



SnapCenter® Software 1.1

Installation and Setup Guide

July 2016 | 215-10969_CO
doccomments@netapp.com

 **NetApp®**

Contents

| | |
|--|-----------|
| SnapCenter overview | 6 |
| SnapCenter features | 6 |
| SnapCenter components | 6 |
| SnapCenter security features | 9 |
| How resources, datasets, and policies are used in data protection | 10 |
| Installation workflow for SnapManager users | 11 |
| Installation workflow for new users | 13 |
| Preparing for the installation | 14 |
| Storage types supported by SnapCenter Plug-in for Microsoft SQL Server | 14 |
| Storage types supported by SnapCenter Plug-in for Oracle Database | 15 |
| Host requirements | 16 |
| Storage system, application, and browser support | 18 |
| Connection and port requirements | 19 |
| SnapCenter licensing | 20 |
| SnapCenter repository identification | 22 |
| Network Load Balancing and Application Request Routing options | 22 |
| Application Request Routing requirements | 23 |
| SnapCenter installation worksheet | 24 |
| Installing SnapCenter and the plug-in packages | 26 |
| Installing the SnapCenter Server | 27 |
| Logging in to SnapCenter | 28 |
| Configuring role-based access control for SnapCenter users | 28 |
| Types of role-based access control in SnapCenter | 29 |
| Role-based access control permissions and roles | 30 |
| Pre-defined roles and permissions | 30 |
| Adding a user to a role | 33 |
| Assigning resources to users | 34 |
| Setting up SVM connections | 34 |
| Setting up Run As credentials | 36 |
| Authentication methods for your Run As credential | 36 |
| Setting up your Run As credentials | 37 |
| Installing plug-in packages | 38 |
| Available plug-in types | 38 |
| SnapCenter plug-in deployment checklist | 39 |
| Adding hosts and installing plug-in packages on remote hosts | 42 |
| Installing plug-ins on multiple remote hosts | 46 |
| Monitoring SnapCenter plug-in package installation status | 47 |
| Managing the SnapCenter Plug-in Loader service | 48 |
| Identifying available resources | 49 |
| Registering VSC for VMware vSphere with SnapCenter | 49 |
| Monitoring virtualization status in SnapCenter | 50 |

| | |
|---|-----------|
| Configuring the host log directory and verification server for SQL Server | 51 |
| Provisioning storage on Windows hosts | 54 |
| Configuring LUN storage | 54 |
| Establishing an iSCSI session | 54 |
| Disconnecting an iSCSI session | 55 |
| Creating and managing igroups | 55 |
| Creating and managing disks | 57 |
| Creating and managing SMB shares | 63 |
| Creating an SMB share | 63 |
| Deleting an SMB share | 64 |
| Reclaiming space on the storage system | 64 |
| Using the SnapCenter Plug-in for Microsoft Windows in VMware environments ... | 65 |
| Supported VMware guest OS platforms | 65 |
| Using FC RDM LUNs in a Microsoft cluster | 66 |
| Troubleshooting RDM LUN creation | 68 |
| SnapCenter Plug-in for Microsoft Windows cmdlets | 68 |
| Preparing storage systems for SnapMirror and SnapVault replication | 70 |
| Understanding the differences between SnapMirror and SnapVault | 70 |
| Preparing storage systems for SnapMirror replication | 70 |
| Preparing storage systems for SnapVault replication | 72 |
| Upgrading SnapCenter and SnapCenter plug-in packages | 75 |
| Configuring SnapCenter to check for available updates | 75 |
| Upgrading SnapCenter | 75 |
| Upgrading your plug-in packages | 76 |
| Uninstalling SnapCenter and the plug-in packages | 78 |
| Preparing for plug-in uninstallation | 78 |
| Detaching policies from a dataset | 78 |
| Deleting datasets for SQL Server | 78 |
| Deleting datasets for Oracle databases | 79 |
| Uninstalling the plug-in packages from a host using SnapCenter GUI | 79 |
| Uninstalling SnapCenter Plug-in for Microsoft SQL Server using SnapCenter GUI | 80 |
| Uninstalling the plug-ins packages from multiple remote hosts | 80 |
| Uninstalling SnapCenter | 81 |
| Features enabled on your Windows host during installation | 83 |
| Installation troubleshooting | 85 |
| Enabling AutoSupport email notifications | 85 |
| HTTP error 503. The service is unavailable. | 85 |
| Unable to display SnapCenter web login page on local host | 85 |
| SnapCenter Plug-ins Package for Linux installation fails due to incorrect Java version | 85 |
| SnapCenter Plug-ins Package for Linux installation fails due to improper uninstallation | 86 |
| SnapCenter Server is unable to communicate with the host | 86 |

| | |
|--|-----------|
| SnapCenter plug-in loader fails with an error | 86 |
| Where to go next | 88 |
| Copyright information | 89 |
| Trademark information | 90 |
| How to send comments about documentation and receive update notifications | 91 |
| Index | 92 |

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. With SnapCenter, database and storage administrators learn a single tool to manage backup, restore, and cloning operations for a variety of applications and databases.

SnapCenter manages data across endpoints in the NetApp Data Fabric. You can use SnapCenter to replicate data between on-premise environments, between on-premise environments and the cloud, and between private, hybrid, or public clouds.

SnapCenter features

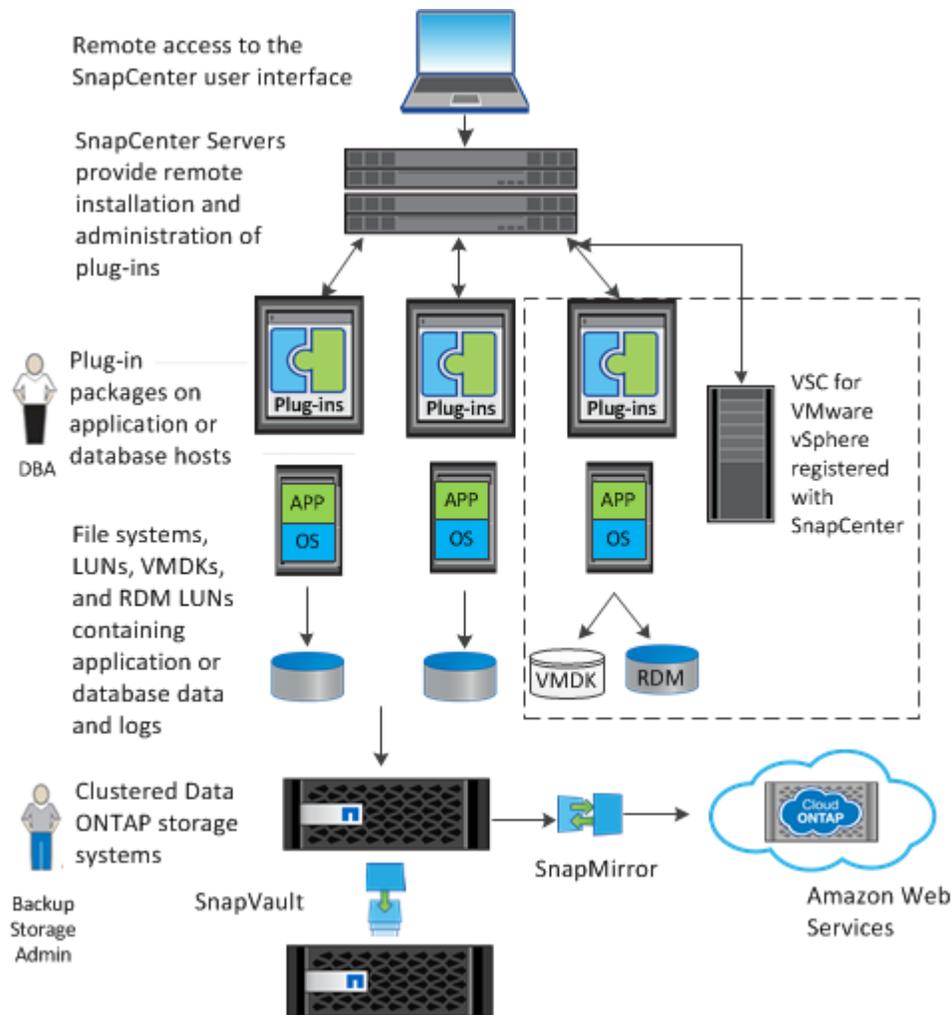
SnapCenter enables you to create application-consistent Snapshot copies and to perform data protection jobs, including Snapshot copy-based backup, clone, restore, and backup verification jobs. SnapCenter creates a centralized management environment, while using role-based access control (RBAC) to delegate data protection and management capabilities to individual application users across your SnapCenter Server and Windows or Linux 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) for security and centralized role delegation
- Application-consistent Snapshot copy management, restore, clone, and backup verification support from both primary and secondary destinations (SnapMirror and SnapVault)
- Remote package installation from the SnapCenter graphical user interface
- Nondisruptive, remote upgrades
- A dedicated SnapCenter repository that provides faster data retrieval
- High availability and load balancing implemented using Microsoft Windows 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-ins Package for Windows, and the SnapCenter Plug-ins Package for Linux. Each of these packages contain plug-ins to SnapCenter. SnapCenter also interacts with Virtual Storage Console for VMware vSphere (VSC) to provide support for database backup, restore, recovery, and cloning on raw device mappings (RDMs) and virtual machine disks (VMDKs). When you are installing and configuring SnapCenter, it is helpful to understand its components.



SnapCenter Server

The SnapCenter Server includes a web server, a centralized HTML5-based user interface, PowerShell cmdlets, APIs, and the SnapCenter repository. SnapCenter enables load balancing, high availability, and horizontal scaling across multiple SnapCenter Servers within a single user interface. You can accomplish high availability by using Network Load Balancing (NLB) and Application Request Routing (ARR) with SnapCenter. For larger environments with thousands of hosts, adding multiple SnapCenter Servers can help balance the load.

The SnapCenter platform is based on a multitiered architecture that includes a centralized management server (SnapCenter Server) and a SnapCenter host agent (SMCore):

- If you are using the SnapCenter Plug-ins Package for Windows, the SMCore runs on the SnapCenter Server and Windows plug-in host. The SnapCenter Server communicates with the Windows plug-ins through the SMCore.
- If you are using the SnapCenter Plug-ins Package for Linux, the SMCore running on the SnapCenter Server host communicates with the SnapCenter Plug-in Loader (SPL) running on the Linux host to perform different data protection operations.

SnapCenter 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, and log and event viewers.

Information about SnapCenter operations is stored in the SnapCenter repository.

SnapCenter Plug-ins Package for Windows

This installation package includes the following plug-ins:

SnapCenter Plug-in for Microsoft SQL Server

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

If you want to perform data protection operations on SQL Servers that are on VMDKs or RDMs, you must register VSC with SnapCenter using the SnapCenter Add Hosts wizard or the VSC Configure SnapCenter Server dialog box.

SnapCenter Plug-in for Microsoft Windows

The Plug-in for Windows provides storage provisioning, Snapshot copy consistency, and space reclamation for Windows hosts. With the plug-in installed on your Windows host, 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 SQL Server databases on SMB shares.

Some features are not supported on all operating systems. See information about host requirements in the installation prerequisites.

SnapCenter Plug-ins Package for Linux

This installation package includes the following plug-ins:

SnapCenter Plug-in for Oracle Database

The Plug-in for Oracle is a host-side component of the NetApp integrated storage solution offering application-aware backup management of Oracle databases. With the Plug-in for Oracle installed on your Oracle host, SnapCenter automates backup, restore, recovery, verify, mount, unmount, and clone operations.

If you want to perform data protection operations on Oracle databases that are on VMDKs or RDMs, you must register VSC with SnapCenter using the SnapCenter Add Hosts wizard or the VSC Configure SnapCenter Server dialog box.

Note: You can use the Plug-in for Oracle to manage Oracle databases for SAP as well. However, SAP BR*Tools integration is not supported.

SnapCenter Plug-in for UNIX

The Plug-in for UNIX handles the underlying host storage stack and enables you to perform backup, restore, clone, mount, and unmount operations on Oracle databases that are running on a Linux host by working in conjunction with the Plug-in for Oracle. The Plug-in for UNIX supports the Network File System (NFS) and storage area network (SAN) protocols on a storage system that is running clustered Data ONTAP.

Virtual Storage Console for VMware vSphere

Virtual Storage Console for VMware vSphere (VSC) is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems. Integrating SnapCenter with VSC enables SnapCenter to perform backup, clone, and restore operations on database environments (SQL Server or Oracle database) that are backed by VMware datastores, VMDKs, or RDMs.

VSC uses SnapCenter to perform backup, restore, and clone operations for storage systems running clustered Data ONTAP 8.2.2 or later. Integrating VSC with SnapCenter enables VSC backup and recovery to use the SnapCenter database to store metadata. This greatly increases the scalability of VSC. This integration also enables the use of backup policies, enabling you to create and reuse policies in VSC, even across multiple VSC environments.

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

If you used VSC to create policies and datasets and registered VSC with SnapCenter, you can view these policies and datasets in SnapCenter. You can also view VSC-based backup, clone, and restore operations in the SnapCenter Jobs view.

VSC is not included in the SnapCenter installation.

Note: You need not register VSC with SnapCenter if you are using Plug-in for SQL Server (and your SQL Server environment uses an iSCSI initiator) or Plug-in for Oracle (and your Oracle environment uses NFS or an iSCSI initiator). If you do not register VSC with SnapCenter, a message appears in the SnapCenter Hosts view that indicates you should configure the hypervisor. For these conditions, you do not need to configure the hypervisor.

Related references

[Host requirements](#) on page 16

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 SnapCenter 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 default period of 20 minutes of inactivity, SnapCenter prevents access to features and you must log in again.

If you have SnapCenter operations that take longer than 20 minutes to complete, you can change the default log out period by using the Windows Internet Information Services (IIS) Manager to change the SnapCenter session state for the ASP.NET_SessionId, located under Cookie Settings.

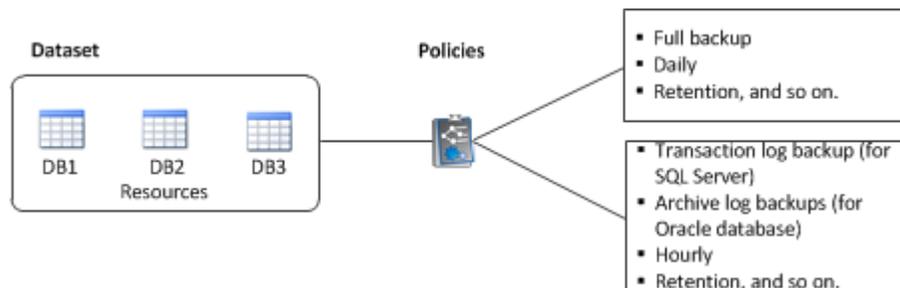
How resources, datasets, and policies are used in data protection

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

- *Resources* are typically databases that you back up or clone.
However, depending on your environment, resources might be database instances, Microsoft SQL server availability groups, Oracle databases, Oracle RAC databases, or anything that you want to back up or clone.
- A SnapCenter *dataset* is a collection of resources on a host or cluster.
When you perform an operation on a dataset, you perform that operation on the *resources* defined in the dataset.
- The *policies* specify the schedule, copy retention, replication, scripts, and other characteristics of data protection operations.
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 all databases of a host, for example, you might create a dataset that includes all the databases in the host. You could then attach two policies to the dataset: one that performs a full backup daily and another that performs transaction log (for SQL) or archive log backups (for Oracle database) hourly.

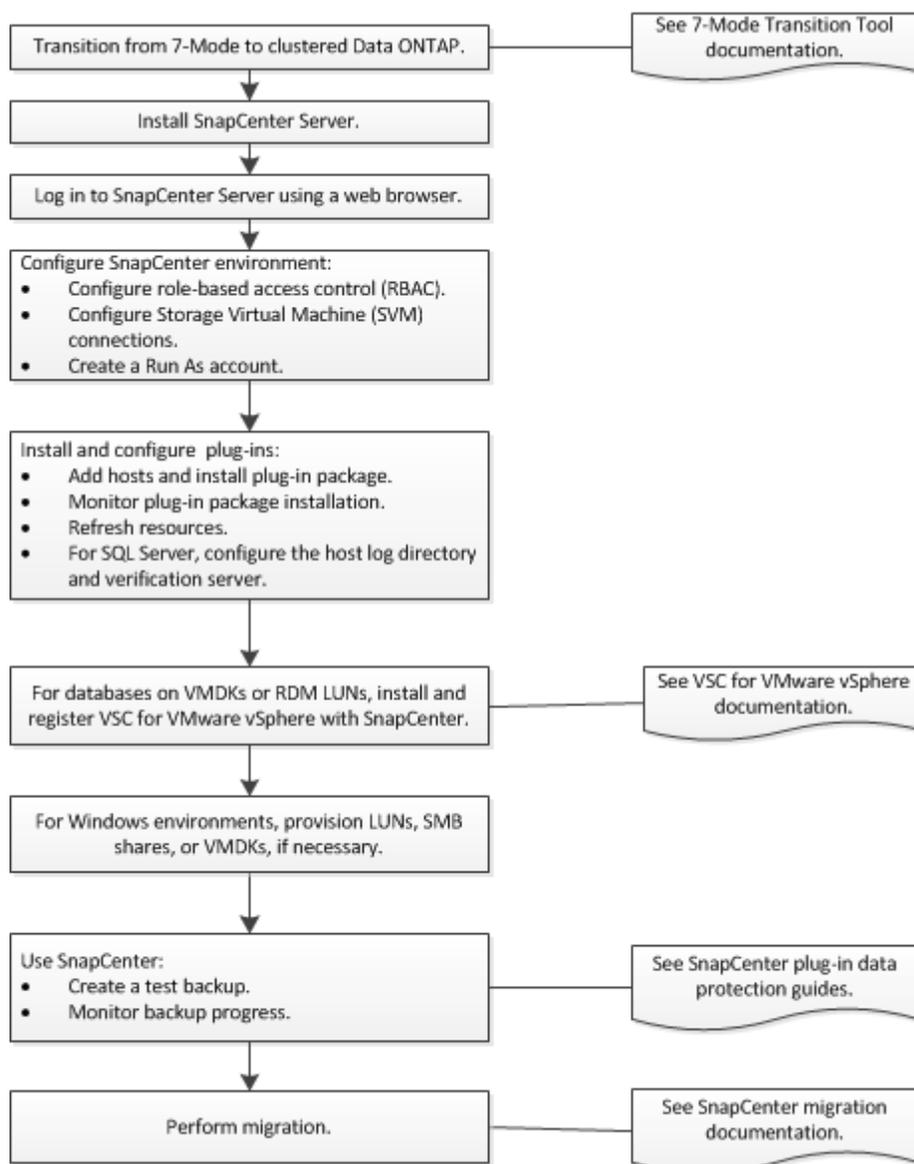
The following image illustrates the relationship between resources, datasets, and policies:



Installation workflow for SnapManager users

If you are coming to SnapCenter from a NetApp SnapManager product, you have already set up storage layouts, defined replication relationships, and configured backup jobs. After you install and configure SnapCenter, you can use the SnapCenter migration feature to migrate from your SnapManager environment to SnapCenter.

