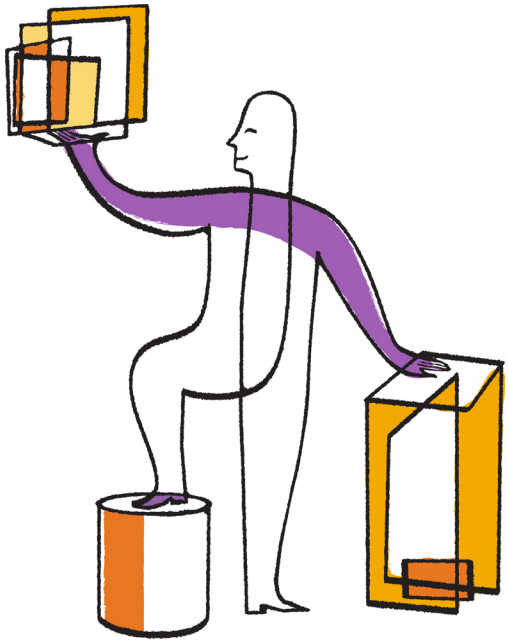
SnapCenter® Software 1.0

Administration Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-09786_B0
October 2015

Contents

SnapCenter overview

SnapCenter is a unified, scalable platform for application-consistent data protection. SnapCenter provides centralized control and oversight, while delegating the ability for users to manage application-specific backup, restore, and clone jobs. SnapCenter also provides you with a single user interface, seamless scalability, high availability, and load balancing.

SnapCenter features

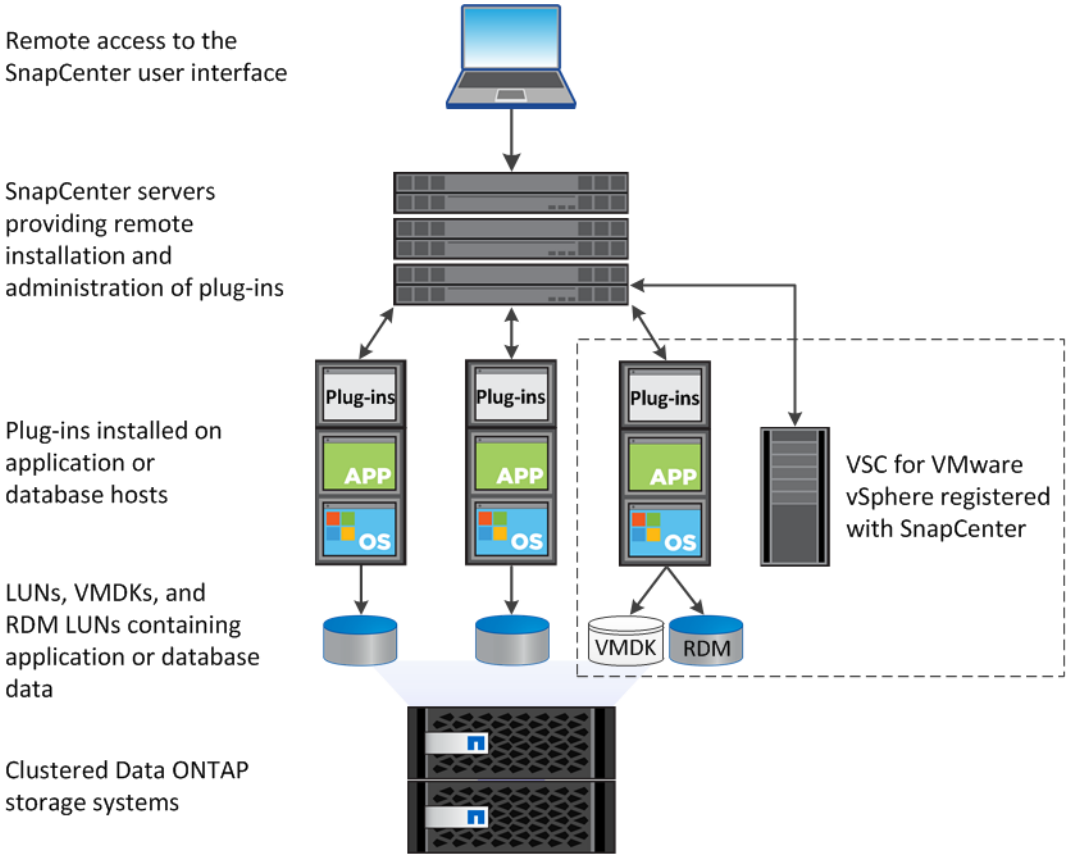
SnapCenter enables you to create application-consistent Snapshot copies and to perform data protection jobs, including Snapshot copy-based backup, clone, restore, and verification jobs. SnapCenter creates a centralized management environment, while using role-based access control (RBAC) to delegate data protection and management capabilities to individual application users across your SnapCenter Server and Windows hosts.

SnapCenter includes the following key features:

- A unified and scalable platform across applications and database environments, powered by SnapCenter Server
- Consistency of features and procedures across plug-ins and environments, supported by the SnapCenter user interface
- Role-based access control (RBAC) security and centralized role delegation
- Application-consistent Snapshot copy management, restore, clone, and verification support from both primary and secondary destinations (SnapMirror and SnapVault)
- Remote plug-in installation from the SnapCenter user interface
- Nondisruptive, remote upgrades
- A dedicated SnapCenter database used by all plug-ins
  SnapCenter stores queried data in its centralized database, which provides faster data retrieval.
- High availability implemented using Network Load Balancing (NLB) and Application Request Routing (ARR), with support for horizontal scaling
- Centralized scheduling and policy management to support backup and clone operations
- Centralized reporting, monitoring, and Dashboard views

SnapCenter components

SnapCenter consists of the SnapCenter Server, the SnapCenter Plug-in for Microsoft SQL Server, and the SnapCenter Plug-in for Microsoft Windows. SnapCenter interacts with Virtual Storage Console for VMware vSphere to provide support for database backup and recovery on RDMs and VMDKs. When you are installing and configuring SnapCenter, it is helpful to understand its components.



SnapCenter Server

SnapCenter Server includes a web server, a centralized HTML5-based user interface, and the SnapCenter database. SnapCenter enables load balancing, high availability, and horizontal scaling across multiple SnapCenter Servers within a single user interface.

You might need multiple SnapCenter Servers for high availability. For larger environments with thousands of SQL hosts or another type of plug-in host, adding multiple SnapCenter Servers can help balance the load.

The SnapCenter platform is based on a multi-tiered architecture, including a centralized management server (SnapCenter Server), which manages different SnapCenter Agents known as *SMCore*. These agents communicate with SnapCenter application plug-ins installed on physical or virtual hosts.

SnapCenter also enables centralized application resource management and easy data protection job execution through the use of datasets and policy management (including scheduling and retention settings). SnapCenter provides unified reporting through the use of a Dashboard, multiple reporting options, job monitoring tools, and log and event viewers.

SnapCenter data protection capabilities can be delegated to application administrators using granular role-based access control (RBAC).

SnapCenter Plug-in for Microsoft SQL Server

The Plug-in for SQL Server is a host-side component of the NetApp integrated storage solution offering application-aware backup management of Microsoft SQL Server databases. With the Plug-in for SQL Server installed in your environment, SnapCenter automates Microsoft SQL Server database backup, restore, and cloning operations.

SnapCenter Plug-in for Microsoft Windows

The Plug-in for Windows provides storage provisioning for the host, Snapshot copy consistency, and space reclamation. With the plug-in installed in your environment, you can use SnapCenter to create and resize disks, initiate iSCSI sessions, manage igroups, and manage SMB shares. The Plug-in for Windows is a required component of the Plug-in for SQL Server workflows.

Support is provided for provisioning SMB shares only. You cannot use SnapCenter to back up databases on SMB shares.

VSC for VMware vSphere

Virtual Storage Console for VMware vSphere enables SnapCenter to communicate with VMware vSphere when SnapCenter performs backup and restore operations for SQL databases on VMDKs or RDMs. In addition, VSC uses SnapCenter to perform backup and restore operations for storage systems running clustered Data ONTAP 8.2.2 or later.

You must register VSC with SnapCenter, using either the SnapCenter Add Hosts wizard or the VSC Configure SnapCenter Server dialog box.

Note: You do not need to register VSC with SnapCenter if your SQL environment uses an iSCSI initiator.

VSC is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.

SnapCenter security features

SnapCenter employs strict security and authentication features.

SnapCenter includes the following security features:

- All communication to SnapCenter uses HTTP over SSL (HTTPS).
- All credentials in SnapCenter are protected using Advanced Encryption Standard (AES) encryption.
- SnapCenter uses security algorithms that are compliant with the Federal Information Processing Standard (FIPS).
- SnapCenter is installed inside your company's firewall to enable access to the SnapCenter Server and to enable communication between the Server and the plug-ins.
- SnapCenter API and operation access uses tokens, which expire after 24 hours.
  Tokens are also encrypted with AES encryption.
- SnapCenter integrates with Windows Active Directory for login and role-based access control (RBAC) that govern access permissions.
- SnapCenter PowerShell cmdlets are session secured.
- After a period of inactivity, SnapCenter prevents access to features and you must log in again.

Resources, datasets, and policies

Before you begin using SnapCenter, it is helpful to understand some basic concepts related to the backup, clone, and restore operations you want to perform. You interact with resources, datasets, and policies in every backup and clone operation that you perform.

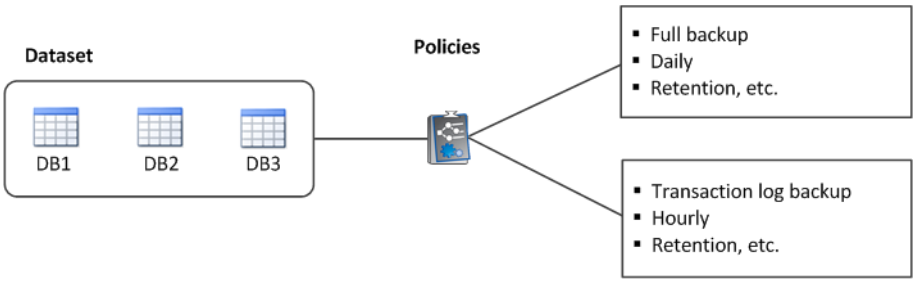
Resources are typically databases but can include anything you back up or clone with a SnapCenter plug-in, including instances and Availability Groups.

A SnapCenter *dataset* is a collection of related resources on a host or Windows cluster. When you back up or clone a dataset in SnapCenter, you back up or clone the *resources* defined in the dataset.

