Back up Unix file systems

SnapCenter software

NetApp
January 09, 2026

Table of Contents

Back up Unix file systems

Discover the UNIX file systems available for backup

After installing the plug-in, all the file systems on that host are automatically discovered and displayed in the Resources page. You can add these file systems to resource groups to perform data protection operations.

Before you begin

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

- If the file systems reside on a Virtual Machine Disk (VMDK) or raw device mapping (RDM), you must deploy the SnapCenter Plug-in for VMware vSphere and register the plug-in with SnapCenter.

  For more information, see Deploy 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 **Path** from the View list.

3. Click **Refresh Resources**.

   The file systems are displayed along with information such as type, host name, associated resource groups and policies, and status.

Create backup policies for Unix file systems

Before you use SnapCenter to back up Unix file systems, you must create a backup policy for the resource or the resource group that you want to back up. A backup policy is a set of rules that governs how you manage, schedule, and retain backups. You can also specify the replication, script, and backup type settings. Creating a policy saves time when you want to reuse the policy on another resource or resource group.

Before you begin

- You must have prepared for data protection by completing tasks such as installing SnapCenter, adding hosts, discovering the file systems, and creating storage system connections.

- If you are replicating Snapshots to a mirror or vault secondary storage, the SnapCenter administrator must have assigned the SVMs to you for both the source and destination volumes.

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

About this task

- SnapLock

  ◦ If 'Retain the backup copies for a specific number of days' option is selected, then the SnapLock retention period must be lesser than or equal to the mentioned retention days.

    Specifying a Snapshot locking period prevents deletion of the Snapshots until the retention period

expires. This could lead to retaining a larger number of Snapshots than the count specified in the policy.

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

Steps

1. In the left navigation pane, click **Settings**.

2. In the Settings page, click **Policies**.

3. Select **Unix File Systems** from the drop-down list.

4. Click **New**.

5. In the Name page, enter the policy name and details.

6. In the Backup and Replication page, perform the following actions:

   a. Specify the backup settings.

   b. Specify the schedule frequency by selecting **On demand**, **Hourly**, **Daily**, **Weekly**, or **Monthly**.

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

For this field…	Do this…
Update SnapMirror after creating a local Snapshot copy	Select this field to create mirror copies of the backup sets on another volume (SnapMirror replication). This option should be enabled for SnapMirror active sync.
Update SnapVault after creating a local Snapshot copy	Select this option to perform disk-to-disk backup replication (SnapVault backups).
Error retry count	Enter the maximum number of replication attempts that can be allowed before the operation stops.

7. In the Retention page, specify the retention settings for the backup type and the schedule type selected in the Backup and Replication page:

If you want to…	Then…

Keep a certain number of Snapshots	Select **Copies to keep**, and then specify the number of Snapshots that you want to keep.
	If the number of Snapshots exceeds the specified number, the Snapshots are deleted with the oldest copies deleted first.
	(i) The maximum retention value is 1018. Backups will fail if retention is set to a value higher than what the underlying ONTAP version supports.
	(i) You must set the retention count to 2 or higher if you plan to enable SnapVault replication. If you set the retention count to 1, the retention operation might fail because the first Snapshot is the reference Snapshot for the SnapVault relationship until a newer Snapshot is replicated to the target.
Keep the Snapshots for a certain number of days	Select **Retain copies for**, and then specify the number of days for which you want to keep the Snapshots before deleting them.
Snapshot copy locking period	Select **Snapshot copy locking period** and specify the duration in days, months, or years. Snaplock retention period should be less than 100 years.

8. Select policy label.

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

9. In the Script page, enter the path and the arguments of the prescript or postscript that you want to run before or after the backup operation, respectively.

> (i) You should check if the commands exist in the command list available on the plug-in host from the _ /opt/NetApp/snapcenter/scc/etc/allowed_commands.config_ path.

You can also specify the script timeout value. The default value is 60 seconds.

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

# Create resource groups and attach policies for Unix file systems

A resource group is a container where you add resources that you want to back up and protect. A resource group allows you to back up all the data that is associated with the file systems.

About this task

- A database with files in ASM disk groups must be in "MOUNT" or "OPEN" state to verify its backups using the Oracle DBVERIFY utility.

  Attach one or more policies to the resource group to define the type of data protection job you want to perform.

