Back up NetApp supported plug-ins resources

SnapCenter software

NetApp
January 09, 2026

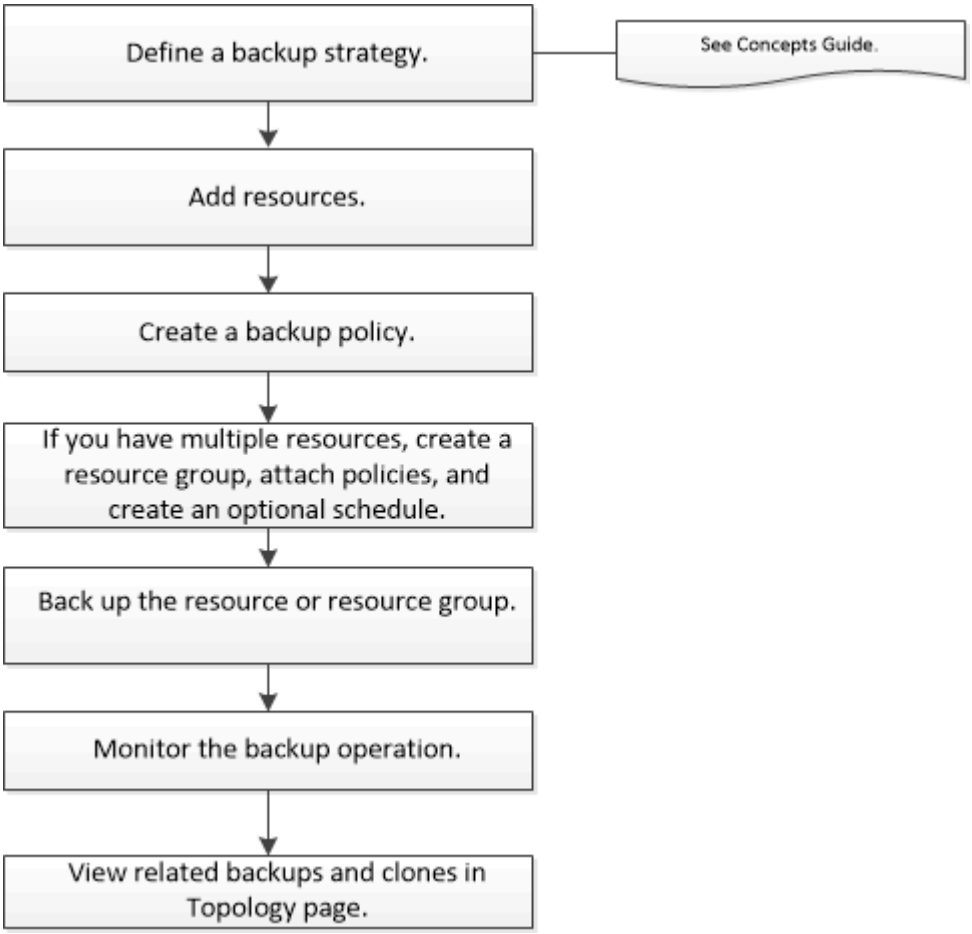
Table of Contents

Back up NetApp supported plug-ins resources

Back up NetApp supported plug-ins resources

The backup workflow includes planning, identifying the resources for backup, managing backup policies, creating resource groups and attaching policies, creating backups, and monitoring the operations.

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



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

Add resources to NetApp supported plug-ins

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

Before you begin

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

- You must have uploaded the plug-ins to SnapCenter Server.

