Work with volume access groups and initiators

Element Software

NetApp
April 17, 2024

Table of Contents

Work with volume access groups and initiators

You can use iSCSI initiators or Fibre Channel initiators to access the volumes defined within volume access groups.

You can create access groups by mapping iSCSI initiator IQNs or Fibre Channel WWPNs in a collection of volumes. Each IQN that you add to an access group can access each volume in the group without requiring CHAP authentication.

There are two types of CHAP authentication methods:

- Account-level CHAP authentication: You can assign CHAP authentication for the account.
- Initiator-level CHAP authentication: You can assign unique CHAP target and secrets for specific initiators without being bound to single CHAP across a single account. This Initiator-level CHAP authentication replaces account level credentials.

Optionally, with per-initiator CHAP, you can enforce initiator authorization and per-initiator CHAP authentication. These options can be defined on a per-initiator basis and an access group can contain a mix of initiators with different options.

Each WWPN that you add to an access group enables Fibre Channel network access to the volumes in the access group.

Volume access groups have the following limits:

- A maximum of 64 IQNs or WWPNs are allowed in an access group.
- An access group can be made up of a maximum of 2000 volumes.
- An IQN or WWPN can belong to only one access group.
- A single volume can belong to a maximum of four access groups.

Find more information

- Create a volume access group
- Add volumes to an access group
- Remove volumes from an access group
- Create an initiator
- Edit an initiator
- Add a single initiator to a volume access group
- Add multiple initiators to a volume access group
- Remove initiators from an access group
- Delete an access group
- Delete an initiator

Create a volume access group

You can create volume access groups by mapping initiators to a collection of volumes for secured access. You can then grant access to the volumes in the group with an account CHAP initiator secret and target secret.

If you use initiator-based CHAP, you can add CHAP credentials for a single initiator in a volume access group, providing more security. This enables you to apply this option for volume access groups that already exist.

Steps

1. Click **Management** > **Access Groups**.
2. Click **Create Access Group**.
3. Enter a name for the volume access group in the **Name** field.
4. Add an initiator to the volume access group in one of the following ways:

Option	Description
Adding a Fibre Channel initiator	a. Under Add Initiators, select an existing Fibre Channel initiator from the Unbound Fibre Channel Initiators list. b. Click **Add FC Initiator**. You can create an initiator during this step if you click the **Create Initiator** link, enter an initiator name, and click **Create**. The system automatically adds the initiator to the Initiators list after you create it. A sample of the format is as follows: `5f:47:ac:c0:5c:74:d4:02`

Option	Description
Adding an iSCSI initiator	Under Add Initiators, select an existing initiator from the Initiators list. **Note:** You can create an initiator during this step if you click the **Create Initiator** link, enter an initiator name, and click **Create**. The system automatically adds the initiator to the Initiators list after you create it. A sample of the format is as follows: `iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b` You can find the initiator IQN for each volume by selecting **View Details** in the Actions menu for the volume on the **Management** > **Volumes** > **Active** list. When you modify an initiator, you can toggle the requiredCHAP attribute to True, which enables you to set the target initiator secret. For details, see API information about the ModifyInitiator API method. Manage storage with the Element API

5. **Optional:** Add more initiators as needed.
6. Under Add Volumes, select a volume from the **Volumes** list.

   The volume appears in the **Attached Volumes** list.

7. **Optional:** Add more volumes as needed.
8. Click **Create Access Group**.

Find more information

Add volumes to an access group

View individual access group details

You can view details for an individual access group, such as attached volumes and initiators, in a graphical format.

1. Click **Management** > **Access Groups**.
2. Click the Actions icon for an access group.
3. Click **View Details**.

Volume access group details

The Access Groups page on the Management tab provides information about volume access groups.

The following information is displayed:

- **ID**: The system-generated ID for the access group.
- **Name**: The name given to the access group when it was created.
- **Active Volumes**: The number of active volumes in the access group.
- **Compression**: The compression efficiency score for the access group.
- **Deduplication**: The deduplication efficiency score for the access group.
- **Thin Provisioning**: The thin provisioning efficiency score for the access group.
- **Overall Efficiency**: The overall efficiency score for the access group.
- **Initiators**: The number of initiators connected to the access group.

