# Concepts

## SnapCenter Software 5.0

NetApp
July 18, 2024

# Table of Contents

# Concepts

## SnapCenter overview

SnapCenter Software is a simple, centralized, scalable platform that provides application-consistent data protection for applications, databases, host file systems, and VMs running on ONTAP systems anywhere in the Hybrid Cloud.

SnapCenter leverages NetApp Snapshot, SnapRestore, FlexClone, SnapMirror, and SnapVault technologies to provide the following:

- Fast, space-efficient, application-consistent, disk-based backups
- Rapid, granular restore, and application-consistent recovery
- Quick, space-efficient cloning

SnapCenter includes both SnapCenter Server and individual lightweight plug-ins. You can automate deployment of plug-ins to remote application hosts, schedule backup, verification, and clone operations, and monitor all data protection operations.

SnapCenter can be deployed in the following ways:

- On premise to protect the following:
  - Data that is on ONTAP FAS, AFF, or All SAN Array (ASA) primary systems and replicated to ONTAP FAS, AFF, or ASA secondary systems
  - Data that is on ONTAP Select primary systems
  - Data that is on ONTAP FAS, AFF, or ASA primary and secondary systems and protected to local StorageGRID object storage
- On premise in a Hybrid Cloud to protect the following:
  - Data that is on ONTAP FAS, AFF, or ASA primary systems and replicated to Cloud Volumes ONTAP
  - Data that is on ONTAP FAS, AFF, or ASA primary and secondary systems and protected to object and archive storage in cloud (using BlueXP backup and recovery integration)
- In a public cloud to protect the following:
  - Data that is on Cloud Volumes ONTAP (formerly ONTAP Cloud) primary systems
  - Data that is on Amazon FSX for ONTAP
  - Data that is on primary Azure NetApp Files (Oracle, Microsoft SQL, and SAP HANA)

SnapCenter includes the following key features:

- Centralized, application-consistent data protection

  Data protection is supported for Microsoft Exchange Server, Microsoft SQL Server, Oracle Databases on Linux or AIX, SAP HANA database, and Windows Host Filesystems running on ONTAP systems.

  Data protection is also supported for other standard or custom applications and databases by providing a framework to create user-defined SnapCenter plug-ins. This enables data protection for other applications and databases from the same single-pane-of-glass. By leveraging this framework, NetApp has released SnapCenter custom plug-ins for IBM DB2, MongoDB, MySQL etc. on the NetApp Automation Store.

NetApp Storage Automation Store

- Policy-based backups

  Policy-based backups leverage NetApp Snapshot technology to create fast, space-efficient, application-consistent, disk-based backups. Optionally, you can automate protection of these backups to secondary storage by updates to existing protection relationships.

- Back ups for multiple resources

  You can back up multiple resources (applications, databases, or host file systems) of the same type, at the same time, by using SnapCenter resource groups.

- Restore and recovery

  SnapCenter provides rapid, granular restores of backups and application-consistent, time-based recovery. You can restore from any destination in the Hybrid Cloud.

- Cloning

  SnapCenter provides quick, space-efficient, application-consistent cloning, which enables accelerated software development. You can clone on any destination in the Hybrid Cloud.

- Single user management graphical user interface (GUI)

  The SnapCenter GUI provides a single, one-stop interface for managing backups and clones of a resource in any destination in the Hybrid Cloud.

- REST APIs, Windows cmdlets, UNIX commands

  SnapCenter includes REST APIs for most functionality for integration with any orchestration software, and use of Windows PowerShell cmdlets and command-line interface.

  For more information on REST APIs see REST API overview.

  For more information on Windows cmdlets see SnapCenter Software Cmdlet Reference Guide.

  For more information on UNIX commands see SnapCenter Software Command Reference Guide.

- Centralized data protection Dashboard and reporting
- Role-Based Access Control (RBAC) for security and delegation.
- Repository database with High Availability

  SnapCenter provides a built-in repository database with High Availability to store all backup metadata.

- Automated push install of plug-ins

  You can automate a remote push of SnapCenter plug-ins from the SnapCenter Server host to application hosts.

- High Availability

  High availability for SnapCenter is set up using external load balancer (F5). Up to two nodes are supported within the same datacenter.