Steps

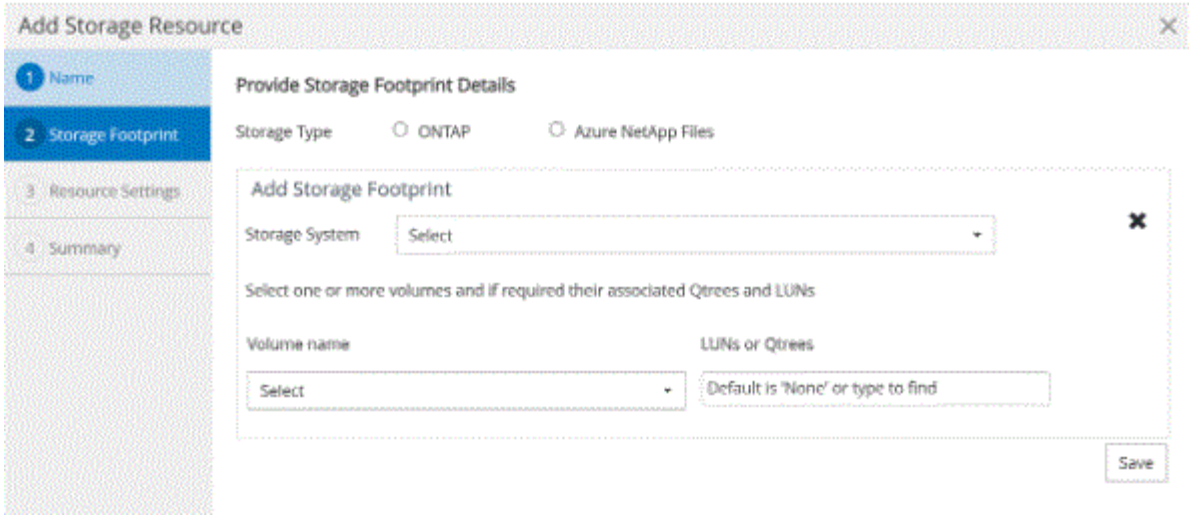
1. In the left navigation pane, select **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, select **Add Resource**.
3. In the Provide Resource Details page, perform the following actions:

For this field…	Do this…
Name	Enter the name of the resource.
Host name	Select the host.
Type	Select the type. Type is user defined as per the plug-in description file. For example, database and instance. In case the type selected has a parent, enter the details of the parent. For example, if the type is Database and the parent is Instance, enter the details of the Instance.
Credential name	Select Credential or create a new credential.
Mount Paths	Enter the mount paths where the resource is mounted. This is applicable only for a Windows host.

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

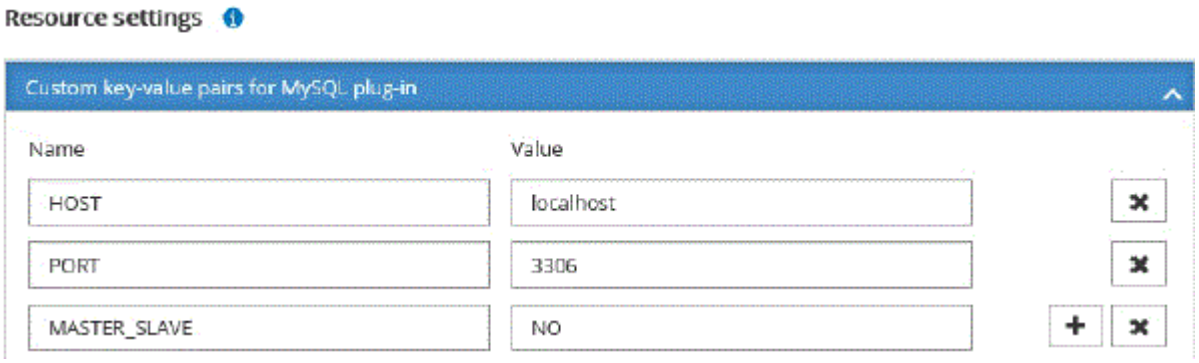
   Optional: Select the + icon to add more volumes, LUNs, and qtrees from other storage systems.

   NetApp supported plug-ins does not support automatic discovery of the resources. The storage details of physical and virtual environments are also not discovered automatically. You must provide the storage information for physical and virtual environments while creating the resources.



5. In the Resource Settings page, provide custom key-value pairs for the resource.

   Ensure that the custom keys name is in uppercase.



   For the respective plug-in parameters, refer Parameters to configure the resource

6. Review the summary, and then select **Finish**.

Result

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

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

After you finish

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

After adding the resources, you can modify the resource details. If a NetApp supported plug-ins resource has backups associated with it, the following fields cannot be modified: resource name, resource type, and host name.

Parameters to configure the resource

If you are adding the plug-ins manually, you can use the following parameters to configure the resource in the Resource Settings page.