Add volumes to an access group

You can add volumes to a volume access group. Each volume can belong to more than one volume access group; you can see the groups that each volume belongs to on the **Active** volumes page.

You can also use this procedure to add volumes to a Fibre Channel volume access group.

1. Click **Management** > **Access Groups**.
2. Click the Actions icon for the access group you want to add volumes to.
3. Click the **Edit** button.
4. Under Add Volumes, select a volume from the **Volumes** list.

   You can add more volumes by repeating this step.

5. Click **Save Changes**.

Remove volumes from an access group

When you remove a volume from an access group, the group no longer has access to that volume.

Modifying CHAP settings in an account or removing initiators or volumes from an access group can cause initiators to lose access to volumes unexpectedly. To verify that volume access will not be lost unexpectedly, always logout iSCSI sessions that will be affected by an account or access group change, and verify that initiators can reconnect to volumes after any changes to initiator settings and cluster settings have been completed.

1. Click **Management** > **Access Groups**.
2. Click the Actions icon for the access group you want to remove volumes from.
3. Click **Edit**.
4. Under Add Volumes in the **Edit Volume Access Group** dialog box, click the arrow on the **Attached Volumes** list.
5. Select the volume you want to remove from the list and click the **x** icon to remove the volume from the list.

   You can remove more volumes by repeating this step.

6. Click **Save Changes**.

Create an initiator

You can create iSCSI or Fibre Channel initiators and optionally assign them aliases.

You can also assign initator-based CHAP attributes by using an API call. To add a CHAP account name and credentials per initiator, you must use the `CreateInitiator` API call to remove and add CHAP access and attributes. Initiator access can be restricted to one or more VLANs by specifying one or more virtualNetworkIDs via the `CreateInitiators` and `ModifyInitiators` API calls. If no virtual networks are specified, the initiator can access all networks.

For details, see the API reference information. Manage storage with the Element API

Steps

1. Click **Management** > **Initiators**.
2. Click **Create Initiator**.
3. Perform the steps to create a single initiator or multiple initiators:

Option	Steps
Create a single initiator	a. Click **Create a Single Initiator**. b. Enter the IQN or WWPN for the initiator in the **IQN/WWPN** field. c. Enter a friendly name for the initiator in the **Alias** field. d. Click **Create Initiator**.
Create multiple initiators	a. Click **Bulk Create Initiators**. b. Enter a list of IQNs or WWPNs in the text box. c. Click **Add Initiators**. d. Choose an initiator from the resulting list and click the corresponding Add icon in the **Alias** column to add an alias for the initiator. e. Click the check mark to confirm the new alias. f. Click **Create Initiators**.

Edit an initiator

You can change the alias of an existing initiator or add an alias if one does not already exist.

To add a CHAP account name and credentials per initiator, you must use the `ModifyInitiator` API call to remove and add CHAP access and attributes.

See Manage storage with the Element API.

Steps

1. Click **Management** > **Initiators**.
2. Click the Actions icon for the initiator you want to edit.
3. Click **Edit**.
4. Enter a new alias for the initiator in the **Alias** field.
5. Click **Save Changes**.

Add a single initiator to a volume access group

You can add an initiator to an existing volume access group.

When you add an initiator to a volume access group, the initiator has access to all volumes in that volume access group.

> You can find the initiator for each volume by clicking the Actions icon and then selecting **View Details** for the volume in the active volumes list.

If you use initiator-based CHAP, you can add CHAP credentials for a single initiator in a volume access group, providing more security. This enables you to apply this option for volume access groups that already exist.

Steps

1. Click **Management** > **Access Groups**.
2. Click the **Actions** icon for the access group you want to edit.
3. Click **Edit**.
4. To add a Fibre Channel initiator to the volume access group, perform the following steps:

   a. Under Add Initiators, select an existing Fibre Channel initiator from the **Unbound Fibre Channel Initiators** list.

   b. Click **Add FC Initiator**.