The *policies* attached to a dataset specify the schedule, copy retention, and other characteristics of backup, clone, or verification jobs associated with the dataset. You select the policy when you perform the operation.

Think of a dataset as defining *what* you want to protect and a policy as defining *how* you want to protect it. If you are backing up an SQL Server instance, for example, you might create a dataset that includes all of the databases in the instance. You could then attach two policies to the dataset, one that performs a full backup daily and another that performs transaction log backups hourly.

The following image illustrates the relationship between resources, datasets, and policies:



Supported storage types

SnapCenter supports a wide range of storage types on both physical and virtual machines. You must verify support for your storage type before installing the plug-in for your host.

Machine	Storage type	Where provisioned	Support notes
Physical server	FC-connected LUNs	User interface or PowerShell cmdlets	
	iSCSI-connected LUNs	User interface or PowerShell cmdlets	
	SMB3 shares residing on a Storage Virtual Machine (SVM)	User interface or PowerShell cmdlets	Support for provisioning only. You cannot use SnapCenter to back up databases on SMB shares.
VMware VM	RDM LUNs connected by an FC or iSCSI HBA	PowerShell cmdlets	You must register Virtual Storage Console (VSC) for VMware vSphere with SnapCenter before you can use SnapCenter to back up databases on RDM LUNs.
	iSCSI LUNs connected directly to the guest system by the iSCSI initiator	User interface or PowerShell cmdlets	
	VMDKs on VMFS or NFS datastores	VMware vSphere, or use the VSC cloning utility	You must register Virtual Storage Console (VSC) for VMware vSphere with SnapCenter before you can use SnapCenter to back up databases on VMDKs.
	A guest system connected to SMB3 shares residing on an SVM	User interface or PowerShell cmdlets	Support for provisioning only. You cannot use SnapCenter to back up databases on SMB shares.
Hyper-V VM	Virtual FC (vFC) LUNs connected by a virtual Fibre Switch	User interface or PowerShell cmdlets	
	iSCSI LUNs connected directly to the guest system by the iSCSI initiator	User interface or PowerShell cmdlets	
	A guest system connected to SMB3 shares residing on an SVM	User interface or PowerShell cmdlets	Support for provisioning only. You cannot use SnapCenter to back up databases on SMB shares.

Note: For more information about support for VMware VMs, see *Using the SnapCenter Plug-In for Microsoft Windows in VMware environments* on page 38.

Related references

SnapCenter Plug-in for Microsoft Windows cmdlets on page 41

Logging in to SnapCenter

When you log in to the SnapCenter user interface, you log in as a specific user role, depending on the tasks you want to perform.

About this task

The SnapCenter user interface URL is configured based on information you provide during installation. It is useful to know where to find it after you complete the SnapCenter installation.

During the installation, the SnapCenter Server Install wizard creates a shortcut and places it on your local host desktop. Additionally, at the end of the installation, the Install wizard provides the SnapCenter URL. You can copy this URL in case the shortcut does not work or if you want to log in from a remote system.

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

For Network Load Balance (NLB) deployment, you must access SnapCenter using the NLB cluster IP (https://<*NLB_Cluster_IP*>:8146).

In addition to using the SnapCenter user interface, you can use PowerShell cmdlets to script configuration, backup, restore, and clone operations. For details, use the SnapCenter cmdlet help or see the SnapCenter cmdlet reference information.

Steps

1. Launch SnapCenter either from the shortcut located on your local host desktop, from the URL provided at the end of the installation, or from the URL provided to you by your SnapCenter administrator.
2. Complete the following steps:

If you want to ...	Do the following …
Log in as the SnapCenter administrator	Enter the domain user with local administrator credentials provided during the SnapCenter installation. The first time you log in to SnapCenter, you must log in as an administrator.
Log in as a SnapCenter user	Enter your user credentials: ***Domain\UserName***

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

   You are logged in to SnapCenter.

Related information

SnapCenter Software 1.0 Cmdlet Reference Guide

Managing your SVM connections

Before you can perform backup, restore, clone and provisioning operations with SnapCenter, you must set up your Storage Virtual Machines (SVMs) so that you can connect to clustered Data ONTAP storage systems.

What SVMs are

Storage Virtual Machines (SVMs, formerly known as Vservers) contain data volumes and one or more data LIFs through which they serve data to the clients. SVMs can also have multiple management LIFs. Before you can perform backup, restore, and clone operations, you must set up your SVMs.

SVMs securely isolate the shared virtualized data storage and network, and each SVM appears as a single dedicated server to the clients. Each SVM has a separate administrator authentication domain and can be managed independently by its SVM administrator.

In a cluster, SVMs facilitate data access. A cluster must have at least one SVM to serve data. SVMs use the storage and network resources of the cluster. However, the volumes and LIFs are exclusive to the SVM. Multiple SVMs can coexist in a single cluster without being bound to any node in a cluster. However, they are bound to the physical cluster on which they exist.

Setting up SVM connections

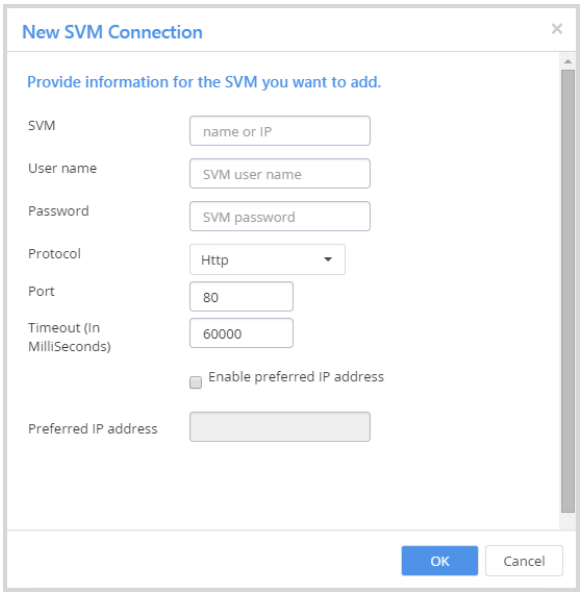
Before you can perform backup, restore, clone, and provisioning operations with SnapCenter, you must set up the Storage Virtual Machine (SVM) connections that give SnapCenter network access to clustered Data ONTAP storage systems.

About this task

If you are planning to replicate Snapshot copies to a mirror or vault, make sure to set up SVM connections for the destination volume as well as the source volume.

Steps

1. In the SnapCenter left navigation pane, click **Settings**.
2. From the **Storage Virtual Machine** page, click **New**.



If you have questions about these values, consult your storage administrator.

3. Provide the following SVM information:

For this field…	Do this…
SVM	Enter the SVM name or IP address.
Username/password	Enter the SVM credentials used to access the storage system.
Protocol	Select the protocol used for connection to the SVM that was configured during SVM setup, typically HTTPS.
Preferred IP	Enter the IP address of the SVM management or data LIF.
Port	Enter the port that the storage system accepts. The defaults typically work.
Timeout	Enter the time in milliseconds that should elapse before communication attempts are halted. The default value is 60,000 milliseconds.

4. Optional: If the SVM has multiple interfaces, select the **Enable preferred IP address** check box, and then enter the preferred IP address for SVM connections.
5. Click **OK**.

Modifying your SVM connection

You can use SnapCenter to modify your Storage Virtual Machine (SVM) connections.

Steps

1. In the SnapCenter left navigation pane, click the **Settings** tab.
2. In the **SVM Connections** field, select an SVM and click **Modify**.
3. In the **Modify SVM Connections** window, provide the information you want to change and click **OK**.

Note: You cannot change the name of the SVM.

Deleting your SVM connection

You can use SnapCenter to delete any unused Storage Virtual Machine (SVM) connections.

Steps

1. In the SnapCenter left navigation pane, click the **Settings** tab.
2. In the **SVM Connections** field, select an SVM and click **Delete**.

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.

Types of role-based access control in SnapCenter

SnapCenter role-based access control (RBAC) enables the SnapCenter administrator to create roles and set access permissions. This centrally managed access empowers application administrators to work securely within delegated environments. Configuring SnapCenter RBAC is a simple process, but it is important to understand the RBAC components and configure them correctly to ensure that all users are able to access SnapCenter and the plug-ins.

SnapCenter uses the following types of role-based access control:

- SnapCenter RBAC
- Application-level RBAC
- Clustered Data ONTAP permissions

SnapCenter RBAC

Roles and permissions

SnapCenter ships with several predefined roles with permissions already assigned. You can add users or groups of users to these existing roles. You can also create new roles and manage permissions and users. You can grant permissions to both roles and resources. You cannot change permissions of the SnapCenterAdmin role.

Authentication

Users are required to provide authentication during login, through the user interface or using PowerShell cmdlets. If users are members of more than one role, after entering login credentials, they are prompted to specify the role they want to use.

Application-level RBAC

SnapCenter uses Run As account credentials to ensure that authorized SnapCenter users also have application-level permissions. For example, if you want to perform Snapshot copy and data protection jobs in a SQL Server environment, you must set your Run As account with the proper Windows or SQL credentials. The SnapCenter Server authenticates the credentials set using either method.

Clustered Data ONTAP permissions

You should ensure that you have vsadmin account 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 users or groups to these roles, to centrally manage SnapCenter access.

Role-based access control permissions and roles

SnapCenter role-based access control (RBAC) enables you to create roles and add permissions to those roles, and then assign users or groups of users to the roles. This enables SnapCenter administrators to create a centrally managed environment, while application administrators can manage data protection jobs. SnapCenter ships with some predefined roles and several permissions.

SnapCenter roles

SnapCenter ships with the following predefined roles. You can either assign users and groups to these roles or create new ones.

- App Backup and Clone Admin
- Backup and Clone Viewer
- Infrastructure Admin
- SnapCenterAdmin

SnapCenter permissions

SnapCenter provides the following permissions:

- Dataset
- Policy
- Backup
- Host
- StorageConnection
- Clone
- Provision
- Dashboard
- Reports
- Restore
- Discovery
- Plug-in Installation

  Note: When you enable Plug-in Installation permissions, you must also enable read and update permissions on Host.

- Migration

Predefined roles and permissions

SnapCenter ships with predefined roles, each with a set of permissions already enabled. When setting up and administering role-based access control (RBAC), you can either use these predefined roles or create new ones. Before adding users to these predefined roles, it is helpful to understand which permissions are and are not enabled.

