Concepts

HCI

NetApp
December 11, 2020

Table of Contents

Concepts

NetApp HCI product overview

NetApp HCI is an enterprise-scale hybrid cloud infrastructure design that combines storage, compute, networking, and hypervisor—and adds capabilities that span public and private clouds.

NetApp's disaggregated hybrid cloud infrastructure allows independent scaling of compute and storage, adapting to workloads with guaranteed performance.

- Meets hybrid multicloud demand
- Scales compute and storage independently
- Simplifies data services orchestration across hybrid multiclouds

Components of NetApp HCI

Here is an overview of the various components of the NetApp HCI environment:

- NetApp HCI provides both storage and compute resources. You use the **NetApp Deployment Engine** wizard to deploy NetApp HCI. After successful deployment, compute nodes appear as ESXi hosts and you can manage them in VMware vSphere Web Client.
- **Management services** or microservices include the Active IQ collector, QoSSIOC for the vCenter Plug-in, and mNode service; they are updated frequently as service bundles. As of the Element 11.3 release, **management services** are hosted on the management node, allowing for quicker updates of select software services outside of major releases. The **management node** (mNode) is a virtual machine that runs in parallel with one or more Element software-based storage clusters. It is used to upgrade and provide system services including monitoring and telemetry, manage cluster assets and settings, run system tests and utilities, and enable NetApp Support access for troubleshooting.

  Learn more about management services releases.

- **NetApp Hybrid Cloud Control** enables you to manage NetApp HCI. You can upgrade management services, expand your system, collect logs, and monitor your installation by using NetApp SolidFire Active IQ. You log in to NetApp Hybrid Cloud Control by browsing to the IP address of the management node.
- The **NetApp Element Plug-in for vCenter Server** (VCP) is a web-based tool integrated with the vSphere user interface (UI). The plug-in is an extension and scalable, user-friendly interface for VMware vSphere that can manage and monitor storage clusters running **NetApp Element software**. The plug-in provides an alternative to the Element UI. You can use the plug-in user interface to discover and configure clusters, and to manage, monitor, and allocate storage from

cluster capacity to configure datastores and virtual datastores (for virtual volumes). A cluster appears on the network as a single local group that is represented to hosts and administrators by virtual IP addresses. You can also monitor cluster activity with real-time reporting, including error and alert messaging for any event that might occur while performing various operations.

Learn more about VCP.

- By default, NetApp HCI sends performance and alert statistics to the **NetApp SolidFire Active IQ** service. As part of your normal support contract, NetApp Support monitors this data and alerts you to any performance bottlenecks or potential system issues. You need to create a NetApp Support account if you do not already have one (even if you have an existing SolidFire Active IQ account) so that you can take advantage of this service.

Learn more about NetApp SolidFire Active IQ.

NetApp HCI URLs

Here are the common URLs you use with NetApp HCI:

URL	Description
`https://[IPv4 address of Bond1G interface on a storage node]`	Access the NetApp Deployment Engine wizard to install and configure NetApp HCI. Learn more.
`https://[management node IP address]`	Access NetApp Hybrid Cloud Control to upgrade, expand, and monitor your NetApp HCI installation, and update management services. Learn more.
`https://[IP address]:442`	From the per-node UI, access network and cluster settings and utilize system tests and utilities. Learn more.
`https://[management node IP address]:9443`	Register the vCenter Plug-in package in the vSphere Web Client.
`https://activeiq.solidfire.com`	Monitor data and receive alerts to any performance bottlenecks or potential system issues.
`https://[management node IP address]/mnode`	Manually update management services using the REST API UI from the management node.
`https://[storage cluster MVIP address]`	Access the NetApp Element software UI.

Find more information

- NetApp HCI Documentation Center

- NetApp HCI Resources page

User accounts

To access storage resources on your system, you'll need to set up user accounts.

User account management

User accounts are used to control access to the storage resources on a NetApp Element software-based network. At least one user account is required before a volume can be created.

When you create a volume, it is assigned to an account. If you have created a virtual volume, the account is the storage container.

Here are some additional considerations:

- The account contains the CHAP authentication required to access the volumes assigned to it.
- An account can have up to 2000 volumes assigned to it, but a volume can belong to only one account.
- User accounts can be managed from the NetApp Element Management extension point.

Using NetApp Hybrid Cloud Control, you can create and manage the following types of accounts:

- Administrator user accounts for the storage cluster
- Authoritative user accounts
- Volume accounts, specific only to the storage cluster on which they were created.