Plug-in for MongoDB

Resource Settings:

- MONGODB_APP_SERVER=(for resource type as sharded cluster) or MONGODB_REPLICASET_SERVER=(for resource type as replicaset)
- OPLOG_PATH=(Optional parameter in case it is provided from MongoDB.propertiesfile)
- MONGODB_AUTHENTICATION_TYPE= (PLAIN for LDAP Authentication and None for others)

You must provide the following parameters needs to be provided n MongoDB.properties file:

- DISABLE_STARTING_STOPPING_SERVICES=
  - N if the start/stop services are performed by the plug-in.
  - Y if start/**stop services are performed by the user.
  - Optional parameter as default value is set to N.
- OPLOG_PATH_= (Optional parameter in case it is already provided as custom key-value pair in SnapCenter).

Plug-in for MaxDB

Resource Settings:

- XUSER_ENABLE (Y|N) enables or disables the use of an xuser for MaxDB so that a password is not required for the database user.
- HANDLE_LOGWRITER (Y|N) executes suspend logwriter (N) or resume logwriter (Y) operations.
- DBMCLICMD (path_to_dbmcli_cmd) specifies the path to the MaxDB dbmcli command. If not set, dbmcli on the search path is used.

  For Windows environment, the path must be within double-quotes ("…").

- SQLCLICMD (path_to_sqlcli_cmd) specifies the path to the MaxDB sqlcli command. If the path is not set, sqlcli is used on the search path.
- MAXDB_UPDATE_HIST_LOG (Y|N) instructs the MaxDB backup program whether it should update the MaxDB history log.
- MAXDB_CHECK_SNAPSHOT_DIR : Example, SID1:directory[,directory…]; [SID2:directoary[,directory…] checks that a Snap Creator Snapshot copy operation is successful and ensures that the snapshot is created.

  This applies to NFS only. The directory must point to the location that contains the .snapshot directory. Multiple directories can be included in a comma-separated list.

  In MaxDB 7.8 and later versions, the database backup request is marked Failed in the backup history.

- MAXDB_BACKUP_TEMPLATES: Specifies a backup template for each database.

The template must exist and be an external type of backup template. To enable snapshot integration for MaxDB 7.8 and later, you must have MaxDB background server functionality and already configured MaxDB backup template of the EXTERNAL type.

- MAXDB_BG_SERVER_PREFIX: Specifies the prefix for the background server name.

  If the MAXDB_BACKUP_TEMPLATES parameter is set, you must also set the MAXDB_BG_SERVER_PREFIX parameter. If you do not set the prefix, the default value na_bg_ is used.

Plug-in for SAP ASE

Resource Settings:

- SYBASE_SERVER (data_server_name) specifies the Sybase data server name (-S option on isql command). For example, p_test.
- SYBASE_DATABASES_EXCLUDE (db_name) allows databases to be excluded if the "ALL" construct is used.

  You can specify multiple databases by using a semicolon-separated list. For example: pubs2;test_db1.

- SYBASE_USER: user_name specifies the operating system user who can run the isql command.

  Required for UNIX. This parameter is required if the user running the Snap Creator Agent start and stop commands (usually the root user) and the user running the isql command are different.

- SYBASE_TRAN_DUMP db_name:directory_path enables you to perform a Sybase transaction dump after creating a snapshot. For example, pubs2:/sybasedumps/ pubs2

  You must specify each database requiring a transaction dump.

- SYBASE_TRAN_DUMP_COMPRESS (Y|N) enables or disables native Sybase transaction dump compression.
- SYBASE_ISQL_CMD (For example, /opt/sybase/OCS-15_0/bin/isql) defines the path to the isql command.
- SYBASE_EXCLUDE_TEMPDB (Y|N) allows you to auto exclude user created temporary databases.

