## Contents

- Deciding whether to read this information .............................................. 7
- **SnapCenter overview** ................................................................................ 8
  - SnapCenter features ................................................................................. 8
  - SnapCenter components ......................................................................... 8
  - SnapCenter security features ................................................................... 12
  - Modifying the SnapCenter default log out period ..................................... 13
  - How resources, resource groups, and policies are used in data protection .... 13
- **Installation workflow for SnapManager users** ................................... 15
- **Installation workflow for new users** ................................................ 18
- **Preparing for the installation** .............................................................. 20
  - Storage types supported by SnapCenter Plug-ins for Microsoft Windows and for
    - Microsoft SQL Server ........................................................................... 20
  - Storage types supported by SnapCenter Plug-in for Oracle Database ........... 22
  - Host requirements .................................................................................. 23
    - Domain requirements ........................................................................... 23
    - Space and sizing requirements ............................................................... 24
    - Supported operating systems ................................................................. 24
    - SAN host requirements ....................................................................... 25
  - Supported storage systems and applications .......................................... 26
  - Supported browsers .................................................................................. 27
  - Supported plug-ins for virtualized applications and virtual machines ........ 27
    - SnapCenter Plug-in for VMware vSphere .............................................. 28
    - Virtual Storage Console for VMware vSphere (VSC) ............................ 28
    - Determine which virtualized application plug-in you need to install ......... 29
  - Connection and port requirements ........................................................... 30
  - SnapCenter licensing requirements .......................................................... 32
  - SnapCenter repository identification ........................................................ 34
  - Network Load Balancing and Application Request Routing options .......... 34
  - Application Request Routing requirements ............................................. 35
  - SnapCenter installation worksheet ............................................................ 36
- **Installing SnapCenter and the plug-in packages** ............................... 38
  - Installing the SnapCenter Server .............................................................. 38
  - Logging in to SnapCenter ......................................................................... 40
  - Configuring role-based access control for SnapCenter users .................... 41
    - Types of role-based access control in SnapCenter .................................. 41
    - ONTAP CLI commands for creating SVM roles ..................................... 42
    - Role-based access control permissions and roles .................................... 45
    - Pre-defined roles and permissions .......................................................... 46
    - Adding a user to a role .......................................................................... 49
    - Assigning users access to assets ............................................................. 50
  - Setting up storage system connections .................................................... 51
| Setting up Run As credentials | 54 |
| Authentication methods for your Run As credentials | 54 |
| Setting up your Run As credentials | 55 |
| Installing plug-in packages | 57 |
| Prerequisites to adding hosts and installing plug-in packages | 57 |
| SnapCenter plug-in deployment checklist | 59 |
| Adding hosts and installing plug-in packages on remote hosts | 62 |
| Installing plug-ins on multiple remote hosts using cmdlets | 67 |
| Increasing the remote plug-in installation process timeout | 68 |
| Monitoring SnapCenter plug-in package installation status | 68 |
| Configuring the host log directory and verification server for SQL Server | 69 |
| Identifying available resources | 71 |
| Adding resources to SnapCenter Custom Plug-ins | 71 |
| Managing the SnapCenter Plug-in Loader service for Linux | 74 |
| Preparing storage systems for SnapMirror and SnapVault replication | 76 |
| Understanding the differences between SnapMirror and SnapVault | 76 |
| Preparing storage systems for SnapMirror replication | 77 |
| Preparing storage systems for SnapVault replication | 78 |
| Provisioning storage on Windows hosts | 81 |
| Configuring LUN storage | 81 |
| Establishing an iSCSI session | 81 |
| Disconnecting an iSCSI session | 82 |
| Creating and managing igroups | 82 |
| Creating and managing disks | 84 |
| Creating and managing SMB shares | 90 |
| Creating an SMB share | 91 |
| Deleting an SMB share | 91 |
| Reclaiming space on the storage system | 92 |
| Using the SnapCenter Plug-in for Microsoft Windows in VMware environments | 92 |
| Supported VMware guest OS platforms | 93 |
| Using FC RDM LUNs in a Microsoft cluster | 94 |
| Troubleshooting RDM LUN creation | 95 |
| SnapCenter Plug-in for Microsoft Windows cmdlets | 96 |
| Setting up protection for virtualized resources | 97 |
| Switching from VSC to SnapCenter Plug-in for VMware vSphere | 97 |
| Registering VSC for VMware vSphere with SnapCenter | 98 |
| Monitoring virtualization status in SnapCenter | 99 |
| Updating hypervisor configuration settings | 100 |
| Updating vCenter or SnapCenter information in the SnapCenter Plug-in for VMware vSphere | 100 |
| Upgrading SnapCenter and SnapCenter plug-in packages | 102 |
| Configuring SnapCenter to check for available updates | 102 |
| Upgrading SnapCenter | 102 |
Upgrading your plug-in packages ................................................................. 104

Uninstalling SnapCenter plug-ins and plug-in packages ...................... 105
 Uninstalling plug-ins from a host using the SnapCenter GUI ................. 105
 Uninstalling Windows plug-ins using the command-line interface on the
  SnapCenter Server host ...................................................................... 106
 Uninstalling Windows plug-ins locally on a host .................................. 107
 Uninstalling SnapCenter Plug-ins Package for Linux using the command-line
  interface ....................................................................................... 107
 Removing a host from SnapCenter ...................................................... 108
 Uninstalling SnapCenter ..................................................................... 108

Installing plug-ins independently ......................................................... 110
 Installing the SnapCenter Plug-in for Microsoft Windows independently ... 110
  Preparation to install the SnapCenter Plug-in for Microsoft Windows ... 110
  Installing the SnapCenter Plug-in for Microsoft Windows silently from
  the command line ........................................................................... 110
 Installing SnapCenter Plug-in for Microsoft SQL Server independently ... 112
  Preparation to install the SnapCenter Plug-in for Microsoft SQL Server ...
  Installing the SnapCenter Plug-in for Microsoft SQL Server silently
  from the command line .................................................................... 113
 Installing SnapCenter Plug-in for Oracle Database independently .......... 114
  Preparation to install the SnapCenter Plug-in for Oracle Database ...... 114
  Installing the SnapCenter Plug-in for Oracle Database interactively ... 114
  Installing the SnapCenter Plug-in for Oracle Database using command-
  line interface ............................................................................. 115
 Installing the SnapCenter Plug-in for VMware vSphere silently .......... 115

Features enabled on your Windows host during installation ............ 117

Troubleshooting ................................................................................. 119
 SnapCenter installation fails to create DB with the error Invalid username/
  password, please try again .............................................................. 119
 Enabling AutoSupport email notifications ........................................... 119
 SnapCenter Plug-in Package for Microsoft Windows or SnapCenter Plug-in for
  Microsoft SQL Server upgrade might fail on hosts with SQL databases on
  VMDK .......................................................................................... 120
 HTTP error 503. The service is unavailable .......................................... 120
 Unable to display SnapCenter web login page on local host ............... 120
 SnapCenter Plug-ins Package for Linux installation fails due to an incorrect
  Java version .................................................................................. 121
 SnapCenter Plug-ins Package for Linux installation fails due to improper
  uninstallation ............................................................................. 121
 SnapCenter Plug-ins Package for Linux installation fails ....................... 122
 SnapCenter Server is unable to communicate with the host ............... 122
 SnapCenter plug-in loader fails with an error ................................... 123
 Registering vCenter details task displays a warning ......................... 123
 Unable to access cluster IP address from outside network ................ 124

Where to go next .............................................................................. 125
Deciding whether to read this information

This information describes how to upgrade your existing SnapCenter software and how to install SnapCenter Server, configure your SnapCenter environment, install plug-ins, provision storage on Windows hosts, and prepare storage for SnapMirror and SnapVault replication.

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

- Upgrade your existing SnapCenter software
  If you are using SnapCenter as part of the Data Fabric Solution for Cloud Backup deployment to protect NAS file services data, a new installation is required.
  If you are using SnapCenter as part of the Data Fabric Solution for Cloud Backup deployment, you should look at the Data Fabric Solution for Cloud Backup information first.
- Download and install the latest release of SnapCenter Server and plug-ins
- Configure role-based access control (RBAC), SVM connections, and Run As accounts
- Set up protection for virtualized resources
- Switch from Virtual Storage Console for VMware vSphere (VSC) to SnapCenter Plug-in for VMware vSphere for protecting your virtualized resources
- Provision storage on Windows hosts
- Prepare storage for SnapMirror and SnapVault replication
- Uninstall SnapCenter Server or individual plug-ins

Before you start the installation, you should read the SnapCenter Software 2.0 Release Notes and read the following information in this installation guide:

- Supported storage types, storage systems, applications, and browsers
- Host requirements, connection and port requirements, and licensing requirements
- SnapCenter plug-in used to support non-virtualized resources, virtualized resources, and virtualized machines
- SnapCenter installation worksheet

Data Fabric Solution for Cloud Backup

If this information is not suitable for your situation, you can find more information about different features and release-specific information for SnapCenter in the documentation available on SnapCenter Software Resources page on the NetApp Support Site at mysupport.netapp.com.

NetApp SnapCenter Software Resources
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 complete data protection operations, including Snapshot copy-based backup, clone, restore, and backup verification operations. SnapCenter provides 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
- 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 package contains plug-ins to SnapCenter. The SnapCenter Custom Plug-ins enables you to create your own plug-ins and protect them using the same SnapCenter interface.

To support virtualized environments, SnapCenter also interacts with the following plug-ins:

- SnapCenter Plug-in for VMware vSphere
  This plug-in is included in the SnapCenter Plug-ins Package for Windows.
SnapCenter Plug-in for VMware vSphere enables you to back up virtualized databases. It does not enable you to back up virtual machines.

- Virtual Storage Console for VMware vSphere (VSC)
  VSC is a vCenter Server plug-in and is not included in SnapCenter install packages.
  VSC enables you to back up virtualized databases and virtual machines.

SnapCenter includes these 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 agent runs on the SnapCenter Server and Windows plug-in host.
  The SnapCenter Server communicates with the Windows plug-ins through the SMCore agent.
If you are using the SnapCenter Plug-ins Package for Linux, the SMCore agent 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.

The SnapCenter Server and plug-ins communicate with the SMCore agent using HTTPS.

SnapCenter enables centralized application resource management and easy data protection job execution through the use of resource groups 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 system database backup, restore, and clone operations.

The Plug-in for Windows is a required component of the Plug-in for SQL Server workflows.

If you want to perform data protection operations on virtualized SQL Servers that are using VMDKs or RDMs, SnapCenter requires either SnapCenter Plug-in for VMware vSphere or VSC.

- If you use VSC, you must use the VSC interface to register SnapCenter.
- If you use SnapCenter Plug-in for VMware vSphere, SnapCenter automatically performs all necessary registration tasks.

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

**SnapCenter Plug-in for Microsoft Windows**

The Plug-in for Windows provides storage provisioning, Snapshot copy consistency, and space reclamation for Windows hosts. It also enables application-aware data protection management of Microsoft file systems. With the plug-in installed on your Windows host, you can use SnapCenter to create and resize disks, initiate iSCSI sessions, manage igroups, manage SMB shares, and perform backup, restore, and clone operations on Windows file systems.

Support is provided for provisioning SMB shares and Windows file systems on physical and RDM LUNs. You cannot use SnapCenter to back up Windows file systems on SMB shares.

**SnapCenter Plug-in for VMware vSphere**

SnapCenter Plug-in for VMware vSphere provides support for native backup, recovery, and cloning of virtualized applications (virtualized databases and Windows file systems) without need of user intervention or a registered VSC instance. SnapCenter Plug-in for VMware vSphere reduces the complexity of protecting virtualized applications. With the plug-in installed on your Windows host, SnapCenter natively leverages SnapCenter Plug-in for VMware vSphere for all data protection operations on virtual machine disks (VMDKs), and on raw device mappings (RDMs) using PowerShell cmdlets.

If you want to perform data protection operations on VMware virtual machines (VMs), in addition to virtualized applications, you must use Virtual Storage Console for VMware vSphere (VSC), not SnapCenter Plug-in for VMware vSphere. VSC is a vCenter Server
plug-in and is not included in the SnapCenter installation. Each installation of SnapCenter Server can support either the SnapCenter Plug-in for VMware vSphere or the VSC plug-in, but not both. For information on which plug-in to install in your environment, see the installation information.

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 Database 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 Database installed on your Oracle host, SnapCenter automates backup, restore, recovery, verify, mount, unmount, and clone operations.

**Note:** You can use the Plug-in for Oracle Database 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 Database. The Plug-in for UNIX supports the Network File System (NFS) and storage area network (SAN) protocols on a storage system that is running ONTAP. Oracle databases are supported on VMDK and RDM LUN when you also use SnapCenter Plug-in for VMware vSphere or Virtual Storage Console for VMware vSphere.

**SnapCenter Custom Plug-ins**

You can create custom plug-ins and use the SnapCenter Custom Plug-ins feature to manage applications of your choice. The SnapCenter Custom Plug-ins feature is a host-side component of SnapCenter that enables application-aware data protection and management of resources.

Custom plug-ins are created by any SnapCenter user to support applications or databases that might not be supported by SnapCenter. They are not provided as part of the SnapCenter installation.

When custom plug-ins are installed, you can use SnapCenter with NetApp SnapMirror technology to create mirror copies of backup sets on another volume and use NetApp SnapVault technology to perform disk-to-disk backup replication. The Custom Plug-ins can be used in both Windows and Linux environments. In Windows environment, custom applications via custom plug-ins can optionally utilize SnapCenter Plug-in for Microsoft Windows to take file system consistent backups.

NetApp supports the capability to create and use custom plug-ins; however, custom plug-ins you create are not supported by NetApp.

NetApp provides MySQL and DB2 custom plug-in samples with SnapCenter Software 2.0. These plug-ins can be downloaded from the NetApp Tool Chest.

**Note:** MySQL and DB2 custom plug-ins are supported via the NetApp communities only.

You can create your own custom plug-ins by referring to developer's guide.

**SnapCenter Plug-in for NAS File Services used with the Data Fabric Solution for Cloud Backup**

With the Data Fabric Solution for Cloud Backup, storage administrators and IT generalists can perform Snapshot copy-based data protection operations for file shares to and from public or private cloud object stores. Delivering high service levels with fast Snapshot copies and efficient array-based replication, the solution includes NetApp ONTAP, SnapCenter data management software, and AltaVault cloud-integrated storage software.
If you are using SnapCenter Plug-in for NAS File Services as part of the Data Fabric Solution for Cloud Backup deployment, you should look at the Data Fabric Solution for Cloud Backup information first.

Related concepts
   Preparing for the installation on page 20

Related references
   Host requirements on page 23

Related information
   SnapCenter Software 2.0 Developer’s Guide for Creating Custom Plug-ins
   Data Fabric Solution for Cloud Backup

SnapCenter security features
SnapCenter employs strict security and authentication features to enable you to keep your data secure.

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 supports Transport Layer Security (TLS) 1.2 communication with ONTAP. You can also use TLS 1.2 communication between clients and servers.
• 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 15 minutes of inactivity, SnapCenter warns you that you will be logged out in 5 minutes. After 20 minutes of inactivity, SnapCenter logs you out, and you must log in again.
   See information about changing the default log out period.
• Login is temporarily disabled after 5 or more incorrect login attempts.

Related tasks
   Modifying the SnapCenter default log out period on page 13
Modifying the SnapCenter default log out period

As a security feature, after a default period of 15 minutes of inactivity SnapCenter warns you that you will be logged out in 5 minutes. After 20 minutes of inactivity, SnapCenter logs you out, and you must log in again.

About this task

You can change the SnapCenter 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.

Steps

1. In the Windows Start menu, click Run.
2. In the Open dialog box, type inetmgr
3. Click OK to open Internet Information Services (IIS) Manager.
4. In the Connections pane on the left, select the local SnapCenter Server, and then browse to Sites > SnapCenter > Repository.
5. In the Repository Home pane on the right, double-click Session State.
6. In the Session State pane, locate Cookie Settings, and then in the Time-Out field, change the ASP.NET_sessionId timeout setting to the number of minutes you want SnapCenter to wait before you are logged out due to inactivity.

Example

For example, enter 60 to cause SnapCenter to log you out after one hour of inactivity.

7. In the Actions pane, click Apply.

How resources, resource groups, 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, resource groups, and policies for different operations.

- **Resources** are typically databases or Windows file systems that you back up or clone with SnapCenter.
  However, depending on your environment, resources might be database instances, Microsoft SQL Server availability groups, Oracle databases, Oracle RAC databases, Windows file systems, or a group of custom applications.

- A SnapCenter resource group, formerly known as a dataset, is a collection of resources on a host or cluster.
  When you perform an operation on a resource group, you perform that operation on the resources defined in the resource group according to the schedule you specify for the resource group.
  You can back up on demand a single resource or a resource group. You also can perform scheduled backups for single resources and resource groups. You should use a database plug-in to back up databases and the Plug-in for Windows to back up Windows file systems.
• The policies specify the backup frequency (also called backup type), copy retention, replication, scripts, and other characteristics of data protection operations.

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

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

The following image illustrates the relationship between resources, resource groups, and policies for databases:

The following image illustrates the relationship between resources, resource groups, and policies for Windows file systems:
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 backups. After you install and configure SnapCenter, you can use the SnapCenter import feature to move from your SnapManager environment to SnapCenter.

Uninstallation of SnapManager products is not required. Your SnapManager products must be present to enable you to import your data SnapCenter.

**Note:** SnapCenter does not support 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.*
Transition from 7-Mode to ONTAP.

Install SnapCenter Server.

Log in to SnapCenter Server using a web browser.

Configure SnapCenter environment:
- Configure role-based access control (RBAC).
- Configure Storage Virtual Machine (SVM) connections.
- Create a Run As account.

Install and configure plug-ins:
- For custom plug-ins, download or create plug-ins.
- Add hosts and install plug-in packages or upload and install custom plug-ins.
- Monitor plug-in package installation.
- Configure database.
  For SQL Server, configure the host log directory and verification server.
  For custom plug-ins, add resources and assign them to users.

Do you want to protect virtualized applications or file systems on VMDKs or RDM LUNs?

Yes

Do you want to protect VMs?

No

Do you want to replicate backups?

Set up SnapMirror and SnapVault.

Use SnapCenter:
- Create a backup policy.
- Create a backup resource group.
- Backup now.
- Monitor backup progress.

Import data from SnapManager to SnapCenter.

See 7-Mode Transition Tool documentation.

For creating custom plug-ins, see developer’s guide.

For Windows environments, provision LUNs, SMB shares, or VMDKs.

Install SnapCenter Plug-in for VMware vSphere.

Install VSC for VMware vSphere and register it with SnapCenter.

See VSC for VMware vSphere documentation.

See SnapCenter plug-in data protection guides.

See Importing Data from SnapManager to SnapCenter Guide.

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

Determine which virtualized application plug-in you need to install on page 29

Related references

Host requirements on page 23

Related information

NetApp Documentation: Virtual Storage Console for VMware vSphere
SnapCenter Software 2.0 Data Protection Guide for Microsoft SQL Server
SnapCenter Software 2.0 Importing Data from SnapManager to SnapCenter
SnapCenter Software 2.0 Data Protection Guide for Oracle Databases
NetApp Documentation: 7-Mode Transition Tool
Installation workflow for new users

If you are new to SnapCenter and you are not using 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.

