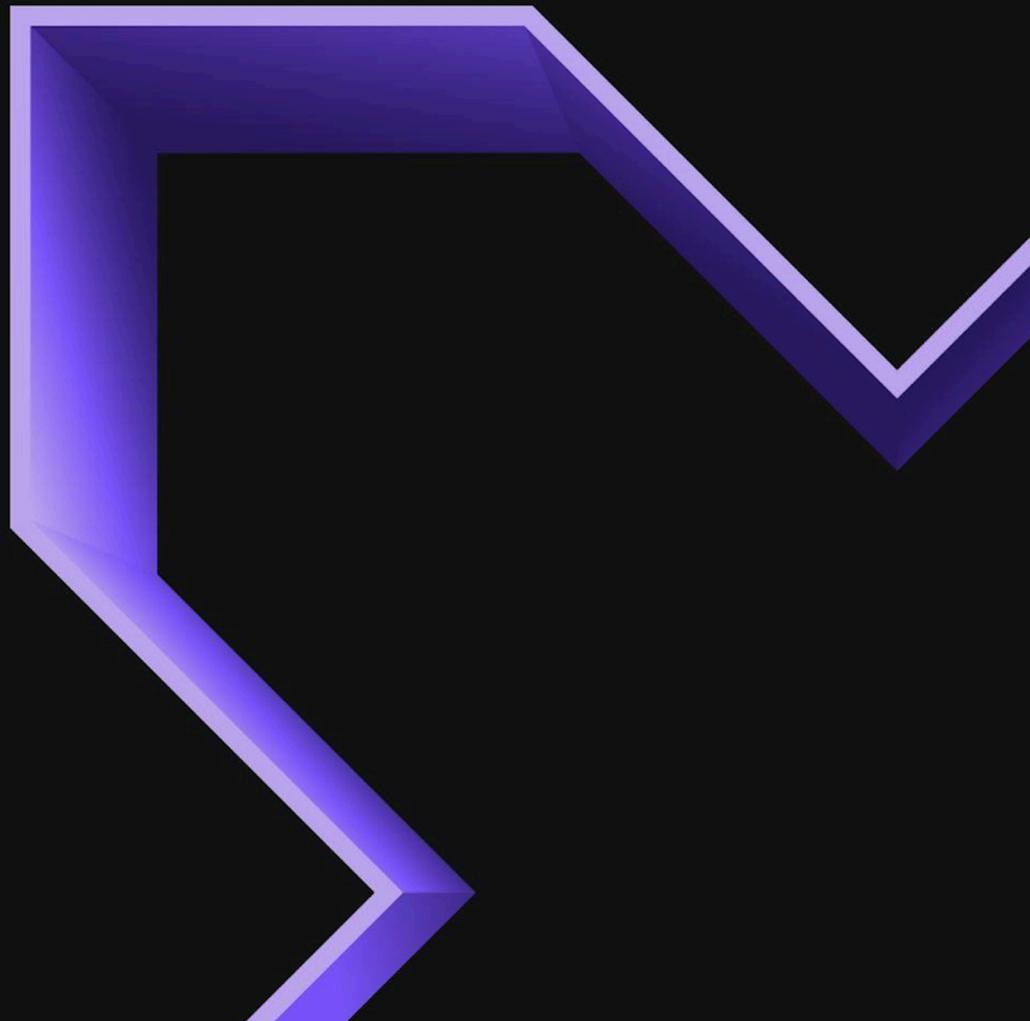


# Prism Element Web Console Guide

Prism 7.3

August 14, 2025



# Contents

<b>Help Organization.....</b>	<b>8</b>
<b>Nutanix Platform Overview.....</b>	<b>9</b>
Guest VM Data Management.....	9
MapReduce Tiering.....	10
Live Migration.....	10
High Availability.....	10
Virtualization Management VM High Availability.....	11
Data Path Redundancy.....	11
Cluster Components.....	12
Zeus.....	12
Zookeeper.....	12
Medusa.....	13
Cassandra.....	13
Stargate.....	13
Curator.....	13
Prism.....	13
Single-node Clusters.....	14
Two-Node Clusters.....	17
Cluster Resiliency.....	21
Failure Handling in a Nutanix Cluster.....	21
Cluster Fault Tolerance.....	25
Fault Domains in a Nutanix Cluster.....	29
Cluster Rebuild Preference.....	39
Replication Factor.....	40
Replication Factor 2.....	41
Replication Factor 3.....	41
Replication Factor 1.....	41
Degraded Node.....	44
Degraded Node Detection.....	47
Enabling or Disabling Degraded Node Detection.....	48
Managing a Degraded Node.....	49
Maximum System Values.....	51
Three Node Cluster Considerations.....	52
<b>Cluster Management.....</b>	<b>53</b>
Prism Element Web Console Overview.....	53
Logging Into the Prism Element Web Console.....	54
Logging Out of the Prism Element Web Console.....	56
Main Menu.....	56
Settings Menu.....	59
Home Dashboard.....	62
Monitoring Disk Rebuild Progress.....	67
Monitoring Node Rebuild Progress.....	68
Understanding Displayed Statistics.....	69
Modifying UI Settings.....	70
Finding the AHV Version on Prism Element.....	72

Finding the AOS Version Using Prism Element.....	72
Prism Licensing.....	73
Modifying Cluster Details.....	73
Virtual IP Address Impact.....	74
iSCSI Data Services IP Address Impact.....	75
Cluster Fault Tolerance Configuration.....	75
Increasing the Cluster Fault Tolerance Level.....	75
Modifying Cluster Rebuild Preference.....	77
Software and Firmware Upgrades.....	77
Life Cycle Management (LCM).....	78
Nutanix Cluster Check (NCC).....	78
Use 1-Click Upgrade in the Prism Element Web Console.....	79
View Task Status.....	87
Multi-Cluster Management.....	91
Installing Prism Central Using 1-Click Method.....	91
Registering a Cluster with Prism Central.....	94
Restoring Prism Central (One-Click Recovery).....	95
CVM Memory Configuration.....	99
Increasing the Controller VM Memory Size.....	100
Resource Requirements Supporting Snapshot Frequency (Asynchronous, NearSync, and Metro).....	101
Rebooting an AHV or ESXI Node in a Nutanix Cluster.....	101
 <b>Storage Management.....</b>	<b>102</b>
Storage Components.....	102
Capacity Management.....	105
Capacity Reservation Best Practices.....	105
Cluster Resilient Capacity.....	105
Configuring a Warning Threshold for Resilient Capacity.....	106
Rebuild Capacity Reservation.....	107
Storage Efficiency.....	110
Deduplication.....	110
Compression.....	111
Erasure Coding.....	112
Storage Dashboard.....	117
Storage Overview View.....	117
Storage Diagram View.....	120
Storage Table View.....	124
Modifying a Storage Pool.....	131
Creating a Storage Container.....	131
Modifying a Storage Container.....	135
Deleting a Storage Container.....	136
Replication Factor Configuration.....	137
Increasing the Replication Factor using CLI.....	137
Enabling Replication Factor 1.....	139
Disabling Replication Factor 1.....	139
Volume Group Configuration.....	140
Concurrent Access from Multiple Clients.....	140
Creating a Volume Group.....	141
Modifying a Volume Group.....	142
Deleting a Volume Group.....	143
Cloning a Volume Group.....	144
Flash Mode for Virtual Machines, Disks, and Volume Groups.....	144
Disabling Flash Mode from Virtual Disks of a Volume Group.....	146
Recycle Bin.....	146

Recycle Bin Guidelines and Limitations.....	146
Enabling Recycle Bin.....	147
Disabling Recycle Bin.....	148
Viewing Recycle Bin Space Usage.....	148
Clearing Storage Space Used by the Recycle Bin.....	148
<b>Network Management.....</b>	<b>150</b>
Network Configuration for Cluster.....	150
Creating a Virtual Switch.....	151
Updating a Virtual Switch.....	154
Deleting a Virtual Switch.....	155
Migrating Bridges after Upgrade.....	156
MAC Address Prefix.....	159
Network Configuration for VM Interfaces.....	162
Creating a Basic VLAN Subnet for Guest VM Interfaces.....	162
Network Segmentation.....	166
Configuring a Network Switch.....	167
Modifying a Network Switch Configuration.....	168
Deleting a Network Switch.....	169
Enabling LACP and LAG (AHV Only).....	169
Create an SNMP profile for the network switch.....	172
Modifying an SNMP Profile.....	173
Deleting an SNMP Profile.....	174
Network Visualization.....	174
Prerequisites.....	174
Network Visualizer.....	175
Viewing the Network Visualizer.....	176
Customizing the Topology View.....	176
Viewing VM NIC Information.....	177
Viewing Host Information.....	179
View Switch Information.....	180
<b>Hardware Management.....</b>	<b>182</b>
Hardware Dashboard.....	182
Hardware Overview View.....	182
Hardware Diagram View.....	183
Hardware Table View.....	191
Expanding a Cluster.....	198
Prerequisites and Requirements.....	204
Expand a Cluster with Flow Virtual Networking Enabled.....	209
Node Maintenance.....	217
Node Maintenance Mode.....	217
Viewing a Node that is in Maintenance Mode.....	220
Guest VM Status when Node is in Maintenance Mode.....	221
Repair Boot Disks.....	222
Cluster Modifications.....	222
Adding a Disk.....	222
Removing a Disk.....	224
Node Removal from a Cluster.....	224
Adding a Node.....	228
Compute-Only and Storage-Only Nodes Management.....	229
Compute-Only Nodes.....	229
Storage-Only Nodes.....	230

