



SnapCenter® Software 4.1

Data Protection Guide

For Microsoft Windows® File Systems

August 2019 | 215-13396_2019-08_en-us
doccomments@netapp.com

Updated for 4.1.1



Contents

Deciding whether to read the SnapCenter Data Protection Guide for	
Windows File Systems	5
SnapCenter Plug-in for Microsoft Windows overview	6
SnapCenter Plug-in for Windows file systems data protection	
workflow	7
Backing up Windows file systems	8
Determining resource availability	8
Viewing related backups and clones in the Topology page	9
Creating backup policies for Windows file systems	11
Creating resource groups for Windows file systems	13
Backing up a single resource on demand	14
Backing up resource groups	16
Monitoring backup operations	17
Monitoring operations in the Activity pane	18
Canceling the backup operations	18
Restoring Windows file system backups	20
Monitoring restore operations	21
Canceling restore operations	22
Cloning from a Windows file system backup	23
Monitoring clone operations in SnapCenter	24
Canceling clone operations	25
Splitting a clone	26
Backing up, restoring, cloning, and removing backups using	
PowerShell cmdlets	27
Creating a storage system connection and a Run As account using PowerShell	
cmdlets	27
Backing up resources using PowerShell cmdlets	28
Restoring and recovering resources using PowerShell cmdlets	30
Cloning backups using PowerShell cmdlets	32
Removing backups using PowerShell cmdlets	35
Cleaning up the secondary backup count using PowerShell cmdlets	36
Troubleshooting data protection operations	37
Back up operation on some hosts might trigger late	37
SnapCenter Plug-in Package for Microsoft Windows or SnapCenter Plug-in for	
Microsoft SQL Server upgrade might fail on hosts with SQL databases on	
VMDK	37
Storage layout could not be determined	38
HTTP error 503. The service is unavailable.	38
Unable to display SnapCenter web login page on local host	38
SnapCenter plug-in loader fails with an error	38

SnapCenter plug-in loader does not start automatically when the host is restarted	39
Unable to access cluster IP address from outside network	40
Backup fails with error: Storage system(s) may need to be added, also ensure that the associated host is in a connected state	40
Unable to find Snapshot copy after successfully creating the backup	41
Backup operation fails if Snapshot copies on the secondary storage reaches maximum limit	41
Scheduled backups fail due to task limit	42
Clone operation will fail due to inaccessible virtual device	42
Clone split estimation fails when the aggregate does not have space	43
Clone split start operation fails	43
Clone split operation stops responding	43
Databases on which the clone split operation was performed are listed as clones ...	44
Managing resource groups	45
Stopping and resuming operations on resource groups	45
Deleting resource groups	46
Managing policies	47
Detaching policies	47
Modifying policies	48
Deleting policies	49
Managing backups	50
Renaming backups	50
Deleting backups	50
Managing clones	52
Deleting clones	52
Copyright	53
Trademark	54
How to send comments about documentation and receive update notifications	55

Deciding whether to read the SnapCenter Data Protection Guide for Windows File Systems

This guide information how to use SnapCenter to perform backup, restore, and clone operations on Windows file systems.

You should read this information if you want to use SnapCenter in the following ways:

- You want to create data protection policies and resource groups for Windows file systems
- You want to perform backup, restore, or clone operations on Windows file systems using the graphical user interface (GUI)
- You want to perform backup, restore, or clone operations on Windows file systems using Windows PowerShell cmdlets

You should have already performed the following tasks:

- Installed SnapCenter Server and the SnapCenter Plug-in for Microsoft Windows
- Configured role-based access control (RBAC), storage system connections, and Run As accounts
- Installed the SnapCenter Plug-in for VMware vSphere and registered it with SnapCenter, if you want to protect Windows file systems on virtual machines
- Set up SnapMirror and SnapVault relationships, if you want backup replication

You can also use the following information to help accomplish your data protection goals:

- SnapCenter Server and plug-in installation and setup
[*Installing and setting up SnapCenter*](#)
[*Getting Started*](#)
- SnapCenter concepts, including architecture, features, and benefits
[*Concepts*](#)
- Other SnapCenter Data Protection Guides for specific types of resources, such as Microsoft SQL Server, Oracle, Windows file systems, and custom plug-ins
- SnapCenter PowerShell commands
[*SnapCenter Software 4.1 Windows Cmdlet Reference Guide*](#)
- SnapCenter administration, including dashboards, reporting capabilities, and REST APIs, and managing licenses, storage connections, and the SnapCenter Server repository
[*Performing administrative tasks*](#)

SnapCenter Plug-in for Microsoft Windows overview

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

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

For information about SnapCenter data protection, see the Data Protection Guide for your plug-in.

For information about the SnapCenter architecture, features, and benefits, see the SnapCenter concepts documentation.

