Back up custom plug-in resources

SnapCenter Software 4.5

NetApp
July 03, 2026

This PDF was generated from https://docs.netapp.com/us-en/snapcenter-45/protect-scc/task_back_up_custom_plug_in_resources.html on July 03, 2026. Always check docs.netapp.com for the latest.

Table of Contents

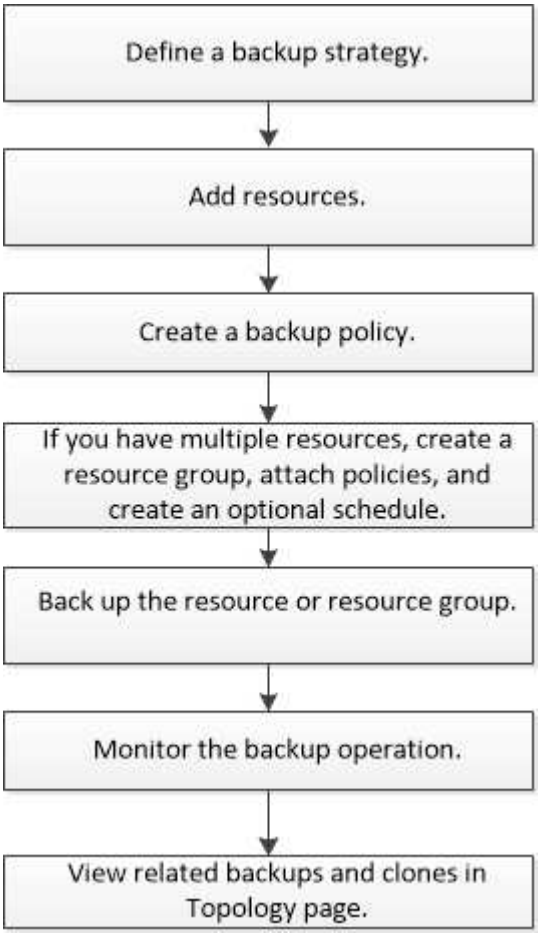
Back up custom plug-in resources . . . 1
- Back up custom plug-in resources . . . 1
- Add resources to SnapCenter Custom Plug-ins . . . 1
- Create policies for custom plug-in resources . . . 4
- Create resource groups and attach policies . . . 6
- Back up individual custom plug-in resources . . . 10
- Back up resource groups of custom plug-in resources . . . 12
- Create a storage system connection and a credential using PowerShell cmdlets . . . 13
- Back up resources using PowerShell cmdlets . . . 14
- Monitor custom plug-in resources backup operations . . . 16
- Cancel backup operations for custom plug-ins . . . 17
- View custom plug-in resource related backups and clones in the Topology page . . . 18

Back up custom plug-in resources

Back up custom plug-in 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 SnapCenter Custom 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.

What you will need

- You must have completed tasks such as installing the SnapCenter Server, adding hosts, creating storage

system connections, and adding credentials.

- You must have created a custom plug-in.