Deployment Specifications and Considerations for Compute-Only and Storage-Only Nodes.....	231
Deployment of Compute-Only Nodes.....	238
Deployment of Storage-only Nodes.....	240
Optimized Database Solution.....	241
Operation Specifications for Optimized Database Solution.....	242
Cluster Requirements for Optimized Database Solution.....	242
Licensing Requirements for Optimized Database Solution.....	244
Configuration and Operation Limits for Optimized Database Solution.....	245
Supported Hardware Platforms for Optimized Database Solution.....	246
Networking Configurations for Compute-Only Nodes in Optimized Database Solution....	246
Deployment of Compute-Only and Storage-Only nodes in Optimized Database Solution.....	247
<b>Nutanix Volumes.....</b>	<b>249</b>
<b>File Server Management.....</b>	<b>250</b>
<b>Data Protection.....</b>	<b>251</b>
<b>Health Monitoring.....</b>	<b>252</b>
Health Dashboard.....	252
Configuring Health Checks.....	255
Configuring NCC Frequency.....	256
Running Checks by Using Prism Element Web Console.....	257
Collecting Logs by Using Prism Element Web Console.....	257
<b>Virtual Machine Management.....</b>	<b>260</b>
VM Dashboard.....	260
VM Overview View.....	261
VM Table View.....	262
VM Management.....	270
Creating a VM (AHV).....	270
Managing a VM (AHV).....	276
Virtual Machine Snapshots.....	282
Adding Multiple vGPUs to the Same VM.....	283
Migrating Live a vGPU-enabled VM Within the Cluster.....	284
VM Management through Prism Element (ESXi).....	285
Creating a VM (ESXi).....	286
Managing a VM (ESXi).....	288
Configuring Images.....	292
Virtual Machine Customization.....	293
Customizing Linux Virtual Machines with Cloud-Init.....	294
Customization of Windows Virtual Machines with System Preparation.....	299
VM High Availability in Acropolis.....	300
Enabling High Availability Reservations for the Cluster.....	301
Nutanix Guest Tools.....	302
Enabling NGT and Mounting the NGT Installer in a VM.....	303
NGT Installation.....	304
Manage Bulk Operations for NGT.....	309
Enabling NGT and Mounting the NGT Installer on Cloned VMs.....	316

Automatic Regeneration of NGT Certificates.....	317
Upgrading NGT.....	318
Reconfiguring NGT.....	318
Uninstalling and Removing Nutanix Guest Tools.....	318
NGT Metrics Collection for Windows Performance Monitor.....	321
VM-Host Affinity Policies Defined in Prism Element.....	324
Configuring Legacy VM-VM Anti-Affinity Policy.....	324
Connect to Citrix Cloud.....	326
Connecting to the Citrix Cloud.....	326
Guest VM Cluster Configuration (AHV Only).....	328
Creating a Guest VM Cluster by Directly Attaching a Volume Group (AHV Only).....	328
<b>Performance Monitoring.....</b>	<b>330</b>
Analysis Dashboard.....	330
Creating an Entity Chart.....	332
Creating a Metric Chart.....	332
Chart Metrics.....	333
Exporting Performance Data.....	342
<b>Alerts and Events.....</b>	<b>344</b>
<b>View Task Status.....</b>	<b>345</b>
View Task Status Dashboard.....	346
<b>System Management.....</b>	<b>348</b>
Configuring a Filesystem Whitelist.....	348
Configuring Name Servers.....	349
Cluster Time Synchronization.....	349
Recommendations for Time Synchronization.....	349
Configuring NTP Servers.....	350
Configuring an SMTP Server.....	351
Configuring SNMP.....	351
Nutanix MIB.....	355
Configuring a Banner Page.....	361
Registering a Cluster to vCenter Server using Prism Element.....	362
Unregistering a Cluster from the vCenter Server using Prism Element.....	363
Migrating a Nutanix Cluster between Two vCenter Servers using Prism Element.....	364
Updating the vCenter Service Account Credentials in Prism Element.....	364
In-Place Hypervisor Conversion.....	365
Requirements and Limitations for In-Place Hypervisor Conversion.....	366
In-Place Hypervisor Conversion Process.....	368
Converting Cluster (ESXi to AHV).....	369
Converting Cluster (AHV to ESXi).....	370
Stopping Cluster Conversion.....	371
Internationalization (i18n).....	371
Localization (L10n).....	372
Changing the Language Settings.....	372
Hyper-V Setup.....	373
Adding the Cluster and Hosts to a Domain.....	373
Creating a Failover Cluster for Hyper-V.....	374
Manually Creating a Failover Cluster (SCVMM User Interface).....	375
Enabling Kerberos for Hyper-V.....	376

<b>Security and User Management.....</b>	<b>380</b>
<b>Support Services.....</b>	<b>381</b>
Pulse Health Monitoring.....	381
Pulse Configuration.....	383
Mask Entity Names and IP Addresses.....	384
Pulse Health Monitoring Data Collection.....	384
Remote Support Connections.....	390
Configuring Remote Connection Using CLI.....	390
Controlling Remote Connections.....	390
Configuring HTTP Proxy.....	391
Accessing the Nutanix Support Portal.....	392
Nutanix REST API.....	394
Accessing the REST API Explorer.....	394
Determining Compatibility Between Hardware and Supported Products.....	395
<b>Help Resources.....</b>	<b>396</b>
Accessing Online Help.....	396
Accessing the Nutanix Next Community.....	397
Glossary.....	397
<b>Copyright.....</b>	<b>398</b>

# HELP ORGANIZATION

---

This documentation is organized as follows:

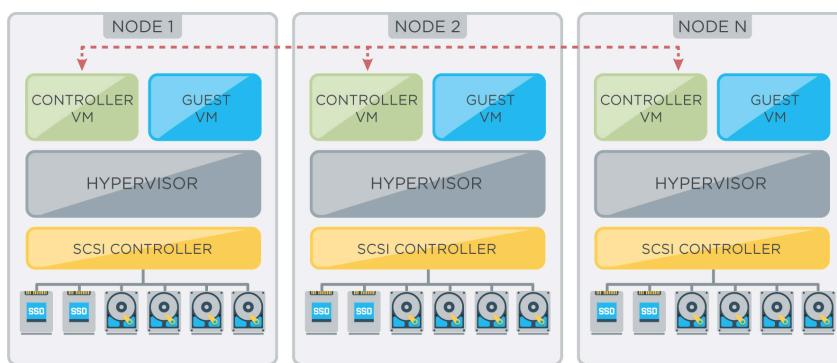
- [Nutanix Platform Overview](#) on page 9 describes the Nutanix architecture.
- [Cluster Management](#) on page 53 describes how to access and use the Prism Element web console, how to apply a Nutanix cluster license, how to upgrade the cluster to a later AOS release, and how to upgrade other software components such as disk firmware.
- [Storage Management](#) on page 102 describes how to monitor storage use in a Nutanix cluster and how to create storage containers.
- [Network Management](#) on page 150 describes how to manage and monitor network settings for the cluster.
- [Hardware Management](#) on page 182 describes how to monitor hardware configurations in a Nutanix cluster and how to expand the cluster.
- [Health Monitoring](#) on page 252 describes how to monitor the health of VMs, hosts, and disks across a Nutanix cluster.
- [Virtual Machine Management](#) on page 260 describes how to monitor status of the VMs across a Nutanix cluster.
- [Performance Monitoring](#) on page 330 describes how to monitor and analyze performance in a Nutanix cluster.
- [System Management](#) on page 348 describes how to configure various system settings such as for SNMP, NTP, and SMTP.
- [Security and User Management](#) on page 380 describes how to configure various security settings including authentication method, SSL certificates, and SSH keys. It also describes how to add, edit, and delete user accounts.
- [Support Services](#) on page 381 describes how to enable (or disable) Nutanix technical support access to your cluster, how to access the Nutanix support portal, and how to access the Nutanix REST API explorer.