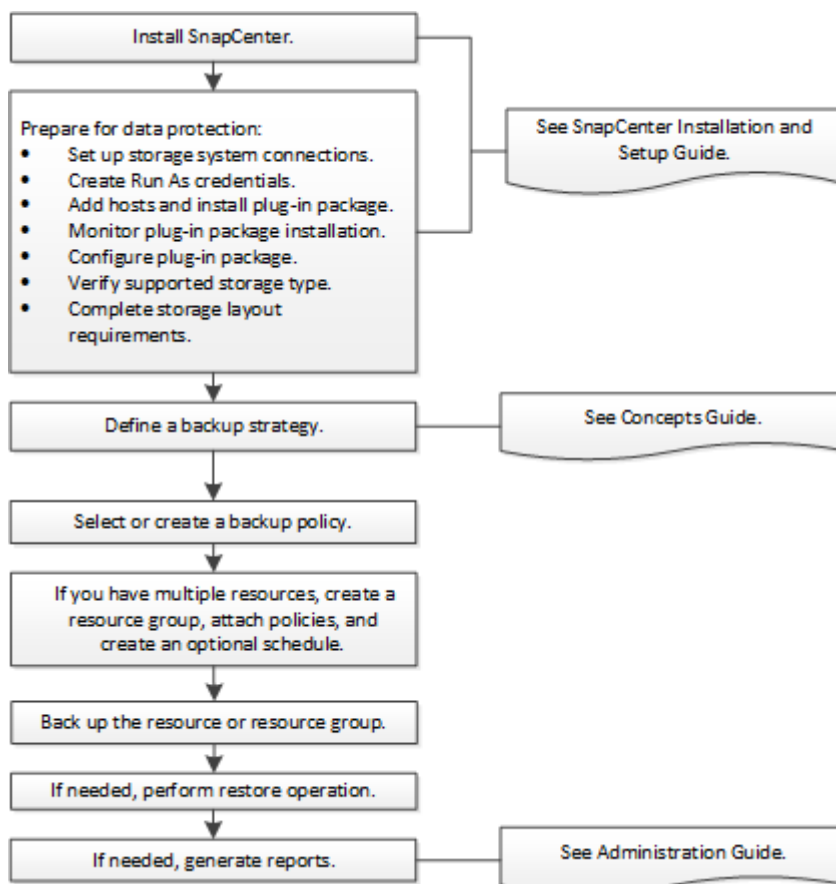
Related information

[*Concepts*](#)

[*Installing and setting up SnapCenter*](#)

SnapCenter Plug-in for Windows file systems data protection workflow

The data protection workflow lists the tasks that you have to perform for data protection.



Related tasks

[Restoring Windows file system backups](#) on page 20

[Cloning from a Windows file system backup](#) on page 23

Related references

[Backing up Windows file systems](#) on page 8

Related information

[Installing and setting up SnapCenter](#)

[Concepts](#)

[Performing administrative tasks](#)

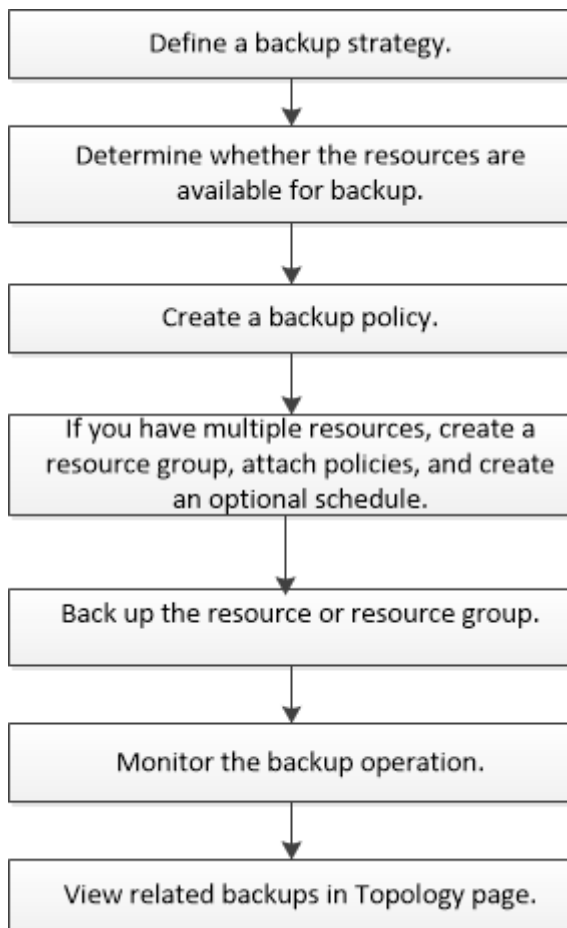
Backing up Windows file systems

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 cmdlet reference information contains detailed information about PowerShell cmdlets.

[*SnapCenter Software 4.1 Windows Cmdlet Reference Guide*](#)

Determining resource availability

Resources are the LUNs and similar components in your file system that are maintained by the plug-ins you have installed. You can add those resources to resource groups so that you can perform data

protection jobs on multiple resources, but first you must identify which resources you have available. Discovering available resources also verifies that the plug-in installation was completed successfully.

Before you begin

- You must have already completed tasks such as installing SnapCenter Server, adding hosts, creating storage virtual machine (SVM) connections, and adding Run As credentials.
- If file systems reside on VMware RDM LUNs or VMDKs, you must have installed the SnapCenter Plug-in for VMware vSphere.

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.

Viewing 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.

Note: 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.

Note: 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.

Note: 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

Manage Copies



Summary Card

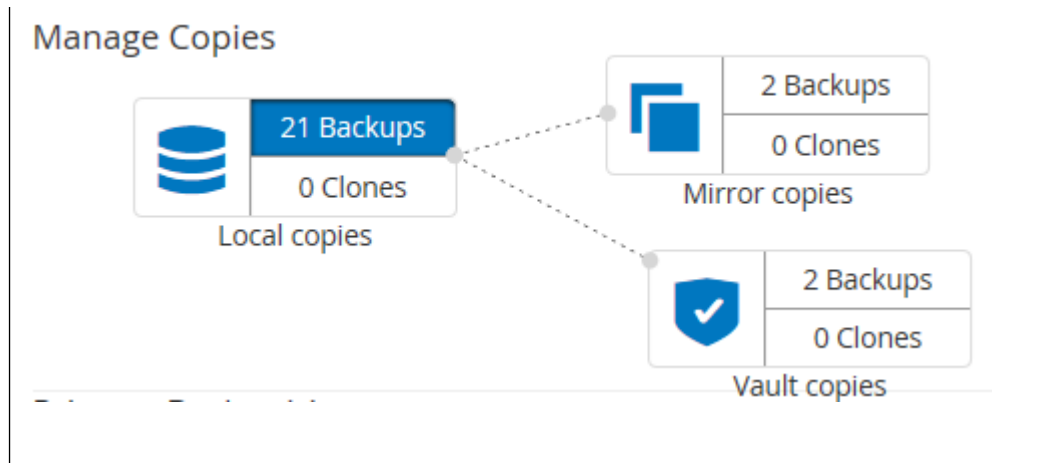
2 Backups

1 Data Backups

1 Log Backups

1 Clones

Example showing backups on the primary and secondary storage



Creating backup policies for Windows file systems

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

Before you begin

- You must have defined your backup strategy.
For details, see the information about defining a data protection strategy for Windows file systems.
[Concepts](#)
- 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.
For information about how administrators assign resources to users, see the SnapCenter installation information.
[Installing and setting up SnapCenter](#)

About this task

Most of the fields on these wizard pages are self-explanatory. The following information describes some of the fields for which you might require guidance.