Note: SnapCenter does not support Data ONTAP running in 7-Mode. You can use the 7-Mode Transition Tool to migrate data and configurations stored on a system running in 7-Mode to a clustered Data ONTAP system. For details, see [NetApp Documentation: 7-Mode Transition Tool](#).



Some features are available only with specific operating systems. See host requirements information.

Related references

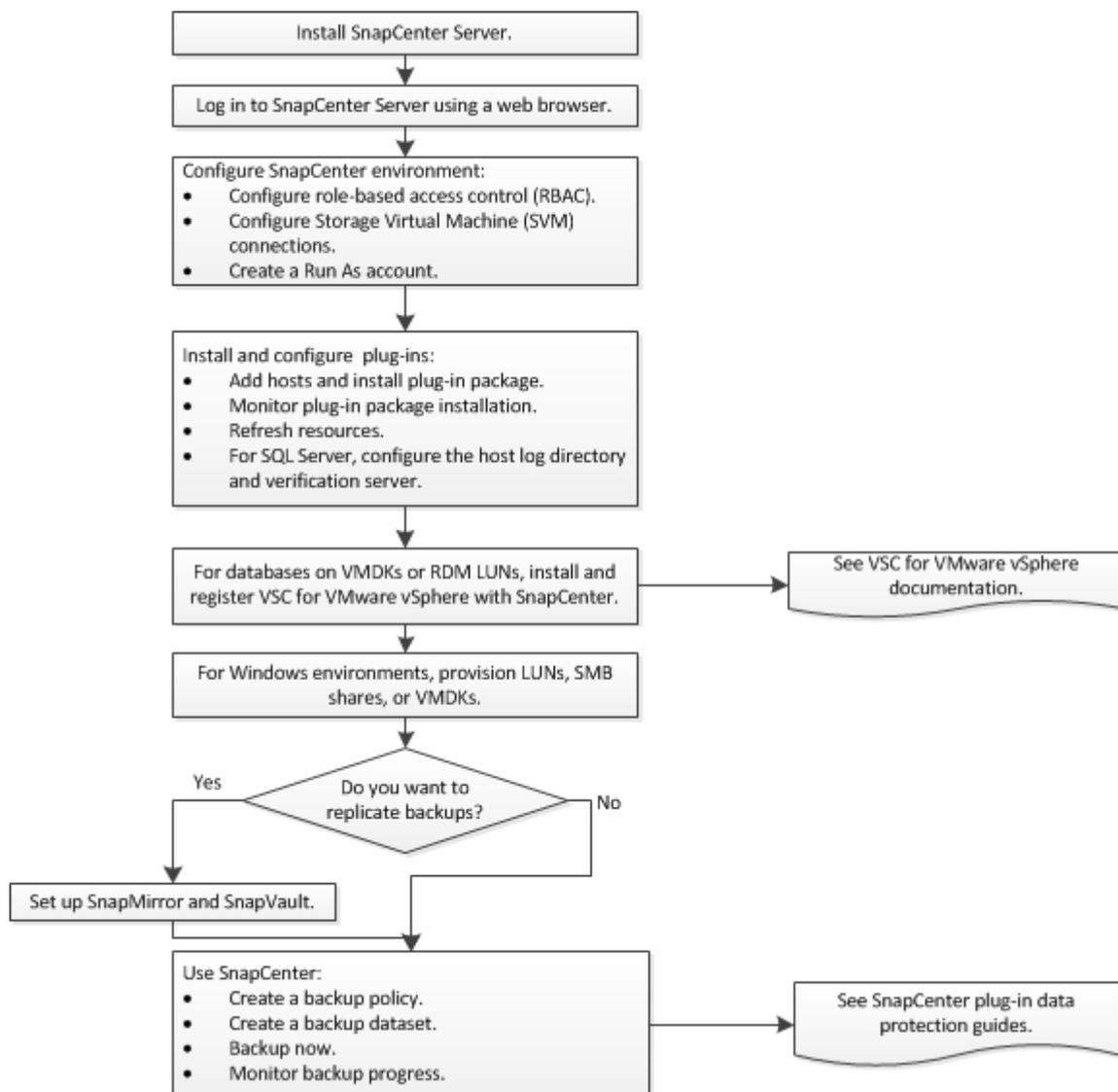
[Host requirements](#) on page 16

Related information

NetApp Documentation: Virtual Storage Console for VMware vSphere
SnapCenter Software 1.1 Data Protection Guide for Microsoft SQL Server
SnapCenter Software 1.1 SnapManager Migration Guide
SnapCenter Software 1.1 Data Protection Guide for Oracle Databases
NetApp Documentation: 7-Mode Transition Tool

Installation workflow for new users

If you are new to SnapCenter and have never used a NetApp SnapManager product, you need to install and configure the server and packages, provision storage, and set up replication relationships before you can create backups.



Some features are available only with specific operating systems. See host requirements information.

Related references

[Host requirements](#) on page 16

Related information

[NetApp Documentation: Virtual Storage Console for VMware vSphere](#)
[SnapCenter Software 1.1 Data Protection Guide for Microsoft SQL Server](#)
[SnapCenter Software 1.1 Data Protection Guide for Oracle Databases](#)

Preparing for the installation

You should be aware of several prerequisites before installing SnapCenter.

- Supported storage types
- Host requirements
- Supported storage systems, applications, and browsers
- Connection and port requirements
- SnapCenter licensing
- Type of database to use during installation
- Use of Microsoft Network Load Balancing and Application Request Routing features

You might benefit from using a SnapCenter installation worksheet.

Related concepts

[SnapCenter repository identification](#) on page 22

[Network Load Balancing and Application Request Routing options](#) on page 22

[Minimum vCenter privileges required for SnapCenter RDM operations](#) on page 66

Related references

[Host requirements](#) on page 16

[Storage system, application, and browser support](#) on page 18

[Connection and port requirements](#) on page 19

[SnapCenter licensing](#) on page 20

[SnapCenter installation worksheet](#) on page 24

Storage types supported by SnapCenter Plug-in for Microsoft SQL Server

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

| Machine | Storage type | Provision using | Support notes |
|-----------------|--|---|--|
| Physical server | FC-connected LUNs | SnapCenter graphical user interface (GUI) or PowerShell cmdlets | See note on provisioning support.* |
| | iSCSI-connected LUNs | SnapCenter GUI or PowerShell cmdlets | See note on provisioning support.* |
| | SMB3 (CIFS) shares residing on a Storage Virtual Machine (SVM) | SnapCenter GUI or PowerShell cmdlets | Support for provisioning only.* You cannot use SnapCenter to back up databases on SMB3 shares. |

| Machine | Storage type | Provision using | Support notes |
|------------|--|---------------------------------------|--|
| 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 | SnapCenter GUI or PowerShell cmdlets | See note on provisioning support.* |
| | Virtual Machine File Systems (VMFS) on VMFS or NFS datastores | VMware vSphere or 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 | SnapCenter GUI 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 Channel Switch | SnapCenter GUI or PowerShell cmdlets | You must use Hyper-V Manager to provision Virtual FC (vFC) LUNs connected by a virtual Fibre Channel Switch. |
| | iSCSI LUNs connected directly to the guest system by the iSCSI initiator | SnapCenter GUI or PowerShell cmdlets | See note on provisioning support.* |
| | A guest system connected to SMB3 shares residing on an SVM | SnapCenter GUI or PowerShell cmdlets | Support for provisioning only.* You cannot use SnapCenter to back up databases on SMB shares. |
| | Note: Hyper-V pass through disks and backing up databases on VHD(x) that are provisioned on NetApp storage are not supported. | | |

*SnapCenter provisioning support is available only on Windows 2012 or 2012 R2. Support for data protection operations (not provisioning support) is available on Windows Server 2008 R2 SP1.

Storage types supported by SnapCenter Plug-in for Oracle Database

SnapCenter supports a wide range of storage types on both physical and virtual machines. You must verify the support for your storage type before installing the SnapCenter Plug-ins Package for Linux.

Provisioning using SnapCenter is not supported for SnapCenter Plug-ins Package for Linux.

| Machine | Storage type | Support notes |
|-----------------|--|---|
| Physical server | FC-connected LUNs | |
| | iSCSI-connected LUNs | |
| | NFS-connected volumes | |
| VMware ESX | RDM LUNs connected by an FC or iSCSI HBA | You must register Virtual Storage Console (VSC) with SnapCenter before you use SnapCenter to back up databases on RDM LUNs. |
| | iSCSI LUNs connected directly to the guest system by the iSCSI initiator | |
| | VMDKs on VMFS or NFS datastores | You must register VSC with SnapCenter before you use SnapCenter to back up databases on VMDKs. |
| | NFS volumes connected directly to the guest system | |

Host requirements

Before you begin the SnapCenter installation, you should be familiar with the installation package space requirements and some basic host system requirements.

Domain requirements

The SnapCenter Server must be installed on a server in the same domain as the Microsoft SQL database hosts or on servers in trusted domains.

After SnapCenter Server is installed, you must not change the domain in which the SnapCenter host is located. If you remove SnapCenter Server from the domain it was in when SnapCenter Server was installed and then try to uninstall SnapCenter Server, the uninstall operation fails.

Note: Data protection using SnapCenter requires a two-way trust relationship between the SnapCenter Server domain and the SQL server domain. The SnapCenter Server domain and the SQL server domain must have a trust relationship between the two domains using the Microsoft Active Directory Domains and Trusts snap-in. While domain trusts, multidomain forests, and cross-domain trusts are supported, cross-forest domains are not.

See Microsoft documentation about Active Directory Domains and Trusts at <https://technet.microsoft.com/en-us/library/cc770299.aspx>.

For installation, you must have domain user rights with local administrator credentials.

Installation package space requirements

After installation, SnapCenter components require the following space:

| Requirements | Space needed |
|---|---|
| SnapCenter with SQL Server Express | 600 MB (depends on data stored in SQL Server Express) |
| SnapCenter without SQL Server Express | 200 MB |
| SnapCenter Plug-ins Package for Windows | 200 MB |

| Requirements | Space needed |
|---------------------------------------|--------------|
| SnapCenter Plug-ins Package for Linux | 100 MB |

SnapCenter Server host system sizing requirements

The SnapCenter host requires the following:

- Minimum RAM: 8 GB
- Minimum CPU: 4 CPUs
- Minimum SnapCenter repository sizing requirements: 10 GB

Plug-in host system requirements

If you are installing the SnapCenter Plug-ins Package for Linux, the Linux host requires the following:

- Minimum RAM: 4 GB
- Minimum space to store logs: 5 GB

If you are installing the SnapCenter Plug-ins Package for Windows, the Windows host requires a minimum of 4 GB RAM.

Supported operating systems

All supported Windows operating systems are 64-bit only.

Ensure that you enable the Windows update feature so that the latest updates or hotfixes are installed automatically on your system.

| Component | Supported host systems |
|---|--|
| SnapCenter Server | <ul style="list-style-type: none"> • Windows Server 2012 DCE • Windows Server 2012 R2 DCE • Windows Server 2012 SE • Windows Server 2012 R2 SE |
| SnapCenter Plug-ins Package for Windows | <ul style="list-style-type: none"> • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 SP1 (host provisioning operations not supported; support for data protection operations only) |
| SnapCenter Plug-ins Package for Linux | <ul style="list-style-type: none"> • Red Hat Enterprise Linux (RHEL) 6.6, 6.7, 7.0, and 7.1 • Oracle Linux 6.6, 6.7, 7.0, and 7.1 If you are using Oracle database on LVM in Oracle Linux or RHEL 6.6 or 7.0 operating systems, install the latest version of Logical Volume Management (LVM). • SUSE Linux Enterprise Server (SLES) 11 SP3 |

Required Microsoft Windows operating system updates

Microsoft has identified an HTTP security vulnerability in their Windows operating systems that requires the installation of KB3042553-x64.

<https://support.microsoft.com/en-us/kb/3042553>

Additional requirements for hosts that SnapCenter Server manages

For hosts with Windows Server 2008 R2 SP1, the installation for SnapCenter Plug-in for Microsoft Windows does not include some required components. You must ensure that the following requirements are installed on the host, or manually install them:

- .NET 4.5.2
- WMF 4.0
- PowerShell 4.0

Storage system, application, and browser support

It is essential that you check the Interoperability Matrix on the NetApp Support Site for all the latest interoperability information. It is helpful to understand the basic storage system, application, and browser support before you begin your installation.

The following information shows the currently supported configurations. For the latest information, see the Interoperability Matrix.

Supported clustered Data ONTAP versions

SnapCenter requires clustered Data ONTAP 8.2.2 and later.

Supported SQL Server versions

| SnapCenter Server repository | Plug-in for SQL Server data protection jobs |
|--|---|
| <ul style="list-style-type: none"> • SQL Server 2014 • SQL Server 2012 SP2 | <ul style="list-style-type: none"> • SQL Server 2014 SP1 • SQL Server 2012 SP2 • SQL Server 2008 R2 SP3 • SQL Server 2008 SP4 |

Supported SQL Express version

The SnapCenter executable includes SQL Server 2012 Express. In addition, SnapCenter supports SQL Express 2008R2 and 2014.

Supported Oracle Database versions

The supported Oracle Database versions are Oracle 11g (11.2.0.4) and Oracle 12c (12.1.0.2).

VSC for VMware vSphere requirements

SnapCenter 1.1 requires Virtual Storage Console 6.2 for VMware vSphere in the following environments:

- Your host is running in a virtual machine, and you plan to use SnapCenter to back up SQL or Oracle databases on VMDKs or RDMs.

Note: You do not need to register VSC with SnapCenter if you are using either Plug-in for SQL Server and your SQL Server environment used an iSCSI initiator or Plug-in for Oracle and your Oracle environment uses NFS or an iSCSI initiator.

- You are a VSC user with storage systems running clustered Data ONTAP 8.2.2 or later, and you want to use SnapCenter features when performing backup and restore operations.

Note: Specific versions of VSC support specific versions of SnapCenter. For example, VSC 6.2 for VMware vSphere does not maintain backward compatibility with SnapCenter 1.0. When setting up your environment, you should always check the Interoperability Matrix to verify that you are installing compatible versions of VSC and SnapCenter.

You cannot install VSC using SnapCenter. The VSC documentation contains instructions for installing VSC, and the Interoperability Matrix contains information about VSC requirements.

Supported browsers

- Chrome version 43 or later
- Internet Explorer 10.0 and 11.0 or later
 - Only default-level security is supported. Making changes to Internet Explorer security settings results in significant browser display issues.
 - Internet Explorer compatibility view must be disabled.

Related information

[NetApp Interoperability Matrix Tool](#)

[NetApp Documentation: Virtual Storage Console for VMware vSphere](#)

Connection and port requirements

Connections and ports must meet minimum requirements before you can install SnapCenter.

SnapCenter uses the following default ports; you can select a custom port when you install:

| Type of port | Default port |
|---|--|
| SnapCenter HTTPS port | 8146 (HTTPS) as in the URL <code>https://server:8146</code> You can configure this port during the SnapCenter installation process. |
| SMCore HTTP communication port | 8145 (HTTP), bidirectional You can modify this port number when you install the plug-in. |
| SnapCenter Plug-ins Package for Windows port | 8145 (HTTP), bidirectional You can modify this port number when you install the plug-in. |
| SnapCenter Plug-ins Package for Linux port | 8145 (HTTPS), bidirectional You can modify this port number when you install the plug-in. |
| Virtual Storage Console for VMware vSphere port | 8146 (HTTPS), bidirectional You can modify this port number when you install the plug-in. |

Consider the following requirements:

- Firewalls, proxies, or other network devices should not interfere with connections.

- If you specify a custom port when you install, you must add a firewall rule on the plug-in host for that port for the SnapCenter plug-in loader (SPL).