# NUTANIX PLATFORM OVERVIEW

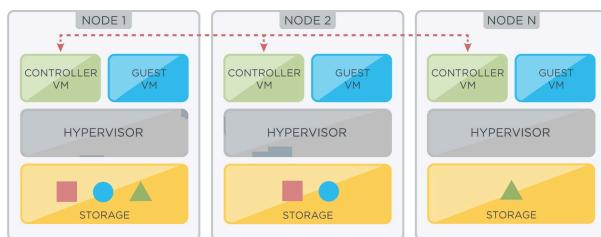
The Nutanix Enterprise Cloud Platform is a converged, scale-out compute and storage system that is purpose-built to host and store virtual machines. All nodes in a Nutanix cluster converge to deliver a unified pool of tiered storage and present resources to VMs for seamless access. A global data system architecture integrates each new node into the cluster, allowing you to scale the solution to meet the needs of your infrastructure.

The foundational unit for the cluster is a Nutanix node. Each node in the cluster runs a standard hypervisor and contains processors, memory, and local storage (SSDs and hard disks).

A Nutanix Controller VM runs on each node, enabling the pooling of local storage from all nodes in the cluster.



## Guest VM Data Management



**Figure 1: Guest VM Data Management**

Hosts read and write data in shared Nutanix datastores as if they were connected to a SAN. From the perspective of a hypervisor host, the only difference is the improved performance that results from data not traveling across a network. VM data is stored locally, and replicated on other nodes for protection against hardware failure.

When a guest VM submits a write request through the hypervisor, that request is sent to the Controller VM on the host. To provide a rapid response to the guest VM, this data is first stored on the metadata drive, within a subset of storage called the oplog. This cache is rapidly distributed across the 10 GbE network to other metadata drives in the cluster. Oplog data is periodically transferred to persistent storage within the cluster. Data is written locally for performance and replicated on multiple nodes for high availability.

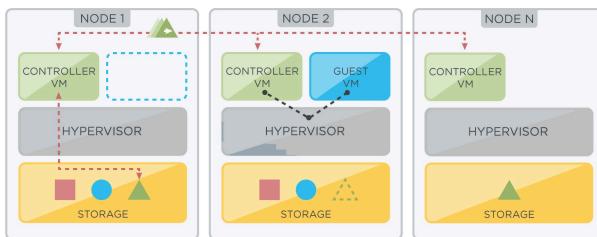
When the guest VM sends a read request through the hypervisor, the Controller VM reads from the local copy first, if present. If the host does not contain a local copy, then the Controller VM reads across the network from a host that does contain a copy. As remote data is accessed, the remote data is migrated to storage devices on the current host, so that future read requests can be local.

## MapReduce Tiering

The Nutanix cluster dynamically manages data based on how frequently it is accessed. When possible, new data is saved on the SSD tier. Frequently-accessed, or *hot* data is kept on this tier, while *cold* data is migrated to the HDD tier. Data that is accessed frequently is again moved back to the SSD tier.

This automated data migration also applies to read requests across the network. If a guest VM repeatedly accesses a block of data on a remote host, the local controller VM migrates that data to the SSD tier of the local host. This migration not only reduces network latency, but also ensures that frequently-accessed data is stored on the fastest storage tier.

## Live Migration

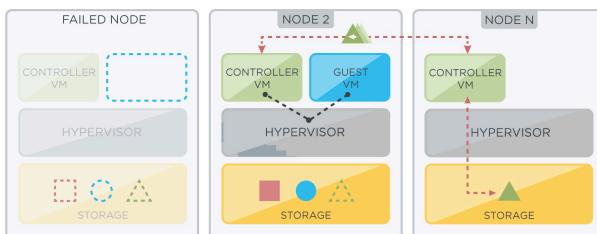


**Figure 2:**

Live migration of VMs, whether it is initiated manually or through an automatic process like vSphere DRS, is fully supported by the Nutanix Enterprise Cloud Computing Platform. All hosts within the cluster have visibility into shared Nutanix datastores through the Controller VMs. Guest VM data is written locally, and is also replicated on other nodes for high availability.

If a VM is migrated to another host, future read requests are sent to a local copy of the data, if it exists. Otherwise, the request is sent across the network to a host that does contain the requested data. As remote data is accessed, the remote data is migrated to storage devices on the current host, so that future read requests can be local.

## High Availability



**Figure 3: High Availability**

The built-in data redundancy in a Nutanix cluster supports high availability provided by the hypervisor. If a node fails, all HA-protected VMs can be automatically restarted on other nodes in the cluster. The hypervisor management system, such as vCenter, selects a new host for the VMs, which may or may not contain a copy of the VM data.

If the data is stored on a node other than the VM's new host, then read requests are sent across the network. As remote data is accessed, the remote data is migrated to storage devices on the current host, so that future read requests can be local. Write requests are sent to the local storage, and also replicated on a different host. During this interaction, the Nutanix software also creates new copies of pre-existing data, to protect against future node or disk failures.

## Virtualization Management VM High Availability

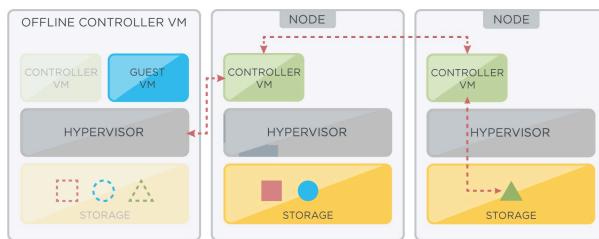
In virtualization management VM high availability, when a node becomes unavailable, VMs that are running on that node are restarted on another node in the same cluster.

Typically, an entity failure is detected by its isolation from the network (the failure to respond to heartbeats).

Virtualization management ensures that at most one instance of the VM is running at any point during a failover. This property prevents concurrent network and storage I/O that could lead to corruption.

Virtualization management VM high availability may implement admission control to ensure that in case of node failure, the rest of the cluster has enough resources to accommodate the VMs.

## Data Path Redundancy



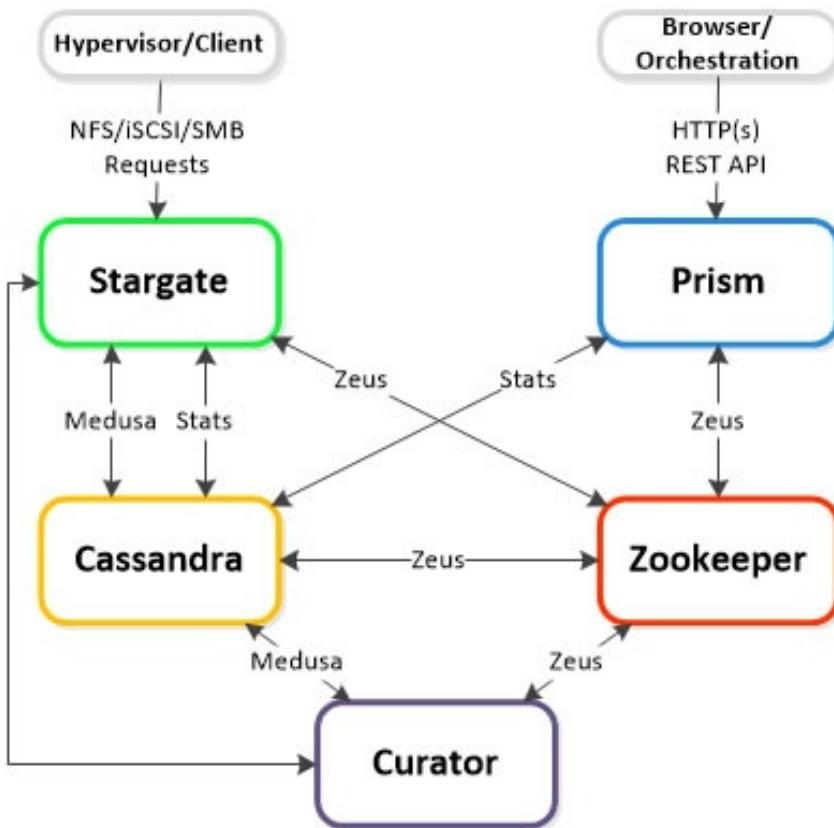
**Figure 4: Data Path Redundancy**

The Nutanix cluster automatically selects the optimal path between a hypervisor host and its guest VM data. The Controller VM has multiple redundant paths available, which makes the cluster more resilient to failures.

When available, the optimal path is through the local Controller VM to local storage devices. In some situations, the data is not available on local storage, such as when a guest VM was recently migrated to another host. In those cases, the Controller VM directs the read request across the network to storage on another host through the Controller VM of that host.

Data Path Redundancy also responds when a local Controller VM is unavailable. To maintain the storage path, the cluster automatically redirects the host to another Controller VM. When the local Controller VM comes back online, the data path is returned to this VM.

## Cluster Components



**Figure 5: Cluster Components**

The Nutanix cluster has a distributed architecture, which means that each node in the cluster shares in the management of cluster resources and responsibilities. Within each node, there are software components that perform specific tasks during cluster operation.

All components run on multiple nodes in the cluster, and depend on connectivity between their peers that also run the component. Most components also depend on other components for information.

### Zeus

A key element of a distributed system is a method for all nodes to store and update the cluster's configuration. This configuration includes details about the physical components in the cluster, such as hosts and disks, and logical components, like storage containers. The state of these components, including their IP addresses, capacities, and data replication rules, are also stored in the cluster configuration.