  Develop a plug-in for your application

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

Steps

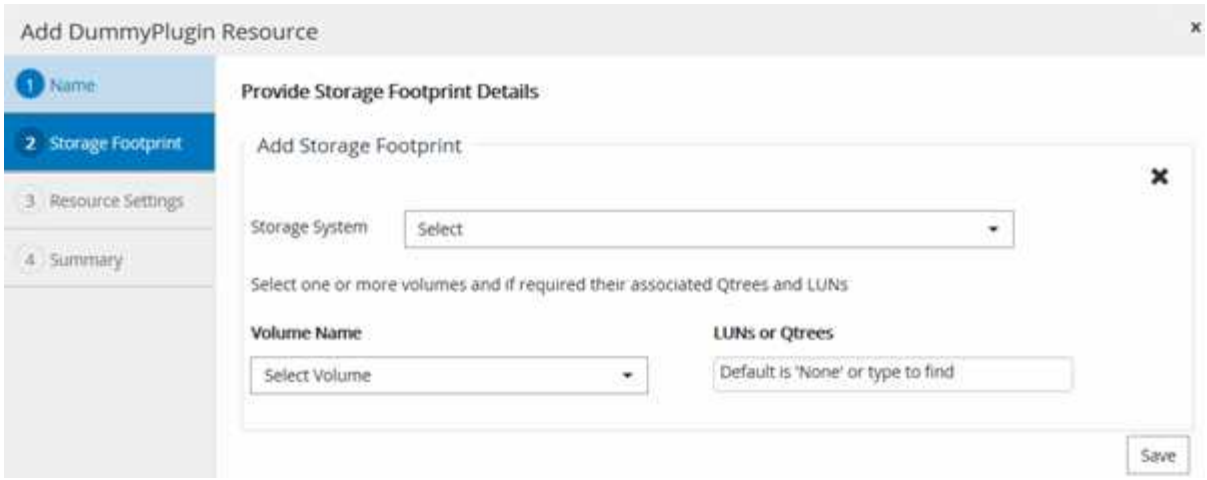
1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the **Resources** page, click **Add Resource**.
3. In the **Provide Resource Details** page, perform the following actions:

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 click **Save**.

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

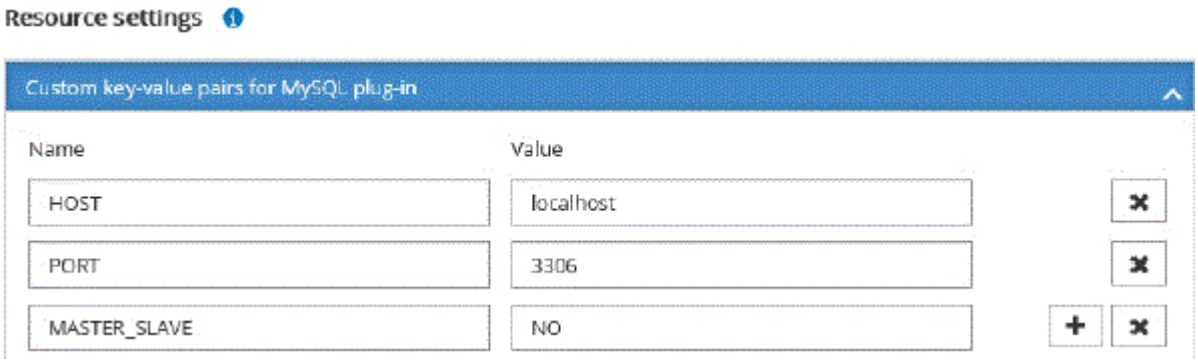
   SnapCenter Custom Plug-ins does not support automatic discovery of the resources and the storage details for physical and virtual environments. You must provide the storage information for physical and virtual environments while creating the resources.



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

   Use the custom key-value pairs if you want to pass resource-specific information. For example, when you are using the MySQL plug-in, you must specify a HOST as HOST=hostname, PORT =port-no used for MySQL and master-slave configuration as MASTER_SLAVE = “YES” or “NO” (name is MASTER_SLAVE and value is “YES” or “NO”).

   Ensure that the words HOST and PORT are in uppercase.



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

Result

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

After you finish

If you want to provide access to the assets to other users, 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 custom plug-in resource has backups associated with it, the following fields cannot be modified: resource name, resource type, and host name.

Create policies for custom plug-in resources

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

What you will need

- You should have defined your backup strategy.

  For details, see the information about defining a data protection strategy for custom 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 Snapshot copies to a mirror or vault.