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 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. In the **Name** page, enter the policy name and a description.
6. In 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.

7. In 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.

Important: You should set the retention count to 2 or higher if you plan to enable SnapVault replication. If you set the replication count to 1, the retention operation can fail. This is because the first Snapshot copy is the reference Snapshot copy for the SnapVault relationship until the newer Snapshot copy is replicated to the target.

Note: 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. In 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	Enter the frequency label for the secondary storage Snapshot copy. Every Snapshot copy has this label to distinguish it from the different groups on the secondary storage system. For example, Snapmirror Label: weekly is a frequency label.
Error retry count	Enter the number of replication attempts that should occur before the process halts.

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

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

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

Related information

[Performing administrative tasks](#)

[Installing and setting up SnapCenter](#)

Creating 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.
Note: 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.
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. In the **Resources** page, perform the following tasks:
 - a. Select the host to filter the list of resources.
If you have recently added resources, they will appear on the list of available resources only after you refresh your resource list.
 - b. In the **Available Resources** section, click the file systems that you want to back up, and then click the right arrow to move them to the **Added** section.
If you select the **Autoselect all resources on same storage volume** option, all of the resources on the same volume are selected. When you move them to the Added section, all of the resources on that volume move together.
To add a single file system, clear the **Autoselect all resources on same storage volume** option and then select the file systems you want to move to the Added section.
6. In the **Policies** page, perform the following tasks:

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

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

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

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

- b. In the **Configure schedules for selected policies** section, click  in the Configure Schedules column for the policy for which you want to configure the schedule.
- c. If the policy is associated with multiple schedule types (frequencies), select the frequency that you want to configure.
- d. In the **Add schedules for policy** *polycynname* 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.

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

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

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

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

Related information

[Performing administrative tasks](#)

Backing up a single resource on demand

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

Before you begin

If you are backing up a resource that has a SnapMirror relationship to secondary storage, you must have SnapCenter admin privileges and the scadmin role must include the “snapmirror all” privilege.

About this task

Note: 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.

Attention: 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 resource does not have protection settings specified (policy, schedule, notifications), the **File System - Protect** wizard starts; otherwise 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 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** *polycyname* 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.

6. In the **Notification** page, perform the following tasks:

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 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**.

8. Monitor the operation progress by clicking **Monitor > Jobs**.

Related tasks

[Monitoring backup operations](#) on page 17

[Backing up resources using PowerShell cmdlets](#) on page 28

Related information

[SnapCenter Software 4.1 Windows Cmdlet Reference Guide](#)

Backing up resource groups

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

Before you begin

- You must have created a resource group with a policy attached.
- If you are backing up a resource that has a SnapMirror relationship to secondary storage, you must have SnapCenter admin privileges and the scadmin role must include the “snapmirror all” privilege.



About this task

Note: 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.

Attention: 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**.

Note: 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.
 - b. Click **Backup**.

5. Monitor the operation progress by clicking **Monitor > Jobs**.

Related tasks

[Creating resource groups for Windows file systems](#) on page 13

[Monitoring backup operations](#) on page 17

[Backing up resources using PowerShell cmdlets](#) on page 28

Related information







[SnapCenter Software 4.1 Windows Cmdlet Reference Guide](#)

Monitoring backup operations


You can monitor the progress of different backup operations by using the SnapCenter Jobs 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 state of the operation:

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

Steps

1. In the left navigation pane, click **Monitor**.
2. In the **Monitor** page, click **Jobs**.
3. Optional: 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.

Note: 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.

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

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


Monitoring 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.

About this task

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

Steps

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

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

Canceling the backup operations

You can cancel backup operations that are queued.

Before you begin

- You must be logged in as the SnapCenter Admin or job owner to cancel operations.


About this task

- You can cancel a backup operation from either the Monitor page or the Activity pane.
- 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.

Step

1. Perform one of the following actions:

From the...	Action
Monitor page	<ol style="list-style-type: none">a. In the left navigation pane, click Monitor > Jobs.b. Select the operation, and click Cancel Job.

From the...	Action
Activity pane	<ul style="list-style-type: none">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.

Result

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

Related information

[*SnapCenter Software 4.1 Windows Cmdlet Reference Guide*](#)

Restoring Windows file system backups

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

Before you begin

- You must have backed up the file system.
- If a scheduled operation, such as a backup operation, is currently in progress for a file system, then that operation must be cancelled before you can start a restore operation.

About this task

- You can only restore a file system backup to the original location, not to an alternate path. You cannot restore a single file from a backup because the restored file system overwrites any data on the original location of the file system. To restore a single file from a file system backup, you must clone the backup and access the file in the clone.
- You cannot restore a system or boot volume.
- SnapCenter can restore file systems in a Windows cluster without taking the cluster group offline.

Most of the fields on the Restore wizard pages are self-explanatory. The following information describes fields for which you might need guidance.

Steps

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

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

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

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

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

After you finish

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

[Protecting Microsoft SQL Server databases](#)

[Protecting Microsoft Exchange Server databases](#)

Related tasks

[Monitoring restore operations](#) on page 21

[Restoring and recovering resources using PowerShell cmdlets](#) on page 30

Related information

[SnapCenter Software 4.1 Windows Cmdlet Reference Guide](#)







Monitoring restore operations

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


About this task

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

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

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

Steps

1. In the left navigation pane, click **Monitor**.
2. In the **Monitor** page, click **Jobs**.
3. Optional: In the **Jobs** page, perform the following steps:
 - a. Click  to filter the list so that only restore operations are listed.

