



Back up Unix file systems

SnapCenter Software 5.0

NetApp
July 18, 2024

This PDF was generated from https://docs.netapp.com/us-en/snapcenter-50/protect-scu/task_determine_whether_unix_file_systems_are_available_for_backup.html on July 18, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Back up Unix file systems 1
 - Discover the UNIX file systems available for backup..... 1
 - Create backup policies for Unix file systems 1
 - Create resource groups and attach policies for Unix file systems 3
- Back up Unix file systems 5
- Back up Unix file systems resource groups 6
- Monitor Unix file systems backup 7

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.

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 description.

- Specify the schedule frequency by selecting **On demand**, **Hourly**, **Daily**, **Weekly**, or **Monthly**.
- In the Retention page, specify the retention settings for the backup type and the schedule type selected in the Backup Type page:


If you want to...	Then...
Keep a certain number of Snapshots	<p>Select Total Snapshot copies to keep, and then specify the number of Snapshots that you want to keep.</p> <p>If the number of Snapshots exceeds the specified number, the Snapshots are deleted with the oldest copies deleted first.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> 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.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> 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.</p> </div>
Keep the Snapshots for a certain number of days	Select Keep Snapshot copies for , and then specify the number of days for which you want to keep the Snapshots before deleting them.



You can retain archive log backups only if you have selected the archive log files as part of your backup.

- In the Replication page, specify the replication settings:

For this field...	Do this...
Update SnapMirror after creating a local Snapshot copy	Select this field to create mirror copies of the backup sets on another volume (SnapMirror replication).
Update SnapVault after creating a local Snapshot copy	Select this option to perform disk-to-disk backup replication (SnapVault backups).

For this field...	Do this...
Secondary policy label	<p>Select a Snapshot label.</p> <p>Depending on the Snapshot label that you select, ONTAP applies the secondary Snapshot retention policy that matches the label.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> If you have selected Update SnapMirror after creating a local Snapshot copy, you can optionally specify the secondary policy label. However, if you have selected Update SnapVault after creating a local Snapshot copy, you should specify the secondary policy label.</p> </div>
Error retry count	Enter the maximum number of replication attempts that can be allowed before the operation stops.



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

- 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.



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.

- 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.

Steps

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



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.



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.



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.



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 either the GUI or the PowerShell command `Set-SmSmtServer`.

9. 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 , 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.



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**.



For email notification, you must have specified the SMTP server details using 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 , and select the tag.

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

Steps

1. In the left navigation pane, click **Monitor**.
2. In the Monitor page, click **Jobs**.
3. In the Jobs page, perform the following steps:
 - a. Click  to filter the list so that only backup operations are listed.
 - b. Specify the start and end dates.
 - c. From the **Type** drop-down list, select **Backup**.
 - d. From the **Status** drop-down, select the backup status.
 - e. Click **Apply** to view the operations completed successfully.
4. Select a backup job, and then click **Details** to view the job details.



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

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


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

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  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.

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

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

Trademark information

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