storage space as is needed at one time, allowing the LUN to grow efficiently to the maximum available capacity. Make sure there is enough space available on the volume to accommodate all the LUN storage you think you will need.
Choose partition type	Select GPT partition for a GUID Partition Table, or MBR partition for a Master Boot Record. MBR partitions might cause misalignment issues in Windows Server failover clusters.

8. On the **Map LUN** page, select the iSCSI or FC initiator on the host:

In this field...	Do this...
Host	Double-click the cluster group name to display a drop-down list that shows the hosts that belong to the cluster and then select the host for the initiator. This field is displayed only if the LUN is shared by hosts in a Windows Server failover cluster.
Choose host initiator	Select Fibre Channel or iSCSI and then select the initiator on the host. You can select multiple FC initiators if you are using FC with multipath I/O (MPIO).

9. On the **Group Type** page, specify whether you want to map an existing igroup to the LUN, or create a new igroup:

Select...	If...
Create new igroup for selected initiators	You want to create a new igroup for the selected initiators.
Choose an existing igroup or specify a new igroup for selected initiators	You want to specify an existing igroup for the selected initiators, or create a new igroup with the name you specify. Type the igroup name in the igroup name field. Type the first few letters of the existing igroup name to autocomplete the field.

10. On the **Summary** page, review your selections and click **Finish**.

SnapCenter creates the LUN and connects it to the specified drive or drive path on the host.

Resizing a disk

You can increase or decrease the size of a disk as your storage system needs change.

About this task

- For thin provisioned LUN, the ONTAP lun geometry size is shown as the maximum size.
- For thick provisioned LUN, the expandable size (available size in the volume) is shown as the maximum size.
- LUNs with MBR-style partitions have a size limit of 2 TB.
LUNs with GPT-style partitions have a storage system size limit of 16 TB.
- It is a good idea to make a Snapshot copy before resizing a LUN.
- If you need to restore a LUN from a Snapshot copy made before the LUN was resized, SnapCenter automatically resizes the LUN to the size of the Snapshot copy.
After the restore operation, data added to the LUN after it was resized must be restored from a Snapshot copy made after it was resized.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Disks**.
3. Select the host from the **Host** drop-down list.
The disks are listed.
4. Select the disk you want to resize and then click **Resize**.
5. In the **Resize Disk** dialog box, use the slider tool to specify the new size of the disk, or enter the new size in the **Size** field.

Note: If you enter the size manually, you need to click outside the **Size** field before the **Shrink** or **Expand** button is enabled appropriately. Also, you must click **MB**, **GB**, or **TB** to specify the unit of measurement.

6. When you are satisfied with your entries, click **Shrink** or **Expand**, as appropriate.

SnapCenter resizes the disk.

Connecting a disk

You can use the Connect Disk wizard to connect an existing LUN to a host, or to reconnect a LUN that has been disconnected.

Before you begin

- You must have started the FC or iSCSI service on the storage system.

- If you are using iSCSI, you must have established an iSCSI session with the storage system.

About this task

- You cannot connect a LUN to more than one host unless the LUN is shared by hosts in a Windows Server failover cluster.
- If the LUN is shared by hosts in a Windows Server failover cluster that uses CSV (Cluster Shared Volumes), you must connect the disk on the host that owns the cluster group.
- The Plug-in for Windows needs to be installed only on the host on which you are connecting the disk.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Disks**.
3. Select the host from the **Host** drop-down list.
4. Click **Connect**.
The Connect Disk wizard opens.
5. On the **LUN Name** page, identify the LUN to connect to:

In this field...	Do this...
Storage System	Select the SVM for the LUN.
LUN path	Click Browse to select the full path of the volume containing the LUN.
LUN name	Enter the name of the LUN.
Cluster size	If the LUN is shared by hosts in a Windows cluster, select the size of the cluster.
LUN label	Optionally, enter descriptive text for the LUN.

6. On the **Disk Type** page, select the disk type:

Select...	If...
Dedicated disk	The LUN can be accessed by only one host.
Shared disk	The LUN is shared by hosts in a Windows Server failover cluster. You need only connect the disk to one host in the failover cluster.
Cluster Shared Volume (CSV)	The LUN is shared by hosts in a Windows Server failover cluster that uses CSV. Make sure that the host on which you are connecting to the disk is the owner of the cluster group.

