Protect Windows file systems

SnapCenter software

NetApp
February 20, 2026

Table of Contents

Protect Windows file systems

SnapCenter Plug-in for Microsoft Windows concepts

SnapCenter Plug-in for Microsoft Windows overview

The SnapCenter Plug-in for Microsoft Windows is a host-side component of the NetApp SnapCenter Software that enables application-aware data protection management of Microsoft file system resources. In addition, it provides storage provisioning, Snapshot consistency, and space reclamation for Windows file systems. The Plug-in for Windows automates file system backup, restore, and cloning operations in your SnapCenter environment.

When the Plug-in for Windows is installed, you can use SnapCenter with NetApp SnapMirror technology to create mirror copies of backup sets on another volume and with NetApp SnapVault technology to perform disk-to-disk backup replication for archival or standards compliance.

- 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.

What you can do with the SnapCenter Plug-in for Microsoft Windows

When the Plug-in for Windows is installed in your environment, you can use SnapCenter to back up, restore, and clone Windows file systems. You can also perform tasks supporting those operations.

- Discover resources
- Back up Windows file systems
- Schedule backup operations
- Restore file system backups
- Clone file system backups
- Monitor backup, restore, and clone operations

The Plug-in for Windows does not support backup and restore of file systems on SMB shares.

SnapCenter Plug-in for Windows features

The Plug-in for Windows integrates with NetApp Snapshot technology on the storage system. To work with the Plug-in for Windows, you use the SnapCenter interface.

The Plug-in for Windows includes these major features:

- **Unified graphical user interface powered by SnapCenter**

  The SnapCenter interface provides you with standardization and consistency across plug-ins and environments. The SnapCenter interface enables you to complete consistent backup and restore processes across plug-ins, use centralized reporting, use at-a-glance dashboard views, set up role-based access control (RBAC), and monitor jobs across all plug-ins. SnapCenter also offers centralized scheduling and policy management to support backup and clone operations.

- **Automated central administration**

  You can schedule routine file system backups, configure policy-based backup retention, and set up restore operations. You can also proactively monitor your file system environment by configuring SnapCenter to send email alerts.

- **Nondisruptive NetApp Snapshot technology**

  The Plug-in for Windows uses NetApp Snapshot technology. This enables you to back up file systems in seconds and restore them quickly without taking host offline. Snapshots consume minimal storage space.

In addition to these major features, the Plug-in for Windows offers the following benefits:

- Backup, restore, and clone workflow support
- RBAC-supported security and centralized role delegation
- Creation of space-efficient copies of production file systems for testing or data extraction by using NetApp FlexClone technology

  For FlexClone licensing information, see SnapCenter licenses.

- Ability to run multiple backups at the same time across multiple servers
- PowerShell cmdlets for scripting of backup, restore, and clone operations
- Support for backup of file systems and virtual machine disks (VMDKs)
- Support for physical and virtualized infrastructures
- Support for iSCSI, Fibre Channel, FCoE, raw device mapping (RDM), Asymmetric LUN Mapping (ALM), VMDK over NFS and VMFS, and virtual FC
- Support for non-volatile memory express (NVMe) on Windows Server 2022
  - Backup, restore, clone, and verification workflows on VMDK layout created on NVMe over TCP/IP.
  - Supports NVMe firmware version 1.3 starting from ESX 8.0 update 2 and requires Virtual hardware version 21.
  - Windows Server Failover Clustering (WSFC) is not supported for applications over VMDK on NVMe over TCP/IP.
  - NVMe controllers are only supported with NVMe datastores.
- Supports SnapMirror active sync (initially released as SnapMirror Business Continuity [SM-BC]) that 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.

How SnapCenter backs up Windows file systems

SnapCenter uses Snapshot technology to back up Windows file system resources that reside on LUNs, CSVs (cluster shared volumes), RDM (raw device mapping) volumes, ALM (asymmetric LUN mapping) in Windows clusters, and VMDKs based on VMFS/NFS (VMware Virtual Machine File System using NFS).

SnapCenter creates backups by creating Snapshots of the file systems. Federated backups, in which a volume contains LUNs from multiple hosts, are faster and more efficient than backups of each individual LUN because only one Snapshot of the volume is created compared to individual Snapshots of each file system.

When SnapCenter creates a Snapshot, the entire storage system volume is captured in the Snapshot. However, the backup is valid only for the host server for which the backup was created.

If data from other host servers resides on the same volume, this data cannot be restored from the Snapshot.

If a Windows file system contains a database, then backing up the file system is not the same as backing up the database. To back up a database, you must use one of the database plug-ins.

Storage types supported by SnapCenter Plug-in for Microsoft Windows

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

Machine	Storage type	Provision using	Support notes
Physical server	FC-connected LUNs	SnapCenter graphical user interface (GUI) or PowerShell cmdlets	
Physical server	iSCSI-connected LUNs	SnapCenter GUI or PowerShell cmdlets	
Physical server	SMB3 (CIFS) shares residing on a storage virtual machine (SVM)	SnapCenter GUI or PowerShell cmdlets	Support for provisioning only.
VMware VM	RDM LUNs connected by an FC or iSCSI HBA	PowerShell cmdlets	
VMware VM	iSCSI LUNs connected directly to the guest system by the iSCSI initiator	SnapCenter GUI or PowerShell cmdlets	

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

Machine	Storage type	Provision using	Support notes
Hyper-V VM	A guest system connected to SMB3 shares residing on an SVM	SnapCenter GUI or PowerShell cmdlets	Support for provisioning only. Hyper-V pass through disks and backing up databases on VHD(x) that are provisioned on NetApp storage are not supported.

Minimum ONTAP privileges required for Windows plug-in

The minimum ONTAP privileges that are required vary according to the SnapCenter plug-ins you are using for data protection.

- All-access commands: Minimum privileges required for ONTAP 9.12.1 and later
  - event generate-autosupport-log
  - job history show
  - job stop
  - lun
  - lun create
  - lun delete
  - lun igroup add
  - lun igroup create
  - lun igroup delete
  - lun igroup rename
  - lun igroup show
  - lun mapping add-reporting-nodes
  - lun mapping create
  - lun mapping delete
  - lun mapping remove-reporting-nodes
  - lun mapping show
  - lun modify
  - lun move-in-volume

- lun offline
- lun online
- lun resize
- lun serial
- lun show
- snapmirror policy add-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- snapmirror restore
- snapmirror show
- snapmirror show-history
- snapmirror update
- snapmirror update-ls-set
- snapmirror list-destinations
- version
- volume clone create
- volume clone show
- volume clone split start
- volume clone split stop
- volume create
- volume destroy
- volume file clone create
- volume file show-disk-usage
- volume offline
- volume online
- volume modify
- volume qtree create
- volume qtree delete
- volume qtree modify
- volume qtree show
- volume restrict
- volume show
- volume snapshot create
- volume snapshot delete
- volume snapshot modify
- volume snapshot rename

    - volume snapshot restore
    - volume snapshot restore-file
    - volume snapshot show
    - volume unmount
    - vserver cifs
    - vserver cifs share create
    - vserver cifs share delete
    - vserver cifs shadowcopy show
    - vserver cifs share show
    - vserver cifs show
    - vserver export-policy
    - vserver export-policy create
    - vserver export-policy delete
    - vserver export-policy rule create
    - vserver export-policy rule show
    - vserver export-policy show
    - vserver iscsi
    - vserver iscsi connection show
    - vserver show
- Read-only commands: Minimum privileges required for ONTAP 8.3.0 and later
    - network interface
    - network interface show
    - vserver

Prepare 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.

SnapCenter performs the updates to SnapMirror and SnapVault after it completes the Snapshot operation. SnapMirror and SnapVault updates are performed as part of the SnapCenter job. If you are using SnapMirror active sync, then go with default SnapMirror or SnapVault schedules for both SnapMirror active sync and asynchronous relationships.

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.

SnapCenter does not support cascade relationships between SnapMirror and SnapVault volumes (**Primary** > **Mirror** > **Vault**). You should use fanout relationships.

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.

Define a backup strategy for Windows file systems

Defining a backup strategy before you create your backups provides you with the backups that you require to successfully restore or clone your file systems. Your service-level agreement (SLA), recovery time objective (RTO), and recovery point objective (RPO) largely determine your backup strategy.

An SLA defines the level of service that is expected and addresses many service-related issues, including the availability and performance of the service. RTO is the time by which a business process must be restored after a disruption in service. RPO defines the strategy for the age of the files that must be recovered from backup storage for regular operations to resume after a failure. SLA, RTO, and RPO contribute to the data protection strategy.

Backup schedules for Windows file systems

Backup frequency is specified in policies; a backup schedule is specified in the resource group configuration. The most critical factor in determining a backup frequency or schedule is the rate of change for the resource and the importance of the data. You might back up a heavily used resource every hour, while you might back up a rarely used resource once a day. Other factors include the importance of the resource to your organization, your Service Level Agreement (SLA), and your Recover Point Objective (RPO).

An SLA defines the level of service expected and addresses many service-related issues, including the availability and performance of service. An RPO defines the strategy for the age of the files that must be recovered from backup storage for regular operations to resume after a failure. The SLA and RPO contribute to the data protection strategy.