Storage cluster administrator accounts

There are two types of administrator accounts that can exist in a storage cluster running NetApp Element software:

- **Primary cluster administrator account**: This administrator account is created when the cluster is created. This account is the primary administrative account with the highest level of access to the cluster. This account is analogous to a root user in a Linux system. You can change the password for this administrator account.
- **Cluster administrator account**: You can give a cluster administrator account a limited range of administrative access to perform specific tasks within a cluster. The credentials assigned to each cluster administrator account are used to authenticate API and Element UI requests within the storage system.

A local (non-LDAP) cluster administrator account is required to access active nodes in a cluster via the per-node UI. Account credentials are not required to access a node that is not yet part of a cluster.

You can manage cluster administrator accounts by creating, deleting, and editing cluster administrator accounts, changing the cluster administrator password, and configuring LDAP settings to manage system access for users.

For details, see the SolidFire and Element Documentation Center.

Authoritative user accounts

Authoritative user accounts can authenticate against any storage asset associated with the NetApp Hybrid Cloud Control instance of nodes and clusters. With this account, you can manage volumes, accounts, access groups, and more across all clusters.

Authoritative user accounts are managed from the top right menu User Management option in NetApp Hybrid Cloud Control.

The authoritative storage cluster is the storage cluster that NetApp Hybrid Cloud Control uses to authenticate users.

All users created on the authoritative storage cluster can log into the NetApp Hybrid Cloud Control. Users created on other storage clusters *cannot* log into Hybrid Cloud Control.

- If your management node only has one storage cluster, then it is the authoritative cluster.
- If your management node has two or more storage clusters, one of those clusters is assigned as the authoritative cluster and only users from that cluster can log into NetApp Hybrid Cloud Control.

While many NetApp Hybrid Cloud Control features work with multiple storage clusters, authentication and authorization have necessary limitations. The limitation around authentication and authorization is that users from the authoritative cluster can execute actions on other clusters tied to NetApp Hybrid Cloud Control even if they are not a user on the other storage clusters. Before proceeding with managing multiple storage clusters, you should ensure that users defined on the authoritative clusters are defined on all other storage clusters with the same permissions. You can manage users from NetApp Hybrid Cloud Control.

Volume accounts

Volume-specific accounts are specific only to the storage cluster on which they were created. These accounts enable you to set permissions on specific volumes across the network, but have no effect outside of those volumes.

Volume accounts are managed within the NetApp Hybrid Cloud Control Volumes table.

Find more information

- Manage user accounts
- Learn about clusters
- SolidFire and Element Documentation Center
- NetApp HCI Resources page
- NetApp HCI Documentation Center
- SolidFire and Element Documentation Center

Data protection

NetApp HCI data protection terms include different types of remote replication, volume snapshots, volume cloning, protection domains, and high availability with double Helix technology.

NetApp HCI data protection includes the following concepts:

- Remote replication types
- Volume snapshots for data protection
- Volume clones
- Backup and restore process overview for SolidFire storage
- Protection domains
- Double Helix high availability

Remote replication types

Remote replication of data can take the following forms:

- Synchronous and asynchronous replication between clusters
- Snapshot-only replication
- Replication between Element and ONTAP clusters using SnapMirror

See TR-4741: NetApp Element Software Remote Replication.

Synchronous and asynchronous replication between clusters

For clusters running NetApp Element software, real-time replication enables the quick creation of remote copies of volume data.

You can pair a storage cluster with up to four other storage clusters. You can replicate volume data synchronously or asynchronously from either cluster in a cluster pair for failover and failback

scenarios.

Synchronous replication

Synchronous replication continuously replicates data from the source cluster to the target cluster and is affected by latency, packet loss, jitter, and bandwidth.

Synchronous replication is appropriate for the following situations:

- Replication of several systems over a short distance
- A disaster recovery site that is geographically local to the source
- Time-sensitive applications and the protection of databases
- Business continuity applications that require the secondary site to act as the primary site when the primary site is down

Asynchronous replication

Asynchronous replication continuously replicates data from a source cluster to a target cluster without waiting for the acknowledgments from the target cluster. During asynchronous replication, writes are acknowledged to the client (application) after they are committed on the source cluster.

Asynchronous replication is appropriate for the following situations:

- The disaster recovery site is far from the source and the application does not tolerate latencies induced by the network.
- There are bandwidth limitations on the network connecting the source and target clusters.

Snapshot-only replication

Snapshot-only data protection replicates changed data at specific points of time to a remote cluster. Only those snapshots that are created on the source cluster are replicated. Active writes from the source volume are not.

You can set the frequency of the snapshot replications.