7. On the **Drive Properties** page, specify the drive properties:

Property	Description
Auto assign	Let SnapCenter automatically assign a volume mount point based on the system drive. For example, if your system drive is C :, the auto assign property creates a volume mount point under your C : drive (C : \scmnp\). The auto assign property is not supported for shared disks.
Assign drive letter	Mount the disk to the drive you select in the adjoining drop-down list.

Property	Description
Use volume mount point	Mount the disk to the drive path you specify in the adjoining field. The root of the volume mount point must be owned by the host on which you are creating the disk.
Do not assign drive letter or volume mount point	Choose this option if you prefer to mount the disk manually in Windows.

8. On the **Map LUN** page, select the iSCSI or FC initiator on the host:

In this field...	Do this...
Host	Double-click the cluster group name to display a drop-down list that shows the hosts that belong to the cluster, then select the host for the initiator. This field is displayed only if the LUN is shared by hosts in a Windows Server failover cluster.
Choose host initiator	Select Fibre Channel or iSCSI , and then select the initiator on the host. You can select multiple FC initiators if you are using FC with MPIO.

9. On the **Group Type** page, specify whether you want to map an existing igroup to the LUN or create a new igroup:

Select...	If...
Create new igroup for selected initiators	You want to create a new igroup for the selected initiators.
Choose an existing igroup or specify a new igroup for selected initiators	You want to specify an existing igroup for the selected initiators, or create a new igroup with the name you specify. Type the igroup name in the igroup name field. Type the first few letters of the existing igroup name to automatically complete the field.

10. On the **Summary** page, review your selections and click **Finish**.

SnapCenter connects the LUN to the specified drive or drive path on the host.

Disconnecting a disk

You can disconnect a LUN from a host without affecting the contents of the LUN, with one exception: If you disconnect a clone before it has been split off, you lose the contents of the clone.

Before you begin

- Make sure that the LUN is not in use by any application.
- Make sure that the LUN is not being monitored with monitoring software.
- If the LUN is shared, make sure to remove the cluster resource dependencies from the LUN and verify that all nodes in the cluster are powered on, functioning properly, and available to SnapCenter.

About this task

If you disconnect a LUN in a FlexClone volume that SnapCenter has created and no other LUNs on the volume are connected, SnapCenter deletes the volume. Before disconnecting the LUN, SnapCenter displays a message warning you that the FlexClone volume might be deleted.

To avoid automatic deletion of the FlexClone volume, you should rename the volume before disconnecting the last LUN. When you rename the volume, make sure that you change multiple characters than just the last character in the name.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Disks**.
3. Select the host from the **Host** drop-down list.
The disks are listed.
4. Select the disk you want to disconnect, and then click **Disconnect**.
5. In the **Disconnect Disk** dialog box, click **OK**.
SnapCenter disconnects the disk.

Deleting a disk

You can delete a disk when you no longer need it. After you delete a disk, you cannot undelete it.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Disks**.
3. Select the host from the **Host** drop-down list.
The disks are listed.
4. Select the disk you want to delete, and then click **Delete**.
5. In the **Delete Disk** dialog box, click **OK**.
SnapCenter deletes the disk.

Creating and managing SMB shares

To configure an SMB3 share on a storage virtual machine (SVM), you can use either the SnapCenter user interface or PowerShell cmdlets.

Best Practice: Using the cmdlets is recommended because it enables you to take advantage of templates provided with SnapCenter to automate share configuration.

The templates encapsulate best practices for volume and share configuration. You can find the templates in the `Templates` folder in the installation folder for the SnapCenter Plug-ins Package for Windows.

Tip: If you feel comfortable doing so, you can create your own templates following the models provided. You should review the parameters in the cmdlet documentation before creating a custom template.

Creating an SMB share

You can use the SnapCenter Shares page to create an SMB3 share on a storage virtual machine (SVM).

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Shares**.

3. Select the SVM from the **Storage Virtual Machine** drop-down list.
4. Click **New**.
The New Share dialog opens.

5. In the **New Share** dialog, define the share:

In this field...	Do this...
Description	Enter descriptive text for the share.
Share name	<p>Enter the share name, for example, <code>test_share</code>. The name you enter for the share will also be used as the volume name.</p> <p>The share name:</p> <ul style="list-style-type: none"> • Must be a UTF-8 string. • Must not include the following characters: control characters from 0x00 to 0x1F (both inclusive), 0x22 (double quotes), and the special characters <code>\ / [] : < > + = ; , ?</code>
Share path	<ul style="list-style-type: none"> • Click in the field to enter a new file system path, for example, <code>/</code>. • Double-click in the field to select from a list of existing file system paths.