- Disaster Recovery (DR)

  You can recover the SnapCenter Server in the event of disasters like resource corruption or server crash.

- SnapLock

  SnapLock is a high-performance compliance solution for organizations that use write once, read many (WORM) storage to retain files in unmodified form for regulatory and governance purposes.

  For more information on SnapLock refer What SnapLock is

- SnapMirror Business Continuity (SM-BC)

  SnapMirror Business Continuity (SM-BC) enables business services to continue operating even through a complete site failure, supporting applications to fail over transparently using a secondary copy. Neither manual intervention nor additional scripting is required to trigger a failover with SM-BC.

  The plug-ins supported for this feature are SnapCenter Plug-in for SQL Server, SnapCenter Plug-in for Windows, and SnapCenter Plug-in for Oracle database.

  For more information on SM-BC refer SnapMirror Business Continuity (SM-BC)

  For SM-BC, ensure that you have met the various hardware, software, and system configuration requirements. For more information refer Prerequisites

- Synchronous mirroring

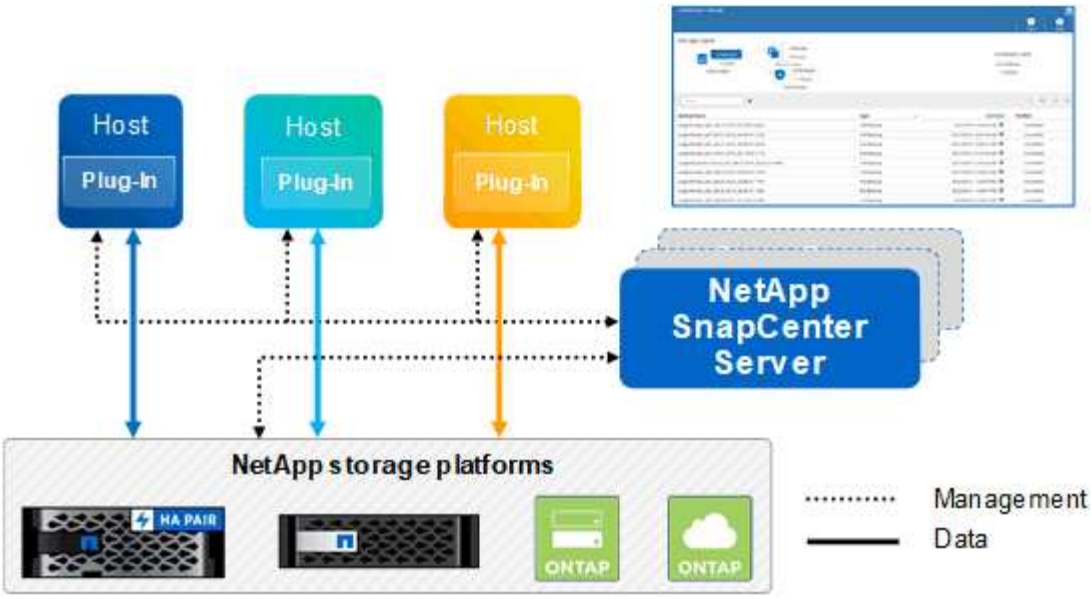
  The Synchronous mirroring feature provides online, real-time data replication between storage arrays over a remote distance.

  For more information on Sync mirror refer Synchronous mirroring overview

## SnapCenter architecture

The SnapCenter platform is based on a multitiered architecture that includes a centralized management server (SnapCenter Server) and a SnapCenter plug-in host.

SnapCenter supports multisite data center. The SnapCenter Server and the plug-in host can be at different geographical locations.




## SnapCenter components

SnapCenter consists of the SnapCenter Server and SnapCenter plug-ins. You should install only the plug-ins that are appropriate for the data you want to protect.