Snapshot replication does not affect asynchronous or synchronous replication.

Replication between Element and ONTAP clusters using SnapMirror

With NetApp SnapMirror technology, you can replicate snapshots that were taken using NetApp Element software to ONTAP for disaster recovery purposes. In a SnapMirror relationship, Element is one endpoint and ONTAP is the other.

SnapMirror is a NetApp Snapshot™ replication technology that facilitates disaster recovery, designed for failover from primary storage to secondary storage at a geographically remote site. SnapMirror technology creates a replica, or mirror, of the working data in secondary storage from which you can

continue to serve data if an outage occurs at the primary site. Data is mirrored at the volume level.

The relationship between the source volume in primary storage and the destination volume in secondary storage is called a data protection relationship. The clusters are referred to as endpoints in which the volumes reside and the volumes that contain the replicated data must be peered. A peer relationship enables clusters and volumes to exchange data securely.

SnapMirror runs natively on the NetApp ONTAP controllers and is integrated into Element, which runs on NetApp HCI and SolidFire clusters. The logic to control SnapMirror resides in ONTAP software; therefore, all SnapMirror relationships must involve at least one ONTAP system to perform the coordination work. Users manage relationships between Element and ONTAP clusters primarily through the Element UI; however, some management tasks reside in NetApp ONTAP System Manager. Users can also manage SnapMirror through the CLI and API, which are both available in ONTAP and Element.

See TR-4651: NetApp SolidFire SnapMirror Architecture and Configuration (login required)

You must manually enable SnapMirror functionality at the cluster level by using Element software. SnapMirror functionality is disabled by default, and it is not automatically enabled as part of a new installation or upgrade.

After enabling SnapMirror, you can create SnapMirror relationships from the Data Protection tab in the Element software.

Volume snapshots for data protection

A volume snapshot is a point-in-time copy of a volume that you could later use to restore a volume to that specific time.

While snapshots are similar to volume clones, snapshots are simply replicas of volume metadata, so you cannot mount or write to them. Creating a volume snapshot also takes only a small amount of system resources and space, which makes snapshot creation faster than cloning.

You can replicate snapshots to a remote cluster and use them as a backup copy of the volume. This enables you to roll back a volume to a specific point in time by using the replicated snapshot; you can also create a clone of a volume from a replicated snapshot.

You can back up snapshots from a SolidFire cluster to an external object store, or to another SolidFire cluster. When you back up a snapshot to an external object store, you must have a connection to the object store that allows read/write operations.

You can take a snapshot of an individual volume or multiple for data protection.

Volume clones

A clone of a single volume or multiple volumes is point-in-time copy of the data. When you clone a volume, the system creates a snapshot of the volume and then creates a copy of the data referenced by

the snapshot.

This is an asynchronous process, and the amount of time the process requires depends on the size of the volume you are cloning and the current cluster load.

The cluster supports up to two running clone requests per volume at a time and up to eight active volume clone operations at a time. Requests beyond these limits are queued for later processing.

Backup and restore process overview for SolidFire storage

You can back up and restore volumes to other SolidFire storage, as well as to secondary object stores that are compatible with Amazon S3 or OpenStack Swift.

You can back up a volume to the following:

- A SolidFire storage cluster
- An Amazon S3 object store
- An OpenStack Swift object store

When you restore volumes from OpenStack Swift or Amazon S3, you need manifest information from the original backup process. If you are restoring a volume that was backed up on a SolidFire storage system, no manifest information is required.

Protection domains

A protection domain is a node or a set of nodes grouped together such that any part or even all of it might fail, while maintaining data availability. Protection domains enable a storage cluster to heal automatically from the loss of a chassis (chassis affinity) or an entire domain (group of chassis).

A protection domain layout assigns each node to a specific protection domain.

Two different protection domain layouts, called protection domain levels, are supported.

- At the node level, each node is in its own protection domain.
- At the chassis level, only nodes that share a chassis are in the same protection domain.
    - The chassis level layout is automatically determined from the hardware when the node is added to the cluster.
    - In a cluster where each node is in a separate chassis, these two levels are functionally identical.

You can manually enable protection domain monitoring using the NetApp Element Configuration extension point in the NetApp Element Plug-in for vCenter Server. You can select a protection domain threshold based on node or chassis domains.

When creating a new cluster, if you are using storage nodes that reside in a shared chassis, you might want to consider designing for chassis-level failure protection using the protection domains feature.

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. For details, see
SolidFire and Element 12.0 Documentation Center.

