Work with file services

NetApp Keystone

NetApp
March 11, 2021

Table of Contents

Overview

This section describes how to manage your file servers and NFS/CIFS file shares. You can view information about your file servers and share, create, modify, and delete them.

View servers

The Servers list displays the file servers belonging to the selected tenant. To view the list, select File Services > Servers from the menu.

The list displays simple information about each server such as:

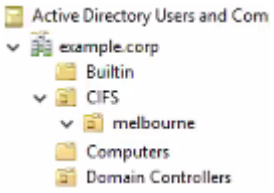
- Server name
- IP address
- Subtenant
- Zone
- Operational state
- Protocols in use (NFS, CIFS)
- The CIFS server name (if relevant).

  For more information on how to use the features of a list, see List view.

Create a file server

File servers belong to a subtenant and are created within a zone. When creating a server, you can optionally:

- Enable disaster recovery DP for the server. For more information about how disaster recovery works in NetApp Service Engine, see Disaster recovery.
- Make it CIFS-enabled. For CIFS-enabled servers:
  - You must provide the Active Directory user name, Active Directory password, domain, DNS servers, server name and, optionally, the Active Directory Organizational Unit (OU).
  - The Active Directory credentials (Active Directory user name and Active Directory password) must be for a user that has the privilege to join a computer to the Active Directory domain.
  - When the Active Directory OU structure is hierarchical, as shown in the image below, specify the OUs from the lowest level to the top. In this example, to specify the Melbourne OU, set `cifs_ou` as `"cifs_ou": "ou=melbourne,ou=cifs".`



Before you begin

Make sure you have the following to create the server:

- The subtenant that will host the server.
- The region and zone in which the server belongs.
- Networking details such as the VLAN ID, subnet, IP address (optional), and gateway (optional). If you are unfamiliar with your network, check with your IT department for the appropriate values.
- To enable asynchronous disaster recovery on the file server, the disaster recovery zone (the zone to which the file server will be replicated).

Steps

1. View the File Servers list.
2. Click **Create Server**.
3. On the Create Server page complete the following fields:

Field	Description
Subtenant	Select the Subtenant from the list.
Region	Select the region in which the server will reside.
Zone	Select the zone in which the server will reside.
Name	Enter the server name.
VLAN	Specify the VLAN id and subnet.
Subnet	
IP address	(Optional) Specify an IP address. If not specified, the server will be given the next available IP address.
Gateway	(Optional)

4. Select the services:

   NFS is enabled by default. The NFS protocol in use is displayed.

   If creating a CIFS-enabled file server:

   a. Toggle the CIFS-enabled button to view the CIFS related fields.
   b. Complete the Active Directory Username, Active Directory Password, Domain, DNS Servers, Server Name and, optionally, the Active Directory Organizational Unit. The Active Directory credentials must be for a user that has the privilege to join a computer to the Active Directory domain.

5. To enable asynchronous disaster recovery DP on this file server:
   a. Toggle the Asynchronous Disaster Recovery button to enable it.
   b. Select the disaster recovery region and zone.
   c. Select the disaster recovery replication schedule.
6. If synchronous disaster recovery DP is enabled, the Synchronous Disaster Recovery toggle is enabled and cannot be disabled.

7. Click **Create**. This creates a job to create the server.

After you finish

Create server is run as an asynchronous job. You can:

- Check the status of the job in the jobs list.
- After the job is finished, check the status of the server in the Servers list.

Modify file server

You can make the following changes to an existing server:

1. Change the server name
2. Make the server CIFS-enabled, and specify the Active Directory user name and password, Active Directory domain, DNS Server, Server name and optionally the Active Directory Organizational Unit. The Active Directory credentials must be for a user that has the privilege to join a computer to the Active Directory domain.
3. Enable asynchronous disaster recovery DP by specifying a region or zone to replicate the server to.

If asynchronous disaster recovery is already enabled, it cannot be disabled. For more information, see Disaster recovery.

Steps

1. View the File Servers list.
2. Locate the server in the list and click the Edit icon for that server. (For details about working with items in lists, see List view actions).
3. Make any changes as required; refer to Create a file server for field descriptions.
4. Click **Done**. This creates a job to modify the server.

After you finish

Modify server is run as an asynchronous job. You can:

- Check the status of the job in the jobs list. For information about tracking jobs, see here.
- After the job is finished, check the status of the sever in the Servers list.

