



# NetApp HCI Documentation

## HCI

NetApp

June 05, 2020

This PDF was generated from <https://docs.netapp.com/us-en/hci/docs/index.html> on June 05, 2020. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.



# Table of Contents

NetApp HCI configuration and management documentation .....	1
Discover what's new .....	1
Get started with NetApp HCI .....	1
Release Notes .....	2
What's new in NetApp HCI .....	2
Additional release information .....	3
Concepts .....	4
NetApp HCI product overview .....	4
NetApp HCI accounts .....	6
Data protection .....	7
Clusters .....	11
Nodes .....	13
NetApp HCI security .....	14
Performance and Quality of Service .....	16
Get started with NetApp HCI .....	20
NetApp HCI installation and deployment overview .....	20
Monitor your NetApp HCI system .....	27
View storage and compute resources on the HCC Dashboard .....	27
View your inventory in the Nodes page .....	27
Monitor performance, capacity, and cluster health with SolidFire Active IQ .....	29
Collect NetApp HCI logs .....	30
Upgrade your NetApp HCI or SolidFire system .....	32
Upgrades overview .....	32
Upgrade sequences .....	32
System upgrade procedures .....	35
vSphere upgrade sequences with vCenter Plug-in .....	78
Expand your NetApp HCI system .....	80
Expansion overview .....	80
Expand NetApp HCI storage resources .....	80
Expand NetApp HCI compute resources .....	83
Expand NetApp HCI storage and compute resources at the same time .....	86
Remove Witness Nodes after expanding cluster .....	89
Legal notices .....	91
Copyright .....	91
Trademarks .....	91
Patents .....	91

Privacy policy .....	91
Open source .....	91

# NetApp HCI configuration and management documentation

NetApp HCI provides both storage and compute resources, combining them to build a VMware vSphere environment backed by the capabilities of NetApp Element software.

You can upgrade, expand, and monitor your system with the NetApp Hybrid Cloud Control interface and manage NetApp HCI resources with NetApp Element Plug-in for vCenter Server.

## Discover what's new

- [What's new in NetApp HCI](#)
- [What's new in NetApp Element software](#)
- [What's new in management services for Element software and NetApp HCI](#)
- [What's new in NetApp Element Plug-in for vCenter Server](#)

## Get started with NetApp HCI

- [NetApp HCI installation and deployment overview](#)
- [Review basic concepts](#)

## Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources page](#)

# Release Notes

## What's new in NetApp HCI

NetApp periodically updates NetApp HCI to bring you new features, enhancements, and bug fixes.

### NetApp HCI 1.8

NetApp HCI 1.8 introduces two-node and three-node storage cluster capability, multi-factor authentication, and NetApp Hybrid Cloud Control enhancements.



NetApp HCI 1.8 includes NetApp Element software 12.0. [Learn more](#) about what's new in Element 12.0.

#### Active IQ Config Advisor

Active IQ Config Advisor is a tool that helps streamline the installation experience and reduce networking failures during deployment. It validates that the configuration is ready for deployment and generates a report that you can use to resolve issues and send to NetApp Professional Services before hardware installation. See the [Deployment Guide](#) for details.

#### NetApp HCI documentation enhancements

You can now access NetApp HCI upgrading, expansion, monitoring, and concepts information in an easy-to-navigate format [here](#)<sup>^</sup>.

#### NetApp Element Plug-in for vCenter Server 4.4 availability

The NetApp Element Plug-in for vCenter Server 4.4 is available outside of the management node 12.0 and NetApp HCI 1.8 releases. To upgrade the plug-in, follow the instructions in the [NetApp HCI Upgrades](#)<sup>^</sup> documentation.

#### NetApp Hybrid Cloud Control enhancements

NetApp Hybrid Cloud Control is enhanced for version 1.8. [Learn more](#).

#### Support for two-node and three-node storage clusters

With version 1.8, you can set up NetApp HCI to use a storage cluster with two or three storage nodes. When you deploy with a two-node or three-node storage cluster, the deployment process automatically configures two NetApp Witness Nodes as virtual machines. Witness Nodes are virtual nodes that enable storage node redundancy in the event of a storage node failure. NetApp HCI supports the H410S-0, H410S-1, and H610S-1 storage nodes in two-node or three-node storage clusters. [Learn more](#)<sup>^</sup>.

## Find more information

- [NetApp HCI Documentation Center](#)
- [SolidFire and Element Software Documentation Center](#)

## Additional release information

You can find links to the latest and earlier release notes for various components of the NetApp HCI and Element storage environment.



You will be prompted to log in using your NetApp Support Site credentials.

### NetApp HCI

- [NetApp HCI 1.8 Release Notes](#)
- [NetApp HCI 1.7P1 Release Notes](#)

### NetApp Element software

- [NetApp Element Software 12.0 Release Notes](#)
- [NetApp Element Software 11.8 Release Notes](#)
- [NetApp Element Software 11.7 Release Notes](#)
- [NetApp Element Software 11.5.1 Release Notes](#)
- [NetApp Element Software 11.3P1 Release Notes](#)

### Management services

- [Management Services Release Notes](#)

### NetApp Element Plug-in for vCenter Server

- [vCenter Plug-in 4.4 Release Notes](#)
- [vCenter Plug-in 4.3 Release Notes](#)

# 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.
- 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. 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 mNode service, are updated frequently as service bundles.



Learn more about [management services releases](#).

- **NetApp Hybrid Cloud Control** enables you to manage NetApp HCI. You can upgrade management services, expand your system, and monitor your installation. 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 alternative scalable, user-friendly interface for VMware vSphere that can manage and monitor storage clusters running **NetApp Element software**. 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 common URLs you use with NetApp HCI:

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

## Find more information

- [NetApp HCI Documentation Center](#)



- [NetApp HCI Resources page](#)

## NetApp HCI accounts

To use NetApp HCI, you'll need to set up some user accounts.

### Storage cluster administrator account types

There are two types of administrator accounts that can exist in a storage cluster running NetApp Element software: the primary cluster administrator account and a cluster administrator account.

- **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](#).

### 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 two thousand volumes assigned to it, but a volume can belong to only one account.
- User accounts can be managed from NetApp Element Management extension point.

For details, see user account information in the [SolidFire and Element Documentation Center](#).

## Find more information

- [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.

## 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.

## 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 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

Scaling 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 scale using the [NetApp Hybrid Cloud Control UI](#). When scaling 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 scale 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 scale 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 (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 mNode 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 [Redeploying Witness Nodes for two and three-node storage clusters](#).

## Find more information

- [NetApp HCI Two-Node Storage Cluster | TR-4823](#)
- [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.

## 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.

## 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.

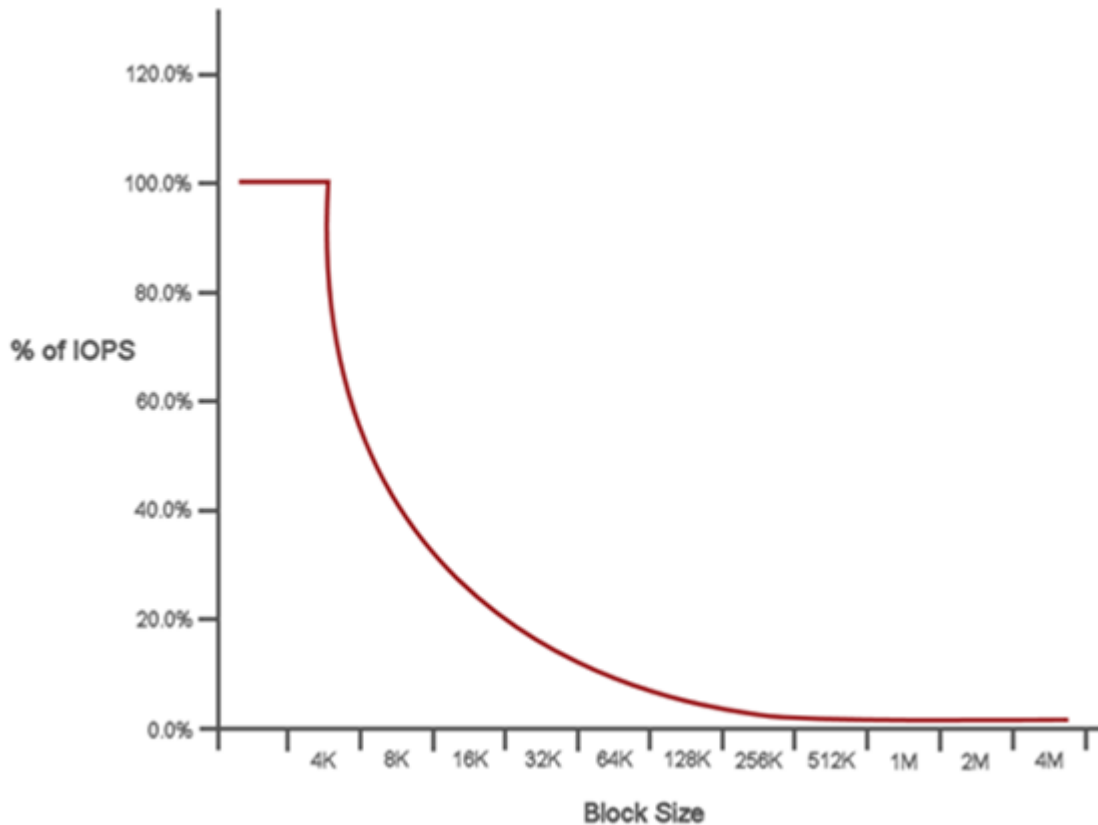
## QoS performance

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. You can create, edit, and delete QoS policies.

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. QoSSIOC automation 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. QoSSIOC automation and QoS policies should not be used together. If you are using QoS policies, do not enable QoSSIOC. QoSSIOC

will override and adjust QoS values for volume QoS settings.

You can view QoS policies on the **Management > QoS Policies** page from the NetApp Element Management extension point.



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

## Find more information

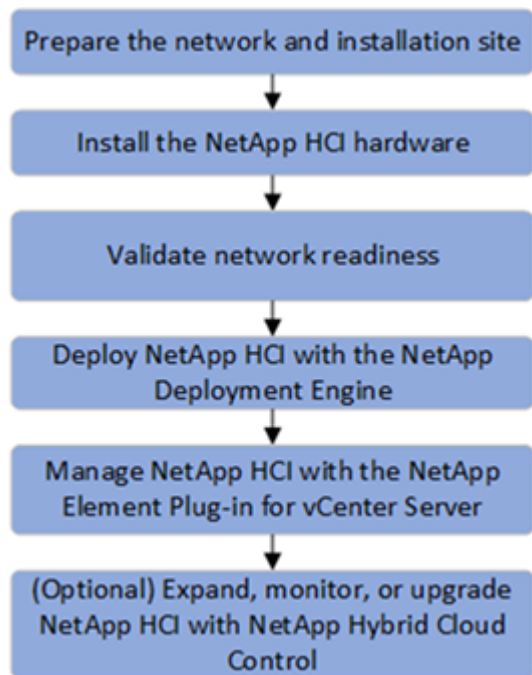
- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources page](#)

# Get started with NetApp HCI

## NetApp HCI installation and deployment overview

Use these instructions to install and deploy NetApp HCI. These instructions include links to more details.

Here is an overview of the process.



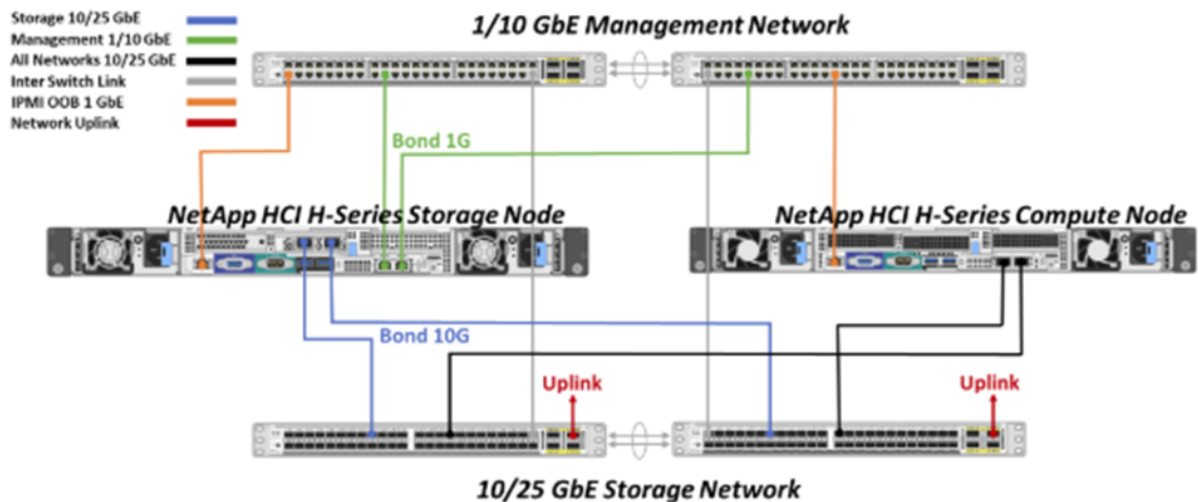
### Prepare for installation

Before you begin the installation, complete the *NetApp HCI Installation Discovery Workbook* pre-flight checklist sent to you prior to receiving the hardware.

### Prepare the network and installation sites

Here is a simplified NetApp HCI network topology installation:

## NetApp HCI Simplified Network Topology Installation



This is the simplified network topology for a single storage node and single compute node. The minimum cluster for NetApp HCI is two storage and two compute nodes.



Your network topology might differ from what is shown here. This is an example only.

This setup uses two network cables on the compute nodes for connectivity to all NetApp HCI networks.

Read these resources:

- Use the *NetApp HCI Installation Discovery Workbook* to configure your network before the installation.
- For details and other supported configurations, see [TR-4820: NetApp HCI Networking Quick Planning Guide](#) and the [NetApp HCI Installation and Setup Instructions](#).
- For information about NetApp HCI configurations smaller than four storage nodes, see [TR-4823: NetApp HCI 2-Node Storage Cluster](#).

This setup consolidates all traffic onto two physical, redundant ports, reducing the cabling and streamlining network configuration. This configuration requires that the storage, vMotion and any virtual machine network segments use VLAN tagging. The management network segment can use native or tagged VLAN; however, native VLAN is the preferred mode so that NetApp Deployment Engine (NDE) can assign network resources in an automated manner (Zero Conf).

This mode requires vSphere Distributed Switches (vDS), which require VMware vSphere Enterprise Plus licensing.

### Networking requirements before you begin

- Bond1G is a logical interface that combines 1GbE network ports on storage nodes and a management interface on compute nodes. This network is used for NDE API traffic. All nodes must be able to communicate over the management interface in the same L2 network.
- Bond10G is a logical interface that combines 10/25GbE ports and are used by NDE for beaconing



and inventory. All nodes must be able to communicate over the Bond10G interface with non-fragmented jumbo frames.

- NDE requires at a minimum one manually assigned IP address on the Bond1G interface on one storage node. NDE will be run from this node.
- All nodes will have temporary IP addresses assigned by NDE discovery, which is accomplished by Automatic Private IP Addressing (APIPA).



During the NDE process, all nodes will then be assigned permanent IP addresses and any APIPA assigned temporary IPs will be released.

- NDE requires separate networks for management, iSCSI and vMotion that are preconfigured on the switch network.