Plug-in for Oracle applications (ORASCPM)

Resource Settings:

- SQLPLUS_CMD specifies the path to SQLplus.
- ORACLE_DATABASES lists the Oracle databases to be backed up and corresponding user (database:user).
- CNTL_FILE_BACKUP_DIR specifies the directory for control file back up.
- ORA_TEMP specifies the directory for temporary files.
- ORACLE_HOME specifies the directory where the Oracle software is installed.
- ARCHIVE_LOG_ONLY specifies whether to back up the archive logs or not.
- ORACLE_BACKUPMODE specifies whether to perform online or offline backup.
- ORACLE_EXPORT_PARAMETERS specifies whether the environment variables defined above should be re-exported while running */bin/su <user running sqlplus> -c sqlplus /nolog <cmd>*. This is typically the case, when the user who is running sqlplus has not set all environment variables necessary to connect to the

database using *connect / as sysdba*.

Create policies for NetApp supported plug-in resources

Before you use SnapCenter to back up NetApp supported plug-in specific resources, you must create a backup policy for the resource or resource group that you want to back up.

Before you begin

- You should have defined your backup strategy.

  For details, see the information about defining a data protection strategy for NetApp supported plug-ins.

- You should have prepared for data protection.

  Preparing for data protection includes tasks such as installing SnapCenter, adding hosts, creating storage system connections, and adding resources.

- The storage virtual machines (SVMs) should be assigned to you for mirror or vault operations.

  The SnapCenter administrator must have assigned the SVMs for both the source and destination volumes to you if you are replicating Snapshots to a mirror or vault.

- You should have manually added the resources that you want to protect.

About this task

- A backup policy is a set of rules that governs how you manage, schedule, and retain backups. Additionally, you can specify replication, script, and application settings.
- Specifying options in a policy saves time when you want to reuse the policy for another resource group.
- 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.

Primary SnapLock settings are managed in SnapCenter backup policy and the secondary SnapLock settings are managed by ONTAP.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Policies**.
3. Click **New**.
4. In the Name page, enter the policy name and details.
5. In the Policy type page, perform the following:
   a. Select storage type.

b. In the Custom backup settings section, provide any specific backup settings that have to be passed to the plug-in in key-value format.

   You can provide multiple key-values to be passed to the plug-in.

6. In the Snapshot and Replication page, perform the following steps:

   a. Specify the schedule type by selecting **On demand**, **Hourly**, **Daily**, **Weekly**, or **Monthly**.

   > You can specify the schedule (start date, end date, and frequency) for the backup operation while creating a resource group. This enables you to create resource groups that share the same policy and backup frequency, but enables you to assign different backup schedules to each policy.

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

   b. In the Snapshot settings section, specify the retention settings for the backup type and the schedule type selected in the **Backup Type** page:

If you want to…	Then…
Keep a certain number of Snapshots	Select **Copies to keep**, and then specify the number of Snapshots that you want to keep. If the number of Snapshots exceeds the specified number, the Snapshots are deleted with the oldest copies deleted first. > You must set the retention count to 2 or higher if you plan to enable SnapVault replication. If you set the retention count to 1, the retention operation might fail because the first Snapshot is the reference Snapshot for the SnapVault relationship until a newer Snapshot is replicated to the target. > The maximum retention value is 1018. Backups will fail if retention is set to a value higher than what the underlying ONTAP version supports.
Keep the Snapshots for a certain number of days	Select **Retain copies for**, and then specify the number of days for which you want to keep the Snapshots before deleting them.

If you want to…	Then…
Snapshot copy locking period	Select **Snapshot copy locking period**, and specify days, months, or years. SnapLock retention period should be less than 100 years.

c. Select a Policy label.

> You can assign SnapMirror labels to primary snapshots for remote replication, allowing the primary snapshots to offload the snapshot replication operation from SnapCenter to ONTAP secondary systems. This can be done without enabling SnapMirror or SnapVault option in the policy page.

7. 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 field to create mirror copies of the backup sets on another volume (SnapMirror replication). If the protection relationship in ONTAP is of type Mirror and Vault and if you select only this option, Snapshot created on the primary will not be transferred to the destination, but will be listed in the destination. If this Snapshot is selected from the destination to perform a restore operation, then the following error message is displayed: Secondary Location is not available for the selected vaulted/mirrored backup. 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 NetApp supported plug-ins resource related backups and clones in the Topology page.

For this field…	Do this…
Update SnapVault after creating a local Snapshot copy	Select this option to perform disk-to-disk backup replication (SnapVault backups). 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 Snapshots to WORM on a vault destination. See View NetApp supported plug-ins resource related backups and clones in the Topology page.
Error retry count	Enter the maximum number of replication attempts that can be allowed before the operation stops.