Delete file server

Attention: Deleting a file server will also delete the following:

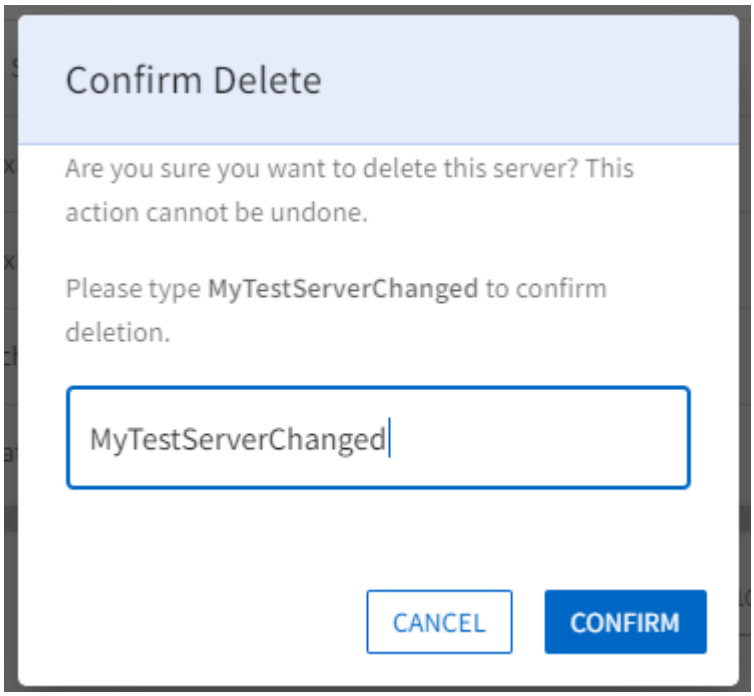
- All backups associated with the file server
- All disaster recovery replicated copies associated with the file serverYou cannot undo deletion of a server.

Before you begin

To delete a file server, you must first delete all shares that exist on the server.

Steps

1. View the File Servers list.
2. Locate the server in the list and click the Delete icon for that server. (For details about working with items in lists, see List view actions).
3. In the Confirm Delete dialog box, enter the file server name to confirm that you want to delete the file server.



4. Click **Confirm**. This creates a job to delete the server.

After you finish

- When deleting CIFS-enabled file servers, the Active Directory computer object remains. Ask your Active Directory administrator to manually remove the computer object for the deleted file server from Active Directory.
- Delete server is run as an asynchronous job. You can:
  - Check the status of the job in the jobs list. For information about tracking jobs, see here.
  - After the job is finished, verify that the sever has been removed from the Servers list.

View file shares

The **Shares** list displays the file shares belonging to the selected Tenant. To view the list, select **FILE SERVICES > Shares** from the menu.

The file shares that are already a part of your existing environment and belong to the storage VMs configured in your NetApp Service Engine, can also be viewed on this screen and be managed as a part of your NetApp Keystone Flex Subscription (Flex Subscription) services. The file shares provisioned outside of the NetApp Service Engine are periodically imported and listed on this page with appropriate status codes.

If the imported file shares are in acceptable standards of NetApp Service Engine, that is all the parameters that

are required for making the shares operational are available, they are imported with the status as `Operational` and can be directly managed through NetApp Service Engine. However, some shares might not be in the same standard as the existing shares on NetApp Service Engine. After import, these file shares are categorized with `Imported` or `Non-Standard` status. For understanding volume statuses and the steps to be taken to make them operational, see Object states

The Shares list displays simple information about each share. For more information about how to use the features of a list, see List view.

- Share name
- Server on which it resides
- Share path
- CIFS share path (used for mounting the CIFS share with DNS integration)
- Subtenant to which it belongs
- Zone in which it exists
- Service level
- Operational state (operational, updating, or contact support)
- Creation date

Create a file share

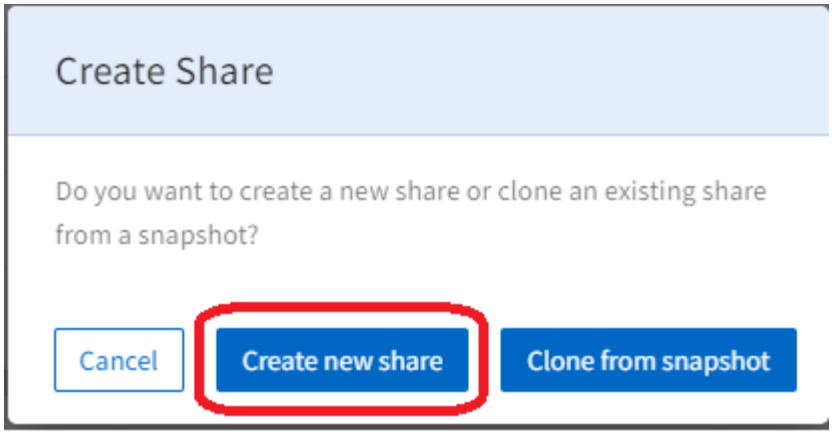
This section describes how to create a new share by directly specifying the share details. To create a new share based on a snapshot of an existing share, see Create Share from Snapshot.

