Manage SnapCenter Server and plug-ins

SnapCenter Software 4.5

NetApp
July 03, 2026

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

Table of Contents

Manage SnapCenter Server and plug-ins . . . 1
View dashboard . . . 1
Overview of dashboard . . . 1
How to view information on the dashboard . . . 5
Request status reports of the jobs from the dashboard . . . 5
Request reports of the protection status from the dashboard . . . 6
Manage RBAC . . . 6
Modify a role . . . 6
Modify users and groups . . . 7
Manage hosts . . . 7
Refresh virtual machine information . . . 8
Modify plug-in hosts . . . 9
Start or restart plug-in services . . . 10
Suspend schedules for host maintenance . . . 10
Operations supported from the Resources page . . . 11
Manage policies . . . 12
Modify policies . . . 12
Detach policies . . . 13
Delete policies . . . 13
Manage resource groups . . . 13
Stop and resume operations on resource groups . . . 14
Delete resource groups . . . 14
Manage backups . . . 15
Rename backups . . . 15
Delete backups . . . 15
Delete clones . . . 16
Monitor jobs, schedules, events, and logs . . . 17
Monitor jobs . . . 17
Monitor schedules . . . 17
Monitor events . . . 17
Monitor logs . . . 18
Remove jobs and logs from SnapCenter . . . 19
Overview of SnapCenter reporting capabilities . . . 19
Access reports . . . 21
Filter your report . . . 21
Export or print reports . . . 22
Set the SMTP server for email notifications . . . 22
Configure the option to email reports . . . 22
Manage the SnapCenter Server repository . . . 23
Prerequisites for protecting the SnapCenter repository . . . 23
Back up the SnapCenter repository . . . 23
View backups of the SnapCenter repository . . . 24
Restore the SnapCenter database repository . . . 24

Migrate the SnapCenter repository . . . 24
Reset the SnapCenter repository password . . . 25
Manage resources of untrusted domains . . . 26
Modify untrusted domains . . . 26
Unregister untrusted Active Directory domains . . . 26
Manage the storage system . . . 27
Modify storage system configuration . . . 27
Delete the storage system . . . 29
Manage EMS data collection . . . 30
Stop EMS data collection . . . 30
Start EMS data collection . . . 30
Change EMS data collection schedule and target SVM . . . 30
Monitor EMS data collection status . . . 30

Manage SnapCenter Server and plug-ins

View dashboard

Overview of dashboard

From the SnapCenter left navigation pane, the Dashboard gives you a first glance into the health of your system, including recent job activity, alerts, protection summary, storage efficiency and usage, status of SnapCenter jobs (Backup, Clone, Restore), configuration status for standalone and Windows cluster hosts, number of Storage Virtual Machines (SVMs) managed by SnapCenter, and license capacity.

Information displayed in the Dashboard view depends on the role assigned to the user that is currently logged in to SnapCenter. Some content might not be displayed if the user does not have permission to view that information.

In many cases, you can view more information about a display by hovering on **i**. In some cases, information in dashboard displays is linked to detailed source information in SnapCenter GUI pages such as Resources, Monitor, and Reports.

Recent Job Activities

The Recent Job Activities tile displays the latest job activity from any Backup, Restore, and Clone jobs that you have access to. Jobs in this display have one of the following states: Completed, Warning, Failed, Running, Queued, and Canceled.

Hovering over a job provides more information. You can view additional job information by clicking a specific job number, which redirects you to the Monitor page. From there, you can get job details or log information, and generate a report specific to that job.

Click **See All** to view a history of all SnapCenter jobs.

Alerts

The Alerts tile displays the latest unresolved Critical and Warning alerts for the hosts and SnapCenter Server.

The total count of Critical and Warning category alerts is shown at the top of the display. Clicking the Critical or Warning totals redirects you to the Alerts page with the specific filter applied in the Alerts page.

Clicking a specific alert redirects you to the Alerts page for details about that alert. Clicking **See All** at the bottom of the display redirects you to the Alerts page for a list of all alerts.

Latest Protection Summary

The Latest Protection Summary tile gives you the protection status for all entities that you have access to. By default, the display is set to provide the status for all plug-ins. Status information is provided for resources backed up to primary storage as Snapshot copies, and to secondary storage using SnapMirror and SnapVault technologies. The availability of protection status information for secondary storage is based on the selected plug-in type.

If you are using a mirror-vault protection policy, the counters for the protection summary are displayed in the SnapVault summary chart and not in the SnapMirror chart.

Protection status for individual plug-ins is available by selecting a plug-in from the drop-down menu. A donut chart shows the percentage of protected resources for the selected plug-in. Clicking a donut slice redirects you to the **Reports** > **Plug-in** page, which provides a detailed report of all primary and secondary storage activity for the specified plug-in.

Reports about secondary storage apply to SnapVault only; SnapMirror reports are not supported.

SAP HANA provides protection status information for primary and secondary storage for Snapshot copies. Only primary storage protection status is available for file-based backups.

Protection status	Primary storage	Secondary storage
Failed	Count of entities that are part of a Resource Group, where the Resource Group has run a backup, but the backup failed.	Count of entities with backups that have failed to transfer to a Secondary destination.
Successful	Count of entities in a resource group, where the Resource Group has been successfully backed up.	Count of entities with backups that have been successfully transferred to a Secondary destination.
Not configured	Count of entities that are not part of any Resource Group and have not been backed up.	Count of entities that are part of one or more Resource Groups that are not configured for backups to be transferred to a Secondary destination.
Not initiated	Count of entities that are part of a Resource Group, but no backup has been run.	Not applicable.

