



Learn about SnapCenter software

SnapCenter software

NetApp
February 20, 2026

Table of Contents

- Learn about SnapCenter software 1
 - SnapCenter overview 1
 - Key features 1
 - SnapCenter architecture and components 2
- Security features in SnapCenter 5
 - CA Certificate Overview 6
 - Two-way SSL communication 6
 - Certificate based authentication Overview 6
 - Multi-factor authentication (MFA) 6
- Role-based access control in SnapCenter 7
 - Types of RBAC in SnapCenter 7
 - Permissions assigned to the pre-defined SnapCenter roles 8
- Disaster recovery in SnapCenter 11
 - SnapCenter Server DR 12
 - SnapCenter Plug-in and Storage DR 12
- Licenses required by SnapCenter 12
- SnapMirror active sync in SnapCenter 15
- Key concepts of data protection 16
 - Resources 16
 - Resource group 16
 - Policies 16
 - Consistency group (CG) 16
 - Usage of prescripts and postscripts 16
- Storage systems and applications supported by SnapCenter 18
 - Supported storage systems 18
 - Supported applications and databases 18
- Authentication methods for SnapCenter credentials 18
 - Windows authentication 18
 - Untrusted domain authentication 18
 - Local workgroup authentication 19
 - SQL Server authentication 19
 - Linux authentication 19
 - AIX authentication 19
 - Oracle database authentication 19
 - Oracle ASM authentication 19
 - RMAN catalog authentication 19

Learn about SnapCenter software

SnapCenter overview

SnapCenter software is a simple, centralized, and scalable platform for application-consistent data protection. It protects applications, databases, host file systems, and VMs on ONTAP systems in the Hybrid Cloud.

SnapCenter uses NetApp Snapshot, SnapRestore, FlexClone, SnapMirror, and SnapVault technologies to provide:

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

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

You can install SnapCenter either on on-premises or on a public cloud to protect data.

- On-premises to protect the following:
 - Data that is on ONTAP FAS, AFF, or 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
 - Data that is on ONTAP ASA r2 primary and secondary systems
- On-premises 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 NetApp 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)

Key features

SnapCenter provides the following key features:

- Centralized, application-consistent data protection of different applications

Data protection is supported for Microsoft Exchange Server, Microsoft SQL Server, Oracle Databases on Linux or AIX, SAP HANA database, IBM Db2, PostgreSQL, MySQL, and Windows Host Filesystems running on ONTAP systems. SnapCenter also supports protection of applications such as MongoDB,

Storage, MaxDB, Sybase ASE, ORASCPM.

- Policy-based backups

Policy-based backups leverage NetApp Snapshot technology to create fast, space-efficient, application-consistent, disk-based backups. You can also set up automatic protection of these backups to secondary storage by updating existing protection relationships.

- Backups for multiple resources

You can back up multiple resources (applications, databases, or host file systems) of the same type at once 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, and application-consistent cloning. You can clone on any destination in the Hybrid Cloud.

- Single user management graphical user interface

SnapCenter provides a single interface to manage backups and clones in any Hybrid Cloud destination.

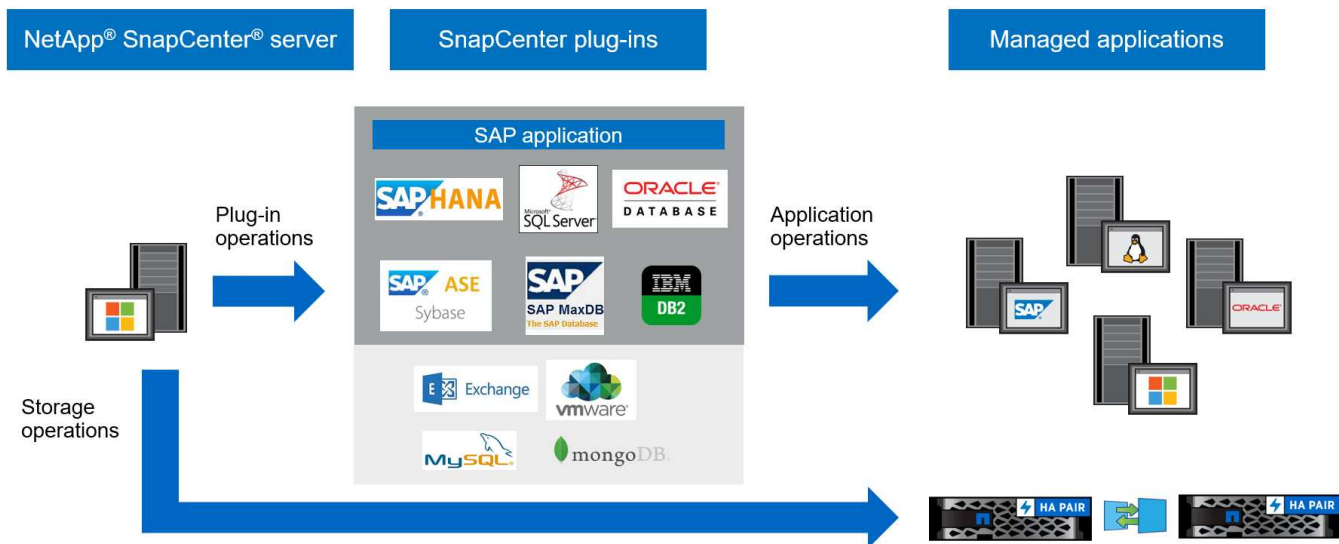
- REST APIs, Windows cmdlets, UNIX commands