Before you begin

- A share is created on a file server. The file server must exist and be in an operational state before you can create a new file share.
- For creating a CIFS or NFS file share, the server must be enabled for the respective service. For a multi-protocol file shares, the server should support both CIFS and NFS services.
- To enable asynchronous disaster recovery options for the share, you must create the share on a server that has asynchronous disaster recovery enabled. For more information, see Disaster recovery.
- To enable synchronous disaster recovery for a share, create the share in a zone that is MetroCluster-enabled.
- You can define a backup policy to capture backups of the file share on a scheduled basis. For more information, see Backups.
- You can define a snapshot policy to capture snapshots of the file share on a scheduled basis. For more information, see Snapshots.

Steps

1. Go to **FILE SERVICES > Shares**.
2. Click **Create Share**.
3. In the Create Share dialog box, select Create New Share.



The Create Share page is displayed.

4. Select the share type: NFS, CIFS, or Multi-protocol. The options are enabled based on the services that your server supports.
5. Complete the following fields:

Field	Description
Name	Enter the share name.
Share Path	Enter the path for the file share. For CIFS shares, adding a $ character to the end of the share path will make it a hidden share (for example, pathtomyhiddenshare$).
Region	Select the region in which the share resides.
Zone	Select the zone of the share.
File Server	Select the file server to host the share. The list of the file server depends on the region, zone, and share type selected.
Security Style	Select the security style applicable to the file share. This list is automatically populated based on the share type selected.

6. Select a Performance Service Level. The IOPS and throughput limits are displayed based on the service level selected.

Select an option to view the performance details for that level (as peak/expected IOPS/throughput). Select the service level that best matches your needs.

7. Specify the capacity of the file share.

NetApp Service Engine displays a warning and the capacity bar changes color if the specified capacity puts the consumed capacity into burst (or even more into burst if it is already in burst). The capacity check is performed against the total capacity for all subscriptions in the tenancy.

8. If asynchronous disaster recovery is enabled on the underlying file server, asynchronous disaster recovery replication is automatically enabled for the new share. If you wish to exclude the share from asynchronous

disaster recovery replication, toggle the Asynchronous Disaster Recovery button so that it is disabled.

9. If the share is being created in a zone that is MetroCluster-enabled, the Synchronous Disaster Recovery button is automatically enabled and cannot be disabled. The share will be replicated to the zone displayed in the panel below the Synchronous Disaster Recovery toggle.
10. If snapshots are required for this file share:
    a. Toggle to enable the Snapshot Policy and view the Snapshot Policy fields.
    b. Specify when to create the Snapshots:
        - **Hourly.** Specify which minute (of the hour) to take snapshot and the number of hourly snapshots to retain.
        - **Daily.** Specify when (hour and minute) to take the snapshot the number of daily snapshots to retain.
        - **Weekly.** Specify when (day of the week, hour, and minute) to take snapshot and the number of weekly snapshots to retain.
        - **Monthly.** Specify when (day of the month, hour, and minute) to take snapshot and the number of monthly snapshots to retain.
11. To enable backups for this file share:
    a. Toggle to enable the Backup Policy and the Backup Policy fields.
    b. Specify the backup zone.
    c. Specify how many of each type of backup to keep: daily, weekly, and/or monthly.
12. For NFS or multi-protocol shares, specify the Export Policy. You can apply multiple export policies on a share. This section is available for only NFS and multi-protocol shares.
    a. Add the IPv4 address (with a subnet mask expressed as a number of bits) of the client to which the rule applies.
    b. Specify the read and write access, and whether the client has root access (superuser).
13. For a CIFS (SMB) or multi-protocol shares, specify the Access Control List (ACL) for restricting user access. This section is available for only CIFS and multi-protocol shares.
    a. Specify the Windows user or group based on the Active Directory (AD) settings to add to the ACL. If you specify the user name, include the user's domain in the `<domain>\<username>` format. The default value is `Everyone`.
    b. Specify the Windows permission. The default value is `Full control`. If a user is a part of two groups, the permissions of the group that has higher privileges get applied on the user's access.

The user or group name should follow the standard AD format. If the entered user or group does not match the user or user group configured on ONTAP, the ACL validation fails during a CIFS operation, even when the file share is operational.

14. If you want to add tags (key-value pairs) to the file share, specify them in the Tags section.
15. Click **Create**. This creates a job to create the share.

After you finish

- For CIFs type shares only: to make the shares available by host name, your domain administrator must update the DNS records with the CIFS server name and IP address. Otherwise, the share is only accessible through the IP address. For example:

- With DNS records updated, use either the host name or IP to access the share: such as \\hostname\share or \\IP\share
- With no DNS records updated, you must use the IP address to access the share i.e. \\IP\share

- Create share is run as an asynchronous job. You can:
  - Check the status of the job in the jobs list.
  - After the job is finished, check the status of the share in the Shares list.