- SnapCenter Server
- SnapCenter Plug-ins Package for Windows, which includes the following plug-ins:
  - SnapCenter Plug-in for Microsoft SQL Server
  - SnapCenter Plug-in for Microsoft Windows
  - SnapCenter Plug-in for Microsoft Exchange Server
  - SnapCenter Plug-in for SAP HANA Database
- SnapCenter Plug-ins Package for Linux, which includes the following plug-ins:
  - SnapCenter Plug-in for Oracle Database
  - SnapCenter Plug-in for SAP HANA Database
  - SnapCenter Plug-in for UNIX file systems
- SnapCenter Plug-ins Package for AIX, which includes the following plug-ins:
  - SnapCenter Plug-in for Oracle Database
  - SnapCenter Plug-in for UNIX file systems
- SnapCenter Custom Plug-ins

  Custom plug-ins are community-supported and can be downloaded from the NetApp Storage Automation Store.

SnapCenter Plug-in for VMware vSphere, formerly NetApp Data Broker, is a standalone virtual appliance that supports SnapCenter data protection operations on virtualized databases and file systems.

## SnapCenter Server

The SnapCenter Server includes a web server, a centralized HTML5-based user interface, PowerShell

cmdlets, REST APIs, and the SnapCenter repository.

SnapCenter enables high availability and horizontal scaling across multiple SnapCenter Servers within a single user interface. You can accomplish high availability by using external load balancer (F5). For larger environments with thousands of hosts, adding multiple SnapCenter Servers can help balance the load.

- If you are using the SnapCenter Plug-ins Package for Windows, the host agent runs on the SnapCenter Server and Windows plug-in host. The host agent executes the schedules natively on the remote Windows host, or for Microsoft SQL Servers, the schedule is executed on the local SQL instance.

  The SnapCenter Server communicates with the Windows plug-ins through the host agent.

- If you are using the SnapCenter Plug-ins Package for Linux or the SnapCenter Plug-ins Package for AIX, schedules are executed on the SnapCenter Server as Windows task schedules.
  - For SnapCenter Plug-in for Oracle Database, the host agent that runs on the SnapCenter Server host communicates with the SnapCenter Plug-in Loader (SPL) that runs on the Linux or AIX host to perform different data protection operations.
  - For SnapCenter Plug-in for SAP HANA Database and SnapCenter Custom Plug-ins, the SnapCenter Server communicates with these plug-ins through the SCCore agent that runs on the host.

The SnapCenter Server and plug-ins communicate with the host agent using HTTPS. Information about SnapCenter operations is stored in the SnapCenter repository.

SnapCenter supports disjoint namespace for Windows hosts. If you face issues when using disjoint namespace, refer to SnapCenter is unable to discover resources when using disjoint namespace.

## SnapCenter plug-ins

Each SnapCenter plug-in supports specific environments, databases, and applications.

| Plug-in name | Included in install package | Requires other plug-ins | Installed on host | Platform supported |
|---|---|---|---|---|
| Plug-in for SQL Server | Plug-ins Package for Windows | Plug-in for Windows | SQL Server host | Windows |
| Plug-in for Windows | Plug-ins Package for Windows | | Windows host | Windows |
| Plug-in for Exchange | Plug-ins Package for Windows | Plug-in for Windows | Exchange Server host | Windows |
| Plug-in for Oracle Database | Plug-ins Package for Linux and Plug-ins Package for AIX | Plug-in for UNIX | Oracle host | Linux or AIX |
| Plug-in for SAP HANA Database | Plug-ins Package for Linux and Plug-ins Package for Windows | Plug-in for UNIX or Plug-in for Windows | HDBSQL client host | Linux or Windows |

| Plug-in name | Included in install package | Requires other plug-ins | Installed on host | Platform supported |
|---|---|---|---|---|
| Custom Plug-ins | NetApp Storage Automation Store | For file system backups, Plug-in for Windows | Custom application host | Linux or Windows |

The SnapCenter Plug-in for VMware vSphere supports crash-consistent and VM-consistent backup and restore operations for virtual machines (VMs), datastores, and Virtual Machine Disks (VMDKs), and it supports the SnapCenter application-specific plug-ins to protect application-consistent backup and restore operations for virtualized databases and file systems.