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

- Centralized data protection dashboard and reporting
- Role-Based Access Control (RBAC) for security and delegation
- A built-in repository database with high-availability to store all backup metadata
- Automated push install of plug-ins
- High Availability
- Disaster Recovery (DR)
- SnapLock [Learn More](#)
- SnapMirror active sync (initially released as SnapMirror Business Continuity [SM-BC])
- Synchronous mirroring [Learn More](#)

SnapCenter architecture and components

SnapCenter uses a layered design with a central management server and plug-in hosts. The server and plug-in hosts can be in different locations.



SnapCenter includes the SnapCenter Server, the SnapCenter Plug-in package for Windows, and the SnapCenter Plug-In Package for Linux. Each package contains plug-ins for various applications and infrastructure components.

SnapCenter Server

The SnapCenter Server supports Microsoft Windows and Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5) operating systems. SnapCenter server includes a web server, a centralized HTML5-based user interface, PowerShell cmdlets, REST APIs, and the SnapCenter repository.

SnapCenter stores information about its operations in the SnapCenter repository.

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
SnapCenter plug-in for Microsoft SQL Server	Plug-ins package for Windows	Plug-in for Windows	SQL Server host	Windows
SnapCenter plug-in for Windows	Plug-ins package for Windows		Windows host	Windows
SnapCenter plug-in for Microsoft Exchange Server	Plug-ins package for Windows	Plug-in for Windows	Exchange Server host	Windows
SnapCentre 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 name	Included in install package	Requires other plug-ins	Installed on host	Platform supported
SnapCenter 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
SnapCenter plug-in for IBM Db2	Plug-ins package for Linux and plug-ins Package for Windows	Plug-in for UNIX or plug-in for Windows	Db2 host	Linux, AIX, or Windows
SnapCenter plug-in for PostgreSQL	Plug-ins package for Linux and plug-ins package for Windows	Plug-in for UNIX or plug-in for Windows	PostgreSQL host	Linux or Windows
SnaoCenter plug-in for MySQL	Plug-ins package for Linux and plug-ins package for Windows	Plug-in for UNIX or Plug-in for Windows	MySQL host	Linux or Windows
SnapCenter plug-in for MongoDB	Plug-ins package for Linux and plug-ins package for Windows	Plug-in for UNIX or plug-in for Windows	MongoDB host	Linux or Windows
SnapCenter plug-in for ORASCPM (Oracle Applications)	Plug-ins package for Linux and plug-ins package for Windows	Plug-in for UNIX or plug-in for Windows	Oracle host	Linux or Windows
SnapCenter plug-in for SAP ASE	Plug-ins package for Linux and plug-ins package for Windows	Plug-in for UNIX or plug-in for Windows	SAP host	Linux or Windows
SnapCenter plug-in for SAP MaxDB	Plug-ins package for Linux and plug-ins package for Windows	Plug-in for UNIX or plug-in for Windows	SAP MaxDB host	Linux or Windows
SnapCenter plug-in for Storage plug-in	Plug-ins package for Linux and Plug-ins package for Windows	Plug-in for UNIX or plug-in for Windows	Storage 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). It also supports

application-consistent backup and restore operations for virtualized databases and file systems.

To protect databases, filesystems, VMs, or datastores on VMs, deploy the SnapCenter Plug-in for VMware vSphere appliance. For information, refer [SnapCenter Plug-in for VMware vSphere documentation](#).

SnapCenter repository

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

The SnapCenter Server installation installs the MySQL Server repository database by default. If you have already installed MySQL Server and want to perform a fresh installation of SnapCenter Server, you must uninstall MySQL Server.