If you are using SnapCenter Server 4.2 and an earlier version of the plug-in (earlier than 4.2) to create backups, the **Latest Protection Summary** tile does not display the SnapMirror protection status of these backups.

Jobs

The Jobs tile provides you with a summary of backup, restore, and clone jobs that you have access to. You can customize the time frame for any report by using the drop-down menu. Time frame options are fixed at last 24 hours, last 7 days, and last 30 days. The default report shows data protection jobs run during the last 7 days.

Backup, restore, and clone job information is displayed in donut charts. Clicking a donut slice redirects you to the Monitor page with job filters pre-applied to the selection.

Job status	Description
Failed	Count of jobs that have failed.
Warning	Count of jobs that have experienced an error.
Successful	Count of jobs that have completed successfully.
Running	Count of jobs that are currently running.

Storage

The Storage tile displays the primary and secondary storage consumed by protection jobs over a 90-day period, graphically depicts consumption trends, and calculates primary storage savings. Storage information is updated once every 24 hours at 12 a.m.

The day's consumption total, which comprises the total number of backups that are available in SnapCenter and size occupied by these backups, will be displayed at the top of the display. A backup could have multiple Snapshot copies associated with it and the count will reflect the same. This is applicable to both primary and secondary Snapshot copies. For example, you have created 10 backups, out of which 2 are deleted due to policy-based backup retention and 1 backup is explicitly deleted by you. Thus, a count of 7 backups will be displayed along with the size occupied by these 7 backups.

The Storage Savings factor for primary storage is the ratio of logical capacity (clone and Snapshot copy savings plus storage consumed) to the physical capacity of primary storage. A bar chart illustrates the storage savings.

The line graph separately plots primary and secondary storage consumption on a day-by-day basis over a rolling 90-day period. Hovering over the charts provides detailed day-by-day results.

If you use SnapCenter Server 4.2 and an earlier version of the plug-in (earlier than 4.2) to create backups, the **Storage** tile does not display the number of backups, the storage consumed by these backups, the Snapshot savings, the clone savings, and the Snapshot size.

Configuration

The Configuration tile provides consolidated status information for all active stand-alone and Windows cluster hosts that SnapCenter is managing, and that you have access to. This includes the plug-in status information associated with those hosts.

Clicking the number adjacent to Hosts redirects you to the Managed Hosts section in the Hosts page. From there, you can obtain detailed information for a selected host.

Additionally, this display shows the sum of Standalone ONTAP SVMs and Cluster ONTAP SVMs that SnapCenter is managing and that you have access to. Clicking the number adjacent to SVM redirects you to the Storage Systems page. From there, you can obtain detailed information for a selected SVM.

The Host configuration state is presented as red (critical), yellow (warning), and green (active), along with the number of hosts in each state. Status messages are provided for each state.

Configuration status	Description
Upgrade mandatory	Count of hosts that are running unsupported plug-ins and need an upgrade. An unsupported plug-in is not compatible with this version of SnapCenter.
Migration mandatory	Count of hosts that are running unsupported plug-ins and need migration. An unsupported plug-in is not compatible with this version of SnapCenter.
No plug-ins installed	Count of hosts that are added successfully but the plug-ins need to be installed, or the plug-ins installation has failed.
Suspended	Count of hosts whose schedules are suspended and are under maintenance.
Stopped	Count of hosts that are up, but the plug-in services are not running.
Host down	Count of hosts that are down or not reachable.
Upgrade available (optional)	Count of hosts where a newer version of the plug-in package is available for upgrade.
Migration available (optional)	Count of hosts where a newer version of the plug-in is available for migration.
Configure log directory	Count of hosts where the log directory has to be configured for SCSQL to take transaction log backup.
Configure VMware plug-ins	Count of hosts where the SnapCenter Plug-in for VMware vSphere needs to be added.
Unknown	Count of hosts that have been registered but the installation is not yet triggered.
Running	Count of hosts that are up and plug-ins are running. And in the case of SCSQL plug-ins, log directory and hypervisor are configured.
Installing\Uninstalling plug-ins	Count of hosts where plug-in installation or uninstallation in progress.

Licensed Capacity

The Licensed Capacity tile displays information about total licensed capacity, used capacity, capacity threshold alerts, and license expiration alerts for SnapCenter Standard capacity-based licenses.

This display appears only if you are using SnapCenter Standard capacity-based licenses on Cloud Volumes ONTAP or ONTAP Select platforms. For FAS or AFF platforms, the SnapCenter license is controller-based and licensed for unlimited capacity, and no capacity license is required.

License status	Description
In use	Amount of capacity currently in use.
Notify	Capacity threshold at which notifications are displayed on the Dashboard, and, if configured, when email notifications are sent.
Licensed	Amount of licensed capacity.
Over	Amount of capacity that has exceeded the licensed capacity.

How to view information on the dashboard

From the SnapCenter left navigation pane, you can view various Dashboard tiles, or displays, along with associated system details. The number of displays available in the Dashboard is fixed and cannot be changed. The content provided within each display is dependent on role-based access control (RBAC).

Steps

1. In the left navigation pane, click **Dashboard**.
2. Click the active areas on each display to obtain additional information.