Double Helix high availability

Double Helix data protection is a replication method that spreads at least two redundant copies of data across all drives within a system. The “RAID-less” approach enables a system to absorb multiple, concurrent failures across all levels of the storage system and repair quickly.

Find more information

- NetApp HCI Resources page
- NetApp HCI Documentation Center

Clusters

A cluster is a group of nodes, functioning as a collective whole, that provide storage or compute resources. Starting with NetApp HCI 1.8, you can have a storage cluster with two nodes. A storage cluster appears on the network as a single logical group and can then be accessed as block storage.

The storage layer in NetApp HCI is provided by NetApp Element software and the management layer is provided by the NetApp Element Plug-in for vCenter Server. A storage node is a server containing a collection of drives that communicate with each other through the Bond10G network interface. Each storage node is connected to two networks, storage and management, each with two independent links for redundancy and performance. Each node requires an IP address on each network. You can create a cluster with new storage nodes, or add storage nodes to an existing cluster to increase storage capacity and performance.

Authoritative storage clusters

The authoritative storage cluster is the storage cluster that NetApp Hybrid Cloud Control uses to authenticate users.

If your management node only has one storage cluster, then it is the authoritative cluster. If your management node has two or more storage clusters, one of those clusters is assigned as the authoritative cluster and only users from that cluster can log into NetApp Hybrid Cloud Control. To find out which cluster is the authoritative cluster, you can use the `GET /mnode/about` API. In the response, the IP address in the `token_url` field is the management virtual IP address (MVIP) of the authoritative storage cluster. If you attempt to log into NetApp Hybrid Cloud Control as a user that is not on the authoritative cluster, the login attempt will fail.

Many NetApp Hybrid Cloud Control features are designed to work with multiple storage clusters, but authentication and authorization have limitations. The limitation around authentication and authorization is that the user from the authoritative cluster can execute actions on other clusters tied to NetApp Hybrid Cloud Control even if they are not a user on the other storage clusters. Before proceeding with managing multiple storage clusters, you should ensure that users defined on the authoritative clusters are defined on all other storage clusters with the same permissions.

You can manage users with NetApp Hybrid Cloud Control.

Before proceeding with managing multiple storage clusters, you should ensure that users defined on the authoritative clusters are defined on all other storage clusters with the same permissions. You can manage users from the Element software user interface (Element web UI).

See Create and manage storage cluster assets for more information on working with management node storage cluster assets.

Stranded capacity

If a newly added node accounts for more than 50 percent of the total cluster capacity, some of the capacity of this node is made unusable ("stranded"), so that it complies with the capacity rule. This remains the case until more storage capacity is added. If a very large node is added that also disobeys the capacity rule, the previously stranded node will no longer be stranded, while the newly added node becomes stranded. Capacity should always be added in pairs to avoid this from happening. When a node becomes stranded, an appropriate cluster fault is thrown.

Two-node storage clusters

Starting with NetApp HCI 1.8, you can set up a storage cluster with two storage nodes.

- You can use certain types of nodes to form the two-node storage cluster. See NetApp HCI 1.8 Release Notes.

  The storage nodes in a two-node cluster must be the same model type.

- Two-node storage clusters are best suited for small-scale deployments with workloads that are not dependent on large capacity and high performance requirements.
- In addition to two storage nodes, a two-node storage cluster also includes two **NetApp HCI Witness Nodes**.

  Learn more about Witness Nodes.

- You can scale a two-node storage cluster to a three-node storage cluster. Three-node clusters increase resiliency by providing the ability to auto-heal from storage node failures.
- Two-node storage clusters provide the same security features and functionality as the traditional four-node storage clusters.

- Two-node storage clusters use the same networks as four-node storage clusters. The networks are set up during NetApp HCI deployment using the NetApp Deployment Engine wizard.

Storage cluster quorum

Element software creates a storage cluster from selected nodes, which maintains a replicated database of the cluster configuration. A minimum of three nodes are required to participate in the cluster ensemble to maintain quorum for cluster resiliency. Witness Nodes in a two-node cluster are used to ensure that there are enough storage nodes to form a valid ensemble quorum. For ensemble creation, storage nodes are preferred over Witness Nodes. For the minimum three-node ensemble involving a two-node storage cluster, two storage nodes and one Witness Node are used.

In a three-node ensemble with two storage nodes and one Witness Node, if one storage node goes offline, the cluster goes into a degraded state. Of the two Witness Nodes, only one can be active in the ensemble. The second Witness Node cannot be added to the ensemble, because it performs the backup role. The cluster stays in degraded state until the offline storage node returns to an online state, or a replacement node joins the cluster.