SnapCenter includes the following predefined roles:

- SnapCenterAdmin role
- Backup and Clone Viewer role
- App Backup and Clone Admin role
- Infrastructure Admin role

When you add a user to roles, you must also assign the StorageConnection permission to enable setting up Storage Virtual Machine (SVM) communication. Without an SVM connection, users cannot complete any backup, clone, or restore operations.

SnapCenterAdmin role

The SnapCenterAdmin role has all permissions enabled. You cannot modify the permissions used for this role. You can add users to the role or remove users from the role.

Backup and Clone Viewer role

The Backup and Clone Viewer role has read-only view of all permissions. This role also has permissions enabled for discovery, reporting, and access to the Dashboard.

Permissions	Enabled	Create	Read	Update	Delete
Dashboard	Yes	Not applicable	Not applicable	Not applicable	Not applicable
Host	Not applicable	No	Yes	No	No
Provision	Not applicable	No	Yes	No	No
Discovery	Yes	Not applicable	Not applicable	Not applicable	Not applicable
Backup	Not applicable	No	Yes	No	No
Restore	No	Not applicable	Not applicable	Not applicable	Not applicable
Clone	Not applicable	No	Yes	No	No
Dataset	Not applicable	No	Yes	No	No
Policy	Not applicable	No	Yes	No	No
Reports	Yes	Not applicable	Not applicable	Not applicable	Not applicable
StorageConnection	Not applicable	No	Yes	No	No
Plug-in Installation	No	Not applicable	Not applicable	Not applicable	Not applicable
Migration	No	Not applicable	Not applicable	Not applicable	Not applicable

App Backup and Clone Admin role

The App Backup and Clone Admin role has the permissions required to perform administrative actions for application backups and clone-related tasks. This role does not have permission for host management, provisioning, storage connection management, or remote installation.

Permissions	Enabled	Create	Read	Update	Delete
Dashboard	Yes	Not applicable	Not applicable	Not applicable	Not applicable
Host	Not applicable	Yes	Yes	Yes	Yes

Permissions	Enabled	Create	Read	Update	Delete
Provision	Not applicable	No	Yes	No	No
Discovery	Yes	Not applicable	Not applicable	Not applicable	Not applicable
Backup	Not applicable	Yes	Yes	Yes	Yes
Restore	Yes	Not applicable	Not applicable	Not applicable	Not applicable
Clone	Not applicable	Yes	Yes	Yes	Yes
Dataset	Not applicable	Yes	Yes	Yes	Yes
Policy	Not applicable	Yes	Yes	Yes	Yes
Reports	Yes	Not applicable	Not applicable	Not applicable	Not applicable
StorageConnection	Not applicable	No	Yes	No	No
Plug-in Installation	No	Not applicable	Not applicable	Not applicable	Not applicable
Migration	No	Not applicable	Not applicable	Not applicable	Not applicable

Infrastructure Admin role

The Infrastructure Admin role has permissions enabled for host management, storage management, provisioning, discovery, remote installation reports, and access to the Dashboard.

Permissions	Enabled	Create	Read	Update	Delete
Dashboard	Yes	Not applicable	Not applicable	Not applicable	Not applicable
Host	Not applicable	Yes	Yes	Yes	Yes
Provision	Not applicable	Yes	Yes	Yes	Yes
Discovery	Yes	Not applicable	Not applicable	Not applicable	Not applicable
Backup	Not applicable	No	Yes	No	No
Restore	No	Not applicable	Not applicable	Not applicable	Not applicable
Clone	Not applicable	No	Yes	No	No
Dataset	Not applicable	No	Yes	No	No

Permissions	Enabled	Create	Read	Update	Delete
Policy	Not applicable	No	Yes	No	No
Reports	Yes	Not applicable	Not applicable	Not applicable	Not applicable
StorageConnection	Not applicable	Yes	Yes	Yes	Yes
Plug-in Installation	Yes	Not applicable	Not applicable	Not applicable	Not applicable
Migration	No	Not applicable	Not applicable	Not applicable	Not applicable

Adding a user to a role

To configure role-based access control for SnapCenter users, you must add each user or group to a role. The role determines the options that SnapCenter users can access.

Before you begin

You must have logged in as the SnapCenter administrator.

About this task

SnapCenter ships with predefined roles. You can either add users to these roles or create new roles.

Steps

1. From the SnapCenter left navigation pane, click **Administration**.
2. From the **Roles** page, select the role to which you want to add the user.
3. Click **Modify**.
4. Click **Next** until you reach the **Users/Groups** page of the wizard.
5. From the **Users/Groups** page, specify the domain to which the user belongs and click **Find**.
6. In the User or Group field, enter a user or group name and click **Add User** or **Add Group**.
7. Click **Next** to view the summary, and then click **Finish**.

Creating a new role

In addition to using the existing SnapCenter roles, you can create your own, customize the permissions, and assign users or groups to the role.

Steps

1. From the SnapCenter left navigation pane, click **Administration**.
2. Ensure that the **Roles** page is selected.
3. Click **New** to launch the **New Role** wizard.
4. Provide the necessary information and click **OK**.

After you finish

You can now add users or groups to the role.

Assigning resources to users

Setting up role-based access control (RBAC) for users is a two-step process. After you add a user to a role that contains the appropriate permissions, you must assign resources to that user. This enables users to perform the actions for which they have permissions on the resources that are assigned to them.

Before you begin

You must have added a user to a role.

About this task

If you are planning to replicate Snapshot copies to a mirror or vault, you must assign the SVM for both the source and destination volume to the user performing the operation.

Steps

1. From the SnapCenter left navigation pane, click **Administration**.
2. Click **Resources**.
3. From the **Resources type** field, select the type of resource you want to assign.
4. In the **Resource name** table, highlight the resource you want to assign and click **Assign User**.
5. Provide the domain name and click **Find**.
6. Enter the user name and select it from the list.
7. Repeat this procedure until each user has all the required resources.

Modifying a role

You can modify a SnapCenter role to add or remove users or groups, change the permissions associated with the role, or rename it. 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. From the SnapCenter left navigation pane, click **Administration**.
2. From the Role name field, click the role you want to modify.
3. Click **Modify**.
4. Using the **Modify Role** wizard to alter the permissions, users, and groups, as needed.

Application-level role-based access control

Application-level role-based access control (RBAC) enables SnapCenter users to provide Run As account credentials for access to applications such as SQL Server.

Setting up your Run As account

The Run As account enables you to set up credentials that can be used to authenticate users for any SnapCenter operations. For example, to execute jobs on a SQL Server instance, you must set up a Run As account with the correct SQL Server credentials.

About this task

If you are using Windows credentials for authentication, you should set up your Run As account before installing plug-ins. However, if you are using a SQL instance to authenticate, you must add the Run As account after installing plug-ins.

Windows authentication and SQL authentication differ according to the following:

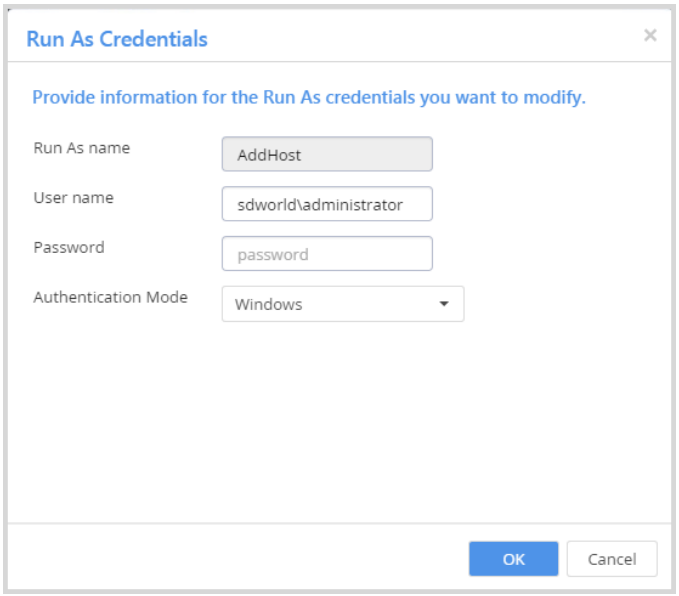
- The Windows authentication mode authenticates against Active Directory.
  For Windows authentication, Active Directory is set up outside of SnapCenter. SnapCenter authenticates with no additional configuration. You need a Windows Run As account to perform tasks such as adding hosts or installing plug-ins.
- The SQL authentication mode authenticates against a SQL instance.
  This means that a SQL instance must be discovered in SnapCenter. As a result, prior to adding a SQL Run As account, you must add a host, install plug-ins, and refresh resources. You need SQL authentication for configuring SQL work flows such as SQL scheduling or discovering resources.

Because some actions require administrator privileges, you should set up the Run As account with administrator privileges, including administrator rights on the remote host.

The Run As account should be a Windows user for scheduling jobs and who has access to the host where the plug-in is installed.

Steps

1. In the left navigation pane, click **Settings.**
2. Click **Run As Credentials**.
3. Click **New**:



4. In the **Run As Credentials** page, provide the following information:

For this field…	Do this…
Run As name	Enter a name for the Run As account.
User name/password	Choose the user account used for authentication.
Authentication Mode	Choose either the SQL or Windows authentication mode.
Host (SQL only)	Choose the host where the SQL instance is located.
SQL Server instance (SQL only)	Choose the SQL instance.

5. Click **OK**.

Configuring credentials for individual resources

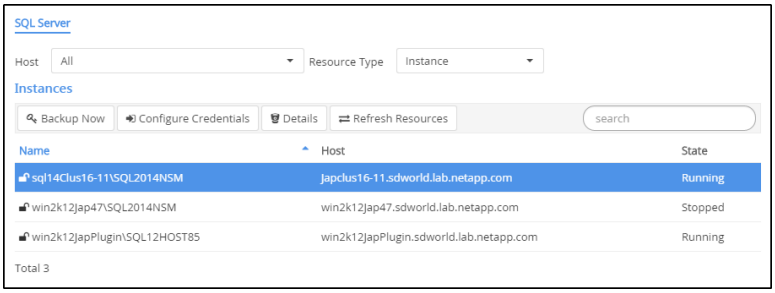
You can configure Run As account credentials to perform data protection jobs on individual resources for each user.

About this task

If you are using Windows credentials for authentication, you should set up your Run As account before installing plug-ins. However, if you are using a SQL instance to authenticate, you must add the Run As account after installing plug-ins.

Steps

1. From the SnapCenter left navigation pane, click **Inventory**.



2. Choose the resource for which you want to configure credentials.

   You must make sure that the Resource Type is **Instance**. This option does not apply to databases and availability groups.