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

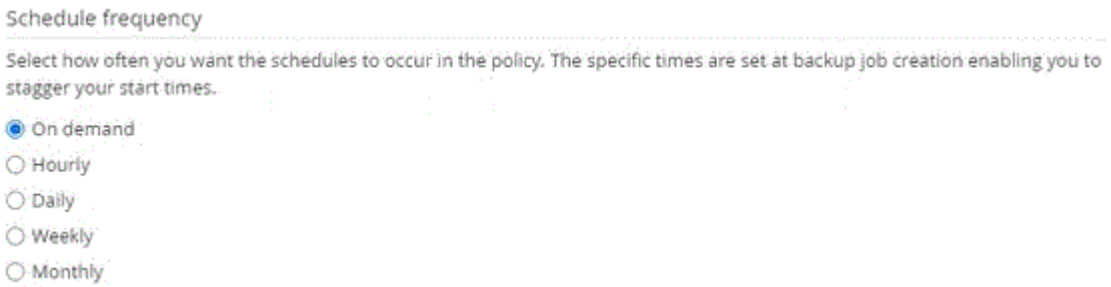
About this task

- 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.

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 description.
5. In the **Settings** page, perform the following steps:
   - 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).

- In the **Custom backup settings** section, provide any specific backup settings that has 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. On the **Retention** page, 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 Snapshot copies	Select **Total Snapshot copies to keep**, and then specify the number of Snapshot copies that you want to keep. If the number of Snapshot copies exceeds the specified number, the Snapshot copies 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 copy is the reference Snapshot copy for the SnapVault relationship until a newer Snapshot copy is replicated to the target. The maximum retention value is 1018 for resources on ONTAP 9.4 or later, and 254 for resources on ONTAP 9.3 or earlier. Backups will fail if retention is set to a value higher than what the underlying ONTAP version supports.
Keep the Snapshot copies for a certain number of days	Select **Keep Snapshot copies for**, and then specify the number of days for which you want to keep the Snapshot copies before deleting them.

7. On the **Replication** page, specify the replication settings:

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 copy created on the primary will not be transferred to the destination, but will be listed in the destination. If this Snapshot copy 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.
Update SnapVault after creating a local Snapshot copy	Select this option to perform disk-to-disk backup replication (SnapVault backups).
Secondary policy label	Select a Snapshot label. Depending on the Snapshot copy label that you select, ONTAP applies the secondary Snapshot copy 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.
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 Snapshot copies 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. A resource group enables you to back up all the data that is associated with a given application simultaneously. A resource group is required for any data protection job. 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, click **Resources**, and then select the appropriate plug-in from the list.
2. On the **Resources** page, click New Resource Group.
3. On the **Name** page, perform the following actions:

For this field…	Do this…
Name	Enter a name for the resource group. The resource group name should not exceed 250 characters.
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 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 copy name. For example, *customtext_resource group_policy_hostname or resource group_hostname*. By default, a timestamp is appended to the Snapshot copy name.