Zeus is the Nutanix library that all other components use to access the cluster configuration, which is currently implemented using Apache Zookeeper.

### Zookeeper

Zookeeper runs on either three or five nodes, depending on the cluster fault tolerance that is applied to the cluster. Using multiple nodes prevents stale data from being returned to other components, while having an odd number provides a method for breaking ties if two nodes have different information.

Of these three nodes, one Zookeeper node is elected as the leader. The leader receives all requests for information and confers with the two follower nodes. If the leader stops responding, a new leader is elected automatically.

Zookeeper has no dependencies, meaning that it can start without any other cluster components running.

## Medusa

Distributed systems that store data for other systems (for example, a hypervisor that hosts virtual machines) must have a way to keep track of where that data is. In the case of a Nutanix cluster, it is also important to track where the replicas of that data is stored.

Medusa is a Nutanix abstraction layer that sits in front of the database that holds this metadata. The database is distributed across all nodes in the cluster, using a modified form of Apache Cassandra.

## Cassandra

Cassandra is a distributed, high-performance, scalable database that stores all metadata about the guest VM data stored in a Nutanix datastore. In the case of NFS datastores, Cassandra also holds small files saved in the datastore. When a file reaches 512K in size, the cluster creates a vDisk to hold the data.

Cassandra runs on all nodes of the cluster. These nodes communicate with each other once a second using the Gossip protocol, ensuring that the state of the database is current on all nodes.

Cassandra depends on Zeus to gather information about the cluster configuration.

## Stargate

A distributed system that presents storage to other systems (such as a hypervisor) needs a unified component for receiving and processing data that it receives. The Nutanix cluster has a large software component called Stargate that manages this responsibility.

From the perspective of the hypervisor, Stargate is the main point of contact for the Nutanix cluster. All read and write requests are sent across vSwitchNutanix to the Stargate process running on that node.

Stargate depends on Medusa to gather metadata and Zeus to gather cluster configuration data.

**Tip:** If Stargate cannot reach Medusa, the log files include an HTTP timeout. Zeus communication issues can include a Zookeeper timeout.

## Curator

In a distributed system, it is important to have a component that watches over the entire process. Otherwise, metadata that points to unused blocks of data could pile up, or data could become unbalanced, either across nodes, or across disk tiers.

In the Nutanix cluster, each node runs a Curator process that handles these responsibilities. A Curator master node periodically scans the metadata database and identifies cleanup and optimization tasks that Stargate or other components should perform. Analyzing the metadata is shared across other Curator nodes, using a MapReduce algorithm.

Curator depends on Zeus to learn which nodes are available, and Medusa to gather metadata. Based on that analysis, it sends commands to Stargate.

## Prism

A distributed system is worthless if users can't access it. Prism provides a management gateway for administrators to configure and monitor the Nutanix cluster. This includes the nCLI and Prism Element web console.

Prism runs on every node in the cluster, and like some other components, it elects a leader. All requests are forwarded from followers to the leader using Linux iptables. This allows administrators to access Prism using any Controller VM IP address. If the Prism leader fails, a new leader is elected.

Prism communicates with Zeus for cluster configuration data and Cassandra for statistics to present to the user. It also communicates with the ESXi hosts for VM status and related information.

## Single-node Clusters

A traditional Nutanix cluster requires a minimum of three nodes, but Nutanix also offers the option of a single-node cluster for ROBO implementations and other situations that require a lower cost option. Unlike a two-node-node cluster that provides many of the resiliency features of a three-node cluster, a single-node cluster provides lowered resiliency protections.

A single-node cluster is capable of running a limited number of user VMs. These are unlike single-node replication targets which are for replication and backup purposes. A single node cluster can comprise either a Hybrid or All-Flash HCI Node. The minimum recovery point objective (RPO) for a one-node cluster is six hours.

For more information, see [Data Protection and Recovery with Prism Element](#)

### Requirements and Limitations

A single-node cluster is configured like a regular (three-node or more) cluster in many ways, but note the following for a single-node cluster:

- Single-node clusters are supported only on a select set of hardware models. For information about supported models, see [KB 5943](#).
- As a best practice, Nutanix recommends configuring up to five guest VMs. However, you can configure more guest VMs depending on the hardware configuration in the cluster and if snapshots are used in the cluster. Ensure that the cluster platform has the minimal physical resources to cater to the compute and disk requirements. Also, ensure that the CVM resources are optimally consumed.

Nutanix also recommends configuring backup for all the guest VMs running on a single-node cluster to protect the guest VMs in a node failure scenario. Failing to configure backup for guest VMs may result in data loss as data cannot be recovered from a single-node cluster. The data loss can be observed when there is any meta-data inconsistency or file system corruption.

- Nutanix recommends that you schedule an appropriate maintenance window (downtime) for your single node clusters when you plan to perform any network configurations or changes thereto.
- Nutanix recommends an IOPS limit of up to 1000. However, the IOPS limits depend on the change rate in the cluster and if snapshots are used in the cluster.
- Do not create a Prism Central instance (VM) in the cluster. There is no built-in resiliency for Prism Central in a single-node cluster, which means that a problem with the node takes out Prism Central with limited options to recover.
- LCM is supported for software updates, but not for firmware updates.
- Async DR is supported for 6 hour RPO only.
- Use external DNS and NTP servers. Nutanix recommends that you host the DNS and NTP servers on a different cluster.
- Ensure that there is more than 1 SSD available for the system to place meta-data. In case of a Hybrid or All-Flash HCI node with 2 SSDs, if an SSD fails, the cluster goes into a read-only state as there is only one remaining SSD for the meta-data purpose.

In the read-only mode, there are no create, read, update, or delete operations and no cluster changes. For more information about the read-only state, see [Read-Only Mode](#) on page 16. If the cluster experiences an unresponsive disk, data resilience is a risk. The Prism Central console offers an override option that allows users to continue writing to single-node clusters after it has entered read-only mode. For more information, see [Overriding Read-Only Mode](#) on page 16.

**Important:** In case of a Hybrid HCI node or All-Flash HCI node with more than 2 SSDs, if a disk (SSD or HDD) fails, the cluster can fill up and write IO fails if there is insufficient rebuild capacity and the other disks do not have enough available space to bring up the data to disk fault tolerance. For more information, see [Resilient Capacity in Nutanix Bible](#).

- All guest VMs must be shut down before upgrading a single-node cluster. If any guest VMs are still running, a warning message appears.

**Important:** A graceful shutdown of the guest VM may not power-off the VM immediately. Based on the operating system in the guest VM and the workloads running on it, the VM could take sometime to get powered off. Therefore, wait for sometime and check if the VM is in the powered off state.

The following table outlines features and limitations of a single-node cluster.

**Table 1: Single-node Cluster Features**

Requirements and Limitations	Description
Controller VM minimum requirements	6 vCPU and 20 GB memory
Replication factor	Replication factor 2 across drives within the same node. Replication factor 1 containers are optional. For more information about replication factor 1 containers, see <a href="#">Replication Factor 1</a> on page 41.
Hypervisors supported	AHV and ESXi
Network segmentation	You can segment the network on a single-node cluster by using Prism Element.
	Network segmentation for disaster recovery is supported on single-node clusters with AOS version 5.19.2 or later.
	Network segmentation for Backplane, Volumes, RDMA, and iSER is not supported on single-node clusters.
	For more information about network segmentation, see <a href="#">Securing Traffic Through Network Segmentation</a> in the <i>Security Guide</i> .
Unsupported features	<ul style="list-style-type: none"> <li>• Cluster expansion. For more information, see <a href="#">Expanding a Cluster</a> on page 198.</li> <li>• Deduplication. For more information, see <a href="#">Deduplication</a> on page 110.</li> <li>• Erasure coding. For more information, see <a href="#">Erasure Coding</a> on page 112.</li> <li>• Volumes. For more information, see <a href="#">Volumes Guide</a>.</li> <li>• NearSync DR and Metro Availability (asynchronous DR is supported). For more information, see <a href="#">Data Protection with Asynchronous Replication (One-hour or Greater RPO)</a> and <a href="#">Metro Availability (ESXi and Hyper-V 2016)</a> in <i>Data Protection and recovery with Prism Element</i>.</li> <li>• Capacity analysis (in Prism)</li> <li>• Rebuild capacity reservation. For more information, see <a href="#">Rebuild Capacity Reservation</a> on page 107.</li> </ul>

## Read-Only Mode

Single-node clusters enter read-only mode when certain requirements are not met or if a disk fails. A yellow exclamation mark is displayed in the Prism Element web console that indicates the single-node cluster has entered read-only mode. The system also generates an alert, [A1195](#), indicating that the single-node cluster has entered read-only mode. For more information, see [KB 8156](#).