You cannot modify the port number after you install. To change a port number after installation, you must uninstall and install again.

SnapCenter licensing

SnapCenter requires plug-in package licenses and several storage system licenses to enable SnapCenter operations. The SnapCenter and plug-in licenses are available in two licensing models: *per-host licensing*, in which the license resides on each host, and *per-storage system licensing*, in which the license resides on the storage system.

Licenses from previous versions of SnapManager and SnapDrive products are accepted.

| License | Description | Where required |
|--|---|---|
| SnapCenter Plug-in for Microsoft SQL Server (per host) | A host-side license for a specific SQL Server host. Licenses are required only for SQL Server production hosts on which the SnapCenter plug-in is installed and for the optional verification server. No SnapCenter plug-in license is required for the storage system. | On the SnapCenter application host. A SnapCenter license is not required on source (primary) and destination (secondary) storage systems when using per-server licensing. |
| SnapCenter Plug-in for Microsoft SQL Server (per storage system) | A storage-side license that supports any number of SQL Server hosts. Required only if you are not using a per-server license on the SQL host. Trial licenses are available for per-storage system licensing only. | On source and destination storage systems. |
| SnapCenter Plug-in for Microsoft Windows (per host) | A license that enables you to execute the Plug-in for Windows on any Windows host system. | You can execute SnapCenter Plug-in for Microsoft Windows host-side operations when you have one of the following license configurations: <ul style="list-style-type: none"> • Per-host license • Storage system license |
| SnapCenter Plug-in for Microsoft Windows (per storage system) | A license that enables you to execute Plug-in for Windows operations only on a storage system. | On source and destination storage systems. |
| SnapCenter Plug-in for Oracle Database (per host) | A host-side license for a specific Oracle Database host. Licenses are required only for database hosts on which the Plug-in for Oracle is installed. No Plug-in for Oracle license is required for the storage system. | On the SnapCenter application host. A SnapCenter license is not required on source (primary) and destination (secondary) storage systems when using per-server licensing. |

| License | Description | Where required |
|---|---|---|
| SnapCenter Plug-in for Oracle Database (per storage system) | A storage-side license that supports any number of database hosts. Required only if you are not using a per-server license on the database host. | On source and destination storage systems. |
| SnapCenter Plug-in for UNIX (per host) | A license that enables you to execute the Plug-in for UNIX on Linux host system. | You can execute Plug-in for UNIX host-side operations when you have one of the following license configurations: <ul style="list-style-type: none"> • Per-host license • Storage system license |
| SnapCenter Plug-in for UNIX (per storage system) | A license that enables you to execute Plug-in for UNIX operations only on a storage system. | On source and destination storage systems. |
| SnapRestore | A required license that enables SnapCenter to restore and verify backup sets. | On source storage systems. Required on SnapVault destination systems to perform remote verification and to restore from a backup. Required on SnapMirror destination systems to perform remote verification. |
| FlexClone | A required license for cloning databases. Not required for restore and verification operations. | On primary and secondary storage systems. Required on SnapVault destination systems when creating clones from secondary vault backup. Required on SnapMirror destination systems when creating clones from secondary SnapMirror backup. |
| SnapMirror | An optional license for mirroring backup sets to a destination storage system. | On source and destination storage systems. |
| SnapVault | An optional license for archiving backup sets to a destination storage system. | On source and destination storage systems. |
| SnapManager for Virtual Infrastructure (SMVI) | A required license if you are using Virtual Storage Console for VMware vSphere and SnapCenter. | On source and destination storage systems. |

| License | Description | Where required |
|-----------|--|--|
| Protocols | <p>The following licenses are required:</p> <ul style="list-style-type: none"> • For LUNs, the iSCSI or FC license • For SMB shares, the CIFS license • For NFS-type VMDKs, the NFS license • For VMFS-type VMDKs, the iSCSI or FC license | On source storage systems. Required on SnapMirror destination systems to serve data if a source volume is unavailable. |

SnapCenter repository identification

The SnapCenter repository, sometimes referred to as the *NSM database*, stores information and metadata for every aspect of SnapCenter. When you install SnapCenter, you can choose either your existing dedicated SQL Server database or a SQL Server Express database (an existing version or one installed during the SnapCenter installation). You should understand your database needs before installing SnapCenter. After you identify the SnapCenter repository, you cannot change to another repository without first uninstalling SnapCenter.

- If you are using SnapCenter in a production environment, you should use SQL Server as the SnapCenter repository, configured with SQL Failover Cluster Instance (FCI) to provide high availability.
- If you want to use SnapCenter in a proof-of-concept or nonproduction environment, you can use SQL Server Express, which is packaged with SnapCenter. You must install it only on the SnapCenter Server. SQL Server Express is supported only on the host on which the SnapCenter Server is installed.

The SnapCenter repository stores information and metadata about the following general areas:

- Backup, clone, restore, and verification metadata
- Reporting, job, and event information
- Host and plug-in information
- Role, user, and permission details
- Storage system connection information

The SQL Server cannot be installed on an SMB share.

SnapCenter can back up its own repository using its repository management features.

Network Load Balancing and Application Request Routing options

Network Load Balancing (NLB) and Application Request Routing (ARR) are Microsoft features that together provide a unified high-availability and load-balancing configuration. When you install SnapCenter, you have the option to configure NLB and ARR. You should understand these options in advance of installation. To use NLB and ARR in SnapCenter, you must choose the option during installation; you cannot configure this later manually.

If you are using SnapCenter in a production environment and plan to deploy the user interface over multiple SnapCenter server hosts, you should configure SnapCenter with both ARR and NLB.

To better understand the NLB high-availability capabilities, see the following Microsoft documentation:

- [Network Load Balancing](#)

To better understand ARR, see the following Microsoft documentation:

- [Application Request Routing Version 2 Overview](#)
- [Application Request Routing download](#)
- [Deployment Recommendations for Application Request Routing](#)

SnapCenter requires a SQL Server (not SQL Express) database for all NLB deployments. You must use the same SQL Server database from all NLB nodes.

When implementing NLB in a SnapCenter environment, your network adapter and NLB cluster must have the same IP setting and Dynamic Host Configuration Protocol (DHCP) must be disabled on the network adapter. To configure NLB, you must have a dedicated IP address (virtual IP) that will be exposed from all NLB nodes. For example, if you select IPv4 virtual IP, all adapters on all nodes designated for NLB must support IPv4 format. The same applies for IPv6: all adapters and cluster IP must have IPv6 support. Additionally, when you add an SVM to an NLB configuration, each node in the NLB configuration must resolve to the same name or FQDN.

When SnapCenter is installed on a cluster that uses the Microsoft Distributed Transaction Coordinator (MS DTC) service, you must add a firewall exception for the service. If a firewall exception for MS DTC is not added on NLB cluster nodes, dataset creation and host removal operations fail.

For details about viewing NLB and ARR status in SnapCenter, see SnapCenter administration documentation.

Related information

[SnapCenter Software 1.1 Administration Guide](#)

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.

If you are using SnapCenter with ARR, each plug-in host must be able to communicate with SnapCenter using the Network Load Balancing (NLB) IP address.

If you do not see the SnapCenter UI when you browse to `https://NLB IP Address:8146` in Internet Explorer (IE), you must add the NLB IP address as a trusted site in IE on each plug-in host, **or** you must disable IE Enhanced Security on each plug-in host.

[NetApp KB Article 2025082: SnapCenter in an HA configuration with Application Request Routing enabled.](#)

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:

- [Microsoft Web Farm Framework 2.x](#)
- [Application Request Routing Version 2 Overview](#)
- [Application Request Routing download](#)
- [Deployment Recommendations for Application Request Routing](#)

SnapCenter installation worksheet

As you prepare to install SnapCenter, you can simplify the installation process by collecting the required information in advance.

| Required information | Your value |
|-----------------------------------|--|
| Application Request Routing (ARR) | You must decide whether you want to enable and install ARR. |
| Network Load Balancing (NLB) | <p>If you want to enable NLB, you must know whether you want to create a NLB cluster or join an existing one.</p> <p>If you want to create a NLB cluster, obtain the following information:</p> <ul style="list-style-type: none"> • Cluster name: • Cluster primary IP: • Interface name: <p>If you want to join an existing NLB cluster, obtain the following information:</p> <ul style="list-style-type: none"> • NLB node IP: • Interface name: <p>You can preconfigure NLB before installing SnapCenter.</p> |
| Credentials | <p>You must know the credentials that you want to use to log in to SnapCenter as the administrator. You need a domain user with local administrator permissions:</p> <ul style="list-style-type: none"> • Account (Domain\User): • Password: <p>If you have entered a certificate in this system's Personal store, you must also enter its friendly name to secure the SnapCenter web site. If you omit the Certificate Friendly Name, a self-signed certificate is used:</p> <ul style="list-style-type: none"> • Certificate Friendly Name: |
| Ports | <ul style="list-style-type: none"> • SnapCenter HTTPS port: 8146 (default) • SMCORE HTTP communication port: 8145 (default) <p>For additional details, see connection and port requirements.</p> |

| Required information | Your value |
|----------------------|---|
| SQL Server database | <p>You must provide a SQL Server database to store SnapCenter data by using an existing SQL Server or SQL Server Express (an existing version or one installed during the SnapCenter installation):</p> <ul style="list-style-type: none"> • SQL Server database: |
| SQL Server settings | <p>If you are using SQL Server, you must specify the following SQL Server settings:</p> <ul style="list-style-type: none"> • Database server: Specify “server\instance” or “server” if the instance is the default. • Authentication mode: • User name: • Password: |

Related references

[Connection and port requirements](#) on page 19

Installing SnapCenter and the plug-in packages

You must follow this order when installing SnapCenter and the plug-in packages: install SnapCenter, log in, perform configuration tasks, and then add the hosts and deploy plug-in packages, and, if needed, register Virtual Storage Console for VMware vSphere with SnapCenter.

The SnapCenter installation and configuration requires multiple tasks in a specific order.

You can perform several installation and configuration procedures by using PowerShell cmdlets. For details, use the SnapCenter cmdlet help or see the cmdlet reference information.

Steps

- 1. [Installing the SnapCenter Server](#) on page 27**
After you have completed the installation prerequisites and filled in the SnapCenter installation worksheet, you can use the InstallShield wizard to install the SnapCenter Server.
- 2. [Logging in to SnapCenter](#) on page 28**
Through SnapCenter role-based access control, users or groups are assigned roles and resources. When you log in to the SnapCenter graphical user interface, you log in with an Active Directory account.
- 3. [Configuring role-based access control for SnapCenter users](#) on page 28**
SnapCenter role-based access control enables you to delegate control of SnapCenter resources to different users or groups of users. You can create and modify roles, and add resource access to users at any time, but when you are setting up SnapCenter for the first time, you should at least add Active Directory users to roles, and then add resource access to users.
- 4. [Setting up SVM connections](#) on page 34**
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 access to clustered Data ONTAP storage.
- 5. [Setting up Run As credentials](#) on page 36**
To execute jobs on a specific database instance, you must set up Run As credentials with the correct authentication method. Run As account credentials authenticate users so they can perform SnapCenter operations, including Windows scheduling and Linux account access.
- 6. [Installing plug-in packages](#) on page 38**
You must register hosts with SnapCenter and install the plug-in packages on the managed host by using the SnapCenter graphical user interface (GUI) or PowerShell cmdlet.
- 7. [Registering VSC for VMware vSphere with SnapCenter](#) on page 49**
Registering Virtual Storage Console for VMware vSphere with SnapCenter adds the VSC host to SnapCenter and enables SnapCenter to communicate with VMware vSphere. You can use either the SnapCenter Add Host wizard or the VSC GUI to register VSC with SnapCenter. You can register multiple instances of VSC with a single instance of SnapCenter.
- 8. [Configuring the host log directory and verification server for SQL Server](#) on page 51**
After you install SnapCenter plug-in packages, you should configure the host log directory before you perform your first backup job. The host log directory is the location that you specify to store the transaction log backup files (.trb files) that enable you to perform up-to-the-minute restore operations. You might also want to configure a verification server so that you can perform backup or clone verification jobs.

Related information

[SnapCenter Software 1.1 Windows Cmdlet Reference Guide](#)
[SnapCenter Software 1.1 Linux Command Reference Guide](#)

Installing the SnapCenter Server

After you have completed the installation prerequisites and filled in the SnapCenter installation worksheet, you can use the InstallShield wizard to install the SnapCenter Server.

Before you begin

- You must have completed filling the installation worksheet.
- You must have installed Microsoft SQL Server 2008 R2 or later or Microsoft SQL Express Server to create the SnapCenter repository database.
- Your SnapCenter host system must be up to date with Windows updates with no pending system restarts.
- You must have enabled Windows installer debugging.
See the Microsoft web site for information about enabling and disabling Windows Installer logging.
- The SnapCenter Server must be installed on a server that is part of a domain.
- A two-way trust relationship between the SnapCenter Server domain and the plug-in domain using the Microsoft Active Directory Domains and Trusts snap-in must have been established. While domain trusts, multidomain forests, and cross-domain trusts are supported, cross-forest domains are not supported.
See Microsoft documentation about Active Directory Domains and Trusts at <https://technet.microsoft.com/en-us/library/cc770299.aspx>.
- You must have added the account that you want to use to install the SnapCenter Server to the administrator group of the remote SQL server database (SnapCenter repository).

Steps

1. Download the SnapCenter Server installation package from the NetApp Support Site at <mysupport.netapp.com>.
2. Install the SnapCenter Server by performing one of the following methods:
 - Double-click the downloaded .exe file to launch the SnapCenter Server installer. Proceed through the wizard by entering the information that you gathered in the SnapCenter installation worksheet.
 - From a Windows command prompt on the local host, change to the directory where you downloaded the installer and run the .exe file.
If you encounter installation issues, run the installation using a command prompt and generate a log file:
snappcenterversion.exe /debuglogDirPath\LogFileName
The debuglog parameter generates a log file that checks the installation against SnapCenter prerequisites.
If necessary, you can find additional troubleshooting information in the log file for the Plug-in for Windows package. Log files for the package are listed (oldest first) in the %Temp% folder.

Related references

[SnapCenter installation worksheet](#) on page 24

Logging in to SnapCenter

Through SnapCenter role-based access control, users or groups are assigned roles and resources. When you log in to the SnapCenter graphical user interface, you log in with an Active Directory account.

About this task

The SnapCenter graphical user interface (GUI) 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, which you can copy if you want to log in from a remote system.

The default GUI 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 GUI, you can use either PowerShell cmdlets to script configuration, backup, restore, verification, and clone operations for Microsoft SQL databases or use the SnapCenter command line interface (CLI), `sccli`, to script configuration, backup, restore, verification, mount, unmount, and clone operations for Oracle database. For details, see the SnapCenter cmdlet or SnapCenter CLI documentation.

Steps

1. Launch SnapCenter 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. Choose which user you want to log in as:

| 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. |
| Log in as a SnapCenter user | Enter your user credentials: <i>Domain\UserName</i> |

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

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

Related information

[SnapCenter Software 1.1 Windows Cmdlet Reference Guide](#)

[SnapCenter Software 1.1 Linux Command Reference Guide](#)

Configuring role-based access control for SnapCenter users

SnapCenter role-based access control enables you to delegate control of SnapCenter resources to different users or groups of users. You can create and modify roles, and add resource access to users

at any time, but when you are setting up SnapCenter for the first time, you should at least add Active Directory users to roles, and then add resource access to users.

Note that user accounts are not created using SnapCenter, but are created in Active Directory in the operating system or database.

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.

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 the permissions of the SnapCenterAdmin role.

You can assign RBAC permissions to users and groups within the same forest and to users belonging to different forests. You cannot assign RBAC permissions to users belonging to nested groups across forests.

Authentication

Users are required to provide authentication during login, through the graphical user interface (GUI) 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 credentials to ensure that authorized SnapCenter users also have application-level permissions.

For example, if you want to perform Snapshot copy and data protection operations in a SQL Server environment, you must set Run As credentials with the proper Windows or SQL credentials. The SnapCenter Server authenticates the credentials set using either method.

Similarly, if you want to perform data protection operations on an Oracle database and if the operating system (OS) authentication is disabled in the database host, you must set Run As credentials with the Oracle database or Oracle ASM credentials. The SnapCenter Server authenticates the credentials set using one of these methods depending on the operation being performed.

Clustered Data ONTAP permissions

You should ensure that you have vsadmin account permissions.

If you are configuring SnapCenter with Virtual Storage Console, you must create a Virtual Storage Console user.

Related information

[NetApp Documentation: Virtual Storage Console for VMware vSphere](#)

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 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
- Storage Connection
- Clone
- Provision (only for Microsoft SQL database)
- Dashboard
- Reports
- Restore
- Discovery

Plug-in privileges are required from the administrator for non-administrators to perform discovery operation.

- Plug-in Install\Uninstall

Note: When you enable Plug-in Installation permissions, you must also modify the Host permission to enable reads and updates.

- Migration
- Mount (only for Oracle database)
- Unmount (only for Oracle database)

Pre-defined roles and permissions

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

SnapCenter includes the following pre-defined roles:

- SnapCenter Admin role
- Backup and Clone Viewer role

- App Backup and Clone Admin role
- Infrastructure Admin role

When you add a user to a role, you must assign either the StorageConnection permission to enable Storage Virtual Machine (SVM) communication, or assign an SVM to the user to enable permission to use the SVM. The StorageConnection permission enables users to create SVMs.