1. Install SnapCenter Server.
2. Log in to SnapCenter Server using a web browser.
3. Configure SnapCenter environment:
   - Configure role-based access control (RBAC).
   - Configure Storage Virtual Machine (SVM) connections.
   - Create a Run As account.
4. Install and configure plug-ins:
   - For custom plug-ins, download or create plug-ins.
   - Add hosts and install plug-in packages or upload and install custom plug-ins.
   - Monitor plug-in package installation.
   - Configure database.
   - For SQL Server, configure the host log directory and verification server.
   - For custom plug-ins, add resources and assign them to users.
5. Do you want to protect virtualized applications or file systems on vMDKs or RDM LUNs?
   - Yes
     - Do you want to protect VMs?
       - Yes
         - Install VSC for VMware vSphere and register it with SnapCenter.
         - See VSC for VMware vSphere documentation.
       - No
         - Install SnapCenter Plug-in for VMware vSphere.
         - For Windows environments, provision LUNs, SMB shares, or VMDKs.
   - No
8. Do you want to replicate backups?
   - Yes
     - Set up SnapMirror and SnapVault.
   - No
9. Use SnapCenter:
   - Create a backup policy.
   - Create a backup resource group.
   - Backup now.
   - Monitor backup progress.
10. See SnapCenter plug-in data protection guides.
Some features are available only with specific operating systems. See host requirements information.

Related concepts

*Determine which virtualized application plug-in you need to install* on page 29

Related references

*Host requirements* on page 23

Related information

*NetApp Documentation: Virtual Storage Console for VMware vSphere*
*SnapCenter Software 2.0 Data Protection Guide for Microsoft SQL Server*
*SnapCenter Software 2.0 Data Protection Guide for Oracle Databases*
*SnapCenter Software 2.0 Data Protection Guide for Custom Plug-ins*
Preparing for the installation

You should be aware of several requirements and prerequisites before installing SnapCenter.

- Supported storage types
- Host requirements
- Supported storage systems and applications
- Supported browsers
- Supported plug-ins for virtualized applications and virtual machines
- Connection and port requirements
- SnapCenter licensing
- SnapCenter repository 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.

For the latest information, see the Interoperability Matrix on the NetApp Support Site.

Related concepts
- Supported plug-ins for virtualized applications and virtual machines on page 27
- SnapCenter repository identification on page 34
- Network Load Balancing and Application Request Routing options on page 34
- Minimum vCenter privileges required for SnapCenter RDM operations on page 93

Related references
- Host requirements on page 23
- Supported storage systems and applications on page 26
- Connection and port requirements on page 30
- SnapCenter licensing requirements on page 32
- SnapCenter installation worksheet on page 36

Storage types supported by SnapCenter Plug-ins for Microsoft Windows and 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 host.

SnapCenter provisioning and data protection support is available on Windows Server 2008 R2 SP1, Windows Server 2012 and 2012 R2, and Windows Server 2016.
<table>
<thead>
<tr>
<th>Machine</th>
<th>Storage type</th>
<th>Provision using</th>
<th>Support notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical server</td>
<td>FC-connected LUNs</td>
<td>SnapCenter graphical user interface (GUI) or PowerShell cmdlets</td>
<td></td>
</tr>
<tr>
<td>iSCSI-connected LUNs</td>
<td></td>
<td>SnapCenter GUI or PowerShell cmdlets</td>
<td></td>
</tr>
<tr>
<td>SMB3 (CIFS) shares residing on a Storage Virtual Machine (SVM)</td>
<td></td>
<td>SnapCenter GUI or PowerShell cmdlets</td>
<td>Support for provisioning only. You cannot use SnapCenter to back up any data or shares using the SMB protocol.</td>
</tr>
<tr>
<td>VMware VM</td>
<td>RDM LUNs connected by an FC or iSCSI HBA</td>
<td>PowerShell cmdlets</td>
<td>Each installation of SnapCenter Server can support either the SnapCenter Plug-in for VMware vSphere or the VSC plug-in, but not both. If you use VSC, you must use the VSC interface to register SnapCenter before you can use SnapCenter to back up databases on RDM LUNs.</td>
</tr>
<tr>
<td></td>
<td>iSCSI LUNs connected directly to the guest system by the iSCSI initiator</td>
<td>SnapCenter GUI or PowerShell cmdlets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Virtual Machine File Systems (VMFS) on VMFS or NFS datastores</td>
<td>VMware vSphere or VSC cloning utility</td>
<td>Each installation of SnapCenter Server can support either the SnapCenter Plug-in for VMware vSphere or the VSC plug-in, but not both. If you use VSC, you must use the VSC interface to register SnapCenter before you can use SnapCenter to back up databases on VMDKs.</td>
</tr>
<tr>
<td></td>
<td>A guest system connected to SMB3 shares residing on an SVM</td>
<td>SnapCenter GUI or PowerShell cmdlets</td>
<td>Support for provisioning only. You cannot use SnapCenter to back up any data or shares using the SMB protocol.</td>
</tr>
</tbody>
</table>
### 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.

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

<table>
<thead>
<tr>
<th>Machine</th>
<th>Storage type</th>
<th>Support notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical server</td>
<td>FC-connected LUNs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>iSCSI-connected LUNs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NFS-connected volumes</td>
<td></td>
</tr>
</tbody>
</table>

*Note: Hyper-V pass through disks and backing up databases on VHD(x) that are provisioned on NetApp storage are not supported.*
<table>
<thead>
<tr>
<th>Machine</th>
<th>Storage type</th>
<th>Support notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESX</td>
<td>RDM LUNs connected by an FC or iSCSI HBA</td>
<td>Each installation of SnapCenter Server can support either the SnapCenter Plug-in for VMware vSphere or the VSC plug-in, but not both. If you use VSC, you must use the VSC interface to register SnapCenter before you can use SnapCenter to back up databases on RDM LUNs.</td>
</tr>
<tr>
<td>iSCSI LUNs</td>
<td>connected directly to the guest system by the iSCSI initiator</td>
<td>Each installation of SnapCenter Server can support either the SnapCenter Plug-in for VMware vSphere or the VSC plug-in, but not both. If you use VSC, you must use the VSC interface to register SnapCenter before you can use SnapCenter to back up databases on VMDKs.</td>
</tr>
<tr>
<td>VMDKs on VMFS or NFS datastores</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFS volumes</td>
<td>connected directly to the guest system</td>
<td></td>
</tr>
</tbody>
</table>

**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**

Before you begin the SnapCenter installation, you should be familiar with the domain requirements.

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

*Note:* Data protection using SnapCenter requires a two-way trust relationship between the SnapCenter Server domain and the plug-in domain. The SnapCenter Server domain and the plug-in 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.

*Note:* 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.


For installation, you must have domain user rights with local administrator credentials.
Space and sizing requirements

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

Installation package space requirements

After installation, SnapCenter components require the following space:

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Space needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnapCenter Server</td>
<td>40 GB</td>
</tr>
<tr>
<td>SnapCenter Plug-ins Package for Windows</td>
<td>500 MB</td>
</tr>
<tr>
<td>SnapCenter Plug-ins Package for Linux</td>
<td>200 MB</td>
</tr>
</tbody>
</table>

SnapCenter Server host system sizing requirements

The SnapCenter host requires the following:

- Minimum RAM: 32 GB
- Minimum CPU: 4 CPUs
- Minimum SnapCenter repository sizing requirements: 40 GB

Plug-in host system sizing 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

Before you begin the SnapCenter installation, you should be familiar with the operating systems that are supported by SnapCenter.

Supported operating systems

All supported Windows operating systems are 64-bit only.

Before installing SnapCenter Server, it is recommended that you apply all available system and security updates.

<table>
<thead>
<tr>
<th>Component</th>
<th>Supported host systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnapCenter Server</td>
<td>• Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 DCE, R2 DCE, SE, R2 SE</td>
</tr>
</tbody>
</table>
## Component | Supported host systems
---|---
SnapCenter Plug-ins Package for Windows | • Windows Server 2016  
• Windows Server 2012 and 2012 R2  
• Windows Server 2008 R2 SP1 *

SnapCenter Plug-ins Package for Linux | • 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

* You must enable the Cluster Shared Volumes (CSV) feature in Windows Server 2008 R2 SP1 if you want to create CSV type disks.

### Additional requirements for hosts that SnapCenter Server manages

For hosts with Windows Server 2008 R2 SP1 and Windows Server 2012 hosts, 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 all hosts, or manually install them:

- Microsoft .NET Framework 4.5.2
- WMF 4.0
- PowerShell 4.0

### SAN host requirements

If your SnapCenter host is part of a FC/iSCSI environment, you might need to install additional software on the system to enable access to ONTAP storage.

If your SnapCenter host is part of a SAN environment, you might need to install the following software:

- Host Utilities  
  The Host Utilities support FC and iSCSI, and allow you to use MPIO on your Windows Servers.
- ONTAP DSM for Windows MPIO  
  This software works with Windows MPIO drivers to manage multiple paths between NetApp and Windows host computers.

For more information, see the Host Utilities and ONTAP DSM for Windows MPIO product documentation and the Interoperability Matrix Tool on the NetApp Support Site.

*NetApp Documentation*

*NetApp Interoperability Matrix Tool*
Supported storage systems and applications

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 and application before you begin your installation.

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

**Supported ONTAP versions**

SnapCenter requires ONTAP 8.2.2 and later.

*Note:* If you are using Data Fabric Solution for Cloud Backup, ONTAP 9.1 RC2 is required.

**Supported SQL versions for SnapCenter Server repository**

MySQL Server 5.7 is installed automatically when you install SnapCenter 2.0. SnapCenter does not support different MySQL Server versions that are already installed.

*Note:* MySQL Server is used for new SnapCenter installations only. If you have SQL Server database installed and you are upgrading to SnapCenter 2.0, SnapCenter continues using SQL Server as the database repository.

You can use SQL Server Enterprise or Standard Edition.

**Supported SQL versions for Plug-in for SQL Server data protection**

The supported SQL Server version for Plug-in for SQL Server data protection are:

- SQL Server 2016
- SQL Server 2014 SP1
- SQL Server 2012 SP2
- SQL Server 2008 R2 SP3
- SQL Server 2008 SP4

**Supported Oracle Database versions**

The supported Oracle Database versions are Oracle 11gR2 (11.2.0.4) and Oracle 12c (12.1.0.2).

**Supported virtualized application environments**

SnapCenter Plug-in for VMware vSphere supports all virtualized applications that are supported by SnapCenter.

*Note:* You do not need to install SnapCenter Plug-in for VMware vSphere in the following scenarios:

- Your SQL Server environment uses an in-guest iSCSI initiator
- Your Oracle environment uses NFS or an in-guest iSCSI initiator

Each installation of SnapCenter Server can support either the SnapCenter Plug-in for VMware vSphere or the VSC plug-in, but not both.
VSC for VMware vSphere requirements

SnapCenter 2.0 requires Virtual Storage Console 6.2P2 or later for VMware vSphere to back up VMs in addition to virtualized databases or virtualized Windows file systems. If you do not need to back up VMs then you can use SnapCenter Plug-in for VMware vSphere instead.

Note: You do not need to install the Virtual Storage Console for the following environments:

- You do not need to back up VMs
- You are using the plug-in for SQL Server and your SQL Server environment uses a FC/iSCSI initiator
- You are using the plug-in for Oracle and your Oracle environment uses NFS mounts or a FC/iSCSI initiator

VSC is not included in the SnapCenter installation. Each installation of SnapCenter Server can support either the SnapCenter Plug-in for VMware vSphere or the Virtual Storage Console, but not both.

Supported custom plug-in versions

- Supported MySQL versions are 5.6.29 and 5.7.12
- Supported DB2 versions are 10.5.0 and 11.1.0

Related information

- NetApp Interoperability Matrix Tool
- NetApp Documentation: Virtual Storage Console for VMware vSphere

Supported browsers

It is helpful to understand the basic browser support before you begin your installation.

For the latest information, see the Interoperability Matrix.

- Chrome version 53 or later
- Internet Explorer 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.
- Microsoft Edge

Supported plug-ins for virtualized applications and virtual machines

SnapCenter supports two plug-ins for virtualized applications and virtual machines. You should determine which plug-in best fits your virtual environment needs.

SnapCenter Plug-in for VMware vSphere provides native backup, recovery, and cloning of virtualized applications (virtualized databases and Windows file systems).
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 and for virtualized applications.

Each installation of SnapCenter Server can support either the SnapCenter Plug-in for VMware vSphere or the VSC plug-in, but not both.

If you plan to use VSC, SnapCenter requires VSC 6.2P2 or later.

**Note:** You do not need to install SnapCenter Plug-in for VMware vSphere or Virtual Storage Console for VMware vSphere if you are using one of the following:

- Plug-in for SQL Server and your SQL Server environment uses an iSCSI initiator
- Plug-in for Oracle and your Oracle environment uses NFS or an in-guest iSCSI initiator

### SnapCenter Plug-in for VMware vSphere

SnapCenter Plug-in for VMware vSphere is included in the SnapCenter Plug-ins Package for Windows. SnapCenter natively uses this plug-in to communicate with your vCenter for data protection operations of virtualized applications without user intervention and without a registered VSC instance, which reduces the complexity of protecting virtualized applications.

SnapCenter Plug-in for VMware vSphere supports virtualized databases (Microsoft SQL Server and Oracle) and virtualized Windows file systems on raw device mapping (RDM) LUNs and virtual machine disks (VMDKs) over VMFS and NFS. After the plug-in is installed, the SnapCenter plug-ins for Microsoft Windows, Microsoft SQL Server, and Oracle Database natively leverage SnapCenter Plug-in for VMware vSphere for all data protection operations for virtualized applications.

Each installation of SnapCenter Server can support either the SnapCenter Plug-in for VMware vSphere or the VSC plug-in, but not both.

You must consider the following requirements when planning your SnapCenter Plug-in for VMware vSphere installation:

- You must have SnapCenter admin privileges to install and manage SnapCenter Plug-in for VMware vSphere.
- Install the plug-in on a dedicated Windows host (virtual or physical).
- Do not install other plug-ins on the SnapCenter Plug-in for VMware vSphere host.
- Do not install the plug-in on the SnapCenter Server.
- Do not install the plug-in on the vCenter Server.

**Note:** SnapCenter Plug-in for VMware vSphere used with VSC 6.2P.x does not support IPV6. Therefore, NFS mount and restore operations from IPV6 LIFs are not supported.

### Virtual Storage Console for VMware vSphere (VSC)

VSC is a vCenter Server plug-in that integrates with SnapCenter to provide backup, recovery, and cloning operation support. It supports VMware virtual machines (VMs) that are using NetApp storage systems running clustered Data ONTAP 8.2.2 or later. It also supports virtualized databases (Microsoft SQL Server and Oracle) and virtualized Windows file systems on raw device mapping (RDM) LUNs and virtual machine disks (VMDKs) over VMFS and NFS.

Integrating VSC with SnapCenter enables VSC backup and restore operations to use the SnapCenter repository 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.
Because NetApp Snapshot technology takes point-in-time copies of data on disks, whether on virtualized or physical servers, the data is always in a consistent state. This allows backup and restore operations to be less complicated. If you are using SnapCenter with VSC to protect VMs, you do not need to take VMware quiesced snapshots; the SnapCenter plug-ins automatically quiesce and unquiesce the supported applications.

VSC also supports backup and restore operations of VMs before and after storage vMotion moves from one datastore to another.

VSC is not included in the SnapCenter installation; you must install it separately and you must use the VSC GUI to register SnapCenter with VSC. Each installation of SnapCenter Server can support either the SnapCenter Plug-in for VMware vSphere or the VSC plug-in, but not both.

**Note:** Each SnapCenter Server can support multiple VSC servers. You must use the VSC GUI to register each VSC server individually with SnapCenter.

You must consider the following requirements when planning your VSC installation:

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

- Do not install VSC on the SnapCenter Server host.
  **Note:** Specific versions of VSC support specific versions of SnapCenter. For example, VSC 6.2P2 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.

If you do not have VMs to protect, you can use the SnapCenter Plug-in for VMware vSphere instead of VSC for native backup, recovery, and cloning of virtualized applications. For information on which plug-in to install in your environment, see the installation information.

If you used VSC to create policies and registered VSC with SnapCenter, you can view these policies in SnapCenter. You can also view VSC-based backup, clone, and restore operations in the SnapCenter Jobs view. You cannot use SnapCenter to view resource groups created with VSC.

**Related concepts**

*Determine which virtualized application plug-in you need to install* on page 29

**Determine which virtualized application plug-in you need to install**

For each installation of SnapCenter Server, you can install either SnapCenter Plug-in for VMware vSphere or Virtual Storage Console for VMware vSphere (VSC), but not both. Your choice depends upon whether you want to protect virtualized applications only or virtualized applications and VMs.

**Note:** You do not need to install SnapCenter Plug-in for VMware vSphere or Virtual Storage Console for VMware vSphere if you are using one of the following:

- Plug-in for SQL Server and your SQL Server environment used an iSCSI initiator
- Plug-in for Oracle and your Oracle environment uses NFS or an iSCSI initiator

If you need to install a plug-in for data protection of virtualized applications or VMs, use the following table to determine which plug-in you need to install.
<table>
<thead>
<tr>
<th>If you are a ...</th>
<th>Using ...</th>
<th>To protect ...</th>
<th>Then do the following ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>New SnapCenter customer</td>
<td>N.A.</td>
<td>Virtualized applications only (in a clustered ONTAP environment)</td>
<td>Install SnapCenter 2.0 and SnapCenter Plug-in for VMware vSphere 2.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Virtualized applications and VMs (in a clustered ONTAP environment)</td>
<td>Install SnapCenter 2.0 and VSC 6.2P2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMs only (in a clustered ONTAP environment)</td>
<td>Install SnapCenter 2.0 and VSC 6.2P2</td>
</tr>
</tbody>
</table>
| Existing SnapCenter customer | SnapCenter 1.1 and VSC 6.2P2 | Virtualized applications only (in a clustered ONTAP environment) | 1. Upgrade to SnapCenter 2.0  
2. Uninstall VSC 6.2P2  
3. Install SnapCenter Plug-in for VMware vSphere 2.0 |
| | | Virtualized applications and VMs (in a clustered ONTAP environment) | Upgrade to SnapCenter 2.0 and continue using VSC 6.2P2 |
| | | VMs only (in a clustered ONTAP environment) | Upgrade to SnapCenter 2.0 and continue using VSC 6.2P2 |
| | | VMs or virtualized applications in a mixed ONTAP environment | Upgrade to SnapCenter 2.0 and continue using VSC 6.2P2* |

* In a mixed ONTAP environment, clustered Data ONTAP jobs use SnapCenter 2.0; 7-Mode Data ONTAP jobs use VSC. You must continue using VSC 6.2P2 for data protection jobs until you decommission your 7-Mode Data ONTAP environment.

### Connection and port requirements

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

- Applications cannot share a port  
  All ports must be dedicated to the appropriate application.

- Customizable ports  
  For customizable ports, you can select a custom port when you install if you do not want to use the default port.  
  You cannot modify a customizable port number after you install. To change a port number after installation, you must uninstall SnapCenter and install again.

- Fixed ports  
  For fixed ports, you must accept the default port number.

- Firewalls  
  - 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).