The following table describes the disk failure scenarios in which a cluster enters into read-only mode:

**Table 2: Read-Only Mode - Scenarios**

HCI Node Type in Cluster	Failure Type	Impact on the single node cluster	Nutanix Recommendations
Hybrid with 2 SSDs	1 SSD fails	The cluster becomes read-only as there is only one SSD remaining to store the meta-data.	Ensure that there is more than one SSD available for the system to place meta-data.
All-Flash with 2 SSDs			
All-Flash with more than 2 SSDs	1 SSD fails	The meta-data attempts to pick another SSD in the node and get the node out of read-only state.  <b>Note:</b> A read-only state exists for a brief period until the meta-data is able to pick the new SSD for its usage.	None

## Overriding Read-Only Mode

### About this task

This section describes how to override the read-only mode. The override operation allows the users to continue writing to single-node clusters after it has entered read-only mode. For more information about read-only mode, see [Read-Only Mode](#) on page 16.

### Procedure

To override read-only mode from Prism Element web console, perform the following steps:

1. Click the yellow exclamation mark to re-enable write mode on the cluster.  
The system prompts you to confirm if you want to override read-only mode.
2. Click **Override** to confirm.

**Note:**

- To override read-only mode from nCLI, perform the following steps:
  1. Log into the cluster using your Nutanix credentials.
  2. Run the following command:

```
nutanix@cvm$ ncli cluster set-operation-mode operation-mode=override
```
- An alert *A101057 - Cluster In Override Mode* is generated by the system. For more information, see [KB-8132](#).

## Two-Node Clusters

A traditional Nutanix cluster requires a minimum of three nodes, but Nutanix also offers the option of a two-node cluster for ROBO implementations and other situations that require a lower cost yet high resiliency option. Unlike a one-node cluster, a two-node cluster can still provide many of the resiliency features of a three-node cluster. This is possible by adding an external Witness VM in a separate failure domain to the configuration. For more information, see [Registering a Witness VM](#) and [Configuring a Witness \(Two-node Cluster\)](#) in the *Data Protection and Recovery with Prism Element* guide. Nevertheless, there are some restrictions when employing a two-node cluster. The following table outlines the features and limitations of a two-node cluster.

**Table 3: Two-Node Cluster Features**

Feature	Description
Controller VM minimum requirements	6 vCPU and 20 GB memory
Replication factor	Replication factor 2 spanned over two nodes and Replication factor 4 for metadata on SSDs over two nodes. Replication factor 4 for metadata helps during a node failure scenario to quickly transition the healthy node to run in single-node mode with the metadata remaining disk fault tolerant. (Metadata in a two-node cluster is typically small, so the storage need for four copies is modest.) Replication factor 1 containers are optional. For more information about replication factor 1 containers, see <a href="#">Replication Factor 1</a> on page 41.
Single node failure effects	50% resource loss. Plan for 40% maximum disk and memory usage to avoid read-only state on the remaining node. Data is made replication factor 2 in the background so that data is resilient.
Drive failure effects	One node + one SSD failure (on other node) = read-only mode.
Hypervisors supported	AHV and ESXi
Unsupported features	<ul style="list-style-type: none"><li>• Cluster expansion</li><li>• Deduplication (compression is supported)</li><li>• Erasure coding</li><li>• Nearsync DR and metro availability (asynchronous DR is supported)</li><li>• Network segmentation</li></ul>

### Two-Node Cluster Guidelines

You can configure and upgrade a two-node cluster similarly to a three-node (or larger) cluster in most aspects. However, note the following considerations for a two-node cluster:

- Two-node clusters do not support IPv6 configuration.
- Two-node clusters support only on a select set of hardware models. For information about supported models, see [KB 5943](#).

- Size your implementation for  $N + 1$  so that in the event of a node loss (50% loss of resources) the remaining node will have sufficient resources to allow the cluster to continue functioning.
- As a best practice, Nutanix recommends configuring up to 15 guest VMs. However, you can configure more guest VMs depending on the hardware configuration in the cluster and if snapshots are used in the cluster. Ensure that the cluster platform has the minimal physical resources to cater to the compute and disk requirements. Also, ensure that the CVM resources are optimally consumed.
- Nutanix recommends an IOPS limit of up to 1000. However, the IOPS limits depend on the change rate in the cluster and if snapshots are used in the cluster.
- There is a heartbeat check (ping) between the nodes every two seconds. If a successful ping does not occur within 10 seconds (5 consecutive failed tries), a failover is initiated. For more information, see [Failure and Recovery Scenarios](#) on page 19. When the cluster recovers, it must remain in healthy status for at least 15 minutes before it will failback.
- The upgrade process in a two-node cluster may take longer than the usual process because of the additional step of syncing data while transitioning between single and two node state. Nevertheless, the cluster remains operational during upgrade.
- Use external DNS and NTP servers. Nutanix recommends that you host the DNS and NTP servers on a different cluster.
- Node or disk failures are handled as follows:
  - Node failure: When a two-node cluster is operating normally, data is replicated across the nodes. If a node fails, data is replicated across disks on the healthy node to maintain resiliency.
  - HDD failure: An HDD failure is handled in the same way as in a three-node cluster, that is, the data is rebuilt in the background. If there is insufficient rebuild capacity when an HDD fails, the cluster can fill up and I/O can fail.
  - SSD failure: If a node loses an SSD, the remedial action is the same as for an HDD failure, that is the cluster remains normal and the data is rebuilt in the background for the disk. Occasionally, an SSD failure on one node can result in the other node in the cluster transitioning to a standalone state because the SSD failure caused a critical storage service to restart, which caused user I/O to stall. If the nodes have only a single SSD left and if either node fails, the healthy node goes into read-only state.
- Direct-connect networking between nodes is not supported.

### **Witness for Two-node Clusters**

A two-node cluster requires a Witness VM that is located in a separate failure domain either off premise or in a different physical platform on premise. For information about how to configure a witness for a two-node cluster, see [Witness Option](#) in the *Data Protection and Recovery with Prism Element* guide.

The Witness option provides a dashboard of status information about all the registered two-node clusters. For information about the Witness dashboard for a two-node cluster, see [Witness VM Dashboard \(Two-node Cluster\)](#) in the *Data Protection and Recovery with Prism Element* guide.

- Witness VM considerations:
  - A Witness VM for two-node clusters requires a minimum of 2 vCPUs, 6 GBs of memory, and 25 GBs of storage.
  - The same Witness VM can be used for both Metro Availability and two-node clusters, and a single Witness VM can support up to 50 instances (any combination of two-node clusters and Metro Availability protection domains).
  - You can bring up a two-node cluster without a Witness VM being present initially, but it is recommended that the Witness VM be alive and running before starting the cluster.
  - The Witness VM might reside on any supported hypervisor, and it can run on either Nutanix or non-Nutanix hardware.

**Note:** Nutanix does not support the deployment of a Witness VM on the AWS and Azure cloud platforms.

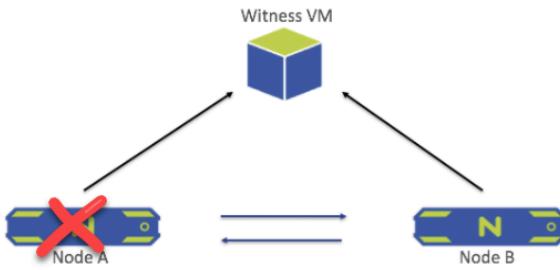
- The Witness VM must reside in a separate failure domain, which means it must have independent power and network connections from any cluster it is managing. This separate platform can be deployed either on-premise (including as an option the Nutanix one-node replication target NX-1155 as an option) or off-premise (centrally, typically where Prism Central is hosted).
- During a node failure, the transition of a healthy node to a single-node mode can take 30-60 seconds. During this period the guest VMs might experience I/O timeouts. Therefore, Nutanix recommends that the SCSI timeout of the guest VM disks should be at least 60 seconds.
- The minimum recovery point objective (RPO) for a two-node cluster is six hours.
- Network latency between a two-node cluster and the Witness VM must not exceed 500 ms. (RPC timeouts are triggered if the network latency is higher.) During a failure scenario, nodes keep trying to ping the Witness VM until successful. Nodes ping the Witness VM every 60 seconds, and each request has a two-second timeout, so it can tolerate up to one second of link latency.
- A Witness VM for two-node clusters supports node replacement (where the node remains part of the cluster) but does not support node removal. When replacing a node, the cluster remains active but briefly transitions to standalone mode.
- All node maintenance work flows (software upgrades, life cycle manager procedures, node and disk break-fix procedures, boot drive break-fix procedure) require that the cluster be registered with a Witness VM.

## Failure and Recovery Scenarios

There are several potential failure scenarios between the nodes and the Witness. The steps for recovering from a failure depend on the nature of the failure. This section describes the steps needed (or not needed) when a failure occurs. Each failure scenario generates one or more alerts that you can review. For information about viewing alert messages, see [Alerts Dashboard](#) in *Prism Element Alerts Reference Guide*.