## Install NetApp HCI hardware

NetApp HCI can be installed in different configurations:

- H410C compute nodes: Two-cable configuration or six-cable configuration
- H610C compute node: Two-cable configuration
- H615C compute node: Two-cable configuration
- H410S storage node
- H610S storage node



For precautions and details, see the [NetApp HCI Installation and Setup Instructions](#).

### Steps

1. Install the rails and the chassis.
2. Install nodes in the chassis and install drives for storage nodes. (Applies only if you are installing H410C and H410S in a NetApp H-series chassis.)
3. Cable the compute node.
4. Cable the storage node.
5. Connect the power cords.
6. Power on the NetApp HCI nodes.

## Validate network readiness

To ensure network readiness for NetApp HCI, install the NetApp Configuration Advisor 5.8.1 or later. This network validation tool is located with other [NetApp Support Tools](#). Use this tool to validate connectivity, VLAN IDs, IP address requirements, switch connectivity and more.

## Deploy NetApp HCI using the NetApp Deployment Engine (NDE)

The NDE UI is the software wizard interface used to install NetApp HCI.

### Launch the NDE UI

NetApp HCI uses a storage node management network IPv4 address for initial access to the NDE. As a best practice, connect from the first storage node.

#### Prerequisites

- You already assigned the initial storage node management network IP address manually or by using DHCP.
- You must have physical access to the NetApp HCI installation.

#### Steps

1. If you do not know the initial storage node management network IP, use the Terminal User Interface (TUI), which is accessed via keyboard and monitor on the storage node or [use a USB stick](#).

For details, see [Accessing the NetApp Deployment Engine](#).

2. If you do know the IP address, from a web browser, connect to the Bond1G address of the primary node via HTTP, not HTTPS.

**Example:** [http://<IP\\_address>:442/nde/](http://<IP_address>:442/nde/)

### Deploy NetApp HCI with the NDE UI

1. In the NDE, accept the prerequisites, check to use Active IQ, and accept license agreements.
2. Optionally, enable Data Fabric File Services by ONTAP Select and accept the ONTAP Select license.
3. Configure a new vCenter deployment. Click **Configure Using a Fully Qualified Domain Name** and enter both the vCenter Server Domain Name and DNS Server IP address.



It is strongly recommended to use the FQDN approach for vCenter installation.


4. Review that the inventory assessment of all nodes completed successfully.

The storage node that is running the NDE is already checked.

5. Select all nodes and click **Continue**.
6. Configure network settings. Refer to the *NetApp HCI Installation Discovery Workbook* for the values to use.
7. Click the blue box to launch the easy form.

## Network Settings


Provide the network settings that will be used for your installation.


Live network validation is: On 

### Infrastructure Services

DNS Server IP Address 1


DNS Server IP Address 2 (Optional)

NTP Server Address 1 


us.pool.ntp.org 

NTP Server Address 2 (Optional)

To save time, launch the easy form to enter fewer network settings. >



### vCenter Networking

VLAN ID	Subnet 	Default Gateway	FQDN	IP Address
Untagged Network	xxx.xxx.xxx.xxx/nm	<input type="text"/>	*	<input type="text"/>

8. On the Network Settings Easy Form:
  - a. Type the Naming Prefix. (Refer to the System Details of the *NetApp HCI Installation Discovery Workbook*.)
  - b. Click **No** for Will you assign VLAN IDs? (You assign them later in the main Network Settings page.)
  - c. Type the subnet CIDR, default gateway, and starting IP address for the management, vMotion, and iSCSI networks according to your workbook. (Refer to the IP Assignment Method section of the *NetApp HCI Installation Discovery Workbook* for these values.)
  - d. Click **Apply to Network Settings**.
9. Join an existing vCenter (optional). See the *NetApp HCI Deployment Guide* in the [NetApp HCI Documentation Center](#).
10. Record node serial numbers in the *NetApp HCI Installation Discovery Workbook*.
11. Specify a VLAN ID for the vMotion Network and any network that requires VLAN tagging. See the *NetApp HCI Installation Discovery Workbook*.
12. Download your configuration as a .CSV file.
13. Click **Start Deployment**.
14. Copy and save the URL that appears.



It can take about 45 minutes to complete the deployment.

## Verify the installation using the vSphere Web Client

1. Launch the vSphere Web Client and log in using the credentials specified during NDE use.

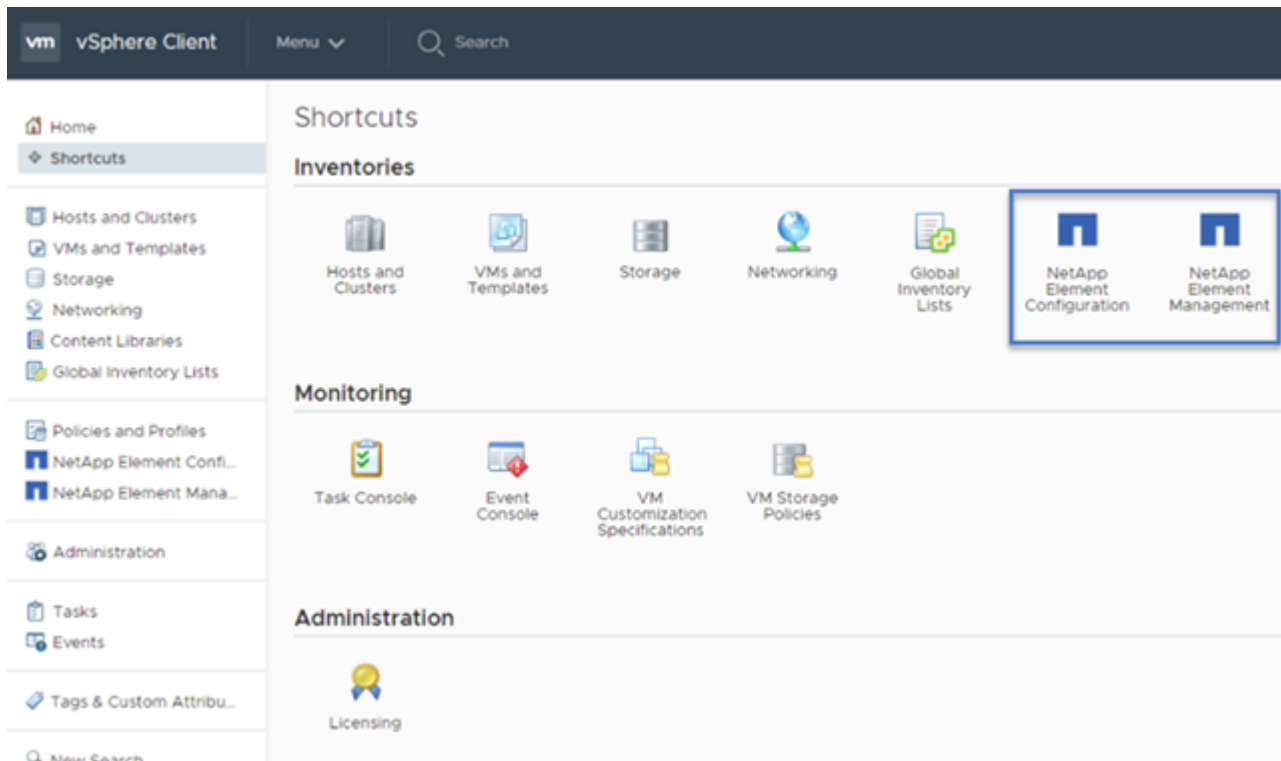
You must append `@vsphere.local` to the user name.

2. Verify that no alarms are present.
3. Verify that the vCenter, mNode, and ONTAP Select (optional) appliances are running without warning icons.
4. Observe that the two default datastores (NetApp-HCI-Datastore\_01 & 02) are created.
5. Select each datastore and ensure that all compute nodes are listed in the Hosts tab.
6. Validate vMotion and Datastore-02.
  - a. Migrate the vCenter Server to NetApp-HCI-Datastore-02 (storage only vMotion).
  - b. Migrate the vCenter Server to each of the compute nodes (compute only vMotion).
7. Go to the NetApp Element Plug-in for vCenter Server and ensure that the cluster is visible.
8. Ensure no alerts appear on the Dashboard.

## Manage NetApp HCI using the vCenter Plug-in

After you install NetApp HCI, you can configure clusters, volumes, datastores, logs, access groups, initiators, and Quality of Service (QoS) policies by using the NetApp Element Plug-in for vCenter Server.

For details, see the [NetApp Element Plug-in for vCenter Server Guide](#).



## (Optional) Expand, monitor, or upgrade NetApp HCI with the Hybrid Cloud Control

You can use the NetApp HCI Hybrid Cloud Control to expand, monitor, or upgrade your system.

You log in to NetApp Hybrid Cloud Control by browsing to the IP address of the management node.

Using the Hybrid Cloud Control, you can do the following:

- [Monitor your NetApp HCI installation](#)
- [Upgrade your NetApp HCI system](#)
- [Expand your NetApp HCI storage or compute resources](#)

### Steps

1. Open a web browser and browse to the IP address of the management node. For example:

`https://<ManagementNodeIP>`

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.

The NetApp Hybrid Cloud Control interface appears.

### Find more information

- [NetApp HCI Resources page](#)
- [NetApp HCI Documentation Center](#)
- [NetApp HCI Installation and Setup Instructions](#)
- [TR-4820: NetApp HCI Networking Quick Planning Guide](#)
- [NetApp Element Plug-in for vCenter Server Guide.](#)
- [NetApp Configuration Advisor 5.8.1 or later network validation tool](#)
- [NetApp SolidFire Active IQ Documentation](#)

# Monitor your NetApp HCI system

## View storage and compute resources on the HCC Dashboard

With the NetApp Hybrid Control (HCC) Dashboard, you can view all your storage and compute resources at a glance.

Only compute nodes that are managed and clusters with at least one managed node in H-series hardware appear on the Dashboard.

### Steps

1. Open a web browser and browse to the IP address of the management node. For example:

```
https://[management node IP address]
```

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.
3. View the Dashboard:
  - **Storage:** Displays the number of storage clusters, storage nodes, and total volumes.
  - **Compute:** Displays the number of compute clusters and total compute nodes.
  - **Storage Capacity:** Displays the total physical storage space available in your cluster on the **RAW** tab, and information about the provisioned storage on the **EFFECTIVE** tab.



To view cluster health, look at the SolidFire Active IQ Dashboard. See [Viewing performance, capacity, and cluster health in SolidFire Active IQ](#).

### Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## View your inventory in the Nodes page

You can view both your storage and compute assets in your system and determine their IP addresses, names, and software versions.

You can view storage information for your two-, three-, and four-node systems and any NetApp HCI Witness Nodes associated with two-node or three-node clusters.

Witness Nodes manage quorum within the cluster; they are not used for storage. Witness Nodes are applicable only to NetApp HCI and not to all-flash storage environments.

For more information about Witness Nodes, see [Nodes definitions](#).

Steps

- 1. Open a web browser and browse to the IP address of the management node. For example:

https://[management node IP address]

- 2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.
- 3. In the left navigation blue box, select the NetApp HCI installation.

The Hybrid Cloud Control Dashboard appears.

- 4. In the left navigation, click **Nodes**.

The Storage tab appears.

Nodes

Only NetApp HCI Nodes are displayed on this page.

STORAGE

COMPUTE

RagnarokNomadCluster

1 of 1

Two-node

Hostname

Node Model

Element Version

Management IP Address

stg01

H410S-0

12.0.0.318

- VLAN 1184

stg02

H410S-0

12.0.0.318

- VLAN 1184

1 - 2 of 2 results

1

30

Witness Nodes

Hostname

Management IP Address

Storage (iSCSI) IP Address

wit01

wit02

- 5. On the **Storage** tab of the Nodes page, review the following information:
  - a. Two-node clusters: A “two-node” label appears on the Storage tab and the associated Witness Nodes are listed.
  - b. Three-node clusters: The storage nodes and associated Witness Nodes are listed. Three-node clusters have a Witness Node deployed on standby to maintain high availability in the case of node failure.

- c. Clusters with four nodes or more: Information for clusters with four or more nodes appears. Witness Nodes do not apply; the Witness Nodes table does not appear.
6. To view compute inventory information, click **Compute**.
7. Options:
  - a. To filter the list of items in the results, click the **Filter** icon and select the filters. You can also enter text for the filter.
  - b. To show or hide columns, click the **Show/Hide Columns** icon.
  - c. To download the table, click the **Download** icon.



To view the number of storage and compute resources, look at the Hybrid Cloud Control (HCC) Dashboard. See [View storage and compute resources in HCC Dashboard](#).

## Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

# Monitor performance, capacity, and cluster health with SolidFire Active IQ

By using SolidFire Active IQ, you can monitor the events, performance, and capacity of your clusters. You can access SolidFire Active IQ from the NetApp Hybrid Control Dashboard.

## Before you begin

- You must have a NetApp Support account to take advantage of this service.
- You must have authorization to use management node REST APIs.
- You have deployed a management node running version 12.0 or later.
- Your cluster version is running NetApp Element software 12.0 or later.
- You have Internet access. The Active IQ collector service cannot be used from dark sites.

## About this task

You can obtain continually updated historical views of cluster-wide statistics. You can set up notifications to alert you about specified events, thresholds, or metrics on a cluster so that they can be addressed quickly.

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 potential system issues.



## Steps

1. Open a web browser and browse to the IP address of the management node. For example:

```
https://[management node IP address]
```

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.
3. From the Dashboard, click the menu on the upper right.
4. Select **View Active IQ**.

The [SolidFire Active IQ Dashboard](#) appears.

5. To learn about SolidFire Active IQ, from the Dashboard, click the menu icon on the upper right and click **Documentation**.
6. From the SolidFire Active IQ interface, verify that the NetApp HCI compute and storage nodes are reporting telemetry correctly to Active IQ:
  - a. If you have more than one NetApp HCI installation, click **Select a Cluster** and choose the cluster from the list.
  - b. In the left navigation pane, click **Nodes**.
7. If a node or nodes are missing from the list, contact NetApp Support.



To view the number of storage and compute resources, look at the Hybrid Cloud Control (HCC) Dashboard. See [View storage and compute resources in HCC Dashboard](#).

## Find more information

- [NetApp SolidFire Active IQ Documentation](#)
- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Collect NetApp HCI logs

If you have trouble with your NetApp HCI installation, you can collect logs to send to NetApp Support to help with diagnosis. You can access the log collection area from the NetApp Hybrid Control Dashboard.

## Steps

1. Open a web browser and browse to the IP address of the management node. For example:

https://[management node IP address]

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.
3. From the Dashboard, click the menu on the upper right.
4. Select **Collect Logs**.

The **Collect Logs** page appears. If you have collected logs before, you can download the existing log package, or begin a new log collection.

5. Select a date range in the **Date Range** drop-down menu to specify what dates the logs should include.

If you specify a custom start date, you can select the date to begin the date range. The logs will cover from that date up to the present time.

6. In the **Log Collection** section, select the types of log files the log package should include.

For storage and compute logs, you can expand the list of storage or compute nodes and select individual nodes to collect logs from (or all nodes in the list).

7. Click **Collect Logs** to start log collection.

Log collection runs in the background, and the page shows the progress.



Depending on the logs you collect, the progress bar might remain at a certain percentage for several minutes, or progress very slowly at some points.

8. Click **Download Logs** to download the log package.

The log package is in a compressed UNIX .tgz file format.

## Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

# Upgrade your NetApp HCI or SolidFire system

## Upgrades overview

The content in this section introduces recommended upgrade sequences for components in a NetApp HCI system or SolidFire all-flash storage system.

**System upgrade sequences** content describes the tasks that are needed to complete a NetApp HCI system or SolidFire all-flash storage system upgrade. Ideally these procedures are performed as part of the larger upgrade sequence and not in isolation. If a component-based upgrade or update is needed, see the procedure prerequisites to ensure additional complexities are addressed.

**vSphere upgrade sequences including Element Plug-in for vCenter Server** content describes additional pre- and post-upgrade steps required to re-install the Element Plug-in for vCenter Server.

## System upgrade sequences

Choose one of the following sequences based on your system:

- [Upgrade your NetApp HCI installation for version 1.8.](#)
- [Upgrade your NetApp SolidFire all-flash storage system for Element 12.0.](#)

## vSphere upgrade sequences including Element Plug-in for vCenter Server

Choose one of the following sequences based on your system:

- [Upgrade your vSphere components for a NetApp HCI system with the Element Plug-in for vCenter Server.](#)
- [Upgrade your vSphere components for a NetApp SolidFire storage system with the Element Plug-in for vCenter Server.](#)

## Find more information

- [NetApp HCI Documentation Center](#)
- [SolidFire and Element Documentation Center](#)

## Upgrade sequences

### Upgrade your NetApp HCI system for version 1.8

You can keep your NetApp HCI system up-to-date after deployment by sequentially upgrading all NetApp HCI software components.

These components include management services, HealthTools, NetApp Hybrid Cloud Control (HCC), Element software, management node, compute firmware, compute drivers, and the Element Plug-in for vCenter Server.

#### *What you'll need*

- You are running management node 11.3 or later. Newer versions of the management node have a modular architecture that provides individual services.



To check the version, log in to your management node and view the Element version number in the login banner. If you do not have 11.3, see [Upgrade your management node](#).

- You have upgraded your management services to at least version 2.1.326.

Upgrades using HCC are not available in earlier service bundle versions.

- You have ensured that the system time on all nodes is synced and that NTP is correctly configured for the storage cluster and nodes. Each node must be configured with a DNS nameserver in the per-node web UI ([https://\[IP address\]:442](https://[IP address]:442)) with no unresolved cluster faults related to time skew.

#### *Steps*

1. [Update management services from Hybrid Cloud Control](#).



You must upgrade to the latest management services bundle before upgrading your Element software to version 12.

2. [Upgrade to the latest HealthTools](#).
3. [Run Element storage health checks prior to upgrading storage](#).
4. [Upgrade your Element software version](#).
5. [Upgrade your management node](#).
6. [Upgrade your Element Plug-in for vCenter Server](#).
7. [Run compute node health checks prior to upgrading compute firmware](#).
8. [Update your compute node firmware](#).
9. [Update your compute node drivers](#).

#### **Find more information**

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Upgrade your NetApp SolidFire all-flash storage system for Element 12.0

You can keep your SolidFire Element storage system up-to-date after deployment by sequentially upgrading all NetApp storage components.

These components include management services, HealthTools, NetApp Hybrid Cloud Control (HCC), Element software, management node, and (depending on your installation) the Element Plug-in for vCenter Server.

### *What you'll need*

- You are running management node 11.3 or later. Newer versions of the management node have a modular architecture that provides individual services.



To check the version, log in to your management node and view the Element version number in the login banner. If you do not have 11.3, see [Upgrade your management node](#).

- You have upgraded your management services to at least version 2.1.326.

Upgrades using HCC are not available in earlier service bundle versions.

- You have ensured that the system time on all nodes is synced and that NTP is correctly configured for the storage cluster and nodes. Each node must be configured with a DNS nameserver in the per-node web UI ([https://\[IP address\]:442](https://[IP address]:442)) with no unresolved cluster faults related to time skew.

### *Steps*

1. [Update management services from Hybrid Cloud Control](#).



You must upgrade to the latest management services bundle before upgrading your Element software to version 12.

2. [Upgrade to the latest HealthTools](#).
3. [Run Element storage health checks prior to upgrading storage](#).
4. [Upgrade your Element software version](#).
5. [Upgrade your management node](#).
6. [Upgrade your Element Plug-in for vCenter Server to version 4.4](#).

### **Find more information**

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

# System upgrade procedures

## Update management services

You can update your management services to the latest bundle version after you have installed management node 11.3 or later.

Beginning with the Element 11.3 management node release, the management node design has been changed based on a new modular architecture that provides individual services. These modular services provide central and extended management functionality for NetApp HCI and SolidFire all-flash storage systems. Management services include system telemetry, logging, and update services, the QoSSIOC service for Element Plug-in for vCenter Server, NetApp Hybrid Cloud Control (HCC), and more.

You can update management services using the NetApp Hybrid Cloud Control (HCC) UI or the management node REST API:

- [Update management services using Hybrid Cloud Control](#) (Preferred method)
- [Update management services using the management node API](#)
- [Update management services using the management node API for dark sites](#)



You must upgrade to the latest management services bundle before upgrading your Element software to version 12.



(Required for any user who has updated to 2.10.27) Due to an upgrade API issue introduced in 2.10.27, management services cannot be upgraded from that version unless you use the workaround described in [these](#) release notes. You must upgrade to 2.10.29 or a later version using this workaround to resolve the issue and restore management services update capabilities.



For the latest management services release notes describing major services, new features, bug fixes, and workarounds for each service bundle, see [NetApp KB 1087586: Management Services Release Notes](#)

## Update management services using Hybrid Cloud Control

You can update your NetApp management services using NetApp Hybrid Cloud Control (HCC).

Management service bundles provide enhanced functionality and fixes to your installation outside of major releases.

*Before you begin*

- You must be running management node 11.3 or later.

- You must have upgraded your management services to at least version 2.1.326. NetApp Hybrid Cloud Control upgrades are not available in earlier service bundles.



For a list of available services for each service bundle version, see the [Management Services Release Notes](#).

### Steps

1. Open a web browser and browse to the IP address of the management node: `<a href="https://&lt;ManagementNodeIP&gt;" class="bare">https://&lt;ManagementNodeIP&gt;</a>;</code>`
2. Log in to NetApp Hybrid Cloud Control by providing the storage cluster administrator credentials.
3. Click **Upgrade** near the top right of the interface.
4. On the Upgrades page, select the **Management Services** tab.

The Management Services tab shows the current and available versions of management services software.



If your installation cannot access the internet, only the current software version is shown.

5. If your installation can access the internet and if a management services upgrade is available, click **Begin Upgrade**.
6. If your installation cannot access the internet, do the following:
  - a. Follow the instructions on the page to download and save a management services upgrade package to your computer.
  - b. Click **Browse** to locate the package you saved and upload it.

After the upgrade begins, you can see the upgrade status on this page.

### Update management services using the management node API

Users should ideally perform management services updates from NetApp Hybrid Cloud Control. You can however manually update management services using the REST API UI from the management node.

#### *Before you begin*

- You have internet access.
- You have deployed a NetApp Element software management node 11.3 or later.
- Your cluster version is running NetApp Element software 11.3 or later.

### Steps

1. Open the REST API UI on the management node: [https://\[management node IP\]/mnode](https://[management node IP]/mnode)

2. Click **Authorize** and complete the following:
  - a. Enter the cluster user name and password.
  - b. Enter the client ID as `mnode-client` if the value is not already populated.
  - c. Copy the token URL string and paste it into another browser tab to initiate a token request.
  - d. Click **Authorize** to begin a session.
  - e. Close the window.
3. (Optional) Confirm available versions of management node services: `GET /services/versions`
4. (Optional) Get detailed information about the latest version: `GET /services/versions/latest`
5. (Optional) Get detailed information about a specific version: `GET /services/versions/{version}/info`
6. Perform one of the following management services update options:
  - a. Run this command to update to the most recent version of management node services: `PUT /services/update/latest`
  - b. Run this command to update to a specific version of management node services: `PUT /services/update/{version}`
7. Run `GET/services/update/status` to monitor the status of the update.

A successful update returns a result similar to the following example:

```
{
  "current_version": "2.10.27",
  "details": "Updated to version 2.10.27",
  "status": "success"
}
```

## Update management services using the management node API for dark sites

Users should ideally perform management services updates from NetApp Hybrid Cloud Control. You can however manually upload, extract, and deploy a service bundle update for management services to the management node using the REST API. You can run each command from the REST API UI for the management node.

### *Before you begin*

- You have deployed a NetApp Element software management node 11.3 or later.
- Your cluster version is running NetApp Element software 11.3 or later.
- You have downloaded the service bundle update from the [NetApp Support Site](#) to a device that can be used in the dark site.

### *Steps*

1. Open the REST API UI on the management node: `https://[management node IP]/mnode`



2. Click **Authorize** and complete the following:
  - a. Enter the cluster user name and password.
  - b. Enter the client ID as `mnode-client` if the value is not already populated.
  - c. Copy the token URL string and paste it into another browser tab to initiate a token request.
  - d. Click **Authorize** to begin a session.
  - e. Close the window.
3. Upload and extract the service bundle on the management node using this command: `PUT /services/upload`
4. Deploy the management services on the management node: `PUT /services/deploy`
5. Monitor the status of the update: `GET /services/update/status`

A successful update returns a result similar to the following example:

```
{
  "current_version": "2.10.27",
  "details": "Updated to version 2.10.27",
  "status": "success"
}
```

### Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Upgrade to the latest HealthTools

Before you begin the Element storage upgrade, you should upgrade your HealthTools suite.

### *What you'll need*

- You are running management node 11.0, 11.1 or later.
- You have upgraded your management services to at least version 2.1.326.

NetApp Hybrid Cloud Control upgrades are not available in earlier service bundle versions.

- You have downloaded the latest version of [HealthTools](#) and copied the installation file to the management node.



You can check the locally installed version of HealthTools by running the `sfupdate-healthtools -v` command.

- To use HealthTools with dark sites, you need to do these additional steps:
  - Download a [JSON file](#) from the NetApp Support Site on a computer that is not the management node and rename it to `metadata.json`.
  - Have the management node up and running at the dark site.

#### About this task

The commands in the HealthTools suite require escalated privileges to run. Either preface commands with `sudo` or escalate your user to root privileges.



The HealthTools version you use might be more up to date than the sample input and response below.

#### Steps

1. Run the `sfupdate-healthtools <path to install file>` command to install the new HealthTools software.

Sample input:

```
sfupdate-healthtools /tmp/solidfire-healthtools-2020.03.01.09.tgz
```

Sample response:

```
Checking key signature for file /tmp/solidfirehealthtools-2020.03.01.09/components.tgz
installing command sfupdate-healthtools
Restarting on version 2020.03.01.09
sfupdate-healthtools /sf/bin/sfupdate-healthtools -r 2020.03.01.09
installing command sfupgradecheck
installing command sfinstall
installing command sfresetupgrade
```

2. Run the `sfupdate-healthtools -v` command to verify the installed version has been upgraded.

Sample response:

```
Currently installed version of HealthTools:
2020.03.01.09
```

#### Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Run Element storage health checks prior to upgrading storage

You must run health checks prior to upgrading Element storage to ensure all storage nodes in your cluster are ready for the next Element storage upgrade.

You can run health checks using NetApp Hybrid Cloud Control (HCC) UI, HCC API, or the HealthTools suite:

- [Use NetApp Hybrid Cloud Control to run Element storage health checks prior to upgrading storage](#) (Preferred method)
- [Use API to run Element storage health checks prior to upgrading storage](#)
- [Use HealthTools to run Element storage health checks prior to upgrading storage](#)

You can also find out more about storage health checks that are run by the service:

- [Storage health checks made by the service](#)

### *What you'll need*

- You have updated to the latest management services bundle (2.10.27 or later).



You must upgrade to the latest management services bundle before upgrading your Element software to version 12.

- You are running management node 11.3 or later.
- Your cluster version is running NetApp Element software 11.3 or later.


## Use NetApp Hybrid Cloud Control to run Element storage health checks prior to upgrading storage

Using NetApp Hybrid Cloud Control (HCC), you can verify that a storage cluster is ready to be upgraded.

### *Steps*

1. Open a web browser and browse to the IP address of the management node:

```
https://<ManagementNodeIP>
```

2. Log in to NetApp Hybrid Cloud Control by providing the storage cluster administrator credentials.
3. Click **Upgrade** near the top right of the interface.
4. On the **Upgrades** page, select the **Storage** tab.
5. Click the health check  for the cluster you want to check for upgrade readiness.

6. On the **Storage Health Check** page, click **Run Health Check**.
7. If there are issues, do the following:
  - a. Go to the specific KB article listed for each issue or perform the specified remedy.
  - b. If a KB is specified, complete the process described in the relevant KB article.
  - c. After you have resolved cluster issues, click **Re-Run Health Check**.

After the health check completes without errors, the storage cluster is ready to upgrade. See storage node upgrade [instructions](#) to proceed.

### Use API to run Element storage health checks prior to upgrading storage

You can use REST API to verify that a storage cluster is ready to be upgraded. The health check verifies that there are no obstacles to upgrading, such as pending nodes, disk space issues, and cluster faults.

#### Steps

1. Locate the storage cluster ID:
  - a. Open the management node REST API UI on the management node:

```
https://[management node IP]/mnode
```
  - b. Click **Authorize** and complete the following:
    - i. Enter the cluster user name and password.
    - ii. Enter the client ID as `mnode-client` if the value is not already populated.
    - iii. Click **Authorize** to begin a session.
  - c. From the REST API UI, click **GET /assets/storage-clusters**.
  - d. Click **Try it out**.
  - e. Click **Execute**.
  - f. From the response, copy the storage cluster ID ("`id`") of the cluster you intend to check for upgrade readiness.
2. Run health checks on the storage cluster:
  - a. Open the storage REST API UI on the management node:

```
https://[management node IP]/storage/1
```

- b. Click **Authorize** and complete the following:
  - i. Enter the cluster user name and password.
  - ii. Enter the client ID as `mnode-client` if the value is not already populated.

- iii. Click **Authorize** to begin a session.
- c. Click **POST /health-checks**.
- d. Click **Try it out**.
- e. Enter the storage cluster ID in the parameter field.
- f. Click **Execute** to run a health check on the specified storage cluster.

The response should indicate state as **initializing**:

```
{
  "_links": {
    "collection": "https://10.117.149.231/storage/1/health-checks",
    "log": "https://10.117.149.231/storage/1/health-checks/358f073f-896e-4751-ab7b-ccbb5f61f9fc/log",
    "self": "https://10.117.149.231/storage/1/health-checks/358f073f-896e-4751-ab7b-ccbb5f61f9fc"
  },
  "config": {},
  "dateCompleted": null,
  "dateCreated": "2020-02-21T22:11:15.476937+00:00",
  "healthCheckId": "358f073f-896e-4751-ab7b-ccbb5f61f9fc",
  "state": "initializing",
  "status": null,
  "storageId": "c6d124b2-396a-4417-8a47-df10d647f4ab",
  "taskId": "73f4df64-bda5-42c1-9074-b4e7843dbb77"
}
```

- g. Copy the **healthCheckId** that is part of response.
3. Verify the results of the health checks:
- a. Click **GET /health-checks/healthCheckId**.
  - b. Click **Try it out**.
  - c. Enter the health check ID in the parameter field.
  - d. Click **Execute**.
  - e. Scroll to the bottom of the response body.
4. If the **message** return indicates that there were problems regarding cluster health, do the following:
- a. Go to the specific KB article listed for each issue or perform the specified remedy.
  - b. If a KB is specified, complete the process described in the relevant KB article.
  - c. After you have resolved cluster issues, run **GET /health-checks/healthCheckId** again.