SnapCenter uses the following default ports:

<table>
<thead>
<tr>
<th>Type of port</th>
<th>Default port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnapCenter port</td>
<td>8146 (HTTPS), fixed, as in the URL <a href="https://server:8146">https://server:8146</a></td>
</tr>
<tr>
<td></td>
<td>Used for communication between the SnapCenter client (the SnapCenter user) and SnapCenter Server. Also used for communication from plug-in hosts to SnapCenter Server.</td>
</tr>
<tr>
<td>SnapCenter SMCore communication port</td>
<td>8145 (HTTPS), bidirectional, customizable</td>
</tr>
<tr>
<td></td>
<td>Used for communication between SnapCenter Server and hosts where SnapCenter plug-ins are installed.</td>
</tr>
<tr>
<td>SnapCenter Plug-in for Microsoft SQL Server port</td>
<td>8145 (HTTPS), bidirectional, customizable</td>
</tr>
<tr>
<td>SnapCenter Plug-in for Microsoft Windows port</td>
<td>Used for communication between SMCore and hosts where the SnapCenter plug-ins are installed.</td>
</tr>
<tr>
<td>SnapCenter file catalog ports on Linux servers</td>
<td>8145, bidirectional, customizable</td>
</tr>
<tr>
<td></td>
<td>The following fixed ports are also required: 2181, 2888, 3888, or 8983.</td>
</tr>
<tr>
<td></td>
<td>Used for communication between SnapCenter Server and the index servers and also between index servers.</td>
</tr>
<tr>
<td>Custom plug-ins for SnapCenter</td>
<td>9090 (HTTPS), fixed</td>
</tr>
<tr>
<td></td>
<td>This is an internal port used only on the custom plug-in host; no firewall exception is required.</td>
</tr>
<tr>
<td></td>
<td>Communication between SnapCenter Server and custom plug-ins is routed through port 8145.</td>
</tr>
<tr>
<td>AltaVault</td>
<td>5010 (TCP), bidirectional, fixed</td>
</tr>
<tr>
<td></td>
<td>Used for communication between ONTAP and AltaVault; requires at least one intercluster LIF. The best practice is to connect to a 10Gb Ethernet switch.</td>
</tr>
<tr>
<td>AltaVault</td>
<td>443 (HTTPS), bidirectional, fixed</td>
</tr>
<tr>
<td></td>
<td>Used for communication between the AltaVault GUI and AltaVault; requires at least one data interface.</td>
</tr>
<tr>
<td>AltaVault Rest API port</td>
<td>8443 (HTTPS), bidirectional, fixed</td>
</tr>
<tr>
<td></td>
<td>Used for API communication between SnapCenter and AltaVault.</td>
</tr>
<tr>
<td>SnapCenter Plug-in for VMware vSphere port</td>
<td>8144 (HTTPS), bidirectional, customizable</td>
</tr>
<tr>
<td></td>
<td>Used for communication between SnapCenter and VMware vSphere.</td>
</tr>
<tr>
<td>Virtual Storage Console for VMware vSphere port</td>
<td>8143 (HTTPS), bidirectional, fixed</td>
</tr>
<tr>
<td></td>
<td>Used for communication between SnapCenter and VSC.</td>
</tr>
</tbody>
</table>
## SnapCenter licensing requirements

SnapCenter requires several licenses to enable data protection operations.

<table>
<thead>
<tr>
<th>License</th>
<th>Description</th>
<th>Where required</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONTAP</td>
<td>ONTAP requires one of the following licenses:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SnapMirror license (by itself or with Premium bundle)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SnapVault license (by itself or with Premium bundle)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Some platforms require the Premium bundle; no separate licenses are available for SnapMirror or SnapVault with these platforms.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Premium bundle can be on a legacy system or on a new platform.</td>
<td></td>
</tr>
<tr>
<td>SnapMirror</td>
<td>A license for mirroring backup sets to a destination storage system. Required for this solution. Existing SnapMirror licenses can be used.</td>
<td>On source and destination storage systems. Typically for FAS to FAS replication, SnapMirror is required on both source and destination systems.</td>
</tr>
<tr>
<td>SnapVault</td>
<td>An optional license for disk-to-disk backup replication to a destination storage system.</td>
<td>On source and destination storage systems.</td>
</tr>
<tr>
<td>SnapRestore</td>
<td>A required license that enables SnapCenter to restore and verify backup sets.</td>
<td>On primary storage systems. Also required on SnapVault destination systems to perform remote verification and to restore from a backup. Also required on SnapMirror destination systems to perform remote verification.</td>
</tr>
<tr>
<td>License</td>
<td>Description</td>
<td>Where required</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>SnapCenter</td>
<td>Depending on your requirements and the features that you want to use, you can use either standard or advanced licenses.</td>
<td>On SnapCenter Server.</td>
</tr>
<tr>
<td></td>
<td>• Standard – Support for backup and recovery of ONTAP storage, Clone Life Cycle management, basic reporting, task automation, host file systems (Windows, Linux, UNIX), support for custom applications or databases, update of Snapshot copies to SnapMirror and SnapVault secondary destinations, virtualization with VMware, and support for enterprise applications (Microsoft SQL Server, Oracle)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ FAS and All Flash FAS: Included in Premium Bundle</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ ONTAP Select and ONTAP Cloud: A la carte license, charged on the used storage capacity that is managed by SnapCenter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Advanced - Optional license support for NAS shares backup to the cloud using AltaVault, and file catalog</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Data Fabric Solution for Cloud Backup features in SnapCenter require the Advanced license.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FAS, All Flash FAS, ONTAP Select, ONTAP Cloud: A la carte license, charged on the used storage capacity that is managed by SnapCenter</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you are using ONTAP Select or ONTAP Cloud, you must have a SnapCenter Standard license before you can add a SnapCenter Advanced license.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A 90 days trial license is available for both SnapCenter standard and advanced licenses.</td>
<td></td>
</tr>
<tr>
<td>Protocols</td>
<td>The following licenses are required:</td>
<td>On source storage systems. Required on SnapMirror destination systems to serve data if a source volume is unavailable.</td>
</tr>
<tr>
<td></td>
<td>• For LUNs, the iSCSI or FC license</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For SMB shares, the CIFS license</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For NFS-type VMDKs, the NFS license</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For VMFS-type VMDKs, the iSCSI or FC license</td>
<td></td>
</tr>
</tbody>
</table>

**Related information**

*Data Fabric Solution for Cloud Backup*
SnapCenter repository identification

The SnapCenter repository, sometimes referred to as the NSM database, stores information and metadata for every aspect of SnapCenter. You should understand your database needs before installing SnapCenter.

When you install SnapCenter for the first time, MySQL Server is deployed as the dedicated database for the repository. If you have SQL Server database installed and you are upgrading to SnapCenter 2.0, SnapCenter continues to use SQL Server as the database repository.

If MySQL Server is already present on the host, it is detected by SnapCenter, and, if necessary, is upgraded to the correct version of MySQL Server.

**Note:** If there is an existing application that relies on a specific version of MySQL Server, that should be resolved before installing SnapCenter.

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

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.

SnapCenter does not support other types of load balancing.

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](#)

For new SnapCenter installations, MySQL Server database is installed automatically. You must use the same MySQL Server database from all NLB nodes. Optionally, you can choose an external
Microsoft SQL Server database for storing SnapCenter data. Choosing the external repository enables you to use a high availability configuration for the SnapCenter database.

**Note:** If you choose the external SQL Server database option, you cannot use the Data Fabric Solution for Cloud Backup feature in SnapCenter.

For SnapCenter upgrade installations, you can use an SQL Server (not SQL Express) database for NLB deployments.

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, resource group creation and host removal operations fail.

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

**Related information**

*SnapCenter Software 2.0 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
- External Cache module

Additionally, ARR requires the following:

- .NET 3.5 and .NET 4.5.2
- Wildcard-based, self-signed certificate created and used across all servers
- A rule configured in the Web Server to avoid request-forward looping
You can ignore the message “Ready for load balancing” on servers. This message has a value of Yes only when applications are provisioned in IIS using the Web Farm Network.

For more information, see the following Microsoft documentation:

- *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.

<table>
<thead>
<tr>
<th>Required information</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Request Routing</td>
<td>You must decide whether you want to enable and install ARR.</td>
</tr>
<tr>
<td>(ARR)</td>
<td></td>
</tr>
<tr>
<td>Network Load Balancing</td>
<td>If you want to enable NLB, you must know whether you want to create an NLB cluster or join an existing cluster.</td>
</tr>
<tr>
<td>(NLB)</td>
<td>If you want to create an NLB cluster, you must obtain the following information:</td>
</tr>
<tr>
<td></td>
<td>• Cluster name:</td>
</tr>
<tr>
<td></td>
<td>• Cluster primary IP:</td>
</tr>
<tr>
<td></td>
<td>• Interface name:</td>
</tr>
<tr>
<td></td>
<td>If you want to join an existing NLB cluster, you must obtain the following information:</td>
</tr>
<tr>
<td></td>
<td>• NLB node IP:</td>
</tr>
<tr>
<td></td>
<td>• Interface name:</td>
</tr>
<tr>
<td></td>
<td>You can preconfigure NLB before installing SnapCenter.</td>
</tr>
<tr>
<td>Credentials</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Account (Domain\User):</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
<tr>
<td></td>
<td>If you have entered a certificate in the 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:</td>
</tr>
<tr>
<td></td>
<td>• Certificate Friendly Name:</td>
</tr>
<tr>
<td>Required information</td>
<td>Your value</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ports</td>
<td>The default ports are as follows:</td>
</tr>
<tr>
<td></td>
<td>• SnapCenter HTTPS port: 8146 (default)</td>
</tr>
<tr>
<td></td>
<td>• SMCore HTTPS communication port: 8145 (default)</td>
</tr>
<tr>
<td></td>
<td>Make sure you specify the correct port numbers. To change a port number, you must reinstall SnapCenter.</td>
</tr>
<tr>
<td></td>
<td>If you specify a custom port when you install SnapCenter, you must add a firewall rule on the plug-in host for that port for the SnapCenter plug-in loader (SPL).</td>
</tr>
<tr>
<td></td>
<td>For additional details, see connection and port requirements.</td>
</tr>
<tr>
<td>MySQL Server settings</td>
<td>If you are using MySQL Server as the SnapCenter database repository, you must specify the following settings:</td>
</tr>
<tr>
<td></td>
<td>• User name: root</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
<tr>
<td>SQL Server settings</td>
<td>If you are upgrading to SnapCenter 2.0 and you are using SQL Server, you must specify the following SQL Server settings:</td>
</tr>
<tr>
<td></td>
<td>• Database server:</td>
</tr>
<tr>
<td></td>
<td>Specify “server\instance” or “server” if the instance is the default.</td>
</tr>
<tr>
<td></td>
<td>• Authentication mode:</td>
</tr>
<tr>
<td></td>
<td>• User name:</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
<tr>
<td>File catalog for NAS file services settings</td>
<td>If you use SnapCenter to manage protection of NAS files services, and you want to configure indexing on one of more file catalog servers, you must specify the following settings:</td>
</tr>
<tr>
<td></td>
<td>• File catalog server:</td>
</tr>
<tr>
<td></td>
<td>Configure one or more file catalog servers, specify the following information for each:</td>
</tr>
<tr>
<td></td>
<td>• Server IP address\host name:</td>
</tr>
<tr>
<td></td>
<td>• Port: 8145</td>
</tr>
<tr>
<td></td>
<td>• OS user name:</td>
</tr>
<tr>
<td></td>
<td>• Password:</td>
</tr>
</tbody>
</table>

For more information about Data Fabric Solution for Cloud Backup and NAS file services, see the *Data Fabric Solution for Cloud Backup Workflow Guide Using ONTAP, SnapCenter and AltaVault.*

*Data Fabric Solution for Cloud Backup*

**Related references**

*Connection and port requirements* on page 30
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.

You can optionally 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 38
   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 40
   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 41
   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 those users.

4. **Setting up storage system connections** on page 51
   Before you can perform backup, restore, clone, and provisioning operations with SnapCenter, you must set up the storage system connections that give SnapCenter access to ONTAP storage. If you are configuring connections for the Data Fabric Solution for Cloud Backup, you must create connections to each AltaVault system and one to an ONTAP Cluster.

5. **Setting up Run As credentials** on page 54
   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 57
   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.

Related information

*SnapCenter Software 2.0 Windows Cmdlet Reference Guide*
*SnapCenter Software 2.0 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 the installation worksheet.
- 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 Windows Installer logging. https://support.microsoft.com/en-us/kb/223300

• The SnapCenter Server must be installed on a server that is part of a domain. Note: SnapCenter Server cannot be installed on a domain controller.

• 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, multi-domain forests, and cross-domain trusts are supported, cross-forest domains are not supported. See Microsoft documentation about Active Directory Domains and Trusts. 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:

```
SnapCenterversion.exe /debuglog"DirPath\LogFileName"
```

   For example,

```
SnapCenter2.0.exe /debug"c:\snapcenterlog.txt"
```

   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.

3. If you use SnapCenter to manage protection of NAS file services in the Data Fabric Solution for Cloud Backup, and you want to configure indexing on one of more file catalog servers, specify the following settings:
   • File catalog server:
       Configure one or more file catalog servers.
       Note: File catalog servers can only be configured during SnapCenter installation.

       Specify the following information for each file server:
   • Server IP address/host name:
   • Port: 8145
   • OS user name:
   • Password:
Data Fabric Solution for Cloud Backup

Related references

SnapCenter installation worksheet on page 36

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

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

Attention: Closing just the SnapCenter browser tab does not log you off of SnapCenter if you have multiple tabs open in your web browser. If you need to comply with security requirements, you must log off of SnapCenter either by clicking the Sign out button or shutting down the entire web browser.

Attention: Do not allow your browser to save your SnapCenter password.

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 the following interfaces depending on the SnapCenter plug-in:

• PowerShell cmdlets on Windows hosts to perform data protection operations.
• SnapCenter command-line interface (CLI), such as sccli for Oracle databases on Linux machines to script configuration and data protection operations.

Note: Some cmdlets have changed in SnapCenter 2.0. If you use cmdlets in older versions of SnapCenter scripts, you might need to update your scripts.

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. Enter your user credentials:

   Domain\UserName

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

   Your current user and associated role are shown in the upper right of SnapCenter.
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 those 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 selected users are able to access SnapCenter.

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

- SnapCenter RBAC
- Application-level RBAC
- 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. Users are also required to provide authentication to run the APIs.

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. If you want to perform Snapshot copy and data protection operations in a Windows file system environment on ONTAP storage, the SnapCenter admin role must have admin privileges.
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.

**ONTAP permissions**

You should ensure that you have vsadmin account permissions to access the storage system.

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*

**ONTAP CLI commands for creating SVM roles**

There are several ONTAP CLI commands you must run when you create a role for a new SVM user in ONTAP. This role is required if you configure SVMs in ONTAP to use with SnapCenter.

**ONTAP CLI command list**

<table>
<thead>
<tr>
<th>Command to run</th>
</tr>
</thead>
<tbody>
<tr>
<td>security login role create -role SVM_Role_Name -cmddirname &quot;event generate-autosupport-log&quot; - vserver SVM_Name -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;job history show&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;job stop&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun delete&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun create&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun igroup add&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun igroup create&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun igroup delete&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun igroup rename&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun igroup show&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun mapping add-reporting-nodes&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun mapping create&quot; -access all</td>
</tr>
<tr>
<td>Command to run</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun mapping delete&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun mapping remove-reporting-nodes&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun mapping show&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun modify&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun move-in-volume&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun offline&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun online&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun resize&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun serial&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;lun show&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;network interface&quot; -access readonly</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;network interface show&quot; -access readonly</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;snapmirror policy add-rule&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;snapmirror policy modify-rule&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;snapmirror policy remove-rule&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;snapmirror policy show&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;snapmirror restore&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;snapmirror update&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;snapmirror update-ls-set&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;version&quot; -access all</td>
</tr>
</tbody>
</table>
**Command to run**

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume clone create&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume clone show&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume clone split start&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume clone split stop&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume create&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume destroy&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume file clone create&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume file show-disk-usage&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume modify&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume offline&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume online&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume qtree create&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume qtree delete&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume qtree modify&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume qtree show&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume restrict&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume show&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume snapshot create&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume snapshot delete&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume snapshot modify&quot; -access all</code></td>
</tr>
<tr>
<td><code>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume snapshot rename&quot; -access all</code></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command to run</th>
</tr>
</thead>
<tbody>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume snapshot restore&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume snapshot restore-file&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume snapshot show&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;volume unmount&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver cifs share create&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver cifs share delete&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver cifs share show&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver cifs share show&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver export-policy create&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver export-policy delete&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver export-policy rule create&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver export-policy rule show&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver export-policy show&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver iscsi connection show&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver show&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver&quot; -access readonly</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver export-policy&quot; -access all</td>
</tr>
<tr>
<td>security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname &quot;vserver iscsi&quot; -access all</td>
</tr>
</tbody>
</table>
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:

- Resource Group
- Policy
- Backup
- Host
- Storage Connection
- Clone
- Provision (only for Microsoft SQL database)
- Dashboard
- Reports
- Restore
  - Full Volume Restore (only for Custom Plug-ins)
- Resource
  - Plug-in privileges are required from the administrator for non-administrators to perform resource 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)
- Catalog (only for NAS File Services)

**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 Storage Connection permission enables users to create SVM connections.

For example, a user with the SnapCenter Admin role can create SVM connections 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 SVM connections. 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.

**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.

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Enabled</th>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Group</td>
<td>Not applicable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy</td>
<td>Not applicable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup</td>
<td>Not applicable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Host</td>
<td>Not applicable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage Connection</td>
<td>Not applicable</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Clone</td>
<td>Not applicable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Provision</td>
<td>Not applicable</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Dashboard</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Reports</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Restore</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Resource</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Plug-in Installation</td>
<td>No</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Migration</td>
<td>No</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Mount</td>
<td>Yes</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>
### Permissions

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Enabled</th>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unmount</td>
<td>Yes</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Full Volume Restore</td>
<td>No</td>
<td>No</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Enabled</th>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Group</td>
<td>Not applicable</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Policy</td>
<td>Not applicable</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Backup</td>
<td>Not applicable</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Host</td>
<td>Not applicable</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Storage Connection</td>
<td>Not applicable</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Clone</td>
<td>Not applicable</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Provision</td>
<td>Not applicable</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Dashboard</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Reports</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Restore</td>
<td>No</td>
<td>No</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Resource</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Plug-in Installation</td>
<td>No</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Migration</td>
<td>No</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Mount</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Unmount</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Full Volume Restore</td>
<td>No</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>
Infrastructure Admin role

The Infrastructure Admin role has permissions enabled for host management, storage management, provisioning, resource groups, remote installation reports, and access to the Dashboard. This role also enables resource group, backup, restore, and catalog permissions for NAS File Services management.

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Enabled</th>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Group</td>
<td>Not applicable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy</td>
<td>Not applicable</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup</td>
<td>Not applicable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Host</td>
<td>Not applicable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage Connection</td>
<td>Not applicable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Clone</td>
<td>Not applicable</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Provision</td>
<td>Not applicable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dashboard</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Reports</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Restore</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Resource</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Plug-in Installation</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Migration</td>
<td>No</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Mount</td>
<td>No</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Unmount</td>
<td>No</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Full Volume Restore</td>
<td>No</td>
<td>No</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

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. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Settings.
2. In the Settings page, click Roles.
3. In the Roles page, select the role to which you want to add the user.
4. Click Modify.
5. Click Next until you reach the Users/Groups page of the wizard.
6. In the Users/Groups page, specify the domain to which the user belongs.
7. 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.
8. Click Next to view the summary, and then click Finish.