Even for a heavily used resource, there is no requirement to run a full backup more than once or twice a day.

Backup schedules have two parts, as follows:

- Backup frequency

  Backup frequency (how often backups are to be performed), called *schedule type* for some plug-ins, is part of a policy configuration. For example, you might configure the backup frequency as hourly, daily, weekly, or monthly, or you can specify **None** which makes the policy an on-demand-only policy. You can access policies by clicking **Settings** > **Policies**.

- Backup schedules

  Backup schedules (exactly when backups are to be performed) are part of a resource group configuration. For example, if you have a resource group that has a policy configured for weekly backups, you might configure the schedule to back up every Thursday at 10:00 PM. You can access resource group schedules by clicking **Resources** > **Resource Groups**.

Number of backups needed for Windows file systems

Factors that determine the number of backups that you need include the size of the Windows file system, the number of volumes used, the rate of change of the file system, and your Service Level Agreement (SLA).

Backup naming convention for Windows file systems

Windows file system backups use the default Snapshot naming convention. The default backup naming convention adds a timestamp to Snapshot names that helps you identify when the copies were created.

The Snapshot uses the following default naming convention: resourcegroupname_hostname_timestamp

You should name your backup resource groups logically, as in the following example:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In this example, the syntax elements have the following meanings:

- `dts1` is the resource group name.
- `mach1x88` is the host name.
- `03-12-2016_23.17.26` is the date and timestamp.

When creating a backup, you can also add a descriptive tag to help identify the backup. In contrast, if you want to use a customized backup naming convention, you need to rename the backup after the backup operation is complete.

Backup retention options

You can choose either the number of days for which to retain backup copies or specify the number of backup copies you want to retain, up to a ONTAP maximum of 255 copies. For example, your organization might require that you retain 10 days of backup copies or 130 backup copies.

While creating a policy, you can specify the retention options for the backup type and the schedule type.

If you set up SnapMirror replication, the retention policy is mirrored on the destination volume.

SnapCenter deletes the retained backups that have retention labels that match the schedule type. If the schedule type was changed for the resource or resource group, backups with the old schedule type label might still remain on the system.

For long-term retention of backup copies, you should use SnapVault backup.

Sources and destinations of clones for Windows file systems

You can clone a file system backup from primary storage or secondary storage. You also can choose the destination that supports your requirements; either the original backup location or a different destination on the same host or on a different host. The destination must be on the same volume as the clone source backup.

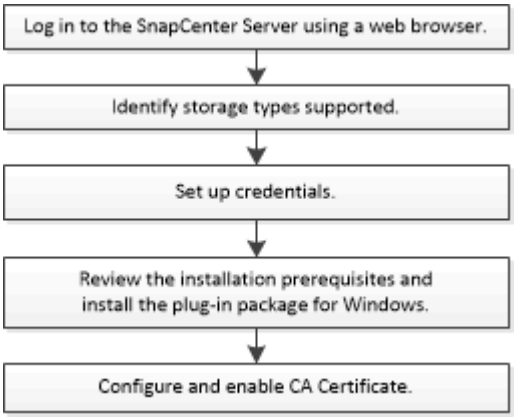
Clone destination	Description
Original, source, location	By default, SnapCenter stores the clone on the same location and the same host as the backup being cloned.
Different location	You can store the clone on a different location on the same host or on a different host. The host must have a configured connection to the storage virtual machine (SVM).

You can rename the clone after the clone operation is complete.

Install SnapCenter Plug-in for Microsoft Windows

Installation workflow of SnapCenter Plug-in for Microsoft Windows

You must install and set up SnapCenter Plug-in for Microsoft Windows if you want to protect Windows files that are not database files.



Installation requirements for SnapCenter Plug-in for Microsoft Windows

You should be aware of certain installation requirements before you install the Plug-in for Windows.

Before you begin to use the Plug-in for Windows, the SnapCenter administrator must install and configure SnapCenter Server and perform prerequisite tasks.

- You must have SnapCenter admin privileges to install the Plug-in for Windows.

  The SnapCenter admin role must have admin privileges.

- You must have installed and configured the SnapCenter Server.
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in or if the user belongs to a local workgroup user, you must disable UAC on the host.
- You must set up SnapMirror and SnapVault if you want backup replication.

Host requirements to install SnapCenter Plug-ins Package for Windows

Before you install the SnapCenter Plug-ins Package for Windows, you should be familiar with some basic host system space requirements and sizing requirements.

Item	Requirements
Operating Systems	Microsoft Windows For the latest information about supported versions, see the NetApp Interoperability Matrix Tool. If you are on a Windows cluster setup, you should also install and configure the Windows Remote Management (WinRM).
Minimum RAM for the SnapCenter plug-in on host	1 GB
Minimum install and log space for the SnapCenter plug-in on host	5 GB You should allocate sufficient disk space and monitor the storage consumption by the logs folder. The log space required varies depending on the number of the entities to be protected and the frequency of data protection operations. If there is no sufficient disk space, the logs will not be created for the recently run operations.
Required software packages	• ASP.NET Core Runtime 8.0.12 (and all subsequent 8.0.x patches) Hosting Bundle • PowerShell Core 7.4.2 For .NET specific troubleshooting information, see SnapCenter upgrade or install fails for legacy systems that do not have internet connectivity.

Set up your credentials for the Plug-in for Windows

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

What you will need

- You must set up Windows credentials before installing plug-ins.
- You must set up the credentials with administrator privileges, including administrator rights, on the remote host.
- If you set up credentials for individual resource groups, and the user does not have full admin privileges,

you must assign at least the resource group and backup privileges to the user.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Credential**.
3. Click **New**.
4. In the Credential page, do the following:

For this field…	Do this…
Credential name	Enter a name for the credentials.
User name/Password	Enter the user name and password used for authentication. • Domain administrator or any member of the administrator group Specify the domain administrator or any member of the administrator group on the system on which you are installing the SnapCenter plug-in. Valid formats for the Username field are as follows: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` ◦ `UserName@upn` • Local administrator (for workgroups only) For systems that belong to a workgroup, specify the built-in local administrator on the system on which you are installing the SnapCenter plug-in. You can specify a local user account that belongs to the local administrators group if the user account has elevated privileges or the User Access control feature is disabled on the host system. The valid format for the Username field is as follows: `UserName` Do not use double quotes (") or backtick (`) in the passwords. You should not use the less than (<) and exclamation (!) symbols together in passwords. For example, lessthan<!10, lessthan10<!, backtick`12.
Password	Enter the password used for authentication.

5. Click **OK**.

After you finish setting up credentials, you might want to assign credential maintenance to a user or group of users on the User and Access page.

Configure gMSA on Windows Server 2016 or later

Windows Server 2016 or later enables you to create a group Managed Service Account (gMSA) that provides automated service account password management from a managed domain account.

Before you begin

- You should have a Windows Server 2016 or later domain controller.
- You should have a Windows Server 2016 or later host, which is a member of the domain.

Steps

1. Create a KDS root key to generate unique passwords for each object in your gMSA.
2. For each domain, run the following command from the Windows domain controller: Add-KDSRootKey -EffectiveImmediately
3. Create and configure your gMSA:
   a. Create a user group account in the following format:

      ```
      domainName\accountName$
      ```

   b. Add computer objects to the group.
   c. Use the user group you just created to create the gMSA.

      For example,

      ```
      New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
      -PrincipalsAllowedToRetrieveManagedPassword <group>
      -ServicePrincipalNames <SPN1,SPN2,…>
      ```

   d. Run `Get-ADServiceAccount` command to verify the service account.
4. Configure the gMSA on your hosts:
   a. Enable the Active Directory module for Windows PowerShell on the host where you want to use the gMSA account.