6. When you are satisfied with your entries, click **OK**.
SnapCenter creates the SMB share on the SVM.

Deleting an SMB share

You can delete an SMB share when you no longer need it.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Shares**.
3. In the **Shares** page, click in the **Storage Virtual Machine** field to display a drop-down with a list of available storage virtual machines (SVMs), then select the SVM for the share you want to delete.
4. From the list of shares on the SVM, select the share you want to delete and click **Delete**.
5. In the **Delete Share** dialog box, click **OK**.

SnapCenter deletes the SMB share from the SVM.

Reclaiming space on the storage system

Although NTFS tracks the available space on a LUN when files are deleted or modified, it does not report the new information to the storage system. You can run the space reclamation PowerShell cmdlet on the Plug-in for Windows host to ensure that newly freed blocks are marked as available in storage.

Before you begin

If you are running the cmdlet on a remote plug-in host, you must have run the `SnapCenter Open-SMConnection` cmdlet to open a connection to the SnapCenter Server.

About this task

- You must ensure that the space reclamation process has completed before performing a restore operation.
- If the LUN is shared by hosts in a Windows Server failover cluster, you must perform space reclamation on the host that owns the cluster group.
- For optimum storage performance, you should perform space reclamation as often as possible. You should ensure that the entire NTFS file system has been scanned.
- Space reclamation is time-consuming and CPU-intensive, so it is usually best to run the operation when storage system and Windows host usage is low.
- Space reclamation reclaims nearly all available space, but not 100 percent.
- You should not run disk defragmentation at the same time as you are performing space reclamation.
Doing so can slow the reclamation process.

Step

1. From the application server PowerShell command prompt, enter the following command:

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

drive_path is the drive path mapped to the LUN.

Using PowerShell cmdlets to provision storage

If you do not want to use the SnapCenter GUI to perform host provisioning and space reclamation jobs, you can use the PowerShell cmdlets that are provided by SnapCenter Plug-in for Microsoft Windows. You can use cmdlets directly or add them to scripts.

If you are running the cmdlets on a remote plug-in host, you must run the SnapCenter `Open-SMConnection` cmdlet to open a connection to the SnapCenter Server.

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](#)

Provisioning storage in VMware environments

You can use the SnapCenter Plug-in for Microsoft Windows in VMware environments to create and manage LUNs and manage Snapshot backup copies.

Supported VMware guest OS platforms

You can use the Plug-in for Windows for LUN provisioning and Snapshot copy management support on x64 guest operating systems running on supported versions of VMware ESXi.

The Plug-in for Windows supports the following VMware guest OS configurations:

- Supported versions of Windows Server
- Microsoft cluster configurations
Support for up to a maximum of 16 nodes supported on VMware when using the Microsoft iSCSI Software Initiator, or up to two nodes using FC
- RDM LUNs
Support for a maximum of 56 RDM LUNs with four LSI Logic SCSI controllers for normal RDMS, or 42 RDM LUNs with three LSI Logic SCSI controllers on a VMware VM MSCS box-to-box Plug-in for Windows configuration

For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT).

[NetApp Interoperability Matrix Tool](#)

VMware ESXi server-related limitations

The SnapCenter Plug-in for Microsoft Windows is supported on VMware Windows guest. Before you use the Plug-in for Windows to perform provisioning and Snapshot copy management operations, you should be aware of some limitations.

- Installing the Plug-in for Windows on a Microsoft cluster on virtual machines using ESXi credentials is not supported.
You should use your vCenter credentials when installing the Plug-in for Windows on clustered virtual machines.
- All clustered nodes must use the same target ID (on the virtual SCSI adapter) for the same clustered disk.
- When you create an RDM LUN outside of the Plug-in for Windows, you must restart the plug-in service to enable it to recognize the newly created disk.
- You cannot use iSCSI and FC initiators at the same time on a VMware guest OS.

Minimum vCenter privileges required for SnapCenter RDM operations

To perform RDM operations in a guest OS, you must have minimum vCenter privileges.

You must have the following minimum privileges set on the host:

- Datastore: **Remove File**
- Host: **Configuration > Storage Partition Configuration**
- Virtual Machine: **Configuration**

You must assign these privileges to a role at the Virtual Center Server level. The role to which you assign these privileges cannot be assigned to any user without root privileges.