If a Witness Node fails, the remaining Witness Node joins the ensemble to form a three-node ensemble. You can deploy a new Witness Node to replace the failed Witness Node.

Auto-healing and failure handling in two-node storage clusters

If a hardware component fails in a node that is part of a traditional cluster, the cluster can rebalance data that was on the component that failed to other available nodes in the cluster. This ability to automatically heal is not available in a two-node storage cluster, because a minimum of three physical storage nodes must be available to the cluster for healing automatically. When one node in a two-node cluster fails, the two-node cluster does not require regeneration of a second copy of data. New writes are replicated for block data in the remaining active storage node. When the failed node is replaced and joins the cluster, the data is rebalanced between the two physical storage nodes.

Storage clusters with three or more nodes

Expanding from two storage nodes to three storage nodes makes your cluster more resilient by allowing auto-healing in the event of node and drive failures, but does not provide additional capacity. You can expand using the NetApp Hybrid Cloud Control UI. When expanding from a two-node cluster to a three-node cluster, capacity can be stranded (see Stranded capacity). The UI wizard shows warnings about stranded capacity before installation. A single Witness Node is still available to keep the ensemble quorum in the event of a storage node failure, with a second Witness Node on standby.
When you expand a three-node storage cluster to a four-node cluster, capacity and performance are increased. In a four-node cluster, Witness Nodes are no longer needed to form the cluster quorum.
You can expand to up to 64 compute nodes and 40 storage nodes.

Find more information

- NetApp HCI Two-Node Storage Cluster | TR-4823
- NetApp HCI Documentation Center
- SolidFire and Element Software Documentation Center

Nodes

Nodes are hardware or virtual resources that are grouped into a cluster to provide block storage and compute capabilities.

NetApp HCI and Element software defines various node roles for a cluster. The four types of node roles are **management node**, **storage node**, **compute node**, and **NetApp HCI Witness Nodes**.

Management node

The management node (sometimes abbreviated as mNode) interacts with a storage cluster to perform management actions, but is not a member of the storage cluster. Management nodes periodically collect information about the cluster through API calls and report this information to Active IQ for remote monitoring (if enabled). Management nodes are also responsible for coordinating software upgrades of the cluster nodes.

The management node is a virtual machine that runs in parallel with one or more Element software-based storage clusters. In addition to upgrades, it is used to provide system services including monitoring and telemetry, manage cluster assets and settings, run system tests and utilities, and enable NetApp Support access for troubleshooting. As of the Element 11.3 release, the management node functions as a microservice host, allowing for quicker updates of select software services outside of major releases. These microservices or management services, such as the Active IQ collector, QoSSIOC for the vCenter Plug-in, and management node service, are updated frequently as service bundles.

Storage nodes

NetApp HCI storage nodes are hardware that provide the storage resources for a NetApp HCI system. Drives in the node contain block and metadata space for data storage and data management. Each node contains a factory image of NetApp Element software. NetApp HCI storage nodes can be managed using the NetApp Element Management extension point.

Compute nodes

NetApp HCI compute nodes are hardware that provides compute resources, such as CPU, memory, and networking, that are needed for virtualization in the NetApp HCI installation. Because each server runs VMware ESXi, NetApp HCI compute node management (adding or removing hosts) must be done outside of the plug-in within the Hosts and Clusters menu in vSphere. Regardless of whether it is a four-node storage cluster or a two-node storage cluster, the minimum number of compute nodes

remains two for a NetApp HCI deployment.

Witness Nodes

NetApp HCI Witness Nodes are virtual machines that run on compute nodes in parallel with an Element software-based storage cluster. Witness Nodes do not host slice or block services. A Witness Node enables storage cluster availability in the event of a storage node failure. You can manage and upgrade Witness Nodes in the same way as other storage nodes. A storage cluster can have up to four Witness Nodes. Their primary purpose is to ensure that enough cluster nodes exist to form a valid ensemble quorum.

Learn more about Witness Node resource requirements and Witness Node IP address requirements.

In a two-node storage cluster, a minimum of two Witness Nodes are deployed for redundancy in the event of a Witness Node failure. When the NetApp HCI installation process installs Witness Nodes, a virtual machine template is stored in VMware vCenter that you can use to redeploy a Witness Node in case it is accidentally removed, lost, or corrupted. You can also use the template to redeploy a Witness Node if you need to replace a failed compute node that was hosting the Witness Node. For instructions, see the **Redeploy Witness Nodes for two and three-node storage clusters** section here.