   > You can create an initiator during this step if you click the **Create Initiator** link, enter an initiator name, and click **Create**. The system automatically adds the initiator to the **Initiators** list after you create it.

   A sample of the format is as follows:

   ```
   5f:47:ac:c0:5c:74:d4:02
   ```

5. To add an iSCSI initiator to the volume access group, under Add Initiators, select an existing initiator from the **Initiators** list.

   > You can create an initiator during this step if you click the **Create Initiator** link, enter an initiator name, and click **Create**. The system automatically adds the initiator to the **Initiators** list after you create it.

   The accepted format of an initiator IQN is as follows: iqn.yyyy-mm, in which y and m are digits, followed by text which must only contain digits, lower-case alphabetic characters, a period (.), colon (:) or dash (-).

A sample of the format is as follows:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

> You can find the initiator IQN for each volume from the **Management** > **Volumes** Active Volumes page by clicking the Actions icon and then selecting **View Details** for the volume.

6. Click **Save Changes**.

Add multiple initiators to a volume access group

You can add multiple initiators to an existing volume access group to allow access to volumes in the volume access group with or without requiring CHAP authentication..

When you add initiators to a volume access group, the initiators have access to all volumes in that volume access group.

> You can find the initiator for each volume by clicking the Actions icon and then **View Details** for the volume in the active volumes list.

You can add multiple initiators to an existing volume access group to enable access to volumes and assign unique CHAP credentials for each initiator within that volume access group. This enables you to apply this option for volume access groups that already exist.

You can assign initator-based CHAP attributes by using an API call. To add a CHAP account name and credentials per initiator, you must use the ModifyInitiator API call to remove and add CHAP access and attributes.

For details, see Manage storage with the Element API.

Steps

1. Click **Management** > **Initiators**.
2. Select the initiators you want to add to an access group.
3. Click the **Bulk Actions** button.
4. Click **Add to Volume Access Group**.
5. In the Add to Volume Access Group dialog box, select an access group from the **Volume Access Group** list.
6. Click **Add**.

Remove initiators from an access group

When you remove an initiator from an access group, it can no longer access the volumes in that volume access group. Normal account access to the volume is not disrupted.

Modifying CHAP settings in an account or removing initiators or volumes from an access group can cause initiators to lose access to volumes unexpectedly. To verify that volume access will not be lost unexpectedly, always logout iSCSI sessions that will be affected by an account or access group change, and verify that

initiators can reconnect to volumes after any changes to initiator settings and cluster settings have been completed.

Steps

1. Click **Management** > **Access Groups**.
2. Click the **Actions** icon for the access group you want to remove.
3. In the resulting menu, select **Edit**.
4. Under Add Initiators in the **Edit Volume Access Group** dialog box, click the arrow on the **Initiators** list.
5. Select the x icon for each initiator you want to remove from the access group.
6. Click **Save Changes**.

Delete an access group

You can delete an access group when it is no longer needed. You do not need to delete Initiator IDs and Volume IDs from the volume access group before deleting the group. After you delete the access group, group access to the volumes is discontinued.

1. Click **Management** > **Access Groups**.
2. Click the **Actions** icon for the access group you want to delete.
3. In the resulting menu, click **Delete**.
4. To also delete the initiators associated with this access group, select the **Delete initiators in this access group** check box.
5. Confirm the action.

Delete an initiator

You can delete an initiator after it is no longer needed. When you delete an initiator, the system removes it from any associated volume access group. Any connections using the initiator remain valid until the connection is reset.

Steps

1. Click **Management** > **Initiators**.
2. Perform the steps to delete a single initiator or multiple initiators:

Option	Steps
Delete single initiator	a. Click the **Actions** icon for the initiator you want to delete. b. Click **Delete**. c. Confirm the action.

Option	Steps
Delete multiple initiators	a. Select the check boxes next to the initiators you want to delete. b. Click the **Bulk Actions** button. c. In the resulting menu, select **Delete**. d. Confirm the action.