For example, a user with the SnapCenter Admin role can create SVMs and assign them to a user with the App Backup and Clone Admin role, which by default does not have permission to create or edit SVMs. Without an SVM connection, users cannot complete any backup, clone, or restore operations.

SnapCenter Admin role

The SnapCenter Admin role has all permissions enabled. You cannot modify the permissions for this role. You can add users and groups to the role or remove them.

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 |
| Mount | Yes | Not applicable | Not applicable | Not applicable | Not applicable |

| Permissions | Enabled | Create | Read | Update | Delete |
|-------------|---------|----------------|----------------|----------------|----------------|
| Unmount | Yes | 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 permissions 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 |
| 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 |
| Mount | Yes | Not applicable | Not applicable | Not applicable | Not applicable |
| Unmount | Yes | 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 |
| 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 |
| Mount | No | Not applicable | Not applicable | Not applicable | Not applicable |
| Unmount | 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 can add users or groups to a role. The role determines the options that SnapCenter users can access.

Before you begin

You must have logged in as the SnapCenterAdmin role.

About this task

SnapCenter includes several 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. In the **Users/Groups** page, specify the domain to which the user belongs.
6. In the **user or group name** field, enter a user or group name and click **Add**.
Repeat to add additional users or groups to the selected role.
7. Click **Next** to view the summary, and then click **Finish**.

Assigning resources to users

Setting up role-based access control (RBAC) for users is a two-step process. After you add a user or group 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.

About this task

You can add resources to users even if the user is not part of a role. This helps you add users; however, you must add the user to a role at some point to take advantage of role-based access control efficiencies.

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**.
5. Provide the domain name to which the resource belongs.
6. Choose whether you want to assign resources to a user or a group.
7. Enter the user or group name and click **Add**.
If you are not sure about the name, use a more advanced search by clicking the **Search users or group** heading, typing a partial name, and clicking **Search**.
8. Repeat this procedure until each user or group has all the required resources.
9. Click **OK** to save your changes.

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 access to clustered Data ONTAP storage.

Before you begin

If you are installing SnapCenter Plug-in for Microsoft Windows on a SQL Server host, that installation must have completed before you add an SVM.

About this task

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

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Storage Virtual Machine** page, click **New** to display the **New SVM Connection** wizard.

3. Provide the following SVM information:

| For this field... | Do this... |
|--------------------|--|
| SVM | Enter the SVM name or IP address. Note: SVM names, not including the domain name, must be 15 characters or less. To create SVMs with names with more than 15 characters, you can use the <code>Add-SmStorageConnection</code> PowerShell cmdlet. |
| User name/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. |
| Port | Enter the port that the storage system accepts. The defaults typically work. |
| Timeout | Enter the time in seconds that should elapse before communication attempts are halted. The default value is 60 seconds. |

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

4. Optional: If the SVM has multiple management interfaces, select the **Preferred IP address** check box and enter the preferred IP address for SVM connections.

Note: If you have more than one iSCSI or FCP session configured per SVM connected to the host, then use the host device for multipathing rather than using the native device. For more information see [Clustered Data ONTAP 8.3 Cluster Management Using OnCommand System Manager](#). While performing a restore, clone, mount, or backup verification operation, if the storage system and the host has iSCSI and FCP configured together, then FCP will be preferred.

5. Click **OK**.

Setting up Run As credentials

To execute jobs on a specific database instance, you must set up Run As credentials with the correct authentication method. Run As account credentials authenticate users so they can perform SnapCenter operations, including Windows scheduling and Linux account access.

Authentication methods for your Run As credential

The Run As credential uses different authentication methods depending on the application or environment. The Run As credentials authenticate users so they can perform SnapCenter operations.

Windows authentication

The Windows authentication method 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 credential to perform tasks such as adding hosts, installing plug-in packages, and scheduling jobs.

SQL Server authentication

The SQL authentication method authenticates against a SQL Server instance. This means that a SQL Server instance must be discovered in SnapCenter. Therefore, before adding a SQL Run As credential, you must add a host, install plug-in packages, and refresh resources. You need SQL Server authentication for performing operations such as scheduling or discovering resources.

Linux authentication

The Linux authentication method authenticates against a Linux host. You need Linux authentication during the initial step of adding the Linux host and installing the SnapCenter Plug-ins Package for Linux remotely from the SnapCenter GUI.

Oracle database authentication

The Oracle database authentication method authenticates against an Oracle database. You need an Oracle database authentication to perform operations on the Oracle database if the operating system (OS) authentication is disabled on the database host. Therefore, before adding a Oracle database Run As credential, you must create an Oracle user in the Oracle database with sysdba privileges.

Oracle ASM authentication

The Oracle ASM authentication method authenticates against an Oracle Automatic Storage Management (ASM) instance. If you are required to access the Oracle ASM instance and if the operating system (OS) authentication is disabled on the database host, you need an Oracle ASM authentication. Therefore, before adding an Oracle ASM Run As credential, you must create an Oracle user in the ASM instance.

Related tasks

[Setting up your Run As credentials](#) on page 37

Setting up your Run As credentials

The Run As credentials enable you to set up the authorizations that are used to authenticate users for any SnapCenter operations.

About this task

Although you can create the Run As account for Linux after deploying hosts and installing plug-ins, you should create Run As accounts before deploying hosts and installing any plug-ins.

If you are on the Windows host, you should set up the Run As account with administrator privileges, including administrator rights on the remote host because some actions require administrator privileges. If you are on the Linux host, you must set up the Run As account for the root user or for a user with root user privileges.

If you are deploying SnapCenter Plug-in for Microsoft SQL Server, you must set up a Run As credential for a user with SQL Server sysadmin permissions.

Steps

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

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

| For this field... | Do this... |
|-------------------|--------------------------------------|
| Run As name | Enter a name for the Run As account. |

| For this field... | Do this... |
|---------------------|---|
| User name/Password | Enter the user name and password used for authentication. |
| Authentication Mode | Select the authentication mode that you want to use. If you have selected the SQL authentication mode, you must also specify the SQL server instance and the host where the SQL instance is located. |

5. Click **OK**.

Related concepts

[Authentication methods for your Run As credential](#) on page 36

Installing plug-in packages

You must register hosts with SnapCenter and install the plug-in packages on the managed host by using the SnapCenter graphical user interface (GUI) or PowerShell cmdlet.

Available plug-in types

Different plug-in types are available for you to install, depending on your data protection goals.

SnapCenter Plug-ins Package for Windows

This installation package includes the following plug-ins:

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.

To install SnapCenter Plug-in for Microsoft SQL Server, you must have a user with sysadmin permissions on the SQL Server.

SnapCenter Plug-in for Microsoft Windows

The Plug-in for Windows provides storage provisioning for Windows hosts, 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.

You should install the Plug-in for Windows if your data protection goals include these operations:

- Using the Plug-in for SQL Server
The Plug-in for Windows is required to support most Plug-in for SQL Server operations.
- Performing host provisioning operations

Note: Provisioning operations are not supported on Windows 2008 R2 servers.

You do not have to be a domain administrator to install Plug-in for Windows on a host in a Windows failover cluster. You can install it as a domain user with local administrative rights.

SnapCenter Plug-ins Package for Linux

This installation package includes the following plug-ins:

SnapCenter Plug-in for Oracle Database

The Plug-in for Oracle is a host-side component of the NetApp integrated storage solution offering application-aware backup management of Oracle databases. With the Plug-in for Oracle installed on your Oracle host, SnapCenter automates backup, restore, recovery, verify, mount, unmount, and clone operations.

If you want to perform data protection operations on Oracle databases that are on VMDKs or RDMs, you must register VSC with SnapCenter, using either the SnapCenter Add Hosts wizard or the VSC Configure SnapCenter Server dialog box.

Note: You can use the Plug-in for Oracle to manage Oracle databases for SAP as well. However, SAP BR*Tools integration is not supported.

SnapCenter Plug-in for UNIX

The Plug-in for UNIX handles the underlying host storage stack and enables you to perform backup, restore, clone, mount, and unmount operations on Oracle databases that are running on a Linux host, by working in conjunction with the Plug-in for Oracle. The Plug-in for UNIX supports the Network File System (NFS) and storage area network (SAN) protocols on a storage system that is running clustered Data ONTAP.

SnapCenter plug-in deployment checklist

Several steps are required to deploy and configure the SnapCenter plug-ins packages. While the procedures for performing these tasks include more detail, you might find it helpful to use the abbreviated checklists.

- [Actions you should complete before deploying plug-in packages](#) on page 39
- [Actions you should complete while deploying plug-in packages](#) on page 40
- [Actions you should complete to configure a backup for a newly added host](#) on page 41

If one person is deploying the plug-in packages and performing all tasks, that person user should be assigned to the SnapCenter Admin role to perform all these actions. However, if you want others to perform various tasks, you must assign roles to other users. When you are setting up SnapCenter for the first time, you must at least add users to roles, and then add resource access to those users.

For details, see information about configuring role-based access control (RBAC).

Actions you should complete before deploying plug-in packages

| Actions | Steps | Notes | Complete? |
|------------------------------|--|--|-----------|
| Add Storage Virtual Machines | <ol style="list-style-type: none"> 1. Select Settings > Storage Virtual Machines. 2. Click New to add an SVM. | Add a connection for each SVM that backs storage for the host. | |

| Actions | Steps | Notes | Complete? |
|------------------------|--|--|-----------|
| Add Run As credentials | <ol style="list-style-type: none"> 1. Select Settings > Run As Credentials. 2. Click New to add a Run As account. | <p>If you are planning to use SQL authentication, instead of completing this step now, complete this step later, after you add a host and discover resources.</p> <p>If you are deploying SnapCenter Plug-in for Microsoft SQL Server, and you are installing using Windows authentication, the user must have sysadmin permissions on the SQL Server.</p> | |

Actions you should complete while deploying plug-in packages

Before you complete actions in this checklist, you must complete the actions required before deploying SnapCenter.

| Actions | Steps | Notes | Complete? |
|---|---|---|-----------|
| Add host and deploy plug-in packages | <ol style="list-style-type: none"> 1. Select Hosts > Managed Hosts > Add. 2. Complete the wizard to initiate plug-in package deployment. | <p>You add a host or a cluster that has many nodes and deploy the plug-in package one host at a time. To deploy multiple hosts using a PowerShell cmdlet, see information about installing multiple hosts.</p> <p>If you add a cluster (Windows Server Failover Clustering (WSFC) or Oracle real application clusters (RAC)), SnapCenter performs a remote installation on all cluster nodes.</p> | |
| Monitor plug-in package installation status | <ol style="list-style-type: none"> 1. Select Monitor > Jobs. 2. Wait until the plug-in package installation job finishes, which might take several minutes. | <p>After this process finishes, the plug-in package is installed on the remote host.</p> | |

| Actions | Steps | Notes | Complete? |
|--|---|---|-----------|
| Refresh resources | <ol style="list-style-type: none"> 1. Select Inventory. 2. Select the application (Oracle Database or SQL Server) that you want to manage. 3. Select the newly added host from the Host drop-down box and click Refresh Resources. 4. If you are using SnapCenter Plug-in for Microsoft SQL Server, change the Resource Type to review instances, databases, and more on the host. | This validates that the plug-in packages were deployed successfully and that SnapCenter can detect resources. | |
| Configure the plug-in log directory and verification server (only if you are using Plug-in for SQL Server) | <ol style="list-style-type: none"> 1. Select Hosts > Managed Hosts. 2. Select the host and click Configure Plug-in. 3. Complete the wizard. | The log directory shows only NetApp LUNs. | |

Actions you should complete to configure a backup for a newly added host

| Actions | Steps | Notes | Complete? |
|-------------------------|---|---------------------------------|-----------|
| Create a backup policy | <ol style="list-style-type: none"> 1. Select Policies > New. 2. Click Backup and complete the wizard. | You can use an existing policy. | |
| Create a backup dataset | <ol style="list-style-type: none"> 1. Select Datasets > New > Backup Dataset. 2. Complete the wizard, selecting databases from the newly added host. | | |

| Actions | Steps | Notes | Complete? |
|-------------------------|---|-------|-----------|
| Backup now | <ol style="list-style-type: none"> 1. Select Datasets. 2. Select the newly added dataset and click Backup Now. 3. Select a policy from the drop-down list and click Backup. | | |
| Monitor backup progress | <ol style="list-style-type: none"> 1. Select Monitor > Jobs. 2. Monitor the backup job for completion. | | |

Related tasks

[Installing plug-ins on multiple remote hosts](#) on page 46

Adding hosts and installing plug-in packages on remote hosts

You must use the Add Host wizard to add the host and then install the plug-ins packages. The plug-ins are automatically installed on the remote hosts. You can add a host and install plug-in packages either for an individual host or a cluster.

Before you begin

- You must have set up the Run As credentials for Windows or Linux host, depending on the type of the host you want to add.
- For Windows hosts:
 - You must have a domain user with local administrator privileges with local login permissions on the remote host.
 - You must have uninstalled SnapDrive for Windows 7.x or earlier if you are installing SnapCenter Plug-in for Microsoft Windows.
 - If you are installing SnapCenter Plug-in for Microsoft SQL Server, you must have a user with sysadmin permissions on the SQL Server. SnapCenter Plug-in for Microsoft SQL Server uses Microsoft VDI Framework, which requires sysadmin access. [Microsoft Support Article 2926557: SQL Server VDI backup and restore operations require Sysadmin privileges](#)
 - If SnapManager for Microsoft SQL Server is installed, you must have stopped or disabled the service and schedules. If you plan to migrate backup or clone jobs into SnapCenter, do not uninstall SnapManager for Microsoft SQL Server.
 - Data protection using SnapCenter requires a two-way trust relationship between the SnapCenter Server domain and the plug-in domain using the Microsoft Active Directory Domains and Trusts snap-in. Although domain trusts, multidomain forests, and cross-domain trusts are supported, cross-forest domains are not. <https://technet.microsoft.com/en-us/library/cc770299.aspx>

- For Linux hosts:
 - You must have enabled the password-based SSH connection for the root user.
 - You must have installed Java 1.7 or Java 1.8 on your Linux host.
- For VSC:
 - You must have installed Virtual Storage Console for VMware vSphere if you want to use SnapCenter to add a vSphere host for managing applications residing on virtual machine disk file (VMDK) or raw device mapping (RDM) configurations.

About this task

You can choose one of the following types of hosts:

- Windows host
- Linux host
- vSphere host
When you add a vSphere host using the Add Host wizard, SnapCenter automatically registers with VSC. If you used the VSC GUI to perform the VSC-SnapCenter registration for this host, you do not need to use the Add Host wizard.
For information about using the VSC GUI, see the VSC documentation.

If you install plug-ins on a cluster (WSFC or Oracle RAC), they are installed on all members of the cluster.

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

Note: You need not register VSC with SnapCenter if you are using Plug-in for SQL Server (and your SQL Server environment uses an iSCSI initiator) or Plug-in for Oracle (and your Oracle environment uses NFS or an iSCSI initiator). If you do not register VSC with SnapCenter, a message appears in the SnapCenter Hosts view that indicates you should configure the hypervisor. For these conditions, you do not need to configure the hypervisor.

Steps

1. In the left navigation pane, click **Hosts**.
2. Verify that the **Managed Hosts** tab is selected.
3. Click **Add**:

4. In the **Host** page, do the following:

| For this field... | Do this... |
|-------------------|---|
| Host name | <p>Enter the fully qualified domain name (FQDN) or the IP address of the host.</p> <p>SnapCenter depends on the proper configuration of the DNS. You should always use fully qualified domain name (FQDN) as the host name.</p> <p>You can enter one of the following:</p> <ul style="list-style-type: none"> • IP address or FQDN of the stand-alone host • IP address or FQDN of the Windows Server Failover Clustering (WSFC) • IP address or FQDN of any node in the Oracle Real Application Clusters (RAC) environment Node VIP or scan IP is not supported. <p>If you are adding a host using SnapCenter and it is part of a subdomain, you must provide the FQDN.</p> |

| For this field... | Do this... |
|------------------------------|--|
| Type | <p>Select Windows, Linux, or vSphere.</p> <p>If you select vSphere, SnapCenter automatically registers the host with VSC. Doing so enables the SnapCenter Server to communicate with VMware vSphere.</p> <p>Note: Unless you are using an iSCSI initiator for SnapCenter Plug-in for Microsoft SQL Server or using an iSCSI initiator or an NFS environment for SnapCenter Plug-in for Oracle Database, you must register SnapCenter with VSC when you are running the plug-in in a VMware vSphere environment and want to use SQL databases on VMDKs or RDM LUNs. If you do not register SnapCenter with VSC, you cannot restore your backups. If you use the Add Host wizard to register SnapCenter with VSC, you do <i>not</i> need to repeat the registration using the VSC GUI.</p> |
| Run As name | <p>Select the Run As credential that you created.</p> <p>The credential must have administrative rights on the remote host. For details, see information about creating a Run As credential.</p> |
| Port | <p>Either retain the default port number or enter the port number.</p> <p>The default port number is 8145.</p> |
| Add all hosts in the cluster | <p>Select this to add all the cluster nodes in an Oracle RAC or WSFC.</p> |

5. In the **Discover plug-ins** page, review the plug-in packages on the host.

For new deployments, no plug-in packages are listed.

6. In the **Plug-in** page, select the plug-in package and enter the plug-in ports, license type, and installation path.

Ensure that you choose the correct license type, either per storage system or per host (license required on each managed host). Otherwise, data protection operations might not succeed.