   For example, clicking a donut chart in **Jobs**, redirects you to the Monitor page for more information about your selection. Clicking a donut chart in **Protection Summary**, redirects you to the Reports page, which can provide more information about your selection.

Request status reports of the jobs from the dashboard

You can request reports about backup, restore, and clone jobs from the Dashboard page. This is useful if you want to identify the total number of successful or failed jobs in your SnapCenter environment.

Steps

1. In the left navigation pane, click **Dashboard**
2. Locate the Jobs tile in the Dashboard, and then select **Backup**, **Restore**, or **Clone**.
3. Using the pull-down menu, select the time frame for which you want Jobs information: 24 hours, 7 days, or 30 days.

   The systems display a donut chart covering the data.

4. Click the donut slice representing the job information for which you want a report.

   When you click the donut chart, you are redirected from the Dashboard page to the Monitor page. The Monitor page displays the jobs with the status you selected from the donut chart.

5. From the Monitor page list, click on a specific job to select it.
6. At the top of the Monitor page, click **Reports**.

Results

The report displays information only for the job you selected. You can review the report or download it to your local system.

Request reports of the protection status from the dashboard

You can request protection details for resources managed by specific plug-ins using the Dashboard. Only data backups are considered for data protection summary.

Steps

1. In the left navigation pane, click **Dashboard**.
2. Locate the Latest Protection Summary tile in the Dashboard and use the pull-down menu to select a plug-in.

   The Dashboard displays a donut chart for resources backed up to Primary storage and, if applicable to the plug-in, a donut chart for resources backed up to secondary storage.

   Data protection reports are available only for specific plug-ins types. Specifying **All Plug-ins** is not supported.

3. Click the donut slice representing the status for which you want a report.

   When you click the donut chart, you are redirected from Dashboard page to the Reports, and then to the Plug-in page. The report displays only status for the plug-in you selected. You can review the report or download it to your local system.

   Redirection to the Reports page for SnapMirror donut chart and File-based SAP HANA backup is not supported.

Manage RBAC

SnapCenter allows you to modify roles, users, and groups.

Modify a role

You can modify a SnapCenter role to remove users or groups and change the permissions associated with the role. It is especially useful to modify roles when you want to change or eliminate the permissions used by an entire role.

What you will need

You must have logged in as the "SnapCenterAdmin" role.

You cannot modify or remove permissions for the SnapCenterAdmin role.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Roles**.
3. From the Role name field, click the role you want to modify.
4. In the Role Details page alter the permissions or unassign the members as needed.
5. Select **All members of this role can see other members' objects** to enable other members of the role to see resources such as volumes and hosts after they refresh the resources list.

   Deselect this option if you do not want members of this role to see objects to which other members are assigned.

   When this option is enabled, assigning users access to objects or resources is not required if users belong to the same role as the user who created the objects or resources.

6. Click **Submit**.

Modify users and groups

You can modify SnapCenter users or groups to alter their roles and assets.

What you will need

You must be logged in as the SnapCenter administrator.

Steps

1. In the left navigation pane, click **Settings**.
2. On the Settings page, click **Users and Access**.
3. From the User or Group name list, click the user or group that you want to modify.
4. On the User or Group details page, alter roles and assets.
5. Click **Submit**.

Manage hosts

You can add hosts and install SnapCenter plug-in packages, add a verification server, remove hosts, migrate backup jobs, and update host to upgrade plug-in packages or add new plug-in packages. Depending on the plug-in you are using, you can also provision disks, manage SMB shares, manage initiator groups (igroups), manage iSCSI sessions, and migrate data.

You can perform these tasks…	For Microsoft Exchange Server	For Microsoft SQL Server	For Microsoft Windows	For Oracle Database	For SAP HANA Database	For Custom Plug-ins
Add hosts and install plug-in package	Yes	Yes	Yes	Yes	Yes	Yes
Update ESXi information for a host	No	Yes	No	No	No	No
Suspend schedules and place hosts in maintenance mode	Yes	Yes	Yes	Yes	Yes	Yes
Modify hosts by adding, upgrading, or removing plug-ins	Yes	Yes	Yes	Yes	Yes	Yes
Remove hosts from SnapCenter	Yes	Yes	Yes	Yes	Yes	Yes
Start plug-in services	Yes	Yes	Yes	Yes	Yes	Yes
Provision disks	No	No	Yes	No	No	No
Manage SMB shares	No	No	Yes	No	No	No
Manage iGroups	No	No	Yes	No	No	No
Manage iSCSI sessions	No	No	Yes	No	No	

Refresh virtual machine information

You should refresh your virtual machine information when VMware vCenter credentials change or the database or file system host restarts. Refreshing your virtual machine information in SnapCenter initiates communication with the VMware vSphere vCenter and obtains vCenter credentials.

RDM-based disks are managed by the SnapCenter Plug-in for Microsoft Windows, which is installed on the database host. To manage RDMs, the SnapCenter Plug-in for Microsoft Windows communicates with the vCenter server that manages the database host.

Steps

1. In the SnapCenter left navigation pane, click **Hosts**.
2. In the Hosts page, click **Managed Hosts**.
3. In the Managed Hosts page, select the host you want to update.
4. Click **Refresh VM**.

Modify plug-in hosts

After installing a plug-in, you can modify the plug-in hosts details if required. You can modify credentials, installation path, plug-ins, log directory details for SnapCenter Plug-in for Microsoft SQL Server, group Managed Service Account (gMSA), and the plug-in port.