      To do this, run the following command from PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install
State
------------                            ----
-------------
[ ] Active Directory Domain Services   AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain
Services, Active ...
WARNING: Windows automatic updating is not enabled. To ensure that
your newly-installed role or feature is
automatically updated, turn on Windows Update.
```

b. Restart your host.

c. Install the gMSA on your host by running the following command from the PowerShell command prompt: `Install-AdServiceAccount <gMSA>`

d. Verify your gMSA account by running the following command: `Test-AdServiceAccount <gMSA>`

5. Assign the administrative privileges to the configured gMSA on the host.
6. Add the Windows host by specifying the configured gMSA account in the SnapCenter Server.

   SnapCenter Server will install the selected plug-ins on the host and the specified gMSA will be used as the service log on account during the plug-in installation.

Add hosts and install SnapCenter Plug-in for Microsoft Windows

You can use the SnapCenter Add Host page to add Windows hosts. The SnapCenter Plug-in for Microsoft Windows is automatically installed on the specified host. This is the recommended method for installing plug-ins. You can add a host and install a plug-in either for an individual host or a cluster.

Before you begin

- If the operating system of the SnapCenter Server host is Windows 2019 and the operating system of the plug-in host is Windows 2022, you should perform the following:
  - Upgrade to Windows Server 2019 (OS Build 17763.5936) or later
  - Upgrade to Windows Server 2022 (OS Build 20348.2402) or later
- 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 role.
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in or if the user

belongs to a local workgroup user, you must disable UAC on the host.

- The SnapCenter user should be added to the “Log on as a service” role of the Windows Server.
- You should ensure that the message queueing service is in running state.
- If you are using group Managed Service Account (gMSA), you should configure gMSA with administrative privileges.

  Configure group Managed Service Account on Windows Server 2016 or later for Windows File System

About this task

- You cannot add a SnapCenter Server as a plug-in host to another SnapCenter Server.
- Windows plug-ins
  - Microsoft Windows
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - SAP HANA
- Installing plug-ins on a cluster

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

- E-series storage

  You cannot install the Plug-in for Windows on a Windows host connected to E-series storage.

SnapCenter does not support adding of the same host (plug-in host) to SnapCenter if the host is already part of a workgroup and changed to another domain or vice versa. If you want to add the same host, you should remove the host from SnapCenter and add it again.

Steps

1. In the left navigation pane, click **Hosts**.
2. Ensure that **Managed Hosts** is selected at the top.
3. Click **Add**.
4. In the Hosts page, do the following:

For this field…	Do this…
Host Type	Select the **Windows** type of host. SnapCenter Server adds the host and then installs the Plug-in for Windows if it is not already installed on the host.

For this field…	Do this…
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 the IP addresses or FQDN of one of the following: • Stand-alone host • Windows Server Failover Clustering (WSFC) If you are adding a host using SnapCenter and it is part of a subdomain, you must provide the FQDN.
Credentials	Select the credential name that you created or create the new credentials. The credential must have administrative rights on the remote host. For details, see information about creating a credential. Details about credentials, including the user name, domain, and host type, are displayed by placing your cursor over the credential name you provided. The authentication mode is determined by the host type that you specify in the Add Host wizard.

5. In the Select Plug-ins to Install section, select the plug-ins to install.

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

6. (Optional) Click **More Options**.

For this field…	Do this…
Port	Either retain the default port number or specify the port number. The default port number is 8145. If the SnapCenter Server was installed on a custom port, that port number will be displayed as the default port. If you manually installed the plug-ins and specified a custom port, you must specify the same port. Otherwise, the operation fails.
Installation Path	The default path is C:\Program Files\NetApp\SnapCenter. You can optionally customize the path. 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.
Add all hosts in the cluster	Select this check box to add all of the cluster nodes in a WSFC.
Skip preinstall checks	Select this check box if you already installed the plug-ins manually and you do not want to validate whether the host meets the requirements for installing the plug-in.
Use group Managed Service Account (gMSA) to run the plug-in services	Select this check box if you want to use group Managed Service Account (gMSA) to run the plug-in services. Provide the gMSA name in the following format: *domainName\accountName$*. gMSA will be used as a log on service account only for SnapCenter Plug-in for Windows service.

7. Click **Submit**.

   If you have not selected the **Skip prechecks** checkbox, the host is validated to see whether it meets the requirements to install the plug-in. The disk space, RAM, PowerShell version, .NET version, and location are validated against the minimum requirements. If the minimum requirements are not met, appropriate error or warning messages are displayed.

   If the error is related to disk space or RAM, you can update the web.config file located at `C:\Program Files\NetApp\SnapCenter` WebApp to modify the default values. If the error is related to other

parameters, you must fix the issue.

> In an HA setup, if you are updating web.config file, you must update the file on both nodes.

8. Monitor the installation progress.

Install SnapCenter Plug-in for Microsoft Windows on multiple remote hosts using PowerShell cmdlets

If you want to install SnapCenter Plug-in for Microsoft Windows on multiple hosts at one time, you can do so by using the `Install-SmHostPackage` PowerShell cmdlet.

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. On the SnapCenter Server host, establish a session using the `Open-SmConnection` cmdlet, and then enter your credentials.
3. Add the standalone host or the cluster to SnapCenter using the `Add-SmHost` cmdlet and the required parameters.

   The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

4. Install the plug-in on multiple hosts using the `Install-SmHostPackage` cmdlet and the required parameters.

   You can use the `-skipprecheck` option when you have installed the plug-ins manually and do not want to validate whether the host meets the requirements to install the plug-in.

Install 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 the SnapCenter GUI. You can run the SnapCenter Plug-in for Microsoft Windows installation program unattended, in silent mode, from the Windows command line.

Before you begin

- You must have installed ASP.NET Core Runtime 8.0.12 (and all subsequent 8.0.x patches) Hosting Bundle.
- You must have installed PowerShell 7.4.2 or later.
- You must be a local administrator on the host.

Steps

1. Download the SnapCenter Plug-in for Microsoft Windows from your install location.

   For example, the default installation path is C:\ProgramData\NetApp\SnapCenter\Package 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_windows_host_plugin.exe"/silent / debuglog"" /log""
BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
ISFeatureInstall=SCW
```

For example:

```
`"C:\ProgramData\NetApp\SnapCenter\Package Repository
\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
\HPPW_SCW_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW`
```

All the parameters passed during the installation of Plug-in for Windows are case sensitive.

Enter the values for the following variables:

Variable	Value
/debuglog"<Debug_Log_Path>	Specify the name and location of the suite installer log file, as in the following example: Setup.exe /debuglog"C:\PathToLog\setupexe.log".
BI_SNAPCENTER_PORT	Specify the port on which SnapCenter communicates with SMCore.
SUITE_INSTALLDIR	Specify host plug-in package installation directory.
BI_SERVICEACCOUNT	Specify SnapCenter Plug-in for Microsoft Windows web service account.
BI_SERVICEPWD	Specify the password for SnapCenter Plug-in for Microsoft Windows web service account.
ISFeatureInstall	Specify the solution to be deployed by SnapCenter on remote host.

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*\.

The installation of Plug-in for Windows registers the plug-in on the host and not on the SnapCenter Server. You can register the plug-in on the SnapCenter Server by adding the host using the SnapCenter GUI or PowerShell cmdlet. After the host is added, the plug-in is automatically discovered.

Monitor SnapCenter plug-in package installation status

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

About this task

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

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

Steps

1. In the left navigation pane, click **Monitor**.
2. In the **Monitor** page, click **Jobs**.
3. In the **Jobs** page, to filter the list so that only plug-in installation operations are listed, do the following:
   a. Click **Filter**.
   b. 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**.

Configure CA certificate

Generate CA Certificate CSR file

You can generate a Certificate Signing Request (CSR) and import the certificate that can be obtained from a Certificate Authority (CA) using the generated CSR. The certificate will have a private key associated with it.

CSR is a block of encoded text that is given to an authorized certificate vendor to procure the signed CA

certificate.

CA Certificate RSA key length must be minimum 3072 bits.

For information to generate a CSR, see How to generate CA Certificate CSR file.

If you own the CA certificate for your domain (*.domain.company.com) or your system (machine1.domain.company.com), you can skip generating the CA Certificate CSR file. You can deploy the existing CA certificate with SnapCenter.

For cluster configurations, the cluster name (virtual cluster FQDN), and the respective host names should be mentioned in the CA certificate. The certificate can be updated by filling the Subject Alternative Name (SAN) field before procuring the certificate. For a wild card certificate (*.domain.company.com), the certificate will contain all the hostnames of the domain implicitly.

Import CA certificates

You must import the CA certificates to the SnapCenter Server and the Windows host plug-ins using the Microsoft management console (MMC).

Steps

1. Go to the Microsoft management console (MMC), and then click **File** > **Add/Remove Snapin**.
2. In the Add or Remove Snap-ins window, select **Certificates** and then click **Add**.
3. In the Certificates snap-in window, select the **Computer account** option, and then click **Finish**.
4. Click **Console Root** > **Certificates – Local Computer** > **Trusted Root Certification Authorities** > **Certificates**.
5. Right-click on the folder “Trusted Root Certification Authorities”, and then select **All Tasks** > **Import** to start the import wizard.
6. Complete the wizard, as follows:

In this wizard window…	Do the following…
Import Private Key	Select the option **Yes**, import the private key, and then click **Next**.
Import File Format	Make no changes; click **Next**.
Security	Specify the new password to be used for the exported certificate, and then click **Next**.
Completing the Certificate Import Wizard	Review the summary, and then click **Finish** to start the import.

Importing certificate should be bundled with the private key (supported formats are: *.pfx, *.p12, and *.p7b).

7. Repeat Step 5 for the “Personal” folder.

Get the CA certificate thumbprint

A certificate thumbprint is a hexadecimal string that identifies a certificate. A thumbprint is calculated from the content of the certificate using a thumbprint algorithm.

Steps

1. Perform the following on the GUI:
   a. Double-click the certificate.
   b. In the Certificate dialog box, click the **Details** tab.
   c. Scroll through the list of fields and click **Thumbprint**.
   d. Copy the hexadecimal characters from the box.
   e. Remove the spaces between the hexadecimal numbers.

      For example, if the thumbprint is: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", after removing the spaces, it will be: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Perform the following from PowerShell:
   a. Run the following command to list the thumbprint of the installed certificate and identify the recently installed certificate by the subject name.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copy the thumbprint.

Configure CA certificate with Windows host plug-in services

You should configure the CA certificate with Windows host plug-in services to activate the installed digital certificate.