For SnapCenter Plug-ins Package for Windows, the default path is `C:\Program Files\NetApp\SnapCenter`. However, if you want, you can customize the default path.

For SnapCenter Plug-ins Package for Linux, the default path is `/opt/NetApp/snapcenter`.

Note: You cannot change the path for Linux.

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

After you finish

After you finish, you should monitor the installation progress.

If you are installing SnapCenter Plug-ins Package for Linux, installation specific log files are available at `/var/opt/snapcenter/logs`.

Note: If the firewall is enabled on the Linux host, the SnapCenter Plug-ins Package for Linux is installed successfully but in the Managed Hosts page, the host status is displayed as down and the overall status is displayed as stopped.

Related concepts

[Configuring role-based access control for SnapCenter users](#) on page 28

SnapCenter role-based access control enables you to delegate control of SnapCenter resources to different users or groups of users. You can create and modify roles, and add resource access to users at any time, but when you are setting up SnapCenter for the first time, you should at least add Active Directory users to roles, and then add resource access to users.

Related tasks

[Setting up your Run As credentials](#) on page 37

[Registering VSC for VMware vSphere with SnapCenter](#) on page 49

Registering Virtual Storage Console for VMware vSphere with SnapCenter adds the VSC host to SnapCenter and enables SnapCenter to communicate with VMware vSphere. You can use either the SnapCenter Add Host wizard or the VSC GUI to register VSC with SnapCenter. You can register multiple instances of VSC with a single instance of SnapCenter.

Related references

[SnapCenter licensing](#) on page 20

Installing plug-ins on multiple remote hosts

If you want to install SnapCenter plug-in packages on multiple hosts at one time, you can do so by using the `Install-SmHostPackage` cmdlet.

Before you begin

You must have logged in to SnapCenter as a domain user with local administrator rights on each host on which you want to install plug-ins.

Steps

1. Launch PowerShell.
2. From the SnapCenter Server command prompt, enter the following and enter your credentials:
`Open-SMConnection`
3. From the command prompt, enter the following:

`Install-SmHostPackage`

Example

```
Install-SmHostPackage -HostNames @"(\"10.231.72.165\", \"10.231.72.99\")
-ApplicationCode SCO -ApplicationLicenseType Storage
-FilesystemCode SCU -FilesystemLicenseType Storage -RunAsName
SmoPlugin
```

The following prompts are displayed:

hostnames

Specifies the list of hosts on which you want to install the available plug-ins. If possible, use the fully qualified domain name (FQDN) because SnapCenter relies on the proper DNS configuration. You must separate host names with a comma. Using quotations is recommended.

ApplicationCode

Specifies the code for one or more plug-ins in the packages that you want to install. The following values are valid:

- MSFT_SQL
- SCO

FilesystemCode

Specifies the code for one or more plug-in packages that you want to install. The following values are valid:

- SCW
- SCU

4. Enter your Run As account name for remote installation.

Monitoring SnapCenter plug-in package installation status

You can monitor the progress of SnapCenter plug-in package installation by using the Jobs page. You might want to check the progress of installation to determine when it is complete or if there is an issue.

About this task

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

-  In progress
-  Completed successfully
-  Failed
-  Completed with warnings or could not start due to warnings
-  Queued

Steps

1. In the left navigation pane, click **Monitor**.
2. In the top navigation bar, click **Jobs**.
3. In the **Jobs** page, to filter the list so that only plug-in installation operations are listed, do the following:
 - a. Click **Filter**.
 - b. Specify the start and end date.
 - c. From the Type drop-down menu, select **Plug-in installation**.
 - d. From the Status drop-down menu, select the installation status.
 - e. Click .
4. Select the installation job and click **Details** to view the job details.
5. In the **Job Details** page, click **View logs**.

Managing the SnapCenter Plug-in Loader service

The SnapCenter Plug-in Loader (SPL) service loads the plug-in package for Linux to interact with the SnapCenter Server.

About this task

After installing the SnapCenter Plug-ins Package for Linux, the SnapCenter Plug-in Loader service is started automatically. However, you can also manually start, stop, and find the status of the services. When you restart the Linux host, the SPL service is started automatically.

The `spl.properties` located at `/var/opt/snapcenter/spl/etc/` contains the following parameters and the default values are assigned to these parameters.

| Parameter name | Description |
|----------------------------|--|
| SPL_PORT | Displays the port number on which SnapCenter Plug-in Loader (SPL) service is running. You can add the value if the default value is missing. Note: You should not change value after installing the plug-ins for Linux. |
| SPL_PROTOCOL | Displays the protocol supported by SPL. Only https protocol is supported. You can add the value if the default value is missing. |
| SPL_KEYSTORE_PATH | Displays the absolute path of the keystore file. |
| SPL_KEYSTORE_PASS | Displays the password of the keystore file. You can change this value only if you change the password or create a new keystore file. |
| SNAPCENTER_SERVER_HOST | Displays IP address or host name of the SnapCenter Server. |
| SNAPCENTER_SERVER_PROTOCOL | Displays the protocol supported by SnapCenter Server. Only https protocol is supported. You can add the value if the default value is missing. |
| SNAPCENTER_SERVER_PORT | Displays the port number on which SnapCenter Server is running. |
| LOG_LEVEL | Displays the log levels supported. The possible values are INFO, DEBUG, TRACE, ERROR, FATAL, and WARN. |

If any of these parameters are not assigned the default value and you want to assign the value or you want to change the value, you can modify the `spl.properties` file. You can also verify the `spl.properties` file and edit it to troubleshoot any issues related to the values assigned to the parameters. After you modify the `spl.properties` file, you must restart the SPL service.

Step

1. Do one of the following:
 - Start the SPL service by entering the following command:

```
/opt/NetApp/snapcenter/spl/bin/spl start
```

You must always start the service as a root user.

- Stop the SPL service by entering the following command:

```
/opt/NetApp/snapcenter/spl/bin/spl stop
```

Note: You can use `-force` option with the stop command to terminate the SPL service. Stopping the SPL forcefully should be used with caution as forcefully stopping the service also terminates the existing operations.

- Find the status of the SPL service by entering the following command:

```
/opt/NetApp/snapcenter/spl/bin/spl status
```

Identifying available resources

Resources are the databases and similar components that are maintained by the plug-ins you have installed. You can add those resources to datasets to perform data protection jobs, but first you must identify available resources. Identifying resources also verifies that the installation of plug-in packages is completed successfully.

Steps

1. In the left navigation pane, click **Inventory**.
2. Select the application (Oracle Database or SQL Server) that you want to manage.
3. To filter the resources, select the host from the **Host** drop-down menu.
If you have installed SnapCenter Plug-ins Package for Windows, you can also filter the resources based on the resource types such as database, instance, and availability group.
4. Click **Refresh Resources**.
The new resources added to the SnapCenter inventory are displayed.

Registering VSC for VMware vSphere with SnapCenter

Registering Virtual Storage Console for VMware vSphere with SnapCenter adds the VSC host to SnapCenter and enables SnapCenter to communicate with VMware vSphere. You can use either the SnapCenter Add Host wizard or the VSC GUI to register VSC with SnapCenter. You can register multiple instances of VSC with a single instance of SnapCenter.

Before you begin

- You must have VSC installed and running.
You cannot install VSC using SnapCenter. The VSC documentation contains instructions for installing and configuring VSC.
- **Recommended:** You should have installed VSC and SnapCenter on separate hosts, not the same host.
- Your storage systems must be running clustered Data ONTAP 8.2.2 or later.
- For SnapCenter 1.1, you must be running Virtual Storage Console 6.2 for VMware vSphere.

About this task

There are two situations where you should register VSC with SnapCenter:

- You are running the Windows and Linux plug-in packages in a VMware vSphere environment and need to back up SQL databases or Oracle databases on VMDKs or RDMs.

SnapCenter manages these backups; however, it needs to be able to communicate with VSC to access vSphere. If you do not register these products, you cannot perform backup, restore, and clone operations of your applications on VMware vSphere.

- You are a VSC user and your storage systems are running clustered Data ONTAP 8.2.2 or later. When you register VSC with SnapCenter, VSC automatically uses SnapCenter to perform the backup, clone, and restore operations for those storage systems. The SnapCenter integration enables VSC to perform operations such as policy-based backups; however, the fact that VSC is using SnapCenter is transparent to you.
If you used VSC to create policies and datasets and registered VSC with SnapCenter, you can view these policies and datasets in SnapCenter. You can also view VSC-based backup, clone, and restore operations in the SnapCenter Jobs view.
If you do not register VSC with SnapCenter, VSC uses its backup and restore features.

Note: You do not need to register VSC with SnapCenter if you are using either the Plug-in for SQL Server (and your SQL Server environment uses an iSCSI initiator) or Plug-in for Oracle (and your Oracle environment uses NFS or an iSCSI initiator). In this case, SnapCenter displays a "configure hypervisor" message, which is appropriate.

You can register SnapCenter with VSC from the SnapCenter GUI or the VSC GUI. You only need to register once; you do **not** need to register from each GUI.

When the AutoSupport option is enabled in the **VSC Configuration > Backup and Recovery Configuration** option, backup jobs created before enabling AutoSupport at the VSC level are not logged in AutoSupport. However, backup jobs created after enabling AutoSupport at the VSC level are logged.

Step

1. Register VSC with SnapCenter.

| If you are the ... | Do this... |
|--------------------------|--|
| SnapCenter administrator | <ol style="list-style-type: none"> From the SnapCenter GUI, start the Add Host wizard. Select the Host type vSphere from the drop-down list. Complete the rest of the steps in the Add Host wizard. <p>When you add a vSphere host, SnapCenter automatically registers with VSC.</p> |
| VSC administrator | <ol style="list-style-type: none"> From the VSC GUI, select Configuration > Configure SnapCenter Server Complete the information in the Configure SnapCenter Server dialog box. <p>For details about using the VSC GUI to register VSC with SnapCenter, see the VSC documentation.</p> |

Related information

[NetApp Documentation: Virtual Storage Console for VMware vSphere](#)

Monitoring virtualization status in SnapCenter

If you have a virtualized environment, you might want to determine whether an application host is registered with Virtual Storage Console for VMware vSphere (VSC). If you want to back up SQL

databases or Oracle databases on VMDKs or RDMs, you must register VSC with SnapCenter. If you do not, you cannot restore your backups. Monitoring that status can help you plan.

Steps

1. From the left navigation pane, click **Hosts**.
2. On the **Managed Hosts** page, select a host, and then click **Details**.
3. In the **Host Details** window, note the information for Virtualization host configured state, which indicates whether an application host is registered with VSC:

Configured

The application host is set up on VSC to work with SnapCenter.

Not Configured

The application host is *not* set up on VSC to work with SnapCenter. This status is displayed even if you are connecting iSCSI directly into a VM, even though configuring with vSphere is not required.

Not Applicable

The application host is a physical or hypervisor host.

Related tasks

[Registering VSC for VMware vSphere with SnapCenter](#) on page 49

Registering Virtual Storage Console for VMware vSphere with SnapCenter adds the VSC host to SnapCenter and enables SnapCenter to communicate with VMware vSphere. You can use either the SnapCenter Add Host wizard or the VSC GUI to register VSC with SnapCenter. You can register multiple instances of VSC with a single instance of SnapCenter.

Configuring the host log directory and verification server for SQL Server

After you install SnapCenter plug-in packages, you should configure the host log directory before you perform your first backup job. The host log directory is the location that you specify to store the transaction log backup files (.trb files) that enable you to perform up-to-the-minute restore operations. You might also want to configure a verification server so that you can perform backup or clone verification jobs.

Before you begin

You must refresh resources from the Inventory page before configuring the plug-in. Refreshing the resources discovers SQL instances and databases.

You can use the Configure Plug-in wizard to specify the location of the host log directory and a verification server. SnapCenter detects NetApp volumes that can host the log directory.

You can set up one log directory per host. You cannot set up a log directory per instance.

If your environment includes a Windows cluster, you must configure a host log for each host. For an SQL cluster, you must set a host log for the Failover Cluster Instance (FCI).

About this task

Steps

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

2. From the **Managed Hosts** page, select a host, and click **Configure Plug-in** to open the **Configure SnapCenter Plug-in** wizard.
3. If the application host is running on a virtual machine (VM), and SnapCenter has not been registered with Virtual Storage Console for VMware vSphere, and the **Host Setup** page appears, choose one of the following options:
 - **I am using a VM in a VMDK or RDM environment**
Choose this option if you plan to use SnapCenter to back up SQL databases on VMDKs or RDMs. A message appears, indicating that you must register SnapCenter with Virtual Storage Console for VMware vSphere before continuing.

Important: If you do not register, you will not be able to restore your backups. You can use either the SnapCenter Add Host wizard or the VSC GUI to perform the registration.
 - **I am using a VM with iSCSI direct attached disks only**
Choose this option if your VM uses an iSCSI initiator. You can proceed to the next page with your existing host configuration.
4. On the **Configure host log directory** page, click **Browse** and complete the following steps:

Configure the log backup directory for newcluqat.smsqlqa2.gdl.englab.netapp.com

Configure host log directory

| | | |
|--------------------|--|--------------|
| Host | cluqat3.smsqlqa2.gdl.englab.netapp.com | |
| Host log directory | dedicated disk directory path | Apply Browse |

Configure FCI instance log directory

| | | |
|-------------------|--------|--------------|
| FCI instance | newnet | |
| FCI log directory | L:\ | Apply Browse |

Only NetApp LUNs (drives) are listed for selection. SnapCenter backs up and replicates the host log directory.

- a. Select the drive letter or mount point on the host where the host log will be stored.
- b. Choose a subdirectory, if required.
- c. Click **Next**.

Configure verification server

Set up SQL Server instance on newcluqat.smsqlqa2.gdl.englab.netapp.com as a verification server

Choose SQL Server instance

| | |
|---------------------|--|
| Host | <input type="text" value="newcluqat.smsqlqa2.gdl.englab.net"/> |
| SQL Server instance | <input type="text" value="newnet"/> |

Update credential for newnet

| | |
|--------------------|-------------------------------------|
| Run As | <input type="text" value="Choose"/> |
| Maximum job counts | <input type="text" value="1"/> |

Choose mount point

Auto assign mount point

Auto assign volume mount point under path

5. If you want to configure a verification server, on the **Verification Server** page, select the **Setup a SQL Server instance** check box, and complete the following steps:
 - a. Select the SQL host and instance that you want to use for verification.
 - b. Select the appropriate **Run As** credential to perform the operation.
 - c. Choose the maximum job count and mount point options.
 - d. Click **Apply**, and then click **Next**.
6. Review your settings, and click **Finish**.

Related tasks

Identifying available resources on page 49

Provisioning storage on Windows hosts

You can use SnapCenter to assign NetApp storage to Windows Server 2012 and 2012 R2 hosts. Provisioning Windows hosts with SnapCenter ensures that the backups you create are application consistent. You must have installed and configured the SnapCenter Plug-ins Package for Windows.

SnapCenter does not support provisioning of Windows Server 2008 R2 hosts. Only SnapCenter data protection operations are supported. For detailed information about this limitation, see the *SnapCenter Software Release Notes*.

[SnapCenter Software 1.1 Release Notes](#)

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

Configuring LUN storage

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

LUNs are the basic unit of storage in a SAN configuration. The Windows host sees LUNs on your system as virtual disks. For more information, see the [Clustered Data ONTAP 8.3 SAN Configuration Guide](#).

Establishing an iSCSI session

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

Before you begin

- You must have defined the storage system node as an iSCSI target.
[Data ONTAP DSM 4.1 For Windows MPIO Installation and Administration Guide](#)
- You must have started the iSCSI service on the storage system.
[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.

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

Steps

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

5. Click **Establish Session**.

The Establish Session wizard is displayed.

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

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

7. When you are satisfied with your entries, click **Connect**.

SnapCenter establishes the iSCSI session.

8. Repeat this procedure to establish a session for each target.

Disconnecting an iSCSI session

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

Steps

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

Creating and managing igroups

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

Creating an igroup

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

Steps

1. In the 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 storage system.

Renaming an igroup

You can use SnapCenter to rename an existing igroup.

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 list of available SVMs, and then select the SVM for the igroup you want to rename.
4. In the list of igroups for the SVM, select the igroup you want to rename and click **Rename**.
5. In the **Rename igroup** dialog box, enter the new name for the igroup and click **Rename**.

Modifying an igroup

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

Steps

1. In the SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Igroup**.
3. In the list of igroups, select an igroup and click **Add Initiator to igroup**.
4. Select a host.
5. Select the initiators and click **OK**.

Deleting an igroup

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

Steps

1. In the 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:

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

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. Select the host from the **Host** drop-down box.
The disks are listed.

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 SnapCenter. For more information, see the [Clustered Data ONTAP 8.3 Logical Storage Management Guide](#).
- **Note:** You cannot create a LUN on a SnapCenter-created clone volume unless the clone has already been split.
- You must have started the FC or iSCSI service on the storage system.
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 54.

About this task

- You cannot connect a LUN to more than one host unless the LUN is shared by hosts in a Windows Server failover cluster.

- If a LUN is shared by hosts in a Windows Server failover cluster that uses CSV (Cluster Shared Volumes), you must create the disk on the host that owns the cluster group.
- The SnapCenter Plug-ins Package for Windows must be installed only on the host on which you are creating the disk.