- b. Optional: Specify the start and end dates.
- c. From the **Type** drop-down list, select **Restore**.
- d. From the **Status** drop-down list, select the restore status.
- e. Click **Apply** to view the operations that are completed successfully.
4. Select the restore job, and then click **Details** to view the job details.
5. Optional: In the **Job Details** page, click **View logs**.

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

Canceling restore operations

You can cancel restore jobs that are queued.

Before you begin


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

About this task

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

Step

1. Perform one of the following actions:

From the...	Action
Monitor page	<ol style="list-style-type: none"> a. In the left navigation pane, click Monitor > Jobs. b. Select the job and click Cancel Job.
Activity pane	<ol style="list-style-type: none"> a. After initiating the restore operation, click  on the Activity pane to view the five most recent operations. b. Select the operation. c. In the Job Details page, click Cancel Job.

Related information

[SnapCenter Software 4.1 Windows Cmdlet Reference Guide](#)

Cloning from a Windows file system backup

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

Before you begin

- You must have prepared for data protection by completing tasks such as adding hosts, identifying resources, and creating storage virtual machine (SVM) connections.
- You must have a backup of the file system.

About this task

- You cannot clone a resource group. You can only clone individual file system backups.
- If a backup resides on a virtual machine with a VMDK disk, SnapCenter cannot clone the backup to a physical server.
- If you clone a Windows cluster (for example, a shared LUN or a cluster shared volume (CSV) LUN), the clone is stored as a dedicated LUN on the host that you specify.
- For a cloning operation, the root directory of the volume mount point cannot be a shared directory.
- You cannot create a clone on a node that is not the home node for the aggregate.
- You cannot schedule recurring clone (clone lifecycle) operations for Windows file systems; you can only clone a backup on demand.
- If you move a LUN that contains a clone to a new volume, SnapCenter can no longer support the clone. For example, you cannot use SnapCenter to delete that clone.

Most of the fields on the Clone wizard pages are self-explanatory. The following information describes some of the fields for which you might require guidance.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the **Resources** page, select **File Systems** from the list.
3. Select the host.
The topology view is automatically displayed if the resource is protected.
4. From the resources list, select the backup that you want to clone, and then click the clone icon.
5. In the **Options** page, do the following:

For this field...	Do this...
Clone server	Choose the host on which the clone should be created.

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

6. In the **Script** page, specify any prescripts or postscripts you want to execute.
7. Review the summary, and then click **Finish**.
8. Monitor the operation progress by clicking **Monitor > Jobs**.

Related tasks

[Monitoring clone operations in SnapCenter](#) on page 24

[Cloning backups using PowerShell cmdlets](#) on page 32

Related information







[SnapCenter Software 4.1 Windows Cmdlet Reference Guide](#)

Monitoring clone operations in SnapCenter

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


About this task

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

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

Steps

1. In the left navigation pane, click **Monitor**.
2. In the **Monitor** page, click **Jobs**.
3. In the **Jobs** page, perform the following steps:

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

Canceling clone operations

You can cancel clone operations that are queued.

Before you begin


- You must be logged in as the SnapCenter Admin or job owner to cancel operations.

About this task

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

Step

- Perform one of the following actions:

From the...	Action
Monitor page	<ol style="list-style-type: none"> a. In the left navigation pane, click Monitor > Jobs. b. Select the operation, and click Cancel Job.
Activity pane	<ol style="list-style-type: none"> a. After initiating the clone operation, click  on the Activity pane to view the five most recent operations. b. Select the operation. c. In the Job Details page, click Cancel Job.

Related information

[SnapCenter Software 4.1 Windows Cmdlet Reference Guide](#)

Splitting a clone

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

About this task

- You cannot perform the clone split operation on an intermediate clone.
For example, after you create clone1 from a database backup, you can create a backup of clone1, and then clone this backup (clone2). After you create clone2, clone1 is an intermediate clone, and you cannot perform the clone split operation on clone1. However, you can perform the clone split operation on clone2.
After splitting clone2, you can perform the clone split operation on clone1 because clone1 is no longer the intermediate clone.


- When you split a clone, the backup copies and clone jobs of the clone are deleted.
- For information about clone split operation limitations, see the *Logical Storage Management Guide*.

[ONTAP 9 Logical Storage Management Guide](#)

Steps

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

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

- Select the cloned resource (for example, the database or LUN), and then click .
- Review the estimated size of the clone that is to be split and the required space available on the aggregate, and then click **Start**.
- Monitor the operation progress by clicking **Monitor > Jobs**.

After you finish

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

For example:

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

Backing up, restoring, cloning, and removing backups using PowerShell cmdlets

The SnapCenter Plug-in for Microsoft SQL Server and the SnapCenter Plug-in for Microsoft Windows include PowerShell cmdlets for scripting of backup, restore, and clone operations.

The following are common tasks you might perform using PowerShell cmdlets:

- Preparing the PowerShell environment
- Creating a storage system connection and a Run As account
- Backing up SQL Server databases or Windows file systems
- Restoring and recovering SQL Server databases
- Restoring Windows file systems
- Cloning backups for SQL Server databases or Windows file systems
- Removing backups
- Cleaning up secondary backup counts

For detailed information about PowerShell cmdlets, use the SnapCenter cmdlet help or see the cmdlet reference information.

[*SnapCenter Software 4.1 Windows Cmdlet Reference Guide*](#)

Creating a storage system connection and a Run As account using PowerShell cmdlets

You must create a storage virtual machine (SVM) connection and a Run As account before using PowerShell cmdlets to back up, restore, or clone SAP HANA databases, custom plug-in resources, SQL Server databases, or Windows file systems.