Find more information

- NetApp HCI Two-Node Storage Cluster | TR-4823
- NetApp HCI Documentation Center
- SolidFire and Element Software Documentation Center

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 HCI Documentation Center

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 HCI Documentation Center
- 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 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

- Manage volume access groups
- NetApp HCI Documentation Center
- SolidFire and Element Software Documentation Center

NetApp HCI licensing

When you use NetApp HCI, you might need additional licenses depending on what you are using.

NetApp HCI and VMware vSphere licensing

VMware vSphere licensing depends on your configuration:

Networking option	Licensing
Option A: Two cables for compute nodes using VLAN tagging (All compute nodes)	Requires use of vSphere Distributed Switch, which requires VMware vSphere Enterprise Plus licensing.
Option B: Six cables for compute nodes using tagged VLANs (H410C 2RU 4-Node compute node)	This configuration uses vSphere Standard Switch as the default. Optional use of vSphere Distributed Switch requires VMware Enterprise Plus licensing.
Option C: Six cables for compute nodes using native and tagged VLANs (H410C, 2RU 4-Node Compute Node)	This configuration uses vSphere Standard Switch as the default. Optional use of vSphere Distributed Switch requires VMware Enterprise Plus licensing.

NetApp HCI and ONTAP Select licensing

If you were provided a version of ONTAP Select for use in conjunction with a purchased NetApp HCI system, the following additional limitations apply:

- The ONTAP Select license, which is bundled with a NetApp HCI system sale, may only be used in conjunction with NetApp HCI compute nodes.
- The storage for those ONTAP Select instances must reside only on the NetApp HCI storage nodes.
- The use of third-party compute nodes or third-party storage nodes is prohibited.

Find more information

- NetApp HCI Documentation Center
- SolidFire and Element Software Documentation Center

NetApp HCI security

When you use NetApp HCI, your data is protected by industry-standard security protocols.

Encryption at Rest for storage nodes

NetApp HCI enables you to encrypt all data stored on the storage cluster.

All drives in storage nodes that are capable of encryption use AES 256-bit encryption at the drive level. Each drive has its own encryption key, which is created when the drive is first initialized. When you enable the encryption feature, a storage-cluster-wide password is created, and chunks of the password are then distributed to all nodes in the cluster. No single node stores the entire password. The password is then used to password-protect all access to the drives. You need the password to unlock the drive, and since the drive is encrypting all data, your data is secure at all times.

When you enable Encryption at Rest, performance and efficiency of the storage cluster are unaffected. Additionally, if you remove an encryption-enabled drive or node from the storage cluster with the Element API or Element UI, Encryption at Rest is disabled on the drives and the drives are securely erased, protecting the data that was previously stored on those drives. After you remove the drive, you can securely erase the drive with the `SecureEraseDrives` API method. If you forcibly remove a drive or node from the storage cluster, the data remains protected by the cluster-wide password and the drive's individual encryption keys.

For information on enabling and disabling Encryption at Rest, see Enabling and disabling encryption for a cluster in the SolidFire and Element Documentation Center.

Software Encryption at Rest

Software Encryption at Rest enables all data written to the SSDs in a storage cluster to be encrypted. This provides a primary layer of encryption in SolidFire Enterprise SDS nodes that do not include Self-Encrypting Drives (SEDs).

External key management

You can configure Element software to use a third-party KMIP-compliant key management service (KMS) to manage storage cluster encryption keys. When you enable this feature, the storage cluster's cluster-wide drive access password encryption key is managed by a KMS that you specify.
Element can use the following key management services:

- Gemalto SafeNet KeySecure
- SafeNet AT KeySecure
- HyTrust KeyControl
- Vormetric Data Security Manager
- IBM Security Key Lifecycle Manager

For more information on configuring External Key Management, see Getting started with External Key Management in the SolidFire and Element Documentation Center.

Multi-factor authentication

Multi-factor authentication (MFA) enables you to require users to present multiple types of evidence to authenticate with the NetApp Element web UI or storage node UI upon login. You can configure Element to accept only multi-factor authentication for logins integrating with your existing user management system and identity provider.
You can configure Element to integrate with an existing SAML 2.0 identity provider which can enforce multiple authentication schemes, such as password and text message, password and email message, or other methods.

You can pair multi-factor authentication with common SAML 2.0 compatible identity providers (IdPs), such as Microsoft Active Directory Federation Services (ADFS) and Shibboleth.

To configure MFA, see Enabling multi-factor authentication in the SolidFire and Element Documentation Center.