3. Click **Configure Credentials**.

4. In the **Configure Instance Credentials** page, provide the requested SQL Server or Windows credentials for just the instance and click **OK**.

Using Application Request Routing and Network Load Balancing

Application Request Routing (ARR) is a Microsoft Internet Information Services (IIS) feature that you can use to enable SnapCenter load balancing across multiple servers with a single user interface. Network Load Balancing (NLB) is a Microsoft feature that SnapCenter uses to provide server high availability.

You can perform the following tasks related to Application Request Routing and Network Load Balancing:

- Setting up a SnapCenter repository folder. NLB requires a shared SnapCenter folder.
- Viewing NLB status
- Determining whether ARR was enabled during the SnapCenter installation

Application Request Routing requirements

Application Request Routing (ARR) requires specific IIS features and configuration. You should understand the basics of how ARR works and how you can set it up to support SnapCenter.

It is a best practice to install ARR and its required modules before you install SnapCenter, and then allow SnapCenter to configure ARR during installation.

ARR requires the following additional IIS features:

- URL Rewrite
- Web Farm Framework 2.x
- External Cache module

Additionally, ARR requires the following system configuration:

- .NET 3.5

For more information, see the following Microsoft documentation:

- *Application Request Routing Version 2 Overview*
- *Application Request Routing download*
- *Deployment Recommendations for Application Request Routing*
- *Microsoft Web Farm Framework 2.x*

Creating a SnapCenter repository folder for Network Load Balancing

To use Network Load Balancing (NLB) features, you must set up a shared SnapCenter repository folder.

About this task

The shared repository folder is needed to guarantee the same set of plug-ins and the compatibility file (`cf.xml`) for all NLB nodes.

Steps

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

```
Open-SMConnection
```

3. From the command prompt, determine the existing SC repository folder:

```
Get-SmDownloadRepository
```

4. If you need to create a repository, do so:

```
Set-SmDownloadRepository
```

5. If you create a repository and you want to keep the already downloaded plug-in packages and compatibility file, copy the contents of the old repository folder into the new one.

Determining load balancing status and Application Request Routing enablement

A SnapCenter web farm is a web farm that groups IIS instances to perform SnapCenter load balancing. Viewing the Load Balancer page helps you determine the status of load balancing and determine whether Application Request Routing (ARR) was enabled during the SnapCenter installation.

Before you begin

- You have installed Microsoft Application Request Routing and any associated components.
- You have configured Application Request Routing automatically during SnapCenter installation.
- You have set up the SnapCenter Server Farm as part of the SnapCenter installation.
  This is done automatically if you chose to enable ARR during the installation.
- You have defined the ARR load balancing algorithm using IIS Manager.

About this task

Every instance of the IIS Server where SnapCenter is deployed requires the same SnapCenter farm configuration.

Steps

1. In the left navigation pane, click **Administration**.
2. Click **Load Balancer**.
3. View the NLB members and the state of ARR.

Provisioning hosts

You can use the SnapCenter Plug-in for Microsoft Windows to assign NetApp storage to most Windows hosts. Provisioning hosts with the plug-in ensures that the backups you create in SnapCenter are application-consistent.

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

Related concepts

Configuring LUN storage on page 26
Creating and managing SMB shares on page 36

Related references

Supported storage types on page 10

Configuring LUN storage

You can use the SnapCenter Plug-in for Microsoft Windows to configure an FC-connected or iSCSI-connected LUN. You can also use the plug-in to connect an existing LUN to a 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 *Clustered Data ONTAP 8.3 SAN Configuration Guide*.

Related information

Clustered Data ONTAP 8.3 SAN Administration Guide
Data ONTAP DSM 4.1 For Windows MPIO Release Notes

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.
  For more information, see the *Data ONTAP DSM 4.1 For Windows MPIO Installation and Administration Guide*.
- You must have started the iSCSI service on the storage system.
  For more information, see the *Clustered Data ONTAP 8.3 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.

Changing the name of an iSCSI initiator can affect access to iSCSI targets. After changing the name, you might need to reconfigure the targets accessed by the initiator, so that they can recognize the new name. Make sure to restart the host after changing the name of an iSCSI initiator.

Steps

1. In the SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **iSCSI Session**.
3. In the **Storage Virtual Machine** drop-down list, select the Storage Virtual Machine (SVM) for the iSCSI target.
4. In the **Host** field, enter the host name for the session, and then click **Find**.

   Tip: Type the first few letters of the host name to automatically complete the field.
5. Click **Establish Session**.

   The Establish Session wizard opens.
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 for each target you want to establish a session with.

Disconnecting an iSCSI session

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

Steps

1. In the SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **iSCSI Session**.
3. In the **Storage Virtual Machine** drop-down list, select the Storage Virtual Machine (SVM) for the iSCSI target.
4. In the **Host** field, enter the host name for the session, then click **Find**.

   Tip: Type the first few letters of the host name to autocomplete the field.
5. From the list of iSCSI sessions, select the session you want to disconnect and click **Disconnect Session**.
6. In the **Disconnect Session** dialog, 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 SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Igroup**.
3. On the **Initiator Groups** page, click **New**.
4. In the **Create Igroup** dialog box, define the igroup:

In this field...	Do this...
SVM	Select the SVM for the LUN you will map to the igroup.
Host	Select the host on which you want to create the igroup. Type the first few letters of the host name to autocomplete the field.
IGroup Name	Enter the name of the igroup.
Initiators	Select the initiator.
Type	Select the initiator type, mixed or iSCSI.

5. When you are satisfied with your entries, click **OK**.

   SnapCenter creates the igroup on the host.

Renaming an igroup

You can use SnapCenter to rename an existing igroup.

Steps

1. In the SnapCenternavigation pane, click **Hosts**.
2. On the **Hosts** page, click **Igroup**.
3. On 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 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**.

   SnapCenter renames the igroup.

Modifying an igroup

You can add igroup initiators to an igroup by running the Add-SdIgroupInitiator cmdlet on the Plug-in for Windows host.

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.

Step

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

   `Add-SdIgroupInitiator -Name` *`igroup_name`* `-Initiators` *`initiator_name1,initiator_name2, initiator_name3`* `-StorageSystem` *`ip_address`*

   Name

   Specifies the igroup name.

   Initiators

   Specifies a comma-separated list of the initiators you want to add.

   StorageSystem

   Specifies the storage system on which the igroup initiators are located.

Deleting an igroup

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

Steps

1. In the SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Igroup**.
3. On 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:

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

- Disconnect from a disk.
- Delete a disk.

Creating a disk

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 the Plug-in for Windows. For more information, see the *Clustered Data ONTAP 8.3 Logical Storage Management Guide*.

  Note: You cannot create a LUN on a Plug-in for Windows-created clone volume unless the clone has already been split.
- You must have started the FC or iSCSI service on the storage system. For more information, see the *Clustered Data ONTAP 8.3 SAN Administration Guide*.
- If you are using iSCSI, you must have established an iSCSI session with the storage system. For more information, see *Starting an iSCSI session* on page 26.

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 Plug-in for Windows needs to be installed only on the host on which you are creating the disk.

Steps

1. In the SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Disks**.
3. On the **Disks** page, enter the host name in the **Host** field.

   Tip: Type the first few letters of the host name to autocomplete the field. Click **Find Disks** to view a list of disks on the host.
4. Click **New**.

   The Create Disk wizard opens.
5. On the **LUN Name** page, identify the LUN:

In this field...	Do this...
SVM	Select the SVM for the LUN.
LUN path	Enter the full path of the folder containing the LUN. For example, `/vol/test_vol`. Type the first few letters of the volume name to autocomplete the field. **Note:** Do not use the UNC path of the LUN. Use ASCII characters only.
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.

In this field...	Do this...
LUN label	Enter descriptive text for the LUN. Optional.

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. **Note:** 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. **Note:** 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	Let SnapCenter Plug-in for Microsoft Windows automatically assign a volume mount point based on the system drive. For example, if your system drive is `D:`, auto assign creates a volume mount point under your `D:` drive. **Note:** 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. **Note:** 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. Select MB, GB, or TB in the adjoining drop-down list.
Use thin provisioning	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. **Note:** Make sure there is enough space available on the volume to accommodate all the LUN storage you think you will need.
Partition type	Select GPT partition for a GUID Partition Table, or MBR partition for a Master Boot Record. **Note:** 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, then select the host for the initiator. **Note:** This field is displayed only if the LUN is shared by hosts in a Windows Server failover cluster.
Choose host initiator	Select **FibreChannel** or **iSCSI**, 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

- You cannot expand a LUN by more than 10 times its original size, or shrink a LUN by more than half.
- 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, the SnapCenter Plug-in for Microsoft Windows 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 SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Disks**.
3. On the **Disks** page, enter the host name in the **Host** field.

   Tip: Type the first few letters of the host name to autocomplete the field.

4. Click **Find Disks** to view a list of disks on the host.
5. From the list of disks on the host, select the disk you want to resize and click **Resize**.
6. 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.

7. Click **MB**, **GB**, or **TB** to specify the unit of measurement.
8. When you are satisfied with your entries, click **Shrink** or **Expand** as appropriate.

   SnapCenter resizes the disk.

Viewing the disks on a host

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

Steps

1. In the SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Disks**.
3. On the **Disks** page, enter the host name in the **Host** field.

   Tip: Type the first few letters of the host name to autocomplete the field.

4. Click **Find Disks** to view a list of disks on the host.

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 SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Disks**.
3. On the **Disks** page, enter the host name in the **Host** field.

   Tip: Type the first few letters of the host name to autocomplete the field. Click **Find Disks** to view a list of disks on the host.

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...
SVM	Select the SVM for the LUN.
LUN path	Enter the full path of the folder containing the LUN. For example, `/vol/test_vol`. ype the first few letters of the volume name to autocomplete the field. **Note:** Do not use the UNC path of the LUN. Use ASCII characters only.
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	Enter descriptive text for the LUN. Optional.

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. **Note:** 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. **Note:** 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 Plug-in for Microsoft Windows automatically assign a volume mount point based on the system drive. For example, if your system drive is `D:`, auto assign creates a volume mount point under your `D:` drive. **Note:** 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. **Note:** 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. **Note:** This field is displayed only if the LUN is shared by hosts in a Windows Server failover cluster.
Choose host initiator	Select **FibreChannel** or **iSCSI**, 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 autocomplete 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 will lose the contents of the clone.