Ensure that the plug-in version is the same as that of the SnapCenter Server version.

About this task

- You can modify a plug-in port only after the plug-in is installed.

  You cannot modify the plug-in port while upgrade operations are in progress.

- While modifying a plug-in port, you should be aware of the following port rollback scenarios:
  - In a standalone setup, if SnapCenter fails to change the port of one of the components, the operation fails and the old port is retained for all of the components.

    If the port was changed for all of the components but one of the components fails to start with the new port, then the old port is retained for all of the components. For example, if you want to change the port for two plug-ins on the stand-alone host and SnapCenter fails to apply the new port to one of the plug-ins, the operation fails (with an appropriate error message) and the old port is retained for both the plug-ins.

  - In a clustered setup, if SnapCenter fails to change the port of the plug-in that is installed on one of the nodes, the operation fails and the old port is retained for all of the nodes.

    For example, if the plug-in is installed on four nodes in a clustered setup, and if the port is not changed for one of the nodes, the old port is retained for all of the nodes.

When plug-ins are installed with gMSA, you can modify in the **More Options** windows. When plug-ins are installed without gMSA, you can specify the gMSA account to use it as the plug-in service account.

Steps

1. In the left navigation pane, click **Hosts**.
2. Verify that **Managed Hosts** is selected at the top.
3. Select the host for which you want to modify and modify any one field.

   Only one field can be modified at a time.

4. Click **Submit**.

Results

The host is validated and added to SnapCenter Server.

Start or restart plug-in services

Starting the SnapCenter plug-in services enable you to start services if they are not running or restart them if they are running. You might want to restart services after maintenance has been performed.

You should ensure that no jobs are running when restarting the services.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Managed Hosts**.
3. In the Managed Hosts page, select the host you want to start.
4. Click icon and click **Start Service** or **Restart Service**.

   You can start or restart service of multiple hosts simultaneously.

Suspend schedules for host maintenance

When you want to prevent the host from running any SnapCenter scheduled jobs, you can place your host in maintenance mode. You should do this before you upgrade the plug-ins or if you are performing maintenance tasks on hosts.

You cannot suspend the schedules on a host that is down because SnapCenter cannot communicate with that host.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Managed Hosts**.
3. In the Managed Hosts page, select the host that you want to suspend.
4. Click the icon, and then click **Suspend Schedule** to place the host for this plug-in in maintenance mode.

   You can suspend the schedule of multiple hosts simultaneously.

You do not have to stop the plug-in service first. The plug-in service can be in a running or stopped state.

Results

After you suspend the schedules on the host, the Managed Hosts page shows **Suspended** in the Overall status field for the host.

After you complete host maintenance, you can bring the host out of maintenance mode by clicking **Activate Schedule**. You can activate the schedule of multiple hosts simultaneously.

Operations supported from the Resources page

You can discover resources and perform data protection operations from the Resources page. The operations you can perform differ based on the plug-in you are using to manage your resources.

From the Resources page, you can perform the following tasks:

You can perform these tasks…	For Microsoft Exchange Server	For Microsoft SQL Server	For Microsoft Windows	For Oracle Database	For SAP HANA Database	For Custom Plug-ins
Determine whether resources are available for backup	Yes	Yes	Yes	Yes	Yes	Yes
Perform on-demand backup of a resource	Yes	Yes	Yes	Yes	Yes	Yes
Restore from backups	Yes	Yes	Yes	Yes	Yes	Yes
Clone backups	No	Yes	Yes	Yes	Yes	Yes
Manage backups	Yes	Yes	Yes	Yes	Yes	Yes
Manage clones	No	Yes	Yes	Yes	Yes	Yes
Manage policies	Yes	Yes	Yes	Yes	Yes	Yes
Manage storage connections	Yes	Yes	Yes	Yes	Yes	Yes
Mount backups	No	No	No	Yes	No	No

You can perform these tasks…	For Microsoft Exchange Server	For Microsoft SQL Server	For Microsoft Windows	For Oracle Database	For SAP HANA Database	For Custom Plug-ins
Unmount backups	No	No	No	Yes	No	No
View details	Yes	Yes	Yes	Yes	Yes	Yes

Manage policies

You can detach policies from a resource or resource group, modify, delete, view, and copy.

Modify 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	Create a new policy and attach it to the necessary resources or resource groups. 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.
Remove or change a schedule type	Perform the following: 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. For example, if a policy specifies hourly backups and you want to change that to daily backups, you must detach the policy first.

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**.

Detach 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.

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.
5. Make any additional modifications to the resource group in the rest of the wizard, and then click **Finish**.

Delete policies

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

What you will need

You should detach the policy from resource or resource groups if the policy is associated with any resource or resource groups.

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**.

Manage resource groups

You can perform various operations on resource groups.

You can perform the following tasks related to resource groups:

- 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.

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

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.

Stop and resume 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**.

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

Delete 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.

About this task

You should manually delete all clones created for any of the resources in the resource group. You can optionally force the deletion of all backups, metadata, policies, and Snapshot copies associated with the resource group.

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**.

Manage backups

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

Rename 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 have cataloged the backups of Oracle databases 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**.

Delete backups

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

What you will need

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 .

   If you are deleting a SAP HANA database backup, the associated SAP HANA catalogs of the backup are also deleted.

   If the last remaining backup is deleted, the associated HANA catalog entries cannot be deleted.