Before you begin

- PowerShell cmdlets must be operative.
You must have prepared the PowerShell environment to execute the PowerShell cmdlets.
- You must have the appropriate permissions.
You must have permissions in the Infrastructure Admin role to create storage connections.
- Plug-in installations must not be 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 might indicate “Not available for backup” or “Not on NetApp storage” in SnapCenter.
- Storage system names must be unique.
SnapCenter does not support multiple storage systems with the same name on different clusters. Each storage system that is supported by SnapCenter must have a unique name and a unique data LIF IP address.

About this task

For information about PowerShell cmdlets, use the SnapCenter cmdlet help or see the cmdlet reference information.

*SnapCenter Software 4.1 Windows Cmdlet Reference Guide***Steps**

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

Example

This example opens a PowerShell session:

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

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

Example

This example creates a new storage system connection:

```
PS C:\> Add-SmStorageConnection -SVM test_vsl -Protocol Https  
-Timeout 60
```

3. Create a new Run As account by using the `Add-SmRunAs` cmdlet.

Example

This example creates a new Run As account named FinanceAdmin with Windows credentials:

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

Backing up resources using PowerShell cmdlets

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.

Before you begin

- You must have prepared the PowerShell environment to execute the PowerShell cmdlets.
- You must have added the storage system connection and created a Run As account.
- You must have added hosts and discovered resources.

About this task

For information about PowerShell cmdlets, use the SnapCenter cmdlet help or see the cmdlet reference information.

*SnapCenter Software 4.1 Windows Cmdlet Reference Guide***Steps**

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

Example

```
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.

Example

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
```

Example

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.

Example

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
```

Example

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.

Example

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"
```

Example

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 Snapshot copy job by using the `New-SmBackup` cmdlet.

Example

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

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

Example

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?
```

Restoring and recovering resources using PowerShell cmdlets

Restoring and recovering a SQL Server database or Windows file system includes initiating a connection session with the SnapCenter Server, listing the backups and retrieving backup information, and restoring a backup.

Before you begin

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

About this task

For information about PowerShell cmdlets, use the SnapCenter cmdlet help or see the cmdlet reference information.

[SnapCenter Software 4.1 Windows Cmdlet Reference Guide](#)

Steps

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

Example

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

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

Example

This example displays information about all available backups:

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

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

Example

This example displays detailed information about the backup
Secondary_SCSPR0019366001_01-15-2015_06.49.08:

```
PS C:\> Get-SmBackupReport
-BackupName Secondary_SCSPR0019366001_01-15-2015_06.49.08

BackedUpObjects : {TestDB1, TestDB2, TestDB3, TestDB4...}
FailedObjects   : {}
BackupType      : Full Backup
IsScheduled     : False
SmBackupId      : 52
SmJobId         : 585
StartDateTime   : 1/15/2015 6:49:07 AM
EndDateTime     : 1/15/2015 6:49:21 AM
Duration        : 00:00:13.8370000
CreatedDateTime : 1/15/2015 6:49:18 AM
Status          : Completed
ProtectionGroupName : Secondary
SmProtectionGroupId : 5
PolicyName      : Vault
SmPolicyId      : 18
BackupName      : Secondary_SCSPR0019366001_01-15-2015_06.49.08
VerificationStatus : NotVerified
```

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

Example

```
C:\PS>PS C:\> Restore-SmBackup -PluginCode SCSQL
-AppObjectId 'vise-f6\PayrollDatabase'
-BackupName 'NetApp_PayrollDataset_Backup Policy_
             vise-f6_NetApp_08-07-2015_08.48.59.6962'
-RestoreWhenOnline

Name           : Restore 'vise-f6\PayrollDatabase'
Id             : 199
StartTime      : 8/7/2015 9:21:36 AM
EndTime       : 
IsCancellable  : False
IsRestartable  : False
IsCompleted    : False
IsVisible      : False
IsScheduled    : False
PercentageCompleted : 0
Description    : 
Status        : Queued
Owner         : 
Error         : 
Priority      : None
Tasks        : {}
ParentJobID   : 0
EventId       : 0
```

Example

```
Restore-SmBackup -PluginCode SCSQL -AppObjectId 'scspr0270378001\abc'
-BackupName 'scspr0270378001_abc_scspr0270378001_07-25-2017_04.51.10.5795' -
AlternatePath @{Source='D:\data\abc.mdf';Destination='D:\data\bharathaewf123.mdf'},@{Source='D:\log\bharath_log.ldf';Destination='D:\log\bharathaef_log123.ldf'} -
SQLInstanceName 'scspr0273089004' -DatabaseName 'abc123adwqa1231' -
ExistingFiles
```

Cloning backups using PowerShell cmdlets

The clone workflow includes planning, performing the clone operation, and monitoring the operation.

Before you begin

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

About this task

For information about PowerShell cmdlets, use the SnapCenter cmdlet help or see the cmdlet reference information.

[SnapCenter Software 4.1 Windows Cmdlet Reference Guide](#)

Steps

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

Example

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

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

Example

This example displays information about all available backups:

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

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

Example

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


```

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

Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMapping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassRunAs : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13

```

```

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

```

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

Example

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

```

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

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

```

Example

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

```

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

```

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

Example

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

```

PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed

```

```

ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}

```

Removing 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.

Before you begin

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

About this task

For information about PowerShell cmdlets, use the `SnapCenter` cmdlet help or see the cmdlet reference information.

Steps

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

Example

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

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

Example

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"):

```

Related information

[SnapCenter Software 4.1 Windows Cmdlet Reference Guide](#)

Cleaning 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 use this cmdlet when the total Snapshot copies displayed in the Manage Copies topology do not match the secondary storage Snapshot copy retention setting.

Before you begin

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

About this task

For information about PowerShell cmdlets, use the `SnapCenter` cmdlet help or see the cmdlet reference information.