Before you begin

- Make sure the LUN is not in use by any application.
- Make sure 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 the SnapCenter Plug-in for Microsoft Windows.

About this task

If you disconnect a LUN in a FlexClone volume that the SnapCenter Plug-in for Microsoft Windows created, and no other LUNs on the volume are connected, the plug-in deletes the volume. Before disconnecting the LUN, the plug-in 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 more than just the last characters in the name.

Steps

1. In the SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Disks**.
3. On the **Disks** page, enter the host name in the **Host** field.

   Tip: Type the first few letters of the host name to autocomplete the field.

4. Click **Find Disks** to view a list of disks on the host.
5. In the list of disks on the host, select the disk you want to disconnect and click **Disconnect**.
6. 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 SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Disks**.
3. On the **Disks** page, enter the host name in the **Host** field.

   Tip: Type the first few letters of the host name to autocomplete the field.
4. Click **Find Disks** to view a list of disks on the host.
5. From the list of disks on the host, select the disk you want to delete and click **Delete**.
6. In the **Delete Disk** dialog box, click **OK**.

   SnapCenter deletes the disk.

Related tasks

Disconnecting a disk on page 35

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. Using the cmdlets is recommended because it enables you to take advantage of templates provided with the plug-in 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 plug-in.

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.

Related references

SnapCenter Plug-in for Microsoft Windows cmdlets on page 41

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 SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Shares**.
3. On the **Shares** page, click **New**.

   The New Share dialog opens.
4. In the **New Share** dialog, define the share:

In this field...	Do this...
SVM	Select the SVM for the share.
Description	Enter descriptive text for the share.
Share name	Enter the share name. For example, `test_share`. The name you enter for the share will also be used as the volume name. The share name: • 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 \ / [ ] : | < > + = ; , ?
Share path	• Click in the field to enter a new file system path. For example, `/` • Double-click in the field to select from a list of existing file system paths.

5. 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 SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Shares**.
3. On 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

- Make sure the space reclamation process has completed before performing a restore.
- 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.

Make sure 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 PowerShell command prompt, enter the following command:

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

   `drive_path` is the drive path mapped to the LUN.

Using the SnapCenter Plug-in for Microsoft Windows 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.

Note: For more information on support for VMware storage, see *Supported storage types* on page 10.

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 VMware ESXi 5.0U3 or later.

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

- Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, on x64 platforms
- Microsoft cluster configurations of up to a maximum of 16 nodes supported on VMware when using the Microsoft iSCSI Software Initiator, or up to two nodes using FC
- 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
- Paravirtual SCSI (PVSCSI) adapters, with some additional requirements:
  - PVSCSI adapters require ESX/ESXi 4.0 or later.
  - The PVSCSI controller must exist before the LUN is created.

VMware ESX server-related limitations

The SnapCenter Plug-in for Microsoft Windows is supported on VMware ESX server. 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 ESX credentials is not supported.

  You should use your vCenter credentials when installing the Plug-in for Windows on clustered virtual machines.
- RDM LUNs greater than 2 TB are not supported either in a VMFS 3.0 datastore or on ESX or ESXi server versions earlier than 5.0.

- The VMFS datastore housing the RDM descriptor files must be VMFS 5.0, and both ESXi and vCenter must be version 5.0U3 or later, 5.1U2 or later, or 5.5 or later.
- 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, 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 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 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 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 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 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 RDM LUNs

The Plug-in for Windows supports Microsoft clusters using FC RDM LUNs on different virtual machines belonging to different ESX 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 using the procedure in the VMware *Setup for Failover Clustering and Microsoft Cluster Service* documentation.

   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 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 ESX Server login settings with the VirtualCenter credentials.

SnapCenter Plug-in for Microsoft Windows cmdlets

The SnapCenter Plug-in for Microsoft Windows provides PowerShell cmdlets to support host provisioning and space reclamation jobs.

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.

Note: If you are a domain user with local administrator rights, you must run the Grant-ClusterAccess PowerShell cmdlet before you can run the Plug-in for Windows cmdlets in a Windows failover cluster.

The following cmdlets are supported by the Plug-in for Windows:

- Add-SdIgroupInitiator
- Connect-SdIscsiTarget
- Connect-SdStorage
- Disconnect-SdIscsiTarget
- Disconnect-SdStorage
- Get-SdAluaPaths
- Get-SdFCPInitiator

- Get-SdIgroup
- Get-SdIscsiInitiator
- Get-SdIscsiTarget
- Get-SdStorage
- Invoke-SdHostVolumeSpaceReclaim
- New-SdIgroup
- New-SdSMBShare
- New-SdStorage
- Remove-SdIgroup
- Remove-SdSMBShare
- Remove-SdStorage
- Rename-SdIgroup
- Repair-SdAluaPaths
- Set-SdAluaStateMonitor
- Set-SdStorageSize

Working with managed hosts

You can add hosts and install plug-ins, add a verification server, and migrate resource metadata from previous plug-in versions. You can also update host information.

You can perform the following tasks related to hosts:

- Add hosts and install plug-ins.
  For details, see installation information.
- Configure plug-ins and add a verification server in one step.
  For details, see installation information.
- Update ESX information for a host.
- Place hosts in maintenance mode.
- Remove hosts from SnapCenter.
- Start and stop plug-ins.
- Migrate plug-ins.
  If you are coming to SnapCenter from a SnapManager product, you can use the migration feature to move your existing backup jobs to SnapCenter. After you migrate these jobs, you can run them in SnapCenter the same way you run jobs created with a SnapCenter plug-in.
  For details, see migration information.
- Upgrade plug-ins.
  For details, see installation information.
- Uninstall plug-ins.
  For details, see installation information.

Related information

SnapCenter Software 1.0 Installation and Setup Guide
SnapCenter Software 1.0 Migration Guide for SnapManager Backup Jobs

Updating ESX information

Updating the ESX information for a particular host ensures successful backup, restore, or clone operations of databases residing on RDM-based disks. You must update ESX information when Virtual Storage Console for VMware vSphere credentials change or the database host restarts.

About this task

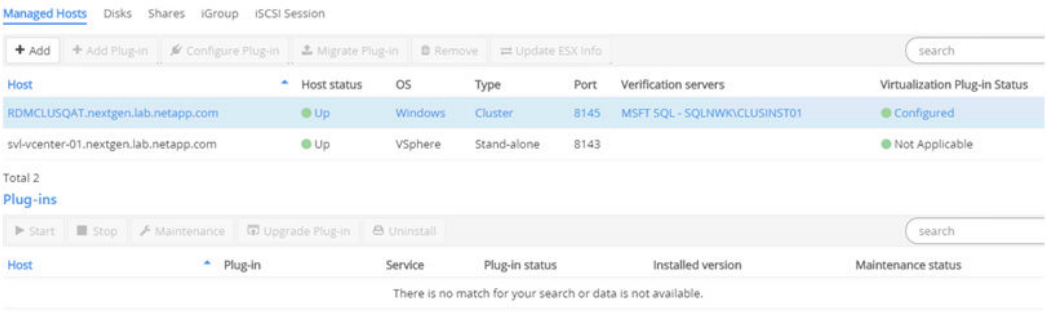
Updating ESX information in SnapCenter initiates communication with Virtual Storage Console for VMware vSphere and obtains vCenter credentials from VSC.

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 VSC server that manages the database host.

Steps

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

2. From the **Managed Hosts** page, select the host you want to update:



3. Click **Update ESX info**.

Stopping and then restarting plug-in services

Stopping SnapCenter plug-in services enables you to perform maintenance actions on them.

Steps

1. From the left navigation pane, click **Hosts**.
2. From the **Managed Hosts** page, select the host.
3. From the **Plug-ins** section, select the plug-in and click **Stop** to stop the plug-in.
4. To start the plug-in again, select the plug-in and click **Start**.

Placing hosts in maintenance mode

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

Steps

1. From the left navigation pane, click **Hosts**.
2. From the **Managed Hosts** page, select the host.
3. From the **Plug-ins** section, select the plug-in and click **Maintenance** to place the host for this plug-in in maintenance mode.

   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 finish

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

Removing a host from SnapCenter

You can remove a host at any time, if you no longer want to use SnapCenter to manage its data protection jobs. You might want to remove a host to gain SnapCenter database space.

Before you begin

You must have removed all the SnapCenter backups and datasets associated with the host you want to delete.

About this task

Removing a host removes all associated resources, such as the SQL Server database and instance.

Removing a host does not remove any operation schedules associated with the host.

Steps

1. From the left navigation pane, click **Hosts**.
2. From the **Managed Hosts** page, select the host you want to remove.
3. Click **Remove** and then **OK** to confirm.

Related tasks

Deleting datasets on page 48
Renaming or deleting backup copies on page 53

Managing datasets

You can create, modify, and delete SQL Server datasets. Also, you can perform backup, clone, and verification operations on datasets. Using a dataset enables you to back up all data associated with a given application at the same time.

About this task

You can perform the following tasks related to datasets:

- Create a backup or clone dataset
- Modify a backup or clone dataset
- Create a backup using the dataset
- Create a clone using the dataset
- Verify the backup
- Delete a backup or clone dataset

For an overview of datasets and when you use them, see the *SnapCenter Software 1.0 Getting Started Guide*.

Related information

SnapCenter Software 1.0 Getting Started Guide
SnapCenter Software 1.0 Operations Guide For SnapCenter Plug-in for Microsoft SQL Server

Types of datasets

Datasets are containers you can use to collect the resources you want to protect. Each data protection job requires a dataset and a policy. Both backup and clone jobs require datasets, and the information you are required to provide varies depending on the job type.

Dataset type	Description
Backup	Backup datasets require the following information: • Name • Resources • Verification • Notification settings

Dataset type	Description
Clone	Clone datasets require the following information: • Name • Resources • Clone options • Notification settings You can add only virtual resources or only physical resources to a clone dataset, not both to the same dataset.

Modifying datasets

You can edit a dataset to modify the information that you provided when creating the dataset.

Steps

1. In the left navigation pane, select **Datasets**.
2. Select a dataset and click **Modify**.
3. Modify the information and click **Finish**.

Stopping operations on datasets temporarily

You can temporarily stop backup, restore, and clone operations on a dataset.

Steps

1. In the left navigation pane, select **Datasets**.
2. Select the dataset for which you want to temporarily stop backup, restore, and clone operations.
3. Click **Maintenance**.
4. Click **OK** in the **Maintenance** window.

Resuming operations on datasets

You can resume backup, restore, and clone operations on a dataset that was stopped temporarily.