6. Click **OK**.

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

Delete clones

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

About this task

You cannot delete clones that acts like source for other clones.

For example, if the production database is db1, database clone1 is cloned from backup of db1 and subsequently clone1 is protected. The database clone2 is cloned from backup of clone1. If you decide to delete clone1, you must first delete clone2, and then delete 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 .

   If you are deleting SAP HANA database clones, in the Delete Clone page, perform the following actions:

   a. In the **Pre clone delete** field, enter the commands that should be run before deleting the clone.
   b. In the **Unmount** field, enter the command to unmount the clone before deleting the clone.

6. Click **OK**.

After you finish

Sometimes the file systems are not deleted. You must increase the value of the CLONE_DELETE_DELAY parameter by running the following command: `./sccli Set-SmConfigSettings`

> The CLONE_DELETE_DELAY parameter specifies the number of seconds to wait after completing the deletion of application clone and before starting the deletion of file system.

After modifying the value of the parameter, restart the SnapCenter Plug-in Loader (SPL) service.

Monitor jobs, schedules, events, and logs

You can monitor the progress of your jobs, get information about scheduled jobs, and review events and logs from the Monitor page.

Monitor jobs

You can view information about SnapCenter backup, clone, restore, and verification jobs. You can filter this view based on start and end date, type of job, resource group, policy, or SnapCenter plug-in. You can also get additional details and log files for specified jobs.

You can also monitor jobs related to SnapMirror and SnapVault operations.

> You can monitor only the jobs that you created and that are relevant to you unless you are assigned SnapCenter Admin or another super user role.

You can perform the following tasks related to monitoring jobs:

- Monitor backup, clone, restore, and verification operations.
- View job details and reports.
- Stop a scheduled job.

Monitor schedules

You might want to view current schedules to determine when the operation starts, when it was last run, and when it runs next. You can also determine the host on which the operation runs, along with the operation's resource group and policy information.

Steps

1. In the left navigation pane, click **Monitor**.
2. In the Monitor page, click **Schedules**.
3. Select the resource group and the schedule type.
4. View the list of scheduled operations.

Monitor events

You can view a list of SnapCenter events in the system, such as when a user creates a resource group or when the system initiates activities, such as creating a scheduled backup. You might want to view events to determine if an operation such as a backup or a restore operation is currently in progress.

About this task

All job information appears in the Events page. For example, when a backup job starts, a “backup start” event appears. When the backup completes, a “backup complete” event appears.

Steps

1. In the left navigation pane, click **Monitor**.
2. In the Monitor page, click **Events**.
3. (Optional) In the Filter box, enter the start or end date, category of event (such as backup, resource group, or policy) and severity level, and click **Apply**. Alternatively, enter characters in the Search box.
4. View the list of events.

Monitor logs

You can view and download SnapCenter Server logs, SnapCenter host agent logs, and plug-in logs. You might want to view the logs to help with troubleshooting.

About this task

You can filter the logs to show only a specific log severity level:

- Debug
- Info
- Warn
- Error
- Fatal

You can also obtain job level logs, for example, logs that help you troubleshoot the reason for a backup job failure. For job level logs, use the **Monitor** > **Jobs** option.

Steps

1. In the left navigation pane, click **Monitor**.
2. In the Jobs page, select a job and click Download logs.

   The downloaded zipped folder contains the job logs and the common logs. The zipped folder name contains the job id and job type selected.

3. In the Monitor page, click **Logs**.
4. Select the log type, host, and instance.

   If you select log type as **plugin**, you can select a host or SnapCenter plug-in. You cannot do this if the log type is **server**.

5. To filter the logs by a specific source, message, or log level, click the filter icon at the top of the column heading.

   To show all logs, choose **Greater than or equal to** as the `Debug` level.

6. Click **Refresh**.
7. View the list of logs.

8. Click **Download** to download the logs.

   The downloaded zipped folder contains the job logs and the common logs. The zipped folder name contains the job id and job type selected.

In large configurations for optimum performance, you should set the log settings for SnapCenter to minimal level by using the PowerShell cmdlet.