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

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

Create resource groups and attach policies

A resource group is the container to which you must add resources that you want to back up and protect. It enables you to back up all the data that is associated with a given application simultaneously. 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.

Steps

1. In the left navigation pane, select **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, select New Resource Group.
3. In the Name page, perform the following actions:

For this field…	Do this…
Name	Enter a name for the resource group. Note: The resource group name should not exceed 250 characters.

For this field…	Do this…
Tags	Enter one or more labels that will help you later search for the resource group. For example, if you add HR as a tag to multiple resource groups, you can later find all the resource groups associated with the HR tag.
Use custom name format for Snapshot copy	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.

4. Optional: In the Resources page, select a host name from the **Host** drop-down list and the resource type from the **Resource Type** drop-down list.

   This helps to filter information on the screen.

5. Select the resources from the **Available Resources** section, and then select the right arrow to move them to the **Selected Resources** section.
6. Optional: In the **Application Settings** page, do the following:
   a. Select the Backups arrow to set additional backup options:

      Enable consistency group backup and perform the following tasks:

For this field…	Do this…
Afford time to wait for Consistency Group Snapshot operation to complete	Select Urgent, Medium, or Relaxed to specify the wait time for Snapshot operation to complete. Urgent = 5 seconds, Medium = 7 seconds, and Relaxed = 20 seconds.
Disable WAFL Sync	Select this to avoid forcing a WAFL consistency point.

   b. Select the Scripts arrow and enter the pre and post commands for quiesce, Snapshot, and unquiesce operations. You can also enter the pre commands to be executed before exiting in the event of a failure.
   c. Select the Custom Configurations arrow and enter the custom key-value pairs required for all data protection operations using this resource.

Parameter	Setting	Description
ARCHIVE_LOG_ENABLE	(Y/N)	Enables the archive log management to delete the archive logs.
ARCHIVE_LOG_RETENTION	number_of_days	Specifies the number of days the archive logs are retained. This setting must be equal to or greater than NTAP_SNAPSHOT_ RETENTIONS.
ARCHIVE_LOG_DIR	change_info_directory/logs	Specifies the path to the directory that contains the archive logs.
ARCHIVE_LOG_EXT	file_extension	Specifies the archive log file extension length. For example, if the archive log is log_backup_0_0_0_0.16151855 1942 9 and if the file_extension value is 5, then the extension of the log will retain 5 digits, which is 16151.
ARCHIVE_LOG_RECURSIVE_ SE ARCH	(Y/N)	Enables the management of archive logs within subdirectories. You should use this parameter if the archive logs are located under subdirectories.

d. Select the **Snapshot Copy Tool** arrow to select the tool to create Snapshots:

If you want…	Then…
SnapCenter to use the plug-in for Windows and put the file system into a consistent state before creating a Snapshot. For Linux resources, this option is not applicable.	Select **SnapCenter with File System Consistency**. This option is not applicable for SnapCenter Plug-in for SAP HANA Database.
SnapCenter to create a storage level Snapshot	Select **SnapCenter without File System Consistency**.

If you want…	Then…
To enter the command to be executed on the host to create Snapshots.	Select **Other**, and then enter the command to be executed on the host to create a Snapshot.

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 selecting + .

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

   b. In the **Configure Schedules** column, select + for the policy you want to configure.
   c. In the Add schedules for policy *policy_name* dialog box, configure the schedule and select 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. From the **Email preference** drop-down list on the **Notification** page, 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. The SMTP server must be configured in **Settings** > **Global Settings**.

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

Create resource groups and enable secondary protection for resources 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 individual NetApp supported plug-ins resources

If an individual NetApp supported plug-ins resource is not part of any resource group, you can back up the resource from the Resources page. You can back up the resource on demand, or, if the resource has a policy attached and a schedule configured, then backups occur automatically according to the schedule.

Before you begin

- You must have created a backup policy.
- If you want to back up a resource that has a SnapMirror relationship with a secondary storage, the ONTAP 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.

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, filter resources from the **View** drop-down list based on resource type.