After you assign these privileges, you can install the Plug-in for Windows on the guest OS.

Using FC RDM LUNs in a Microsoft cluster

You can use the Plug-in for Windows to manage a Microsoft cluster using FC RDM LUNs, but you must first create the shared RDM quorum and shared storage outside the plug-in, and then add the disks to the virtual machines in the cluster.

Starting with ESXi 5.5, you can also use ESX iSCSI and FCoE hardware to manage a Microsoft cluster. The Plug-in for Windows includes out-of-box support for Microsoft clusters.

Requirements for using FC RDM LUNs in a Microsoft cluster

The Plug-in for Windows provides support for Microsoft clusters using FC RDM LUNs on two different virtual machines that belong to two different ESX or ESXi servers, also known as *cluster access boxes*, when you meet specific configuration requirements.

The following configuration requirements must be met to use FC RDM LUNs on virtual machines in a Microsoft cluster:

- The VMs must be running the same Windows Server version.
- ESX or ESXi server versions must be the same for each VMware parent host.
- Each parent host must have at least two network adapters.
- There must be at least one VMFS datastore shared between the two ESX or ESXi servers.
- VMware recommends that the shared datastore be created on an FC SAN. If necessary, the shared datastore can also be created over iSCSI.
- The shared RDM LUN must be in physical compatibility mode.
- The shared RDM LUN must be created manually outside of the Plug-in for Windows. You cannot use virtual disks for shared storage.
- A SCSI controller must be configured on each virtual machine in the cluster in physical compatibility mode:
Windows Server 2008 R2 requires you to configure the LSI Logic SAS SCSI controller on each virtual machine.
Shared LUNs cannot use the existing LSI Logic SAS controller if only one of its type exists and it is already attached to the C: drive.
SCSI controllers of type paravirtual are not supported on VMware Microsoft clusters.

Note: When you add a SCSI controller to a shared LUN on a virtual machine in physical compatibility mode, you must select the **Raw Device Mappings** option and not the **Create a new disk** option in the VMware Infrastructure Client.
- Microsoft virtual machine clusters cannot be part of a VMware cluster.
- You must use vCenter credentials and not ESX or ESXi credentials when you install the Plug-in for Windows on virtual machines that will belong to a Microsoft cluster.
- The Plug-in for Windows cannot create a single igroup with initiators from multiple hosts. The igroup containing the initiators from all ESXi hosts must be created on the storage controller prior to creating the RDM LUNs that will be used as shared cluster disks.
- You can create an RDM LUN on ESXi 5.0 using an FC initiator. When you create an RDM LUN, an initiator group is created with ALUA.

Microsoft cluster support limitations when using FC/iSCSI RDM LUNs

The Plug-in for Windows supports Microsoft clusters using FC/iSCSI RDM LUNs on different virtual machines belonging to different ESX or ESXi servers.

Note: This feature is not supported in releases before ESX 5.5i.

- The Plug-in for Windows does not support clusters on ESX iSCSI and NFS datastores.
- The Plug-in for Windows does not support mixed initiators in a cluster environment. Initiators must be either FC or Microsoft iSCSI, but not both.
- ESX iSCSI initiators and HBAs are not supported on shared disks in a Microsoft cluster.
- The Plug-in for Windows does not support virtual machine migration with vMotion if the virtual machine is part of a Microsoft cluster.
- The Plug-in for Windows does not support MPIO on virtual machines in a Microsoft cluster.

Creating a shared FC RDM LUN

Before you can use FC RDM LUNs to share storage between nodes in a Microsoft cluster, you must first create the shared quorum disk and shared storage disk, and then add them to both virtual machines in the cluster.

About this task

The shared disk is not created using the Plug-in for Windows.

Step

1. Create and then add the shared LUN to each virtual machine in the cluster, as documented in the *VMware Setup for Failover Clustering and Microsoft Cluster Service*.

See the section that describes how to cluster virtual machines across physical hosts.

Troubleshooting RDM LUN creation

If you experience errors creating RDM LUNs, you should be aware of some of the common errors and workarounds.

Error message

```
Failed to create disk in virtual machine, Failed to Map virtual disk: File [datastore] path_name was not found.
```

Problem

You might encounter this error when you attempt to create an RDM LUN with ESX or ESXi Software Initiator on a VM with a name with more than 33 characters.