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

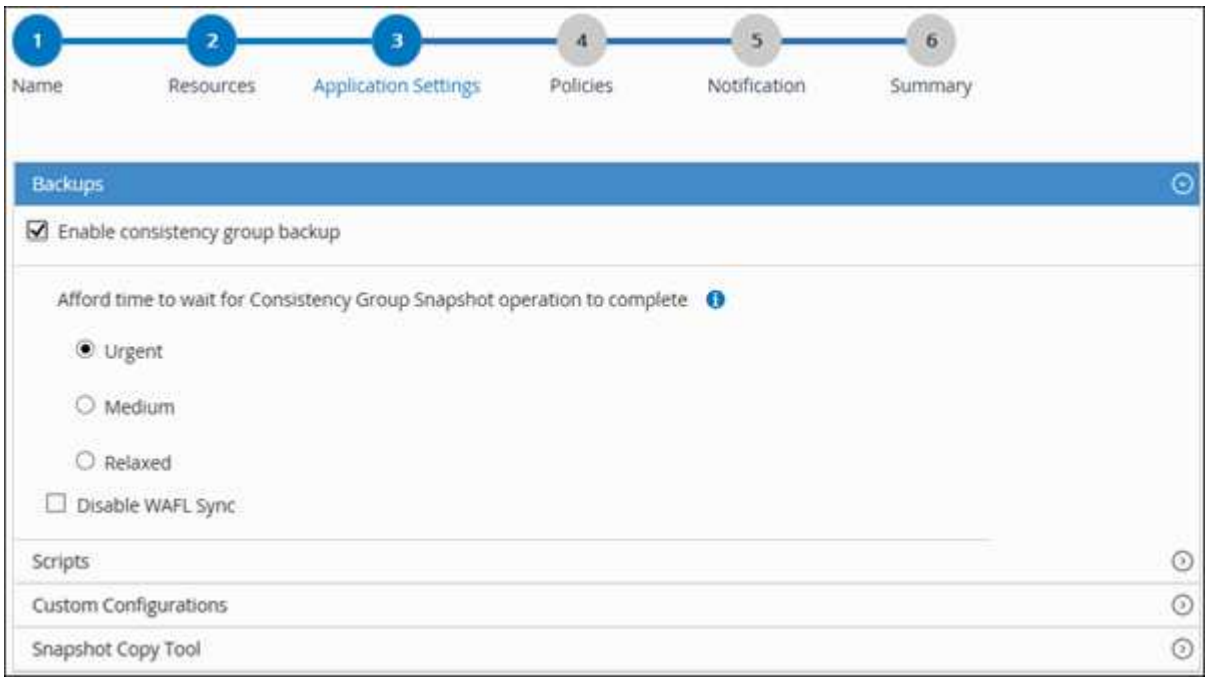
   This helps to filter information on the screen.

5. Select the resources from the **Available Resources** section, and then click the right arrow to move them to the **Selected Resources** section.
6. Optional: On the **Application Settings** page, do the following:
   a. Click 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 copy operation to complete. Urgent = 5 seconds, Medium = 7 seconds, and Relaxed = 20 seconds.

For this field…	Do this…
Disable WAFL Sync	Select this to avoid forcing a WAFL consistency point.



b. Click the Scripts arrow and enter the pre and post commands for quiesce, Snapshot copy, and unquiesce operations. You can also enter the pre commands to be executed before exiting in the event of a failure.

c. Click 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.

Parameter	Setting	Description
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. Click the **Snapshot Copy Tool** arrow to select the tool to create Snapshot copies:

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 copy. 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 copy	Select SnapCenter without File System Consistency.
To enter the command to be executed on the host to create Snapshot copies.	Select Other, and then enter the command to be executed on the host to create a Snapshot copy.

7. On 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 + .

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

b. In the **Configure Schedules** column, click + for the policy you want to configure.

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

8. On 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. The SMTP server must be configured in **Settings** > **Global Settings**.

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

Back up individual custom plug-in resources

If an individual custom plug-in 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.

What you will need

- 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.

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 copy name.