   Click  , and then select the host name and the resource type to filter the resources. You can then click  to close the filter pane.
3. Click the resource that you want to back up.
4. In the Resource page, if you want to use a custom name, select the **Use custom name format for Snapshot copy** check box , and then enter a custom name format for the Snapshot name.

   For example, *customtext_policy_hostname* or *resource_hostname*. By default, a timestamp is appended to the Snapshot name.
5. In the Application Settings page, do the following:
   a. Click the **Backups** arrow to set additional backup options:

      Enable consistency group backup, if needed, and perform the following tasks:

For this field…	Do this…
Afford time to wait for Consistency Group Snapshot operation to complete	Select Urgent, Medium, or Relaxed to specify the wait time for Snapshot operation to complete. Urgent = 5 seconds, Medium = 7 seconds, and Relaxed = 20 seconds.
Disable WAFL Sync	Select this to avoid forcing a WAFL consistency point.

b. Click the **Scripts** arrow to run pre and post commands for quiesce, Snapshot, and unquiesce operations. You can also run pre commands before exiting the backup operation.

   Prescripts and postscripts are run in the SnapCenter Server.

c. Click the **Custom Configurations** arrow, and then enter the custom value pairs required for all jobs using this resource.

d. Click the **Snapshot Copy Tool** arrow to select the tool to create Snapshots:

If you want…	Then…
SnapCenter to take a storage level Snapshot	Select **SnapCenter without File System Consistency**.
SnapCenter to use the plug-in for Windows to put the file system into a consistent state and then take a Snapshot	Select **SnapCenter with File System Consistency**.
To enter the command to create a Snapshot	Select **Other**, and then enter the command to create a Snapshot.

6. 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* dialog box, 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.

7. 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. SMTP must also be configured in **Settings** > **Global Settings**.

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

   The resources topology page is displayed.

9. Click **Back up Now**.

10. 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**.

11. 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. Add resources by using the Add-SmResources cmdlet.

   This example adds resources:

```
Add-SmResource -HostName 'scc55.sccore.test.com' -PluginCode
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database
-StorageFootPrint (
@{"VolumeName"="qtree_vol1_scc55_sccore_test_com";"QTREENAME"="qtree
Vol1";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

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

   This example creates a new backup policy:

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'
-PluginPolicyType DummyPlugin  -description 'testPolicy'
```

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

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

```
Add-SmResourceGroup -ResourceGroupName
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'
-Resources
@(@{"Host"="scc55.sccore.test.com";"Uid"="QTREE2";"PluginName"="Dumm
yPlugin"},@{"Host"="scc55.sccore.test.com";"Uid"="QTREE";"PluginName
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'
-usesnapcenterwithoutfilesystemconsistency
```

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

```
New-SMBackup -DatasetName
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy
test2
```

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:

```
Get-SmBackupReport -JobId 149

BackedUpObjects           : {QTREE2, QTREE}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 1
SmJobId                   : 149
StartDateTime             : 1/15/2024 1:35:17 AM
EndDateTime               : 1/15/2024 1:36:19 AM
Duration                  : 00:01:02.4265750
CreatedDateTime           : 1/15/2024 1:35:51 AM
Status                    : Completed
ProtectionGroupName       :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows
SmProtectionGroupId       : 1
PolicyName                : test2
SmPolicyId                : 4
BackupName                :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows_scc55_01-
15-2024_01.35.17.4467
VerificationStatus        : NotApplicable
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
PluginCode                : SCC
PluginName                : DummyPlugin
PluginDisplayName         : DummyPlugin
JobTypeId                 :
JobHost                   : scc55.sccore.test.com
```

Back up resource groups of NetApp supported plug-in resources

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 ONTAP 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.

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**.
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 NetApp supported plug-in resources 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.

Cancel backup operations for NetApp supported plug-ins

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 NetApp supported plug-ins resource related backups and clones in the Topology page

When you are preparing to back up or clone a resource, you might find it helpful to 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.

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.

   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.

   After on demand backup, by clicking the **Refresh** button refreshes the details of backup or clone.

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.

   You cannot rename the backups that are on the primary storage system.

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

Copyright information

Trademark information