If all health checks are successful, the return is similar to the following example:

```
"message": "All checks completed successfully.",  
"percent": 100,  
"timestamp": "2020-03-06T00:03:16.321621Z"
```

## Use HealthTools to run Element storage health checks prior to upgrading storage

You can verify that the storage cluster is ready to be upgraded by using the `sfupgradecheck` command. This command verifies information such as pending nodes, disk space, and cluster faults.

If your management node is at a dark site, the upgrade readiness check needs the `metadata.json` file you downloaded during [HealthTools upgrades](#) to run successfully.

### About this task

This procedure describes how to address upgrade checks that yield one of the following results:

- Running the `sfupgradecheck` command runs successfully. Your cluster is upgrade ready.
- Checks within the `sfupgradecheck` tool fail with an error message. Your cluster is not upgrade ready and additional steps are required.
- Your upgrade check fails with an error message that HealthTools is out-of-date.
- Your upgrade check fails because your management node is on a dark site.

### Steps

1. Run the `sfupgradecheck` command:

```
sfupgradecheck -u <cluster-user-name> MVIP
```



For passwords that contain special characters, add a backslash (\) before each special character. For example, `mypass!@1` should be entered as `mypass!\!@.`

Sample input command with sample output in which no errors appear and you are ready to upgrade:

```
sfupgradecheck -u admin 10.117.78.244
```

```
check_pending_nodes:
Test Description: Verify no pending nodes in cluster
More information:
https://kb.netapp.com/support/s/article/ka11A00000008lt0QQAQ/pendingnodes
check_cluster_faults:
Test Description: Report any cluster faults
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of available disk
space
Passed node IDs: 1, 2, 3
More information: https://kb.netapp.com/support/s/article/ka11A00000008ltTQAQ/
SolidFire-Disk-space-error
check_mnode_connectivity:
Test Description: Verify storage nodes can communicate with management node
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A00000008ltYQAQ/mNodeconnectivity
check_files:
Test Description: Verify options file exists
Passed node IDs: 1, 2, 3
check_cores:
Test Description: Verify no core or dump files exists
Passed node IDs: 1, 2, 3
check_upload_speed:
Test Description: Measure the upload speed between the storage node and the
management node
Node ID: 1 Upload speed: 90063.90 KBs/sec
Node ID: 3 Upload speed: 106511.44 KBs/sec
Node ID: 2 Upload speed: 85038.75 KBs/sec
```

2. If there are errors, additional actions are required. See the following sub-sections for details.

### **Your cluster is not upgrade ready**

If you see an error message related to one of the health checks, follow these steps:

1. Review the **sfupgradecheck** error message.

Sample response:

The following tests failed:

check\_root\_disk\_space:

Test Description: Verify node root directory has at least 12 GBs of available disk space

Severity: ERROR

Failed node IDs: 2

Remedy: Remove unneeded files from root drive

More information: <https://kb.netapp.com/support/s/article/ka11A000000081tTQAQ/SolidFire-Disk-space-error>

check\_pending\_nodes:

Test Description: Verify no pending nodes in cluster

More information: <https://kb.netapp.com/support/s/article/ka11A000000081tOQAQ/pendingnodes>

check\_cluster\_faults:

Test Description: Report any cluster faults

check\_root\_disk\_space:

Test Description: Verify node root directory has at least 12 GBs of available disk space

Passed node IDs: 1, 3

More information: <https://kb.netapp.com/support/s/article/ka11A000000081tTQAQ/SolidFire-Disk-space-error>

check\_mnode\_connectivity:

Test Description: Verify storage nodes can communicate with management node

Passed node IDs: 1, 2, 3

More information:

<https://kb.netapp.com/support/s/article/ka11A000000081tYQAQ/mNodeconnectivity>

check\_files:

Test Description: Verify options file exists

Passed node IDs: 1, 2, 3

check\_cores:

Test Description: Verify no core or dump files exists

Passed node IDs: 1, 2, 3

check\_upload\_speed:

Test Description: Measure the upload speed between the storage node and the management node

Node ID: 1 Upload speed: 86518.82 KBs/sec

Node ID: 3 Upload speed: 84112.79 KBs/sec

Node ID: 2 Upload speed: 93498.94 KBs/sec

In this example, node 1 is low on disk space. You can find more information in the [knowledge base \(KB\)](#) article listed in the error message.

### HealthTools is out of date

If you see an error message indicating that HealthTools is not the latest version, follow these instructions:

1. Review the error message and note that the upgrade check fails.

Sample response:



```
sfupgradecheck failed: HealthTools is out of date:
installed version: 2018.02.01.200
latest version: 2020.03.01.09.
The latest version of the HealthTools can be downloaded from:
https://mysupport.netapp.com/NOW/cgi-bin/software/
Or rerun with the -n option
```

2. Follow the instructions described in the response.

#### Your management node is on a dark site

1. Review the message and note that the upgrade check fails:

Sample response:

```
sfupgradecheck failed: Unable to verify latest available version of healthtools.
```

2. Download a [JSON file](#) from the NetApp Support Site on a computer that is not the management node and rename it to `metadata.json`.
3. Run the following command:

```
sfupgradecheck -l --metadata=<path-to-metadata-json>
```

4. For details, see additional [HealthTools upgrades](#) information for dark sites.
5. Verify that the HealthTools suite is up-to-date by running the following command:

```
sfupgradecheck -u <cluster-user-name> -p <cluster-password> MVIP
```

#### Storage health checks made by the service

Storage health checks make the following checks per cluster.

Check Name	Node/Cluster	Description
check_async_results	Cluster	Verifies that the number of asynchronous results in the database is below a threshold number.
check_cluster_faults	Cluster	Verifies that there are no upgrade blocking cluster faults (as defined in Element source).

Check Name	Node/Cluster	Description
check_upload_speed	Node	Measures the upload speed between the storage node and the management node.
connection_speed_check	Node	Verifies that nodes have connectivity to the management node serving upgrade packages and estimates connection speed.
check_cores	Node	Checks for kernel crash dump and core files on the node. The check fails for any crashes in a recent time period (threshold 7 days).
check_root_disk_space	Node	Verifies the root file system has sufficient free space to perform an upgrade.
check_var_log_disk_space	Node	Verifies that <code>/var/log</code> free space meets some percentage free threshold. If it does not, the check will rotate and purge older logs in order to fall under threshold. The check fails if it is unsuccessful at creating sufficient free space.
check_pending_nodes	Cluster	Verifies that there are no pending nodes on the cluster.

### Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Upgrade Element software

To upgrade to NetApp Element software 12.0, you must use the `sfinstall` file included in the HealthTools suite of tools. Certain operations are suppressed during an Element software upgrade, such as adding and removing nodes, adding and removing drives, and commands associated with initiators, volume access groups, and virtual networks, among others.

Choose one of the following Element software upgrade options that use HealthTools for the procedure:

- [Upgrade Element software at connected sites](#)
- [Upgrade Element software at dark sites](#)



If you are upgrading an H610S series node to Element 12.0 or later, you will need to upgrade Element software (phase 1) and then perform additional upgrade steps (phase 2) for each storage node. See [Upgrading H610S storage nodes to Element 12.0 or later \(phase 2\)](#) after you complete the `sfinstall` procedure with HealthTools.

#### *What you'll need*

- You have updated your management services bundle to the latest version.



You must upgrade to the latest management services bundle before upgrading your Element software to version 12.

- You have checked upgrade path information for the Element version you are upgrading to and verified that the upgrade path is valid.

[NetApp KB 1088254: Upgrade matrix for storage clusters running NetApp Element Software](#)

- You have the latest version of HealthTools.
- You have verified that the cluster is ready to be upgraded. See [Run Element storage health checks prior to upgrading storage](#).
- You have ensured that the system time on all nodes is synced and that NTP is correctly configured for the storage cluster and nodes. Each node must be configured with a DNS nameserver in the per-node web UI ([https://\[IP address\]:442](https://[IP address]:442)) with no unresolved cluster faults related to time skew.
- The management node in your environment is running version 11.0, 11.1 or later.

## **Upgrade Element software at connected sites**

### *Steps*

1. For NetApp HCI systems, go to the NetApp HCI software [download page](#). For SolidFire storage systems, go to the Element software [download page](#).
2. Select the correct software release and download the latest storage node image to a computer that is not the management node.
3. Copy the ISO file to the management node in an accessible location like `/tmp`.



You can do this by using, for example, SCP.

When you upload the ISO file, make sure that the name of the file does not change, otherwise later steps will fail.

4. **Optional:** Download the ISO from the management node to the cluster nodes before the upgrade.

This step reduces the upgrade time by pre-staging the ISO on the storage nodes and running

additional internal checks to ensure that the cluster is in a good state to be upgraded. Performing this operation will not put the cluster into "upgrade" mode or restrict any of the cluster operations.

```
sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO> --stage
```



Omit the password from the command line to allow **sfinstall** to prompt for the information. For passwords that contain special characters, add a backslash (\) before each special character. For example, **mypass!@1** should be entered as **mypass\!\@.**

### Example

See the following sample input:

```
sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfisodium-11.0.0.345.iso --stage
```

The output for the sample shows that **sfinstall** attempts to verify if a newer version of **sfinstall** is available:

```
sfinstall 10.117.0.244 -u admin
/tmp/solidfire-rtfisodium-11.0.0.345.iso 2018-10-01 16:52:15:
Newer version of sfinstall available.
This version: 2018.09.01.130, latest version: 2018.06.05.901.
The latest version of the HealthTools can be downloaded from:
https://mysupport.netapp.com/NOW/cgi-bin/software/
or rerun with --skip-version-check
```

See the following sample excerpt from a successful pre-stage operation:



When staging completes, the message will display **Storage Node Upgrade Staging Successful** after the upgrade event.

```
flabv0004 ~ # sfinstall -u admin
10.117.0.87 solidfire-rtfi-sodium-patch3-11.3.0.14171.iso --stage
2019-04-03 13:19:58: sfinstall Release Version: 2019.01.01.49 Management Node
Platform:
Ember Revision: 26b042c3e15a Build date: 2019-03-12 18:45
2019-04-03 13:19:58: Checking connectivity to MVIP 10.117.0.87
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.86
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.87
...
2019-04-03 13:19:58: Successfully connected to cluster and all nodes
...
2019-04-03 13:20:00: Do you want to continue? ['Yes', 'No']: Yes
...
2019-04-03 13:20:55: Staging install pack on cluster nodes
2019-04-03 13:20:55: newVersion: 11.3.0.14171
2019-04-03 13:21:01: nodeToStage: nlabp2814, nlabp2815, nlabp2816, nlabp2813
2019-04-03 13:21:02: Staging Node nlabp2815 mip=[10.117.0.87] nodeID=[2] (1 of 4
nodes)
2019-04-03 13:21:02: Node Upgrade serving image at
http://10.117.0.204/rtfi/solidfire-rtfisodium-
patch3-11.3.0.14171/filesystem.squashfs
...
2019-04-03 13:25:40: Staging finished. Repeat the upgrade command without the --stage
option to start the upgrade.
```

The staged ISOs will be automatically deleted after the upgrade completes. However, if the upgrade has not started and needs to be rescheduled, ISOs can be manually de-staged using the command:

```
sfinstall <MVIP> -u <cluster_username> --destage
```

After the upgrade has started, the de-stage option is no longer available.

5. Start the upgrade with the **sfinstall** command and the path to the ISO file:

```
sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO>
```

### Example

See the following sample input command:

```
sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-11.0.0.345.iso
```

The output for the sample shows that **sfinstall** attempts to verify if a newer version of **sfinstall** is available:

```
sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-11.0.0.345.iso
2018-10-01 16:52:15: Newer version of sfinstall available.
This version: 2018.09.01.130, latest version: 2018.06.05.901.
The latest version of the HealthTools can be downloaded from:
https://mysupport.netapp.com/NOW/cgi-bin/software/ or rerun with --skip-version-check
```

See the following sample excerpt from a successful upgrade. Upgrade events can be used to monitor the progress of the upgrade.

```
# sfinstall 10.117.0.161 -u admin solidfire-rtfi-sodium-11.0.0.761.iso
2018-10-11 18:28
Checking connectivity to MVIP 10.117.0.161
Checking connectivity to node 10.117.0.23
Checking connectivity to node 10.117.0.24
...
Successfully connected to cluster and all nodes
#####
You are about to start a new upgrade
10.117.0.161
10.3.0.161
solidfire-rtfi-sodium-11.0.0.761.iso
Nodes:
10.117.0.23 nlabp1023 SF3010 10.3.0.161
10.117.0.24 nlabp1025 SF3010 10.3.0.161
10.117.0.26 nlabp1027 SF3010 10.3.0.161
10.117.0.28 nlabp1028 SF3010 10.3.0.161
#####
Do you want to continue? ['Yes', 'No']: yes
...
Watching for new network faults. Existing fault IDs are set([]).
Checking for legacy network interface names that need renaming
Upgrading from 10.3.0.161 to 11.0.0.761 upgrade method=rtfi
Waiting 300 seconds for cluster faults to clear
Waiting for caches to fall below threshold
...
Installing mip=[10.117.0.23] nodeID=[1] (1 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[7] away from mip[10.117.0.23] nodeID[1] ssid[11] to new ssid[15]
Moving primary slice=[12] away from mip[10.117.0.23] nodeID[1] ssid[11] to new
ssid[15]
...
Installing mip=[10.117.114.24] nodeID=[2] (2 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[5] away from mip[10.117.114.24] nodeID[2] ssid[7] to new
ssid[11]
...
Install of solidfire-rtfi-sodium-11.0.0.761 complete.
Removing old software
No staged builds present on nodeID=[1]
No staged builds present on nodeID=[2]
...
Starting light cluster block service check
```



If you are upgrading an H610S series node to Element 12.0 or later, you will need to perform additional upgrade steps (phase 2) for each storage node. See [Upgrading H610S storage nodes to Element 12.0 or later \(phase 2\)](#).

## Upgrade Element software at dark sites

You must use the HealthTools suite of tools to update NetApp Element software at a dark site.

### What you'll need

1. For NetApp HCI systems, go to the NetApp HCI software [download page](#). For SolidFire storage systems, go to the Element software [download page](#).
2. Select the correct software release and download the latest storage node image to a computer that is not the management node.
3. Download this [JSON file](#) ([https://library.netapp.com/ecm/ecm\\_get\\_file/ECMLP2840740](https://library.netapp.com/ecm/ecm_get_file/ECMLP2840740)) from the NetApp Support Site on a computer that is not the management node and rename it to `metadata.json`.
4. Copy the ISO file to the management node in an accessible location like `/tmp`.



You can do this by using, for example, SCP. When you upload the ISO file, make sure that the name of the file does not change, otherwise later steps will fail.