Perform the following steps on the SnapCenter Server and all the plug-in hosts where CA certificates are already deployed.

Steps

1. Remove the existing certificate binding with SMCore default port 8145, by running the following command:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   For example:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:8145
   ```

2. Bind the newly installed certificate with the Windows host plug-in services, by running the following commands:

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

For example:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Enable CA Certificates for plug-ins

You should configure the CA certificates and deploy the CA certificates in the SnapCenter Server and the corresponding plug-in hosts. You should enable the CA certificate validation for the plug-ins.

Before you begin

- You can enable or disable the CA certificates using the run *Set-SmCertificateSettings* cmdlet.
- You can display the certificate status for the plug-ins using the *Get-SmCertificateSettings*.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Managed Hosts**.
3. Select single or multiple plug-in hosts.
4. Click **More options**.
5. Select **Enable Certificate Validation**.

After you finish

The Managed Hosts tab host displays a padlock and the color of the padlock indicates the status of the connection between SnapCenter Server and the plug-in host.

- indicates that the CA certificate is neither enabled nor assigned to the plug-in host.
- indicates that the CA certificate is successfully validated.
- indicates that the CA certificate could not be validated.
- indicates that the connection information could not be retrieved.

When the status is yellow or green, the data protection operations completes successfully.

Install SnapCenter Plug-in for VMware vSphere

If your database or filesystem is stored on virtual machines (VMs), or if you want to protect VMs and datastores, you must deploy the SnapCenter Plug-in for VMware vSphere virtual appliance.

For information to deploy, see Deployment Overview.

Deploy CA certificate

To configure the CA Certificate with SnapCenter Plug-in for VMware vSphere, see Create or import SSL certificate.

Configure the CRL file

SnapCenter Plug-in for VMware vSphere looks for the CRL files in a pre-configured directory. Default directory of the CRL files for SnapCenter Plug-in for VMware vSphere is */opt/netapp/config/crl*.

You can place more than one CRL file in this directory. The incoming certificates will be verified against each CRL.

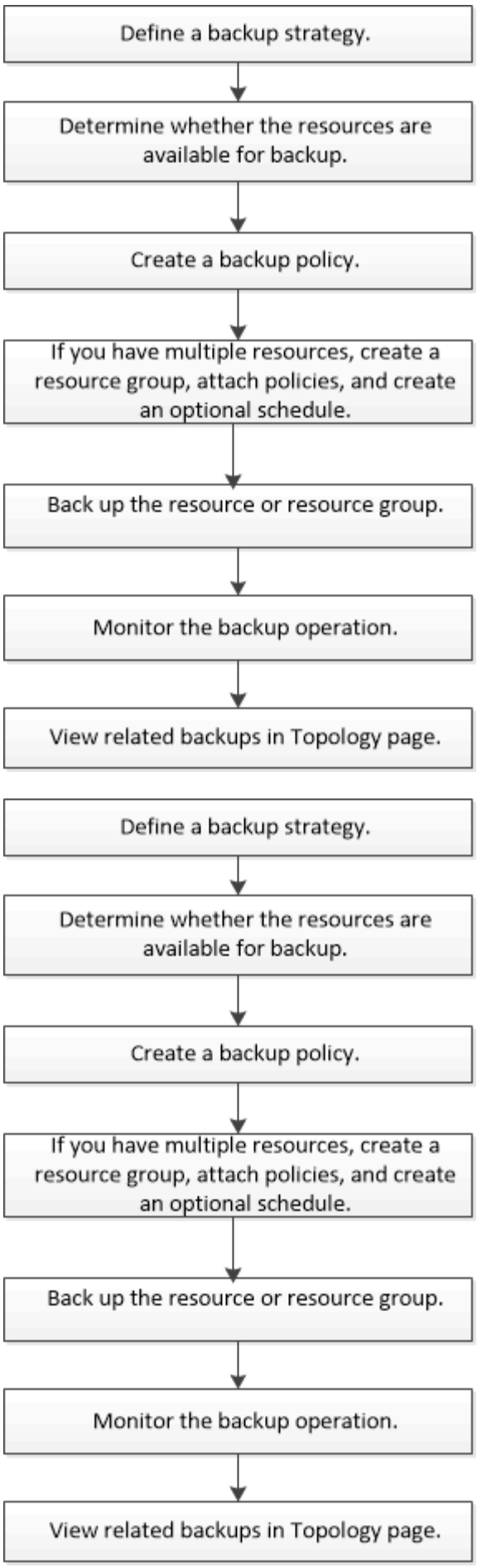
Back up Windows file systems

Back up Windows file systems

When you install the SnapCenter Plug-in for Microsoft Windows in your environment, you can use SnapCenter to back up Windows file systems. You can back up a single file system or a resource group that contains multiple file systems. You can back up on demand or according to a defined protection schedule.

You can schedule multiple backups to run across servers simultaneously. Backup and restore operations cannot be performed simultaneously on the same resource.

The following workflow shows the sequence in which you must perform the backup operations:


Define a backup strategy.
Determine whether the resources are available for backup.
Create a backup policy.
If you have multiple resources, create a resource group, attach policies, and create an optional schedule.
Back up the resource or resource group.
Monitor the backup operation.
View related backups in Topology page.
Define a backup strategy.
Determine whether the resources are available for backup.
Create a backup policy.
If you have multiple resources, create a resource group, attach policies, and create an optional schedule.
Back up the resource or resource group.
Monitor the backup operation.
View related backups in Topology page.

You can also use PowerShell cmdlets manually or in scripts to perform backup, restore, and clone operations. The SnapCenter cmdlet help or the SnapCenter Software Cmdlet Reference Guide contains detailed information about PowerShell cmdlets.

Determine resource availability for Windows file systems

Resources are the LUNs and similar components in your file system that are maintained by the plug-ins you have installed. You can add those resources to resource groups so that you can perform data protection jobs on multiple resources, but first you must identify which resources you have available. Discovering available resources also verifies that the plug-in installation was completed successfully.

Before you begin

- You must have already completed tasks such as installing SnapCenter Server, adding hosts, creating storage virtual machine (SVM) connections, and adding credentials.
- If files reside on VMware RDM LUNs or VMDKs, you must deploy the SnapCenter Plug-in for VMware vSphere and register the plug-in with SnapCenter. For more information, see SnapCenter Plug-in for VMware vSphere documentation.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, select **File Systems** from the list.
3. Select the host to filter the list of resources, and then click **Refresh Resources**.

   The newly added, renamed, or deleted file systems are updated to the SnapCenter Server inventory.

   You must refresh the resources if the databases are renamed outside of SnapCenter.

Create backup policies for Windows file systems

You can create a new backup policy for resources before you use SnapCenter to back up Windows file systems, or you can create a new backup policy at the time you create a resource group or when you back up a resource.

Before you begin

- You must have defined your backup strategy. Learn more
- You must have prepared for data protection.

  To prepare for data protection, you must complete tasks such as installing SnapCenter, adding hosts, discovering resources, and creating storage virtual machine (SVM) connections.

- If you are replicating Snapshots to a mirror or vault secondary storage, the SnapCenter administrator must have assigned the SVMs to you for both the source and destination volumes.
- If you want to run the PowerShell scripts in prescripts and postscripts, you should set the value of the usePowershellProcessforScripts parameter to true in the web.config file.

  The default value is false

- Review the SnapMirror active sync specific prerequisites and limitations. For information, refer Object limits for SnapMirror active sync.

About this task

- The SCRIPTS_PATH is defined using the PredefinedWindowsScriptsDirectory key located in the SMCoreServiceHost.exe.Config file of the plug-in host.

  If needed, you can change this path and restart SMcore service. It is recommended that you use the default path for security.

  The value of the key can be displayed from swagger through the API: API /4.7/configsettings

  You can use the GET API to display the value of the key. SET API is not supported.

- SnapLock
  - If 'Retain the backup copies for a specific number of days' option is selected, then the SnapLock retention period must be lesser than or equal to the mentioned retention days.
  - Specifying a Snapshot locking period prevents deletion of the Snapshots until the retention period expires. This could lead to retaining a larger number of Snapshots than the count specified in the policy.
  - For ONTAP 9.12.1 and below version, the clones created from the SnapLock Vault Snapshots as part of restore will inherit the SnapLock Vault expiry time. Storage admin should manually cleanup the clones post the SnapLock expiry time.

Steps

1. In the left navigation pane, select **Settings**.
2. In the Settings page, select **Policies**.
3. Select **New**.
4. In the Name page, enter the policy name and details.
5. In the Backup and Replication page, perform the following tasks:
   a. Select a backup setting.

Option	Description
File System Consistent Backup	Choose this option if you want SnapCenter to quiesce the disk drive on which the file system resides before the backup operation begins and then resume the disk drive after the backup operation ends.
File System Crash-consistent Backup	Choose this option if you do not want SnapCenter to quiesce the disk drive on which the file system resides.

   b. Select a schedule frequency (also called a policy type).

      The policy specifies the backup frequency only. The specific protection schedule for backing up is defined in the resource group. Therefore, two or more resource groups can share the same policy and backup frequency but have different backup schedules.

If you have scheduled for 2:00 a.m., the schedule will not be triggered during daylight saving time (DST).

c. Select a policy label.

Depending on the Snapshot label that you select, ONTAP applies the secondary Snapshot retention policy that matches the label.

If you have selected **Update SnapMirror after creating a local Snapshot copy**, you can optionally specify the secondary policy label. However, if you have selected **Update SnapVault after creating a local Snapshot copy**, you should specify the secondary policy label.

6. In the Select secondary replication options section, select one or both of the following secondary replication options:

For this field…	Do this…
Update SnapMirror after creating a local Snapshot copy	Select this option to create mirror copies of backup sets on another volume (SnapMirror). This option should be enabled for SnapSnapMirror active sync. During secondary replication, the SnapLock expiry time loads the primary SnapLock expiry time. Clicking the **Refresh** button in the Topology page refreshes the secondary and primary SnapLock expiry time that are retrieved from ONTAP. See View related backups and clones in the Topology page.
Update SnapVault after creating a Snapshot copy	Select this option to perform disk-to-disk backup replication. During secondary replication, the SnapLock expiry time loads the primary SnapLock expiry time. Clicking the Refresh button in the Topology page refreshes the secondary and primary SnapLock expiry time that are retrieved from ONTAP. When SnapLock is configured only on the secondary from ONTAP known as SnapLock Vault, clicking the Refresh button in the Topology page refreshes the locking period on the secondary that is retrieved from ONTAP. For more information on SnapLock Vault see Commit Snapshot copies to WORM on a vault destination

For this field…	Do this…
Error retry count	Enter the number of replication attempts that should occur before the process halts.

You should configure SnapMirror retention policy in ONTAP for the secondary storage to avoid reaching the maximum limit of Snapshots on the secondary storage.

7. In the Retention settings page, specify the retention settings for on-demand backups and for each schedule frequency you selected.

Option	Description
Total Snapshot copies to keep	Choose this option if you want to specify the number of Snapshots SnapCenter stores before automatically deleting them.
Keep Snapshot copies for	Choose this option if you want to specify the number of days SnapCenter retains a backup copy before deleting it.
Snapshot copy locking period	Select Snapshot locking period, and specify the duration days, months, or years. SnapLock retention period should be less than 100 years.

You should set the retention count to 2 or higher. The minimum value for the retention count is 2.