Steps

1. In the left navigation pane, select **Datasets**.
2. Select the dataset for which you want to resume backup, restore, and clone operations.
3. Click **Production**.
4. Click **OK** in the **Production** window.

Deleting datasets

You can delete a dataset if you no longer need it to perform backup, restore, clone, or provisioning operations. You must ensure that datasets are deleted before you remove plug-ins from SnapCenter.

Before you begin

For clone datasets, you must have manually deleted all clones associated with dataset.

About this task

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

Steps

1. In the left navigation pane, select **Datasets**.
2. Select the dataset that you want to delete.
3. Click **Delete**.
4. To remove all backups, metadata, policies, and Snapshot copies associated with the dataset, click the **Delete backups and policies associated with this dataset** option.
5. Click **OK**.

Managing policies

You can create, copy, modify, view, and delete SQL Server policies. Policies are required when you perform backup, clone, or verification operations.

About this task

You can perform the following tasks related to policies:

- Create a backup, clone, or verification policy.
- Modify a backup, clone, or verification policy.
- Copy a backup, clone, or verification policy.
- View details of the policy.
- Delete backup, clone, or verification policy.

For an overview of policies and when you use them, see information about getting started with SnapCenter Server.

Types of policies

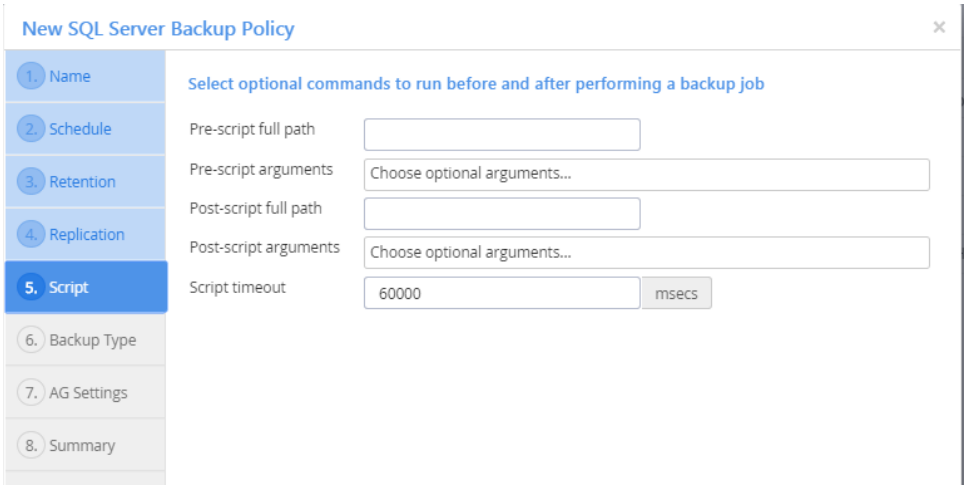
A *policy* is a set of rules governing backup and clone and verification jobs. Policy components vary depending on plug-in and job, but they can include schedule, retention, and replication settings, and provide prescript and postscript arguments and other settings. You are required to create different policies for the different types of data protection jobs.

Policy type	Description
Backup	Backup policies require the following information: • Name • Schedule • Retention • Replication • Prescript and postscript arguments • Backup type • Availability Group settings
Clone	Clone policies require the following information: • Name • Schedule • Options • Prescript and postscript arguments
Verification	Verification policies require the following information: • Name • Schedule • Replication • Prescript and postscript arguments • Options

Understanding policy prescripts and postscripts

You can use set up prescripts and postscripts as part of your backup, clone, or verification policies. These scripts enable automation either before your data protection job or after. For example, you might include a script that automatically notifies you of data protection job failures or warnings. Before you set up your prescripts and postscripts, you should understand some of the requirements for creating these scripts.

Add prescript and postscript information as part of the New Policy or Modify wizards for backup, clone, or verification policies.



Supported script types

The following type of scripts are supported:

- Batch files
- PowerShell scripts
- Perl scripts

Script path location

If you want to create a common script repository, the script path must be a UNC path (for example:`\\IP address\share name`). You must also have read and write permissions on this UNC path.

If you want to keep scripts locally, then you must store the scripts on the local or remote plug-in host where SMCore is installed.

Supported prescript and postscript arguments

The following arguments are supported in prescripts:

- $Database
- $ServerInstance

The following arguments are supported in postscripts:

- $Database
- $ServerInstance

- $BackupName
- $LogBackupFile
- $LogDirectory
- $LogSnapshot

Modifying policies

You can edit a SQL Server policy to modify the information that you provided when creating the SQL server policies. You might want to change the schedule, replication options, Snapshot copy retention settings, scripts, and types.

Steps

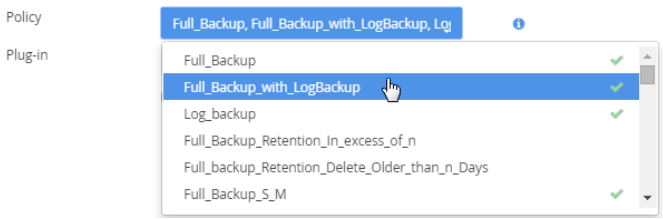
1. In the left navigation pane, select **Policies**.
2. Select the policy and click **Modify**.
3. Modify the information and click **Finish**.

Detaching policies from a dataset

Any time you no longer want policies for a dataset, you might want to detach one or more policies from that dataset.

Steps

1. In the left navigation pane, click **Datasets**.
2. Select the dataset for which you want to detach one or more policies.
3. Click **Modify**.
4. In the **Name** page of the **Modify Dataset** wizard, deselect the policies you want to detach.



5. Make any additional modifications to the dataset in the rest of the wizard, and click **Finish**.

Copying policies

You can copy SQL Server policies if you want to create a policy. Copying a policy rather than creating a new one saves time.

Steps

1. In the left navigation pane, select **Policies**.

2. Select the policy to copy.
3. Click **Copy**.
4. Accept the default name or type a new name and click **OK**.

Viewing policy details

You can view details of SQL Server policies before you perform backup and clone operations or copy a policy. You might want to view the details to ensure the correct options will apply to the operation.

Steps

1. In the left navigation pane, select **Policies**.
2. Select the policy for which you want to view details.
3. Click **Details**.
4. Review the details, and then click **Close**.

Deleting policies

If you no longer need policies that were formerly attached to datasets for backup, restore, or clone operations on SnapCenter, you might want to delete them. Additionally, if you want to remove plug-ins from SnapCenter, you must ensure that the plug-in policies are deleted.

Before you begin

You must have detached the policy from any datasets.

Steps

1. In the left navigation pane, select **Policies**.
2. Select the policy that you want to delete.
3. Click **Delete**.
4. Click **Yes**.

Managing backups

You can view a list of backup copies, delete backup copies interactively, or delete multiple backup copies by using the command-line interface when they are no longer required.

Renaming or deleting backup copies

You can rename or delete backup copies for a selected host resource. If the backup is associated with a cloned database, you cannot delete the backup copy.

Before you begin

For deleting backups, you must have delete the associated clones.

About this task

If you rename or delete a resource, it displays in the Inventory page with a Deleted status. Resources continue to display with the Deleted status until all backups of that resource have also been deleted.

Steps

1. In the left navigation pane, click **Inventory**.
2. To filter the list, select the resource from the **Host**, **Resource Type**, and **SQL Server Instance** (if you chose a database as the resource type).
3. Click **Manage Backups**.

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

4. On the **Manage Backups** page, select the backup copy and rename or delete it.

   To delete backup copy, click **OK** in the Delete Backup window.

5. Click **Close**.

Deleting multiple backup copies using the command-line interface

You can delete multiple backup copies by using the `Remove-SmBackup command`.

Before you begin

- You must be logged in to SnapCenter as a domain user with local administrator rights on each host on which you want to delete multiple backup copies.
- You must have deleted associated clones.

About this task

If you rename or delete a resource, it is displayed in the Inventory page with a Deleted status. Resources continue to be displayed with the Deleted status until all backups of that resource have also been deleted.

Steps

1. Launch PowerShell.
2. From the command prompt, enter:
   `Open-SMConnection`
3. Delete multiple backup copies:
   `Remove-SmBackup –BackupNames (`*`bkupname1, bkupname2,…`*`)`
   `Remove-SmBackup –BackupIds (`*`id1, id2,…`*`)`

Managing clones

SnapCenter clones the databases that you select to the active file system. You can view details about the clones you have created and delete them if you find them no longer necessary.

About this task

For an overview of clones, see information about creating clones in the SnapCenter Plug-in for Microsoft SQL Server Operations Guide.

Related information

SnapCenter Software 1.0 Operations Guide For SnapCenter Plug-in for Microsoft SQL Server

Viewing clone details

You can view details about clones associated with a database. You might want to view clone details for review, or to ensure that the right clone was deleted.

Steps

1. In the left navigation pane, select **Inventory**.
2. Filter the list of resources by selecting the **Host**, **Resource Type**, and **SQL Server Instance** fields.

   From the SQL Server Instance list, you can also select the primary database as the SQL Server Instance.
3. From the resource table, select the parent database for the clone you want to view details about.
4. Click **Manage Clone** to view the list of clones with details taken from the parent database.
5. Click **Close**.

Deleting clones

You can delete clones associated with a database if you find them no longer necessary.

About this task

A clone that has been cloned again cannot be deleted. For example, the production database **db1** is cloned to **db1_clone1** and subsequently cloned to **db1_clone2**. To delete the **db1_clone1** clone, you must first delete the **db1_clone2** clone and then delete **db1_clone1** clone.

Steps

1. In the left navigation pane, click **Inventory**.
2. To filter the list of resources, select the **Host**, **Resource Type**, and **SQL Server Instance**.

   Optionally, from the SQL Server Instance list, select the primary database as the SQL Server Instance.
3. From the resource table, select the parent database for the clone you want to delete.
4. Click **Manage Clone** to view the list of clones taken from the parent database.

5. Select the clone, click **Delete**, and click **OK** to confirm the deletion.

Managing the SnapCenter Server database

Information related to various operations performed from SnapCenter is stored in the SnapCenter database. You must create backups to save and recover SnapCenter Server from data loss.

You can perform the following tasks to protect the SnapCenter database:

- Protects the SnapCenter database by setting the configuration that is required to create a backup of the SnapCenter database.
- Gets the SnapCenter database backups that were backed up on schedule.
- Restores the SnapCenter database when required.