  The following image illustrates the relationship between resources, resource groups, and policies for databases:
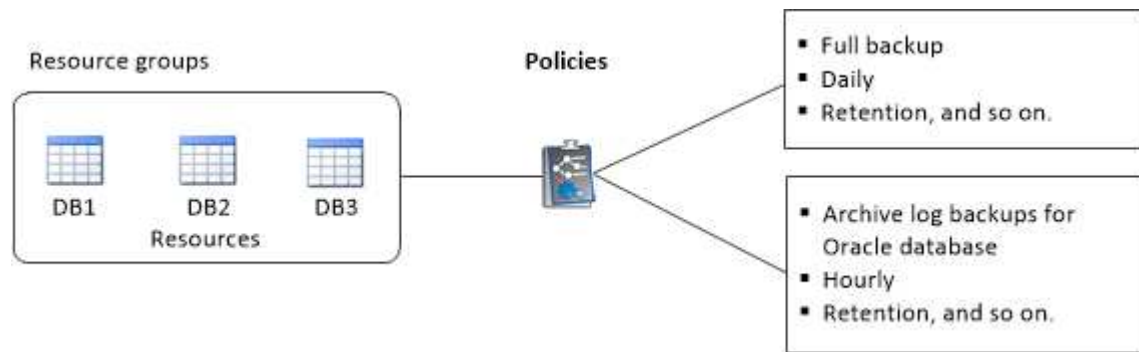
- For SnapLock enabled policies, for ONTAP 9.12.1 and below version, if you specify a Snapshot locking period, the clones created from the tamper proof Snapshots as part of restore will inherit the SnapLock expiry time. Storage admin should manually cleanup the clones post the SnapLock expiry time.

- Adding new file systems without SnapMirror active sync to an existing resource group which contains resources with SnapMirror active sync, is not supported.

- Adding new file systems to an existing resource group in failover mode of SnapMirror active sync is not supported. You can add resources to the resource group only in regular or fail-back state.

Steps

1. In the left navigation pane, select **Resources**, and the appropriate plug-in from the list.

2. In the Resources page, click **New Resource Group**.

3. In the Name page, perform the following actions:

   a. Enter a name for the resource group in the Name field.

   > (i) The resource group name should not exceed 250 characters.

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

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

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

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

4. In the Resources page, select an Unix file systems host name from the **Host** drop-down list.

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

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

6. In the Application Settings page, perform the following:

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

   ◦ Select one of the backup consistency options:

      ▪ Select **File System Consistent** if you want to ensure that file systems cached data is flushed before creating the backup and no input or output operations are allowed on filesystem while creating the backup.

         > (i) For File System Consistent, Consistency group snapshots will be taken for LUNs involved in Volume group.

      ▪ Select **Crash Consistent** if you want to ensure that file systems cached data is flushed before creating the backup.

         > (i) If you have added different file systems in the resource group, then all volumes from different file systems in the resource group will be put in a Consistency group.

7. In the Policies page, perform the following steps:

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

      > (i) You can also create a policy by clicking [+] .

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

   b. Click [+] in the Configure Schedules column for the policy for which you want to configure a schedule.

   c. In the Add schedules for policy *policy_name* window, configure the schedule, and then click **OK**.

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

      The configured schedules are listed in the Applied Schedules column.

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

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

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

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

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

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

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

Before you begin

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

- You should ensure that you do not have a database with both ONTAP 9.x resources and ASA r2 resources.

About this task

- The secondary protection is available only if the logged-in user is assigned to the role that has the **SecondaryProtection** capability enabled.

- If you enabled secondary protection, the resource group is put into maintenance mode while creating the primary and secondary consistency groups. After the primary and secondary consistency groups are created, the resource group is put out of maintenance mode.

- SnapCenter does not support secondary protection for a clone resource.

Steps

1. In the left navigation pane, select **Resources**, and the appropriate plug-in from the list.

2. In the Resources page, click **New Resource Group**.

3. In the Name page, perform the following actions:

   a. Enter a name for the resource group in the Name field.

   > ⓘ The resource group name should not exceed 250 characters.

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

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

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

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

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

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

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

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

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

6. In the Application Settings page, select the backup option.

7. In the Policies page, perform the following steps:

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

   > ⓘ You can also create a policy by clicking ➕ .

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

   b. Click ➕ in the Configure Schedules column for the policy for which you want to configure a schedule.

   c. In the Add schedules for policy *policy_name* window, configure the schedule, and then click **OK**.

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

   The configured schedules are listed in the Applied Schedules column.

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

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

   a. Select the type of the replication policy.

   > ⓘ Synchronous replication policy is not supported.

   b. Specify the consistency group suffix that you want to use.

   c. From the Destination Cluster and Destination SVM drop-downs select the peered cluster and SVM that you want to use.