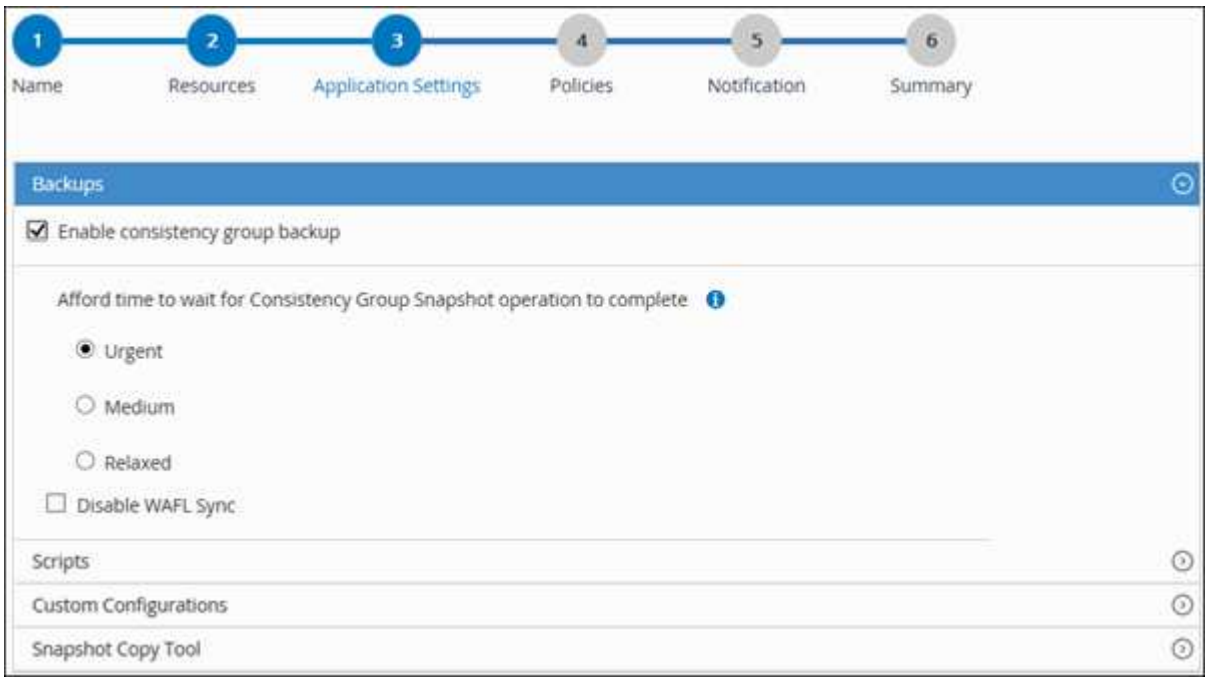
   For example, *customtext_policy_hostname* or *resource_hostname*. By default, a timestamp is appended to the Snapshot copy name.

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 copy operation to complete. Urgent = 5 seconds, Medium = 7 seconds, and Relaxed = 20 seconds.

For this field…	Do this…
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 copy, 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 Snapshot copies:

If you want…	Then…
SnapCenter to take a storage level Snapshot copy	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 copy	Select **SnapCenter with File System Consistency**.
To enter the command to create a Snapshot copy	Select **Other**, and then enter the command to create a Snapshot copy.

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**.

Back up resource groups of custom 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.

What you will need

- 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`.

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.

What you will need

- 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 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 resources using PowerShell cmdlets

Backing up a resource includes establishing a connection with the SnapCenter Server, adding resources, adding a policy, creating a backup resource group, and backing up.

What you will need

- You must have prepared the PowerShell environment to execute the PowerShell cmdlets.
- You must have added the storage system connection and created a credential.

About this task

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\
```

The username and password prompt is displayed.

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

   This example adds resources:

```
Add-SmResource -HostName '10.232.206.248' -PluginCode 'DB2'
-ResourceName NONREC1 -ResourceType Database -StorageFootPrint ( @
{"VolumeName"="DB2_NONREC1DB";"LunName"="DB2_NONREC1DB";"Vserver"="vserv
er_scauto_secondary"}) -Instance db2inst1
```

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

   This example creates a new backup policy:

```
Add-SMPolicy -PolicyName 'db2VolumePolicy' -PolicyType 'Backup'
-PluginPolicyType DB2  -description 'VolumePolicy'
```

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_ManualBackup_DatabaseLevel_MultipleVolume_unix' -Resources @(@
{"Host"="10.232.206.248";"Uid"="db2inst2\NONREC"},@{"Host"="10.232.206.2
48";"Uid"="db2inst1\NONREC"}) -Policies db2ManualPolicy
```

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

```
New-SMBackup -DatasetName
Verify_ManualBackup_DatabaseLevel_MultipleVolume_unix -Policy
db2ManualPolicy
```

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-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

Monitor custom 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. On 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. On the **Job Details** page, click **View logs**.

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

Cancel backup operations for custom 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**.

From the…	Action
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. On the Job Details page, click **Cancel Job**.

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

View custom plug-in 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.

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

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

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

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

Trademark information

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