### Steps

1. Run the `sfupdate-healthtools` command:

```
sfupdate-healthtools <path-to-healthtools-package>
```

2. Check the installed version:

```
sfupdate-healthtools -v
```

3. Check the latest version against the metadata JSON file:

```
sfupdate-healthtools -l --metadata=<path-to-metadata-json>
```

4. Ensure that the cluster is ready:

```
sudo sfupgradecheck -u <cluster_username> -p <cluster_password> MVIP --metadata=<path-to-metadata-json>
```



5. Run the **sfinstall** command with the path to the ISO file and the metadata JSON file:

```
sfinstall -u <cluster_username> <MVIP> <path-toinstall-file-ISO> --metadata=<path-to  
-metadata-json-file>
```

See the following sample input command:

```
sfinstall -u admin 10.117.78.244 /tmp/solidfire-rtfi-11.3.0.345.iso  
--metadata=/tmp/metadata.json
```

**Optional** You can add the **--stage** flag to the **sfinstall** command to pre-stage the upgrade in advance.



If you are upgrading an H610S series node to Element 12.0 or later, you will need to perform additional upgrade steps (phase 2) for each storage node. See [Upgrading H610S storage nodes to Element 12.0 or later \(phase 2\)](#).

## What happens if an upgrade fails

If the software upgrade fails, you can pause the upgrade.



You should pause an upgrade only with Ctrl-C. This enables the system to clean itself up.

When **sfinstall** waits for cluster faults to clear and if any failure causes the faults to remain, **sfinstall** will not proceed to the next node.

### Steps

1. You should stop **sfinstall** with Ctrl+C.
2. Contact NetApp Support to assist with the failure investigation.
3. Resume the upgrade with the same **sfinstall** command.
4. When an upgrade is paused by using Ctrl+C, if the upgrade is currently upgrading a node, choose one of these options:
  - **Wait:** Allow the currently upgrading node to finish before resetting the cluster constants.
  - **Continue:** Continue the upgrade, which cancels the pause.
  - **Abort:** Reset the cluster constants and abort the upgrade immediately.



Aborting the cluster upgrade while a node is being updated might result in the drives being ungracefully removed from the node. If the drives are ungracefully removed, adding the drives back during an upgrade will require manual intervention by NetApp Support. The node might be taking longer to do firmware updates or post update syncing activities. If the upgrade progress seems stalled, contact NetApp Support for assistance.

## Upgrading H610S storage nodes to Element 12.0 or later (phase 2)

If you are upgrading an H610S series node to Element 12.0 or later, the upgrade process involves two phases.

Phase 1, which is performed first, follows the same steps as the standard upgrade to Element 12.0 process. It installs Element Software and all 5 firmware updates in a rolling fashion across the cluster one node at a time. Due to the firmware payload, the process is estimated to take approximately 1.5 to 2 hours per H610S node, including a single cold-boot cycle at the end of the upgrade for each node.

Phase 2 involves completing steps to perform a complete node shutdown and power disconnect for each H610S node that are described in a required [KB](#). This phase is estimated to take approximately one hour per H610S node.



After you complete phase 1, four of the five firmware updates are activated during the cold boot on each H610S node; however, the Complex Programmable Logic Device (CPLD) firmware requires a complete power disconnect and reconnect to fully install. The CPLD firmware update protects against NVDIMM failures and metadata drive eviction during future reboots or power cycles. This power reset is estimated to take approximately one hour per H610S node. It requires shutting down the node, removing power cables or disconnecting power via a smart PDU, waiting approximately 3 minutes, and reconnecting power.

### *Before you begin*

- You have completed phase 1 of the H610S upgrade process and have upgraded your storage nodes using one the standard Element storage upgrade procedures:
  1. [Upgrade Element software at connected sites](#)
  2. [Upgrade Element software at dark sites](#)



Phase 2 requires on-site personnel.

### *Steps*

1. (Phase 2) Complete the power reset process required for each H610S node in the cluster:



If the cluster also has non-H610S nodes, these non-H610S nodes are exempt from phase 2 and do not need to be shut down or have their power disconnected.

- a. Contact NetApp Support for assistance and to schedule this upgrade.
- b. Follow the phase 2 upgrade procedure in this [KB](#) that is required to complete an upgrade for each H610S node.

## Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Upgrade a management node

You can upgrade your management node to management node version 12.0 from version 11.0 or later.

Choose one of the following management node upgrade options:

- If you are upgrading from management node 11.3 or later:  
[Upgrade a management node to version 12.0 from 11.3 or later](#)
- If you are upgrading from management node 11.0 or 11.1:  
[Upgrade a management node to version 12.0 from 11.1 or 11.0](#)
- If you are upgrading from a management node version 10.x:  
[Migrating from management node version 10.x to 11.x](#)

Choose this option if you have **sequentially** updated (1) your management services version and (2) your Element storage version and you want to **keep** your existing management node:

- If you are keeping existing management node:  
[Reconfigure authentication using the management node REST API](#)



If you do not sequentially update your management services followed by Element storage, you cannot reconfigure reauthentication using this procedure. Follow the appropriate upgrade procedure instead.

### *Before you begin*

- The vCenter Plug-in 4.4 or later requires a management node 11.3 or later that is created with modular architecture and provides individual services.

## Upgrade a management node to version 12.0 from 11.3 or later

You can perform an in-place upgrade of the management node from 11.3 or later to version 12.0 without needing to provision a new management node virtual machine. You can use this procedure if you are upgrading from any of the following management node versions: 11.3, 11.5, 11.7, or 11.8.

### *Before you begin*

- The management node you are intending to upgrade is version 11.3 or later and uses IPv4 networking. The management node version 12.0 does not support IPv6.



To check the version of your management node, log in to your management node and view the Element version number in the login banner.

- You have updated your management services bundle to the latest version using Hybrid Cloud Control (HCC). You can access HCC from the following IP: `<a href="https://&lt;ManagementNodeIP&gt;" class="bare">https://&lt;ManagementNodeIP&gt;</a></code>`
- You have configured an additional network adapter (if required) using the instructions for configuring a storage NIC (eth1) in the management node user guide your product.



Persistent volumes might require an additional network adapter if eth0 is not able to be routed to the SVIP. Configure a new network adapter on the iSCSI storage network to allow the configuration of persistent volumes.

- Storage nodes are running Element 11.3 or later. Use the latest HealthTools to upgrade Element software.

### Steps

1. Log in to the management node virtual machine using SSH or console access.
2. Download the management node ISO for [NetApp HCI](#) or [Element](#) software from the NetApp Support Site to the management node virtual machine.



The name of the ISO is similar to `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. Check the integrity of the download by running md5sum on the downloaded file and compare the output to what is available on NetApp Support Site for NetApp HCI or Element software, as in the following example:

```
sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

4. Mount the management node ISO image and copy the contents to the file system using the following commands:

```
sudo mkdir -p /upgrade
```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso> /mnt
```

```
sudo cp -r /mnt/* /upgrade
```

5. Change to the home directory, and unmount the ISO file from `/mnt`:

```
sudo umount /mnt
```

6. Delete the ISO to conserve space on the management node:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

7. On an 11.3 or later management node, run the following command to upgrade your management node OS version. The script retains all necessary configuration files after the upgrade, such as Active IQ collector and proxy settings.

```
sudo /sf/rftfi/bin/sfrtfti_inplace file:///upgrade/casper/filesystem.squashfs  
sf_upgrade=1
```

The management node reboots with a new OS after the upgrade process completes.

8. On the 11.3 or later management node, run the `redeploy-mnode` script to retain previous management services configuration settings:



The script retains previous management services configuration, including configuration from the Active IQ collector service, controllers (vCenters), or proxy, depending on your settings.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

## Upgrade a management node to version 12.0 from 11.1 or 11.0

You can perform an in-place upgrade of the management node from 11.0 or 11.1 to version 12.0 without needing to provision a new management node virtual machine.

### *Before you begin*

- Storage nodes are running Element 11.3 or later.



Use the latest HealthTools to upgrade Element software.

- The management node you are intending to upgrade is version 11.0 or 11.1 and uses IPv4 networking. The management node version 12.0 does not support IPv6.



To check the version of your management node, log in to your management node and view the Element version number in the login banner. For management node 11.0, the VM memory needs to be manually increased to 12GB.

- You have configured an additional network adapter (if required) using the instructions for configuring a storage NIC (eth1) in the management node user guide your product.



Persistent volumes might require an additional network adapter if eth0 is not able to be routed to the SVIP. Configure a new network adapter on the iSCSI storage network to allow the configuration of persistent volumes.

### Steps

1. Log in to the management node virtual machine using SSH or console access.
2. Download the management node ISO for [NetApp HCI](#) or [Element](#) software from the NetApp Support Site to the management node virtual machine.



The name of the ISO is similar to `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. Check the integrity of the download by running md5sum on the downloaded file and compare the output to what is available on NetApp Support Site for NetApp HCI or Element software, as in the following example:

```
sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

4. Mount the management node ISO image and copy the contents to the file system using the following commands:

```
sudo mkdir -p /upgrade
```

```
sudo mount solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso /mnt
```

```
sudo cp -r /mnt/* /upgrade
```

5. Change to the home directory, and unmount the ISO file from /mnt:

```
sudo umount /mnt
```

6. Delete the ISO to conserve space on the management node:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

7. Run one of the following scripts with options to upgrade your management node OS version. Only run the script that is appropriate for your version. Each script retains all necessary configuration files after the upgrade, such as Active IQ collector and proxy settings.

- a. On an 11.1 (11.1.0.73) management node, run the following command:

```
sudo /sf/rftfi/bin/sftrtfi_inplace file:///upgrade/casper/filesystem.squashfs  
sf_upgrade=1 sf_keep_paths="/sf/packages/solidfire-sioc-4.2.3.2288  
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc /sf/packages/nma"
```

- b. On an 11.1 (11.1.0.72) management node, run the following command:

```
sudo /sf/rftfi/bin/sftrtfi_inplace file:///upgrade/casper/filesystem.squashfs  
sf_upgrade=1 sf_keep_paths="/sf/packages/solidfire-sioc-4.2.1.2281  
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc /sf/packages/nma"
```

- c. On an 11.0 (11.0.0.781) management node, run the following command:

```
sudo /sf/rftfi/bin/sftrtfi_inplace file:///upgrade/casper/filesystem.squashfs  
sf_upgrade=1 sf_keep_paths="/sf/packages/solidfire-sioc-4.2.0.2253  
/sf/packages/solidfire-nma-1.4.8/conf /sf/packages/sioc /sf/packages/nma"
```

The management node reboots with a new OS after the upgrade process completes.

8. On the 12.0 management node, run the **upgrade-mnode** script to retain previous configuration settings.



If you are migrating from an 11.0 or 11.1 management node, the script copies the Active IQ collector to the new configuration format.

- a. For a single storage cluster managed by an existing management node 11.0 or 11.1 with persistent volumes:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true - persistent  
volume> -pva <persistent volume account name - storage volume account>
```

- b. For a single storage cluster managed by an existing management node 11.0 or 11.1 with no persistent volumes:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user>
```

- c. For multiple storage clusters managed by an existing management node 11.0 or 11.1 with persistent volumes:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true - persistent volume> -pva <persistent volume account name - storage volume account> -pvm <persistent volumes mvip>
```

- d. For multiple storage clusters managed by an existing management node 11.0 or 11.1 with no persistent volumes (the **-pvm** flag is just to provide one of the cluster's MVIP addresses):

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pvm <mvip for persistent volumes>
```

9. (For all NetApp HCI installations and SolidFire stand-alone storage installations with NetApp Element Plug-in for vCenter Server) Update the vCenter Plug-in on the 12.0 management node by following the steps in the [Upgrade the Element Plug-in for vCenter Server to version 4.4](#) topic.

10. Use the management node API to add assets:

- a. From a browser, log into the management node REST API UI:

- i. Go to the storage MVIP and log in.

This action causes certificate to be accepted for the next step.

- ii. Open the REST API UI on the management node:

```
https://[management node IP]/mnode
```

- b. From the management node REST API UI, click **Authorize** or any lock icon and complete the following:

- i. Enter the cluster user name and password.

- ii. Enter the client ID as **mnode-client** if the value is not already populated.

- iii. Copy the token URL string and paste it into another browser tab to initiate a token request.

- iv. Click **Authorize** to begin a session.

- v. Close the window.

- c. Run **GET /assets** to find the base asset ID that you will need for the next steps:

- i. Click **GET /assets**.

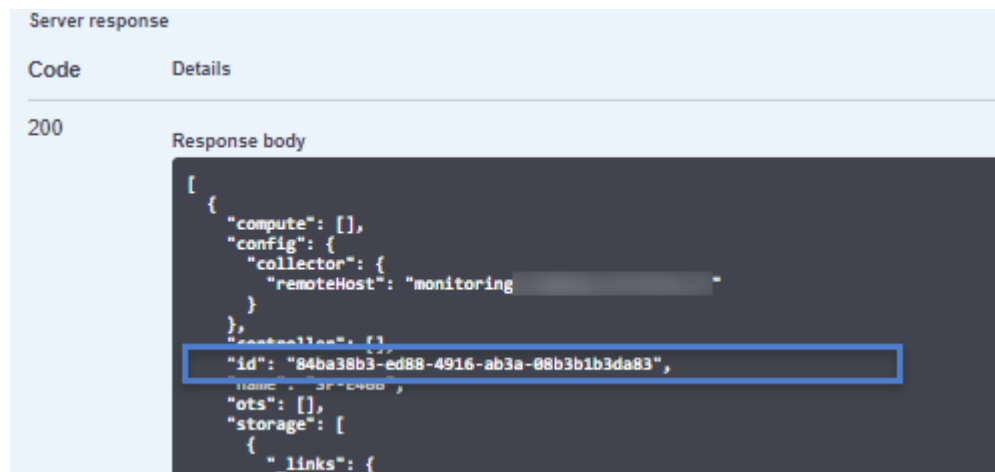
- ii. Click **Try it out**.



iii. Click **Execute**.

iv. Copy the value for **"id"** for the base asset to your clipboard:

NOTE: Your installation has a base asset configuration that was created during installation or upgrade.



d. Add a vCenter controller asset for HCI monitoring (NetApp HCI installations only) and Hybrid Cloud Control (for all installations) to the management node known assets:

i. Click **POST /assets/{asset\_id}/controllers** to add a controller sub-asset.

ii. Click **Try it out**.

iii. Enter the required payload values as defined in the **Model** tab with type **vCenter** and vCenter credentials.

iv. Enter the parent base asset ID you copied to your clipboard in the **asset\_id** field.

v. Click **Execute**.

e. (For NetApp HCI only) Add a compute node asset to the management node known assets:

i. Click **POST/assets/{asset\_id}/compute-nodes** to add a compute node sub-asset with credentials for the compute node asset.

ii. Click **Try it out**.

iii. In the payload, enter the required payload values as defined in the **Model** tab. Use type **ESXi Host** and remove the **hardware\_tag** parameter.

iv. Enter the parent base asset ID you copied to your clipboard in the **asset\_id** field.

v. Click **Execute**.

## Migrating from management node version 10.x to 11.x

If you have a management node at version 10.x, you cannot upgrade from 10.x to 11.x. You can instead use this migration procedure to copy over the configuration from 10.x to a newly deployed 11.1 management node. If your management node is currently at 11.0 or higher, you should skip this procedure. You need management node 11.0 or 11.1 and the latest HealthTools to upgrade Element software from 10.3 + through 11.x.

## Steps

1. From the VMware vSphere interface, deploy the management node 11.1 OVA and power it on.
2. Open the management node VM console, which brings up the terminal user interface (TUI).
3. Use the TUI to create a new administrator ID and assign a password.
4. In the management node TUI, log in to the management node with the new ID and password and validate that it works.
5. From the vCenter or management node TUI, get the management node 11.1 IP address and browse to the IP address on port 9443 to open the management node UI.