You have several options to work around this issue.

Workaround 1

Manually create the same directory inside the datastore.

Workaround 2

Rather than selecting your datastore with the `Store with Virtual machine` option, select the datastore in which you intend to create the RDM LUN. When you create the RDM LUN, use the same datastore you just selected.

Workaround 3

Configure the Plug-in for Windows VirtualCenter or ESXi Server login settings with the VirtualCenter credentials.

Managing EMS data collection

You can schedule and manage Event Management System (EMS) data collection using PowerShell cmdlets. EMS data collection involves gathering details about the SnapCenter Server, the installed SnapCenter plug-in packages, the hosts, and similar information, and then sending it to a specified ONTAP storage virtual machine (SVM).

Note: System CPU utilization is high when data-collection task is in progress. CPU utilization remains high as long as the operation is progress irrespective of the data size.

Stopping EMS data collection

EMS data collection is enabled by default and runs every seven days after your installation date. You can disable data collection at any time by using the PowerShell cmdlet `Disable-SmDataCollectionEMS`.

Steps

1. From a PowerShell command line, establish a session with SnapCenter by entering `Open-SmConnection`.
2. Disable EMS data collection by entering `Disable-SmDataCollectionEms`.

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](#)

Starting EMS data collection

EMS data collection is enabled by default and is scheduled to run every seven days from the installation date. If you have disabled it, you can start EMS data collection again by using the `Enable-SmDataCollectionEMS` cmdlet.

Before you begin

The Data ONTAP event generate-autosupport-log permission has been granted to the storage virtual machine (SVM) user.

Steps

1. From a PowerShell command line, establish a session with SnapCenter by entering `Open-SmConnection`.
2. Enable EMS data collection by entering `Enable-SmDataCollectionEMS`.

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](#)

Changing EMS data collection schedule and target SVM

You can use PowerShell cmdlets to change the EMS data collection schedule or the target storage virtual machine (SVM).

Steps

1. From a PowerShell command line, to establish a session with SnapCenter, enter the `Open-SmConnection` cmdlet.
2. To change the EMS data collection target, enter the `Set-SmDataCollectionEmsTarget` cmdlet.
3. To change the EMS data collection schedule, enter the `Set-SmDataCollectionEmsSchedule` cmdlet.

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](#)

Monitoring EMS data collection status

You can monitor the status of your EMS data collection using several PowerShell cmdlets. You can get information about the schedule, storage virtual machine (SVM) target, and status.

Steps

1. From a PowerShell command line, establish a session with SnapCenter by entering `Open-SmConnection`.
2. Retrieve information about the EMS data collection schedule by entering `Get-SmDataCollectionEmsSchedule`.
3. Retrieve information about the EMS data collection status by entering `Get-SmDataCollectionEmsStatus`.
4. Retrieve information about the EMS data collection target by entering `Get-SmDataCollectionEmsTarget`.

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](#)

Using REST APIs

You can use REST APIs to perform several SnapCenter operations. 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](#)

Accessing REST APIs using the Swagger API web page

REST APIs are exposed through the Swagger web page. You can access the Swagger web page to display the SnapCenter Server REST APIs, as well as to manually issue an API call. You can use REST APIs to help manage your SnapCenter Server or to perform data protection operations.

Before you begin

You must know the management IP address or domain name of the SnapCenter Server on which you want to execute the REST APIs.

About this task

You do not need special permissions to run the REST API client. Any user can access the Swagger web page. The respective permissions on the objects that are accessed via the REST API are based on the user who generates the token to login to the REST API.

Steps

1. From a browser, enter the URL to access the Swagger web page in the format `https://<SnapCenter_IP_address_or_name>:8146/swagger/`.

Note: Ensure that the REST API URL does not have the following characters: +, ., %, and &.

Example

Access SnapCenter Server REST APIs:

```
https://192.0.2.85:8146/swagger/
```

```
https://netapp_host_domain:8146/swagger/
```

2. If the Swagger API documentation does not display automatically, in the Swagger **Explore** field, type the URL to the location of the Swagger documentation: `https://<SnapCenter_IP_address_or_name>:8146/Content/swagger/SnapCenter.yaml` or `https://<vCenter_host_IP_address>:8146/Content/swagger/SnapCenter.yaml`, and click **Explore**.

A list of API resource types, or categories, is displayed.