Steps

1. In the SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Disks**.
3. Select the host from the **Host** drop-down box.
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 | Click Browse to select the full path of the folder containing the LUN. |
| LUN name | Enter the name of the LUN. |
| Cluster size | Select the LUN block allocation size for the cluster. Cluster size depends upon the operating system and applications. |
| LUN label | Optionally, enter descriptive text for the LUN. |

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

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

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

| Property | Description |
|------------------------|---|
| Auto assign | Allow SnapCenter to automatically assign a volume mount point based on the system drive. For example, if your system drive is C:, auto assign creates a volume mount point under your C: drive (C:\scmnt\). Auto assign is not supported for shared disks. |
| Assign drive letter | Mount the disk to the drive you select in the adjoining drop-down list. |
| Use volume mount point | Mount the disk to the drive path you specify in the adjoining field. The root of the volume mount point must be owned by the host on which you are creating the disk. |

| Property | Description |
|--|---|
| 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. 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. MBR partitions might cause misalignment issues in Windows Server failover clusters. |

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

| In this field... | Do this... |
|-----------------------|---|
| Host | Double-click the cluster group name to display a drop-down list that shows the hosts that belong to the cluster and then select the host for the initiator. This field is displayed only if the LUN is shared by hosts in a Windows Server failover cluster. |
| Choose host initiator | Select FibreChannel or iSCSI and 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.

Related tasks

[Viewing the disks on a host](#) on page 57

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, SnapCenter automatically resizes the LUN to the size of the Snapshot copy.
After the restore operation, data added to the LUN after it was resized must be restored from a Snapshot copy made after it was resized.

Steps

1. In the SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Disks**.
3. Select the host from the **Host** drop-down box.
The disks are listed.
4. Select the disk you want to resize and click **Resize**.
5. In the **Resize Disk** dialog box, use the slider tool to specify the new size of the disk, or enter the new size in the **Size** field.
Note: If you enter the size manually, you need to click outside the **Size** field before the **Shrink** or **Expand** button is enabled appropriately. Also, you must click **MB**, **GB**, or **TB** to specify the unit of measurement.
6. When you are satisfied with your entries, click **Shrink** or **Expand**, as appropriate.
SnapCenter resizes the disk.

Related tasks

[Viewing the disks on a host](#) on page 57

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. Select the host from the **Host** drop-down box.
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 | Click Browse to select the full path of the folder containing the LUN. |
| LUN name | Enter the name of the LUN. |
| Cluster size | If the LUN is shared by hosts in a Windows cluster, select the size of the cluster. |
| LUN label | Optionally, enter descriptive text for the LUN. |

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

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

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

| Property | Description |
|--|--|
| Auto assign | Let SnapCenter automatically assign a volume mount point based on the system drive. For example, if your system drive is C :, the auto assign property creates a volume mount point under your C : drive (C : \scmnt\). The auto assign property is not supported for shared disks. |
| Assign drive letter | Mount the disk to the drive you select in the adjoining drop-down list. |
| Use volume mount point | Mount the disk to the drive path you specify in the adjoining field. The root of the volume mount point must be owned by the host on which you are creating the disk. |
| Do not assign drive letter or volume mount point | Choose this option if you prefer to mount the disk manually in Windows. |

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

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

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

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

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

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

Related tasks

[Viewing the disks on a host](#) on page 57

Disconnecting a disk

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

Before you begin

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

About this task

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

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

Steps

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

Related tasks

[Viewing the disks on a host](#) on page 57

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. Select the host from the **Host** drop-down box.
The disks are listed.
4. Select the disk you want to delete, and then click **Delete**.
5. In the **Delete Disk** dialog box, click **OK**.
SnapCenter deletes the disk.

Related tasks

[Viewing the disks on a host](#) on page 57

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 SnapCenter to automate share configuration.

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

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

Creating an SMB share

You can use the SnapCenter Shares page to create an SMB3 share on a Storage Virtual Machine (SVM).

Steps

1. In the SnapCenter navigation pane, click **Hosts**.
2. On the **Hosts** page, click **Shares**.
3. Select the SVM from the **Storage Virtual Machine** drop-down box.
4. Click **New**.
The New Share dialog opens.
5. In the **New Share** dialog, define the share:

| In this field... | Do this... |
|------------------|---------------------------------------|
| Description | Enter descriptive text for the share. |

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

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

SnapCenter creates the SMB share on the SVM.

Deleting an SMB share

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

Steps

1. In the 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

- You must ensure that the space reclamation process has completed before performing a restore operation.
- If the LUN is shared by hosts in a Windows Server failover cluster, you must perform space reclamation on the host that owns the cluster group.
- For optimum storage performance, you should perform space reclamation as often as possible. You should ensure that the entire NTFS file system has been scanned.

- Space reclamation is time-consuming and CPU-intensive, so it is usually best to run the operation when storage system and Windows host usage is low.
- Space reclamation reclaims nearly all available space, but not 100 percent.
- You should not run disk defragmentation at the same time as you are performing space reclamation.
Doing so can slow the reclamation process.

Step

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

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

drive_path is the drive path mapped to the LUN.

Related information

[SnapCenter Software 1.1 Windows Cmdlet Reference Guide](#)

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 14.

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, and then add the disks to the virtual machines in the cluster.

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

Requirements for using FC RDM LUNs in a Microsoft cluster

The Plug-in for Windows provides support for Microsoft clusters using FC RDM LUNs on two different virtual machines that belong to two different ESX 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:

```
Open-SmConnection -SMSbaseUr1 https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME -  
RoleName "ROLE_NAME"
```

Where:

- *SNAPCENTER_SERVER_NAME* is the server name or IP address of the machine where SnapCenter is installed.
- *DOMAIN_NAME* is the domain (for example, `nextgen`).
- "*ROLE_NAME*" is the role name for the user assigned with the Admin role (for example, "Snap Admin"). Role name is required only if the user is a member of multiple roles. Typically, you do not need to specify this.

Provide the credentials you used to log in to the SnapCenter GUI.

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.

For detailed information about the Plug-in for Windows cmdlets, including syntax and examples, see the *SnapCenter Software Cmdlet Reference*.

[*SnapCenter Software 1.1 Windows Cmdlet Reference Guide*](#)

Preparing storage systems for SnapMirror and SnapVault replication

You can use a SnapCenter plug-in with Data ONTAP SnapMirror technology to create mirror copies of backup sets on another volume, and with Data ONTAP SnapVault technology to perform disk-to-disk backup replication for standards compliance and other governance-related purposes. Before you perform these tasks, you must configure a *data-protection relationship* between the source and destination volumes and *initialize* the relationship.

Note: If you are coming to SnapCenter from a NetApp SnapManager product and are satisfied with the data protection relationships you have configured, you can skip this section.

A data protection relationship replicates data on primary storage (the source volume) to secondary storage (the destination volume). When you initialize the relationship, Data ONTAP transfers the data blocks referenced on the source volume to the destination volume.

Note: SnapCenter does not support cascade relationships between SnapMirror and SnapVault volumes (**Primary > Mirror > Vault**). Use fanout relationships only (**Primary > Mirror, Primary > Vault**).

Understanding the differences between SnapMirror and SnapVault

SnapMirror is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. SnapVault is disk-to-disk backup replication technology, designed for standards compliance and other governance-related purposes.

These objectives account for the different balance each technology strikes between the goals of backup currency and backup retention:

- SnapMirror stores *only* the Snapshot copies that reside in primary storage, because, in the event of a disaster, you need to be able to fail over to the most recent version of primary data you know to be good.
Your organization, for example, might mirror hourly copies of production data over a ten-day span. As the failover use case implies, the equipment on the secondary system must be equivalent or nearly equivalent to the equipment on the primary system to serve data efficiently from mirrored storage.
- SnapVault, in contrast, stores Snapshot copies *whether or not* they currently reside in primary storage, because, in the event of an audit, access to historical data is likely to be as important as access to current data.
You might want to keep monthly Snapshot copies of your data over a 20-year span, for example, to comply with government accounting regulations for your business. Because there is no requirement to serve data from secondary storage, you can use slower, less expensive disks on the vault system.

The different weights that SnapMirror and SnapVault give to backup currency and backup retention ultimately derive from the limit of 255 Snapshot copies for each volume. While SnapMirror retains the most recent copies, SnapVault retains the copies made over the longest period of time.

Preparing storage systems for SnapMirror replication

Before you can use a SnapCenter plug-in to mirror Snapshot copies, you need to configure a *data-protection relationship* between the source and destination volumes, then initialize the relationship.

Upon initialization, SnapMirror makes a Snapshot copy of the source volume, then transfers the copy and all the data blocks that it references to the destination volume. It also transfers any other, less recent Snapshot copies on the source volume to the destination volume.

Before you begin

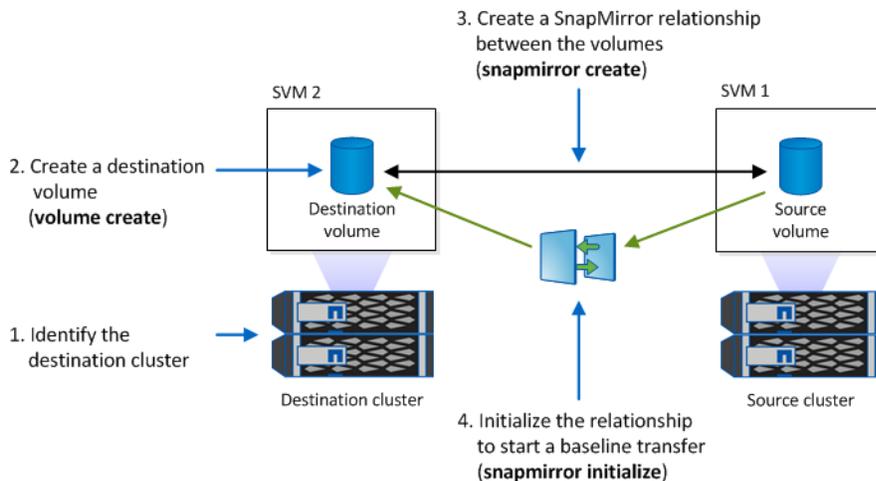
- You must have created the source and destination volumes in peered clusters with peered Storage Virtual Machines (SVMs).
For more information, see the *Clustered Data ONTAP 8.3 Cluster Peering Express Guide*.
- You must be a cluster administrator.
- For Snapshot copy verification on the destination volume, the source and destination Storage Virtual Machines (SVMs) must have a management LIF as well as a data LIF.
The management LIF must have the same DNS name as the SVM. Set the management LIF role to **data**, the protocol to **none**, and the firewall policy to **mgmt**.

About this task

You can use the Data ONTAP command-line interface (CLI) or OnCommand System Manager to create a SnapMirror relationship. The following procedure documents CLI usage.

Important: If you are storing database files and transaction logs on different volumes, you must create relationships between the source and destination volumes for the database files and between the source and destination volumes for the transaction logs.

The following illustration shows the procedure for initializing a SnapMirror relationship:



Steps

1. Identify the destination cluster.
2. On the destination cluster, use the `volume create` command with the `-type DP` option to create a SnapMirror destination volume that is either the same or greater in size than the source volume.

Important: The language setting of the destination volume must match the language setting of the source volume.

Example

The following command creates a 2 GB destination volume named `dstvolB` in SVM2 on the aggregate `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate node01_aggr -type DP
-size 2GB
```

3. On the destination SVM, use the `snapmirror create` command with the `-type DP` parameter to create a SnapMirror relationship.

The `DP` type defines the relationship as a SnapMirror relationship.

Example

The following command creates a SnapMirror relationship between the source volume `srcvolA` on SVM1 and the destination volume `dstvolB` on SVM2, and assigns the default SnapMirror policy `DPDefault`:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination-path SVM2:dstvolB
-type DP
```

Note: Do not define a mirror schedule for the SnapMirror relationship. The SnapCenter plug-in does that for you when you create a backup schedule.

If you do not want to use the default SnapMirror policy, you can invoke the `snapmirror policy create` command to define a SnapMirror policy.

4. Use the `snapmirror initialize` command to initialize the relationship.

The initialization process performs a *baseline transfer* to the destination volume. SnapMirror makes a Snapshot copy of the source volume, then transfers the copy and all the data blocks it references to the destination volume. It also transfers any other Snapshot copies on the source volume to the destination volume.

Example

The following command initializes the relationship between the source volume `srcvolA` on SVM1 and the destination volume `dstvolB` on SVM2:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Preparing storage systems for SnapVault replication

Before you can use a SnapCenter plug-in to perform disk-to-disk backup replication, you need to configure a *data-protection relationship* between the source and destination volumes, then initialize the relationship. On initialization, SnapVault makes a Snapshot copy of the source volume, then transfers the copy and all the data blocks it references to the destination volume.

Before you begin

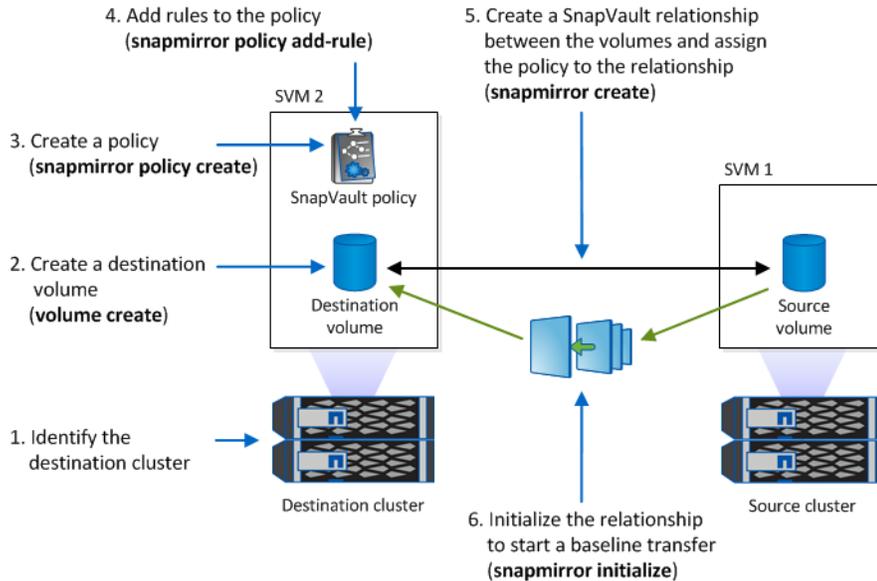
- You must have created the source and destination volumes in peered clusters with peered Storage Virtual Machines (SVMs).
For more information, see the [Clustered Data ONTAP 8.3 Cluster Peering Express Guide](#).
- You must be a cluster administrator.

About this task

You can use the Data ONTAP command-line interface (CLI) or OnCommand System Manager to create SnapVault relationships. The following procedure documents CLI usage.

Important: If you are storing database files and transaction logs on different volumes, you must create relationships between the source and destination volumes for the database files and between the source and destination volumes for the transaction logs.

The following illustration shows the procedure for initializing a SnapVault relationship:



Steps

1. Identify the destination cluster.
2. On the destination cluster, use the `volume create` command with the `-type DP` option to create a SnapVault destination volume that is the same size as or larger than the source volume.

Important: The language setting of the destination volume must match the language setting of the source volume.

Example

The following command creates a 2 GB destination volume named `dstvolB` in SVM2 on the aggregate `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate node01_aggr -type DP -size 2GB
```

3. On the destination SVM, use the `snapmirror policy create` command to create a SnapVault policy.

Example

The following command creates the SVM-wide policy `SVM1-vault`:

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-vault
```

Note: Do not define a cron schedule or Snapshot copy policy for the SnapVault relationship. The SnapCenter plug-in does that for you when you create a backup schedule.

4. Use the `snapmirror policy add-rule` command to add rules to the policy that define the following Snapshot copy labels and the retention policy for each label:
 - One Time
 - Hourly
 - Daily

- Weekly
- Monthly

Important: The labels are case-sensitive.

These are fixed labels for options displayed when you perform a backup. You select one of these options when you archive the backup. You must execute this command once for each of the rules you are adding.

Example

The following command adds a rule to the SVM1-vault policy that defines the “Daily” label and specifies that 30 Snapshot copies matching the label should be kept in the vault:

```
SVM2::> snapmirror policy add-rule -vserver SVM2 -policy SVM1-vault
-snapmirror-label Daily -keep 30
```

5. Use the `snapmirror create` command with the `-type XDP` parameter and the `-policy` parameter to create a SnapVault relationship and assign a vault policy.

The **XDP** type defines the relationship as a SnapVault relationship.