SnapCenter supports MySQL Server 8.0.37 or later as the SnapCenter repository database. If you use an earlier version of MySQL Server with an earlier release of SnapCenter, the SnapCenter upgrade process upgrades MySQL Server to version 8.0.37 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 in SnapCenter

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.
- Supports security algorithms that are compliant with the Federal Information Processing Standard (FIPS).
- Supports using the authorized CA certificates provided by the customer.
- Supports Transport Layer Security (TLS) 1.3 for communication with ONTAP. You can also use TLS 1.2 for communication between clients and servers.
- Supports a certain set of SSL Cipher suites to provide security across network communication. [Learn more](#).
- 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 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](#).

Role-based access control in SnapCenter

SnapCenter role-based access control (RBAC) and ONTAP permissions allow SnapCenter administrators to assign resource access to users or groups. This centrally managed access empowers application administrators to work securely within designated environments.

You should create or modify roles and add resource access to users. When setting up SnapCenter for the first time, add Active Directory users or groups to roles and assign resources to those users or groups.



SnapCenter does not create user or group accounts. Create user or group accounts in the Active Directory of the operating system or the database.

Types of RBAC in SnapCenter

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

- SnapCenter RBAC
- Application-level RBAC
- SnapCenter plug-in for VMware vSphere RBAC
- ONTAP permissions

SnapCenter RBAC

SnapCenter has predefined roles and you can assign users or groups to these roles.

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

When you assign a role to a user, SnapCenter displays the jobs that are relevant to that user on the Jobs page, unless the user has the SnapCenterAdmin role.

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

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.



When you create a custom role, make sure it includes all permissions of the SnapCenterAdmin role. If you copy only some permissions, SnapCenter prevents you from performing all operations.

Users must authenticate when logging in through the user interface or PowerShell cmdlets. If users have multiple roles, they select a role after logging in. Authentication is also required to run APIs.

Application-level RBAC

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

For example, to perform data protection operations in a SQL Server environment, set the right Windows or SQL credentials. If you want to perform 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 on 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 ONTAP RBAC. [Learn More](#)

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

ONTAP permissions

You should create vsadmin account with the required permissions to access the storage system. [Learn More](#)

Permissions assigned to the pre-defined SnapCenter roles

When you add a user to a role, assign either the StorageConnection permission to enable storage virtual machine (SVM) communication, or assign an SVM to the user to grant permission to use the SVM. The Storage Connection permission allows users to create SVM connections.

For example, a SnapCenter Admin can create SVM connections and assign them to App Backup and Clone Admin users, who cannot create or edit SVM connections. Without an SVM connection, users cannot perform 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

Permissions	Enabled	Create	Read	Update	Delete
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
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
Secondary Protection	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 the 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

Permissions	Enabled	Create	Read	Update	Delete
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
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
Secondary Protection	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
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
Secondary Protection	No	No	Not applicable	Not applicable	Not applicable
Job Monitor	Yes	Not applicable	Not applicable	Not applicable	Not applicable

Disaster recovery in SnapCenter

The SnapCenter disaster recovery (DR) feature lets you recover from disasters like resource corruption or server crashes. It helps to restore the SnapCenter repository,

server schedules, configuration components, and the SnapCenter Plug-in for SQL Server and its storage.

This section explains the two types of 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 log in 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 the 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 the restore operation. You should manually repeat the Audit log settings.


SnapCenter Plug-in and Storage DR


DR is available only for SnapCenter Plug-in for SQL Server. If the plug-in is down, switch to another SQL host and recover the data by following a few steps. See [Disaster recovery of SnapCenter Plug-in for SQL Server](#).

SnapCenter uses ONTAP SnapMirror to replicate data, which can be used for DR by keeping data synchronized at to a secondary site. To initiate failover, break the SnapMirror replication. During fallback, reverse the synchronization to replicate data from the DR site back to the primary location.

Licenses required by SnapCenter

SnapCenter requires several licenses to enable data protection of applications, databases, file systems, and virtual machines. The type of SnapCenter licenses you install depends on your storage environment and the features that you want to use.