3. Click an API resource type to display the APIs in that resource type.

Plug-in support for REST APIs

Support for REST APIs depends on which SnapCenter plug-ins you have installed.

The SnapCenter...	Supports REST APIs
Plug-in for SQL Server	✓
Plug-in for Oracle Database	
Plug-in for Windows	
Plug-in for Exchange	
Plug-in for SAP HANA Database	✓
Custom Plug-ins	✓

Troubleshooting SnapCenter REST APIs

If you encounter unexpected behavior when executing SnapCenter REST APIs, you can use the log files to identify the cause and resolve the problem.

You can download the log files from the SnapCenter user interface by clicking **Monitor > Logs > Download**.

File restore API gives error 400

Error 400 is displayed when restoring a file using the `/2.0/plugins/SP/resources/{key}/restorefile` API.

Corrective actions

- Use escape characters (\\) when providing a source path in Swagger. For example: `\\\\vol1\\path1\\path2`.
- Use escape characters (\\) when providing the domain and user name for API login authentication. For example: `domain\\username`
- Use escape characters (\\) when providing the user credentials for the local account. For example: `localhost\\username`

Copyright

Copyright © 2019 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, 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).

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*](mailto: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

Index

B

- backing up
 - prerequisites for protecting the SnapCenter repository [23](#)
- backup details reports
 - described [16](#)
- backup reports
 - described [16](#)
- backups
 - overview of repository management [23](#)
 - SnapCenter repository [24](#)
- best practices
 - for volume and share configurations [51](#)
 - using the FQDN [33](#), [35](#)

C

- capabilities, SnapCenter reporting
 - introduction to using [16](#)
- clone reports
 - described [16](#)
- Cluster Shared Volumes
 - connecting to disks [48](#)
 - creating disks [46](#)
- clusters, Microsoft
 - introduction to using FC RDM LUNs in [55](#)
 - support limitations when using FC/iSCSI RDM LUNs [56](#)
- cmdlets
 - Disable-SmDataCollectionEms [58](#)
 - Enable-SmDataCollectionEMS [58](#)
 - Get-SmDataCollectionEmsSchedule [59](#)
 - Get-SmDataCollectionEmsStatus [59](#)
 - Get-SmDataCollectionEmsTarget [59](#)
 - Set-SmDataCollectionEmsSchedule [59](#)
 - Set-SmDataCollectionEmsTarget [59](#)
 - SnapCenter Plug-in for Microsoft Windows support [53](#)
- comments
 - how to send feedback about documentation [64](#)
- connections, storage systems
 - deleting [40](#)
 - modifying [39](#)
- connections, SVM
 - modifying [39](#)
- credentials
 - supported for installing plug-ins for Windows [54](#), [55](#)
- CSV
 - See* Cluster Shared Volume

D

- Dashboard
 - purpose [10](#)
 - viewing [10](#)
 - viewing job status [14](#)
- dashboards

- information in reports [10](#)
- data protection job updates
 - configuring the option to email reports [18](#)
- disks
 - connecting to LUNs in SnapCenter [48](#)
 - creating in SnapCenter [46](#)
 - deleting LUNs in SnapCenter [51](#)
 - disconnecting from LUNs in SnapCenter [50](#)
 - resizing in SnapCenter [48](#)
 - tasks you can perform using SnapCenter [45](#)
 - viewing on a host [45](#)
- documentation
 - how to receive automatic notification of changes to [64](#)
 - how to send feedback about [64](#)
- domains
 - managing untrusted resources [30](#)
- downloading
 - logs [21](#)

E

- email
 - configuring SnapCenter to send reports [18](#)
 - testing configuration [18](#)
- EMS data collection
 - changing schedule [59](#)
 - changing target SVM [59](#)
 - disabling [58](#)
 - getting status information [59](#)
 - starting [58](#)
- ESXi servers
 - limitations of SnapCenter Plug-in for Microsoft Windows support [54](#)
- events
 - monitoring [20](#)

F

- FC RDM LUNs
 - creating shared [56](#)
 - introduction to using in Microsoft clusters [55](#)
 - requirements for using in Microsoft clusters [55](#)
- FC-connected LUNs
 - creating [46](#)
- FC/iSCSI RDM LUNs
 - Microsoft cluster support limitations when using [56](#)
- feedback
 - how to send comments about documentation [64](#)

G

- global settings
 - configuring SMTP server [18](#)