Assigning users access to assets
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 the user access to SnapCenter assets, such as hosts and storage connections. This enables users to perform the actions for which they have permissions on the assets that are assigned to them.

About this task
You can assign access 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.

You can also assign Run As credential maintenance to a user.

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

You must use the Admin role to assign permissions to Plug-in for VMware vSphere.

Steps
1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Settings.
2. In the Settings page, click SnapCenter Assets.
3. In the User Access page, select the type of asset you want to assign from the Asset drop-down list.
4. In the Asset table, select the asset and click Assign.
5. Provide the domain name to which the user or group belongs.
6. Choose whether you want to assign access 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 access to all the required assets.

9. Click OK to save your changes.

Related tasks

Adding resources to SnapCenter Custom Plug-ins on page 71

Setting up storage system connections

Before you can perform backup, restore, clone, and provisioning operations with SnapCenter, you

must set up the storage system connections that give SnapCenter access to ONTAP storage. If you are

configuring connections for the Data Fabric Solution for Cloud Backup, you must create connections
to each AltaVault system and one to an ONTAP Cluster.

Before you begin

• You must have permissions in the Infrastructure Admin role to create storage connections.

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

• Storage system names must be unique
SnapCenter does not support multiple storage systems with the same name on different clusters.
Each storage system supported by SnapCenter must have a unique name.

About this task

If you are planning to replicate Snapshot copies to a SnapMirror or SnapVault destination, make sure
to set up storage system connections for the destination Storage Virtual Machine (SVM) as well as
the source SVM.

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click

Storage Systems.

2. In the Storage Systems page, click New.
3. In the **New Storage Connection** wizard, provide the following information:

<table>
<thead>
<tr>
<th>For this field…</th>
<th>Do this…</th>
</tr>
</thead>
</table>
| Storage System  | Enter the storage system name or IP address.  
**Note:** Storage system names, not including the domain name, must be 15 characters or fewer. To create storage system connections with names with more than 15 characters, you can use the `Add-SmStorageConnection` PowerShell cmdlet.  
SnapCenter does not support multiple SVMs with the same name on different clusters. Each SVM supported by SnapCenter must have a unique name. |
| User name/Password | Do one of the following:  
  - ONTAP: Enter the credentials used (usually vsadmin) to access the storage system.  
  - AltaVault: Enter the role-based access control credentials you entered in AltaVault. |
## For this field... | Do this...
---|---
**Storage Type** | Select ONTAP SVM, ONTAP Cluster, or AltaVault.  
If you are configuring connections for SnapCenter application plug-ins, choose ONTAP SVM as the storage type.  
If you are configuring connections for the Data Fabric Solution for Cloud Backup, you must add connections to each AltaVault system and to an ONTAP Cluster. For each AltaVault system, choose AltaVault as the storage type, and choose ONTAP Cluster as the second storage type.  
**Note:** If you add a new ONTAP SVM connection and you have already added an ONTAP Cluster for the Data Fabric Solution for Cloud Backup, after you add the SVM, you must run the **Modify Storage Connection** wizard on the ONTAP Cluster that you already added to ensure the following updates are made:  
- The SVM is in the NSM database  
- CIFS server discovery is enabled on the SVM  
- The SnapCenter cache is updated with information about the new SVM

**Site** | Applicable only if you choose ONTAP Cluster or AltaVault as your storage type. Enter the physical site name, for example, the data center city. The site you enter is displayed in the SnapCenter interface.

**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.  
If you are configuring the AltaVault connection, enter the AltaVault port.

**Timeout** | Applicable only if you choose ONTAP Cluster or ONTAP SVM as the storage type. 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 then enter the preferred IP address for SVM connections.

**Note:** If you have more than one iSCSI or FC session configured per SVM connected to the host, then use the host device for multipathing rather than using the native device. While performing a restore, clone, mount, or backup verification operation, if the storage system and the host have iSCSI and FC configured together, then FC is preferred.

*ONTAP 9 Cluster Management Using OnCommand System Manager*

### 5. Applicable only if you choose ONTAP Cluster or ONTAP SVM as the storage type. If you want to have Event Management System (EMS) messages sent to the storage system syslog or have AutoSupport messages sent to the storage system for failed operations, select the appropriate check box.
When you select the AutoSupport check box, the EMS messages check box is also selected because EMS messaging is required to enable AutoSupport notifications.

6. 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 credentials

Run As credentials use different authentication methods depending upon the application or environment. Run As credentials authenticate users so they can perform SnapCenter operations. You should create one set of Run As credentials for installing plug-ins and another set for data protection 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.

RMAN catalog authentication

The RMAN catalog authentication method authenticates against the Oracle Recovery Manager (RMAN) catalog database. If you have configured an external catalog mechanism and registered your database to catalog database, you need to add RMAN catalog authentication.
Related tasks

*Setting up your Run As credentials* on page 55

**Setting up your Run As credentials**

SnapCenter uses Run As credentials to authenticate users for SnapCenter operations. You should create Run As credentials for installing SnapCenter plug-ins and additional Run As credentials for performing data protection operations on databases or Windows file systems.

**About this task**

- **Linux hosts**
  
  You must set up Run As credentials for scheduling on Linux hosts.
  
  Although you are allowed to create Run As credentials for Linux after deploying hosts and installing plug-ins, the best practice is to create Run As credentials after you add SVMs, before you deploy hosts and install plug-ins. You must set up the Run As credentials for the root user or a non root user who has sudo privileges to install and start the plug-in process.

- **Windows hosts**
  
  You must set up Windows Run As credentials before installing plug-ins.
  
  Set up the Run As credentials with administrator privileges, including administrator rights on the remote host.

- **SQL authentication on Windows hosts**
  
  You must set up SQL Run As credentials after installing plug-ins.
  
  If you are deploying SnapCenter Plug-in for Microsoft SQL Server, you must set up SQL Run As credentials after installing plug-ins. Set up a Run As credential for a user with SQL Server sysadmin permissions.
  
  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.

- **Custom Plug-ins applications**
  
  The plug-in uses the Run As credentials selected or created when adding a resource. If a resource does not require a Run As credentials during data protection operations, you can set the Run As credentials as *None*.

- **For Data Fabric Solution for Cloud Backup for CIFS shares only (not for NFS), you must create Run As credentials and configure a CIFS server for the ONTAP cluster.**

**Steps**

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click **Settings**.

2. In the **Settings** page, click **Run As Credentials**.

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

<table>
<thead>
<tr>
<th>For this field…</th>
<th>Do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run As name</td>
<td>Enter a name for the Run As credentials.</td>
</tr>
<tr>
<td>Username/Password</td>
<td>Enter the user name and password used for authentication. You must add the domain name as the prefix to the username.</td>
</tr>
<tr>
<td>Authentication Mode</td>
<td>Select the authentication mode that you want to use. If you select the SQL authentication mode, you must also specify the SQL server instance and the host where the SQL instance is located. For Data Fabric Solution for Cloud Backup for CIFS shares only, select Windows as the mode.</td>
</tr>
<tr>
<td>Use sudo privileges</td>
<td>Applicable to Linux users only. Select the Use sudo privileges check box if you are creating run as credentials for a non-root user.</td>
</tr>
</tbody>
</table>

5. Click OK.

After you finish

After you finish setting up Run As credentials, you might want to assign Run As credential maintenance to a user or group of users on the My SnapCenter Assets page.

Related concepts

Authentication methods for your Run As credentials on page 54
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.

Prerequisites to adding hosts and installing plug-in packages

Before you add a host and install the plug-ins packages, you must complete all the requirements.

General

If you are using iSCSI, the iSCSI service must be running.

Windows hosts

- You must have a domain user with local administrator privileges with local login permissions on the remote host.
- If you manage cluster nodes in SnapCenter, you must have a user with administrative privileges to all the nodes in the cluster.
- 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 import 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.

Linux hosts

- You must have enabled the password-based SSH connection for the root or non-root user.
  From SnapCenter 2.0, SnapCenter Plug-in for Oracle Database can be installed by a non-root user. However, you must configure the sudo privileges for the non-root user to install and start the plug-in process.
- You must have installed Java 1.7 or 1.8, 64-bit, on your Linux host.
  Java Downloads for All Operating Systems
- For Oracle databases that are running on a Linux host, you must install both SnapCenter Plug-in for Oracle Database and SnapCenter Plug-in for UNIX.
  Note: You can use the Plug-in for Oracle Database to manage Oracle databases for SAP as well. However, SAP BR*Tools integration is not supported.
Virtualized databases and virtualized Windows file systems

- You must have installed either SnapCenter Plug-in for VMware vSphere or Virtual Storage Console for VMware vSphere (VSC) (but not both) if you want to use SnapCenter to manage applications residing on virtual machine disk file (VMDK) or raw device mapping (RDM) configurations.

- If you install SnapCenter Plug-in for VMware vSphere, you must have a user with SnapCenter Admin privileges.

- If you install VSC, you must use the VSC GUI to register SnapCenter. VSC is a vCenter Server plug-in and is not included in the SnapCenter installation.

- If your VMs are on UTF-8 qtree datastores and you are using VSC 6.2.1 or earlier, restore operations from SnapMirror or SnapVault destinations are not supported.

Custom Plug-ins

- You must have created the custom plug-in for your application by referring to the Custom Plug-ins Developer’s Guide.

- If you want to manage MySQL or DB2 applications, you must download the MySQL and DB2 Custom Plug-ins that are provided by NetApp.

- You must have installed Java 1.7 or 1.8, 64-bit, on your Linux and Windows host.

Related concepts

Determine which virtualized application plug-in you need to install on page 29

Related tasks

Configuring sudo privileges for non-root user on page 58

Configuring sudo privileges for non-root user

SnapCenter 2.0 enables a non-root user to install the Plug-in for Oracle Database and start the plug-in process. However, you must configure sudo privileges for the non-root user to provide access to several paths. You can configure sudo privileges for the non-root user also if you deploy SnapCenter in the Data Fabric Solution for Cloud Backup, since the file catalog uses a Linux server.

About this task

You must configure sudo privileges for the non-root user to provide access to the following paths:

- /tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin
- /opt/NetApp/snapcenter/spl/installation/plugins/uninstall
- /opt/NetApp/snapcenter/spl/bin/spl

Steps

1. Create a key by running the following command:
   ```bash
dgst -binary -sha224 /tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin | openssl base64
   ```

2. Open the /etc/sudoers file by running the visudo command.

   You must use Sudo 1.8.7 or later.

3. Edit the file to include the non-root user name:
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 adding a host** on page 59
- **Actions you should complete while adding a host** on page 60
- **Actions you should complete to configure a backup for a newly added host** on page 62

If one person is deploying the plug-in packages and performing all tasks, that person 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 adding a host**

<table>
<thead>
<tr>
<th>Actions</th>
<th>Steps</th>
<th>Notes</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Storage Virtual Machines</td>
<td>1. Select Storage Systems.</td>
<td>Add a connection for each SVM that backs storage for the host.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Click New to add an SVM.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: The **Use sudo privileges** checkbox is selected by default for non-root users.
### Actions you should complete while adding a host

Before you complete actions in this checklist, you must complete the actions required before adding hosts.

<table>
<thead>
<tr>
<th>Actions</th>
<th>Steps</th>
<th>Notes</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Run As credentials</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Select <strong>Settings &gt; Run As Credentials</strong>.</td>
<td>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. 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>New</strong> to add a Run As credential.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install and register VSC if you are adding a host VM</td>
<td>1. Install Virtual Storage Console for VMware vSphere (VSC)</td>
<td>To protect VMs in addition to virtualized resources (SQL Server, Oracle, and Windows file systems), you must install and register VSC. If you are protecting only virtualized resources, then deploy SnapCenter Plug-in for VMware vSphere in the next step; there is no need to install VSC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Register SnapCenter using the VSC interface <strong>Configure SnapCenter Server</strong> dialog box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actions</td>
<td>Steps</td>
<td>Notes</td>
<td>Complete?</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>-------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| Add host and deploy plug-in packages | 1. Select **Hosts** > **Managed Hosts** > **Add**.  
2. Complete the wizard to initiate plug-in package deployment. | 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. If you add a cluster (Windows Server Failover Clustering (WSFC), Oracle real application clusters (RAC)), or SQL Always On Availability Groups, SnapCenter performs a remote installation on all cluster nodes. | |
| Monitor plug-in package installation status | 1. Select **Monitor** > **Jobs**.  
2. Wait until the plug-in package installation job finishes, which might take several minutes. | After this process finishes, the plug-in package is installed on the remote host. | |
| Add resources (only if you are using Custom Plug-ins) | 1. Select **Resources** > **Add Resources**.  
2. Complete the wizard to add resources to Custom Plug-ins. | After this process finishes, resources will be available for data protection operations. | |
| Configure the plug-in log directory and verification server (only if you are using Plug-in for SQL Server) | 1. Select **Hosts** > **Managed Hosts**.  
2. Select the host and click **Configure Plugin**.  
3. Complete the wizard. | The log directory shows only NetApp LUNs. | |
### Actions you should complete to configure a backup for a newly added host

<table>
<thead>
<tr>
<th>Actions</th>
<th>Steps</th>
<th>Notes</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a backup policy</td>
<td>1. Select <strong>Settings &gt; Policies &gt; New</strong>.</td>
<td>You can copy an existing policy.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Backup</strong> and complete the wizard.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create a backup resource group</td>
<td>1. Choose a plug-in, and then click <strong>Resource Group &gt; New Resource Group</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Select <strong>Resources</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Complete the wizard, selecting resources from the newly added host.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup now</td>
<td>1. Select <strong>Resources &gt; Resource Group</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Select the newly added resource group and click <strong>Backup Now</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Select a policy from the drop-down list and click <strong>Backup</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitor backup progress</td>
<td>1. Select <strong>Monitor &gt; Jobs</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Monitor the backup job for completion.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Related concepts**

*Determine which virtualized application plug-in you need to install* on page 29

**Related tasks**

*Installing plug-ins on multiple remote hosts using cmdlets* on page 67

### Adding hosts and installing plug-in packages on remote hosts

You must use the Add Host wizard to add hosts 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 be a user that is assigned to a role that has the plug-in install and uninstall permissions, such as the SnapCenter Admin.
About this task

You can use the plug-in deployment check list to help you complete this task.

You can choose one of the following types of hosts:

- Windows host
- Linux host
- vSphere host

For information about using the VSC GUI, see the VSC documentation.

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

If you are installing SnapCenter Plug-in for VMware vSphere, you must consider the following requirements:

- Install the plug-in on a dedicated Windows host (virtual or physical).
- Do not install other plug-ins on the SnapCenter Plug-in for VMware vSphere host.
- Do not install the plug-in on the SnapCenter Server.
- Do not install the plug-in on the vCenter Server.

**Note:** SnapCenter Plug-in for VMware vSphere used with VSC 6.2Px does not support IPV6. Therefore, NFS mount and restore operations from IPV6 LIFs are not supported.

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

**Note:** You do not need to install SnapCenter Plug-in for VMware vSphere or Virtual Storage Console for VMware vSphere in the following scenarios:

- Your SQL Server environment uses an in-guest iSCSI initiator
- Your Oracle environment uses NFS or an in-guest iSCSI initiator

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.

2. Verify that Managed Hosts is selected at the top.

3. Click Add:
4. On the **Hosts** page, do the following:

<table>
<thead>
<tr>
<th>For this field…</th>
<th>Do this…</th>
</tr>
</thead>
</table>
| Host name       | Enter the fully qualified domain name (FQDN) or the IP address of the host. SnapCenter depends on the proper configuration of the DNS. Therefore, the best practice is to enter the fully qualified domain name (FQDN). You can enter one of the following:  
  - 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.  
  - IP address or FQDN of the SQL Availability Groups  
If you are adding a host using SnapCenter and it is part of a subdomain, you must provide the FQDN. |
<table>
<thead>
<tr>
<th>For this field…</th>
<th>Do this…</th>
</tr>
</thead>
</table>
| Type           | Select the type of host:  
|                | • Windows  
|                | SnapCenter Server adds the host and then installs the Plug-in for Windows if it is not already installed on the host.  
|                | If you also select the Microsoft SQL Server option on the Plug-ins page, SnapCenter Server also installs the Plug-in for SQL Server.  
|                | • Linux  
|                | SnapCenter Server adds the host and then installs on the host the Plug-in for Oracle Database Database and the Plug-in for UNIX if they are not already installed.  
|                | • vSphere  
|                | SnapCenter Server adds the host and then installs on the host the SnapCenter Plug-in for VMware vSphere, if it is not already installed, to facilitate data protection operations for virtualized applications. The SnapCenter Server establishes communication with vCenter, using the vCenter information provided on the Plug-ins page.  
|                | **Note:** If you are using VSC to manage VMs in addition to virtualized applications, do not use SnapCenter to add hosts. Instead, you must install VSC separately and then use the VSC interface to register with SnapCenter. |
| Run As credentials | Select the Run As credential that you created or create new Run As credentials.  
|                  | The credential must have administrative rights on the remote host. For details, see information about creating a Run As credential. Details about Run As credentials, including the user name, domain, and host type, are displayed by placing your cursor over the Run As credential name you provided.  
|                  | **Note:** Run As credentials authentication mode is determined by the host type you specify in the Add Host wizard. |
| Port            | Either retain the default port number or enter the port number. The default port number is 8145. |
| Add all hosts in the cluster | Select this to add all the cluster nodes in an Oracle RAC, WSFC, or SQL Availability Groups. |

5. On the **Discover plug-ins** page, review the plug-in packages on the host.  
   For new deployments, no plug-in packages are listed.

6. On the **Plug-ins** page, do the following actions:
<table>
<thead>
<tr>
<th>For plug-in packages...</th>
<th>Do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnapCenter Plug-ins Package for Windows</td>
<td>On the Plug-ins page, select the plug-in package and enter the plug-in ports and installation path.</td>
</tr>
<tr>
<td>SnapCenter Plug-ins Package for Linux</td>
<td></td>
</tr>
</tbody>
</table>
| SnapCenter Plug-in for VMware vSphere | • SnapCenter Plug-ins Package for Windows  
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.  
• SnapCenter Plug-ins Package for Linux  
For SnapCenter Plug-ins Package for Linux, the default path is /opt/NetApp/snapcenter.  
**Note:** You cannot change the path for Linux.  
• SnapCenter Plug-in for VMware vSphere  
For SnapCenter Plug-in for VMware vSphere, the default path is C:\Program Files\NetApp\SnapCenter. However, if you want, you can customize the default path. Enter the requested vCenter information to allow SnapCenter Plug-in for VMware vSphere to complete VMDK discovery. |

**SnapCenter Custom Plug-ins**

b. Click **Upload**.  
The descriptor xml file in the zipped custom plug-in folder is validated before uploading the package.  
If you want to manage MySQL or DB2 applications, you can use the MySQL and DB2 custom plug-ins that are provided by NetApp. The MySQL and DB2 custom plug-ins are available at [website name or URL]. |

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

**After you finish**

After you finish, you should monitor the installation progress. Refresh the Hosts page after a few minutes to see the newly added host.

**Note:** If you are installing a vSphere host, the SnapCenter Plug-in for VMware vSphere does not validate the vCenter information you provide before adding the host. If the vCenter information is not correct, the add host operation completes and a warning is displayed for the "Registering vCenter details with SnapCenter Plug-in for VMware vSphere" task. You can update the vCenter information for that host from the Hosts page.