For SnapCenter 4.1.1 users, the SnapCenter Plug-in for VMware vSphere 4.1.1 documentation has information on protecting virtualized databases and file systems. For SnapCenter 4.2.x users, the NetApp Data Broker 1.0 and 1.0.1, documentation has information on protecting virtualized databases and file systems using the SnapCenter Plug-in for VMware vSphere that is provided by the Linux-based NetApp Data Broker virtual appliance (Open Virtual Appliance format). For users using SnapCenter 4.3 or later, the SnapCenter Plug-in for VMware vSphere documentation has information on protecting virtualized databases and file systems using the Linux-based SnapCenter Plug-in for VMware vSphere virtual appliance (Open Virtual Appliance format).

### SnapCenter Plug-in for Microsoft SQL Server features

- Automates application-aware backup, restore, and clone operations for Microsoft SQL Server databases in your SnapCenter environment.
- Supports Microsoft SQL Server databases on VMDK and raw device mapping (RDM) LUNs when you deploy the SnapCenter Plug-in for VMware vSphere and register the plug-in with SnapCenter
- Supports provisioning SMB shares only. Support is not provided for backing up SQL Server databases on SMB shares.
- Supports importing backups from SnapManager for Microsoft SQL Server to SnapCenter.

### SnapCenter Plug-in for Microsoft Windows features

- Enables application-aware data protection for other plug-ins that are running in Windows hosts in your SnapCenter environment
- Automates application-aware backup, restore, and clone operations for Microsoft file systems in your SnapCenter environment
- Supports storage provisioning, Snapshot consistency, and space reclamation for Windows hosts

The Plug-in for Windows provisions SMB shares and Windows file systems on physical and RDM LUNs but does not support backup operations for Windows file systems on SMB shares.

### SnapCenter Plug-in for Microsoft Exchange Server features

- Automates application-aware backup and restore operations for Microsoft Exchange Server databases and Database Availability Groups (DAGs) in your SnapCenter environment
- Supports virtualized Exchange Servers on RDM LUNs when you deploy the SnapCenter Plug-in for VMware vSphere and register the plug-in with SnapCenter

### SnapCenter Plug-in for Oracle Database features

- Automates application-aware backup, restore, recovery, verify, mount, unmount, and clone operations for Oracle databases in your SnapCenter environment
- Supports Oracle databases for SAP, however, SAP BR*Tools integration is not provided

### SnapCenter Plug-in for UNIX features

- Enables the Plug-in for Oracle Database to perform data protection operations on Oracle databases by handling the underlying host storage stack on Linux or AIX systems
- Supports Network File System (NFS) and storage area network (SAN) protocols on a storage system that is running ONTAP.
- For Linux systems, Oracle databases on VMDK and RDM LUNs is supported when you deploy the SnapCenter Plug-in for VMware vSphere and register the plug-in with SnapCenter.
- Supports Mount Guard for AIX on SAN filesystems and LVM layout.
- Supports Enhanced Journaled File System (JFS2) with inline logging on SAN filesystems and LVM layout for AIX systems only.

  SAN native devices, filesystems, and LVM layouts built on SAN devices are supported.

- Automates application-aware backup, restore, and clone operations for UNIX file systems in your SnapCenter environment

### SnapCenter Plug-in for SAP HANA Database features

- Automates application-aware backup, restore, and cloning of SAP HANA databases in your SnapCenter environment

### SnapCenter Custom Plug-ins features

- Supports custom plug-ins to manage applications or databases that are not supported by other SnapCenter plug-ins. Custom plug-ins are not provided as part of the SnapCenter installation.
- Supports creating mirror copies of backup sets on another volume and performing disk-to-disk backup replication.
- Supports both Windows and Linux environments. In Windows environments, custom applications via custom plug-ins can optionally utilize SnapCenter Plug-in for Microsoft Windows to take file system consistent backups.

MySQL, DB2, and MongoDB custom plug-in samples for SnapCenter Software can be downloaded from the NetApp Storage Automation Store.

MySQL, DB2, and MongoDB custom plug-ins are supported via the NetApp communities only.

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

For more information, see Develop a plug-in for your application

### SnapCenter repository

The SnapCenter repository, sometimes referred to as the NSM database, stores information and metadata for every SnapCenter operation.

MySQL Server repository database is installed by default when you install the SnapCenter Server. If MySQL Server is already installed and you are doing a fresh installation of SnapCenter Server, you should uninstall MySQL Server.