License	Where required
SnapCenter Standard controller-based	<p>Required for FAS, AFF, ASA</p> <p>SnapCenter Standard license is a controller-based license and is included as part of NetApp ONTAP One. If you have the SnapManager Suite license, you also get the SnapCenter Standard license entitlement. If you want to install SnapCenter on a trial basis with FAS, AFF, or ASA storage, you can obtain a NetApp ONTAP One evaluation license by contacting the sales representative.</p> <p>For information on licenses included with NetApp ONTAP One, refer to Licenses included with NetApp ONTAP One.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  SnapCenter is also offered as part of data protection bundle. If you have purchased A400 or later, you should purchase the data protection bundle. </div>
SnapMirror or SnapVault	<p>ONTAP</p> <p>Either SnapMirror or SnapVault license is required if replication is enabled in SnapCenter.</p>
SnapRestore	<p>Required to restore and verify backups.</p> <p>On primary storage systems</p> <ul style="list-style-type: none"> • Required on SnapVault destination systems to perform remote verification and to restore from a backup. • Required on SnapMirror destination systems to perform remote verification.
FlexClone	<p>Required to clone databases and verification operations.</p> <p>On primary and secondary storage systems</p> <ul style="list-style-type: none"> • Required on SnapVault destination systems to create clones from secondary vault backup. • Required on SnapMirror destination systems to create clones from secondary SnapMirror backup.

License	Where required
Protocol licenses	<ul style="list-style-type: none"> • iSCSI or FC license for LUNs • CIFS license for SMB shares • NFS license for NFS type VMDKs • iSCSI or FC license for VMFS type VMDKs <p>Required on SnapMirror destination systems to serve data if a source volume is unavailable.</p>
SnapCenter Standard licenses (optional)	<p>Secondary destinations</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-left: 20px;"> <p> It is recommended, but not required, that you add SnapCenter Standard licenses to secondary destinations. If SnapCenter Standard licenses are not enabled on secondary destinations, you cannot use SnapCenter to backup resources on the secondary destination after performing a failover operation. However, a FlexClone license is required on secondary destinations to perform clone and verification operations.</p> </div>
Single Mailbox Recovery (SMBR) licenses	<p>If you are using SnapCenter Plug-in for Exchange to manage Microsoft Exchange Server databases and Single Mailbox Recovery (SMBR), you would need additional license for SMBR which needs to be purchased separately based on user mailbox.</p> <p>NetApp® Single Mailbox Recovery has come to the end of availability (EOA) on May 12, 2023. For more information, refer CPC-00507. NetApp will continue to support customers that have purchased mailbox capacity, maintenance, and support through marketing part numbers introduced on June 24, 2020, for the duration of the support entitlement.</p> <p>NetApp Single Mailbox Recovery is a partner product provided by Ontrack. Ontrack PowerControls offers capabilities that are similar to those of NetApp Single Mailbox Recovery. Customers can procure new Ontrack PowerControls software licenses and Ontrack PowerControls maintenance and support renewals from Ontrack (through licensingteam@ontrack.com) for granular mailbox recovery after the May 12, 2023, EOA date.</p>



SnapCenter Advanced and SnapCenter NAS File Services licenses are deprecated, and are no longer available. The standard license and capacity-based license are no longer required for Amazon FSx for NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP, and Azure NetApp Files.

You should install one or more SnapCenter licenses. For information on how to add licenses, see [Add SnapCenter Standard controller-based licenses](#).

SnapMirror active sync in SnapCenter

SnapMirror active sync 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 SnapMirror active sync.

For more information on SnapMirror active sync refer [SnapMirror active sync overview](#).

For SnapMirror active sync, ensure that you have met the various hardware, software, and system configuration requirements. For information refer [Prerequisites](#)

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

After installing the SnapCenter Server and plug-ins, you should enable the REST API for SnapCenter to detect SnapMirror active sync relationships.

- On the SnapCenter server host, edit the `C:\Program Files\NetApp\SMCore\SMCoreServiceHost.dll.config` file to modify the value of the `IsRestEnabledForStorageConnection` parameter to `true` and then restart the SnapCenter SMCORE service.
- On the Windows plug-in hosts:
 - Edit the `C:\Program Files\NetApp\SnapCenter\SMCore\SMCoreServiceHost.dll.config` file to modify the value of the `IsRestEnabledForStorageConnection` parameter to `true`.
 - Edit the `C:\Program Files\NetApp\SnapCenter\SMCore\SnapDriveService.dll.config` file to modify the value of the `IsRestEnabledForStorageConnection` parameter to `true`.
 - Restart the SnapCenter SMCORE service.



To support host initiator proximity in SnapCenter, it's value, either source or destination should be set in ONTAP.

The use cases not supported in SnapCenter:

- If you convert the existing asymmetric SnapMirror active sync workloads to symmetric by changing the policy on the SnapMirror active sync relationships from `automatedfailover` to `automatedfailoverduplex` in ONTAP, the same is not supported in SnapCenter.
- If there are backups of a resource group (already protected in SnapCenter) and then storage policy is changed on the SnapMirror active sync relationships from `automatedfailover` to `automatedfailoverduplex` in ONTAP, the same is not supported in SnapCenter.