### Node Failure

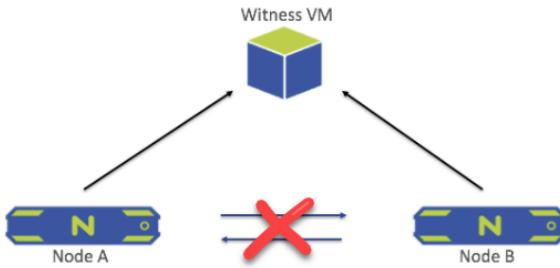
When a node goes down, the live node sends a leadership request to the Witness and goes into single-node mode. In this mode the cluster retains replication factor 2 at the disk level, meaning data is copied to two disks. (Normally, the cluster maintains replication factor 2 at the node level meaning data is copied to each node.) If one of the two metadata SSDs fails while in single-node mode, the cluster (node) goes into read-only mode until a new SSD is picked for metadata service. When the node that was down is back up and stable again, the system automatically returns to the previous state (replication factor 2 at the node level). No user intervention is necessary during this transition.



**Figure 6: Failure Diagram: Node Down**

### Network Failure Between The Nodes

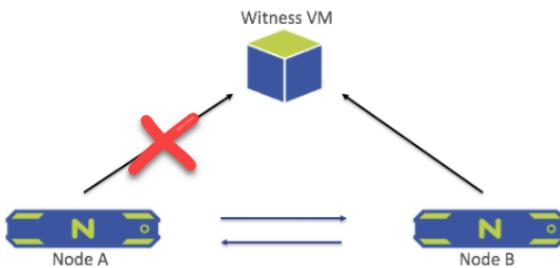
When the network connection between the nodes fails, both nodes send a leadership request to the Witness. The node receives the leadership lock stays active and goes into single-node mode. All operations and services on the other node are shut down, and the node goes into a waiting state. When the connection is re-established, the same recovery process as mentioned in the Node Failure scenario begins.



**Figure 7: Failure Diagram: Node-to-Node Communication Down**

### Network Failure Between Node and Witness

When the network connection between a single node (Node A in this example) and the Witness fails, an alert is generated that Node A is not able to reach the Witness. The cluster is otherwise unaffected, and no administrator intervention is required.

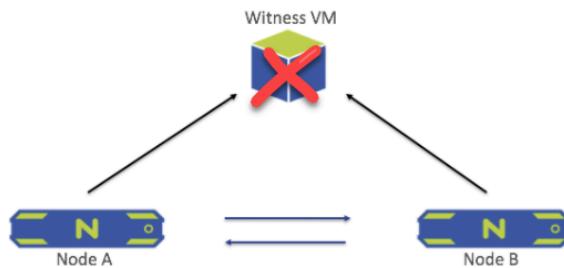


**Figure 8: Failure Diagram: Node-to-Witness Communication Down**

## **Witness VM Failure**

When the Witness goes down (or the network connections to both nodes and Witness fail), an alert is generated but the cluster is otherwise unaffected. When connection to Witness is re-established, Witness process resumes automatically. No administrator intervention is required.

If the Witness VM goes down permanently (unrecoverable), follow the steps for configuring a new Witness through the **Configure Witness** option of the Prism Element web console. For more information, see [Configuring a Witness \(Two-node Cluster\)](#) in the *Data Protection and Recovery with Prism Element* guide.



**Figure 9: Failure Diagram: Witness Down**

## **Cluster Resiliency**

Nutanix AOS provides cluster resilience capability to protect your clusters from failures.

To ensure that a cluster can remain resilient during a failure, ensure that the cluster has enough free memory and vCPU capacity available for critical workloads to fail over to another node.

## **Failure Handling in a Nutanix Cluster**

Hardware failures are a part of any datacenter lifecycle. The Nutanix architecture was designed with this inevitability in mind.

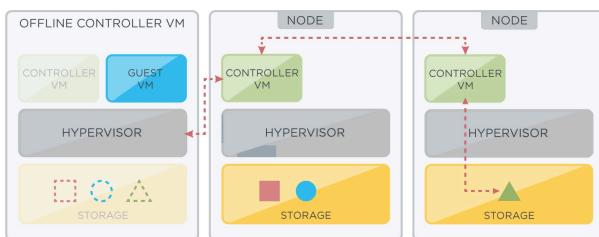
Depending on the fault tolerance of the cluster and the replication factor of the containers in the cluster, a cluster can tolerate one or two failures of a variety of hardware components while still running guest VMs and responding to commands through the management console. Many of these failures also trigger an alert through that same management console to give the administrator a chance to respond to the situation.

Nutanix provides the ability to tolerate rack failures for extended data availability, in addition to drive, node, block, and network link failure.

### **Node Failure**

A Nutanix node is comprised of a physical host and a Controller VM. Either component can fail without impacting the rest of the cluster.

## Controller VM Failure



**Figure 10: Controller VM Failure**

The Nutanix cluster monitors the status of Controller VMs in the cluster. If any Stargate process fails to respond two or more times in a 30-second period, another Controller VM (CVM) redirects the storage path on the related host to another Stargate. Reads and writes occur over the 10 GbE network until the missing Stargate comes back online.

To prevent constant switching between Stargates, the data path is not restored until the original Stargate has been stable for 30 seconds.

A CVM failure may include a user powering down the CVM, a CVM rolling upgrade, or any event, which might bring down the CVM. In any of these cases the storage traffic is served by another CVM in the cluster. The hypervisor and CVM communicate using a private network on a dedicated virtual switch. This means that the entire storage traffic is routed through an internal IP address on the CVM. The external IP address of the CVM is used for remote replication and for CVM to CVM communication.

In the event of a local CVM failure, the local addresses previously used by the local CVM become unavailable. In this case, the Nutanix Distributed File System (NDFS) automatically detects the outage and redirects the storage traffic to another CVM in the cluster over the network. The re-routing is done transparently to the hypervisor and to the VMs running on the host. This indicates that even if a CVM is powered-off, the VMs continue to perform the I/O operations. The NDFS is also self-healing, which means that NDFS detects when a CVM is powered-off and it automatically reboots the local CVM. Once the local CVM is available, the traffic is seamlessly transferred back to be served by the local CVM.

The NDFS uses replication factor and checksum to ensure data redundancy and availability in the case of a node or disk failure or corruption. In the case of a node or disk failure the data is then re-replicated among all nodes in the cluster to maintain the replication factor, which is called re-protection. Re-protection might be triggered when a CVM goes down.

### What Will Users Notice?

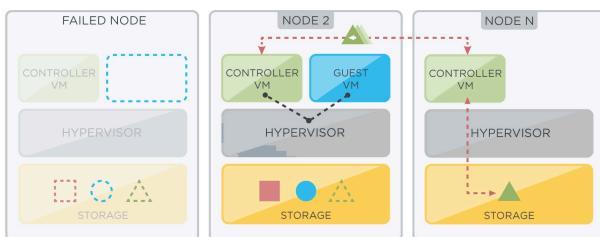
During the switching process, the host with a failed Controller VM may report that the shared storage is unavailable. Guest VMs on this host appear to *hang* until the storage path is restored. Although the primary copy of the guest VM data is unavailable because it is stored on disks mapped to the failed Controller VM, the replicas of that data are still accessible.

As soon as the redirection takes place, VMs can resume reads and writes. Performance may decrease slightly, because the IO is traveling across the network, rather than across the internal network. Because all traffic goes across the 10 GbE network, most workloads do not diminish in a way that is perceivable to users.

### What Happens If Another One Fails?

A second Controller VM failure has the same impact on the VMs on the other host, which means there will be two hosts sending IO requests across the network. More importantly, however, is the additional risk to guest VM data. With two Controller VMs unavailable, there are now two sets of physical disks that are inaccessible. In a cluster with a replication factor 2, there is now a chance that some VM data extents are missing completely, at least until one of the Controller VMs resumes operation.

## Host Failure



**Figure 11: Host Failure**

The built-in data redundancy in a Nutanix cluster supports high availability (HA) provided by the hypervisor. If a node fails, all HA-protected VMs can be automatically restarted on other nodes in the cluster.

Curator and Stargate responds to two issues that arise from the host failure. First, when the guest VM begins reading across the network, Stargate begins migrating those extents to the new host. This improves performance for the guest VM. Second, Curator notices that there is a missing replica of those extents, and instruct Stargate to begin creating a second replica.

### What Will Users Notice?

Users who are accessing HA-protected VMs might notice that their VM is unavailable until it restarts on the new host. Without HA, the VM requires a manual restart.

### What Happens If Another One Fails?

Depending on how fully loaded the cluster is, a second host failure could leave the remaining hosts with insufficient processing power to restart the VMs from the second host. However, even in a lightly-loaded cluster, the bigger concern is additional risk to guest VM data. With two sets of physical disks that are inaccessible, there would be a chance that some VM data extents are missing completely and the IO requests are not served.