SnapCenter supports MySQL Server 5.7.25 or later as the SnapCenter repository database. If you were using an earlier version of MySQL Server with an earlier release of SnapCenter, during SnapCenter upgrade, the MySQL Server is upgraded to 5.7.25 or later.

The SnapCenter repository stores the following information and metadata:

- 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

# 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 using the authorized CA certificates provided by the customer.
- SnapCenter 4.1.1 or later supports Transport Layer Security (TLS) 1.2 for communication with ONTAP. You can also use TLS 1.2 for communication between clients and servers.

  From 5.0, SnapCenter supports (TLS) 1.3 for communication with ONTAP.

- SnapCenter supports a certain set of SSL Cipher suites to provide security across network communication.

  For more information, see How to configure supported SSL Cipher Suite.

- 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 encrypted with AES encryption, which expire after 24 hours.
- SnapCenter integrates with Windows Active Directory for login and role-based access control (RBAC) that govern access permissions.
- IPsec is supported with SnapCenter on ONTAP for Windows and Linux host machines. Learn more.

- 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. You can modify the log out period.
- Login is temporarily disabled after 5 or more incorrect login attempts.
- Supports CA certificate authentication between SnapCenter Server and ONTAP. Learn more.
- Integrity Verifier is added to the SnapCenter Server and the plug-ins and it validates all the shipped binaries during fresh installation and upgrade operations.

### CA Certificate Overview

The SnapCenter Server installer enables the Centralized SSL Certificate Support during installation. To enhance the secured communication between the server and the plug-in, SnapCenter supports using the authorized CA certificates provided by the customer.

You should deploy CA certificates after installing the SnapCenter Server and the respective plug-ins. For more information, see Generate CA Certificate CSR file.

You can also deploy CA certificate for SnapCenter plug-in for VMware vSphere. For more information, see Create and import certificates.

### Two-way SSL communication

Two-way SSL communication secures the mutual communication between SnapCenter Server and the plug-ins.

### Certificate based authentication Overview

Certificate based authentication verifies the authenticity of respective users who try to access the SnapCenter plug-in host. User should export the SnapCenter Server certificate without private key and import it in the plug-in host trusted store. Certificate based authentication works only if the two-way SSL feature is enabled.

### Multi-factor authentication (MFA)

MFA uses a third-party Identity Provider (IdP) via the Security Assertion Markup Language (SAML) to manage user sessions. This functionality enhances the authentication security by having an option to use multiple factors such as TOTP, biometrics, push notifications etc. along with the existing username & password. Also, it enables the customer to use their own user identity providers to get unified user login (SSO) across their portfolio.

MFA is applicable only for SnapCenter Server UI login. The logins are authenticated through the IdP Active Directory Federation Services (AD FS). You can configure various authentication factors at AD FS. SnapCenter is the service provider and you should configure SnapCenter as a relying party in AD FS. To enable MFA in SnapCenter, you will require the AD FS metadata.

For information to enable MFA, see Enable Multi-factor authentication.

# SnapCenter role-based access control (RBAC)

## Types of RBAC

SnapCenter role-based access control (RBAC) and ONTAP permissions enable SnapCenter administrators to delegate control of SnapCenter resources to different users or groups of users. This centrally managed access empowers application administrators to work securely within delegated environments.

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 or group to roles, and then add resource access to those users or groups.

> You cannot use SnapCenter to create user or group accounts. You should create user or group accounts in Active Directory of the operating system or database.

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

- SnapCenter RBAC
- SnapCenter plug-in RBAC (for some plug-ins)
- Application-level RBAC
- ONTAP permissions

### SnapCenter RBAC

#### Roles and permissions

SnapCenter ships with predefined roles with permissions already assigned. You can assign users or groups of users to these roles. You can also create new roles and manage permissions and users.

### Assigning permissions to users or groups

You can assign permissions to users or groups to access SnapCenter objects such as hosts, storage connections, and resource groups. 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.

> If you create a custom role, it must contain all of the permissions of the SnapCenter Admin role. If you only copy some of the permissions, for example, Host add or Host remove, you cannot perform those operations.

#### 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 credentials to verify that authorized SnapCenter users also have application-level permissions.