H

- host agent logs

- downloading [21](#)
- monitoring [21](#)

hosts

- creating an igroup in SnapCenter Plug-in for Microsoft Windows [44](#)
- creating SMB shares [51](#)
- deleting an igroup [45](#)
- disconnecting LUNs from [50](#)
- modifying an igroup [44](#)
- placing in maintenance mode [28](#)
- provisioning Windows with SnapCenter Plug-in for Microsoft Windows [42](#)
- renaming an igroup [44](#)
- updating virtual machine information [27](#)
- viewing a list of disks on [45](#)

I

igroups

- creating in SnapCenter Plug-in for Microsoft Windows [44](#)
- deleting in SnapCenter Plug-in for Microsoft Windows [45](#)
- managing [44](#)
- modifying [44](#)
- purpose [44](#)
- renaming [44](#)

information

- how to send feedback about improving documentation [64](#)

initiators

- adding to an igroup [44](#)
- creating an igroup [44](#)

iSCSI

- disconnecting a session [43](#)
- establishing a session [42](#)

iSCSI-connected LUNs

- creating [46](#)

J

job status reports

- described [16](#)

jobs

- monitoring [20](#)
- removing [22](#)
- status report from the Dashboard [14](#)

K

key files

- for securing communication between SnapCenter Server and MySQL Server [33](#)

L

license installation

- viewing status for storage controllers [40](#)

limitations

- support when using FC/iSCSI RDM LUNs in Microsoft clusters [56](#)
- VMware ESXi server-related [54](#)

log files

- using to troubleshoot REST APIs [61](#)

logs

- downloading [21](#)
- monitoring [21](#)
- removing [22](#)

LUNs

- connecting to in SnapCenter [48](#)
- creating in SnapCenter [46](#)
- creating shared FC RDM [56](#)
- deleting in SnapCenter [51](#)
- disconnecting before deleting [50](#)
- disconnecting in SnapCenter [50](#)
- disk-related tasks you can perform using SnapCenter [45](#)
- FC RDM, requirements for using in a Microsoft cluster [55](#)
- introduction to configuring [42](#)
- introduction to creating and managing using SnapCenter Plug-in for Microsoft Windows in VMware environments [54](#)
- prerequisites for iSCSI connections [42](#)
- RDM, support through PowerShell cmdlets [54](#)
- RDM, troubleshooting creation of [56](#)
- resizing in SnapCenter [48](#)

LUNs, FC RDM

- introduction to using in Microsoft clusters [55](#)

LUNs, FC/iSCSI RDM

- FC/iSCSI RDM Microsoft cluster support limitations when using [56](#)

M

maintenance mode

- placing hosts in [28](#)

Microsoft clusters

- introduction to using FC RDM LUNs in [55](#)
- support limitations when using FC/iSCSI RDM LUNs [56](#)

modifying

- roles [8](#)

monitoring

- EMS data collection status [59](#)
- events [20](#)
- jobs [20](#)
- logs [21](#)
- schedules [20](#)

MySQL database

- resetting repository password [25](#)

N

NSM

- migrating to another disk [25](#)

P

plug-in logs

- downloading [21](#)
- monitoring [21](#)

plug-in reports

- described [16](#)

- plug-ins
 - restarting after a temporary stop [28](#)
 - starting [28](#)
- PowerShell cmdlets
 - reclaiming storage space with [52](#)
 - SnapCenter Plug-in for Microsoft Windows support [53](#)

R

- RDM
 - minimum vCenter privileges required for operations [54](#)
- RDM LUNs
 - creating shared FC [56](#)
 - introduction to using FC in Microsoft clusters [55](#)
 - Microsoft cluster support limitations when using for FC/iSCSI [56](#)
 - requirements for FC support [55](#)
 - troubleshooting creation of [56](#)
- reporting capabilities, SnapCenter
 - introduction to using [16](#)
- reports
 - accessing [16](#)
 - backup and backup details, described [16](#)
 - configuring [17](#)
 - configuring the option to email [18](#)
 - exporting [17](#)
 - job status [14](#)
 - job status, described [16](#)
 - parameters used to filter information [17](#)
 - plug-in, described [16](#)
 - printing [17](#)
 - types of [10](#), [16](#)
 - viewing from the Dashboard [10](#)
- repository
 - accessing repository backups [24](#)
- repository database
 - resetting password [25](#)
- repository management
 - overview [23](#)
- resizing
 - disks [48](#)
 - LUNs [48](#)
- resource groups
 - configuring the option to email reports [18](#)
- REST APIs
 - accessing from Swagger [60](#)
 - support by plug-in [61](#)
 - troubleshooting [61](#)
- restore reports
 - described [16](#)
- restoring
 - SnapCenter database backups [24](#)
- role-based access control
 - adding SnapCenter users or groups to a role [6](#)
- role-based access control (RBAC)
 - creating roles [8](#)
- roles
 - adding SnapCenter users or groups to [6](#)
 - creating [8](#)
 - modifying [8](#)