Steps

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

Example

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

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

Example

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"):
```

Related information

[SnapCenter Software 4.1 Windows Cmdlet Reference Guide](#)

Troubleshooting data protection operations

If you encounter unexpected behavior while performing data protection operations, you can use the log files to identify the cause and resolve the problem.

You can download the log files from the SnapCenter user interface by clicking **Monitor > Logs > Download**.

Back up operation on some hosts might trigger late

Description

If a resource group has multiple databases from different hosts, the backup operation on some hosts might trigger late because of network issues.

Error message

Scheduled job is not triggered on host(s) <HOST_NAMES>

Corrective action

You should configure the key `MaxRetryForUninitializedHosts` value in `web.config` by using the `Set-SmConfigSettings PS cmdlet cmdlet`. In the following example, the default value of the retry count is 10:

```
Set-SmConfigSettings -Server -configSettings
@{"MaxRetryForUninitializedHosts"=10}
```

SnapCenter Plug-in Package for Microsoft Windows or SnapCenter Plug-in for Microsoft SQL Server upgrade might fail on hosts with SQL databases on VMDK

Description

When upgrading SnapCenter Plug-in for Microsoft Windows or SnapCenter Plug-in for Microsoft SQL Server on hosts with SQL databases on VMDK, the upgrade might fail.

Error message

The installation log displays the error `Engine: error 80070002 while running parcel operations .`

Workaround

Delete the following directories on the plug-in host:

- `C:\Windows\SnapCenter plugin`
- All files and directories in `C:\Users\Administrator.domain_name\AppData\Local\Downloaded Installations`

If the upgrade does not succeed after you delete the specified files and directories, you might need to reboot the SQL server host, and then delete the files and directories.

Storage layout could not be determined

Description

If the OTAP CIFS Server name is not resolvable, then an APPLY PSL job fails.

Error message

Storage layout could not be determined.

Corrective action

Make sure the CIFS Server name is resolvable.

HTTP error 503. The service is unavailable.

Description

Launching SnapCenter from a browser or opening a connection from the CLI might fail after installation if Windows Process Activation Service (WAS) is not enabled.

Corrective action

Verify in Windows Server Manager that Windows Process Activation Service is enabled.

Unable to display SnapCenter web login page on local host

Description

When using Internet Explorer with Protected Mode enabled, the SnapCenter login page does not display when logging in to the local SnapCenter host as a user from another trusted domain.

Corrective action

Disable Protected Mode in Internet Explorer.

SnapCenter plug-in loader fails with an error

Description

SnapCenter plug-in loader fails with an error.

Error message

Error retrieving current directory.

Corrective action

- You must ensure that you have not deleted any directory where the plug-in is operating on.
- You must increase the memory space allotted to the Java Virtual Machine.

SnapCenter plug-in loader does not start automatically when the host is restarted

Description

When the host is restarted, the SnapCenter plug-in loader (SPL) does not start automatically if there is no symbolic link in `/user/bin/Java`, or if Java is mounted from an external entity.

Error message