For example, if you want to perform Snapshot and data protection operations in a SQL Server environment, you must set credentials with the proper Windows or SQL credentials. The SnapCenter Server authenticates the credentials set using either method. If you want to perform Snapshot and data protection operations in a Windows file system environment on ONTAP storage, the SnapCenter admin role must have admin privileges on the Windows host.

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 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.

#### SnapCenter Plug-in for VMware vSphere RBAC

If you are using the SnapCenter VMware plug-in for VM-consistent data protection, the vCenter Server provides an additional level of RBAC. The SnapCenter VMware plug-in supports both vCenter Server RBAC and Data ONTAP RBAC.

For information, see SnapCenter Plug-in for VMware vSphere RBAC

#### ONTAP permissions

You should create vsadmin account with required permissions to access the storage system.

For information to create the account and assign permissions, see Create an ONTAP cluster role with minimum privileges

## RBAC permissions and roles

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

#### SnapCenter roles

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

When you assign a role to a user, only jobs that are relevant to that user are visible in the Jobs page unless you assigned the SnapCenter Admin role.

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

#### SnapCenter Plug-in for VMware vSphere roles

For managing VM-consistent data protection of VMs, VMDKs, and datastores, the following roles are created in vCenter by the SnapCenter Plug-in for VMware vSphere:

- SCV Administrator
- SCV View
- SCV Backup
- SCV Restore
- SCV Guest File Restore

For more information, see Types of RBAC for SnapCenter Plug-in for VMware vSphere users

**Best Practice:** NetApp recommends that you create one ONTAP role for SnapCenter Plug-in for VMware vSphere operations and assign it all the required privileges.

#### 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 or Uninstall

  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)
- Job Monitor

  Job Monitor permission enables members of different roles to see the operations on all the objects to which they are assigned.

## Pre-defined SnapCenter 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.

SnapCenter includes the following pre-defined roles:

- SnapCenter Admin role
- App Backup and Clone Admin role
- Backup and Clone Viewer 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.

| Permissions | Enabled | Create | Read | Update | Delete |
|---|---|---|---|---|---|
| Resource Group | Not applicable | Yes | Yes | Yes | Yes |
| Policy | Not applicable | Yes | Yes | Yes | Yes |
| Backup | Not applicable | Yes | Yes | Yes | Yes |
| Host | Not applicable | Yes | Yes | Yes | Yes |
| Storage Connection | Not applicable | No | Yes | No | No |
| Clone | Not applicable | Yes | Yes | Yes | Yes |
| Provision | Not applicable | No | Yes | No | No |

| Permissions | Enabled | Create | Read | Update | Delete |
|---|---|---|---|---|---|
| Dashboard | Yes | Not applicable | Not applicable | Not applicable | Not applicable |
| Reports | Yes | Not applicable | Not applicable | Not applicable | Not applicable |
| Restore | Yes | Not applicable | Not applicable | Not applicable | Not applicable |
| Resource | Yes | Yes | Yes | Yes | Yes |
| Plug-in Install/Uninstall | No | Not applicable | | Not applicable | Not applicable |
| Migration | No | Not applicable | Not applicable | Not applicable | Not applicable |
| Mount | Yes | Yes | Not applicable | Not applicable | Not applicable |
| Unmount | Yes | Yes | Not applicable | Not applicable | Not applicable |
| Full Volume Restore | No | No | Not applicable | Not applicable | Not applicable |
| Job Monitor | Yes | Not applicable | Not applicable | Not applicable | Not applicable |

**Backup and Clone Viewer role**

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

| Permissions | Enabled | Create | Read | Update | Delete |
|---|---|---|---|---|---|
| Resource Group | Not applicable | No | Yes | No | No |
| Policy | Not applicable | No | Yes | No | No |
| Backup | Not applicable | No | Yes | No | No |
| Host | Not applicable | No | Yes | No | No |
| Storage Connection | Not applicable | No | Yes | No | No |
| Clone | Not applicable | No | Yes | No | No |
| Provision | Not applicable | No | Yes | No | No |

