Back up Windows file systems

SnapCenter Software 4.5

NetApp
July 03, 2026

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

Table of Contents

Back up Windows file systems . . . 1
- Back up Windows file systems . . . 1
- Determine resource availability for Windows file systems . . . 1
- Create backup policies for Windows file systems . . . 2
- Create resource groups for Windows file systems . . . 4
- Back up a single resource on demand for Windows file systems . . . 6
- Back up resource groups for Windows file systems . . . 8
- Create a storage system connection and a credential using PowerShell cmdlets . . . 9
- Back up resources using PowerShell cmdlets . . . 10
- Monitor backup operations . . . 12
  - Monitor operations in the Activity pane . . . 13
- Cancel backup operations . . . 13
- View related backups and clones in the Topology page . . . 14
- Remove backups using PowerShell cmdlets . . . 16
- Clean up the secondary backup count using PowerShell cmdlets . . . 17

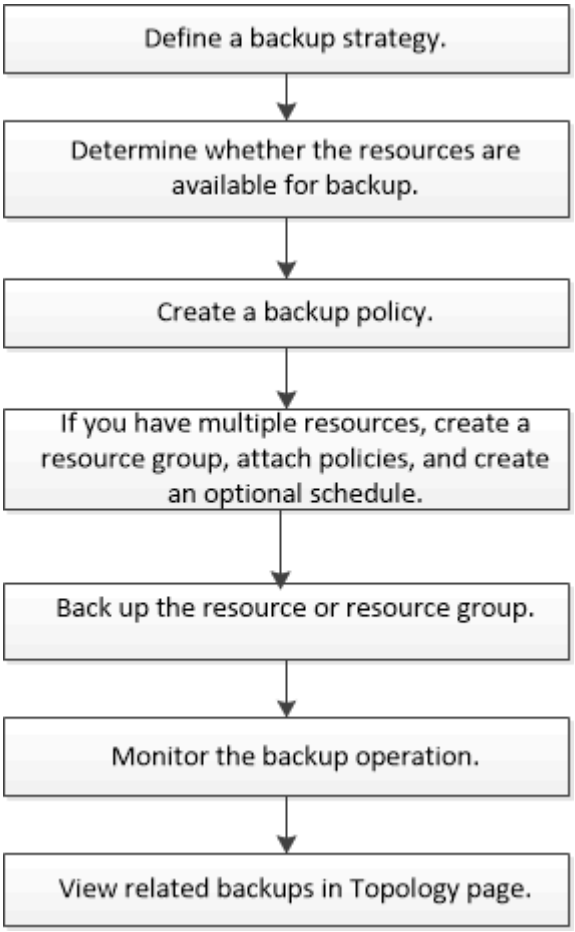
Back up Windows file systems

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:



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.

What you will need

- 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.

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.

What you will need

- 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 Snapshot copies 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

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Policies**.
3. To determine if you can use an existing policy, select the policy name and then click **Details**.

   After reviewing the existing policies, you can perform one of the following:

   - Use an existing policy.

- Copy an existing policy and modify the policy configuration.
- Create a new policy.

4. To create a new policy, click **New**.
5. On the Name page, enter the policy name and a description.
6. On the Backup Options 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).

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

Option	Description
Total Snapshot copies to retain	Choose this option if you want to specify the number of Snapshot copies SnapCenter stores before automatically deleting them.
Delete Snapshot copies older than	Choose this option if you want to specify the number of days SnapCenter retains a backup copy before deleting it.

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 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.

8. On the Replication page, specify replication to the secondary storage system:

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).
Update SnapVault after creating a Snapshot copy	Select this option to perform disk-to-disk backup replication.
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 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 Snapshot copies on the secondary storage.

9. On 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.

10. 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.

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. On 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 copy name and format. For example, customtext_resourcegroup_policy_hostname or resourcegroup_hostname. By default, a timestamp is appended to the Snapshot copy name.
Tag	Enter a descriptive tag to help when finding a resource group.

5. On 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. On 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. On 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.

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, SnapCenter Plug-in for Microsoft Exchange Server, or a custom plug-in for database files).

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 copy.

   For example, customtext_resourcegroup_policy_hostname or resourcegroup_hostname. By default, a timestamp is appended to the Snapshot copy 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.

      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. On 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**.

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.

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 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, SnapCenter Plug-in for Microsoft Exchange Server, or a custom plug-in for database files).

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`.

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

You can use the PowerShell cmdlets to backup SQL Server databases or Windows file systems. This would include backing up a SQL Server database or Windows file system includes establishing a connection with the SnapCenter Server, discovering the SQL Server database instances or Windows file systems, adding a policy,

creating a backup resource group, backing up, and verifying the backup.

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.
- You must have added hosts and discovered resources.

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.

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. 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.

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. If you are using Plug-in for SQL Server or Plug-in for Exchange Server, the Activity pane also displays information about the reseed operation.

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. On 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.
  - If you have upgraded from SnapCenter 1.1, the clones on the secondary (mirror or vault) are not displayed under Mirror copies or Vault copies in the Topology page. All the clones created using SnapCenter 1.1 are displayed under the Local copies in SnapCenter 3.0.

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. 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.

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.

   If you are using SnapCenter Custom Plug-ins, you cannot rename the backups that are on the primary storage system.

   - If you select a backup of an Oracle resource or resource group, you can also perform mount and unmount operations.
   - If you have selected a log backup of an Oracle resource or resource group, you can perform rename,

mount, unmount, and delete operations.

- If you are using SnapCenter Plug-ins Package for Linux and have cataloged the backup using Oracle Recovery Manager (RMAN), you cannot rename those cataloged backups.

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

Remove backups using PowerShell cmdlets

You can use the Remove-SmBackup cmdlet to delete backups if you no longer require them for other data protection operations.

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. Delete one or more backup using the Remove-SmBackup cmdlet.

   This example deletes two backups using their backup IDs:

```
Remove-SmBackup -BackupIds 3,4
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"):
```

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 copies. You might want to use this cmdlet when the total Snapshot copies displayed in the Manage Copies topology do not match the secondary storage Snapshot copy 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 Snapshot copies:

```
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"):
```

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.