## Drive Failures

Drives in a Nutanix node store four primary types of data: persistent data (hot-tier and cold-tier), storage metadata, oplog, and Controller VM boot files. Cold-tier persistent data is stored in the hard-disk drives of the node. Storage metadata, oplog, hot-tier persistent data, and Controller VM boot files are kept in the SATA-SSD in drive bay one. SSDs in a dual SSD system are used for storage metadata, oplog, hot-tier persistent data according to the replication factor of system and in a RAID-1 configuration for CVM files. In all-flash nodes, data of all types is stored in the SATA-SSDs.

**Note:** On hardware platforms that contain PCIe-SSD drives, the SATA-SSD holds only the Controller VM boot files. Storage metadata, oplog, and hot-tier persistent data reside on the PCIe-SSD.

## Boot Drive Failure

Each Controller VM boots from a SATA-SSD. During cluster operation, this drive also holds component logs and related files.

A boot drive failure eventually causes the Controller VM to fail. The host does not access the boot drive directly, so other guest VMs can continue to run. Data Path Redundancy redirects the storage path to another Controller VM. For more information, see [Controller VM Failure](#) on page 22.

**Note:** The Controller VM might restart under certain rare conditions on dual SSD nodes if a boot drive fails, or if you unmount a boot drive without marking the drive for removal and the data has not successfully migrated.

## Metadata Drive Failure

The metadata *drive* (metadata spans multiple drives) serves many purposes. It holds the oplog for each host, which provides a fast response to VMs that send write requests. It is used as a persistent data tier. It is also used by the Cassandra database to provide fast read and write responses for cluster metadata. To protect against potential failure, the metadata is replicated to metadata drives in other hosts in the cluster.

Metadata is shared, and Cassandra uses up to four SSDs to store metadata. If any metadata drive fails on a host, the Controller VM restarts. Once the Cassandra process restarts, the missing metadata is retrieved from the other Controller VMs and shared across the remaining metadata drives. When the faulty drive recovers or is replaced, metadata is stored on that drive again.

If the Cassandra process is down on a node for more than 30 minutes, the surviving Cassandra nodes detach the node from the Cassandra database so that the unavailable metadata can be replicated on other nodes. The process of healing the database takes about 30-40 minutes. If the Cassandra process restarts and remains up for 30 minutes while the healing procedure is still running, the node detachment process is canceled if the healing procedure is still running. If the process resumes and is stable after the healing procedure is complete, the node can be manually added to the database using the nCLI command:

```
ncli> host enable-metadata-store id=host_id
```

### What Will Users Notice?

Performance might decrease slightly for user VMs on the host due to the reboot and the fact that some I/O is traveling across the network. However, most workloads should not diminish in a way that is perceivable to users (other than during the reboot).

### What Happens If Another One Fails?

Multiple drive failures in a single selected domain (node, block, or rack) is tolerated.

## Data Drive Failure

Each node contributes data drives to the cluster storage pool. Cold-tier data is stored in HDDs, while hot-tier data is stored in SSDs for faster performance. Because the HDDs have moving parts, and outnumber any other hardware component, this is the most likely component to experience a failure. Data is replicated across the cluster, so a single hard-disk drive failure does not result in data loss. In all-flash nodes, data of all types is stored in SSDs.

In case of a data drive failure, the cluster software receives a hardware alert from the host that a data drive (HDD or SSD) has failed, and immediately begins working to reduce the impact of a second failure. Curator instructs Stargate to create a second replica of any guest VM data that was stored on the drive.

**Note:** The Controller VM restarts if a data drive fails, or if you remove a data drive without marking the drive for removal and the data has not successfully migrated.

### What Will Users Notice?

For a brief period of time, guest VMs with files on the failed data drive reads across the network. Curator will eventually instruct Stargate to migrate the relevant data to another drive on the current host.

### What Happens If Another One Fails?

In a cluster with a replication factor of 2, losing two drives on different domains (node, block, or rack) means that some VM data extents could lose both replicas. Although a single drive failure does not have the same impact as a host failure, it is important to replace the failed drive as soon as possible.

## Network Link Failure

The physical network adapters on each host are grouped together on the external network. This grouping of network adapters enables load balancing and failover capabilities, thus improving the performance and redundancy of the system.

In case of a network link failure, the network traffic fails over to the secondary link. This failover behavior is different for AHV and ESXi hypervisors, based on their NIC teaming and failover configuration.

For more information about hypervisor specific network link failure, see:

- [Networking recommendations for ESXi](#)
- [Networking recommendations for AHV](#)

## Cluster Fault Tolerance

Cluster fault tolerance is the number of simultaneous disk or node failures a cluster can withstand within the configured fault domain while maintaining operational resilience.

Following are the types of cluster fault tolerance supported in a Nutanix cluster:

- [One Node or One Disk \(1N/1D\)](#)
- [One Node and One Disk \(1N&1D\)](#)
- [Two Nodes or Two Disks \(2N/2D\)](#)

### Minimum Requirements

The following table lists the minimum number of nodes and replication factor required to configure the respective cluster fault tolerance.

Cluster Fault Tolerance	Replication Factor	Minimum Number of Nodes
1N/1D	2	3
1N&1D	3	You can configure 1N&1D fault tolerance on a cluster with only three nodes. You cannot configure 1N&1D fault tolerance on a cluster if the number of nodes in the cluster is less than or more than three.
2N/2D	3	5

### One Node or One Disk Cluster Fault Tolerance

A cluster with one node or one disk (1N/1D) cluster fault tolerance can withstand the failure of either one node or one disk within the fault domain of a node, and remain resilient.

To configure 1N/1D fault tolerance, a cluster must have a minimum of three nodes to store the minimum required metadata copies to maintain resiliency and data integrity.

By default, the storage containers in a cluster with 1N/1D fault tolerance are configured with a replication factor of 2, distributing two data copies across two distinct nodes. This ensures that, in the event of a node or disk failure, at least two metadata copies remain accessible to sustain cluster operations, while at least one copy of the container data is preserved.

When you enable rack or block awareness in the cluster, the system aims to distribute three copies of metadata and two copies of container data across nodes within the configured fault domains of rack or block. This ensures that,

in the event of a rack or block failure, the system retains the minimum required number of metadata and data copies across the fault domains to maintain operations.

**Note:** If the system cannot distribute metadata and data copies across the rack or block due to node unavailability, it places the data copies on different nodes within the same fault domain.

In the event of a node or disk failure, the system automatically rebuilds the lost data on a healthy node or disk, restoring resiliency and self-healing the cluster. Therefore, when sizing the system, Nutanix recommends that you consider the spare capacity required for rebuilding operations. The spare capacity required for a cluster with 1N/1D fault tolerance is equal to the capacity of the largest node in the cluster. For more information on usable capacity, see [Storage Overheads and Usable Capacity](#) on page 28.

For information on how to configure cluster fault tolerance, see [Cluster Fault Tolerance Configuration](#) on page 75.

For information on how to increase the existing 1N/1D cluster fault tolerance of a cluster, see [Increasing the Cluster Fault Tolerance Level](#) on page 75.

### One Node and One Disk Cluster Fault Tolerance

A cluster configured with one node and one disk (1N&1D) cluster fault tolerance can withstand the simultaneous failure of one node and one disk in another node, or the failure of two disks across different fault domains, and remain resilient.

To configure 1N&1D fault tolerance, a cluster must have a minimum of three nodes. A cluster with 1N&1D fault tolerance maintains three copies of metadata, locally mirrored across three different nodes, ensuring data integrity. This configuration guarantees that, in the event of a node or disk failure, enough metadata copies remain available to sustain cluster operations.

By default, storage containers in a cluster with 1N&1D fault tolerance are configured with a replication factor of 3, with three copies of data distributed across three different nodes. A Write operation is considered complete only after at least three copies of the data are successfully written. This ensures that in case of failure of a node and disk at least one copy of data remains accessible.

**Note:** You can modify the replication factor of the storage containers to 2. However, with replication factor 2, these containers can only tolerate the failure of a single node or disk within the fault domains. Therefore, Nutanix recommends that you configure replication factor 3 for the storage containers to attain optimal cluster resiliency.

When you enable rack or block awareness, the system attempts to distribute metadata and container data across unique nodes within the configured fault domains. This ensures that, in the event of a rack or block failure, the system retains the minimum required copies of metadata and data across the fault domains to maintain operations.

**Note:** If the system is unable to place metadata and data copies on nodes within the same rack or block due to unavailability, it places the copies on other nodes within the same configured fault domain.

### Adaptive Replication Factor 3

Clusters configured with 1N&1D fault tolerance utilize an adaptive mechanism to maintain operations during node downtime, whether caused by a node failure or node maintenance. During such events, the system temporarily reduces the replication factor of the containers to 2, storing only two copies of the data and marking the Write operation as complete. This ensures that the cluster can continue functioning with two active nodes. When the node is restored, the system automatically upgrades the containers to a replication factor of 3. The system also regenerates the third copy of any data written with only two copies during the downtime, fully restoring fault tolerance and data redundancy.