Create a file share from a Snapshot

You can create a new file share from an existing Snapshot. The new file share, cloned from the Snapshot, has the same properties as the file share from which the Snapshot is created.

Steps

1. Select **FILE SERVICES** from the left navigation pane and select **Shares**.
2. Click **Create Share** and select **Clone from snapshot**.
   The **Select Share** screen is displayed with all the file shares for the tenant. You can filter file shares by region, zone, and subtenant. You can select any file share that is in operational state.
3. Select the checkbox next to the file share that you want and click **Next**.
   The **Select Snapshot** screen is displayed with all the Snapshots for the file share.

   For the selected file share, if you have some Snapshots created in your SnapCenter environment outside of NetApp Service Engine, you can find these Snapshots imported and listed for your selection. You can select these imported Snapshots and clone the new file shares from them.

   You can search for a particular Snapshot or select the schedule type to filter the Snapshots.
4. Select the checkbox next to the Snapshot that you want to clone from and click **Next**.
   The new file share inherits the properties of the selected Snapshot.
5. Add **Name** and **Share Path**. Update the other settings, such as assigning a **Service Level**, and click **Create**.

After you finish

- For CIFs type shares only: To make the shares available by host name, your domain administrator should update the DNS records with the CIFS server name and IP address. Otherwise, the share is only accessible through the IP address. For example:
  - With DNS records updated, use either the host name or IP to access the share: such as \\hostname\share or \\IP\share
  - With no DNS records updated, you should use the IP address to access the share i.e. \\IP\share
- **Create Share** is run as an asynchronous job. You can:
  - Check the status of the job in the jobs list. For information about tracking jobs, see here.
  - After the job is finished, check the status of the share in the **Shares** list.

Modify a file share

You can change the share name, the share type (CIFS, NFS, multi-protocol), service level, capacity, snapshot policy, export policy, Access Control List (ACL), and tags.

Using this method, you can move your shares to different performance levels if available. You can change the share type only if the server supports the respective services.

Before you begin

The file share must be in the operational state. For understanding volume statuses and the steps to be taken to make them operational, see View disks and Object states

Steps

1. View the Shares list.
2. Locate the share in the list and click the Edit icon for that share. (For details about working with items in lists, see List view actions).
3. Make any changes as required; for field descriptions, see Create a new file share.
4. Click **Done**. This creates a job to modify the share.

After you finish

Modify share is run as an asynchronous job. You can:

- Check the status of the job in the jobs list. For information about tracking jobs, see here.
- After the job is finished, check the status of the share in the Shares list.

Delete a file share

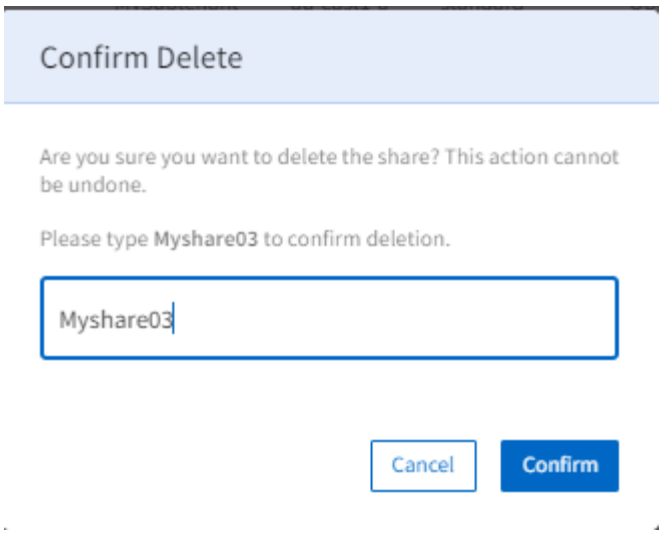
This section describes how to delete a file share.

Attention:

- You cannot undo deletion of a share. After it is deleted, data cannot be recovered.
- Deleting a primary file share will delete all associated backups

Steps

1. View the Shares list.
2. Locate the share in the list and click the Delete icon for that share. (For details about working with items in lists, see List view actions).
3. In the Confirm Delete dialog box, enter the file share name to confirm that you want to delete the file share.



4. Click **Confirm**. This creates a job to delete the share.

After you finish

Delete share is run as an asynchronous job. You can:

- Check the status of the job in the jobs list. For information about tracking jobs, see here.
- After the job is finished, verify that the share has been removed from the Shares list.

Create adhoc snapshot of a file share

This section describes how to create an adhoc snapshot of a file share.

Steps

1. View the Shares list.
2. Locate the share in the list and click the Snapshot icon for that share. (For details about working with items in lists, see List view actions.
3. In the Create Snapshot dialog, enter a name for your snapshot and click **Create**.

After you finish

The snapshot can take a few minutes to become available.