Prerequisites for protecting the SnapCenter database

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

- Adding hosts
  The SnapCenter database host should be added in SnapCenter.
- Managing SVM connections
  Storage credentials should be configured.
- Provisioning hosts
  At least one NetApp storage disk should be present on the host. A NetApp disk on the SnapCenter database host must be created if it is not present on the host.
  For details about adding hosts, setting up SVM connections, and provisioning hosts, see the installation instructions.

Related information

SnapCenter Software 1.0 Installation and Setup Guide

Configuring the SnapCenter database for protection

You can configure the SnapCenter database to protect from data loss by running the `Protect-SmRepository` command.

About this task

- Moves the SnapCenter database from one disk to another disk; the destination must be NetApp
- Creates a dataset named DS_SC_Repository and a policy named Backup_SC_Repository
- Creates backup schedule for the SnapCenter database

Steps

1. Launch PowerShell.
2. From the command prompt, enter:
   `Open-SMConnection`
3. Protect the database:

Protect-SmRepository [-HostName] *string*[-Path] *string* [-AuthMode] *SmAuthMode* {Windows | SQL} [-InstanceCredential] *pscredential* -ScheduleType *SmSchedulerType* {None | OneTime | Hourly | Daily | Weekly | Monthly} [[-SchedulerType] *SmAuthMode* {None | Windows | SQL}] [[-StartTime] *datetime*] [[-EndTime] *datetime*] [[-RetentionCount] *int*] [-WhatIf] [-Confirm] *CommonParameters*

HostName

Specifies the SnapCenter database host name. If the SnapCenter database is hosted by a failover cluster instance (FCI), then specify the FCI owner host name.

Path

Specifies the NetApp destination disk path.

InstanceCredential

Specifies the SnapCenter database instance user name and password.

AuthMode

Specifies the SnapCenter database instance authentication mode.

ScheduleType

Specifies the backup schedule type.

Options are as follows:

SchedulerType

Specifies the scheduler. Default is Windows scheduler.

StartTime

Specifies the scheduled backup start time. The default is the current time.

EndTime

Specifies the scheduled end time.

RetentionCount

Specifies the number of backups to retain. By default, seven backups are retained.

The following command configures the SnapCenter database for protection:

```
Protect-SmRepository -HostName NB-MVA-
DEV057.nbsdsm.lab.eng.btc.netapp.in -Path E:\DBs  -
InstanceCredential sa -AuthMode SQL -ScheduleType Hourly
```

Getting backups of the SnapCenter database

You can access the backups that were backed up on schedule by running the `Get-SmRepositoryBackups` command. The backup is created according to the schedule specified in the `Protect-SmRepository` command or you can create the backup from the SnapCenter UI.

Steps

1. Launch PowerShell.
2. List all available SnapCenter database backups:

   Get-SmRepositoryBackups [[-HostName] *string*] [[-SMSbaseUrl] *string*] [-WhatIf] [-Confirm] [*CommonParameters*]

   Options are as follows:

   HostName

Specifies the SnapCenter database host name. If the SnapCenter database is hosted by a failover cluster instance (FCI), then specify the FCI owner host name.

SMSbaseUrl

Specifies the SnapCenter Server URL. This is required when executing a power shell command from a plug-in machine.

Restoring the SnapCenter database backup

You can restore the SnapCenter database when required by running the `Restore-SmRepositoryBackup` command.

Steps

1. Launch PowerShell.
2. Restore the backup with the correct options:

   `Restore-SmRepositoryBackup [-BackupName] string [-AuthMode] SmAuthMode {None | Windows | SQL} [-InstanceCredential] pscredential [[-SMSbaseUrl] string] [-WhatIf] [-Confirm] [CommonParameters] HostNamestring`

   BackupName

   Specifies the name of the backup to restore.

   AuthMode

   Specifies the SnapCenter database instance authentication mode.

   Options are as follows:

   HostName

   Specifies the SnapCenter database host name. If the SnapCenter database is hosted by a failover cluster instance (FCI), then specify the FCI owner host name.

   SMSbaseUrl

   Specifies the SnapCenter Server URL. This is required when executing a power shell command from a plug-in machine.

The following command restores the SnapCenter database:

```
Restore-SmRepositoryBackup -AuthMode SQL -InstanceCredential sa –
BackupName DS_SC_Repository_NB-MVA-DEV057_05-15-2015_12.32.27.8228
```

Using SnapCenter reporting capabilities

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

Centralized reporting options

SnapCenter makes it easy for you to monitor the health of your systems and your data protection job status, get more detailed information about data protection jobs, monitor SnapCenter activity, and use system log files for troubleshooting.

Dashboard

From the SnapCenter left navigation pane, the Dashboard gives you a first glance into the health of your system, the status of your data protection jobs (backup, restore, and clone), your database protection status, and a SnapVault status.

You can also request more detailed reports about data protection jobs from the Dashboard by clicking one of the pie charts. The report you generate from here pertains only to the jobs you clicked.

Reports

From the SnapCenter left navigation pane, the Reports page offers a more detailed view into data protection jobs (backup, restore, and clone) and plug-in information. You can run reports about all jobs of the selected type (backup, clone, or restore), jobs for a specific host, jobs for a specific dataset, jobs for a specific policy, jobs with a specific status (completed, failed, or warning), and jobs for a specific resource. The plug-in report provides details on resource protection. You can export reports in a variety of formats and print them.

Monitor options

From the SnapCenter left navigation pane, the Monitor page enables you to view the following details:

Jobs

Displays information about host, dataset, policy, plug-in installation and uninstallation, provision, discovery, backup, restore, clone, and verification jobs. You can filter this view based on either start and end date, type of job, or status. You can also get additional details by clicking **Details** after selecting a job. The Details window enables you to view log details. You can also view the log details by clicking **View Logs**. For backup jobs, you can click **Report** and view the detailed report for that specific job.

Schedules

Displays information about schedules you have created in your SnapCenter environment. In the Schedule section, when you select a specific dataset from the drop-down box and select a schedule type, the details about the schedule (such as the policy that initiated the schedule, the host, the start time, the schedule expire time, the next run, and the last run of the schedule) are displayed.

Events

Displays information about system activity, such as when a user creates a dataset or when the system initiates activities, such as creating a scheduled backup. 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.

Logs

Displays SnapCenter Server and plug-in logs. Plug-in logs are available by host and plug-in. You can also filter by a specific source or message or select a log level. You can use these logs for advanced troubleshooting.

Related concepts

Monitoring SnapCenter jobs on page 66
Monitoring SnapCenter schedules on page 67
Monitoring SnapCenter events on page 68
Monitoring SnapCenter logs on page 68

Dashboard reports

The Dashboard gives you a first glance into the health of your system, the status of your data protection jobs, and SnapVault status. To understand the information provided in SnapCenter reports, it is helpful for you to know some of the terminology. Similar reports display on the Reports pages.

Host status tile

The host status tile gives you information about all hosts you have added to SnapCenter and the plug-ins you have installed on these hosts.

Note: After adding a new host or after starting SnapCenter it might take several minutes for the host status to be updated.

Host status	
Host up	The host is up and communicating with SnapCenter.
Host down	SnapCenter is not able to communicate with this host.
Plug-ins inactive	These hosts are up and communicating with SnapCenter but do not have plug-ins running.
Plug-in unsupported	These hosts have one or more unsupported plug-ins. An unsupported plug-in is not compatible with this version of SnapCenter.
Plug-in upgradeable	These hosts have one or more plug-ins that you can upgrade.

Backup, restore, and clone job tiles

The backup, restore, and clone job tiles give you information about the data protection jobs you have run during the specified time period. You can customize the time frame for the report by using the drop-down list located in each tile. The default report provides information about data protection jobs run for the past seven days.

Backup, restore, and clone jobs	
Running	Specifies the number of jobs that are currently running.
Failed	Specifies the number of jobs that have failed.
Warning	Specifies the number of jobs that have experienced an error.
Completed	Specifies the number of jobs that have successfully completed.

MS SQL Database Protection on Primary Storage tile

The MS SQL Database Protection on Primary Storage tile gives you information about the databases you have on your primary storage system, whether they are associated with datasets, and if they are being successfully backed up.

If the plug-in has a newer version available, an Upgradable status appears. If the plug-in is no longer supported, an Unsupported status appears.

MS SQL Database Protection on Primary Storage	
Unprotected	The number of databases that are not part of any dataset and have not been backed up.
Not backed up	The number of databases that are part of a dataset, but a backup has not been performed during the specified time period.
Failed	The number of databases that are part of a dataset that has run a backup during the specified time period, but the backup failed.
Protected	The number of databases in a dataset that has been successfully backed up during the specified time period.

MS SQL Database SnapVault Summary tile

The MS SQL Database SnapVault Summary tile gives you information about databases being backed up to secondary storage systems using SnapVault and the status of the SnapVault relationships.

If the plug-in has a newer version available, an Upgradable status appears. If the plug-in is no longer supported, an Unsupported status appears.

MS SQL Database SnapVault Summary	
No SnapVault updates	The database is part of one or more datasets that are not updating SnapVault relationships.
SnapVault updates successful	The number of databases that have a SnapVault relationship with recent and successful updates. These databases are SnapVault protected.
SnapVault updates failed	The number of databases with a SnapVault relationship but with updates that have failed.

Requesting job status reports from the Dashboard

You can request reports about backup and restore jobs that have a particular status 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. From the SnapCenter left navigation pane, click **Dashboard**.
2. Locate the pie chart for the job for which you want to obtain a job status report.
3. Click the pie slice representing the status for which you want a report.

Result

When you click the pie chart, you are redirected from Dashboard page to the Reports page. The report displays only jobs with the status you selected. You can review the report or download it to your local system.

Configuring your dashboard

You can modify the Dashboard display to best suit your SnapCenter configuration and information needs.

Steps

1. From the SnapCenter left navigation pane, click **Dashboard**.
2. Click **Modify**, select the tiles that you want to display in the **Dashboard** view, and click **OK**.

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 Details 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. There is no clone details report.
Restore Report	The Restore Report provides overall information about restore jobs. There is no restore details report.
Plug-in Report	These reports provide protection details for resources managed by all plug-in instances. You can see an overview, details about databases outside of datasets (unprotected), databases that have not been backed up during this report period, databases that belong to a dataset for which backups have failed, and database SnapVault status.

Configuring your reports

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

Steps

1. From the SnapCenter 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:
   - Dataset
   - 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. From the SnapCenter 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.
Export a report to an alternate format	Choose a format from the **Export** icon drop-down list: • CSV • Excel • PDF • Rich Text Format • TIFF • Web Archive

3. To print the reports in either case, click the **Print** icon.

Configuring the option to email reports

If you want to have regular SnapCenter data protection job updates sent to yourself or to others, you can configure the option to email the SnapCenter reports when you are creating a dataset.