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 on 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 41
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 those users.

Related tasks

*Setting up your Run As credentials* on page 55
*Registering VSC for VMware vSphere with SnapCenter* on page 98

Related references

*SnapCenter licensing requirements* on page 32
*Registering vCenter details task displays a warning* on page 123

### Installing plug-ins on multiple remote hosts using cmdlets

If you want to install SnapCenter plug-in packages on multiple hosts at one time, you can do so by using the `Install-SmHostPackage` PowerShell 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:
   ```powershell
   Open-SMConnection
   ```
3. From the command prompt, enter the following:
   ```powershell
   Install-SmHostPackage
   ```

**Example**

```powershell
Install-SmHostPackage -HostNames @("10.231.72.165","10.231.72.99")
-ApplicationCode SCO -FilesystemCode SCU -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:

- SCSQL
- SCO
- SCV
• Name of the custom plug-in, for example: HRPlug-in

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 credentials for remote installation.

Increasing the remote plug-in installation process timeout
You can increase the remote plug-in installation timeout from the default of 10 minutes by using the Set-SmConfigSettings cmdlet. You might want to do this if your plug-in package installation, upgrade, or uninstallation is failing with the message “Process timed out and was killed on server: hostname.”

Steps
1. Launch PowerShell.
2. From the SnapCenter Server command prompt, enter the following command and enter your credentials:
   ```
   Open-SMConnection
   ```
3. Display the current remote installation process timeout by entering the following command:
   ```
   Get-SmConfigSettings -Server -Key WindowsRemoteInstallProcessTimeout
   ```
4. Increase the remote installation process timeout by entering the Set-SmConfigSettings command:
   ```
   Set-SmConfigSettings -Server -configSettings @{"WindowsRemoteInstallProcessTimeout"="900"}
   ```
   The remote installation process timeout is increased to 15 minutes.

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, select the appropriate plug-in from the drop-down list, and then click Monitor.

2. In the Monitor page, click Jobs.

3. On the Jobs page, to filter the list so that only plug-in installation operations are listed, do the following:
   a. Click Filter.
   b. Optional: 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 Apply.

4. Select the installation job and click Details to view the job details.

5. In the Job Details page, click View logs.

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 or clone 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.

Before you begin
- 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).
- If you are using a remote verification server, an iSCSI or FC connection must already exist for that host.

Steps
1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.

2. In the Hosts page, click Managed Hosts.

3. From the Managed Hosts page, select an SQL host, and click Configure Plug-in to open the Configure Plug-in wizard.

4. On the Configure host log directory page, click Browse and complete the following steps:
Only NetApp LUNs (drives) are listed for selection. SnapCenter backs up and replicates the host log directory as part of the backup operation.

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

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:

- Select the SQL host and instance that you want to use for verification.
- Select the appropriate **Run As** credential to perform the operation.
- Choose the maximum job count and mount point options. The maximum job count you can specify is 5.
- Click **Apply**, and then click **Next**.
6. Review your settings, and click Finish.

Related tasks

Identifying available resources on page 71

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 resource groups 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.

About this task

SnapCenter Custom Plug-ins does not allow you to refresh resources.

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Resources.

2. From the drop-down list, select the application (Oracle Database or SQL Server or Windows File System) 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.

Adding resources to SnapCenter Custom Plug-ins

You must add resources that you want to backup or clone. Depending on your environment, resources might be database instances or collections that you want to back up or clone.

Before you begin

- You must have completed tasks such as installing the SnapCenter Server, adding hosts, creating storage system connections, and adding “Run As” credentials.

- You must have created a custom plug-in. For details, see the Developer Guide for Creating Custom Plug-ins.

- You must have uploaded the plug-ins to SnapCenter Server. For details, see the SnapCenter Software 2.0 Installation and Setup Guide.

About this task

You can also add resources for MySQL and DB2 applications. These plug-ins can be downloaded from the NetApp Tool Chest.

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Resources.

2. In the Resources page, click Add Resource.
3. In the **Provide Resource Details** page, perform the following actions:

<table>
<thead>
<tr>
<th>For this field...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the resource.</td>
</tr>
<tr>
<td>Host name</td>
<td>Select the host.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type. Type is user defined as per the plug-in description file. For example, database, instance. In case the type selected has a parent, enter the parent details. For example: If the type is Database and the parent is Instance, enter the Instance details.</td>
</tr>
<tr>
<td>Run As name</td>
<td>(Optional) Select Run as or create a new Run As account.</td>
</tr>
<tr>
<td>Mount Points</td>
<td>Enter the mount paths where the resource is mounted. This is applicable only for Windows host.</td>
</tr>
</tbody>
</table>

4. In the **Provide Storage Footprint** page, select a storage system and choose one or more volumes, LUNs and Qtrees and click **Save**.

(Optional) Click , to add more volumes, LUNs, and Qtrees from other storage systems.

**Note:** SnapCenter Custom Plug-ins does not support auto discovery of the resources and the storage details for physical and virtual environment. You must provide the storage information for physical and virtual environments while creating the resources.
5. In the **Resource Settings** page, provide custom key-value pairs for the resource.

Use the custom key-value pairs if you want to pass resource specific information. For example, when you are using MySQL plug-in, you can specify a master-slave configuration as

```
MASTER_SLAVE = “YES” or “NO” (name is MASTER_SLAVE and value is “YES” or “NO”).
```

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

**Result**

The resources are displayed along with information such as type, host or cluster name, associated resource groups and policies, and overall status.

**After you finish**

If you want to provide access to the assets to other users, SnapCenter administrator must assign assets to those users. This enables users to perform the actions for which they have permissions on the assets that are assigned to them.

**Related tasks**

- *Installing the SnapCenter Server* on page 38
  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.
- *Setting up your Run As credentials* on page 55
- *Assigning users access to assets* on page 50
Managing the SnapCenter Plug-in Loader service for Linux

The SnapCenter Plug-in Loader (SPL) service loads the plug-in package for Linux to interact with the SnapCenter Server. The SPL service is installed when you install the the SnapCenter Plug-ins Package for Linux.

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/NetApp/snapcenter/spl/etc/` contains the following parameters and the default values are assigned to these parameters.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOG_LEVEL</td>
<td>Displays the log levels supported. The possible values are INFO, DEBUG, TRACE, ERROR, FATAL, and WARN.</td>
</tr>
<tr>
<td>SPL_PROTOCOL</td>
<td>Displays the protocol supported by SPL. Only https protocol is supported. You can add the value if the default value is missing.</td>
</tr>
<tr>
<td>SNAPCENTER_SERVER_PROTOCOL</td>
<td>Displays the protocol supported by SnapCenter Server. Only https protocol is supported. You can add the value if the default value is missing.</td>
</tr>
<tr>
<td>SPL_KEYSTORE_PASS</td>
<td>Displays the password of the keystore file. You can change this value only if you change the password or create a new keystore file.</td>
</tr>
<tr>
<td>SPL_PORT</td>
<td>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. <strong>Note:</strong> You should not change value after installing the plug-ins for Linux.</td>
</tr>
<tr>
<td>SNAPCENTER_SERVER_HOST</td>
<td>Displays IP address or host name of the SnapCenter Server.</td>
</tr>
<tr>
<td>SPL_KEYSTORE_PATH</td>
<td>Displays the absolute path of the keystore file.</td>
</tr>
<tr>
<td>SNAPCENTER_SERVER_PORT</td>
<td>Displays the port number on which SnapCenter Server is running.</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SPL_LOGS_MAX_COUNT</td>
<td>Displays the number of SPL log files that are retained in the <code>/var/opt/snapcenter/spl/logs</code> folder. The default value is set to 5000. If the count is more than specified value, then the last modified 5000 files will be retained. The check for the number of files is done automatically every 24 hours from when SPL is started. <strong>Note:</strong> If you have manually deleted the <code>spl.properties</code> file then the number of files to be retained is 9999.</td>
</tr>
</tbody>
</table>

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
     ```
Preparing storage systems for SnapMirror and SnapVault replication

You can use a SnapCenter plug-in with ONTAP SnapMirror technology to create mirror copies of backup sets on another volume, and with 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, 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).

SnapCenter supports the management of version-flexible SnapMirror relationships. For details about version-flexible SnapMirror relationships and how to set them up, see the ONTAP documentation.

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).
- 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 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:

![Procedure for initializing 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).
- You must be a cluster administrator.
About this task

You can use the 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:

![SnapVault relationship diagram]

**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`:

   ```bash
   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`:

   ```bash
   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:

   ```shell
   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`:

   ```shell
   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:

   ```shell
   SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
   ```
Provisioning storage on Windows hosts

You can use SnapCenter to assign NetApp storage to Windows Server 2008 R2, 2012, 2012 R2, and 2016 hosts. Provisioning Windows hosts with SnapCenter ensures that the backups you create are application consistent. You must have installed and configured the SnapCenter Plug-ins Package for Windows.

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

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 ONTAP 9 SAN Configuration Guide.

Establishing an iSCSI session

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

Before you begin

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

ONTAP 9 SAN Administration Guide

About this task

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

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

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

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.
2. In the Hosts page, click iSCSI Session.
3. From the Storage Virtual Machine drop-down list, select the Storage Virtual Machine (SVM) for the iSCSI target.
4. From the Host drop-down list, select the host for the session.
5. Click Establish Session.

The Establish Session wizard is displayed.

6. In the Establish Session wizard, identify the target:
<table>
<thead>
<tr>
<th>In this field...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target node name</td>
<td>The node name of the iSCSI target</td>
</tr>
<tr>
<td></td>
<td>If there is an existing target node name, the</td>
</tr>
<tr>
<td></td>
<td>name is displayed in read-only format.</td>
</tr>
<tr>
<td>Target portal address</td>
<td>The IP address of the target network portal</td>
</tr>
<tr>
<td>Target portal port</td>
<td>The TCP port of the target network portal</td>
</tr>
<tr>
<td>Initiator portal address</td>
<td>The IP address of the initiator network portal</td>
</tr>
</tbody>
</table>

7. When you are satisfied with your entries, click **Connect**. SnapCenter establishes the iSCSI session.

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

**Disconnecting an iSCSI session**

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

**Steps**

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click **Hosts**.

2. In the **Hosts** page, click **iSCSI Session**.

3. From the **Storage Virtual Machine** drop-down list, select the Storage Virtual Machine (SVM) for the iSCSI target.

4. From the **Host** drop-down list, select the host for the session.

5. From the list of iSCSI sessions, select the session that you want to disconnect and click **Disconnect Session**.

6. In the **Disconnect Session** dialog box, click **OK**.

   SnapCenter disconnects the iSCSI session.

**Creating and managing igroups**

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

**Creating an igroup**

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

**Steps**

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click **Hosts**.

2. In the **Hosts** page, click **Igroup**.

3. In the **Initiator Groups** page, click **New**.

4. In the **Create Igroup** dialog box, define the igroup:
In this field... | Do this...
---|---
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 left navigation pane, select the appropriate plug-in from the drop-down list, and then click **Hosts**.
2. In the **Hosts** page, click **Igroup**.
3. In the **Initiator Groups** page, click in the **Storage Virtual Machine** field to display a list of available SVMs, and then select the SVM for the igroup you want to rename.
4. In the list of igroups for the SVM, select the igroup you want to rename and click **Rename**.
5. In the **Rename igroup** dialog box, enter the new name for the igroup and click **Rename**.

**Modifying an igroup**

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

**Steps**

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

4. In the list of igroups for the SVM, select the igroup you want to delete and click **Delete**.

5. In the **Delete igroup** dialog box, click **OK**.

SnapCenter deletes the igroup.

**Creating and managing disks**

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

**About this task**

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

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

**Viewing the disks on a host**

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

**Steps**

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click **Hosts**.

2. In the **Hosts** page, click **Disks**.

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

The disks are listed.

**Creating FC-connected or iSCSI-connected LUNs or disks**

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

**Before you begin**

- You must have created a volume for the LUN on your storage system.

  The volume should hold LUNs only, and only LUNs created with SnapCenter.

  *ONTAP 9 Logical Storage Management Guide*

  **Note:** You cannot create a LUN on a SnapCenter-created clone volume unless the clone has already been split.

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

  *ONTAP 9 SAN Administration Guide*

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

  *Starting an iSCSI session* on page 81
About this task

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

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.
2. In the Hosts page, click Disks.
3. Select the host from the Host drop-down list.
4. Click New.
   The Create Disk wizard opens.
5. On the LUN Name page, identify the LUN:

<table>
<thead>
<tr>
<th>In this field...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage System</td>
<td>Select the SVM for the LUN.</td>
</tr>
<tr>
<td>LUN path</td>
<td>Click Browse to select the full path of the folder containing the LUN.</td>
</tr>
<tr>
<td>LUN name</td>
<td>Enter the name of the LUN.</td>
</tr>
<tr>
<td>Cluster size</td>
<td>Select the LUN block allocation size for the cluster. Cluster size depends upon the operating system and applications.</td>
</tr>
<tr>
<td>LUN label</td>
<td>Optionally, enter descriptive text for the LUN.</td>
</tr>
</tbody>
</table>
6. On the Disk Type page, select the disk type:

<table>
<thead>
<tr>
<th>Select...</th>
<th>If...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated disk</td>
<td>The LUN can be accessed by only one host. Ignore the Resource Group field.</td>
</tr>
<tr>
<td>Shared disk</td>
<td>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.</td>
</tr>
<tr>
<td>Cluster Shared Volume (CSV)</td>
<td>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.</td>
</tr>
</tbody>
</table>
7. On the Drive Properties page, specify the drive properties:

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

Do not assign drive letter or volume mount point | Choose this option if you prefer to mount the disk manually in Windows.

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:

<table>
<thead>
<tr>
<th>In this field...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>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.</td>
</tr>
</tbody>
</table>

Choose host initiator | Select **Fibre Channel** or **iSCSI** and then select the initiator on the host. You can select multiple FC initiators if you are using FC with multipath I/O (MPIO). |

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

<table>
<thead>
<tr>
<th>Select...</th>
<th>If...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new igroup for selected initiators</td>
<td>You want to create a new igroup for the selected initiators.</td>
</tr>
</tbody>
</table>

| Create 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 84
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 left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.
2. In the Hosts page, click Disks.
3. Select the host from the Host drop-down list.
4. The disks are listed.
5. Select the disk you want to resize and then click Resize.
6. In the Resize Disk dialog box, use the slider tool to specify the new size of the disk, or enter the new size in the Size field.
   
   Note: If you enter the size manually, you need to click outside the Size field before the Shrink or Expand button is enabled appropriately. 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 84

Connecting a disk

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

Before you begin

- You must have started the FC or iSCSI service on the storage system.
- If you are using iSCSI, you must have established an iSCSI session with the storage system.

About this task

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

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.

2. In the Hosts page, click Disks.

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

4. Click Connect.

The Connect Disk wizard opens.

5. On the LUN Name page, identify the LUN to connect to:

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

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

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

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto assign</td>
<td>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:\scmpt). The auto assign property is not supported for shared disks.</td>
</tr>
<tr>
<td>Assign drive letter</td>
<td>Mount the disk to the drive you select in the adjoining drop-down list.</td>
</tr>
<tr>
<td>Use volume mount point</td>
<td>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.</td>
</tr>
<tr>
<td>Do not assign drive letter or volume mount point</td>
<td>Choose this option if you prefer to mount the disk manually in Windows.</td>
</tr>
</tbody>
</table>

8. On the Map LUN page, select the iSCSI or FC initiator on the host:
In this field... | Do this...
---|---
Host | Double-click the cluster group name to display a drop-down list that shows the hosts that belong to the cluster, then select the host for the initiator.
This field is displayed only if the LUN is shared by hosts in a Windows Server failover cluster.

Choose host initiator | Select Fibre Channel or iSCSI, and then select the initiator on the host. You can select multiple FC initiators if you are using FC with MPIO.

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

<table>
<thead>
<tr>
<th>Select...</th>
<th>If...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new igroup for selected initiators</td>
<td>You want to create a new igroup for the selected initiators.</td>
</tr>
<tr>
<td>Choose an existing igroup or specify a new igroup for selected initiators</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 84

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

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

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

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

Steps
1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.
2. In the Hosts page, click Disks.
3. Select the host from the Host drop-down list. The disks are listed.

4. Select the disk you want to disconnect, and then click Disconnect.

5. In the Disconnect Disk dialog box, click OK. SnapCenter disconnects the disk.

Related tasks
   Viewing the disks on a host on page 84

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

Steps
1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.

2. In the Hosts page, click Disks.

3. Select the host from the Host drop-down list. The disks are listed.

4. Select the disk you want to delete, and then click Delete.

5. In the Delete Disk dialog box, click OK. SnapCenter deletes the disk.

Related tasks
   Viewing the disks on a host on page 84

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 left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.

2. In the Hosts page, click Shares.

3. Select the SVM from the Storage Virtual Machine drop-down list.

4. Click New.

   The New Share dialog opens.

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

<table>
<thead>
<tr>
<th>In this field...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter descriptive text for the share.</td>
</tr>
<tr>
<td>Share name</td>
<td>Enter the share name, for example, test_share. The name you enter for the share will also be used as the volume name.</td>
</tr>
<tr>
<td>Share path</td>
<td>• Click in the field to enter a new file system path, for example, ./</td>
</tr>
<tr>
<td></td>
<td>• Double-click in the field to select from a list of existing file system paths.</td>
</tr>
</tbody>
</table>

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

   SnapCenter creates the SMB share on the SVM.

Deleting an SMB share

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

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.

2. In the Hosts page, click Shares.

3. In the Shares page, click in the Storage Virtual Machine field to display a drop-down with a list of available Storage Virtual Machines (SVMs), then select the SVM for the share you want to delete.

4. From the list of shares on the SVM, select the share you want to delete and click Delete.

5. In the Delete Share dialog box, click OK.

   SnapCenter deletes the SMB share from the SVM.
Reclaiming space on the storage system

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

Before you begin

If you are running the cmdlet on a remote plug-in host, you must have run the SnapCenter OpenSMConnection 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 2.0 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.

Related references

Storage types supported by SnapCenter Plug-ins for Microsoft Windows and for Microsoft SQL Server on page 20
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:

- 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 ESXi 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. You can use cmdlets directly or add them to scripts.

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

```
Open-SmConnection -SMSbaseURL https://SNAPCENTER_SERVER_NAME.DOMAIN_NAME:8146 -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).
- 8146 is the default SnapCenter HTTPS port.
  
  You can configure this port during the SnapCenter installation process. If you want to modify the port, you must reinstall SnapCenter and specify a new port number during the new installation.
- “`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 2.0 Windows Cmdlet Reference Guide*
Setting up protection for virtualized resources

After you install SnapCenter, you might need to switch from Virtual Storage Console for VMware vSphere (VSC) to the SnapCenter Plug-in for VMware vSphere. Or you might need to update the vCenter or SnapCenter configuration information for the SnapCenter Plug-in for VMware vSphere. If you are using Virtual Storage Console for VMware vSphere (VSC), you need to register it with SnapCenter.

SnapCenter supports two ways to protect data in virtualized resources: the SnapCenter Plug-in for VMware vSphere is the easiest to use because it is built into SnapCenter. However, if you need to protect VMs, you need to use Virtual Storage Console for VMware vSphere (VSC) for all your virtualized resources.