```
https://<mNode 11.1 IP address>:9443
```

6. In vSphere, select **NetApp Element Configuration > mNode Settings**. (In older versions, the top-level menu is **NetApp SolidFire Configuration**.)
7. Click **Actions > Clear**.
8. To confirm, click **Yes**. The mNode Status field should report Not Configured.



When you go to the **mNode Settings** tab for the first time, the mNode Status field might display as **Not Configured** instead of the expected **UP**; you might not be able to choose **Actions > Clear**. Refresh the browser. The mNode Status field will eventually display **UP**.

9. Log out of vSphere.
10. In a web browser, open the management node registration utility and select **QoSSIOC Service Management**:

```
https://<mNode 11.1 IP address>:9443
```

11. Set the new QoSSIOC password.



The default password is **solidfire**. This password is required to set the new password.

12. Click the **vCenter Plug-in Registration** tab.
13. Select **Update Plug-in**.
14. Enter required values. When you are finished, click **UPDATE**.
15. Log in to vSphere and select **NetApp Element Configuration > mNode Settings**.
16. Click **Actions > Configure**.
17. Provide the management node IP address, management node user ID (the user name is **admin**),

password that you set on the **QoSSIOC Service Management** tab of the registration utility, and vCenter user ID and password.

In vSphere, the **mNode Settings** tab should display the mNode status as **UP**, which indicates management node 11.1 is registered to vCenter.

18. From the management node registration utility (<https://<mNode 11.1 IP address>:9443>), restart the SIOC service from **QoSSIOC Service Management**.
19. Wait for one minute and check the **NetApp Element Configuration > mNode Settings** tab. This should display the mNode status as **UP**.

If the status is **DOWN**, check the permissions for `/sf/packages/sioc/app.properties`. The file should have read, write, and execute permissions for the file owner. The correct permissions should appear as follows:

```
-rwx-----
```

20. After the SIOC process starts and vCenter displays mNode status as **UP**, check the logs for the `sf-hci-nma` service on the management node. There should be no error messages.
21. (For management node 11.1 only) SSH into the management node version 11.1 with root privileges and start the NMA service with the following commands:

```
# systemctl enable /sf/packages/nma/systemd/sf-hci-nma.service
```

```
# systemctl start sf-hci-nma21
```

22. Perform actions from vCenter to remove a drive, add a drive or reboot nodes. This triggers storage alerts, which should be reported in vCenter. If this is working, NMA system alerts are functioning as expected.
23. If ONTAP Select is configured in vCenter, configure ONTAP Select alerts in NMA by copying the `.ots.properties` file from the previous management node to the management node version 11.1 `/sf/packages/nma/conf/.ots.properties` file, and restart the NMA service using the following command:

```
systemctl restart sf-hci-nma
```

24. Verify that ONTAP Select is working by viewing the logs with the following command:

```
journalctl -f | grep -i ots
```

25. Configure Active IQ by doing the following:

- a. SSH in to the management node version 11.1 and go to the `/sf/packages/collector` directory.
- b. Run the following command:

```
sudo ./manage-collector.py --set-username netapp --set-password --set-mvip <MVIP>
```

- c. Enter the management node UI password when prompted.
- d. Run the following commands:

```
./manage-collector.py --get-all
```

```
sudo systemctl restart sfcollector
```

- e. Verify `sfcollector` logs to confirm it is working.

26. In vSphere, the **NetApp Element Configuration** > **mNode Settings** tab should display the mNode status as **UP**.

27. Verify NMA is reporting system alerts and ONTAP Select alerts.

28. If everything is working as expected, shut down and delete management node 10.x VM.

### Reconfigure authentication using the management node REST API

You can keep your existing management node if you have sequentially upgraded (1) management services and (2) Element storage. If you have followed a different upgrade order, see the procedures for in-place management node upgrades.

#### *Before you begin*

- You have updated your management services to 2.10.29 or later.
- Your storage cluster is running Element 12.0 or later.
- Your management node is 11.3 or later.
- You have sequentially updated your management services followed by upgrading your Element storage. You cannot reconfigure authentication using this procedure unless you have completed upgrades in the sequence described.

#### *Steps*

1. Open the management node REST API UI on the management node:

```
https://[management node IP]/mnode
```

2. Click **Authorize** and complete the following:
  - a. Enter the cluster user name and password.
  - b. Enter the client ID as `mnode-client` if the value is not already populated.
  - c. Click **Authorize** to begin a session.
3. From the REST API UI, click **POST /services/reconfigure-auth**.
4. Click **Try it out**.
5. For the `load_images` parameter, select `true`.
6. Click **Execute**.

The response body indicates that reconfiguration was successful.

### Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Upgrade the Element Plug-in for vCenter Server to version 4.4

For existing vSphere environments with a registered NetApp Element Plug-in for vCenter Server (VCP), you can update your plug-in registration after you first update the management services package that contains the plug-in service.

You can update the plug-in registration on vCenter Server Virtual Appliance (vCSA) or Windows using the registration utility. You must change your registration for the vCenter Plug-in on every vCenter Server where you need to use the plug-in.

This upgrade procedure covers the following upgrade scenarios:

- You are upgrading to a 6.5 or 6.7 HTML5 vSphere Web Client.
- You are upgrading to a 6.5 or 6.7 Flash vSphere Web Client.



The plug-in is not compatible with version 6.7 U2 of the HTML5 vSphere Web Client. It is compatible with the version 6.7 U2 vSphere Web Client for Flash. The plug-in has not yet been tested for use with vSphere 7.0.

### *Before you begin*

- **Admin privileges:** You have vCenter Administrator role privileges to install a plug-in.
- **vSphere upgrades:** You have performed any required vCenter upgrades before upgrading the NetApp Element Plug-in for vCenter Server. This procedure assumes that vCenter upgrades have already been completed.

- **vCenter Server:** Your vCenter Plug-in version 4.x is registered with a vCenter Server. From the registration utility ([https://\[management node IP\]:9443](https://[management node IP]:9443)), click **Registration Status**, complete the necessary fields, and click **Check Status** to verify that the vCenter Plug-in is already registered and the version number of the current installation.
- **Management services updates:** You have updated your [management services bundle](#) to the latest version. Updates to the vCenter plug-in are distributed using management services updates that are released outside of major product releases for NetApp HCI and SolidFire all-flash storage.
- **Management node upgrades:** You are running a management node that has been [upgraded](#) to version 11.3 or later. vCenter Plug-in 4.4 or later requires a an 11.3 or later management node with a modular architecture that provides individual services. Your management node must be powered on with its IP address or DHCP address configured.
- **Element storage upgrades:** You have a cluster running NetApp Element software 11.3 or later.
- **vSphere Web Client:** You have logged out of the vSphere Web Client before beginning any plug-in upgrade. The web client will not recognize updates made during this process to your plug-in if you do not log out.

### Steps

1. Enter the IP address for your management node in a browser, including the TCP port for registration:

[https://\[management node IP\]:9443](https://[management node IP]:9443)

The registration utility UI opens to the **Manage QoSSIOC Service Credentials** page for the plug-in.

**NetApp** NetApp Element Plug-in for vCenter Server Management Node

QoSSIOC Service Management vCenter Plug-in Registration

GoSSIOC Management

Manage Credentials  
Restart QoSSIOC Service

### Manage QoSSIOC Service Credentials

**Warning:** The current QoSSIOC password is set to the default value of 'solidfire'. You should customize credentials to better ensure QoSSIOC service security.

Old Password  Current password

New Password  New password ⓘ

Confirm Password  Confirm New Password ⓘ

**SUBMIT CHANGES**

Contact NetApp Support at <http://mysupport.netapp.com>

2. Click **vCenter Plug-in Registration**.

The screenshot shows the 'vCenter Plug-in - Registration' page. On the left, under 'Manage vCenter Plug-in', the 'Register Plug-in' option is selected. The main area contains registration details: 'vCenter Address' (vCenter Server Address), 'vCenter User' (vCenter Admin User Name), 'vCenter Password' (vCenter Admin Password), and 'Plug-in Zip URL' (with a 'Customize URL' checkbox). A 'REGISTER' button is at the bottom. A footer link points to 'http://mysupport.netapp.com'.

3. Within **Manage vCenter Plug-in**, select **Update Plug-in**.

4. Confirm or update the following information:

- The IPv4 address or the FQDN of the vCenter service on which you will register your plug-in.
- The vCenter Administrator user name.



The user name and password credentials you enter must be for a user with vCenter Administrator role privileges.

- The vCenter Administrator password.
- (For in-house servers/dark sites) A custom URL for the plug-in ZIP.



You can click **Custom URL** to customize the URL if you are using an HTTP or HTTPS server (dark site) or have modified the ZIP file name or network settings. For additional configuration steps if you intend to customize a URL, see Element Plug-in for vCenter Server documentation about modifying vCenter properties for an in-house (dark site) HTTP server.

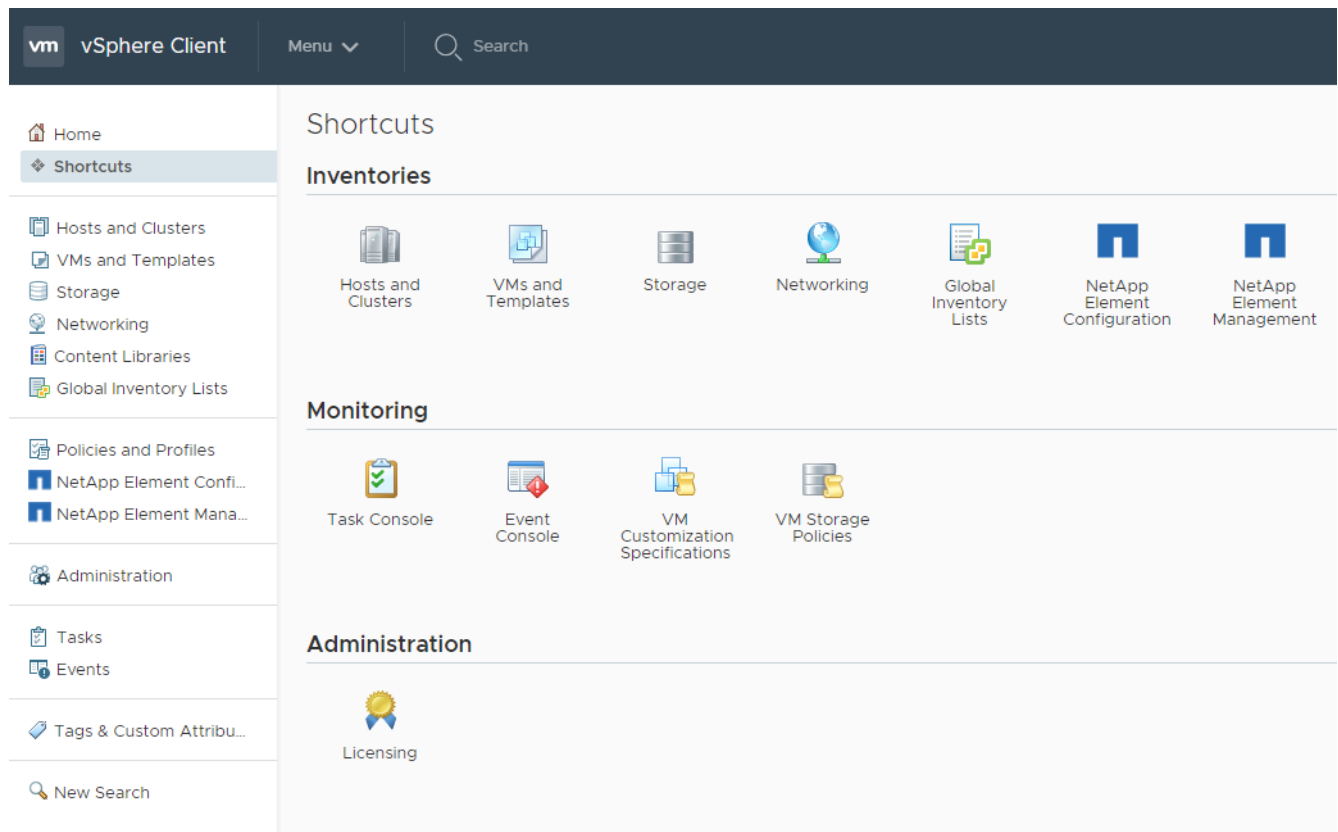
5. Click **Update**.

6. Log in to the vSphere Web Client as a vCenter Administrator.



This action creates a new database and completes the installation in the vSphere Web Client. If the vCenter Plug-in icons are not visible from the vSphere main page, see [Element Plug-in for vCenter Server documentation](#) about troubleshooting the plug-in.

7. Verify that the NetApp Element Configuration and Management extension points appear in the Shortcuts tab of the vSphere Web Client and in the side panel.



If the vCenter Plug-in icons are not visible, see [Element Plug-in for vCenter Server documentation](#) about troubleshooting the plug-in.

8. Verify the version change in the **About** tab in the **NetApp Element Configuration** extension point of the plug-in.

You should see the following version details or details of a more recent version:

NetApp Element Plug-in Version: 4.4.0  
NetApp Element Plug-in Build Number: 72





The vCenter Plug-in contains online Help content. To ensure that your Help contains the latest content, clear your browser cache after upgrading your plug-in.

### Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Run compute node health checks prior to upgrading compute firmware

You must run health checks prior to upgrading compute firmware to ensure all compute nodes in your cluster are ready to be upgraded. Compute node health checks can only be run against compute clusters of one or more managed NetApp HCI compute nodes.

You can run health checks using NetApp Hybrid Cloud Control (HCC) UI or HCC API:

- [Use NetApp Hybrid Cloud Control to run compute node health checks prior to upgrading firmware](#) (Preferred method)
- [Use API to run compute node health checks prior to upgrading firmware](#)

You can also find out more about compute node health checks that are run by the service:

- [Compute node health checks made by the service](#)

### *What you'll need*

- You have updated to the latest management services bundle (2.11 or later).
- You are running management node 11.3 or later.
- Your storage cluster is running NetApp Element software 11.3 or later.

## Use NetApp Hybrid Cloud Control to run compute node health checks prior to upgrading firmware


Using NetApp Hybrid Cloud Control (HCC), you can verify that a compute node is ready for a firmware upgrade.

### *Steps*

1. Open a web browser and browse to the IP address of the management node:

```
https://<ManagementNodeIP>
```

2. Log in to NetApp Hybrid Cloud Control by providing the storage cluster administrator credentials.

3. Click **Upgrade** near the top right of the interface.
4. On the **Upgrades** page, select the **Compute firmware** tab.
5. Click the health check  for the cluster you want to check for upgrade readiness.
6. On the **Compute Health Check** page, click **Run Health Check**.
7. If there are issues, do the following:
  - a. Go to the specific KB article listed for each issue or perform the specified remedy.
  - b. If a KB is specified, complete the process described in the relevant KB article.
  - c. After you have resolved cluster issues, click **Re-Run Health Check**.

After the health check completes without errors, the compute nodes in the cluster are ready to upgrade. See [Update compute node firmware](#) to proceed.

### Use API to run compute node health checks prior to upgrading firmware

You can use REST API to verify that compute nodes in a cluster are ready to be upgraded. The health check verifies that there are no obstacles to upgrading, such as ESXi host issues or other vSphere issues. You will need to run compute node health checks for each compute cluster in your environment.

#### Steps

1. Locate the controller ID and cluster ID:
  - a. Open the inventory service REST API UI on the management node:

```
https://[management node IP]/inventory/1
```
  - b. Click **Authorize** and complete the following:
    - i. Enter the cluster user name and password.
    - ii. Enter the client ID as `mnode-client` if the value is not already populated.
    - iii. Click **Authorize** to begin a session.
  - c. From the REST API UI, click **GET /installations**.
  - d. Click **Try it out**.
  - e. Click **Execute**.
  - f. From the code 200 response body, copy the `"id"` for the installation you plan to use for health checks.
  - g. From the REST API UI, click **GET /installations/{id}**.
  - h. Click **Try it out**.
    - i. Enter the installation ID.

- j. Click **Execute**.
- k. From the code 200 response body, copy the IDs for each of the following:
  - i. The cluster ID ("**clusterID**")
  - ii. A controller ID ("**controllerId**")

```
{
  "_links": {
    "collection": "https://10.117.187.199/inventory/1/installations",
    "self": "https://10.117.187.199/inventory/1/installations/xx94f6f0-12a6-412f-8b5e-4cf2z58329x0"
  },
  "compute": {
    "errors": [],
    "inventory": {
      "clusters": [
        {
          "clusterId": "domain-1",
          "controllerId": "abc12c3a-aa87-4e33-9f94-xx588c2cdcf6",
          "datacenterName": "NetApp-HCI-Datacenter-01",
          "installationId": "xx94f6f0-12a6-412f-8b5e-4cf2z58329x0",
          "installationName": "test-nde-mnode",
          "inventoryType": "managed",
          "name": "NetApp-HCI-Cluster-01",
          "summary": {
            "nodeCount": 2,
            "virtualMachineCount": 2
          }
        }
      ]
    }
  }
},
```

2. Run health checks on the compute nodes in the cluster:

- a. Open the compute service REST API UI on the management node:

```
https://[management node IP]/vcenter/1
```

- b. Click **Authorize** and complete the following:
  - i. Enter the cluster user name and password.
  - ii. Enter the client ID as **mnode-client** if the value is not already populated.
  - iii. Click **Authorize** to begin a session.
- c. Click **POST /compute/{CONTROLLER\_ID}/health-checks**.
- d. Click **Try it out**.

- e. Enter the **"controllerId"** you copied from the previous step in the **Controller\_ID** parameter field.
- f. In the payload, enter the **"clusterId"** that you copied from the previous step as the **"cluster"** value and remove the **"nodes"** parameter.

```
{
  "cluster": "domain-1"
}
```

- g. Click **Execute** to run a health check on the cluster.

The code 200 response gives a **"resourceLink"** URL with the task ID appended that is needed to confirm the health check results.

```
{
  "resourceLink": "https://10.117.150.84/vcenter/1/compute/tasks/[This is the task ID for health check task results]",
  "serviceName": "vcenter-v2-svc",
  "taskId": "ab12c345-06f7-42d7-b87c-7x64x56x321x",
  "taskName": "VCenter service health checks"
}
```

- h. Copy the task ID portion of the **"resourceLink"** URL to verify the task result.
3. Verify the result of the health checks:
- a. Return to the compute service REST API UI on the management node:

```
https://[management node IP]/vcenter/1
```

- b. Click **GET /compute/tasks/{task\_id}**.
- c. Click **Try it out**.
- d. Enter the task ID portion of the **"resourceLink"** URL from the **POST /compute/{CONTROLLER\_ID}/health-checks** code 200 response in the **task\_id** parameter field.
- e. Click **Execute**.
- f. If the **status** returned indicates that there were problems regarding compute node health, do the following:
  - i. Go to the specific KB article (**KbLink**) listed for each issue or perform the specified remedy.
  - ii. If a KB is specified, complete the process described in the relevant KB article.
  - iii. After you have resolved cluster issues, run **POST /compute/{CONTROLLER\_ID}/health-checks** again (see step 2).

If health checks complete without issues, the response code 200 indicates a successful result.

### Compute node health checks made by the service

Compute health checks, whether performed by HCC or API methods, make the following checks per node.

Check description	Node/cluster	Action needed to resolve	Knowledgebase article with procedure
Is DRS enabled and fully automated?	Cluster	Turn on DRS and make sure it is fully automated.	<a href="#">See this KB.</a>
Is DPM disabled in vSphere?	Cluster	Turn off Distributed Power Management.	<a href="#">See this KB.</a>
Is HA admission control enabled in vSphere?	Cluster	Turn off HA admission control.	<a href="#">See this KB.</a>
Is FT enabled for a VM on a host in the cluster?	Node	Suspend Fault Tolerance on any affected virtual machines.	<a href="#">See this KB.</a>
Are there critical alarms in vCenter for the cluster?	Cluster	Launch vSphere and resolve and/or acknowledge any alerts before proceeding.	No KB needed to resolve issue.
Are there generic/global informational alerts in vCenter?	Cluster	Launch vSphere and resolve and/or acknowledge any alerts before proceeding.	No KB needed to resolve issue.
Are management services up to date?	HCI system	You must update management services before you perform an upgrade or run pre-upgrade health checks.	No KB needed to resolve issue.
Are there errors on the current ESXi node in vSphere?	Node	Launch vSphere and resolve and/or acknowledge any alerts before proceeding.	No KB needed to resolve issue.
Is virtual media mounted to a VM on a host in the cluster?	Node	Unmount all virtual media disks (CD/DVD/floppy) from the VMs.	No KB needed to resolve issue.

Check description	Node/cluster	Action needed to resolve	Knowledgebase article with procedure
Is BMC version the minimum required version that has RedFish support?	Node	Manually update your BMC firmware.	No KB needed to resolve issue.
Is ESXi host up and running?	Node	Start your ESXi host.	No KB needed to resolve issue.
Is ESXi host in maintenance mode?	Node	Your ESXi host should be placed in maintenance mode prior to updating firmware.	No KB needed to resolve issue.
Is BMC up and running?	Node	Power on your BMC and ensure it is connected to a network this management node can reach.	No KB needed to resolve issue.
Are there partner ESXi host(s) available?	Node	Make one or more ESXi host(s) in cluster available (not in maintenance mode) to migrate virtual machines.	No KB needed to resolve issue.
Are you able to connect with BMC via IPMI protocol?	Node	Enable IPMI protocol on BMC.	No KB needed to resolve issue.

### Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Update compute node firmware

For any H-Series compute node, you can update the firmware for hardware components such as the BMC, BIOS, and NIC using the RTFI image while leaving the ESXi installation and other configuration data in place.

After the update, the compute node boots into ESXi and works as before, retaining the configuration.

*Before you begin*

See the firmware and driver matrix for your hardware in [NetApp KB article 1088658](#) (login required).

### *About this task*

In production environments, only update the firmware on one compute node at a time.

As an alternative to using the USB thumb drive method described in this procedure, you can mount the compute node RTFI image on the compute node using the **Virtual CD/DVD** option in the Virtual Console in the Baseboard Management Controller (BMC) interface. The BMC method takes considerably longer than the USB thumb drive method. Ensure your workstation or server has the necessary network bandwidth and that your browser session with the BMC does not time out.

### *Steps*

1. Browse to the [NetApp HCI software downloads](#) page and click the download link for correct version of NetApp HCI.
2. Accept the End User License Agreement.
3. Under the **Compute and Storage Nodes** heading, download the NetApp HCI compute node image.
4. Write the raw contents of the compute node RTFI image to a USB thumb drive with at least 32GB capacity (using dd or Etcher).
5. Place the compute node in maintenance mode using VMware vCenter, and evacuate all virtual machines from the host.



If VMware Distributed Resource Scheduler (DRS) is enabled on the cluster (this is the default in NetApp HCI installations), virtual machines will automatically be migrated to other nodes in the cluster.

6. Insert the USB thumb drive into a USB port on the compute node and reboot the compute node using VMware vCenter.
7. During the compute node POST cycle, press **F11** to open the Boot Manager. You may need to press **F11** multiple times in quick succession. You can perform this operation by connecting a video/keyboard or by using the console in **BMC**.
8. Select **One Shot > USB Flash Drive** from the menu that appears. If the USB thumb drive does not appear in the menu, verify that USB Flash Drive is part of the legacy boot order in the BIOS of the system.
9. Press **Enter** to boot the system from the USB thumb drive. The firmware flash process begins.

After firmware flashing is complete and the node reboots, it might take a few minutes for ESXi to start.

10. After the reboot is complete, exit maintenance mode on the updated compute node using vCenter.
11. Remove the USB flash drive from the updated compute node.
12. Repeat this task for other compute nodes in your ESXi cluster until all compute nodes are updated.

## Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Update compute node drivers

For any H-Series compute node, you can update the drivers used on the nodes using VMware Update Manager.

### *Before you begin*

See the firmware and driver matrix for your hardware in [NetApp KB article 1088658](#) (login required).

### *About this task*

Perform only one of these update operations at a time.

### *Steps*

1. Browse to the [NetApp HCI software downloads](#) page and click the download link for correct version of NetApp HCI.
2. Accept the End User License Agreement.
3. Under the **Driver Packages for VMWare ESXi** heading, download the driver package for your node type and ESXi version.
4. Extract the downloaded driver bundle on your local computer.



The NetApp driver bundle includes one or more VMware Offline Bundle ZIP files; do not extract these ZIP files.

5. After upgrading the firmware on the compute nodes, go to **VMware Update Manager** in vCenter.
6. Import the driver offline bundle file for the compute nodes into the **Patch Repository**.
7. Create a new host baseline for the compute node.
8. Choose **Host Extension** for Name and Type and select all imported driver packages to be included in the new baseline.
9. In the **Host and Clusters** menu in vCenter, select the cluster with the compute nodes you would like to update and navigate to the **Update Manager** tab.
10. Click **Remediate** and then select the newly created host baseline. Ensure that drivers included in the baseline are selected.
11. Proceed through the wizard to the **Host Remediation Options** and ensure that the **Do Not Change VM Power State** option is selected to keep virtual machines online during the driver update.





If VMware Distributed Resource Scheduler (DRS) is enabled on the cluster (this is the default in NetApp HCI installations), virtual machines will automatically be migrated to other nodes in the cluster.

12. Proceed to the **Ready to Complete** page in the wizard and click **Finish**.

The drivers for all compute nodes in the cluster are updated one node at a time while virtual machines stay online.

#### Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## vSphere upgrade sequences with vCenter Plug-in

### Upgrade your vSphere components for a NetApp HCI system with the Element Plug-in for vCenter Server

When you upgrade the VMware vSphere components of your NetApp HCI installation, there are some additional steps you will need to take for the Element Plug-in for vCenter Server.

#### Steps

1. For vCSA upgrades, [clear](#) mNode settings in the plug-in (**NetApp Element Configuration > mNode Settings**). The **mNode Status** field displays **Not Configured** after the process is complete.
2. For vCSA and Windows upgrades, [unregister](#) the plug-in from the vCenter Server with which it is associated using the registration utility.
3. [Upgrade vSphere, including vCenter Server, ESXi, VMs, and other VMware components.](#)



When upgrading ESXi for compute nodes for a [two-node cluster](#), upgrade only one compute node at a time so that only one witness node is temporarily unavailable and cluster quorum can be maintained.

4. [Register](#) the Element Plug-in for vCenter Server again with vCenter.
5. [Add clusters](#) using the plug-in.
6. [Configure QoSSIOC settings](#) using the plug-in.
7. [Enable QoSSIOC](#) for all datastores controlled by the plug-in.

#### Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)
- [NetApp HCI Two-Node Storage Cluster Technical Report](#)

## Upgrade your vSphere components for a NetApp SolidFire storage system with the Element Plug-in for vCenter Server

When you upgrade the VMware vSphere components of your SolidFire Element storage installation, there are some additional steps you will need to take for systems with Element Plug-in for vCenter Server.

### *Steps*

1. For vCSA upgrades, [clear](#) mNode settings in the plug-in (**NetApp Element Configuration > mNode Settings**). The **mNode Status** field displays **Not Configured** after the process is complete.
2. For vCSA and Windows upgrades, [unregister](#) the plug-in from the vCenter Server with which it is associated using the registration utility.
3. [Upgrade vSphere, including vCenter Server, ESXi, VMs, and other VMware components.](#)
4. [Register](#) the Element Plug-in for vCenter Server again with vCenter.
5. [Add clusters](#) using the plug-in.
6. [Configure QoSSIOC settings](#) using the plug-in.
7. [Enable QoSSIOC](#) for all datastores controlled by the plug-in.

### Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

# Expand your NetApp HCI system

## Expansion overview

You can expand your NetApp HCI system by using NetApp Hybrid Cloud Control. You can expand storage or compute resources separately or expand them at the same time.

After installing the node in the NetApp HCI chassis, you use NetApp Hybrid Cloud Control to configure NetApp HCI to utilize the new resources. NetApp HCI detects the existing network configuration and offers you configuration options within the existing networks and VLANs, if any.



If you recently expanded your installation and the new assets were not added automatically to your configuration, you might need to add the assets manually. See the [Management Node User Guide](#).

NetApp HCI uses VMware Enhanced vMotion Compatibility (EVC) to ensure vMotion functionality when there are compute nodes with different CPU generations in the vSphere cluster. When EVC is required for expansion, NetApp HCI enables it automatically whenever possible.

In the following situations, you might need to manually change EVC settings in the vSphere client to complete expansion:

- The existing compute nodes have a newer CPU generation than the compute nodes you are trying to add.
- The controlling vCenter instance does not support the required EVC level.
- The compute nodes you are trying to add have an older CPU generation than the EVC setting of the controlling vCenter instance.



When expanding NetApp HCI compute or storage resources in the NetApp Deployment Engine, you should connect to the vCenter instance that manages your existing NetApp HCI compute nodes.

## Find more information

- [NetApp HCI Resources page](#)
- [NetApp HCI Documentation Center](#)

## Expand NetApp HCI storage resources

After you finish NetApp HCI deployment, you can expand and configure NetApp

## HCI storage resources by using NetApp Hybrid Cloud Control.

### Before you begin

- Ensure that you have free and unused IPv4 addresses on the same network segment as existing nodes (each new node must be installed on the same network as existing nodes of its type).
- Ensure that you have one of the following types of SolidFire storage cluster accounts:
  - The native administrator account that was created during initial deployment
  - A custom user account with Cluster Admin, Drives, Volumes, and Nodes permissions
- Ensure that you have performed the following actions with each new node:
  - Installed the new node in the NetApp HCI chassis by following the installation instructions available in the [NetApp HCI Documentation Center](#).
  - Cabled and powered on the new node
- Ensure that you have the management IPv4 address of an already installed storage node. You can find the IP address in the **NetApp Element Management > Cluster > Nodes** tab of the NetApp Element Plug-in for vCenter Server.
- Ensure that each new node uses the same network topology and cabling as the existing storage or compute clusters.



When you are expanding storage resources, storage capacity should be split evenly across all chassis for the best reliability.

### Steps

1. Open a web browser and browse to the IP address of the management node. For example:

```
https://[management node IP address]
```

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.
3. Click **Expand** at the top right corner of the interface.

The browser opens the NetApp Deployment Engine.

4. Log in to the NetApp Deployment Engine by providing the NetApp HCI storage cluster administrator credentials.
5. On the **Welcome** page, click **No** and click **Continue**.
6. On the **Available Inventory** page, select the storage nodes you want to add and click **Continue**.
7. On the **Network Settings** page, some of the network information has been detected from the initial deployment. Each new storage node is listed by serial number, and you need to assign the new

network information to it. For each new storage node, complete the following steps:

- a. **Hostname:** If NetApp HCI detected a naming prefix, copy it from the Detected Naming Prefix field, and insert it as the prefix for the new unique hostname you add in the Hostname field.
- b. **Management Address:** Enter a management IP address for the new storage node that is within the management network subnet.
- c. **Storage (iSCSI) IP Address:** Enter an iSCSI IP address for the new storage node that is within the iSCSI network subnet.
- d. Click **Continue**.



NetApp HCI might take some time to validate the IP addresses you enter. The Continue button becomes available when IP address validation completes.

8. On the **Review** page in the Network Settings section, new nodes are shown in the bold text. To make changes in any section, do the following:
  - a. Click **Edit** for that section.
  - b. After you finish, click **Continue** on any subsequent pages to return to the Review page.
9. **Optional:** If you do not want to send cluster statistics and support information to NetApp hosted Active IQ servers, clear the final checkbox.

This disables real-time health and diagnostic monitoring for NetApp HCI. Disabling this feature removes the ability for NetApp to proactively support and monitor NetApp HCI to detect and resolve issues before production is impacted.

10. Click **Add Nodes**.

You can monitor the progress while NetApp HCI adds and configures the resources.

11. **Optional:** Verify that any new storage nodes are visible in the Element Plug-in for vCenter Server.



If you expanded a two-node storage cluster to four nodes or more, the pair of Witness Nodes previously used by the storage cluster are still visible as standby virtual machines in vSphere. The newly expanded storage cluster does not use them; if you want to reclaim VM resources, you can [manually remove](#)^ the Witness Node virtual machines.

## Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

# Expand NetApp HCI compute resources

After you finish NetApp HCI deployment, you can expand and configure NetApp HCI compute resources by using NetApp Hybrid Cloud Control.

## Before you begin

- Ensure that the vSphere instance of NetApp HCI is using vSphere Enterprise Plus licensing if you are expanding a deployment with Virtual Distributed Switches.
- Ensure that none of the vCenter or vSphere instances in use with NetApp HCI have expired licenses.
- Ensure that you have free and unused IPv4 addresses on the same network segment as existing nodes (each new node must be installed on the same network as existing nodes of its type).
- Ensure that you have the vCenter administrator account credentials ready.
- Ensure that you have performed the following actions with each new node:
  - Installed the new node in the NetApp HCI chassis by following the installation instructions available in the [NetApp HCI Documentation Center](#).
  - Cabled and powered on the new node
- Ensure that each new node uses the same network topology and cabling as the existing storage or compute clusters.

## Steps

1. Open a web browser and browse to the IP address of the management node. For example:

```
https://[management node IP address]
```

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.
3. Click **Expand** at the top right corner of the interface.

The browser opens the NetApp Deployment Engine.

4. Log in to the NetApp Deployment Engine by providing the NetApp HCI storage cluster administrator credentials.
5. On the **Welcome** page, click **Yes** and click **Continue**.
6. On the **End User License** page, read the VMware End User License Agreement and click **I accept** to accept the terms and click **Continue**.
7. On the **vCenter** page, complete the following steps:
  - a. Enter a FQDN or IP address and administrator credentials for the vCenter instance associated

with your NetApp HCI installation.

b. Click **Continue**.

c. Select a vSphere datacenter where you want to add the compute nodes, or click **Create New Datacenter** to add the compute nodes to a new datacenter.



If you click Create New Datacenter, the Cluster field is automatically populated.

d. If you selected an existing datacenter, select a vSphere cluster with which the new compute nodes should be associated.



If NetApp HCI cannot recognize the network settings of the cluster you have selected for expansion, ensure that the vmkernel and vmnic mapping for the management, storage and vMotion networks are set to the deployment defaults. See Supported networking changes in the [NetApp HCI Documentation Center](#) for more information.

e. Click **Continue**.

8. On the **ESXi Credentials** page, enter an ESXi root password for the compute node or nodes you are adding.

You should use the same password that was created during the initial NetApp HCI deployment.

9. Click **Continue**.

10. If you created a new vSphere datacenter cluster, on the **Network Topology** page, select a network topology to match the new compute nodes you are adding.



You can select the two-cable option only if your compute nodes are using the two-cable topology and the existing NetApp HCI deployment is configured with VLAN IDs.

11. On the **Available Inventory** page, select the nodes you want to add to the existing NetApp HCI installation.



For some compute nodes, you might need to enable EV at the highest level that your vCenter version supports before you can add them to your installation. You need to use the vSphere client to enable EVC for these compute nodes. After you enable it, refresh the Inventory page and try adding the compute nodes again.

12. Click **Continue**.

13. **Optional:** If you created a new vSphere datacenter cluster, on the **Network Settings** page, import network information from an existing NetApp HCI deployment by selecting the **Copy Setting from an Existing Cluster** checkbox.

This populates the default gateway and subnet information for each network.

14. On the **Network Settings** page, some of the network information has been detected from the initial deployment. Each new compute node is listed by serial number, and you need to assign new network information to it. For each new compute node, complete the following steps:
  - a. **Hostname:** If NetApp HCI detected a naming prefix, copy it from the **Detected Naming Prefix** field, and insert it as the prefix for the new hostname.
  - b. **Management IP Address:** Enter a management IP address for the new compute node that is within the management network subnet.
  - c. **vMotion IP Address:** Enter a vMotion IP address for the new compute node that is within the vMotion network subnet.
  - d. **iSCSI A - IP Address:** Enter an IP address for the first iSCSI port of the compute node that is in the iSCSI network subnet.
  - e. **iSCSI B - IP Address:** Enter an IP address for the second iSCSI port of the compute node that is in the iSCSI network subnet
  - f. Click **Continue**.
15. On the **Review** page in the Network Settings section, new nodes are shown in the bold text. To make changes in any section, do the following:
  - a. Click **Edit** for that section.
  - b. After you finish, click **Continue** on any subsequent pages to return to the **Review** page.
16. **Optional:** If you do not want to send cluster statistics and support information to NetApp hosted SolidFire Active IQ servers, clear the final checkbox.

This disables real-time health and diagnostic monitoring for NetApp HCI. Disabling this feature removes the ability for NetApp to proactively support and monitor NetApp HCI to detect and resolve issues before production is impacted.

17. Click **Add Nodes**.

You can monitor the progress while NetApp HCI adds and configures the resources.

18. **Optional:** Verify that any new compute nodes are visible in the VMware vSphere Web Client.

## Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)



# Expand NetApp HCI storage and compute resources at the same time

After you finish NetApp HCI deployment, you can expand and configure NetApp HCI storage and compute resources at the same time by using NetApp Hybrid Cloud Control.

## Before you begin

- Ensure that the vSphere instance of NetApp HCI is using vSphere Enterprise Plus licensing if you are expanding a deployment with Virtual Distributed Switches.
- Ensure that none of the vCenter or vSphere instances in use with NetApp HCI have expired licenses.
- Ensure that you have the vCenter administrator account credentials ready.
- Ensure that you have free and unused IPv4 addresses on the same network segment as existing nodes (each new node must be installed on the same network as existing nodes of its type).
- Ensure that you have one of the following types of SolidFire storage cluster accounts:
  - The native administrator account that was created during initial deployment
  - A custom user account with Cluster Admin, Drives, Volumes, and Nodes permissions
- Ensure that you have performed the following actions with each new node:
  - Installed the new node in the NetApp HCI chassis by following the installation instructions available in the [NetApp HCI Documentation Center](#).
  - Cabled and powered on the new node
- Ensure that you have the management IPv4 address of an already installed storage node. You can find the IP address in the **NetApp Element Management > Cluster > Nodes** tab of the NetApp Element Plug-in for vCenter Server.
- Ensure that each new node uses the same network topology and cabling as the existing storage or compute clusters.

## About this task

- You can intermix the H410C compute node with existing NetApp HCI compute and storage nodes in the same chassis and cluster.
- You cannot intermix compute nodes and BPU-enabled compute nodes in the same cluster. If you select a GPU-enabled compute node, CPU-only compute nodes become unselectable, and vice versa.
- If you are adding compute nodes with CPU generations that are different than the CPU generation of the existing compute nodes and Enhanced vMotion Compatibility (EVC) is disabled on the controlling vCenter instance, you must enable EVC before proceeding. This ensures vMotion functionality after expansion is complete.

## Steps

1. Open a web browser and browse to the IP address of the management node. For example:

```
https://[management node IP address]
```

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.
3. Click **Expand** at the top right corner of the interface.

The browser opens the NetApp Deployment Engine.

4. Log in to the NetApp Deployment Engine by providing the NetApp HCI storage cluster administrator credentials.
5. On the **Welcome** page, click **Yes** and click **Continue**.
6. On the **End User License** page, read the VMware End User License Agreement and click **I accept** to accept the terms and click **Continue**.
7. On the **vCenter** page, complete the following steps:
  - a. Enter a FQDN or IP address and administrator credentials for the vCenter instance associated with your NetApp HCI installation.
  - b. Click **Continue**.
  - c. Select a vSphere datacenter where you want to add the compute nodes, or click **Create New Datacenter** to add the compute nodes to a new datacenter.



If you click **Create New Datacenter**, the **Cluster** field is automatically populated.

- d. If you selected an existing datacenter, select a vSphere cluster with which the new compute nodes should be associated.



If NetApp HCI cannot recognize the network settings of the cluster you have selected for expansion, ensure that the vmkernel and vmnic mapping for the management, storage and vMotion networks are set to the deployment defaults. See Supported networking changes in the [NetApp HCI Documentation Center](#) for more information.

- e. Click **Continue**.
8. On the **ESXi Credentials** page, enter an ESXi root password for the compute node or nodes you are adding.

You should use the same password that was created during the initial NetApp HCI deployment.

9. Click **Continue**.

10. If you created a new vSphere datacenter cluster, on the **Network Topology** page, select a network topology to match the new compute nodes you are adding.



You can select the two-cable option only if your compute nodes are using the two-cable topology and the existing NetApp HCI deployment is configured with VLAN IDs.

11. On the **Available Inventory** page, select the storage and compute nodes you want to add and click **Continue**.



For some compute nodes, you might need to enable EV at the highest level that your vCenter version supports before you can add them to your installation. You need to use the vSphere client to enable EVC for these compute nodes. After you enable it, refresh the Inventory page and try adding the compute nodes again.

12. Click **Continue**.

13. **Optional:** If you created a new vSphere datacenter cluster, on the **Network Settings** page, import network information from an existing NetApp HCI deployment by selecting the **Copy Setting from an Existing Cluster** checkbox.

This populates the default gateway and subnet information for each network.

14. On the **Network Settings** page, some of the network information has been detected from the initial deployment. Each new storage node is listed by serial number, and you need to assign the new network information to it. For each new storage node, complete the following steps:

- a. **Hostname:** If NetApp HCI detected a naming prefix, copy it from the Detected Naming Prefix field, and insert it as the prefix for the new unique hostname you add in the Hostname field.
- b. **Management Address:** Enter a management IP address for the new storage node that is within the management network subnet.
- c. **Storage (iSCSI) IP Address:** Enter an iSCSI IP address for the new storage node that is within the iSCSI network subnet.
- d. Click **Continue**.



NetApp HCI might take some time to validate the IP addresses you enter. The Continue button becomes available when IP address validation completes.

15. On the **Review** page in the Network Settings section, new nodes are shown in the bold text. To make changes in any section, do the following:

- a. Click **Edit** for that section.
- b. After you finish, click **Continue** on any subsequent pages to return to the Review page.

16. **Optional:** If you do not want to send cluster statistics and support information to NetApp hosted Active IQ servers, clear the final checkbox.

This disables real-time health and diagnostic monitoring for NetApp HCI. Disabling this feature removes the ability for NetApp to proactively support and monitor NetApp HCI to detect and resolve issues before production is impacted.

17. Click **Add Nodes**.

You can monitor the progress while NetApp HCI adds and configures the resources.

18. **Optional:** Verify that any new nodes are visible in the VMware vSphere Web Client (for compute nodes) or the Element Plug-in for vCenter Server (for storage nodes).



If you expanded a two-node storage cluster to four nodes or more, the pair of Witness Nodes previously used by the storage cluster are still visible as standby virtual machines in vSphere. The newly expanded storage cluster does not use them; if you want to reclaim VM resources, you can [manually remove](#) the Witness Node virtual machines.

## Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Remove Witness Nodes after expanding cluster

After you expand a two-node storage cluster to four or more nodes, you can delete the pair of Witness Nodes to free up compute resources in your NetApp HCI installation. The Witness Nodes previously used by the storage cluster are still visible as standby virtual machines (VM) in vSphere Web Client.

### *About this task*

Witness Nodes are not required in clusters with more than four storage nodes. This is an optional procedure if you want to free up CPU and memory after you expand your two-node cluster to four or more nodes.



Verify that no cluster faults or errors are reported. You can find information about system alerts by clicking **Reporting > Alerts** in the NetApp Element Management extension point in vSphere.

### *Steps*

1. From vSphere, access the NetApp Element Management extension point from the **Shortcuts** tab or

the side panel.

2. Select **NetApp Element Management > Cluster > Nodes**.

NetApp Element Management

Cluster **SFPS-CLUSTER** MVIP: 10.146 SVIP: 10.84 vCenter: 10.140

Getting Started Reporting Management Protection **Cluster** VVols

<input type="checkbox"/>	Node ID	Node Name	Node State	Available 4k IOPS	Node Role	Node Type	Active Drives	Management IP	Storage IP	Management VLAN ID	Storage VLAN
<input type="checkbox"/>	1	sfps-stg-01	Active	50000	Ensemble Node	H410S-0	6	10.147	10.85	0	101
<input type="checkbox"/>	2	sfps-stg-02	Active	50000	Ensemble Node, Cluster Master	H410S-0	6	10.148	10.86	0	101
<input checked="" type="checkbox"/>	3	sfps-witness-01	Active	0		SFVIRT	0	10.42	10.90		
<input checked="" type="checkbox"/>	4	sfps-witness-02	Active	0		SFVIRT	0	10.43	10.91		
<input type="checkbox"/>	5	sfps-stg-03	Active	50000	Ensemble Node	H410S-0	6	10.149	10.87	0	101
<input type="checkbox"/>	6	sfps-stg-04	Active	50000		H410S-0	6	10.150	10.88	0	101

3. Select the checkbox for the Witness Node that you want to delete, and click **Actions > Remove**.
4. Confirm the action in the prompt.
5. Click **Hosts and Clusters**.
6. Navigate to the Witness Node VM that you removed earlier.
7. Right-click the VM and power it off.
8. Right-click the VM that you powered off, and click **Delete from Disk**.
9. Confirm the action in the prompt.

## Find more information

- [NetApp HCI Two-Node Storage Cluster | TR-4823](#)
- [NetApp HCI Documentation Center](#)
- [SolidFire and Element Software Documentation Center](#)

# Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

## Copyright

<http://www.netapp.com/us/legal/copyright.aspx>

## Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/us/media/patents-page.pdf>

## Privacy policy

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## Open source

Notice files provide information about third-party copyright and licenses.

- [Notice for Management Services 2.11^](#)
- [Notice for NetApp HCI 1.8](#)

## Copyright Information

Copyright © 2020 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## 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.