```
ERROR: JAVA_HOME is set to an invalid directory.
```

```
Failed to start SnapCenter Plugin Loader.
```

Corrective action

If the host is running on...	Then...
<code>init.d</code>	<ol style="list-style-type: none"> 1. Create the <code>spl</code> configuration file at <code>/etc/default/</code>. 2. Add export <code>JAVA_HOME=path_where_java_is_mounted</code> to the <code>spl</code> configuration file. 3. Add <code>[-f /etc/default/spl]</code> <code>&& . /etc/default/spl</code> to the beginning of the SPL init script located at <code>/etc/init.d/</code>.
<code>system.d</code>	<ol style="list-style-type: none"> 1. Create the <code>spl.conf</code> configuration file at <code>/etc/systemd/system/spl.service.d/</code>. 2. Add the following lines to the <code>spl.conf</code> configuration file: <ul style="list-style-type: none"> • <code>Environment=JAVA_HOME=path_where_java_is_mounted</code> • <code>RestartSec=30</code> • <code>StartLimitInterval=200</code> • <code>StartLimitBurst=5</code> 3. After updating <code>spl.conf</code>, reload <code>systemctl</code> by running the <code>systemctl daemon-reload</code> command.

Unable to access cluster IP address from outside network

Description

There is no response when you try to access the cluster IP address from outside the network.

Corrective action

Verify that you can use **ping** to access the dedicated IP addresses of the cluster host from a computer outside the router. If this test fails and you are using multiple network adapters, the issue is not related to Network Load Balancing (NLB). If you are using a single network adapter for the dedicated and cluster IP addresses, consider the following scenarios:

Scenario	Solution
If you are using multicast support, you might find that your router has difficulty resolving the primary IP address into a multicast media access control (MAC) address by using the Address Resolution Protocol (ARP)	Verify that you can use ping to access the cluster from a client on the cluster's subnet and the cluster host's dedicated IP address from a computer outside the router. If these tests work properly, the router is probably at fault. You should be able to add a static ARP entry to the router to circumvent the issue.
When using NLB in multicast or unicast mode, routers need to accept proxy ARP responses (IP-to-network address mappings that are received with a different network source address in the ethernet frame).	You must ensure that that your router has proxy ARP support turned on. You can also set a static ARP entry to keep proxy ARP support disabled in the router.
Internet control message protocol (ICMP) to the cluster is blocked by a router or firewall.	Allow ICMP traffic through the router or firewall. However, allowing ICMP traffic through router or firewall might expose your system to additional security risk.

Backup fails with error: Storage system(s) may need to be added, also ensure that the associated host is in a connected state

Description

A backup failed because the preferred IP address that was configured for the SVM went down. When the preferred IP comes up again, the SnapCenter cache is not automatically refreshed. Therefore, SnapCenter could not find the Preferred IP when attempting to perform the backup.

Corrective action

Refresh the SnapCenter cache for the SVM:

1. In the left navigation pane of the SnapCenter GUI, click **Storage Systems**.
2. In the Storage Systems page, select the storage system used by the backup, and then click **Modify**.

3. Make sure that the **Preferred IP** check box is selected and that the IP is correct.
4. Reenter the storage system password, and then click **OK**.
This action refreshes the SnapCenter cache and updates the storage system configuration.

Unable to find Snapshot copy after successfully creating the backup

Description

Backup operations with an update to SnapVault or SnapMirror might fail.

Depending on the rate of change of data between Snapshot copies, the time taken to update the Snapshot copy to secondary varies. If the delta between Snapshot copies is very high, it is recommended to change `SnapshotCheckRetry` and `SnapshotCheckTimeout` values.

Error message

Snapshot copy could not be found on the destination storage system.

Corrective action

You must include the following parameters and specify the value in the `appsetting` section of the `SMCoreServiceHost.exe.Config` file located under `SmCore` in the SnapCenter Server.

- `<add key="SnapshotCheckRetry" value=retry_value/>`
The `retry_value` assigned to `SnapshotCheckRetry` defines the maximum number of retries that are performed to discover the Snapshot copies on the secondary location.
- `<add key="SnapshotCheckTimeout" value=timeout_value/>`
The `timeout_value` (milliseconds) assigned to `SnapshotCheckTimeout` defines the wait or sleep period for every retry.

Backup operation fails if Snapshot copies on the secondary storage reaches maximum limit

Description

When the number of Snapshot copies on the secondary storage (mirror-vault) reaches the maximum limit, the activity to register backup and apply retention in the backup operation fails.

Error message

This Snapshot copy is currently used as a reference Snapshot copy by one or more SnapMirror relationships. Deleting the Snapshot copy can cause future SnapMirror operations to fail.

Corrective action

You should configure SnapMirror retention policy for the secondary storage to avoid reaching the maximum limit of Snapshot copies on the secondary storage.

Scheduled backups fail due to task limit

Description

When SnapCenter is running scheduled jobs, the Windows scheduler returns an error and some scheduled data protection operations fail. This error occurs when the number of tasks reaches the maximum configured for the machine.

Error message

User Action: Reduce the number of tasks running in the specified user context.

Corrective action

1. See the Microsoft support document *Error 0x80041323 when running high number of Scheduled tasks* <https://support.microsoft.com/en-in/kb/2696472>.
This document contains instructions on how to change the values configured for the registry keys.
2. Set the values in the following registry keys to 1000.
 - TasksInMemoryQueue
 - TasksPerHighestPrivEngine
 - TasksPerLeastPrivEngine
3. Reboot the machine.

Clone operation will fail due to inaccessible virtual device

Description

One of the possible reasons a clone operation can fail is because a virtual device that is listed in vCenter is inaccessible because of a permanent device loss.

For example, if the LUN ID of a newly created LUN for a clone operation matches a LUN ID that is being used by an inaccessible LUN in vCenter, the clone operation fails.

Error message

Failed to clone resources, error is Failed to Mount/Attach Disk

Corrective action

1. Using the vCenter interface, remove the inaccessible LUN.
Refer to the VMware documentation for information.
2. Using the SnapCenter interface, run the clone operation again.

Clone split estimation fails when the aggregate does not have space

Description

If the aggregate has no space, clone split estimation fails.

Corrective action

Increase the space on the aggregate.

Clone split start operation fails

Description

The clone split start operation fails when one of the following conditions are met:

- The volume or aggregate is offline.
- A clone split operation, backup operation, or restore operation is in progress on the clone resource.
- A clone split operation is in progress on an intermediate clone.

Corrective action

- If the volume or aggregate is offline, check the status of the volume or aggregate on the storage system and bring it back online.
- If a clone split operation, backup operation, or restore operation is in progress on the clone resource, restart the clone split operation after the clone split operation, backup operation, or restore operation is complete.
- If a clone split operation is in progress on an intermediate clone, split the child clones, and then restart the clone split start operation on this clone.

Clone split operation stops responding

Description

The clone split operation stops responding if the SMCore service restarts.

Corrective action

Use the `Stop-SmJob` cmdlet to stop the clone split operation, and then perform the clone split operation again.

Databases on which the clone split operation was performed are listed as clones

Description

During the clone split operation, if the SMCore service restarts, the status of the operation will not be sent to the server. Therefore, the databases on which the clone split operation was performed are listed as clones in the Resources page.

Corrective action

Run the split clone cmdlet again to clean the clone metadata in SnapCenter repository.

Managing resource groups

You can create, modify, and delete resource groups. You can also perform backup and verification operations on resource groups.

About this task

You can perform the following tasks related to resource groups:

- Create a resource group.
- Modify a resource group by selecting the resource group and clicking **Modify Resource Group** to edit the information you provided while creating the resource group.

Note: You can change the schedule while modifying the resource group. However, to change the schedule type you must modify the policy.