Switching from VSC to SnapCenter Plug-in for VMware vSphere

If you are currently using SnapCenter with Virtual Storage Console for VMware vSphere (VSC) to manage your virtualized databases and applications, you might want to use the SnapCenter Plug-in for VMware vSphere instead because it does not require any additional steps to register SnapCenter with your vCenter.

About this task

Note: You cannot use the SnapCenter Plug-in for VMware vSphere to manage VMs. If you need to manage VMs, then you must continue to use VSC.

Steps

1. Upgrade to SnapCenter 2.0.
2. From the SnapCenter GUI, remove the VSC hosts.
   a. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.
   b. In the Hosts page, select the host to remove and then click Remove.
      Repeat this step for every VSC host.
   When you remove a VSC host, SnapCenter removes all host registration from the SnapCenter Server repository. It does not uninstall VSC from remote hosts.
3. Uninstall the VSC software from remote hosts.
   For information on uninstalling VSC, see the VSC documentation.
4. From the SnapCenter GUI, add a vSphere host.
   When you add a vSphere host, SnapCenter automatically installs the SnapCenter Plug-in for VMware vSphere on the host.
   vCenter resource groups that you previously created are not visible in SnapCenter. For information on creating SnapCenter resource groups, see the SnapCenter Data Protection Guide for your environment.

After you finish

Use SnapCenter to perform backup, restore, and clone operations, as needed.
Registering VSC for VMware vSphere with SnapCenter

If you are using Virtual Storage Console for VMware vSphere (VSC), then registering VSC with SnapCenter adds the VSC host to SnapCenter and enables SnapCenter to communicate with VMware vSphere. You can only register VSC with SnapCenter using the VSC GUI. You can register multiple instances of VSC with a single instance of SnapCenter.

Before you begin

Note: If you are using SnapCenter Plug-in for VMware vSphere to manage virtualized resources, then you cannot install or register VSC. SnapCenter Plug-in for VMware vSphere automatically deploys when you use SnapCenter to add a host. However, if you want to manage VMs, you must install and register VSC instead of installing SnapCenter Plug-in for VMware vSphere.

- 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 Data ONTAP 8.2.2 or later.
- For SnapCenter 2.0, you must be running Virtual Storage Console 6.2P2 for VMware vSphere.

About this task

Each SnapCenter Server can support multiple VSC servers. You must use the VSC GUI to register each VSC server individually with SnapCenter.

There are two situations for which 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 and VMs. 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 resource groups and registered VSC with SnapCenter, you can view these policies and resource groups in SnapCenter. You can also view VSC-based backup, clone, and restore operations on the SnapCenter Jobs page.

If you do not register VSC with SnapCenter, VSC uses its backup and restore features.
Note: If you only need to back up SQL databases or Oracle databases on VMDKs or RDMs, and do not need to protect VMs, then you should consider installing SnapCenter Plug-in for VMware vSphere instead of VSC.

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 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, backups created before enabling AutoSupport at the VSC level are not logged in AutoSupport. However, backups created after enabling AutoSupport at the VSC level are logged.

For details about using the VSC GUI to register VSC with SnapCenter, see the VSC documentation.

Steps

1. Log on to the VSC GUI as a VSC administrator and then select Configuration > Configure SnapCenter Server.

2. Complete the information in the Configure SnapCenter Server dialog box.
   To push SVM credentials into SnapCenter, you must register the SVMs, not the clusters.

Related tasks

   Updating hypervisor configuration settings on page 100

Related information

   NetApp Documentation: Virtual Storage Console for VMware vSphere

Monitoring virtualization status in SnapCenter

If you have a virtualized environment and you are using Virtual Storage Console for VMware vSphere (VSC) instead of SnapCenter Plug-in for VMware vSphere, 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. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.

2. In the Hosts page, click Managed Hosts.

3. On the Managed Hosts page, select a host, and then click Details.

4. 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 98

Updating hypervisor configuration settings
If you are using VSC with SnapCenter to manage your virtualized databases, and you are using either the SnapCenter Plug-in for Microsoft SQL Server or SnapCenter Plug-in for Oracle Database, depending on your environment, you can update your hypervisor configuration settings so that SnapCenter no longer displays a “configure hypervisor” message in the host status area.

Before you begin
• If you are using SnapCenter Plug-in for Microsoft SQL Server, your SQL Server environment must be using an iSCSI initiator.
• If you are using SnapCenter Plug-in for Oracle Database, your Oracle environment must be using NFS or an iSCSI initiator.

Steps
1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Settings.
2. In the Settings page, click Global Settings.
3. In the Hypervisor configuration settings area, select VMs have iSCSI direct attached disks or NFS for all the hosts.
   The host status for the VM changes from “configure hypervisor” to “Running.”

Related tasks
Registering VSC for VMware vSphere with SnapCenter on page 98

Updating vCenter or SnapCenter information in the SnapCenter Plug-in for VMware vSphere
You might need to update the vCenter or SnapCenter host information that the SnapCenter Plug-in for VMware vSphere uses when communicating with vCenter. For example, an update might be necessary if the vCenter password for a host was changed.

Steps
1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.
2. In the Hosts page, select the vSphere-type host.
3. Click the Add/Update vCenter details button.

4. In the dialog box, select the type of information you want to update:
   - Add/Update vCenter Details
   - Add/Update SnapCenter Details

5. In the dialog box, enter only the information that needs to be updated.
   Blank fields are not changed.

6. Click OK.
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 check for available updates. Then, you must install them. In addition, you may need to update the SnapCenter Plug-in for VMware vSphere with newly changed vCenter or SnapCenter information.

You can upgrade SnapCenter from version v1.1.x to 2.0. To upgrade from v1.0.X, you must first upgrade to v1.1.x and then upgrade to 2.0.

If you are going to use SnapCenter as part of the Data Fabric Solution for Cloud Backup, you cannot upgrade from SnapCenter 1.1 to 2.0. You must perform a new 2.0 installation.

Related concepts

Preparing for the installation on page 20

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. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Settings.
2. In the Settings page, click Software.
   
   The Available Software page 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 resource groups 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 resource groups or the host in maintenance mode. If you are using NLB, you should have the same version of SnapCenter on all NLB nodes.

- You must have backed up the SnapCenter repository (also called the NSM database). See the SnapCenter Software Administration Guide.

- If you are upgrading from SnapCenter 1.1 to SnapCenter 2.0, you must have installed .NET 4.5.2 on all Windows hosts.

- If you are upgrading from SnapCenter 1.1 or earlier to SnapCenter 2.0, you must have reviewed the Release Notes to understand the workflow changes related to policies, datasets, and schedules. SnapCenter Software 2.0 Release Notes

Steps

1. Download the SnapCenter upgrade package from the NetApp Support Site at mysupport.netapp.com.

2. Place all hosts with plug-ins in maintenance mode:
   a. In the left navigation pane, select Hosts, and in the Managed Hosts list, select the host you want to upgrade.
   b. In the Information pane, select the host and its plug-in, and then click Suspend Schedule.
   c. Repeat for each host.

3. From the upgrade package that you downloaded, 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.

4. Click Hosts > Activate Schedule to bring the host out of maintenance mode so that operations can resume.

After you finish

- After successfully upgrading the server host, you must also upgrade the plug-in hosts.
  If the plug-in hosts are not upgraded, the status of the plug-ins will be “Plug-ins are incompatible”.
  
  **Note:** You do not have to upgrade the VSC host.

- If upgrade fails, you can restore the NSM database to its previous state and you can continue using the earlier version of SnapCenter without losing any data.

- You must perform a fresh discovery of resources on the hosts.

Related concepts

Network Load Balancing and Application Request Routing options on page 34
Related information

SnapCenter Software 2.0 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. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.

2. On 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.

   Note: For SnapCenter Plug-in for Microsoft SQL Server, after upgrading from SnapCenter 1.1 to SnapCenter 2.0, you must refresh the resources to view the Availability Group type.

   Note: For SnapCenter Plug-in for Microsoft SQL Server, after upgrading from SnapCenter 1.1 to SnapCenter 2.0, the values of Repeat every option for monthly schedules are not retained. You must provide new values for Repeat every option.

After you finish

After the plug-in package is upgraded, bring the host out of maintenance mode by clicking Activate Schedule.
Uninstalling SnapCenter plug-ins and plug-in packages

You can remove hosts and uninstall individual plug-ins or plug-in packages using the SnapCenter GUI. You can also uninstall individual plug-ins or plug-in packages on remote hosts using the command-line interface (CLI) on your SnapCenter Server host or using the Windows Uninstall a program option locally on any host.

Uninstalling plug-ins from a host using the SnapCenter GUI

When you decide that you no longer require an individual plug-in or a plug-in package, you can uninstall it using the SnapCenter interface.

Before you begin

• You must have removed the resource groups for the plug-in package that you are uninstalling.

• You must have detached the policies associated with the resource groups for the plug-in package that you are uninstalling.

About this task

You can uninstall an individual plug-in. For example, you might need to uninstall the SnapCenter Plug-in for VMware vSphere because a host is running out of resources and you want to move that plug-in to a more powerful host. You can also uninstall an entire plug-in package. For example, you might need to uninstall the SnapCenter Plug-ins Package for Linux, which includes SnapCenter Plug-in for Oracle Database and SnapCenter Plug-in for UNIX.

• Removing a host includes uninstalling all plug-ins

  When you remove a host from SnapCenter, SnapCenter uninstalls all the plug-in packages on the host before removing the host.

• SnapCenter GUI removes plug-ins from one host at a time

  When you use the SnapCenter GUI, you can uninstall plug-ins on only one host at a time. However, you can have several uninstallation operations running at the same time. You can uninstall a plug-in from multiple hosts by using the command-line interface (CLI).

Attention: 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. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.

2. In the Hosts page, click Managed Hosts.

3. In the Managed Hosts page, select the host from which you want to uninstall the plug-in or plug-in package.

4. Click Modify.

5. In the Modify Host page, select Remove plug-ins.
6. In the **Plug-ins** page, do the following:

   • If you are uninstalling a single plug-in, do not make any selection on this page.
   
   • If you are uninstalling a plug-in package, select the package you want to uninstall.

7. In the **Summary** page, review your selections and then click **Finish**.

**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 the 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 Windows plug-ins using the command-line interface on the SnapCenter Server host

You can uninstall individual plug-ins or uninstall plug-ins packages from one or more hosts by using the `Uninstall-SmHostPackage` cmdlet on the SnapCenter Server host command-line interface.

**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:
   
   ```powerShell
   Open-SMConnection
   ```

3. From the command prompt, enter:
   
   ```powerShell
   Uninstall-SmHostPackage -HostNames hostname1[,hostname2...] -ApplicationCode plugincode
   ```
   
   • You can specify one or more host names, separated by commas.
   
   • If you do not specify a host name, a prompt is displayed for you to list the host names.
   
   • If you do not specify an application (plug-in) code, SnapCenter uninstalls all SnapCenter plug-ins on the host by default. Valid ApplicationCode values are as follows:

<table>
<thead>
<tr>
<th>ApplicationCode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCSQL</td>
<td>SnapCenter Plug-ins Package for Windows</td>
</tr>
<tr>
<td>SCO</td>
<td>SnapCenter Plug-ins Package for Linux</td>
</tr>
<tr>
<td>SCV</td>
<td>SnapCenter Plug-in for VMware vSphere</td>
</tr>
<tr>
<td>Name of the custom plug-in</td>
<td>SnapCenter Custom Plug-ins</td>
</tr>
</tbody>
</table>

**Example**

The following command uninstalls SnapCenter Plug-in for VMware vSphere from the specified host.
The following command uninstalls SnapCenter Custom Plug-ins from the specified host.

```
Uninstall-SmHostPackage -HostNames lab-esx90.test1.com
-ApplicationCode SCV
```

Where, `HRPlug-in` is the name of the custom plug-in.

**Uninstalling Windows plug-ins locally on a host**

You can uninstall SnapCenter plug-ins packages locally on a host if you cannot reach the host from the SnapCenter Server.

**About this task**

The best practice for uninstalling individual plug-ins or plug-in packages is to either use the SnapCenter GUI or use the `Uninstall-SmHostPackage` cmdlet on the SnapCenter Server host command-line interface. These procedures help the SnapCenter Server to stay up to date with any changes. However, you might have a rare need to uninstall plug-ins locally. For example, you might have run an uninstall job from the SnapCenter Server but the job failed, or you uninstalled your SnapCenter Server and orphan plug-ins remain on a host.

**Attention:** Uninstalling a plug-in package locally on a host does not delete data associated with the host; for example scheduled jobs and backup metadata.

**Steps**

1. On the host system, navigate to the Control Panel and click Uninstall a program.
2. In the list of programs, select the SnapCenter package you want to uninstall and click Uninstall. Windows uninstalls all plug-ins in the selected package.

**Uninstalling SnapCenter Plug-ins Package for Linux using the command-line interface**

You should uninstall SnapCenter Plug-ins Package for Linux by using the SnapCenter user interface. However, if you cannot uninstall it for some reason, you can uninstall SnapCenter Plug-ins Package for Linux using the command-line interface.

**Before you begin**

You must have deleted the scheduled jobs and running jobs must have been completed.

**Step**

1. Enter the following command:

```
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall
```
Removing a host from SnapCenter

You can remove a host if you no longer want to use SnapCenter to manage its data protection jobs. For example, you might want to remove a host if it no longer has data that needs to be protected.

Before you begin

A host can only be removed after all SnapCenter backups and resource groups associated with the host are deleted. The recommended practice is to delete these manually, however, in some situations you can use the force removal option.

When you remove the resource groups, all the associated schedules are also removed.

About this task

When the SnapCenter Server removes a host, it first uninstalls the plug-in packages installed on the host and then removes all the resources listed for that host in the SnapCenter Resources page.

You can force the removal of a host that is associated with backups and resource groups. However, the force removal option is not supported in the following situations:

- Oracle RAC clusters
  You should delete all the backups and resource groups associated with Oracle RAC hosts before removing the host.
- Availability Group (AG) cluster in SQL Server
  Force removal is not supported if there are database level resource groups containing databases from more than one node of the cluster.
- If the host has a resource group that is shared with another host
- If the host has a clone
- If a backup, restore, or clone operation is running for the host
- If a backup, restore, or clone operation is running for the host
- For databases, if an RMAN or cataloging operation is running

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.
2. In the Hosts page, click Managed Hosts.
3. Select the host you want to remove, and then click Remove.
4. For Oracle RAC clusters, to remove SnapCenter software from all the hosts in the cluster, select Include all the hosts of cluster.
5. Select Force removal of host if you want to remove the host that is associated with backups and resource groups.
6. Click OK to continue.

Uninstalling SnapCenter

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 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 node from the NLB cluster and the Application Request Routing server farm.
6. If you do not want to use this SnapCenter repository with a newly installed SnapCenter Server, select to remove the SnapCenter repository. In NLB configurations, you can only delete the repository from the last NLB node.

**After you finish**

- Removing the NLB node from an 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 (if you are uninstalling an earlier version of SnapCenter) 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).
Installing plug-ins independently

It is a best practice to install the plug-ins remotely from the SnapCenter user interface. If for some reason you are unable to install a plug-in remotely, you can use the independent plug-in installation package to install the plug-in locally.

The independent plug-in installation packages are available for the following plug-ins:

- SnapCenter Plug-in for Microsoft Windows
- SnapCenter Plug-in for Microsoft SQL Server
- SnapCenter Plug-in for Oracle Database
- SnapCenter Plug-in for VMware vSphere

Note: The independent installation of SnapCenter Custom Plug-ins is not supported.

Installing the SnapCenter Plug-in for Microsoft Windows independently

You can install the SnapCenter Plug-in for Microsoft Windows locally on a Windows host if you are unable to install the plug-in remotely from the SnapCenter user interface.

Preparation to install the SnapCenter Plug-in for Microsoft Windows

The Windows host on which you install the SnapCenter Plug-in for Microsoft Windows must meet the specified software, browser, and operating system requirements.

Before you begin

- If installed, you must have stopped the Windows Host utilities and provisioning and protection capabilities of the OnCommand Unified Manager Core Package.
- You must have installed Microsoft .Net 4.5.2.
- You must have installed PowerShell 4.0 or later.
- You must have turned on Windows message queuing.
- You must be a local administrator on the host.

About this task

Installing the plug-in remotely using the SnapCenter user interface is the preferred method. You should install the plug-in locally only if you are unable to install it remotely from SnapCenter.

Installing the SnapCenter Plug-in for Microsoft Windows silently from the command line

You can install the SnapCenter Plug-in for Microsoft Windows locally on a Windows host if you are unable to install the plug-in remotely from SnapCenter. You can run the SnapCenter Plug-in for Microsoft Windows installation program unattended, in silent mode, from the Windows command line.

Steps

1. Download the SnapCenter Plug-in for Microsoft Windows from C:\inetpub\wwwroot\SnapCenter\Repository.
This path is accessible from the host where the SnapCenter Server is installed.

2. Copy the installation file to the host on which you want to install the plug-in.

3. From the command prompt, navigate to the directory where you downloaded the installation file.

4. Enter the following command, replacing variables with your data:

   "SnapCenter Plug-in for Microsoft Windows.exe" /silent /debuglog
   "DirPath\LogFileName" ISFeatureInstall="SCW"
   BI_SDW_NG_DEST="InstallDirectory" BI_SERVICEACCOUNT=Domain\UserName
   BI_SERVICEPWD=Password BI_WEBSERVICE_PORT=808
   PREFERRED_STORAGE_SYSTEM_NAME=PreferredSystemName LICENSE_TYPE_SERVER=1
   LPSM_SERIALNUMBER="LicenseKey"

   Enter the following for each variable:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DirPath\LogFileName</td>
<td>The location and name of the installation log file</td>
</tr>
<tr>
<td>InstallDirectory</td>
<td>The directory where you want to install the plug-in</td>
</tr>
<tr>
<td>Domain\UserName</td>
<td>The user account that Windows uses to run the plug-in</td>
</tr>
<tr>
<td></td>
<td>This account must have the domain user with local administrator permissions on the Windows host.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the specified account</td>
</tr>
<tr>
<td>PreferredSystemName</td>
<td>The storage system name that the plug-in should use for management traffic</td>
</tr>
<tr>
<td>LicenseKey</td>
<td>The per-server license key</td>
</tr>
<tr>
<td></td>
<td>Leave this field blank if you are using per-storage system licensing.</td>
</tr>
</tbody>
</table>

Example

   "C:\inetpub\wwwroot\SnapCenter\Repository\snapcenter_windows_host_plugin.exe" /silent /debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\"
   BI_SNAPCENTER_PORT=8145
   SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
   BI_SERVICEACCOUNT=domain\administrator
   BI_SERVICEPWD=password
   ISFeatureInstall=SCW

   The debuglog parameter includes the path of the log file for SnapCenter. Writing to this log file is the preferred method of obtaining troubleshooting information, because the file contains the results of checks that the installation performs for plug-in prerequisites.

   If necessary, you can find additional troubleshooting information in the log file for the SnapCenter for Windows package. Log files for the package are listed (oldest first) in the %Temp% folder, for example, C:\temp\.
Installing SnapCenter Plug-in for Microsoft SQL Server independently

You can install the SnapCenter Plug-in for Microsoft SQL Server locally if you are unable to install the plug-in from the SnapCenter user interface.

Preparation to install the SnapCenter Plug-in for Microsoft SQL Server

The SnapCenter Plug-in for Microsoft SQL Server installer consists of third-party and NetApp packages. You can also upgrade, repair, or remove the packages using the installer.