FIPS 140-2 for HTTPS and data at rest encryption

NetApp SolidFire storage clusters and NetApp HCI systems support encryption that complies with the Federal Information Processing Standard (FIPS) 140-2 requirements for cryptographic modules. You can enable FIPS 140-2 compliance on your NetApp HCI or SolidFire cluster for both HTTPS communications and drive encryption.

When you enable FIPS 140-2 operating mode on your cluster, the cluster activates the NetApp Cryptographic Security Module (NCSM) and leverages FIPS 140-2 Level 1 certified encryption for all communication via HTTPS to the NetApp Element UI and API. You use the `EnableFeature` Element API with the `fips` parameter to enable FIPS 140-2 HTTPS encryption. On storage clusters with FIPS-compatible hardware, you can also enable FIPS drive encryption for data at rest using the `EnableFeature` Element API with the `FipsDrives` parameter.

For more information about preparing a new storage cluster for FIPS 140-2 encryption, see Creating a cluster supporting FIPS drives.

For more information about enabling FIPS 140-2 on an existing, prepared cluster, see The EnableFeature Element API.

Performance and Quality of Service

A SolidFire storage cluster has the ability to provide Quality of Service (QoS) parameters on a per-volume basis. You can guarantee cluster performance measured in inputs and outputs per second (IOPS) using three configurable parameters that define QoS: Min IOPS, Max IOPS, and Burst IOPS.

SolidFire Active IQ has a QoS recommendations page that provides advice on optimal configuration and set up of QoS settings.

Quality of Service parameters

IOPS parameters are defined in the following ways:

- **Minimum IOPS** - The minimum number of sustained inputs and outputs per second (IOPS) that the storage cluster provides to a volume. The Min IOPS configured for a volume is the guaranteed level of performance for a volume. Performance does not drop below this level.
- **Maximum IOPS** - The maximum number of sustained IOPS that the storage cluster provides to a volume. When cluster IOPS levels are critically high, this level of IOPS performance is not exceeded.
- **Burst IOPS** - The maximum number of IOPS allowed in a short burst scenario. If a volume has been running below the Max IOPS, burst credits are accumulated. When performance levels become very high and are pushed to maximum levels, short bursts of IOPS are allowed on the volume.

  Element software uses Burst IOPS when a cluster is running in a state of low cluster IOPS utilization.

  A single volume can accrue Burst IOPS and use the credits to burst above their Max IOPS up to their Burst IOPS level for a set "burst period." A volume can burst for up to 60 seconds if the cluster has the capacity to accommodate the burst. A volume accrues one second of burst credit (up to a maximum of 60 seconds) for every second that the volume runs below its Max IOPS limit.

  Burst IOPS are limited in two ways:

  - A volume can burst above its Max IOPS for a number of seconds equal to the number of burst credits that the volume has accrued.
  - When a volume bursts above its Max IOPS setting, it is limited by its Burst IOPS setting. Therefore, the burst IOPS never exceeds the burst IOPS setting for the volume.
- **Effective Max Bandwidth** - The maximum bandwidth is calculated by multiplying the number of IOPS (based on the QoS curve) by the IO size.

  Example: QoS parameter settings of 100 Min IOPS, 1000 Max IOPS, and 1500 Burst IOPs have the following effects on quality of performance:

- Workloads are able to reach and sustain a maximum of 1000 IOPS until the condition of workload contention for IOPS becomes apparent on the cluster. IOPS are then reduced incrementally until IOPS on all volumes are within the designated QoS ranges and contention for performance is relieved.
- Performance on all volumes is pushed toward the Min IOPS of 100. Levels do not drop below the Min IOPS setting but could remain higher than 100 IOPS when workload contention is relieved.
- Performance is never greater than 1000 IOPS, or less than 100 IOPS for a sustained period. Performance of 1500 IOPS (Burst IOPS) is allowed, but only for those volumes that have accrued burst credits by running below Max IOPS and only allowed for a short periods of time. Burst levels are never sustained.

QoS value limits

Here are the possible minimum and maximum values for QoS.