S

- schedules
 - monitoring [20](#)
- secured MySQL connections
 - configuring for NLB configurations [35](#)
 - configuring for standalone SnapCenter Server [33](#)
- server logs
 - downloading [21](#)
 - monitoring [21](#)
- servers
 - VMware ESXi limitations of SnapCenter Plug-in for Microsoft Windows support [54](#)
- shared FC RDM LUNs
 - creating [56](#)
 - using in a Microsoft cluster [56](#)
- shares, SMB
 - creating in SnapCenter Plug-in for Microsoft Windows [51](#)
- SMB shares
 - creating in SnapCenter Plug-in for Microsoft Windows [51](#)
 - deleting in SnapCenter [52](#)
- SMTP server
 - configuring globally [18](#)
- SnapCenter
 - Reports page terminology [10](#)
 - repository protection [23](#)
 - templates for creating SMB shares [51](#)
- SnapCenter Plug-in for Microsoft Windows
 - creating an igroup [44](#)
 - creating SMB shares [51](#)
 - deleting an igroup [45](#)
 - limitations when using VMware ESXi server [54](#)
 - modifying an igroup [44](#)
 - PowerShell cmdlet support [53](#)
 - renaming an igroup [44](#)
- SnapCenter repository
 - backing up [23](#)
 - migrating to another disk [25](#)
- SnapCenter users
 - adding to a role [6](#)
- Snapshot copies
 - introduction to managing using SnapCenter Plug-in for Microsoft Windows in VMware environments [54](#)
- space reclamation
 - on storage systems [52](#)
- SSL certificates
 - for securing communication between SnapCenter Server and MySQL Server [33](#)
- starting
 - plug-in services [28](#)
- storage
 - introduction to configuring LUNs [42](#)
- storage controller license
 - viewing installation status of [40](#)
- storage system
 - managing configuration [39](#)
- storage systems
 - deleting connections to [40](#)
 - modifying connections to [39](#)
 - modifying connections to SVMs [39](#)
 - reclaiming space on [52](#)

- suggestions
 - how to send feedback about documentation [64](#)
- support limitations
 - when using FC/iSCSI RDM LUNs in Microsoft clusters [56](#)

- SVMs
 - deleting connections to [40](#)
 - modifying connections to [39](#)
- Swagger API web page
 - accessing REST APIs [60](#)

T

- templates
 - for creating SMB shares [51](#)
- terminology
 - used on the Reports page display [10](#)
- troubleshooting
 - RDM LUN creation [56](#)
 - REST APIs using log files [61](#)
- Twitter
 - how to receive automatic notification of documentation changes [64](#)

U

- untrusted Active Directory domains
 - registering [30](#)
 - unregistering [32](#)
- untrusted domain resources
 - managing [30](#)
- untrusted domains
 - modifying [31](#)
- upgrades

- placing hosts in maintenance mode prior to [28](#)
- users or groups
 - modifying [9](#)

V

- vCenter
 - minimum privileges required for RDM operations [54](#)
- virtual disks (VMDKs)
 - tasks you can perform using SnapCenter [45](#)
- virtual machines
 - updating information about [27](#)
- VMware
 - ESXi servers limitations of SnapCenter Plug-in for Microsoft Windows support [54](#)
 - SnapCenter Plug-in for Windows support for [54](#)
 - support for ESX iSCSI initiators [54](#)
 - support for FC HBAs [54](#)
 - support for guest OS platforms [54](#)
 - support for iSCSI HBAs [54](#)
 - support for iSCSI initiators [54](#)
 - using Virtual Storage Console to provision Windows hosts [42](#)

W

- Windows hosts
 - creating an igroup in SnapCenter Plug-in for Microsoft Windows [44](#)
- Windows Server failover clusters
 - requirements for connecting to a disk [48](#)
 - requirements for creating a disk [46](#)