Storage

HCI

NetApp
September 16, 2021

Table of Contents

Storage

Maintenance mode

If you need to take a storage node offline for maintenance such as software upgrades or host repairs, you can minimize the I/O impact to the rest of the storage cluster by enabling maintenance mode for that node. You can use maintenance mode with both appliance nodes as well as SolidFire Enterprise SDS nodes.

You can only transition a storage node to maintenance mode if the node is healthy (has no blocking cluster faults) and the storage cluster is tolerant to a single node failure. Once you enable maintenance mode for a healthy and tolerant node, the node is not immediately transitioned; it is monitored until the following conditions are true:

- All volumes hosted on the node have failed over
- The node is no longer hosting as the primary for any volume
- A temporary standby node is assigned for every volume being failed over

After these criteria are met, the node is transitioned to maintenance mode. If these criteria are not met within a 5 minute period, the node will not enter maintenance mode.

When you disable maintenance mode for a storage node, the node is monitored until the following conditions are true:

- All data is fully replicated to the node
- All blocking cluster faults are resolved
- All temporary standby node assignments for the volumes hosted on the node have been inactivated

After these criteria are met, the node is transitioned out of maintenance mode. If these criteria are not met within one hour, the node will fail to transition out of maintenance mode.

You can see the states of maintenance mode operations when working with maintenance mode using the Element API:

- **Disabled**: No maintenance has been requested.
- **FailedToRecover**: The node failed to recover from maintenance.
- **RecoveringFromMaintenance**: The node is in the process of recovering from maintenance.
- **PreparingForMaintenance**: Actions are being taken to allow a node to have maintenance performed.
- **ReadyForMaintenance**: The node is ready for maintenance to be performed.

Find more information

- NetApp Element API documentation
- NetApp HCI Resources page
- NetApp Element Plug-in for vCenter Server

Volumes

Storage is provisioned in the NetApp Element system as volumes. Volumes are block devices accessed over the network using iSCSI or Fibre Channel clients.

The NetApp Element Plug-in for vCenter Server enables you to create, view, edit, delete, clone, backup or restore volumes for user accounts. You can also manage each volume on a cluster, and add or remove volumes in volume access groups.

Persistent volumes

Persistent volumes allow management node configuration data to be stored on a specified storage cluster, rather than locally with a VM, so that data can be preserved in the event of management node loss or removal. Persistent volumes are an optional yet recommended management node configuration.

If you are deploying a management node for NetApp HCI using the NetApp Deployment Engine, persistent volumes are enabled and configured automatically.

An option to enable persistent volumes is included in the installation and upgrade scripts when deploying a new management node. Persistent volumes are volumes on an Element software-based storage cluster that contain management node configuration information for the host management node VM that persists beyond the life of the VM. If the management node is lost, a replacement management node VM can reconnect to and recover configuration data for the lost VM.

Persistent volumes functionality, if enabled during installation or upgrade, automatically creates multiple volumes with NetApp-HCI- pre-pended to the name on the assigned cluster. These volumes, like any Element software-based volume, can be viewed using the Element software web UI, NetApp Element Plug-in for vCenter Server, or API, depending on your preference and installation. Persistent volumes must be up and running with an iSCSI connection to the management node to maintain current configuration data that can be used for recovery.

Persistent volumes that are associated with management services are created and assigned to a new account during installation or upgrade. If you are using persistent volumes, do not modify or delete the volumes or their associated account

Find more information

- Manage volumes
- NetApp Element Plug-in for vCenter Server
- SolidFire and Element Software Documentation Center

Volume access groups

A volume access group is a collection of volumes that users can access using either iSCSI or Fibre Channel initiators.

By creating and using volume access groups, you can control access to a set of volumes. When you associate a set of volumes and a set of initiators with a volume access group, the access group grants those initiators access to that set of volumes.

Volume access groups have the following limits:

- A maximum of 128 initiators per volume access group.
- A maximum of 64 access groups per volume.
- An access group can be made up of a maximum of 2000 volumes.
- An IQN or WWPN can belong to only one volume access group.

Find more information

- Manage volume access groups
- NetApp Element Plug-in for vCenter Server
- SolidFire and Element Software Documentation Center

Initiators

Initiators enable external clients access to volumes in a cluster, serving as the entry point for communication between clients and volumes. You can use initiators for CHAP-based rather than account-based access to storage volumes. A single initiator, when added to a volume access group, allows volume access group members to access all storage volumes added to the group without requiring authentication. An initiator can belong to only one access group.

Find more information

- Manage initiators
- Volume access groups
- Manage volume access groups
- NetApp Element Plug-in for vCenter Server
- SolidFire and Element Software Documentation Center

Custom protection domains

You can define a custom protection domain layout, where each node is associated with one and only one custom protection domain. By default, each node is assigned to the same default custom protection domain.

If no custom protection domains are assigned:

- Cluster operation is unaffected.
- Custom level is neither tolerant nor resilient.

If more than one custom protection domain is assigned, each subsystem will assign duplicates to separate custom protection domains. If this is not possible, it reverts to assigning duplicates to separate nodes. Each subsystem (for example, bins, slices, protocol endpoint providers, and ensemble) does this independently.

Using custom protection domains assumes that no nodes share a chassis.

The following Element API methods expose these new protection domains:

- GetProtectionDomainLayout - shows which chassis and which custom protection domain each node is in.
- SetProtectionDomainLayout - allows a custom protection domain to be assigned to each node.

Contact NetApp support for further details on using custom protection domains.

Find more information

Manage storage with the Element API