Third-party packages

Following are the third-party packages:

- Microsoft Visual C++ 2012 Redistributable Package (x86)
  This installs runtime components that are required to run C++ applications built with Visual Studio 2012.

- Microsoft SQL Server 2016 CLR Types (x64)
  This is part of the Microsoft SQL Server Feature Pack but also is a stand-alone software that can be installed separately. The SQL Server System CLR Types package contains the components implementing the new geometry, geography, and hierarchy ID types in SQL Server 2016. You can install this component separately from the server to allow client applications to use these types outside of the server.

- Microsoft SQL Server 2016 Management Objects (x64)
  This is a collection of objects that are designed for programming all aspects of managing Microsoft SQL Server. This object model works with SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, SQL Server 2014, and SQL Server 2016. It is included in all SQL Server editions, including the Express Edition and requires Microsoft SQL Server System CLR Types.

- Microsoft SQL Server 2016 CLR types (x64)
  The SnapCenter Plug-in for Microsoft SQL Server requires all these packages to perform backup, restore, and recovery operations for SQL databases running on NetApp storage systems.

Prerequisites

The following must have already been installed:

- SnapCenter Plug-in for Microsoft Windows on the same host where SnapCenter Plug-in for Microsoft SQL Server is installed
  SnapCenter Server must be installed on a separate host.

- Windows PowerShell v4.0 for Windows Server 2008 R2 SP1

- Microsoft .Net Framework v4.5.2

- Microsoft Hotfixes
Installing the SnapCenter Plug-in for Microsoft SQL Server silently from the command line

You should install SnapCenter Plug-in for Microsoft SQL Server from within the SnapCenter user interface. However, if you cannot for some reason, you can run the SnapCenter Plug-in for Microsoft SQL Server installation program unattended in silent mode from the Windows command line.

Before you begin

- You must have backed up your SQL databases.
- SnapCenter plug-in packages must be installed.

Steps

1. Download the SnapCenter Plug-in for Microsoft Windows from C:\inetpub\wwwroot\SnapCenter\Repository. This path is accessible from the host where the SnapCenter Server is installed.
2. Copy the installation file to the host on which you want to install the plug-in.
3. From a Windows command prompt on the local host, navigate to the directory to which you saved the plug-in installation files.
4. Enter the following command to install replacing the variables with your data:

   "snapcenter_windows_host_plugin.exe"/silent /debuglog"<Debug_Log_Path>" /log"<Log_Path>" BI_SNAPCENTER_PORT=<Num> SUITE_INSTALLDIR="<Install_Directory_Path>" BI_SERVICEACCOUNT=<domain\administrator> BI_SERVICEPWD=<password> ISFeatureInstall=SCW,SCSQL

   For example,

   "C:\inetpub\wwwroot\SnapCenter\Repository\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:\HPPW_SCSQL_Install.log" /log"C:" BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter" BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password ISFeatureInstall=SCW,SCSQL

Enter the following values for the variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/debuglog&quot;&lt;Debug_Log_Path&gt;&quot;</td>
<td>Specify the name and location of the suite installer log file, as in the following example: Setup.exe /debuglog&quot;C:\PathToLog\setupexe.log&quot;.</td>
</tr>
<tr>
<td>BI_SNAPCENTER_PORT</td>
<td>Specify the port on which SnapCenter communicates with SMCore.</td>
</tr>
<tr>
<td>SUITE_INSTALLDIR</td>
<td>Specify host plug-in package installation directory.</td>
</tr>
<tr>
<td>BI_SERVICEACCOUNT</td>
<td>Specify SnapCenter Plug-in for Microsoft Windows web service account.</td>
</tr>
<tr>
<td>BI_SERVICEPWD</td>
<td>Specify the password for SnapCenter Plug-in for Microsoft Windows web service account.</td>
</tr>
<tr>
<td>ISFeatureInstall</td>
<td>Specify the solution to be deployed by SnapCenter on remote host.</td>
</tr>
</tbody>
</table>
Installing SnapCenter Plug-in for Oracle Database independently

You can install the SnapCenter Plug-in for Oracle Database locally on the Linux host if you are unable to install the plug-in from the SnapCenter user interface. You can use an interactive wizard or the command-line interface to install the plug-in.

The Plug-in for Oracle Database must be installed on each Linux host where the Oracle database resides.

Preparation to install the SnapCenter Plug-in for Oracle Database

The Linux host on which you are installing the SnapCenter Plug-in for Oracle Database must meet the specified software, browser, database, and operating system requirements.

For latest information about the supported configurations, see the Interoperability Matrix Tool.

*NetApp Interoperability Matrix Tool*

Before you install SnapCenter Plug-ins Package for Linux, you must have already installed SnapCenter 2.0 on a Windows host and copied the SnapCenter Plug-ins Package for Linux to the target host.

**Related information**

*NetApp Interoperability Matrix Tool*

Installing the SnapCenter Plug-in for Oracle Database interactively

You should install SnapCenter Plug-in for Oracle Database from within the SnapCenter user interface. However, if you cannot for some reason, you can use the installation wizard to install SnapCenter Plug-in for Oracle Database interactively on a Linux host.

**Before you begin**

- You must have reviewed the prerequisites for installing Plug-in for Oracle Database.
- You must set the `DISPLAY` environment variable to specify the IP address and port number of the Linux host where you want to launch the wizard.

**Steps**

1. Download the Plug-in for Oracle Database from `C:\inetpub\wwwroot\SnapCenter\Repository`.
   
   This path is accessible from the host where the SnapCenter Server is installed.
2. Copy the installation file to the host on which you want to install the plug-in.
3. From the command prompt, navigate to the directory where you downloaded the installation file.
4. Enter the following command to run the executable file:
   
   `./SnapCenter_linux_host_plugin.bin -swing`
5. Follow the on-screen prompts in the wizard to install the SnapCenter Plug-in for Oracle Database.
6. Click **Finish** to complete the installation.
Installing the SnapCenter Plug-in for Oracle Database using command-line interface

You should install SnapCenter Plug-in for Oracle Database from within the SnapCenter user interface. However, if you cannot for some reason, you can install the SnapCenter Plug-in for Oracle Database either in console mode or in silent mode using command-line interface.

Before you begin

• You must have reviewed the prerequisites for installing Plug-in for Oracle Database.
• You must ensure that the DISPLAY environment variable is not set.

About this task

The console mode installation requires you to provide the required installation information while installing Plug-in for Oracle Database.

The silent mode installation does not require you to provide installation information while installing Plug-in for Oracle Database.

Steps

1. Download the Plug-in for Oracle Database from C:\inetpub\wwwroot\SnapCenter\Repository.
   This path is accessible from the host where the SnapCenter Server is installed.
2. From the command prompt, navigate to the directory where you downloaded the installation file.
3. Perform the following steps to install Plug-in for Oracle Database in console mode:
   a. Enter the following command to run the executable file:
      ./SnapCenter_linux_host_plugin.bin -console
   b. Follow the on-screen prompts to complete the installation.
4. Enter the following command to install in silent mode:
   ./SnapCenter_linux_host_plugin.bin -i silent -DPORT -DSERVER_IP -DSERVER_PORT

Installing the SnapCenter Plug-in for VMware vSphere silently

You should install the SnapCenter Plug-in for VMware vSphere from within the SnapCenter user interface. However, if you cannot for some reason, you can install the plug-in in silent mode using the command line.

Before you begin

• You must have installed PowerShell 4.0 or later.
• You must have installed Microsoft .Net 4.5.2.
• You must have turned on Windows message queuing.
• You must be a local administrator on the host.
Steps

1. Download the SnapCenter installer from the NetApp Support Site at mysupport.netapp.com.
   The SnapCenter Plug-ins Package for Windows includes the SnapCenter Plug-in for VMware vSphere.

2. From a Windows command prompt on the local host, navigate to the directory where you downloaded the installer.

3. Enter the following command, replacing variables with your data:

   ```
   "snapcenter_windows_host_plugin.exe"/silent /debuglog"DirPath \DebugLogFileName" /log"DirPath\InstallLogFileName"
   SUITE_INSTALLDIR="InstallDirectory" BI_SCV_PORT=8144
   ISFeatureInstall=SCV
   ```

   Enter the following for each variable:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DirPath</td>
<td>The location and name of the plug-in prerequisite checks log</td>
</tr>
<tr>
<td>DebugLogFileName</td>
<td></td>
</tr>
<tr>
<td>DirPath</td>
<td>The location and name of the installation log</td>
</tr>
<tr>
<td>InstallLogFileName</td>
<td></td>
</tr>
<tr>
<td>InstallDirectory</td>
<td>The directory where you want to install the plug-in</td>
</tr>
</tbody>
</table>

Example

```
"snapcenter_windows_host_plugin.exe"/silent /debuglog"c:\VSC\Add_Plugin_SCV.log" /log"c:\VSC\SUITE_INSTALLDIR="c:\Program Files\NetApp\SnapCenter" BI_SCV_PORT=8144 ISFeatureInstall=SCV
```
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.

<table>
<thead>
<tr>
<th>Category</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server</td>
<td>• Internet Information Services</td>
</tr>
<tr>
<td></td>
<td>• World Wide Web Services</td>
</tr>
<tr>
<td></td>
<td>• Common HTTP Features</td>
</tr>
<tr>
<td></td>
<td>◦ Default Document</td>
</tr>
<tr>
<td></td>
<td>◦ Directory Browsing</td>
</tr>
<tr>
<td></td>
<td>◦ HTTP Errors</td>
</tr>
<tr>
<td></td>
<td>◦ HTTP Redirection</td>
</tr>
<tr>
<td></td>
<td>◦ Static Content</td>
</tr>
<tr>
<td></td>
<td>◦ WebDAV Publishing</td>
</tr>
<tr>
<td></td>
<td>• Health and Diagnostics</td>
</tr>
<tr>
<td></td>
<td>◦ Custom Logging</td>
</tr>
<tr>
<td></td>
<td>◦ HTTP Logging</td>
</tr>
<tr>
<td></td>
<td>◦ Logging Tools</td>
</tr>
<tr>
<td></td>
<td>◦ Request Monitor</td>
</tr>
<tr>
<td></td>
<td>◦ Tracing</td>
</tr>
<tr>
<td></td>
<td>• Performance Features</td>
</tr>
<tr>
<td></td>
<td>◦ Static Content Compression</td>
</tr>
<tr>
<td></td>
<td>• Security</td>
</tr>
<tr>
<td></td>
<td>◦ IP Security</td>
</tr>
<tr>
<td></td>
<td>◦ Basic Authentication</td>
</tr>
<tr>
<td></td>
<td>◦ Centralized SSL Certificate Support</td>
</tr>
<tr>
<td></td>
<td>◦ Client Certificate Mapping Authentication</td>
</tr>
<tr>
<td></td>
<td>◦ IIS Client Certificate Mapping Authentication</td>
</tr>
<tr>
<td></td>
<td>◦ IP and Domain Restrictions</td>
</tr>
<tr>
<td></td>
<td>◦ Request Filtering</td>
</tr>
<tr>
<td></td>
<td>◦ URL Authorization</td>
</tr>
<tr>
<td></td>
<td>◦ Windows Authentication</td>
</tr>
<tr>
<td></td>
<td>• Application Development Features</td>
</tr>
<tr>
<td></td>
<td>◦ .NET Extensibility 4.5</td>
</tr>
<tr>
<td></td>
<td>◦ Application Initialization</td>
</tr>
<tr>
<td></td>
<td>◦ ASP.NET 4.5</td>
</tr>
<tr>
<td></td>
<td>◦ Server-Side Includes</td>
</tr>
<tr>
<td></td>
<td>◦ WebSocket Protocol</td>
</tr>
<tr>
<td></td>
<td>• Management Tools</td>
</tr>
<tr>
<td></td>
<td>◦ IIS Management Console</td>
</tr>
<tr>
<td>IIS Management Scripts and Tools</td>
<td>• IIS Management Service</td>
</tr>
<tr>
<td></td>
<td>• Web Management Tools</td>
</tr>
<tr>
<td>Category</td>
<td>Feature</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>.NET Framework 4.5 Features</td>
<td>• .NET Framework 4.5</td>
</tr>
<tr>
<td></td>
<td>• ASP.NET 4.5</td>
</tr>
<tr>
<td></td>
<td>• Windows Communication Foundation (WCF) HTTP Activation45</td>
</tr>
<tr>
<td></td>
<td>◦ TCP Activation</td>
</tr>
<tr>
<td></td>
<td>◦ HTTP Activation</td>
</tr>
<tr>
<td></td>
<td>◦ Message Queuing (MSMQ) Activation</td>
</tr>
<tr>
<td>Message Queuing</td>
<td>• Message Queuing Services</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Message Queue (MSMQ) Server</td>
</tr>
<tr>
<td>Windows Process Activation</td>
<td>• Process Model</td>
</tr>
<tr>
<td>Service</td>
<td></td>
</tr>
<tr>
<td>Configuration APIs</td>
<td>All</td>
</tr>
</tbody>
</table>
Troubleshooting

If you encounter unexpected behavior or failure while installing Storage Replication Adapter (SRA) 4.0, you can use the installation log files to identify the cause and resolve the issue.

SnapCenter installation fails to create DB with the error Invalid username/password, please try again

Description
After uninstalling SnapCenter and initiating a fresh installation, the installation fails because a hidden MySQL folder exists.

Error message
The SnapCenter installer displays the following message: Invalid username/password, please try again, and the installation log displays the message

```
CreateDB: Invalid username/password, please try again
CreateDB: ERROR exception: Access denied for user
```

Corrective action
1. Find and remove the MySQL folder from C:\ProgramData.
2. Run the SnapCenter installer again.

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.

About this task
Only a cluster administrator can perform AutoSupport management. The Storage Virtual Machine (SVM) administrator has no access to AutoSupport.

To have email notifications sent from all storage systems to which SnapCenter has access, a cluster administrator must enable AutoSupport on each storage system node.

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`
SnapCenter Plug-in Package for Microsoft Windows or SnapCenter Plug-in for Microsoft SQL Server upgrade might fail on hosts with SQL databases on VMDK

**Description**
When upgrading SnapCenter Plug-in for Microsoft Windows or SnapCenter Plug-in for Microsoft SQL Server on hosts with SQL databases on VMDK, the upgrade might fail.

**Error message**
The installation log displays the error `Engine: error 80070002 while running parcel operations`.

**Workaround**
Delete the following directories on the plug-in host:
- `C:\Windows\SnapCenter plugin``
- All files and directories in `C:\Users\Administrator.domain_name\AppData\Local\Downloaded Installations`

If the upgrade does not succeed after you delete the specified files and directories, you might need to reboot the SQL server host, and then delete the files and directories.

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 an incorrect Java version

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

Corrective action
1. Add the Java executable path to the `PATH` environmental variable.
2. Add the environment variable `JAVA_HOME` to the `.bashrc` file for the root user.
   For example, `JAVA_HOME=/usr/java/jre1.8.0_60`
3. 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.
4. Verify if the SPL service is running by entering the following command:
   `Ps -ef | grep spl`
5. If SPL service is still running, kill the process by running the following command:
   `Kill -9 process_id`
SnapCenter Plug-ins Package for Linux installation fails

Description
After installing SnapCenter and adding hosts, installing the SnapCenter Plug-ins Package for Linux fails and the plug-in discovery operation cannot be performed. This issue occurs because of disconnection between SnapCenter and the host during plug-in installation.

Corrective action
You must perform the following steps:

1. Find the status of the SPL service by running the following command:
   ```bash
   /custom_location/NetApp/snapcenter/spl/bin/spl status
   ```
2. Manually uninstall the plug-in by running the following command:
   ```bash
   /custom_location/NetApp/snapcenter/spl/installation/plugins uninstall
   ```
3. Verify if the SPL service is running by entering the following command:
   ```bash
   Ps -ef | grep spl
   ```
4. If SPL service is still running, kill the process by running the following command:
   ```bash
   Kill -9 process_id
   ```

   If manual uninstallation fails, you must perform the following steps:

   1. List the RPM packages:
      ```bash
      rpm -qa | grep netapp-snapcenter-plugin
      ```
   2. Delete the RPM packages:
      ```bash
      rpm -e netapp-snapcenter-plugin-loader netapp-snapcenter-plugin-oracle
      netapp-snapcenter-plugin-unix
      ```
   3. Remove the `/var/.com.zerog.registry.xml` file manually.
   4. Verify if the SPL service is running by entering the following command:
      ```bash
      Ps -ef | grep spl
      ```
   5. If SPL service is still running, kill the process by running the following command:
      ```bash
      Kill -9 process_id
      ```

   After successfully uninstalling the plug-in, remove the host and then try again.

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.

**Registering vCenter details task displays a warning**

**Description**
You added a vSphere type of host and the Add Host operation completed successfully. However, the SnapCenter Plug-in for VMware vSphere was not able to communicate with the vCenter using the vCenter information you entered. The task "Registering vCenter details with SnapCenter Plug-in for VMware vSphere" in the operation details displays error information and is marked with a warning.

**Task marked with a warning**
Registering vCenter details with SnapCenter Plug-in for VMware vSphere.

**Corrective action**
Perform the following steps to update the vCenter information in the SnapCenter Plug-in for VMware vSphere:

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Hosts.
2. In the Hosts page, select the vSphere-type host.
3. Click the Add/Update vCenter details button.
4. In the dialog box, select the type of information you want to update:
   - Add/Update vCenter Details
   - Add/Update SnapCenter Details
5. In the dialog box, enter only the information that needs to be updated. Blank fields are not changed.
6. Click OK.
Unable to access cluster IP address from outside network

Description

There is no response when you try to access the cluster IP address from outside the network.

Corrective action

Verify that you can use **ping** to access the dedicated IP addresses of the cluster host from a computer outside the router. If this test fails and you are using multiple network adapters, the issue is not related to Network Load Balancing (NLB). If you are using a single network adapter for the dedicated and cluster IP addresses, consider the following scenarios:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using multicast support, you might find that your router has</td>
<td>Verify that you can use <strong>ping</strong> to access the cluster from a client on the cluster's subnet and the cluster host's dedicated IP address from a computer outside the router. If these tests work properly, the router is probably at fault. You should be able to add a static ARP entry to the router to circumvent the issue.</td>
</tr>
<tr>
<td>difficulty resolving the primary IP address into a multicast media access</td>
<td></td>
</tr>
<tr>
<td>control (MAC) address by using the Address Resolution Protocol (ARP)</td>
<td></td>
</tr>
<tr>
<td>When using NLB in multicast or unicast mode, routers need to accept proxy ARP responses (IP-to-network address mappings that are received with a different network source address in the ethernet frame).</td>
<td>You must ensure that that your router has proxy ARP support turned on. You can also set a static ARP entry to keep proxy ARP support disabled in the router.</td>
</tr>
<tr>
<td>Internet control message protocol (ICMP) to the cluster is blocked by a</td>
<td>Allow ICMP traffic through the router or firewall. However, allowing ICMP traffic through router or firewall might expose your system to additional security risk.</td>
</tr>
<tr>
<td>router or firewall.</td>
<td></td>
</tr>
</tbody>
</table>
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.