Key concepts of data protection

Before using SnapCenter, understand key concepts for backup, clone, and restore.

Resources

Resources include databases, Windows file systems, or file shares backed up or cloned with SnapCenter. Depending on your environment, resources might also be database instances, SQL Server availability groups, Oracle databases, RAC databases, or custom application groups.

Resource group

A resource group is a collection of resources on a host or cluster, potentially from multiple hosts and clusters. Operations performed on a resource group apply to all its resources based on the specified schedule. You can perform on-demand or scheduled backups for individual resources or groups.



If one host in a shared resource group enters maintenance mode, all scheduled operations for that group will be suspended across all hosts.

Use relevant plug-ins to back up specific resources: database plug-ins for databases, file system plug-ins for file systems, and SnapCenter Plug-in for VMware vSphere for VMs and datastores.

Policies

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

One or more policies can be selected when creating a resource group or when performing an on-demand backup.

A resource group defines what needs to be protected and when it should be protected in terms of day and time. A policy describes how the protection will be carried out. For example, if backing up all databases or file systems of a host is necessary, a resource group including all databases or file systems in the host might be created. Two policies could then be attached to the resource group: a daily policy and an hourly policy.

When creating the resource group and attaching the policies, it is possible to configure it to perform a full backup daily and another schedule for log backups hourly.

Custom prescripts and postscripts can be used in data protection operations. These scripts allow automation either before or after the data protection job. For instance, a script could automatically notify of data protection job failures or warnings. Understanding the requirements for creating these scripts is crucial before setting up prescripts and postscripts.

Consistency group (CG)

A consistency group is a collection of volumes managed as a single unit. CGs are synchronized for data consistency across storage units and volumes. In ONTAP, they provide easy management and a protection guarantee for an application workload spanning multiple volumes. Learn more about [consistency groups](#).

Usage of prescripts and postscripts

Custom prescripts and postscripts can automate your data protection tasks before or after the job. For

instance, you can add a script to notify you of job failures or warnings. Before setting them up, ensure you understand the requirements for 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 both nonvirtualized and 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 starts, 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.

Storage systems and applications supported by SnapCenter

You should know the storage systems, applications, and databases supported by SnapCenter.

Supported storage systems

- NetApp ONTAP 9.12.1 and later
- Azure NetApp Files
- Amazon FSx for NetApp ONTAP

Amazon FSx for NetApp ONTAP supports non-volatile memory express (NVMe) over Transport Control Protocol (TCP).

For information about Amazon FSx for NetApp ONTAP, see [Amazon FSx for NetApp ONTAP documentation](#).

- NetApp ASA r2 systems that are running NetApp ONTAP 9.16.1 and later

You should use ONTAP 9.17.1, if you are using SnapCenter Server 6.2 and SnapCenter plug-ins 6.2.

Supported applications and databases

SnapCenter supports protection of different applications and databases.

SnapCenter supports protection of Oracle and Microsoft SQL workloads in VMware Cloud on Amazon Web Services (AWS) Software-Defined Data Center (SDDC) environments. [Learn More](#).

Authentication methods for SnapCenter credentials

Credentials use different authentication methods depending on the application or environment. Credentials authenticate users so they can perform SnapCenter operations. You should create one set of credentials for installing plug-ins and another 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 credential to add hosts, install plug-in packages, and schedule jobs.

Untrusted domain authentication

SnapCenter allows users and groups belonging to untrusted domains to create Windows credentials. For the authentication to succeed, you should register the untrusted domains with SnapCenter.

Local workgroup authentication

SnapCenter allows the creation of Windows credentials with local workgroup users and groups. The Windows authentication for local workgroup users and groups does not happen during Windows credential creation but is deferred until the host registration and other host operations are performed.

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 credential, you must add a host, install plug-in packages, and refresh resources. You need SQL Server authentication to perform operations such as scheduling on SQL Server 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.

AIX authentication

The AIX authentication method authenticates against an AIX host. You need AIX authentication during the initial step of adding the AIX host and installing the SnapCenter Plug-ins Package for AIX 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 an Oracle database credential, you should 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. Oracle ASM authentication is required if you need to access an Oracle ASM instance and OS authentication is disabled on the database host. Before adding an Oracle ASM credential, create an Oracle user with system privileges 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.

Copyright information

Copyright © 2026 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.