Parameters	Min value	Default	4 4KB	5 8KB	6 16KB	262KB
Min IOPS	50	50	15,000	9,375*	5556*	385*
Max IOPS	100	15,000	200,000**	125,000	74,074	5128
Burst IOPS	100	15,000	200,000**	125,000	74.074	5128

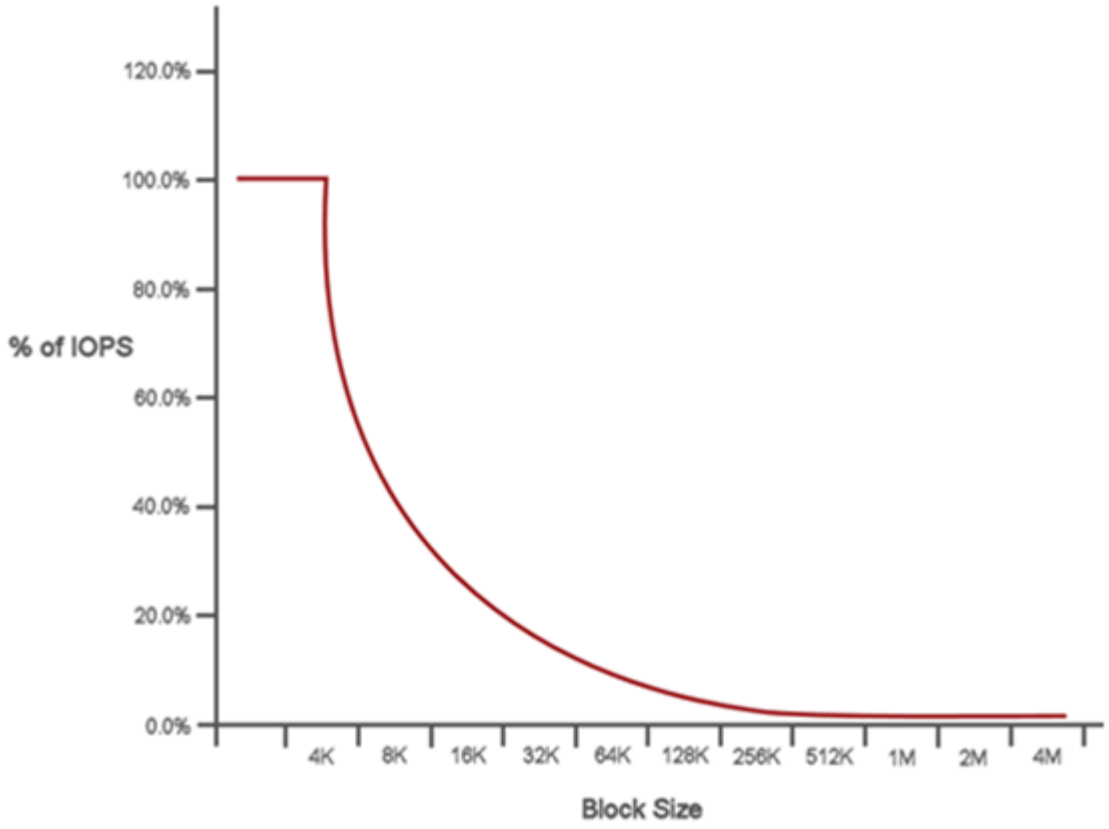
*These estimations are approximate.
**Max IOPS and Burst IOPS can be set as high as 200,000; however, this setting is allowed only to effectively uncap the performance of a volume. Real-world maximum performance of a volume is limited by cluster usage and per-node performance.

QoS performance

The QoS performance curve shows the relationship between block size and the percentage of IOPS.

Block size and bandwidth have a direct impact on the number of IOPS that an application can obtain. Element software takes into account the block sizes it receives by normalizing block sizes to 4k. Based on workload, the system might increase block sizes. As block sizes increase, the system increases bandwidth to a level necessary to process the larger block sizes. As bandwidth increases the number of IOPS the system is able to attain decreases.

The QoS performance curve shows the relationship between increasing block sizes and the decreasing percentage of IOPS:



As an example, if block sizes are 4k, and bandwidth is 4000 KBps, the IOPS are 1000. If block sizes increase to 8k, bandwidth increases to 5000 KBps, and IOPS decrease to 625. By taking block size into account, the system ensures that lower priority workloads that use higher block sizes, such as backups and hypervisor activities, do not take too much of the performance needed by higher priority traffic using smaller block sizes.

QoS policies

A QoS policy enables you to create and save a standardized quality of service setting that can be applied to many volumes.

QoS policies are best for service environments, for example, with database, application, or infrastructure servers that rarely reboot and need constant equal access to storage. Individual volume QoS is best for light use VMs, such as virtual desktops or specialized kiosk-type VMs, that may be rebooted, powered on, or powered off daily or several times a day.

QoS and QoS policies should not be used together. If you are using QoS policies, do not use custom QoS on a volume. Custom QoS will override and adjust QoS policy values for volume QoS settings.

The selected cluster must be Element 10.0 or later to use QoS policies; otherwise, QoS policy functions are not available.

Find more information

- NetApp HCI Documentation Center
- NetApp HCI Resources page