- **Release Notes**
  Provides important information about this release of SnapCenter Server and the SnapCenter plug-in packages, including fixed issues, known issues, cautions, limitations, and any documentation updates or corrections.
  *SnapCenter Software 2.0 Release Notes*

- **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 2.0 Administration Guide*

- **Importing Data from SnapManager to SnapCenter**
  Describes how to import data from previous versions of SnapDrive and SnapManager to your SnapCenter environment.
  *SnapCenter Software 2.0 Importing Data from SnapManager to SnapCenter*

- **Data Protection Guide for Microsoft SQL Server**
  Describes how to use SnapCenter to perform backup, restore, clone, and verification operations on Microsoft SQL Server databases.
  *SnapCenter Software 2.0 Data Protection Guide for Microsoft SQL Server*

- **Data Protection Guide for Oracle Databases**
  Describes how to use SnapCenter to perform backup, restore, and clone jobs on custom plug-in resources.
  *SnapCenter Software 2.0 Data Protection Guide for Oracle Databases*

- **Data Protection Guide for Windows File Systems**
  Provides information on how to perform backup, restore, and clone operations on Windows file systems using the SnapCenter user interface.
  *SnapCenter Software 2.0 Data Protection Guide for Windows File Systems*

- **Cloud Backup**
  Describes how to use SnapCenter to perform backup and restore operations on NAS file systems.
  *Data Fabric Solution for Cloud Backup*

- **Developer's Guide for Creating Custom Plug-ins**
  Provides information on how to create custom plug-ins.
  *SnapCenter Software 2.0 Developer's Guide for Creating Custom Plug-ins*

- **Data Protection Guide for Custom Plug-ins**
  Describes how to use SnapCenter to perform backup, restore, and clone jobs on custom plug-in resources.
  *SnapCenter Software 2.0 Data Protection Guide for Custom Plug-ins*

- **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 2.0 Windows Cmdlet Reference Guide*
• 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.
  *SnapCenter Software 2.0 Linux Command Reference Guide*

• SnapCenter Software Resources
  Provides a collection of videos, technical reports, and SnapCenter documentation.
  *NetApp SnapCenter Software Resources*
Copyright information

Copyright © 1994–2017 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

Active IQ, AltaVault, Arch Design, ASUP, AutoSupport, Campaign Express, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Element, Fitness, Flash Accel, Flash Cache, Flash Pool, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, Fueled by SolidFire, GetSuccessful, Helix Design, LockVault, Manage ONTAP, MetroCluster, MultiStore, NetApp, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANscreen,SANshare, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, SolidFire, SolidFire Helix, StorageGRID, SyncMirror, 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.

How to send comments about documentation and receive update notifications

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

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

doccomments@netapp.com

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

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

You can also contact us in the following ways:

• NetApp, Inc., 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

about this guide 7
deciding whether to use 7
access
assigning to users 50
logging in to SnapCenter 40
administrator
logging in to SnapCenter as 40
role 41, 45, 46
Application Request Routing
configuring 34
removing server farm 108
requirements for installation 35
understanding 34, 35
architecture
overview of SnapCenter components 8
ASM instance
setting up your Run As account credentials 54, 55
audience
for this guide 7
authentication
encryption 12
for Run As credential 54
setting up your Run As account 54, 55
types 54
AutoSupport
enabling email notifications 119
enabling notifications for storage system connections 51
Virtual Storage Console 98

B

backups
configuring log directory 69
resources, resource groups, and policies overview 13
using SnapMirror and SnapVault replication 76
best practices
for installing plug-ins, about 110
for uninstalling plug-ins 105
for uninstalling SnapCenter 108
for volume and share configurations 90
getting started with SnapCenter 71
setting up your Run As account 54, 55
browsers
supported versions 27

C

CIFS licenses
required for SnapCenter 32
clone operations
resources, resource groups, and policies overview 13
Cluster Shared Volumes
connecting to disks 87
creating disks 84
clusters, Microsoft
introduction to using FC RDM LUNs in 94
support limitations when using FC RDM LUNs 95
cmdlets
SnapCenter Plug-in for Microsoft Windows support 96
comments
how to send feedback about documentation 129
configuring
AutoSupport email notifications 119
host log directory 69
the frequency of software update checks 102
updating hypervisor message in host status 100
connections
required before installing SnapCenter 30
setting up for storage systems 51
credentials
setting up your Run As account 54, 55
supported for installing plug-ins for Windows 93, 94
CSV
See Cluster Shared Volume
custom plug-ins
adding resources to SnapCenter Custom Plug-ins 71

D

Data ONTAP DSM
requirements for SAN environments 25
data protection
resources, resource groups, and policies overview 13
SnapCenter 8
databases
preparing for SnapMirror replication 77
preparing storage systems for SnapVault replication 78
disks
connecting to LUNs in SnapCenter 87
creating in SnapCenter 84
deleting LUNs in SnapCenter 90
disconnecting from LUNs in SnapCenter 89
resizing in SnapCenter 87
tasks you can perform using SnapCenter 84
viewing on a host 84
documentation
additional resources 125
how to receive automatic notification of changes to 129
how to send feedback about 129
downloading
SnapCenter software updates 102

E

email notifications
enabling for AutoSupport messages 119
EMS messaging
enabling for storage systems connections 51
error messages
Error retrieving current directory 123
launching SnapCenter 120
ESX servers
   limitations of SnapCenter Plug-in for Microsoft Windows support 93

F
FC RDM LUNs
   creating shared 95
   introduction to using in Microsoft clusters 94
   Microsoft cluster support limitations when using 95
   requirements for using in Microsoft clusters 94
FC-connected LUNs
   creating 84
   introduction to configuring with SnapCenter Plug-in for Windows 81
FC/iSCSI
   host requirements 25
   features
      enabled during installation on Windows hosts 117
      of SnapCenter 8
   feedback
      how to send comments about documentation 129
Fibre Channel licenses
   required for SnapCenter 32

H
Host Utilities
   requirements for SAN, FC/iSCSI environments 25
   hosts
      adding to SnapCenter 57, 62
      creating an igroup in SnapCenter Plug-in for Microsoft Windows 82
      creating SMB shares 91
      deleting an igroup 83
      disconnecting LUNs from 89
      domain requirements for installing SnapCenter 23
      features enabled during installation on Windows 117
      licenses for SnapCenter plug-ins 32
      modifying an igroup 83
      operating systems supported 24
      provisioning Windows with SnapCenter Plug-in for Microsoft Windows 81
      remote, installing plug-ins on 62
      remote, installing prerequisites for plug-in packages on 57
      removing from SnapCenter 105, 108
      removing from SnapCenter, introduction to 105
      renaming an igroup 83
      requirements for SAN, FC/iSCSI environments 25
      space and sizing requirements for installing SnapCenter 24
      supported systems 26
      system requirements for installing SnapCenter 23
      updating status for virtual machines (VMs) 100
      viewing a list of disks on 84
HTTP
   error 503 launching SnapCenter 120
   port requirements 30
   hypervisors
      updating settings for 100

I
igroups
   creating in SnapCenter Plug-in for Microsoft Windows 82
   deleting in SnapCenter Plug-in for Microsoft Windows 83
   managing 82
   modifying 83
   purpose 82
   renaming 83
   information
      how to send feedback about improving documentation 129
   initiators
      adding to an igroup 83
      creating an igroup 82
   installation
      connection and port requirements for SnapCenter 30
      domain requirements for packages 23
      features enabled on Windows hosts 117
      monitoring 68
      operating systems supported 24
      plug-in checklist 59
      preparing for 36
      required information 36
      SAN, FC/iSCSI host requirements 25
      SnapCenter Plug-in Loader service 74
      space and sizing requirements for packages 24
      space requirements for packages 23
      troubleshooting invalid username and password issues 119
   installation fails
      improper uninstallation 121
      incorrect Java version 121
   plug-in 122
   installing
      on multiple hosts 67
      plug-in packages on remote hosts 62
      plug-ins independently, about 110
      preparation overview 20
      prerequisites for plug-in packages on remote hosts 57
      SnapCenter 38
      SnapCenter and the plug-ins, overview of 38
      SnapCenter process overview for new users 18
      SnapCenter process overview for SnapManager users 15
   Internet Explorer Protected Mode
      disabling 120
   iSCSI
      disconnecting a session 82
      establishing a session 81
      licenses required for SnapCenter 32
   iSCSI-connected LUNs
      creating 84
      introduction to configuring with SnapCenter Plug-in for Windows 81
   jobs
      backups, configuring the log for 69
identifying available resources for monitoring progress of plug-in package installation

L

licensing
for existing SnapManager products for SnapCenter
limitations
support when using FC RDM LUNs in Microsoft clusters
VMware ESX server-related
Linux
operating systems supported
setting up your Run As account credentials on host
load balancing
best practices
using Application Request Routing
local hosts
troubleshooting issues with displaying web login page
log out period
modifying
logging in
as a SnapCenter administrator
as a SnapCenter user
SnapCenter
with more than one role
LUN storage
introduction to configuring with SnapCenter Plug-in for Windows
LUNs
connecting to in SnapCenter
creating in SnapCenter
creating shared FC RDM
deleting in SnapCenter
disconnecting before deleting
disconnecting in SnapCenter
disk-related tasks you can perform using SnapCenter
FC RDM, requirements for using in a Microsoft cluster
introduction to creating and managing using SnapCenter Plug-in for Microsoft Windows in VMware environments
prerequisites for iSCSI connections
RDM, support through PowerShell cmdlets
RDM, troubleshooting creation of
resizing in SnapCenter
LUNs, FC RDM
FC RDM Microsoft cluster support limitations when using
introduction to using in Microsoft clusters
M

messages
enabling AutoSupport email notifications
Microsoft clusters
introduction to using FC RDM LUNs in
support limitations when using FC RDM LUNs
Microsoft SQL Server
independently installing SnapCenter Plug-in
silently installing SnapCenter Plug-in from command line
MySQL Server
identifying a repository for SnapCenter metadata
N

Network Load Balancing
configuring
removing cluster
understanding
NFS licenses
required for SnapCenter
non-root user
installing plug-in for Oracle databases
notifications
enabling for AutoSupport email
O

ONTAP
account permission requirements for SnapCenter
supported versions
ONTAP CLI commands
creating SVM roles
operating systems
supported for SnapCenter
Oracle Database
independently installing SnapCenter Plug-in
installing SnapCenter Plug-in from command line
interactively installing SnapCenter Plug-in
plug-in support for virtualized
plug-in support for VMs
setting up your Run As account credentials
versions supported
P

permissions
associated with pre-defined roles
list
role-based access control
setting for applications
understanding how to set
plug-in loader
failure
plug-in packages
installing on remote hosts
introduction to installing
prerequisites to installing
upgrading
plug-ins
about installing independently
configuring
deployment checklist
description
installing for Microsoft SQL Server independently
112
installing for Microsoft SQL Server silently from command line 113
installing for Microsoft Windows independently 110
installing for Microsoft Windows silently from command line 110
installing for Oracle Database from command line 115
installing for Oracle Database independently 114
installing for Oracle Database interactively 114
installing on multiple hosts 67
installing SnapCenter Plug-in for VMware vSphere silently from command line 115
monitoring package installation 68
overview of installing SnapCenter and preparation to install for Microsoft Windows 110
preparation to install for Oracle Database 114
preparation to install Microsoft SQL server 112
removing from a host 105
space and sizing requirements for SnapCenter installation 24
uninstalling from SnapCenter, introduction to 105
uninstalling locally on host 107
uninstalling using command line 106, 107
updating SnapCenter information in SnapCenter Plug-in for VMware vSphere 100
updating vCenter information in SnapCenter Plug-in for VMware vSphere 100, 123
plug-ins package for Linux
uninstalling using command line 107
plug-ins package for Windows
uninstalling locally on host 107
uninstalling using command line 106
policies
used in SnapCenter data protection 13
port requirements
before installing SnapCenter 30
ports
modifying 30
PowerShell cmdlets
reclaiming storage space with 92
SnapCenter Plug-in for Microsoft Windows support 96

R

RDM
minimum vCenter privileges required for operations 93
RDM LUNs
creating shared FC 95
introduction to using FC in Microsoft clusters 94
Microsoft cluster support limitations when using for FC 95
requirements for FC support 94
troubleshooting creation of 95
registering
Virtual Storage Console with SnapCenter 98
remote hosts
installing plug-in packages on 62
prerequisites for installing plug-in packages on 57
remote installation
on multiple hosts 67
remote plug-in installation
increasing timeout for 68
removing
a host from SnapCenter 105, 108
hosts from SnapCenter, introduction to 105
the Application Request Routing server farm 108
the Network Load Balancing cluster 108
the SnapCenter repository 108
replication
considerations for preparing storage systems for SnapMirror and SnapVault 76
preparing storage systems for SnapMirror 77
preparing storage systems for SnapVault 78
repositories
for SnapCenter, overview of 8
identifying for SnapCenter metadata 34
requirements
Application Request Routing 35
connection and port, before installing SnapCenter 30
for SnapCenter installation 36
resizing
disks 87
LUNs 87
resource groups
used in SnapCenter data protection 13
resources
adding to SnapCenter Custom Plug-ins 71
discovering 71
identifying available 71
used in SnapCenter data protection 13
virtualized environments 97
restore operations
resources, resource groups, and policies overview 13
role-based access control
adding users to a role 49
assigning access to users 50
introduction to configuring for SnapCenter users 41
list of roles and permissions 45
pre-defined roles and permissions 46
understanding 41
roles
adding users to 49
app backup and clone admin role, defined 46
available pre-defined 46
backup and clone viewer role, defined 46
infrastructure admin role, defined 46
list of 45
understanding role-based access control 41
Run As account
authentication methods 54
overview 41
setting up 54, 55
S

SAN environments
host requirements 25
security
modifying default log out period 13
overview 12
servers
SQL, preparation to install SnapCenter plug-in for 112
SQL, silently installing SnapCenter plug-in for 113
VMware ESX limitations of SnapCenter Plug-in for Microsoft Windows support 93
shared FC RDM LUNs
  creating 95
  using in a Microsoft cluster 95
shares, SMB
  creating in SnapCenter Plug-in for Microsoft Windows 91
  deleting in SnapCenter 91
SMB shares
  creating in SnapCenter Plug-in for Microsoft Windows 91
  deleting in SnapCenter 91
SnapCenter
  adding a VSC host 98
  archiving Snapshot copies 78
  components 8
  connection and port requirements for installation 30
  data protection 8
  finding the URL 40
  installation process overview for new users 18
  installation process overview for SnapManager users 15
  installation worksheet 36
  installing 38
  introduction to configuring role-based access control for users 41
  mirroring Snapshot copies 77
  overview 8
  registering Virtual Storage Console with 98
  removing repository 108
  templates for creating SMB shares 91
  uninstalling 108
  uninstalling, introduction to 105
  upgrading plug-in packages 104
SnapCenter Plug-in for Linux installation failure 121, 122
SnapCenter Plug-in for Microsoft SQL Server
  installing independently 112
  installing silently from command line 113
  overview of components 8
  preparation to install 112
SnapCenter Plug-in for Microsoft Windows
  creating an igroup 82
  creating SMB shares 91
  deleting an igroup 83
  installing independently 110
  installing silently from command line 110
  limitations when using VMware ESX server 93
  modifying an igroup 83
  overview of components 8
  PowerShell cmdlet support 96
  preparation to install 110
  prerequisites to install 110
  renaming an igroup 83
SnapCenter Plug-in for Oracle Database
  installing in console mode from command line 115
  installing in silent mode from command line 115
  installing independently 114
  installing interactively 114
  overview of components 8
  preparation to install 114
SnapMirror
  considerations for preparing storage systems for replication 76
  differences from SnapVault 76
  licenses required for SnapCenter 32
  preparing storage systems for replication 77
Snapshot copies
  features in SnapCenter 8
  introduction to managing using SnapCenter Plug-in for Microsoft Windows in VMware environments 92
  preparing for SnapVault replication 78
  preparing storage systems for SnapMirror replication 77
SnapVault
  considerations for preparing storage systems for replication 76
  differences from SnapMirror 76
  licenses required for SnapCenter 32
  preparing storage systems for replication 78
SQL Server
  setting up your Run As account credentials 54, 55
  supported versions 26
SQL Server Database
  plug-in support for virtualized 27, 28
  plug-in support for VMs 28
storage system connections
  enabling AutoSupport notifications for 51
  enabling EMS messaging for 51
storage systems
  considerations for preparing for SnapMirror and SnapVault replication 76
  licenses for SnapCenter plug-ins 32
  reclaiming space on 92
  settings up connections to 51
storage types
  supported by plug-ins package for Linux 22
  supported by SnapCenter Plug-In for Microsoft SQL Server 20
Index | 135

T

templates
  for creating SMB shares 90
terminology
  resources, resource groups, and policies data protection 13
timeout
  increasing for remote plug-in installation 68
troubleshooting
  cannot access cluster IP address 124
  features enabled during installation 117
  HTTP error 503 120
  installation issues with invalid username and password 119
  RDM LUN creation 95
  Storage Replication Adapter installation 119
  upgrade issues with Plug-in for Microsoft SQL Server with databases on VMDK 120
  upgrade issues with Plug-in for Microsoft Windows 120
  web login page not displaying 120
Twitter
  how to receive automatic notification of documentation changes 129

U

uninstalling
  plug-ins from a host 105
  SnapCenter 108
  SnapCenter plug-ins, introduction to 105
  SnapCenter, introduction to 105
updates, software
  configuring SnapCenter to automatically check for 102
upgrade
  troubleshooting issues with Plug-in for Microsoft SQL Server with databases on VMDK 120
  troubleshooting issues with Plug-in for Microsoft Windows 120
upgrading
  overview 102
  SnapCenter 102
  SnapCenter plug-in packages 104
users
  adding to a role 49
  assigning access to 50
  introduction to configuring role-based access control for 41
  using roles at login 40

V

vCenter
  minimum privileges required for RDM operations 93
  registering fails, updating vCenter information in SnapCenter Plug-in for VMware vSphere 123
  updating SnapCenter Plug-in for VMware vSphere 100, 123
virtual disks
  tasks you can perform using SnapCenter 84
Virtual Storage Console
  adding a VSC host to SnapCenter 98
  comparison to SnapCenter Plug-in for VMware vSphere 27
  plug-in description 28
  registering with SnapCenter 98
  supported versions 26
  switching to another plug-in 97
  when to install 29
virtualized databases
  determining correct plug-in for 29
  plug-in support for 27, 28
virtualized environments
  managing virtualized resources 97
  monitoring virtualization status 99
  registering Virtual Storage Console 98
  storage types supported 20
  switching to SnapCenter Plug-in for VMware vSphere 97
VMs
  determining correct plug-in for 29
  monitoring virtualization status 99
  plug-in support for 27, 28
  supported storage types 20, 22
VMware
  ESX servers limitations of SnapCenter Plug-in for Microsoft Windows support 93
  SnapCenter Plug-in for Windows support for 93
  support for ESX iSCSI initiators 93
  support for FC HBAs 93
  support for guest OS platforms 93
  support for iSCSI HBAs 93
  support for iSCSI initiators 93
  using Virtual Storage Console to provision Windows hosts 81
W

web address
  for SnapCenter 40
web login page
  troubleshooting issues with displaying on local host 120
Windows file systems
  plug-in support for virtualized 27, 28
Windows hosts
  creating an igroup in SnapCenter Plug-in for
    Microsoft Windows 82
  features enabled during installation 117
  independently installing SnapCenter Plug-in for 110
  silently installing SnapCenter Plug-in from command line 110
Windows Process Activation Service (WAS)
  enabling 120
Windows Server
  operating systems supported 24
  failover clusters
    requirements for connecting to a disk 87
    requirements for creating a disk 84
workflows
  getting started 71
  SnapCenter installation for new users 18
  SnapCenter installation for SnapManager users 15