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10
-JobLogsMaxFileSize 10MB -Server
```

To access health or configuration information after a failover job finishes, run the cmdlet `Get-SmRepositoryConfig`.

Remove jobs and logs from SnapCenter

You can remove backup, restore, clone, and verification jobs and logs from SnapCenter. SnapCenter stores successful and failed job logs indefinitely unless you remove them. You might want to remove them to replenish storage.

About this task

There must be no jobs currently in operation. You can remove a specific job by providing a Job ID or you can remove jobs within a specified period.

You do not need to place the host in maintenance mode to remove jobs.

Steps

1. Launch PowerShell.
2. From the command prompt, enter: `Open-SMConnection`
3. From the command prompt, enter: `Remove-SmJobs`
4. In the left navigation pane, click **Monitor**.
5. In the Monitor page, click **Jobs**.
6. In the Jobs page, review the status of the job.

Find more information

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Overview of SnapCenter reporting capabilities

SnapCenter provides a variety of reporting options that enable you to monitor and manage your system health and operation success.

Report type	Description
Backup Report	The Backup Report provides overall data about backup trends for your SnapCenter environment, the backup success rate, and some information about each backup performed during the specified time. If a backup is deleted, the report does not display any status information for the deleted backup. The Backup Detail Report provides detailed information about a specified backup job and lists the resources successfully backed up and any that have failed.
Clone Report	The Clone Report provides overall data about clone trends for your SnapCenter environment, the clone success rate, and some information about each clone job performed during the specified time. If a clone is deleted, the report does not display any status information for the deleted clone. The Clone Detail Report provides details about the specified clone, clone host, and clone job task status. If a task fails, the Clone Detail Report displays information about the failure.
Restore Report	The Restore Report provides overall information about restore jobs. The Restore Detail Report provides details about a specified restore job, including host name, backup name, job start and duration, and the status of individual job tasks. If a task fails, the Restore Detail Report displays information about the failure.
Protection Report	These reports provide protection details for resources managed by all SnapCenter plug-in instances. This report provides protection details for resources managed by all plug-in instances. You can see an overview, details of unprotected resources, resources that have not been backed up when the report was generated, resources of a resource group for which backup operations have failed, and SnapVault status.

Report type	Description
Scheduled Report	These reports are scheduled to run periodically like daily, weekly or monthly. The reports are generated automatically on the specified date and time and the report is sent to the respective people through e-mail. You can enable, disable, modify, or delete the schedules. The enabled schedule can be run on demand by clicking on the **Run Now** button. The administrator can run any schedule, but the generated report will contain data based on the permission provided by the user who created the schedule. Any other user other than Administrator will be able to see or modify schedule based on their permission .If All members of this role can see other members' objects option is selected in the Add Role page, then other members of the role will be able to see and modify.

Access reports

You can use the SnapCenter Dashboard to get a quick overview of the health of your system. From the Dashboard you can drill into more details. Alternatively, you can access the detailed reports directly.

You can access reports by one of the following methods:

- In the left navigation pane, click **Dashboard**, and then click **Last Protection Summary** pie chart to see more details in the Reports page.
- In the left navigation pane, click **Reports**.

Filter your report

You might want to filter your report data according to a range of parameters, depending on the level of detail and time span of information you require.

Steps

1. In the left navigation pane, click **Reports**.
2. If the Parameter view is not displayed, click the **Toggle Parameters Area** icon from the report toolbar.
3. Specify the time range for which you want to run your report.
   If you omit the end date, you retrieve all available information.
4. Filter your report information based on any of the following criteria:
   - Resource group
   - Host
   - Policy
   - Resource
   - Status

- Plug-in Name

5. Click **Apply**.

Export or print reports

Exporting SnapCenter reports enables you to view the report in a variety of alternative formats. You can also print reports.

Steps

1. In the left navigation pane, click **Reports**.
2. From the reports toolbar, perform one of the following:
   - Click the **Toggle Print Preview** icon to preview a printable report.
   - Select a format from the **Export** icon drop-down list to export a report to an alternate format.
3. To print a report, click the **Print** icon.
4. To view a specific report summary, scroll to the appropriate section of the report.

Set the SMTP server for email notifications

You can specify the SMTP server to use for sending data protection job reports to yourself or to others. You can also send a test email to verify the configuration. The settings are applied globally for any SnapCenter job for which you configure email notification.

This option configures the SMTP server for sending all data protection job reports. However, if you want to have regular SnapCenter data protection job updates for a particular resource sent to yourself or to others so that you can monitor the status of those updates, you can configure the option to email the SnapCenter reports when you are creating a resource group.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Global Settings**.
3. Enter the SMTP server and click **Save**.
4. To send a test email, enter the email address from and to which you will send the email, enter the subject, and click **Send**.

Configure the option to email reports

If you want to have regular SnapCenter data protection job updates sent to yourself or to others so that you can monitor the status of those updates, you can configure the option to email the SnapCenter reports when you are creating a resource group.

What you will need

You must have configured your SMTP server on the Global Settings page under Settings.

Steps

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

2. Select the type of resource you want to view and click **New Resource Group**, or select an existing resource group and click **Modify** to configure email reports for an existing resource group.
3. In the Notification panel of the New Resource Group wizard, select from the pull-down menu whether you want to receive reports always, on failure, or on failure or warning.
4. Enter the address the email is sent from, the address the email is sent to, and the subject of the email.

Manage the SnapCenter Server repository