The maximum retention value is 1018. Backups will fail if retention is set to a value higher than what the ONTAP version supports.

8. In the Script page, enter the path of the prescript or postscript that you want the SnapCenter Server to run before or after the backup operation, respectively and a time limit that SnapCenter waits for the script to execute before timing out.

   For example, you can run a script to update SNMP traps, automate alerts, and send logs.

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

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

Create resource groups for Windows file systems

A resource group is the container to which you can add multiple file systems that you want to protect. You must also attach one or more policies to the resource group to define the type of data protection job that you want to perform, and then specify the backup

schedule.

About this task

- For ONTAP 9.12.1 and below version, the clones created from the SnapLock Vault Snapshots as part of restore will inherit the SnapLock Vault expiry time. Storage admin should manually cleanup the clones post the SnapLock expiry time.
- Adding new filesystems without SnapMirror active sync to an existing resource group which contains resources with SnapMirror active sync, is not supported.
- Adding new filesystems to an existing resource group in failover mode of SnapMirror active sync is not supported. You can add resources to the resource group only in regular or fail-back state.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, select **File Systems** from the list.

   If you have recently added a file system to SnapCenter, click **Refresh Resources** to view the newly added resource.

3. Click **New Resource Group**.
4. In the Name page in the wizard, do the following:

For this field…	Do this…
Name	Enter the resource group name. The resource group name should not exceed 250 characters.
Use custom name format for Snapshot copy	Optional: Enter a custom Snapshot name and format. For example, customtext_resourcegroup_policy_hostname or resourcegroup_hostname. By default, a timestamp is appended to the Snapshot name.
Tag	Enter a descriptive tag to help when finding a resource group.

5. In the Resources page, perform the following tasks:
   a. Select the host to filter the list of resources.

      If you have recently added resources, they will appear on the list of available resources only after you refresh your resource list.

   b. In the Available Resources section, click the file systems that you want to back up, and then click the right arrow to move them to the Added section.

      If you select the **Autoselect all resources on same storage volume** option, all of the resources on

the same volume are selected. When you move them to the Added section, all of the resources on that volume move together.

To add a single file system, clear the **Autoselect all resources on same storage volume** option and then select the file systems you want to move to the Added section.

6. In the Policies page, perform the following tasks:

   a. Select one or more policies from the drop-down list.

      You can select any existing policy and click **Details** to determine whether you can use that policy.

      If no existing policy meets your requirements, you can create a new policy by clicking  to start the policy wizard.

      The selected policies are listed in the Policy column in the Configure schedules for selected policies section.

   b. In the Configure schedules for selected policies section, click  in the Configure Schedules column for the policy for which you want to configure the schedule.

   c. If the policy is associated with multiple schedule types (frequencies), select the frequency that you want to configure.

   d. In the Add schedules for policy *policy_name* dialog box, configure the schedule by specifying the start date, expiration date, and frequency, and then click **Finish**.

      The configured schedules are listed in the Applied Schedules column in the Configure schedules for selected policies section.

   Third party backup schedules are not supported when they overlap with SnapCenter backup schedules. You should not modify the schedules from the Windows task scheduler and SQL Server Agent.

7. In the Notification page, provide notification information, as follows:

For this field…	Do this…
Email preference	Select **Always**, **On Failure**, or **On failure or warning**, to send emails to recipients after creating backup resource groups, attaching policies, and configuring schedules. Enter the SMTP server, default email subject line, and the To and From email addresses.
From	Email address
To	Email to address
Subject	Default email subject line

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

   You can perform a backup on demand or wait for the scheduled backup to occur.

Create resource groups and enable secondary protection for Windows file systems on ASA r2 systems

You should create the resource group to add the resources that are on ASA r2 systems. You can also provision the secondary protection while creating the resource group.

Before you begin

- You should ensure that you are not adding both ONTAP 9.x resources and ASA r2 resources to the same resource group.
- You should ensure that you do not have a database with both ONTAP 9.x resources and ASA r2 resources.

About this task

- The secondary protection is available only if the logged-in user is assigned to the role that has the **SecondaryProtection** capability enabled.
- If you enabled secondary protection, the resource group is put into maintenance mode while creating the primary and secondary consistency groups. After the primary and secondary consistency groups are created, the resource group is put out of maintenance mode.
- SnapCenter does not support secondary protection for a clone resource.

Steps

1. In the left navigation pane, select **Resources**, and the appropriate plug-in from the list.
2. In the Resources page, click **New Resource Group**.
3. In the Name page, perform the following actions:
   a. Enter a name for the resource group in the Name field.

      The resource group name should not exceed 250 characters.

   b. Enter one or more labels in the Tag field to help you search for the resource group later.

      For example, if you add HR as a tag to multiple resource groups, you can later find all resource groups associated with the HR tag.

   c. Select this check box, and enter a custom name format that you want to use for the Snapshot name.

      For example, customtext_resource group_policy_hostname or resource group_hostname. By default, a timestamp is appended to the Snapshot name.

   d. Specify the destinations of the archive log files that you do not want to back up.

      You should use the exact same destination as it was set in the application including prefix, if needed.

4. In the Resources page, select the database host name from the **Host** drop-down list.

   The resources are listed in the Available Resources section only if the resource is discovered successfully. If you have recently added resources, they will appear on the list of available resources only after you refresh your resource list.

5. Select the ASA r2 resources from the Available Resources section and move them to the Selected

Resources section.

6. In the Application Settings page, select the backup option.
7. In the Policies page, perform the following steps:
   a. Select one or more policies from the drop-down list.

      You can also create a policy by clicking + .

      In the Configure schedules for selected policies section, the selected policies are listed.

   b. Click + in the Configure Schedules column for the policy for which you want to configure a schedule.
   c. In the Add schedules for policy *policy_name* window, configure the schedule, and then click **OK**.

      Where, *policy_name* is the name of the policy that you have selected.

      The configured schedules are listed in the Applied Schedules column.

   Third party backup schedules are not supported when they overlap with SnapCenter backup schedules.

8. If the secondary protection is enabled for the policy that you have selected, then Secondary Protection page is displayed and you need to perform the following steps:
   a. Select the type of the replication policy.

      Synchronous replication policy is not supported.

   b. Specify the consistency group suffix that you want to use.
   c. From the Destination Cluster and Destination SVM drop-downs select the peered cluster and SVM that you want to use.

      The cluster and SVM peering is not supported by SnapCenter. You should use System Manager or ONTAP CLIs to perform cluster and SVM peering.

If the resources are already protected outside of SnapCenter, those resources will be displayed in the Secondary Protected Resources section.

1. On the Verification page, perform the following steps:
   a. Click **Load locators** to load the SnapMirror or SnapVault volumes to perform verification on secondary storage.
   b. Click + in the Configure Schedules column to configure the verification schedule for all the schedule types of the policy.
   c. In the Add Verification Schedules policy_name dialog box, perform the following actions:

If you want to…	Do this…
Run verification after backup	Select **Run verification after backup**.
Schedule a verification	Select **Run scheduled verification** and then select the schedule type from the drop-down list.

d. Select **Verify on secondary location** to verify your backups on secondary storage system.

e. Click **OK**.

The configured verification schedules are listed in the Applied Schedules column.

2. In the Notification page, from the **Email preference** drop-down list, select the scenarios in which you want to send the emails.

You must also specify the sender and receiver email addresses, and the subject of the email. If you want to attach the report of the operation performed on the resource group, select **Attach Job Report**.

For email notification, you must have specified the SMTP server details using the either the GUI or the PowerShell command Set-SmSmtpServer.

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

Create a storage system connection and a credential using PowerShell cmdlets

You must create a storage virtual machine (SVM) connection and a credential before using PowerShell cmdlets to perform data protection operations.

Before you begin

- You should have prepared the PowerShell environment to execute the PowerShell cmdlets.
- You should have the required permissions in the Infrastructure Admin role to create storage connections.
- You should ensure that the plug-in installations are not in progress.

  Host plug-in installations must not be in progress while adding a storage system connection because the host cache might not be updated and databases status might be displayed in the SnapCenter GUI as “Not available for backup” or “Not on NetApp storage”.

- Storage system names should be unique.

  SnapCenter does not support multiple storage systems with the same name on different clusters. Each storage system that is supported by SnapCenter should have a unique name and a unique management LIF IP address.

Steps

1. Initiate a PowerShell Core connection session by using the Open-SmConnection cmdlet.

   This example opens a PowerShell session:

```
PS C:\> Open-SmConnection
```

2. Create a new connection to the storage system by using the Add-SmStorageConnection cmdlet.

   This example creates a new storage system connection:

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Create a new credential by using the Add-SmCredential cmdlet.

   This example creates a new credential named FinanceAdmin with Windows credentials:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Back up a single resource on demand for Windows file systems

If a resource is not in a resource group, you can back up the resource on demand from the Resources page.

About this task

If you want to back up a resource that has a SnapMirror relationship with secondary storage, the role assigned to the storage user should include the “snapmirror all” privilege. However, if you are using the “vsadmin” role, then the “snapmirror all” privilege is not required.

When backing up a file system, SnapCenter does not back up LUNs that are mounted on a volume mount point (VMP) in the file system that is being backed up.

If you are working in a Windows file system context, do not back up database files. Doing so creates an inconsistent backup and a possible loss of data when restoring. To protect database files, you must use the appropriate SnapCenter plug-in for the database (for example, SnapCenter Plug-in for Microsoft SQL Server or SnapCenter Plug-in for Microsoft Exchange Server).

SnapCenter UI

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, select the File System resource type, and then select the resource that you want to back up.
3. If the File System - Protect wizard does not start automatically, click **Protect** to start the wizard.

   Specify the protection settings, as described in the Creating resource groups tasks.
4. Optional: In the Resource page of the wizard, enter a custom name format for the Snapshot.

   For example, customtext_resourcegroup_policy_hostname or resourcegroup_hostname. By default, a timestamp is appended to the Snapshot name.
5. In the Policies page, perform the following tasks:
   a. Select one or more policies from the drop-down list.

      You can select any existing policy, and then click **Details** to determine whether you can use that policy.

      If no existing policy meets your requirements, you can copy an existing policy and modify it or you can create a new policy by clicking  to start the policy wizard. If no existing policy meets your requirements, you can copy an existing policy and modify it or you can create a new policy by clicking  to start the policy wizard.

      The selected policies are listed in the Policy column in the Configure schedules for selected policies section.

   b. In the Configure schedules for selected policies section, click  in the Configure Schedules column for the policy for which you want to configure the schedule.
   c. In the Add schedules for policy *policy_name* dialog box, configure the schedule by specifying the start date, expiration date, and frequency, and then click **Finish**.

      The configured schedules are listed in the Applied Schedules column in the Configure schedules for selected policies section.

      Scheduled operations might fail
6. In the Notification page, perform the following tasks:

For this field…	Do this…
Email preference	Select **Always**, or **On Failure**, or **On failure or warning**, to send emails to recipients after creating backup resource groups, attaching policies, and configuring schedules. Enter the SMTP server information, default email subject line, and the “To” and “From” email addresses.
From	Email address
To	Email to address
Subject	Default email subject line

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

   The database topology page is displayed.

8. Click **Back up Now**.
9. In the Backup page, perform the following steps:
   a. If you have applied multiple policies to the resource, from the Policy drop-down list, select the policy that you want to use for backup.

      If the policy selected for the on-demand backup is associated with a backup schedule, the on-demand backups will be retained based on the retention settings specified for the schedule type.

   b. Click **Backup**.
10. Monitor the operation progress by clicking **Monitor** > **Jobs**.

PowerShell cmdlets

Steps

1. Initiate a connection session with the SnapCenter Server for a specified user by using the Open-SmConnection cmdlet.

   ```
   Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
   ```

   The username and password prompt is displayed.

2. Create a backup policy by using the Add-SmPolicy cmdlet.

   This example creates a new backup policy with a SQL backup type of FullBackup:

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

This example creates a new backup policy with a Windows file system backup type of CrashConsistent:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Discover host resources by using the Get-SmResources cmdlet.

   This example discovers the resources for the Microsoft SQL plug-in on the specified host:

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

   This example discovers the resources for Windows file systems on the specified host:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Add a new resource group to SnapCenter by using the Add-SmResourceGroup cmdlet.

   This example creates a new SQL database backup resource group with the specified policy and resources:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

   This example creates a new Windows file system backup resource group with the specified policy and resources:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Initiate a new backup job by using the New-SmBackup cmdlet.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. View the status of the backup job by using the Get-SmBackupReport cmdlet.

   This example displays a job summary report of all jobs that were run on the specified date:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Back up resource groups for Windows file systems

A resource group is a collection of resources on a host or cluster. A backup operation on the resource group is performed on all resources defined in the resource group. You can back up a resource group on demand from the Resources page. If a resource group has a policy attached and a schedule configured, then backups occur automatically according to the schedule.

Before you begin

- You must have created a resource group with a policy attached.
- If you want to back up a resource that has a SnapMirror relationship to secondary storage, the role assigned to the storage user should include the “snapmirror all” privilege. However, if you are using the “vsadmin” role, then the “snapmirror all” privilege is not required.
- If a resource group has multiple databases from different hosts, the backup operation on some of the hosts might trigger late because of network issues. You should configure the value of MaxRetryForUninitializedHosts in web.config by using the Set-SmConfigSettings PowerShell cmdlet

When backing up a file system, SnapCenter does not back up LUNs that are mounted on a volume mount point (VMP) in the file system that is being backed up.

If you are working in a Windows file system context, do not back up database files. Doing so creates an inconsistent backup and a possible loss of data when restoring. To protect database files, you must use the appropriate SnapCenter plug-in for the database (for example, SnapCenter Plug-in for Microsoft SQL Server or SnapCenter Plug-in for Microsoft Exchange Server).

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, select **Resource Group** from the **View** list.

You can search the resource group either by entering the resource group name in the search box or by clicking and selecting the tag. You can then click to close the filter pane.

3. In the Resource Groups page, select the resource group that you want to back up, and then click **Back up Now**.

   For SnapCenter Plug-in for Oracle Database, if you have a federated resource group with two databases and one of the database has datafile on a non-NetApp storage, the backup operation is aborted even though the other database is on a NetApp storage.

4. In the Backup page, perform the following steps:
   a. If you have associated multiple policies with the resource group, from the **Policy** drop-down list, select the policy that you want to use for backup.

      If the policy selected for the on-demand backup is associated with a backup schedule, the on-demand backups will be retained based on the retention settings specified for the schedule type.

   b. Click **Backup**.
5. Monitor the operation progress by clicking **Monitor** > **Jobs**.
   - In MetroCluster configurations, SnapCenter might not be able to detect a protection relationship after a failover.

     Unable to detect SnapMirror or SnapVault relationship after MetroCluster failover

   - If you are backing up application data on VMDKs and the Java heap size for the SnapCenter Plug-in for VMware vSphere is not large enough, the backup might fail. To increase the Java heap size, locate the script file `/opt/netapp/init_scripts/scvservice`. In that script, the `do_start method` command starts the SnapCenter VMware plug-in service. Update that command to the following: `Java -jar -Xmx8192M -Xms4096M`.

Monitor backup operations

You can monitor the progress of different backup operations by using the SnapCenterJobs page. You might want to check the progress 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 corresponding state of the operations:

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

Steps

1. In the left navigation pane, click **Monitor**.
2. In the Monitor page, click **Jobs**.
3. In the Jobs page, perform the following steps:
   a. Click  to filter the list so that only backup operations are listed.
   b. Specify the start and end dates.
   c. From the **Type** drop-down list, select **Backup**.
   d. From the **Status** drop-down, select the backup status.
   e. Click **Apply** to view the operations completed successfully.
4. Select a backup job, and then click **Details** to view the job details.

Though the backup job status displays  , when you click on job details you might see that some of the child tasks of the backup operation are still in progress or marked with warning signs.

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

   The **View logs** button displays the detailed logs for the selected operation.

Monitor operations in the Activity pane

The Activity pane displays the five most recent operations performed. The Activity pane also displays when the operation was initiated and the status of the operation.

The Activity pane displays information regarding backup, restore, clone, and scheduled backup operations.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. Click  on the Activity pane to view the five most recent operations.

   When you click one of the operations, the operation details are listed in the **Job Details** page.

Cancel backup operations

You can cancel backup operations that are queued.

What you will need

- You must be logged in as the SnapCenter Admin or job owner to cancel operations.
- You can cancel a backup operation from either the **Monitor** page or the **Activity** pane.
- You cannot cancel a running backup operation.
- You can use the SnapCenter GUI, PowerShell cmdlets, or CLI commands to cancel the backup operations.
- The **Cancel Job** button is disabled for operations that cannot be canceled.
- If you selected **All members of this role can see and operate on other members objects** in Users\Groups page while creating a role, you can cancel the queued backup operations of other members while using that role.

Steps

1. Perform one of the following actions:

From the…	Action
Monitor page	a. In the left navigation pane, click **Monitor** > **Jobs**. b. Select the operation, and then click **Cancel Job**.
Activity pane	a. After initiating the backup operation, click on the Activity pane to view the five most recent operations. b. Select the operation. c. In the Job Details page, click **Cancel Job**.

The operation is canceled, and the resource is reverted to the previous state.

View related backups and clones in the Topology page

When you are preparing to back up or clone a resource, you can view a graphical representation of all backups and clones on the primary and secondary storage. In the Topology page, you can see all of the backups and clones that are available for the selected resource or resource group. You can view the details of those backups and clones, and then select them to perform data protection operations.

About this task

You can review the following icons in the Manage Copies view to determine whether the backups and clones are available on the primary or secondary storage (Mirror copies or Vault copies).

- displays the number of backups and clones that are available on the primary storage.
- displays the number of backups and clones that are mirrored on the secondary storage using SnapMirror technology.

  Clones of a backup of a version-flexible mirror on a mirror-vault type volume are displayed in the topology view but the mirror backup count in the topology view does not include the version-flexible backup.

- displays the number of backups and clones that are replicated on the secondary storage using SnapVault technology.
  - The number of backups displayed includes the backups deleted from the secondary storage. For

example, if you have created 6 backups using a policy to retain only 4 backups, the number of backups displayed are 6.

Clones of a backup of a version-flexible mirror on a mirror-vault type volume are displayed in the topology view but the mirror backup count in the topology view does not include the version-flexible backup.

If you have secondary relationship as SnapMirror active sync (initially released as SnapMirror Business Continuity [SM-BC]), you can see following additional icons:

-  The replica site is up.
-  The replica site is down.
-  The secondary mirror or vault relationship has not been re-established.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, either select the resource or resource group from the **View** drop-down list.
3. Select the resource either from the resource details view or from the resource group details view.

   If the resource is protected, the topology page of the selected resource is displayed.

4. Review the Summary card to see a summary of the number of backups and clones available on the primary and secondary storage.

   The Summary Card section displays the total number of backups and clones. For Oracle database only, the Summary Card section also displays the total number of log backups.

   Clicking the **Refresh** button starts a query of the storage to display an accurate count.

   If SnapLock enabled backup is taken, then clicking the **Refresh** button refreshes the primary and secondary SnapLock expiry time retrieved from ONTAP. A weekly schedule also refreshes the primary and secondary SnapLock expiry time retrieved from ONTAP.

   When the application resource is spread across multiple volumes, the SnapLock expiry time for the backup will be the longest SnapLock expiry time that is set for a Snapshot in a volume. The longest SnapLock expiry time is retrieved from ONTAP.

   For SnapMirror active sync, clicking the **Refresh** button refreshes the SnapCenter backup inventory by querying ONTAP for both primary and replica sites. A weekly schedule also performs this activity for all databases containing SnapMirror active sync relationship.

   - For SnapMirror active sync and only for ONTAP 9.14.1, Async Mirror or Async MirrorVault relationships to the new primary destination should be manually configured after failover. From ONTAP 9.15.1 onwards Async Mirror or Async MirrorVault is auto configured to the new primary destination.
   - After failover, a backup should be created for SnapCenter to be aware of the failover. You can click **Refresh** only after a backup has been created.

5. In the Manage Copies view, click **Backups** or **Clones** from the primary or secondary storage to see details of a backup or clone.

The details of the backups and clones are displayed in a table format.

6. Select the backup from the table, and then click the data protection icons to perform restore, clone, rename, and delete operations.

   You cannot rename or delete backups that are on the secondary storage system.

7. If you want to delete a clone, then select the clone from the table and click to delete the clone.

Example showing backups and clones on the primary storage

Clean up the secondary backup count using PowerShell cmdlets

You can use the Remove-SmBackup cmdlet to clean up the backup count for secondary backups that have no Snapshot. You might want to use this cmdlet when the total Snapshots displayed in the Manage Copies topology do not match the secondary storage Snapshot retention setting.

You must have prepared the PowerShell environment to execute the PowerShell cmdlets.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Steps

1. Initiate a connection session with the SnapCenter Server for a specified user by using the Open-SmConnection cmdlet.

   ```
   Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
   ```

2. Clean up secondary backups count using the -CleanupSecondaryBackups parameter.

   This example cleans up the backup count for secondary backups with no Snapshots:

```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Restore Windows file systems

Restore Windows file system backups

You can use SnapCenter to restore file system backups. File system restoration is a multiphase process that copies all the data from a specified backup to the original location of the file system.

Before you begin

- You must have backed up the file system.
- If a scheduled operation, such as a backup operation, is currently in progress for a file system, then that operation must be cancelled before you can start a restore operation.
- You can only restore a file system backup to the original location, not to an alternate path.

  You cannot restore a single file from a backup because the restored file system overwrites any data on the original location of the file system. To restore a single file from a file system backup, you must clone the backup and access the file in the clone.

- You cannot restore a system or boot volume.
- SnapCenter can restore file systems in a Windows cluster without taking the cluster group offline.

About this task

- The SCRIPTS_PATH is defined using the PredefinedWindowsScriptsDirectory key located in the SMCoreServiceHost.exe.Config file of the plug-in host.

  If needed, you can change this path and restart SMcore service. It is recommended that you use the default path for security.

  The value of the key can be displayed from swagger through the API: API /4.7/configsettings

  You can use the GET API to display the value of the key. SET API is not supported.

- For SnapMirror active sync restore operation, you must select the backup from the primary location.
- For ONTAP 9.12.1 and below version, the clones created from the SnapLock Vault Snapshots as part of restore will inherit the SnapLock Vault expiry time. Storage admin should manually cleanup the clones post the SnapLock expiry time.

SnapCenter UI

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. To filter the list of resources, select the File System and Resource Group options.
3. Select a resource group from the list, and then click **Restore**.
4. In the Backups page, select whether you want to restore from primary or secondary storage systems, and then select a backup to restore.
5. Select your options in the Restore wizard.
6. You can enter the path and the arguments of the prescript or postscript that you want SnapCenter to run before or after the restore operation, respectively.

   For example, you can run a script to update SNMP traps, automate alerts, send logs, and so on.

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

7. In the Notification page, select one of the following options:

For this field…	Do this…
Log SnapCenter server events to storage system syslog	Select this option to log SnapCenter Server events to the syslog of the storage system.
Send AutoSupport notification for failed operations to storage system	Select this option to send information about any failed operations to NetApp using AutoSupport.
Email preference	Select **Always**, **On Failure**, or **On failure or warning** to send email messages to recipients after restoring backups. Enter the SMTP server, default email subject line, and To and From email addresses.

8. Review the summary, and then click **Finish**.
9. Monitor the operation progress by clicking **Monitor** > **Jobs**.

> If the restored file system contains a database, then you must also restore the database. If you do not restore the database, then your database might be in an invalid state. For information on restoring databases, see the Data Protection Guide for that database.

PowerShell cmdlets

Steps

1. Initiate a connection session with the SnapCenter Server for a specified user by using the Open-SmConnection cmdlet.

```
PS C:\> Open-Smconnection
```

2. Retrieve the information about the one or more backups that you want to restore by using the Get-SmBackup and Get-SmBackupReport cmdlets.

   This example displays information about all available backups:

```
PS C:\> Get-SmBackup

BackupId                      BackupName
BackupTime                    BackupType
--------                      ----------
----------                    ----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32
AM                 Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17
AM
```

   This example displays detailed information about the backup from January 29th 2015 to February 3rd, 2015:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. Restore data from the backup by using the Restore-SmBackup cmdlet.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Restore resources using PowerShell cmdlets

Restoring a resource backup includes initiating a connection session with the SnapCenter Server, listing the backups and retrieving backup information, and restoring a backup.

You must have prepared the PowerShell environment to execute the PowerShell cmdlets.

Steps

1. Initiate a connection session with the SnapCenter Server for a specified user by using the Open-SmConnection cmdlet.

```
PS C:\> Open-Smconnection
```

2. Retrieve the information about the one or more backups that you want to restore by using the Get-SmBackup and Get-SmBackupReport cmdlets.