Steps

1. From the SnapCenter left navigation pane, click **Datasets**.
2. Click **New** and select the type of dataset you want to create, or click **Modify** and select the existing dataset you want to modify.
3. In the **New Dataset** wizard, to email reports, select to receive reports always, on failure, or on failure or warning.
4. Enter your SMTP server, 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

Viewing active jobs, scheduled tasks, events, and log information related to SnapCenter enables you to monitor the health of your system, assess your data protection status, and use system log files for troubleshooting.

You can perform the following tasks related to monitoring:

Using this page...	You can perform these tasks...
Jobs	View information about backup, clone, restore, and verification jobs. You can filter this view based on start and end date, type of job, dataset, policy, or plug-in type. You can also get additional details and log files for specified jobs.
Schedules	View backup, clone, or verification schedules that you created in your SnapCenter configuration.
Events	View information about SnapCenter system activities, such as when a user creates a dataset or when the system initiates activities, such as creating a scheduled backup. 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.
Logs	View SnapCenter Server and plug-in logs for troubleshooting.

Related concepts

Monitoring SnapCenter jobs on page 66
Monitoring SnapCenter schedules on page 67
Monitoring SnapCenter events on page 68
Monitoring SnapCenter logs on page 68

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, dataset, policy, or plug-in type. You can also get additional details and log files for specified jobs.

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 backup operations on the Jobs page

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

About this task

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

- In progress
- Completed successfully
- Failed
- Completed with warnings
- Queued
- Verification job is queued

Steps

1. From the left navigation pane, click **Monitor**.
2. From the top navigation bar, click **Jobs**.
3. Optional: On the **Jobs** page, filter the list so that only backup operations appear in the list by clicking **Filter**, selecting **Backup** from **Type**, and clicking .
4. Optional: To see the logs, select a backup copy from the list and click **Details**.

Stopping a scheduled job

If you are performing maintenance on a dataset or one of its resources, you should stop a scheduled job by placing the dataset in maintenance mode or by detaching the policy from the dataset.

Steps

1. In the navigation pane, select **Datasets**.
2. Select the dataset for which you want to temporarily stop backup, restore, and clone operations.
3. Click **Maintenence**.
4. Click **Yes** in the **Maintenance** window.

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 dataset and policy information.

Steps

1. From the SnapCenter left navigation pane, click **Monitor**.
2. From the top navigation pane, click **Schedules**.
3. Select the dataset 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 dataset 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. From the SnapCenter left navigation pane, click **Monitor**.
2. From the top navigation pane, click **Events**.
3. Optional. In the Filter box, enter the start or end date, category of event (such as backup, dataset, 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 logs to help with troubleshooting.

About this task

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. From the SnapCenter left navigation pane, click **Monitor**.
2. From the top navigation pane, click **Logs**.
3. Choose the log type, host, and instance.
   If you select a log type of **plugin**, you can select a host or a 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 on the filter icon at the top of the column heading.
   To show all logs, choose “Greater than or equal to”" the level of “Debug”.
5. Click **Refresh**.
6. View the list of logs.

Related tasks

Monitoring backup operations on the Jobs page on page 66

Types of SnapCenter logs

Because you might need to troubleshoot operations in SnapCenter, it is helpful to know the types of logs that you can use.

Logs that appear in the Monitor > Logs page

The following types of logs appear on the Logs page:

Server logs

Include information from your SnapCenter Server. These are typically located at C:\inetpub\wwwroot\SnapCenter\App_Data\log.

Plug-in logs

Show information from hosts that have SnapCenter plug-ins installed. These include logs from SMCore, as well as logs from the SnapCenter Plug-in for Microsoft SQL Server and SnapCenter Plug-in for Microsoft Windows.

Note: You can find the plug-in log in the installation directory for the plug-in. For RDM and VMDK support, you should also review `VirtualizationAPI.log` in the installation directory for the SnapCenter Plug-in for Microsoft Windows.

Job logs

Show information associated with a specific job. Job logs can span from the SnapCenter Server down to the hosts and plug-ins.

Installation logs

SnapCenter Server installer log (SMSInstall log)

A Microsoft Windows Installer (MSI) log file provided at the end of the installation or uninstall process. This log is useful if an error occurred in the process or the installation was interrupted.

SMCore Installer log

An MSI log file provided at the end of the installation or uninstall process. This log is also useful if an error occurred in the process or the installation was interrupted.

SnapCenter*version*.exe/debug log

Install and uninstall logs that you can use to troubleshoot installation and uninstallation processes.

Using the MSI log files

Both MSI files show error and success codes at the "MainEngineThread is returning" line. If the file includes "Remove = All," the log file resulted from an uninstallation process.

Steps

1. To search through the log, search for " error " (without the quotes and including a space before and after the word).

   Note: You can ignore lines such as the following containing the word "error" in the text:

   ```
   SchedSecureObjectsRollback: Failed to store ACL rollback
   information
   with error 0x80070002 - continuing
   ```

Using the SnapCenter*version*.exe/debug log

SnapCenter creates one or more install and uninstall logs in a single bundle installation log file, `InstallShield.log`, in the same folder as SnapCenter*version*.exe. Each section of the log starts with a line that includes “InstallShield suite engine (Unicode) started.”

Steps

1. To specify a log file location and name, enter the path and name:

```
SnapCenter1.0.exe /debuglog c:\SCBundleInstallLog.txt
```

2. Look for the final status by searching for "final exit status" text.
   The final status includes a code that indicates either that the installation was successful or that errors occurred:
   - 0x00000000 indicates success.
   - 0x00000642 indicates that the user cancelled the installation process.
   - 0x00000643 indicates that an error occurred in the installation process.
3. Search for the error by searching up from the "final exit status" text at the end of the log section.
   For example:

```
4-24-2015[02:33:43 PM]: UI DLL: Display Error: The following items
are required
to launch this setup: System restart since there is a pending restart.
```

4. To determine which MSI installer log includes the error, locate "Parcel operation return status" and find the product code:
   - {DEF09FA0-E342-4378-A38C-A4E49D3B05A9} indicates SnapCenter Server.
   - {3F29BA2D-F761-4A6C-AC76-EB07B5D1B713} indicates SMCore.

Event log locations

SnapCenter gives you access to powerful event log monitoring and tracking capabilities. You should know where to look for the types of events about which you want information.

Event type	Event log location
Completed and failed backup, restore, clone, and verify jobs	Plug-in host event viewer | application
Start events for backup, restore, clone, and verify jobs	SnapCenter host event viewer | application
Add, remove, and update policies and datasets events	SnapCenter host event viewer

Exporting logs

You can export SnapCenter logs so that you can view them in hard copy or in another format.

About this task

You can view logs from remote hosts for a specific log type or a specific plug-in and host combination.

Note: Installer logs from the remote hosts are not included.

Steps

1. From the SnapCenter left navigation pane, click **Monitor**.
2. From the top navigation pane, click **Logs**.
3. Choose the log type, host, and instance.

   If you select a log type of **plugin**, you can select a host or a plug-in. You cannot do this if the log type is **server**.
4. Click **Refresh**.
5. To filter the results 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”" the level of “Debug”.
6. Click **Download**.

   SnapCenter creates a .zip file that includes the specified logs.

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.

Steps

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

   ```
   Open-SMConnection
   ```
3. From the command prompt, enter:

   ```
   Remove-SmJobs
   ```
4. From the left navigation pane of SnapCenter, click **Monitor**.
5. From the top navigation bar, click **Jobs**.
6. From the **Jobs** page, review the status of the job.

Administering 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 plug-ins, the hosts, and similar information, and sending it to a specified clustered Data ONTAP Storage Virtual Machine (SVM).

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, enter:

```
Open-SmConnection
```

2. Now disable EMS data collection by entering:

```
Disable-SmDataCollectionEms
```

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, enter:

```
Open-SmConnection
```

2. Now enable EMS data collection by entering:

```
Enable-SmDataCollectionEMS
```

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, enter the `Open-SmConnection` cmdlet.

   ```
   Open-SmConnection
   ```

2. To change the EMS data collection target, enter the `Set-SmDataCollectionEmsTarget` cmdlet.

   This cmdlet has the format:

   ```
   Set-SmDataCollectionEmsTarget
   -Target SVM_name
   ```

   `SVM_name` is the name of the SVM you want to use for the target.

3. To change the EMS data collection schedule, enter the `Set-SmDataCollectionEmsSchedule` cmdlet.

   This cmdlet has the format:

   ```
   Set-SmDataCollectionEmsSchedule
   -RunAs RunAs_account_credentials
   -DaysInterval
   -StartDateTime
   ```

   `RunAs_account_credentials` is the Run As account that you set up earlier.

   This cmdlet changes the Windows Scheduled Task that triggers the data collection EMS process.

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, open the connection by entering:

   ```
   Open-SmConnection
   ```

2. To retrieve information about the EMS data collection schedule, enter:

   ```
   Get-SmDataCollectionEmsSchedule
   ```

3. To retrieve information about the EMS data collection status, enter:

   ```
   Get-SmDataCollectionEmsStatus
   ```

4. To retrieve information about the EMS data collection target, enter:

```
Get-SmDataCollectionEmsTarget
```

Where to go next

You can use SnapCenter to perform backup and clone data protection jobs. You can also explore other features, such as PowerShell cmdlets, in other information resources.

You can find more information about these features, as well as release-specific information for SnapCenter, in the following documentation, available on the NetApp Support Site at *mysupport.netapp.com*:

- *SnapCenter Software 1.0 Release Notes*
  Describes new features, important cautions, known issues, and limitations of the product.
- *SnapCenter Software 1.0 Migration Guide for SnapManager Backup Jobs*
  Provides information about how to migrate your data from previous versions of SnapDrive and SnapManager to your SnapCenter environment.
- *SnapCenter Software 1.0 Cmdlet Reference Guide*
  Describes the Orchestrator activities and properties and provides syntax and examples of the PowerShell cmdlets and parameters that are used by SnapCenter for backing up, cloning, and restoring application data.
- *SnapCenter Software 1.0 Operations Guide For SnapCenter Plug-in for Microsoft SQL Server*
  Describes how to perform backup, restore, clone and verification jobs on Microsoft SQL Server databases using the SnapCenter user interface.

Copyright information

Trademark information

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 to *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., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

E

F

H

I

J

L

M

N

P

R

S

T

U

V

W