Information related to various operations performed from SnapCenter is stored in the SnapCenter Server database repository. You must create backups of the repository to protect the SnapCenter Server from data loss.

The SnapCenter Server repository is sometimes referred to as the NSM database.

Prerequisites for protecting the SnapCenter repository

Your environment should meet certain prerequisites to protect the SnapCenter repository.

- Managing storage virtual machine (SVM) connections

  You should configure the storage credentials.

- Provisioning hosts

  At least one NetApp storage disk should be present on the SnapCenter repository host. If a NetApp disk is not present on the SnapCenter repository host, you must create one.

  For details about adding hosts, setting up SVM connections, and provisioning hosts, see the installation instructions.

- Provisioning iSCSI LUN or VMDK

  For high availability (HA) configuration, you can provision either a iSCSI LUN or a VMDK in one of the SnapCenter Servers.

Back up the SnapCenter repository

Backing up the SnapCenter Server repository helps protect it from data loss. You can back up the repository by running the *Protect-SmRepository* cmdlet.

About this task

The *Protect-SmRepository* cmdlet accomplishes the following tasks:

- Creates a resource group and a policy
- Creates a backup schedule for the SnapCenter repository

Steps

1. Launch PowerShell.
2. On the SnapCenter Server host, establish a session using the *Open-SmConnection* cmdlet, and then enter

your credentials.

3. Back up the repository using the *Protect-SmRepository* cmdlet and the required parameters.

View backups of the SnapCenter repository

You can display a list of SnapCenter Server database repository backups by running the *Get-SmRepositoryBackups* cmdlet.

The repository backups are created according to the schedule specified in the *Protect-SmRepository* cmdlet.

Steps

1. Launch PowerShell.
2. From the command prompt, enter the following cmdlet, and then provide credentials to connect to the SnapCenter Server: *Open-SMConnection*
3. List all available SnapCenter database backups using the *Get-SmRepositoryBackups* cmdlet.

Restore the SnapCenter database repository

You can restore the SnapCenter repository by running the *Restore-SmRepositoryBackup* cmdlet.

When you are restoring the SnapCenter repository, other SnapCenter operations that are running will be impacted because during the restore operation the repository database is not accessible.

Steps

1. Launch PowerShell.
2. From the command prompt, enter the following cmdlet, and then provide credentials to connect to the SnapCenter Server: *Open-SMConnection*
3. Restore the repository backup using the *Restore-SmRepositoryBackup* cmdlet.

   The following cmdlet restores the SnapCenter MySQL database repository from the backups existing on either iSCSI LUN or VMDK:

   ```
   C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445
   ```

   The following cmdlet restores the SnapCenter MySQL database when backup files are deleted accidentally in the iSCSI LUN. For VMDK manually restore the backup from ONTAP Snapshot copies.

   ```
   C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
   ```

Migrate the SnapCenter repository

You can migrate the SnapCenter Server database repository from the default location to another disk. You might migrate the repository when you want to relocate it to a disk with more space.

Steps

1. Stop the MYSQL57 service in Windows.
2. Locate the MySQL data directory.

   You can usually find the data directory at C:\ProgramData\MySQL\MySQL Server 5.7\Data.

3. Copy the MySQL data directory to the new location, for example, E:\Data\nsm.
4. Right click on the new directory, and then select **Properties** > **Security** to add the Network Service local server account to the new directory, and then assign the account full control.
5. Rename the original database directory, for example, nsm_copy.
6. From a Windows command prompt, create a symbolic directory link by using the *mklink* command.

   ```
   "mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
   ```

7. Start the MYSQL57 service in Windows.
8. Verify that the database location change is successful by logging in to SnapCenter and checking repository entries, or by logging in to the MySQL utility and connecting to the new repository.
9. Delete the original, renamed, database repository directory (nsm_copy).

Reset the SnapCenter repository password

The MySQL Server repository database password is automatically generated during SnapCenter Server installation from SnapCenter 4.2. This automatically generated password is not known to SnapCenter user at any point. If you want to access the repository database, you should reset the password.

What you will need

You should have the SnapCenter administrator privileges to reset the password.

Steps

1. Launch PowerShell.
2. From the command prompt, enter the following command, and then provide the credentials to connect to the SnapCenter Server: *Open-SMConnection*
3. Reset the repository password: *Set-SmRepositoryPassword*

   The following command resets the repository password:

   ```
   Set-SmRepositoryPassword at command pipeline position 1
   Supply values for the following parameters:
   NewPassword: ********
   ConfirmPassword: ********
   Successfully updated the MySQL server password.
   ```

Find more information

The information regarding the parameters that can be used with the cmdlet and their descriptions can be

obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Manage resources of untrusted domains

In addition to managing hosts in Active Directory (AD) trusted domains, SnapCenter also manages hosts in multiple AD untrusted domains. The untrusted AD domains must be registered with the SnapCenter Server. SnapCenter supports users and groups of multiple untrusted AD domains.

You can install the SnapCenter Server on a machine that is in either a domain or a workgroup. To install the SnapCenter Server, you should specify the domain credentials if the machine is in a domain or the local administrator credentials if the machine is in a workgroup.

Active Directory (AD) groups that belong to domains not registered with the SnapCenter Server are not supported. Although you can create SnapCenter roles with these AD groups, logging in to SnapCenter Server fails with the following error message: The user you are trying to login does not belong to any roles. Please contact your administrator.

Modify untrusted domains

You can modify an untrusted domain when you want to update the domain controller IP addresses or the fully qualified domain name (FQDN).

About this task

After you modify the FQDN, the associated assets (hosts, users, and groups) might not function as expected.

To modify an untrusted domain, you can use either the SnapCenter user interface or PowerShell cmdlets.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Global Settings**.
3. In the Global Settings page, click **Domain Settings**.
4. Click , and then provide the following details:

For this field…	Do this…
Domain FQDN	Specify the FQDN, and click **Resolve**.
Domain controller IP addresses	If the domain FQDN is not resolvable, specify one or more domain controller IP addresses.

5. Click **OK**.

Unregister untrusted Active Directory domains

You can unregister an untrusted Active Directory domain if you do not want to use the assets that are

associated with that domain.

What you will need