| Permissions | Enabled | Create | Read | Update | Delete |
|---|---|---|---|---|---|
| Dashboard | Yes | Not applicable | Not applicable | Not applicable | Not applicable |
| Reports | Yes | Not applicable | Not applicable | Not applicable | Not applicable |
| Restore | No | No | Not applicable | Not applicable | Not applicable |
| Resource | No | No | Yes | Yes | No |
| Plug-in Install/Uninstall | No | Not applicable | Not applicable | Not applicable | Not applicable |
| Migration | No | Not applicable | Not applicable | Not applicable | Not applicable |
| Mount | Yes | Not applicable | Not applicable | Not applicable | Not applicable |
| Unmount | Yes | Not applicable | Not applicable | Not applicable | Not applicable |
| Full Volume Restore | No | Not applicable | Not applicable | Not applicable | Not applicable |
| Job Monitor | Yes | Not applicable | Not applicable | Not applicable | Not applicable |

**Infrastructure Admin role**

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

| Permissions | Enabled | Create | Read | Update | Delete |
|---|---|---|---|---|---|
| Resource Group | Not applicable | Yes | Yes | Yes | Yes |
| Policy | Not applicable | No | Yes | Yes | Yes |
| Backup | Not applicable | Yes | Yes | Yes | Yes |
| Host | Not applicable | Yes | Yes | Yes | Yes |
| Storage Connection | Not applicable | Yes | Yes | Yes | Yes |
| Clone | Not applicable | No | Yes | No | No |
| Provision | Not applicable | Yes | Yes | Yes | Yes |

| Permissions | Enabled | Create | Read | Update | Delete |
|---|---|---|---|---|---|
| Dashboard | Yes | Not applicable | Not applicable | Not applicable | Not applicable |
| Reports | Yes | Not applicable | Not applicable | Not applicable | Not applicable |
| Restore | Yes | Not applicable | Not applicable | Not applicable | Not applicable |
| Resource | Yes | Yes | Yes | Yes | Yes |
| Plug-in Install/Uninstall | Yes | Not applicable | Not applicable | Not applicable | Not applicable |
| Migration | No | Not applicable | Not applicable | Not applicable | Not applicable |
| Mount | No | Not applicable | Not applicable | Not applicable | Not applicable |
| Unmount | No | Not applicable | Not applicable | Not applicable | Not applicable |
| Full Volume Restore | No | No | Not applicable | Not applicable | Not applicable |
| Job Monitor | Yes | Not applicable | Not applicable | Not applicable | Not applicable |

# SnapCenter Disaster Recovery

You can recover the SnapCenter Server in the event of disasters like resource corruption or server crash using the SnapCenter disaster recovery (DR) feature. You can recover SnapCenter repository, server schedules, and server configuration components. You can also recover the SnapCenter Plug-in for SQL Server and SnapCenter Plug-in for SQL Server storage.

This section describes the two types of disaster recovery (DR) in SnapCenter:

**SnapCenter Server DR**

- SnapCenter Server data is backed up and can be recovered without any plug-in added to or managed by the SnapCenter Server.
- Secondary SnapCenter Server should be installed on the same installation directory and on the same port as the primary SnapCenter Server.
- For Multi-factor authentication (MFA), during Snapcenter Server DR, close all the browser tabs and reopen a browser to login again. This will clear the existing or active session cookies and update that the correct configuration data.
- SnapCenter disaster recovery functionality uses REST APIs to backup SnapCenter Server. See REST API workflows for disaster recovery of SnapCenter Server.
- Audit settings related configuration file is not backed up in DR backup and neither on the DR server after restore operation. You should manually repeat the Audit log settings.

**SnapCenter Plug-in and Storage DR**

DR is supported only for SnapCenter Plug-in for SQL Server. When the SnapCenter Plug-in for SQL Server is down, switch to a different SQL host and recover the data by performing few steps. See Disaster recovery of SnapCenter Plug-in for SQL Server.

SnapCenter uses ONTAP SnapMirror technology to replicate data. It can be used to replicate data to a secondary site for DR and keep it in sync. A failover can be initiated by breaking the replication relationship in SnapMirror. During failback the synchronization can be reversed and data from the DR site can be replicated back to the primary location.

# Resources, resource groups, and policies

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, Windows file systems, or file shares 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 **resource group** is a collection of resources on a host or cluster. The resource group can also contain resources from multiple hosts and multiple clusters.