Note: If you remove resources from a resource group, the backup retention settings defined in the policies currently attached to the resource group will continue to be applied to the removed resources.

- Create a backup of a resource group.
- Create a clone of a backup.
You can clone from the existing backups of SQL, Oracle, Windows file systems, custom applications, and SAP HANA database resources or resource groups.
- Create a clone of a resource group.
This operation is supported only for SQL resource groups (which contains only databases). You can configure a schedule for cloning a resource group (clone lifecycle).
- Prevent scheduled operations on resource groups from starting.
- Delete a resource group.

Related tasks

[Creating resource groups for Windows file systems](#) on page 13

[Backing up resource groups](#) on page 16

Stopping and resuming operations on resource groups

You can temporarily disable scheduled operations from starting on a resource group. Later when you want, you can enable those operations.

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.
3. Select the resource group and click **Maintenance**.
4. Click **OK**.

After you finish

If you want to resume operations on the resource group that you had put on maintenance mode, select the resource group and click **Production**.

Deleting resource groups

You can delete a resource group if you no longer need to protect the resources in the resource group. You must ensure that resource groups are deleted before you remove plug-ins from SnapCenter.

Before you begin

If you are managing SQL or Windows file system resources, you must have manually deleted all clones created for any of the resources in the resource group.

About this task

You can optionally force the deletion of all backups, metadata, policies, and Snapshot copies associated with the resource group.

Note: In a SnapVault relationship, the last Snapshot copy cannot be deleted; therefore, the resource group cannot be deleted. Before deleting a resource group that is part of a SnapVault relationship, you must remove the SnapVault relationship and then delete the last Snapshot copy.

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.
3. Select the resource group, and then click **Delete**.
4. Optional: Select the **Delete backups and detach policies associated with this Resource Group** check box to remove all backups, metadata, policies, and Snapshot copies associated with the resource group.
5. Click **OK**.

Managing policies

You can create, copy, modify, view, and delete backup policies.

About this task

You can perform the following tasks related to policies:

- Create a policy.
- Modify a policy.

Note: You can change the schedule type for a policy only after you detach the policy. To change the schedule you must modify the resource group.
- Copy a policy by accepting the default name or typing a new name.
- Detach a policy from a resource group.
- Delete a policy.

Related tasks

[Creating backup policies for Windows file systems](#) on page 11

Detaching policies

You can detach policies from a resource or resource group any time that you no longer want those policies to govern data protection for the resources. You must detach a policy before you can delete it or before you modify the schedule type.

About this task

Attention: You cannot detach a policy from a resource or resource group if it is the only policy attached.

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.
3. Select the resource group, and then click **Modify Resource Group**.
4. In the **Policies** page of the **Modify Resource Group** wizard, from the drop-down list, clear the check mark next to the policies you want to detach.

Note: You cannot detach the last remaining policy from an individual resource because every resource must have at least one policy attached. Therefore, if you want to delete or modify the only policy attached to a resource, you must perform the following:

- a. Attach a second placeholder policy.
 - b. Detach the original policy from the resource.
5. Make any additional modifications to the resource group in the rest of the wizard, and then click **Finish**.

Modifying policies

You can modify the replication options, Snapshot copy retention settings, error retry count, or scripts information while a policy is attached to a resource or resource group. You can modify the schedule type (frequency) only after you detach a policy.

About this task

Modifying the schedule type in a policy requires additional steps because the SnapCenter Server registers the schedule type only at the time the policy is attached to a resource or resource group.

If you want to...	Then...
Add an additional schedule type	<p>Create a new policy and attach it to the necessary resources or resource groups.</p> <p>For example, if a resource group policy specifies only hourly backups and you want to add daily backups also, you can create a policy with a daily schedule type and add it to the resource group. The resource group would then have two policies: hourly and daily.</p>
Remove or change a schedule type	<ol style="list-style-type: none"> 1. Detach the policy from every resource and resource group that uses that policy. 2. Modify the schedule type. 3. Attach the policy again to all the resources and resource groups. <p>For example, if a policy specifies hourly backups and you want to change that to daily backups, you must detach the policy first.</p> <p>Note: You cannot detach the last remaining policy from a individual resource because every resource must have at least one policy attached. Therefore, if you want to modify the schedule type of the only policy attached to a resource, you must perform the following:</p> <ol style="list-style-type: none"> 1. Attach a second placeholder policy. 2. Detach the original policy from every resource and resource group that uses that policy. 3. Modify the schedule type. 4. Attach the modified policy again to all the resources and resource groups. 5. Detach the placeholder policy.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Policies**.
3. Select the policy, and then click **Modify**.

4. Modify the information, and then click **Finish**.

Deleting policies

If you no longer require policies, you might want to delete them.

Before you begin

You must have detached the policy from resource groups if the policy is associated with any resource group.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Policies**.
3. Select the policy, and then click **Delete**.
4. Click **Yes**.

Managing backups

You can rename and delete backups. You can also delete multiple backups simultaneously.

Related tasks

[Backing up a single resource on demand](#) on page 14

[Backing up resource groups](#) on page 16

Renaming backups

You can rename backups if you want to provide a better name to improve searchability.

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 or resource group from the list.

The resource or resource group topology page is displayed. If the resource or resource group is not configured for data protection, the Protect wizard is displayed instead of the topology page.

4. From the **Manage Copies** view, select **Backups** from the primary storage systems.

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

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.

5. Select the backup, and then click .
6. In the **Rename backup as** field, enter a new name and click **OK**.

Deleting backups

You can delete backups if you no longer require the backup for other data protection operations.

Before you begin

You must have deleted the associated clones before deleting a backup.

If a backup is associated with a cloned resource, you cannot delete the 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 or resource group from the list.

The resource or resource group topology page is displayed.

4. From the **Manage Copies** view, select **Backups** from the primary storage systems.

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

5. Select the backup, and then click .
6. Click **OK**.

Note: If you have some stale database backups in SnapCenter which do not have corresponding backups on the storage system, you must use `remove-smbbackup` command to clean up these stale backup entries. If the stale backups were cataloged, they will be uncataloged from the recovery catalog database.

Managing clones

You can view and delete clones.

Related tasks

[Cloning from a Windows file system backup](#) on page 23

Deleting clones

You can delete clones if you find them no longer necessary.


About this task

A clone that has been cloned again cannot be deleted. For example, if the production database *db1* is cloned to *db1_clone1* and subsequently cloned to *db1_clone2*, and you decide that you want to delete *db1_clone1*, you must first delete *db1_clone2*, and then delete *db1_clone1*.

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 or resource group from the list.

The resource or the resource group topology page is displayed.

4. From the **Manage Copies** view, select **Clones** either from the primary or secondary (mirrored or replicated) storage systems.
5. Select the clone, and then click .
6. Click **OK**.

Copyright

Copyright © 2019 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, 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).

Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277