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

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

1. On the Verification page, perform the following steps:

a. Click **Load locators** to load the SnapMirror or SnapVault volumes to perform verification on secondary storage.

b. Click ![+] in the Configure Schedules column to configure the verification schedule for all the schedule types of the policy.

c. In the Add Verification Schedules policy_name dialog box, perform the following actions:

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

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

e. Click **OK**.

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

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

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

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

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

Back up Unix file systems

If a resource is not part of any resource group, you can back up the resource from the Resources page.

Steps

1. In the left navigation pane, select **Resources**, and the appropriate plug-in from the list.

2. In the Resources page, select **Path** from the View list.

3. Click ![filter icon], and then select the host name and the Unix File Systems to filter the resources.

4. Select the file system that you want to back up.

5. In the Resources page, you can perform the following steps:

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

For example, `customtext_policy_hostname` or `resource_hostname`. A timestamp is appended to the Snapshot name by default.

6. In the Application Settings page, perform the following:

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

- Select one of the backup consistency options:

  ▪ Select **File System Consistent** if you want to ensure that file systems cached data is flushed before creating the backup and no operations are performed on filesystem while creating the backup.

  ▪ Select **Crash Consistent** if you want to ensure that file systems cached data is flushed before creating the backup.

7. In the Policies page, perform the following steps:

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

   (i) You can create a policy by clicking [+].

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

   b. Click [+] in the Configure Schedules column to configure a schedule for the policy you want.

   c. In the Add schedules for policy *policy_name* window, configure the schedule, and then select OK.

   policy_name is the name of the policy that you have selected.

   The configured schedules are listed in the Applied Schedules column.

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

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

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

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

   The topology page is displayed.

10. Click **Back up Now**.

11. In the Backup page, perform the following steps:

    a. If you have applied multiple policies to the resource, from the Policy drop-down list, select the policy that you want to use for backup.

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

    b. Click **Backup**.

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

Back up Unix file systems resource groups

You can back up the Unix file systems 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 are created according to the schedule.

Steps

1. In the left navigation pane, select **Resources**, and the appropriate plug-in from the list.

2. In the Resources page, select **Resource Group** from the **View** list.

3. Enter the resource group name in the search box, or click ![filter icon], and select the tag.

    Click ![filter icon] to close the filter pane.

4. In the Resource Group page, select the resource group to back up.

5. In the Backup page, perform the following steps:

    a. If you have multiple policies associated with the resource group, select the backup policy you want to use from the **Policy** drop-down list.

       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. Select **Backup**.

6. Monitor the progress by selecting **Monitor > Jobs**.

Monitor Unix file systems backup

Learn how to monitor the progress of backup operations and data protection operations.

Monitor Unix file systems 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 icon] In progress
- ![completed icon] Completed successfully
- ![failed icon] Failed
- ![warning icon] Completed with warnings or could not start due to warnings
- ![queued icon] Queued
- ![canceled icon] 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 ![filter icon] 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.

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

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

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

Monitor data protection operations in the Activity pane

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

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

Steps
1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. Click ![activity icon] 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.

View protected Unix file systems in the Topology page

When you are preparing to back up, restore, or clone a resource, you might find it helpful to view a graphical representation of all backups, restored file systems, and clones on the primary and secondary storage.

About this task

In the Topology page, you can see all the backups, restored file systems, and clones that are available for the selected resource or resource group. You can view the details of those backups, restored file systems, and clones, and then select them to perform data protection operations.

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).

* ![database icon] 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.

- 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 created 6 backups using a policy to retain only 4 backups, the number of backups displayed is 6.

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

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

- The replica site is up.

- The replica site is down.

- The secondary mirror or vault relationship has not been re-established.

Steps

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

2. In the Resources page, either select the resource or resource group from the **View** drop-down list.

3. Select the resource either from the resource details view or from the resource group details view.

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

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

   The Summary Card section displays the total number of backups and clones.

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

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

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

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

◦ For SnapMirror active sync and only for ONTAP 9.14.1, Async Mirror or Async MirrorVault relationships to the new primary destination should be manually configured after failover. From ONTAP 9.15.1 onwards Async Mirror or Async MirrorVault is auto configured to the new primary destination.

◦ After failover, a backup should be created for SnapCenter to be aware of the failover. You can click **Refresh** only after a backup has been created.

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

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

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

   (i) You cannot rename or delete backups that are on the secondary storage.

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

Example showing backups and clones on the primary storage

13