  When you perform an operation on a resource group, you perform that operation on all 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 configure scheduled backups for single resources and resource groups.

  > If you put one host of a shared resource group on maintenance mode, and if there are schedules associated with the same shared resource group, all the scheduled operations will be suspended for all of the other hosts of the shared resource group.

  You should use a database plug-in to back up databases, a file system plug-in to back up file systems, and the SnapCenter Plug-in for VMware vSphere to backup VMs and datastores.

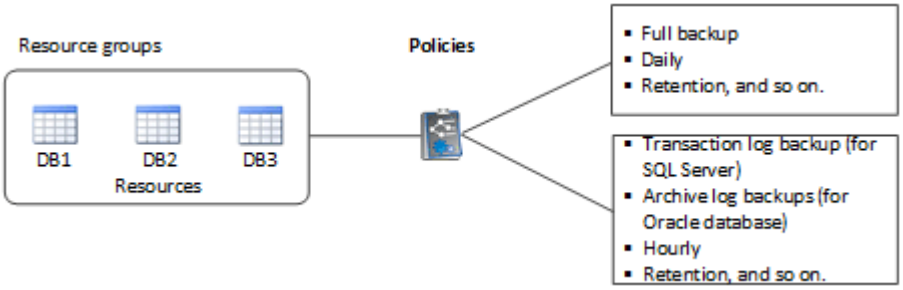
- **Policies** specify the backup frequency, copy retention, replication, scripts, and other characteristics of data protection operations.

  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.

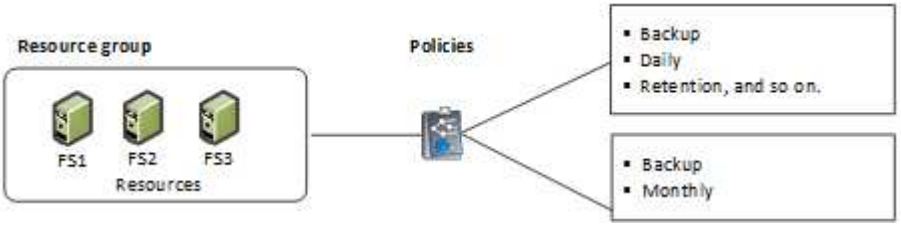
Think of a resource group as defining *what* you want to protect and when you want to protect it in terms of day and time. Think of a policy as defining *how* you want to protect it. If you are backing up all databases or backing up all file systems of a host, for example, you might create a resource 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 files systems:




# Prescripts and postscripts

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

## Supported script types

The following types of scripts are supported for Windows:

- Batch files
- PowerShell scripts
- Perl scripts

The following types of scripts are supported for UNIX:

- Perl scripts
- Python scripts
- Shell scripts

Along with default bash shell other shells like sh-shell, k-shell, and c-shell are also supported.

### Script path

All prescripts and postscripts that are run as part of SnapCenter operations, on nonvirtualized and on virtualized storage systems, are executed on the plug-in host.

- The Windows scripts should be located on the plug-in host.

The prescripts or postscripts path should not include drives or shares. The path should be relative to the SCRIPTS_PATH.

- The UNIX scripts should be located on the plug-in host.

The script path is validated at the time of execution.

### Where to specify scripts

Scripts are specified in backup policies. When a backup job is started, the policy automatically associates the script with the resources being backed up. When you create a backup policy, you can specify the prescript and postscript arguments.

You cannot specify multiple scripts.

### Script timeouts

The timeout is set to 60 seconds, by default. You can modify the timeout value.

### Script output

The default directory for the Windows prescripts and postscripts output files is Windows\System32.

There is no default location for the UNIX prescripts and postscripts. You can redirect the output file to any preferred location.

# SnapCenter Automation using REST APIs

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

| The REST APIs for… | Are located in… |
|---|---|
| SnapCenter Server | https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/ |
| SnapCenter Plug-in for VMware vSphere | https://<OVA_IP_address_or_host_name>:<scv_plugin_port>/api/swagger-ui.html# |

For information on SnapCenter REST APIs, see Overview of REST APIs

For information on SnapCenter Plug-in for VMware vSphere REST APIs, see SnapCenter Plug-in for VMware vSphere REST APIs

## Copyright information



## Trademark information