You should have removed the hosts, users, groups, and credentials that are associated with the untrusted domain.

About this task

- After the domain is unregistered from SnapCenter Server, users of that domain cannot access SnapCenter Server.
- If there are associated assets (hosts, users, and groups), after unregistering the domain, the assets will be non-operational.
- To unregister an untrusted domain, you can use either the SnapCenter user interface or PowerShell cmdlets.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Global Settings**.
3. In the Global Settings page, click **Domain Settings**.
4. From the list of domains, select the domain that you want to unregister.
5. Click , and then click **OK**.

Manage the storage system

After adding the storage system, you can modify the storage system configuration and connections, or delete the storage system.

Modify storage system configuration

You can use SnapCenter to modify your storage system configuration if you want to change the user name, password, platform, port, protocol, timeout period, preferred IP address, or messaging options.

About this task

You can modify storage connections for an individual user or for a group. If you belong to one or more groups with permission to the same storage system, the storage connection name is displayed multiple times in the storage connection list, once for each group with permission to the storage system.

Steps

1. In the left navigation pane, click **Storage Systems**.
2. On the Storage Systems page, from the **Type** drop-down perform one of the following actions:

Select…	Steps…
ONTAP SVMs	To view all the storage virtual machines (SVMs) that were added, and to modify the required SVM configuration. 1. On the Storage Connections page, click the appropriate SVM name. 2. Perform one of the following actions: ◦ If the SVM is not part of any cluster, on the Modify Storage System page, modify the configurations such as user name, password, EMS and AutoSupport settings, platform, protocol, port, timeout, and preferred IP. ◦ If the SVM is part of a cluster, then on the Modify Storage System page, select **Manage SVM Independently** and modify the configurations such as user name, password, EMS and AutoSupport settings, platform, protocol, port, timeout, and preferred IP. After modifying the SVM to be managed independently, if you decide to manage it through cluster, you should delete the SVM and then click **Rediscover**. The SVM will be added to the ONTAP cluster. When a storage system password is updated on SnapCenter GUI, you should restart the SMCore services of the respective plug-in or the server host because the updated password does not reflect in SMCore, and the backup jobs will fail with an incorrect credential error.

Select…	Steps…
ONTAP Clusters	To view all the clusters that were added and modify the required cluster configuration. 1. On the Storage Connections page, click the cluster name. 2. On the Modify Storage System page, click the edit icon next to Username and modify the user name and password. 3. Select or clear the EMS and AutoSupport settings. 4. Click **More Options** and modify other configurations such as platform, protocol, port, timeout, and preferred IP.

3. Click **Submit**.

Delete the storage system

You can use SnapCenter to delete any unused storage system.

About this task

You can delete storage connections for an individual user or for a group. If you belong to one or more groups with permission to the same storage system, the storage system name is displayed multiple times in the storage connection list, once for each group with permission to the storage system.

When you are deleting a storage system, all operations that are being performed on that storage system will fail.

Steps

1. In the left navigation pane, click **Storage Systems**.
2. In the Storage Systems page, from the **Type** drop-down, select either **ONTAP SVMs** or **ONTAP Clusters**.
3. In the Storage Connections page, either select the check box next to the SVM, or the cluster that you want to delete.

   You cannot select the SVM that is part of a cluster.

4. Click **Delete**.
5. In the Delete Storage System Connection Settings page, click **OK**.

   If an SVM is deleted from ONTAP cluster using ONTAP GUI, in the SnapCenter GUI click **Rediscover** to update the SVM list.

Manage EMS data collection

You can schedule and manage Event Management System (EMS) data collection using PowerShell cmdlets. EMS data collection involves gathering details about the SnapCenter Server, the installed SnapCenter plug-in packages, the hosts, and similar information, and then sending it to a specified ONTAP storage virtual machine (SVM).

System CPU utilization is high when data-collection task is in progress. CPU utilization remains high as long as the operation is progress irrespective of the data size.

Stop EMS data collection

EMS data collection is enabled by default and runs every seven days after your installation date. You can disable data collection at any time by using the PowerShell cmdlet *Disable-SmDataCollectionEMS*.

Steps

1. From a PowerShell command line, establish a session with SnapCenter by entering *Open-SmConnection*.
2. Disable EMS data collection by entering *Disable-SmDataCollectionEms*.

Start EMS data collection

EMS data collection is enabled by default and is scheduled to run every seven days from the installation date. If you have disabled it, you can start EMS data collection again by using the *Enable-SmDataCollectionEMS* cmdlet.

The Data ONTAP event generate-autosupport-log permission has been granted to the storage virtual machine (SVM) user.

Steps

1. From a PowerShell command line, establish a session with SnapCenter by entering *Open-SmConnection*.
2. Enable EMS data collection by entering *Enable-SmDataCollectionEMS*.

Change EMS data collection schedule and target SVM

You can use PowerShell cmdlets to change the EMS data collection schedule or the target storage virtual machine (SVM).

Steps

1. From a PowerShell command line, to establish a session with SnapCenter, enter the *Open-SmConnection* cmdlet.
2. To change the EMS data collection target, enter the *Set-SmDataCollectionEmsTarget* cmdlet.
3. To change the EMS data collection schedule, enter the *Set-SmDataCollectionEmsSchedule* cmdlet.

Monitor EMS data collection status

You can monitor the status of your EMS data collection using several PowerShell cmdlets. You can get information about the schedule, storage virtual machine (SVM) target, and status.

Steps

1. From a PowerShell command line, establish a session with SnapCenter by entering *Open-SmConnection*.
2. Retrieve information about the EMS data collection schedule by entering *Get-SmDataCollectionEmsSchedule*.
3. Retrieve information about the EMS data collection status by entering *Get-SmDataCollectionEmsStatus*.
4. Retrieve information about the EMS data collection target by entering *Get-SmDataCollectionEmsTarget*.

Find more information

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Copyright information

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

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

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

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

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

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

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

Trademark information

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