   This example displays information about all available backups:

```
PS C:\> Get-SmBackup

BackupId                      BackupName                    BackupTime
BackupType
--------                      ----------                    ----------
----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32 AM
Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17 AM
```

   This example displays detailed information about the backup from January 29th 2015 to February 3rd, 2015:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. Restore data from the backup by using the Restore-SmBackup cmdlet.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Monitor restore operations

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

About this task

Post-restore states describe the conditions of the resource after a restore operation and any further restore actions that you can take.

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
- Canceled

Steps

1. In the left navigation pane, click **Monitor**.
2. In the **Monitor** page, click **Jobs**.
3. In the **Jobs** page, perform the following steps:
   a. Click to filter the list so that only restore operations are listed.
   b. Specify the start and end dates.
   c. From the **Type** drop-down list, select **Restore**.
   d. From the **Status** drop-down list, select the restore status.
   e. Click **Apply** to view the operations that have been completed successfully.
4. Select the restore job, and then click **Details** to view the job details.
5. In the **Job Details** page, click **View logs**.

   The **View logs** button displays the detailed logs for the selected operation.

Cancel restore operations

You can cancel restore jobs that are queued.

You should be logged in as the SnapCenter Admin or job owner to cancel restore operations.

About this task

- You can cancel a queued restore operation from either the **Monitor** page or the **Activity** pane.
- You cannot cancel a running restore operation.
- You can use the SnapCenter GUI, PowerShell cmdlets, or CLI commands to cancel the queued restore operations.
- The **Cancel Job** button is disabled for restore operations that cannot be canceled.
- If you selected **All members of this role can see and operate on other members objects** in Users\Groups page while creating a role, you can cancel the queued restore operations of other members while using that role.

Step

Perform one of the following actions:

From the…	Action
Monitor page	a. In the left navigation pane, click **Monitor** > **Jobs**. b. Select the job and click **Cancel Job**.

From the…	Action
Activity pane	a. After initiating the restore operation, click on the Activity pane to view the five most recent operations. b. Select the operation. c. In the Job Details page, click **Cancel Job**.

Clone Windows file systems

Clone from a Windows file system backup

You can use SnapCenter to clone a Windows file system backup. If you want a copy of a single file that was mistakenly deleted or changed, then you can clone a backup and access that file in the clone.

Before you begin

- You should have prepared for data protection by completing tasks such as adding hosts, identifying resources, and creating storage virtual machine (SVM) connections.
- You should have a backup of the file system.
- You should ensure that the aggregates hosting the volumes should be in the assigned aggregates list of the storage virtual machine (SVM).
- You cannot clone a resource group. You can only clone individual file system backups.
- If a backup resides on a virtual machine with a VMDK disk, SnapCenter cannot clone the backup to a physical server.
- If you clone a Windows cluster (for example, a shared LUN or a cluster shared volume (CSV) LUN), the clone is stored as a dedicated LUN on the host that you specify.
- For a cloning operation, the root directory of the volume mount point cannot be a shared directory.
- You cannot create a clone on a node that is not the home node for the aggregate.
- You cannot schedule recurring clone (clone lifecycle) operations for Windows file systems; you can only clone a backup on demand.
- If you move a LUN that contains a clone to a new volume, SnapCenter can no longer support the clone. For example, you cannot use SnapCenter to delete that clone.
- You cannot clone across environments. For example, cloning from a physical disk to a virtual disk or vice versa.

About this task

- The SCRIPTS_PATH is defined using the PredefinedWindowsScriptsDirectory key located in the SMCoreServiceHost.exe.Config file of the plug-in host.

  If needed, you can change this path and restart SMcore service. It is recommended that you use the default path for security.

  The value of the key can be displayed from swagger through the API: API /4.7/configsettings

  You can use the GET API to display the value of the key. SET API is not supported.

- For ONTAP 9.12.1 and below version, the clones created from the SnapLock Vault Snapshots as part of restore will inherit the SnapLock Vault expiry time. Storage admin should manually cleanup the clones post the SnapLock expiry time.

SnapCenter UI

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, select **File Systems** from the list.
3. Select the host.

   The topology view is automatically displayed if the resource is protected.

4. From the resources list, select the backup that you want to clone, and then click the clone icon.
5. In the Options page, do the following:

For this field…	Do this…
Clone server	Choose the host on which the clone should be created.
“Auto assign mount point” or “Auto assign volume mount point under path”	Choose whether to automatically assign a mount point or a volume mount point under a path. Auto assign volume mount point under path: The mount point under a path enables you to provide a specific directory in which the mount points will be created. Before you choose this option, you must verify that the directory is empty. If there is a backup in the directory, the backup will be in an invalid state after the mount operation.
Archive location	Choose an archive location if you are cloning a secondary backup.

6. In the Script page, specify any prescripts or postscripts you want to execute.

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

7. Review the summary, and then click **Finish**.
8. Monitor the operation progress by clicking **Monitor** > **Jobs**.

PowerShell cmdlets

Steps

1. Initiate a connection session with the SnapCenter Server for a specified user by using the Open-SmConnection cmdlet.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. List the backups that can be cloned by using the Get-SmBackup or Get-SmResourceGroup cmdlet.

This example displays information about all available backups:

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                      BackupTime   BackupType
--------   ----------                      ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

This example displays information about a specified resource group, its resources, and associated policies:

```
PS C:\> Get-SmResourceGroup -ListResources –ListPolicies

Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMaping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
```

```
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeOut : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
```

```
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
```

3. Initiate a clone operation from an existing backup by using the New-SmClone cmdlet.

   This example creates a clone from a specified backup with all logs:

```
PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

   This example creates a clone to a specified Microsoft SQL Server instance:

```
PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. View the status of the clone job by using the Get-SmCloneReport cmdlet.

   This example displays a clone report for the specified job ID:

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                   Sally_DRAPER}
```

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Monitor clone operations

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

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
- Canceled

Steps

1. In the left navigation pane, click **Monitor**.
2. In the **Monitor** page, click **Jobs**.
3. In the **Jobs** page, perform the following steps:
   a. Click  to filter the list so that only clone operations are listed.
   b. Specify the start and end dates.
   c. From the **Type** drop-down list, select **Clone**.
   d. From the **Status** drop-down list, select the clone status.
   e. Click **Apply** to view the operations that are completed successfully.
4. Select the clone job, and then click **Details** to view the job details.
5. In the Job Details page, click **View logs**.

Cancel clone operations

You can cancel clone operations that are queued.

You should be logged in as the SnapCenter Admin or job owner to cancel clone operations.

About this task

- You can cancel a queued clone operation from either the **Monitor** page or the **Activity** pane.
- You cannot cancel a running clone operation.
- You can use the SnapCenter GUI, PowerShell cmdlets, or CLI commands to cancel the queued clone operations.
- If you selected **All members of this role can see and operate on other members objects** in Users\Groups page while creating a role, you can cancel the queued clone operations of other members while using that role.

Step

Perform one of the following actions:

From the…	Action
Monitor page	a. In the left navigation pane, click **Monitor** > **Jobs**. b. Select the operation, and click **Cancel Job**.
Activity pane	a. After initiating the clone operation, click  on the Activity pane to view the five most recent operations. b. Select the operation. c. In the **Job Details** page, click **Cancel Job**.

Split a clone

You can use SnapCenter to split a cloned resource from the parent resource. The clone that is split becomes independent of the parent resource.

About this task

- You cannot perform the clone split operation on an intermediate clone.

  For example, after you create clone1 from a database backup, you can create a backup of clone1, and then clone this backup (clone2). After you create clone2, clone1 is an intermediate clone, and you cannot perform the clone split operation on clone1. However, you can perform the clone split operation on clone2.

  After splitting clone2, you can perform the clone split operation on clone1 because clone1 is no longer the intermediate clone.

- When you split a clone, the backup copies and clone jobs of the clone are deleted.
- For information about FlexClone volume split operations, see, Split a FlexClone volume from its parent volume.
- Ensure that the volume or aggregate on the storage system is online.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the **Resources** page, select the appropriate option from the View list:

Option	Description
For database applications	Select **Database** from the View list.
For file systems	Select **Path** from the View list.

3. Select the appropriate resource from the list.

   The resource topology page is displayed.

4. From the **Manage Copies** view, select the cloned resource (for example, the database or LUN), and then click  .
5. Review the estimated size of the clone that is to be split and the required space available on the aggregate, and then click **Start**.
6. Monitor the operation progress by clicking **Monitor** > **Jobs**.

   The clone split operation stops responding if the SMCore service restarts. You should run the Stop-SmJob cmdlet to stop the clone split operation, and then retry the clone split operation.

   If you want a longer poll time or shorter poll time to check whether the clone is split or not, you can change the value of *CloneSplitStatusCheckPollTime* parameter in *SMCoreServiceHost.exe.config* file to set the time interval for SMCore to poll for the status of the clone split operation. The value is in milliseconds and the default value is 5 minutes.

   For example:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   The clone split start operation fails if backup, restore, or another clone split is in progress. You should restart the clone split operation only after the running operations are complete.

Related information

SnapCenter clone or verification fails with aggregate does not exist

Copyright information

Trademark information