Example

The following command creates a SnapVault relationship between the source volume `srcvolA` on SVM1 and the destination volume `dstvolB` on SVM2, and assigns the policy `SVM1-vault`:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination-path SVM2:dstvolB
-type XDP -policy SVM1-vault
```

6. Use the `snapmirror initialize` command to initialize the relationship.

The initialization process performs a *baseline transfer* to the destination volume. SnapMirror makes a Snapshot copy of the source volume, then transfers the copy and all the data blocks it references to the destination volume.

Example

The following command initializes the relationship between the source volume `srcvolA` on SVM1 and the destination volume `dstvolB` on SVM2:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Upgrading SnapCenter and SnapCenter plug-in packages

Periodic SnapCenter plug-in package updates are available. Plug-in package updates are distributed with the SnapCenter installer. You can configure SnapCenter to automatically check for available updates. Then, you must install them.

Configuring SnapCenter to check for available updates

SnapCenter periodically communicates with the NetApp Support Site to notify you of available software updates. You can also create a schedule to specify the interval in which you want to receive information about available updates.

Steps

1. From the left navigation pane, click **Administration**.
2. Click **Software**.
The Available Software table displays the available plug-in packages, versions available, and their installation status.
3. Click **Check for updates** to see if any newer versions of plug-in packages are available.
4. Click **Schedule Updates** to create a schedule to specify the interval in which you want to receive information about available updates:
 - a. Select the interval in **Check for updates**.
 - b. Select the Run as credential and click **OK**.

Upgrading SnapCenter

To upgrade the SnapCenter Server, you must have the SnapCenter Server installation package on the server where SnapCenter is installed. You can download the installation package directly from the NetApp Support Site. If the server where SnapCenter is installed is in a secure environment, you can download the installation package in a non-secure environment, then copy it to the server in the secure environment.

Before you begin

If you are not using Network Load Balancing (NLB), you should place datasets or the hosts or both in maintenance mode prior to the upgrade so that scheduled backups do not occur and you avoid creating failed backups. If you are using NLB, you do not need to place datasets or the host in maintenance mode. If you are using NLB, you should have the same version of SnapCenter on all NLB nodes.

Steps

1. Download the SnapCenter upgrade package from the NetApp Support Site at mysupport.netapp.com.
2. Place the host in maintenance mode:
 - a. From the left navigation pane, click **Hosts**.

- b. Select the host and its plug-in, and then click **Suspend Schedule**.
3. Place datasets in maintenance mode:
 - a. From the left navigation pane, click **Datasets**.
 - b. Select the dataset, and then click **Maintenance**.
4. Launch the SnapCenter upgrade wizard and follow the instructions.

During the upgrade, you can complete the following tasks:

 - Enable the Application Request Routing (ARR) for SnapCenter.
 - Enable and configure Network Load Balancing (NLB) on the host by either creating a new NLB cluster or joining an existing NLB cluster.
 - Specify user credentials for the SnapCenter administrator.
 - Change SQL Server settings to use either Windows authentication or SQL authentication.
 - Start the upgrade process.
5. Click **Datasets > Production** to bring the datasets out of maintenance mode so that operations can resume.
6. Click **Hosts > Resume Schedule** to bring the host out of maintenance mode so that operations can resume.

Related concepts

[Network Load Balancing and Application Request Routing options](#) on page 22

Related information

[SnapCenter Software 1.1 Administration Guide](#)

Upgrading your plug-in packages

The plug-in packages are distributed as part of the SnapCenter upgrade.

About this task

This procedure places your host in maintenance mode, which prevents the host from running any scheduled jobs.

Steps

1. From the left navigation pane, click **Hosts**.
2. From the **Managed Hosts** page, select the host on which you want to upgrade a plug-in package.
3. From the **Information** section, select the plug-in package you want to upgrade, and then click **Suspend Schedule** to place the host for this plug-in in maintenance mode.
4. Select the host that contains the plug-in package you want to upgrade, and then click **Modify**.
5. Supply the information and then click **OK**.

After you finish

After the plug-in package is upgraded, bring the host out of maintenance mode by clicking **Resume Schedule**.

Uninstalling SnapCenter and the plug-in packages

You can remove hosts and their plug-in packages using the SnapCenter interface. There are several steps you must take in preparation for removing hosts. If you no longer wish to use SnapCenter to manage data protection jobs, you can uninstall SnapCenter using the Programs and Features Control Panel on the SnapCenter host system.

Preparing for plug-in uninstallation

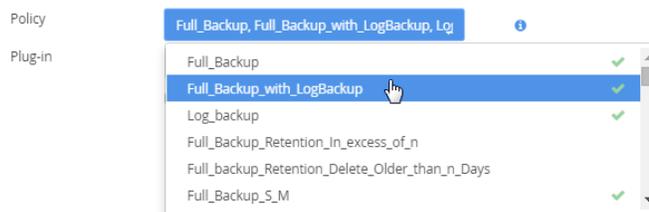
You must delete the datasets and policies that you created for a plug-in before you remove the plug-in.

Detaching policies from a dataset

Any time that you no longer want policies for a dataset, you can detach them.

Steps

1. In the left navigation pane, click **Datasets**.
2. Select the dataset and click **Modify**.
3. In the **Name** page of the **Modify Dataset** wizard, clear the check mark next to the names of the policies you want to detach:



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

Deleting datasets for SQL Server

You can delete a dataset if you no longer need it to perform different 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 that 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, click **Datasets**.
2. Select the dataset and click **Delete**.

3. To remove all backups, metadata, policies, and Snapshot copies associated with the dataset, select the **Delete backups and policies associated with this dataset** check box.
4. Click **OK**.

Deleting datasets for Oracle databases

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

About this task

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

Steps

1. In the left navigation pane, click **Datasets**.
2. Select the dataset and click **Delete**.
3. Select the **Delete backups and policies associated with this dataset** check box to remove all backups, metadata, policies, and Snapshot copies associated with the dataset.
4. Click **OK**.

Uninstalling the plug-in packages from a host using SnapCenter GUI

When you decide that you no longer require a particular plug-in package, you can uninstall it any time. Before you uninstall, you must be aware of several prerequisites and the dependencies between plug-ins.

Before you begin

- You must have removed the datasets for the plug-in package that you are uninstalling.
- You must have detached the policies associated with the datasets for the plug-in package that you are uninstalling.

About this task

- If you have removed a host from SnapCenter, all the plug-in packages installed on the host are removed.
- If you are using the user interface, you can remove plug-ins on a per-host basis only. If you want to uninstall a plug-in from multiple hosts, you must use the PowerShell cmdlet `Uninstall-SmPlugin`. However, if you want to uninstall the plug-in packages, you must use the PowerShell cmdlet `Uninstall-SmHostPackage`.

Note: Uninstalling the SnapCenter Plug-ins Package for Windows from a host on which the SnapCenter Server is installed will damage the SnapCenter Server installation. Do not uninstall the SnapCenter Plug-ins Package for Windows unless you are certain that you no longer require the SnapCenter Server.

Steps

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

2. From the **Managed Hosts** page, select the host from which you want to uninstall the plug-in.
3. Click **Remove**.

If the host is a member of a cluster, you can select **Include all the hosts of cluster** to remove all the hosts in the cluster.

4. Click **OK** to proceed.

After you finish

After you uninstall a plug-in, you must wait for 5 minutes before you reinstall the plug-in on that host. This time period is sufficient for SnapCenter GUI to refresh the status of the managed host. The installation fails if you immediately reinstall the plug-in.

If you are uninstalling SnapCenter Plug-ins Package for Linux, uninstallation-specific log files are available at: `/var/opt/snapcenter/logs`.

Uninstalling SnapCenter Plug-in for Microsoft SQL Server using SnapCenter GUI

When you decide that you no longer require SnapCenter Plug-in for Microsoft SQL Server, you can uninstall it at any time.

Before you begin

- You must have removed the datasets for the plug-in that you are uninstalling.
- You must have detached the policies associated with the datasets for the plug-in that you are uninstalling.

Steps

1. From the left navigation pane, click **Hosts**.
2. From the **Managed Hosts** page, select the host from which you want to uninstall the plug-in.
3. Click **Modify**.
4. Select **Remove plug-ins** and click **Next**.
5. Select **Microsoft SQL Server**.
6. Click **Finish**.

Uninstalling the plug-ins packages from multiple remote hosts

If you want to uninstall SnapCenter plug-ins packages from multiple hosts at one time, you can do so by using the `Uninstall-SmHostPackage` cmdlet.

Before you begin

You must have logged in to SnapCenter as a domain user with local administrator rights on each host on which you want to uninstall the plug-ins.

Steps

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

```
Open-SMConnection
```

3. From the command prompt, enter:

```
Uninstall-SmHostPackage
```

The following prompts are displayed:

hostnames

Specifies the list of hosts on which you want to uninstall the available plug-ins package.

plugincode

Specifies the plug-in code for one or more plug-ins that you want to uninstall. The valid values are SCO and MSFT_SQL. Omitting the plug-in code uninstalls the available plug-ins.

Uninstalling SnapCenter

You should uninstall SnapCenter using the Programs and Features Control Panel on your SnapCenter Server host system. Uninstalling SnapCenter removes the Network Load Balancing (NLB) cluster, the Application Request Routing server farm, and, if appropriate, the SnapCenter database.

About this task

The domain in which the SnapCenter host is located must remain unchanged. If you remove SnapCenter Server from the domain it was in when SnapCenter Server was installed and then try to uninstall SnapCenter Server, the uninstall operation fails.

Steps

1. On your SnapCenter host system, navigate to the **Control Panel**.
2. Make sure you are in the **Category** view.
3. Under **Programs**, click **Uninstall a program**.
Programs and Features opens.
4. Select NetApp SnapCenter Server and click **Uninstall**.
5. Select to remove the NLB cluster and the Application Request Routing server farm.
6. If you do not want to use this SnapCenter repository in with a newly installed SnapCenter Server, select to remove the SnapCenter repository.

After you finish

- Deleting the NLB cluster requires that you restart your SnapCenter Server host system. If you do not restart the host system, you might experience a failure if you attempt to reinstall SnapCenter Server.
- Some non-NetApp components installed by SnapCenter are not removed during uninstallation, including SQL Server Express and .NET Framework. If you want to remove these components, you must uninstall them manually.

If you want to uninstall SQL Express, first delete the SnapCenter Server repository, then uninstall SQL Express by selecting Microsoft SQL Server 2012 (64-bit).

Features enabled on your Windows host during installation

The SnapCenter Server installer enables the Windows features and roles on your Windows host during installation. These might be of interest for troubleshooting and host system maintenance purposes.

| Category | Feature |
|----------------------------------|--|
| Web Server | <ul style="list-style-type: none"> • Internet Information Services • World Wide Web Services • Common HTTP Features <ul style="list-style-type: none"> ◦ Default Document ◦ Directory Browsing ◦ HTTP Errors ◦ HTTP Redirection ◦ Static Content ◦ WebDAV Publishing • Health and Diagnostics <ul style="list-style-type: none"> ◦ Custom Logging ◦ HTTP Logging ◦ Logging Tools ◦ Request Monitor ◦ Tracing • Performance Features <ul style="list-style-type: none"> ◦ Static Content Compression • Security <ul style="list-style-type: none"> ◦ IP Security ◦ Basic Authentication ◦ Centralized SSL Certificate Support ◦ Client Certificate Mapping Authentication ◦ IIS Client Certificate Mapping Authentication ◦ IP and Domain Restrictions ◦ Request Filtering ◦ URL Authorization ◦ Windows Authentication • Application Development Features <ul style="list-style-type: none"> ◦ .NET Extensibility 4.5 ◦ Application Initialization ◦ ASP.NET 4.5 ◦ Server-Side Includes ◦ WebSocket Protocol • Management Tools <ul style="list-style-type: none"> ◦ IIS Management Console |
| IIS Management Scripts and Tools | <ul style="list-style-type: none"> • IIS Management Service • Web Management Tools |

| Category | Feature |
|------------------------------------|---|
| .NET Framework 4.5 Features | <ul style="list-style-type: none">• .NET Framework 4.5• ASP.NET 4.5• Windows Communication Foundation (WCF) HTTP Activation45<ul style="list-style-type: none">◦ TCP Activation◦ HTTP Activation◦ Message Queuing (MSMQ) Activation |
| Message Queuing | <ul style="list-style-type: none">• Message Queuing Services• Microsoft Message Queue (MSMQ) Server |
| Windows Process Activation Service | <ul style="list-style-type: none">• Process Model |
| Configuration APIs | All |

Installation troubleshooting

If you encounter unexpected behaviour or failure while performing the installation, you can use the installation log files to identify the cause and resolve the issue.

Enabling AutoSupport email notifications

You can enable AutoSupport email notifications on your storage system so that AutoSupport messages are sent to a specified storage system user. AutoSupport messages can alert you to issues such as failed backups.

Step

1. Enable AutoSupport email notifications from the storage system command line:

```
autosupport trigger modify -node nodename -autosupport-message  
client.app.info enable -noteto enable
```

HTTP error 503. The service is unavailable.

Description

Launching SnapCenter from a browser or opening a connection from the CLI might fail after installation if Windows Process Activation Service (WAS) is not enabled.

Corrective action

Verify in Windows Server Manager that Windows Process Activation Service is enabled.

Unable to display SnapCenter web login page on local host

Description

When using Internet Explorer with Protected Mode enabled, the SnapCenter login page does not display when logging in to the local SnapCenter host as a user from another trusted domain.

Corrective action

Disable Protected Mode in Internet Explorer.

SnapCenter Plug-ins Package for Linux installation fails due to incorrect Java version

Description

The SnapCenter Plug-ins Package for Linux installation might fail if the Java Virtual Machine (JVM) is not found or the JVM version required for installation of SnapCenter Plug-ins Package for Linux is not available.

Corrective action

1. Add java executable path to the `PATH` environmental variable.
2. Verify the java version by running the following command:

```
#ssh root@host_name java -version
```

SnapCenter Plug-ins Package for Linux installation fails due to improper uninstallation

Description

The SnapCenter Plug-ins Package for Linux installation might fail if the uninstallation was not performed properly.

Error message

An instance of SnapCenter plug-in for Oracle is already installed

Corrective action

1. List the RPM packages:

```
rpm -qa | grep netapp-snapcenter-plugin
```

2. Delete the RPM packages:

```
rpm -e netapp-snapcenter-plugin-loader netapp-snapcenter-plugin-oracle  
netapp-snapcenter-plugin-unix
```

3. Remove the `/var/.com.zerog.registry.xml` file manually.

SnapCenter Server is unable to communicate with the host

Description

After installing the plug-in remotely, SnapCenter Server is unable to communicate with the host.

Corrective action

1. Verify whether the SnapCenter plug-in loader is started on the correct port with proper host name.
2. Configure the FQDN of the host if the SnapCenter plug-in loader has been started with localhost: 8145.
3. Run the `hostname -f` command to find the FQDN of the host.
4. Restart the SnapCenter plug-in loader service after changing the host name.

SnapCenter plug-in loader fails with an error

Description

SnapCenter plug-in loader fails with an error.

Error message

Error retrieving current directory.

Corrective action

- You must ensure that you have not deleted any directory where the plug-in is operating on.
- You must increase the memory space allotted to the Java Virtual Machine.

Where to go next

You can find more information about different features and release-specific information for SnapCenter in the documentation available on the NetApp Support Site at mysupport.netapp.com.

- [SnapCenter Software 1.1 Release Notes](#)
Provides important information about this release of Snap Creator Server and the SnapCenter plug-in packages, including fixed issues, known issues, cautions, limitations, and any documentation updates or corrections.
- [SnapCenter Software 1.1 SnapManager Migration Guide](#)
Describes how to migrate data from previous versions of SnapDrive and SnapManager to your SnapCenter environment.
- [SnapCenter Software 1.1 Getting Started Guide](#)
Provides simple information about how to get started with SnapCenter, regardless of which plug-in packages you have installed, and outlines a simple workflow to help you perform your first backup operation.
- [SnapCenter Software 1.1 Administration Guide](#)
Provides information about how to administer SnapCenter, provision Windows hosts with storage, configure and maintain role-based access control (RBAC), and use the centralized reporting options.
- [SnapCenter Software 1.1 Data Protection Guide for Microsoft SQL Server](#)
Describes how to use SnapCenter to perform backup, restore, clone, and verification jobs on Microsoft SQL Server databases.
- [SnapCenter Software 1.1 Data Protection Guide for Oracle Databases](#)
Describes how to use SnapCenter to perform backup, restore, clone, mount, unmount, and verification jobs on Oracle databases.
- [SnapCenter Software 1.1 Windows Cmdlet Reference Guide](#)
Provides reference information about the Windows PowerShell cmdlets available in SnapCenter, including a description of each cmdlet, its syntax, and examples for its use. This content is also available through the SnapCenter PowerShell cmdlet help.
- [SnapCenter Software 1.1 Linux Command Reference Guide](#)
Provides reference information about the Linux commands available for Linux plug-ins, including a description of each command, its syntax, and examples for its use. This content is also available through the SnapCenter command-line interface help.

Copyright information

Copyright © 1994–2016 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web.

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

How to send comments about documentation and receive update notifications

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

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

[*doccomments@netapp.com*](mailto:doccomments@netapp.com)

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

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

You can also contact us in the following ways:

- NetApp, Inc., 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

A

- administrator
 - role [29, 30](#)
- administrator role
 - logging in as [28](#)
- Application Request Routing
 - configuring [22](#)
 - removing server farm [81](#)
 - requirements for installation [23](#)
 - understanding [22, 23](#)
- architecture
 - overview of SnapCenter components [6](#)
- ASM instance
 - setting up your Run As account credentials [36, 37](#)
- authentication
 - encryption [9](#)
 - for Run As credential [36](#)
 - types [36](#)
- authentication mode
 - setting up your Run As account [36, 37](#)
- authentication SnapCenter [9](#)
- AutoSupport
 - enabling email notifications [85](#)
 - Virtual Storage Console [49](#)

B

- backup operations
 - resources, datasets, and policies overview [10](#)
- backups
 - configuring log directory [51](#)
 - using SnapMirror and SnapVault replication [70](#)
- best practices
 - for uninstalling plug-ins [79](#)
 - for uninstalling SnapCenter [81](#)
 - for volume and share configurations [63](#)
 - getting started with SnapCenter [49](#)
 - setting up your Run As account [36, 37](#)

C

- CIFS licenses
 - required for SnapCenter [20](#)
- clone operations
 - resources, datasets, and policies overview [10](#)
- Cluster Shared Volumes
 - connecting to disks [60](#)
 - creating disks [57](#)
- clusters, Microsoft
 - introduction to using FC RDM LUNs in [66](#)
 - support limitations when using FC RDM LUNs [67](#)
- cmdlets
 - SnapCenter Plug-in for Microsoft Windows support [68](#)
- comments
 - how to send feedback about documentation [91](#)
- configuring

- AutoSupport email notifications [85](#)
- host log directory [51](#)
- the frequency of software update checks [75](#)
- connections
 - required before installing SnapCenter [19](#)
 - setting up for SVMs [34](#)
- credentials
 - setting up your Run As account [36, 37](#)
 - supported for installing plug-ins for Windows [65, 66](#)
- CSV
 - See* Cluster Shared Volume

D

- Data ONTAP
 - account permission requirements for SnapCenter [29](#)
 - supported versions [18](#)
- data protection
 - resources, datasets, and policies overview [10](#)
 - SnapCenter [6](#)
- databases
 - preparing for SnapMirror replication [70](#)
 - preparing storage systems for SnapVault replication [72](#)
- datasets
 - deleting [78, 79](#)
 - detaching policies from [78](#)
 - used in SnapCenter data protection [10](#)
- deleting
 - datasets [78, 79](#)
- disks
 - connecting to LUNs in SnapCenter [60](#)
 - creating in SnapCenter [57](#)
 - deleting LUNs in SnapCenter [63](#)
 - disconnecting from LUNs in SnapCenter [62](#)
 - resizing in SnapCenter [59](#)
 - tasks you can perform using SnapCenter [57](#)
 - viewing on a host [57](#)
- documentation
 - additional resources [88](#)
 - how to receive automatic notification of changes to [91](#)
 - how to send feedback about [91](#)
- downloading
 - SnapCenter software updates [75](#)

E

- email notifications
 - enabling for AutoSupport messages [85](#)
- error messages
 - Error retrieving current directory [86](#)
 - launching SnapCenter [85](#)
- ESX servers
 - limitations of SnapCenter Plug-in for Microsoft Windows support [65](#)

F

- FC RDM LUNs
 - creating shared [67](#)
 - introduction to using in Microsoft clusters [66](#)
 - Microsoft cluster support limitations when using [67](#)
 - requirements for using in Microsoft clusters [66](#)
- FC-connected LUNs
 - creating [57](#)
 - introduction to configuring with SnapCenter Plug-in for Windows [54](#)
- features
 - enabled during installation on Windows hosts [83](#)
 - of SnapCenter [6](#)
- feedback
 - how to send comments about documentation [91](#)
- Fibre Channel licenses
 - required for SnapCenter [20](#)
- FlexClone licenses
 - required for SnapCenter [20](#)

H

- hosts
 - creating an igroup in SnapCenter Plug-in for Microsoft Windows [55](#)
 - creating SMB shares [63](#)
 - deleting an igroup [56](#)
 - disconnecting LUNs from [62](#)
 - features enabled during installation on Windows [83](#)
 - licenses for SnapCenter plug-ins [20](#)
 - modifying an igroup [56](#)
 - provisioning Windows with SnapCenter Plug-in for Microsoft Windows [54](#)
 - remote, installing plug-in packages on [42](#)
 - removing from SnapCenter [79](#)
 - removing from SnapCenter, introduction to [78](#)
 - renaming an igroup [56](#)
 - supported systems [18](#)
 - system requirements for installing SnapCenter [16](#)
 - viewing a list of disks on [57](#)
- HTTP
 - error 503 launching SnapCenter [85](#)
 - port requirements [19](#)

I

- igroups
 - creating in SnapCenter Plug-in for Microsoft Windows [55](#)
 - deleting in SnapCenter Plug-in for Microsoft Windows [56](#)
 - managing [55](#)
 - modifying [56](#)
 - purpose [55](#)
 - renaming [56](#)
- information
 - how to send feedback about improving documentation [91](#)
- initiators
 - adding to an igroup [56](#)
 - creating an igroup [55](#)

- installation
 - connection and port requirements for SnapCenter [19](#)
 - features enabled on Windows hosts [83](#)
 - monitoring [47](#)
 - plug-in checklist [39](#)
 - preparing for [24](#)
 - required information [24](#)
 - SnapCenter Plug-in Loader service [48](#)
 - space requirements for packages [16](#)
 - installation fails
 - improper uninstallation [86](#)
 - incorrect Java version [85](#)
 - installing
 - on multiple hosts [46](#)
 - plug-in packages on remote hosts [42](#)
 - plug-ins [38](#)
 - preparation overview [14](#)
 - SnapCenter [27](#)
 - SnapCenter and the plug-ins, overview of [26](#)
 - SnapCenter process overview for new users [13](#)
 - SnapCenter process overview for SnapManager users [11](#)
 - Internet Explorer Protected Mode
 - disabling [85](#)
 - iSCSI
 - disconnecting a session [55](#)
 - establishing a session [54](#)
 - licenses required for SnapCenter [20](#)
 - iSCSI-connected LUNs
 - creating [57](#)
 - introduction to configuring with SnapCenter Plug-in for Windows [54](#)
- J**
- jobs
 - backups, configuring the log for [51](#)
 - identifying available resources for [49](#)
 - monitoring progress of plug-in package installation [47](#)
- L**
- licensing
 - for existing SnapManager products [20](#)
 - for SnapCenter [20](#)
 - limitations
 - support when using FC RDM LUNs in Microsoft clusters [67](#)
 - VMware ESX server-related [65](#)
 - Linux host
 - setting up your Run As account credentials [36, 37](#)
 - load balancing
 - best practices [23](#)
 - using Application Request Routing [23](#)
 - local hosts
 - troubleshooting issues with displaying web login page on [85](#)
 - logging in
 - as a SnapCenter administrator [28](#)
 - as a SnapCenter user [28](#)
 - to SnapCenter [28](#)

- with more than one role [28](#)
- LUN storage
 - introduction to configuring with SnapCenter Plug-in for Windows [54](#)
- LUNs
 - connecting to in SnapCenter [60](#)
 - creating in SnapCenter [57](#)
 - creating shared FC RDM [67](#)
 - deleting in SnapCenter [63](#)
 - disconnecting before deleting [62](#)
 - disconnecting in SnapCenter [62](#)
 - disk-related tasks you can perform using SnapCenter [57](#)
 - FC RDM, requirements for using in a Microsoft cluster [66](#)
 - introduction to creating and managing using SnapCenter Plug-in for Microsoft Windows in VMware environments [65](#)
 - prerequisites for iSCSI connections [54](#)
 - RDM, support through PowerShell cmdlets [65](#)
 - RDM, troubleshooting creation of [68](#)
 - resizing in SnapCenter [59](#)
- LUNs, FC RDM
 - FC RDM Microsoft cluster support limitations when using [67](#)
 - introduction to using in Microsoft clusters [66](#)

M

- messages
 - enabling AutoSupport email notifications for [85](#)
- Microsoft clusters
 - introduction to using FC RDM LUNs in [66](#)
 - support limitations when using FC RDM LUNs [67](#)

N

- Network Load Balancing
 - configuring [22](#)
 - removing cluster [81](#)
 - understanding [22](#)
- NFS licenses
 - required for SnapCenter [20](#)
- notifications
 - enabling for AutoSupport email [85](#)

O

- Oracle database
 - setting up your Run As account credentials [36, 37](#)
 - versions supported [18](#)

P

- permissions
 - associated with pre-defined roles [30](#)
 - list of [30](#)
 - role-based access control [30](#)
 - setting for applications [36, 37](#)
 - understanding how to set [29](#)
- plug-in loader
 - failure [86](#)

- plug-in packages
 - installing on remote hosts [42](#)
 - introduction to installing [38](#)
 - uninstalling on multiple hosts [80](#)
 - upgrading [76](#)
- plug-ins
 - configuring [51](#)
 - deployment checklist [39](#)
 - installing [38](#)
 - installing on multiple hosts [46](#)
 - monitoring package installation [47](#)
 - overview of installing SnapCenter and [26](#)
 - preparing for uninstallation [78](#)
 - removing from a host [79](#)
 - uninstalling from SnapCenter, introduction to [78](#)
- policies
 - detaching from a dataset [78](#)
 - used in SnapCenter data protection [10](#)
- port requirements
 - before installing SnapCenter [19](#)
- PowerShell cmdlets
 - reclaiming storage space with [64](#)
 - SnapCenter Plug-in for Microsoft Windows support [68](#)

R

- RDM
 - minimum vCenter privileges required for operations [66](#)
- RDM LUNs
 - creating shared FC [67](#)
 - introduction to using FC in Microsoft clusters [66](#)
 - Microsoft cluster support limitations when using for FC [67](#)
 - requirements for FC support [66](#)
 - troubleshooting creation of [68](#)
- registering
 - Virtual Storage Console with SnapCenter [49](#)
- remote hosts
 - installing plug-in packages on [42](#)
- remote installation
 - on multiple hosts [46](#)
- remote uninstallation
 - on multiple hosts [80](#)
- removing
 - a host from SnapCenter [79](#)
 - hosts from SnapCenter, introduction to [78](#)
 - the Application Request Routing server farm [81](#)
 - the Network Load Balancing cluster [81](#)
 - the SnapCenter repository [81](#)
- replication
 - considerations for preparing storage systems for SnapMirror and SnapVault [70](#)
 - preparing storage systems for SnapMirror [70](#)
 - preparing storage systems for SnapVault [72](#)
- repositories
 - for SnapCenter, overview of [6](#)
 - identifying for SnapCenter metadata [22](#)
- requirements
 - Application Request Routing [23](#)
 - connection and port, before installing SnapCenter [19](#)
 - for SnapCenter installation [24](#)

- resizing
 - disks [59](#)
 - LUNs [59](#)
 - resources
 - assigning to users [34](#)
 - discovering [49](#)
 - identifying available [49](#)
 - used in SnapCenter data protection [10](#)
 - restore operations
 - resources, datasets, and policies overview [10](#)
 - role-based access control
 - adding users to a role [33](#)
 - assigning resources to users [34](#)
 - introduction to configuring for SnapCenter users [28](#)
 - list of roles and permissions [30](#)
 - pre-defined roles and permissions [30](#)
 - understanding [29](#)
 - roles
 - adding users to [33](#)
 - app backup and clone admin role, defined [30](#)
 - available pre-defined [30](#)
 - backup and clone viewer role, defined [30](#)
 - infrastructure admin role, defined [30](#)
 - list of [30](#)
 - understanding role-based access control [29](#)
 - Run As account
 - authentication methods [36](#)
 - overview [29](#)
 - setting up [36, 37](#)
- ## S
- security features
 - described [9](#)
 - servers
 - VMware ESX limitations of SnapCenter Plug-in for Microsoft Windows support [65](#)
 - shared FC RDM LUNs
 - creating [67](#)
 - using in a Microsoft cluster [67](#)
 - shares, SMB
 - creating in SnapCenter Plug-in for Microsoft Windows [63](#)
 - SMB shares
 - creating in SnapCenter Plug-in for Microsoft Windows [63](#)
 - deleting in SnapCenter [64](#)
 - SnapCenter
 - adding a VSC host [49](#)
 - archiving Snapshot copies [72](#)
 - components [6](#)
 - connection and port requirements for installation [19](#)
 - data protection [6](#)
 - finding the URL [28](#)
 - installation process overview for new users [13](#)
 - installation process overview for SnapManager users [11](#)
 - installing [27](#)
 - introduction to configuring role-based access control for users [28](#)
 - mirroring Snapshot copies [70](#)
 - overview [6](#)
 - registering Virtual Storage Console with [49](#)
 - removing repository [81](#)
 - templates for creating SMB shares [63](#)
 - uninstalling [81](#)
 - uninstalling, introduction to [78](#)
 - upgrading plug-in packages [76](#)
 - SnapCenter Plug-in for Linux
 - installation failure [86](#)
 - SnapCenter Plug-in for Microsoft SQL Server
 - overview of components [6](#)
 - removing from a host [80](#)
 - SnapCenter Plug-in for Microsoft Windows
 - creating an igroup [55](#)
 - creating SMB shares [63](#)
 - deleting an igroup [56](#)
 - limitations when using VMware ESX server [65](#)
 - modifying an igroup [56](#)
 - overview of components [6](#)
 - PowerShell cmdlet support [68](#)
 - renaming an igroup [56](#)
 - SnapCenter Plug-in for Oracle database
 - overview of components [6](#)
 - SnapCenter Plug-in for UNIX
 - installation failure [85](#)
 - overview of components [6](#)
 - SnapCenter Plug-in Loader service
 - start [48](#)
 - status [48](#)
 - stop [48](#)
 - SnapCenter Server
 - overview [6](#)
 - unable to communicate with the host [86](#)
 - upgrading [75](#)
 - SnapMirror
 - differences from SnapVault [70](#)
 - licenses required for SnapCenter [20](#)
 - SnapMirror replication
 - considerations for preparing storage systems for [70](#)
 - preparing storage systems for [70](#)
 - SnapRestore
 - licenses required for SnapCenter [20](#)
 - Snapshot backup copies
 - introduction to managing using SnapCenter Plug-in for Microsoft Windows in VMware environments [65](#)
 - Snapshot copies
 - features in SnapCenter [6](#)
 - preparing for SnapVault replication [72](#)
 - preparing storage systems for SnapMirror replication [70](#)
 - SnapVault
 - differences from SnapMirror [70](#)
 - licenses required for SnapCenter [20](#)
 - preparing storage systems for replication [72](#)
 - SnapVault replication
 - considerations for preparing storage systems for [70](#)
 - software updates
 - configuring SnapCenter to automatically check for [75](#)
 - space reclamation
 - on storage systems [64](#)
 - SQL Server
 - identifying a repository for SnapCenter metadata [22](#)
 - setting up your Run As account credentials [36, 37](#)
 - supported versions [18](#)

- SQL Server Express
 - identifying a repository for SnapCenter metadata [22](#)
- storage systems
 - considerations for preparing for SnapMirror and SnapVault replication [70](#)
 - licenses for SnapCenter plug-ins [20](#)
 - reclaiming space on [64](#)
 - setting up SVM connections to [34](#)
- storage types
 - supported by plug-ins package for Linux [15](#)
 - supported by SnapCenter Plug-In for Microsoft Windows [14](#)
 - SVMs [14](#)
 - VMs [14](#)
- storage, LUN
 - introduction to configuring with SnapCenter Plug-in for Windows [54](#)
- suggestions
 - how to send feedback about documentation [91](#)
- support limitations
 - when using FC RDM LUNs in Microsoft clusters [67](#)
- SVMs
 - setting up connections [34](#)
 - supported storage types [14, 15](#)
- systems
 - considerations for preparing for SnapMirror and SnapVault replication [70](#)
 - requirements for SnapCenter installation [16](#)

T

- templates
 - for creating SMB shares [63](#)
- terminology
 - resources, datasets, and policies data protection [10](#)
- troubleshooting
 - features enabled during installation [83](#)
 - HTTP error 503 [85](#)
 - RDM LUN creation [68](#)
 - SnapCenter installation [85](#)
 - web login page not displaying [85](#)
- Twitter
 - how to receive automatic notification of documentation changes [91](#)

U

- uninstalling
 - on multiple hosts [80](#)
 - plug-ins from a host [79](#)
 - preparing for plug-in uninstallation [78](#)
 - SnapCenter [81](#)
 - SnapCenter Plug-in for Microsoft SQL Server from a host [80](#)
 - SnapCenter plug-ins, introduction to [78](#)
 - SnapCenter, introduction to [78](#)
- updates, software
 - configuring SnapCenter to automatically check for [75](#)
- upgrading

- overview [75](#)
- SnapCenter [75](#)
- SnapCenter plug-in packages [76](#)
- users
 - adding to a role [33](#)
 - assigning resources to [34](#)
 - introduction to configuring role-based access control for [28](#)
 - using roles at login [28](#)

V

- vCenter
 - minimum privileges required for RDM operations [66](#)
- virtual disks
 - tasks you can perform using SnapCenter [57](#)
- Virtual Storage Console
 - adding a VSC host to SnapCenter [49](#)
 - registering with SnapCenter [49](#)
 - supported versions [18](#)
- virtualized environments
 - monitoring virtualization status [50](#)
 - registering Virtual Storage Console [49](#)
 - storage types supported [14](#)
- VMs
 - monitoring virtualization status [50](#)
 - supported storage types [14, 15](#)
- VMware
 - ESX servers limitations of SnapCenter Plug-in for Microsoft Windows support [65](#)
 - SnapCenter Plug-in for Windows support for [65](#)
 - support for ESX iSCSI initiators [65](#)
 - support for FC HBAs [65](#)
 - support for guest OS platforms [65](#)
 - support for iSCSI HBAs [65](#)
 - support for iSCSI initiators [65](#)
 - using Virtual Storage Console to provision Windows hosts [54](#)

W

- web address
 - for SnapCenter [28](#)
- web login page
 - troubleshooting issues with displaying on local host [85](#)
- Windows hosts
 - creating an igroup in SnapCenter Plug-in for Microsoft Windows [55](#)
 - features enabled during installation [83](#)
- Windows Process Activation Service (WAS)
 - enabling [85](#)
- Windows Server failover clusters
 - requirements for connecting to a disk [60](#)
 - requirements for creating a disk [57](#)
- workflows
 - getting started [49](#)
 - SnapCenter installation for new users [13](#)
 - SnapCenter installation for SnapManager users [11](#)