The cluster maintains sufficient copies of data to ensure continuous operation and service I/O even in the event of multiple failures, balancing resiliency with the overhead required for self-healing. In a steady state, the cluster maintains enough copies of data and metadata to withstand the simultaneous failure of one node and one disk. In a degraded state, when a failure has already occurred, the cluster prioritizes application availability over restoring full data resiliency.

In the event of a node failure, the system does not immediately initiate a rebuild of the data on the failed node. This ensures that the system can continue to operate, even if there is no spare capacity available for rebuilding the node, and sustain operations during the failure. In the event of a disk failure, the system rebuilds the data from the failed disk to restore resiliency and facilitate self-healing. This ensures that the system can maintain the ability to recover from disk failures, which are more likely to occur. Therefore, when sizing the system, Nutanix recommends that you consider spare capacity for rebuilding operations to account for a disk failure on a node. The spare capacity required for a cluster with 1N/1D fault tolerance is equal to the total capacity of the largest disk on every node. For more information on usable capacity, see [Storage Overheads and Usable Capacity](#) on page 28.

For information on how to configure 1N&1D cluster fault tolerance, see [Cluster Fault Tolerance Configuration](#) on page 75.

## Limitations

The following limitations apply when you configure 1N&1D fault tolerance in your cluster:

- You cannot configure 1N&1D fault tolerance on a cluster if the number of nodes in the cluster is less than or more than three.
- You cannot configure 1N&1D cluster fault tolerance on clusters running Hyper-V.
- You cannot increase the fault tolerance of a cluster from 1N/1D to 1N&1D; 1N&1D cluster fault tolerance must be configured when you create the cluster.
- You cannot configure 1N&1D cluster fault tolerance on clusters deployed in Nutanix Cloud Clusters (NC2) environments.
- You cannot enable erasure coding or deduplication on clusters with 1N&1D cluster fault tolerance.
- You cannot deploy compute-only or storage-only nodes on clusters with 1N&1D cluster fault tolerance.
- Nutanix recommends not configuring storage policies on clusters with 1N&1D cluster fault tolerance. Clusters with 1N&1D fault tolerance and storage policies take significantly longer to transition the replication factor 2 to replication factor 3 data after recovery from a node failure or planned maintenance, compared to clusters without storage policies.

## Two Nodes or Two Disks Cluster Fault Tolerance

A cluster configured with two nodes or two disks (2N/2D) cluster fault tolerance can withstand the simultaneous failure of either two nodes or two disks within a fault domain of a node, and remain resilient.

To configure 2N/2D fault tolerance, a cluster must have a minimum of five nodes to store the minimum required metadata copies to maintain resiliency and data integrity. By default, storage containers in a cluster with 2N/2D fault tolerance are configured with a replication factor of 3, with three copies of data distributed across three different nodes.

**Note:** You can modify the replication factor of the storage containers to 2. However, with a replication factor of 2, these containers can only tolerate the failure of a single node or disk within the fault domains. Therefore, Nutanix recommends that you configure replication factor 3 for the storage containers to attain optimal cluster resiliency.

When you enable rack or block awareness in the cluster, the system aims to distribute five copies of metadata and three copies of container data across nodes within the configured fault domains. This ensures that, in the event of a rack or block failure, the system retains the minimum required number of metadata and data copies across the fault domains to maintain operations.

**Note:** If the system cannot distribute metadata and data copies across the rack or block due to node unavailability, it places the data copies on different nodes within the same fault domain.

In the event of a failure, the system automatically rebuilds the lost data on a healthy node or disk, restoring resiliency and self-healing the cluster. Therefore, when sizing the system, Nutanix recommends that you consider spare capacity for rebuilding operations. The spare capacity for a cluster with 2N/2D fault tolerance is equal to the capacity of the

two largest nodes in the cluster. For more information on usable capacity, see [Storage Overheads and Usable Capacity](#) on page 28.

For information on how to configure cluster fault tolerance, see [Cluster Fault Tolerance Configuration](#) on page 75.

### Storage Overheads and Usable Capacity

The usable storage container capacity is the actual amount of storage space available for use within a storage container after accounting for overheads like system metadata, resiliency overheads (additional copies of data written for redundancy), and spare capacity for rebuilding the data during failures and planned maintenance. It is the effective capacity that users can access and use to store their data.

The following table shows the overheads associated with the different types of cluster fault tolerance.

**Table 4: Cluster Fault Tolerance and Overheads**

Cluster Fault Tolerance	Resiliency Overhead	Spare Capacity Overhead	Other System Overheads
1N/1D	1x	The capacity of the largest node in the cluster.	All flash: ~10% of raw capacity
1N&1D	2x	Total capacity of the largest disk on every node.	Hybrid: ~15% of raw capacity
2N/2D	2x	Total capacity of the two largest nodes in the cluster.	

x = Total size of application data written in the system.

The following table shows the total overheads (including resiliency overhead, spare capacity overhead, and other system overheads) based on the different types of cluster fault tolerance and the number of nodes.

**Note:** The total overhead shown in the table is calculated assuming that the cluster is an all-flash configuration with uniform nodes, each containing 12 disks.

**Table 5: Total Overhead Comparison Based On Cluster Fault Tolerance**

Number of Nodes	Total Overhead (includes resiliency overhead, spare capacity overhead, and other system overheads)		
	1N/1D	1N&1D	2N/2D
3	3x	3.09x	NA
4	2.67x	NA	NA
5	2.50x	NA	5x
6	2.40x	NA	4.5x
7	2.33x	NA	4.2x
8	2.29x	NA	4x
9	2.25x	NA	3.86x

Number of Nodes	Total Overhead (includes resiliency overhead, spare capacity overhead, and other system overheads)		
	1N/1D	1N&1D	2N/2D
10	2.22x	NA	3.75x

x = Total size of application data written in the system.

The following table displays the approximate usable storage container capacity available based on the different types of cluster fault tolerance and the number of nodes.

**Note:** The usable capacity shown in the table is calculated assuming that the cluster is an all-flash configuration with uniform nodes, each containing 12 disks.

**Table 6: Usable Capacity Comparison Based On Cluster Fault Tolerance and Replication Factor**

Number of Nodes	Usable Capacity		
	1N/1D	1N&1D	2N/2D
3	30%	29%	NA
4	34%	NA	NA
5	36%	NA	18%
6	38%	NA	20%
7	39%	NA	21%
8	39%	NA	23%
9	40%	NA	23%
10	41%	NA	24%

## Fault Domains in a Nutanix Cluster

Fault domains, also known as the fault tolerance level, are entities in a cluster (like a node, block, or rack) that can fail without impacting cluster operations. You can configure a node in the cluster, a block, or a rack as a failure domain.

- [Configuring Node Fault Tolerance](#) on page 29
- [Block Fault Tolerance](#) on page 30
- [Rack Fault Tolerance](#) on page 35

### Configuring Node Fault Tolerance

#### About this task

To configure node fault tolerance, do the following.

#### Procedure

1. Log in to the Prism Element web console.
2. Go to **Settings > Setup > Rack Configuration..**

3. Select **Node** as the fault tolerance domain, and click **Next**.
4. (Optional) To specify rack and block mapping, click **Add New Rack** and follow the steps 4 through 6 in Configuring Rack Fault Tolerance.

**Note:** Nutanix recommends configuring rack and block mapping if you want to enable rack awareness at a later stage.

### Block Fault Tolerance

*Block fault tolerance* allows a Nutanix cluster to make redundant copies of data and metadata and place them on nodes in different blocks.

A *block* is a rack-mountable enclosure that contains one to four Nutanix nodes. All nodes in a block share power supplies, front control panels (ears), backplane, and fans.

Nutanix offers block fault tolerance as an opt-in procedure or a best-effort procedure. The opt-in block fault tolerance feature offers guaranteed data resiliency when required conditions are met. For more information, see [Configuring Block Fault Tolerance](#) on page 30. For best-effort fault tolerance mode, data copies remain on the same block when there is insufficient space across all blocks. For more information, see [Block Fault Tolerance in Best Effort mode](#) on page 30.

With block fault tolerance enabled, guest VMs can continue to run after a block failure because redundant copies of guest VM data and metadata exist on other blocks.

### Configuring Block Fault Tolerance

#### About this task

To configure block fault tolerance, do the following.

#### Procedure

1. Log in to the Prism Element web console.
2. Go to **Settings > Setup > Rack Configuration..**
3. Select **Block** as the fault tolerance domain, and click **Next**.
4. (Optional) To specify rack and block mapping, click **Add New Rack** and follow the steps 4 through 6 in Configuring Rack Fault Tolerance.

**Note:** Nutanix recommends configuring rack and block mapping to enable rack awareness at a later stage.

### Block Fault Tolerance in Best Effort mode

When certain conditions are met, Nutanix clusters become block fault tolerant. Block fault tolerance is applied automatically when:

- Every storage tier in the cluster contains at least one drive on each block.
- Every storage container in the cluster has replication factor of at least two.
- For replication factor 2, there are a minimum of three blocks in the cluster.
- The required number of blocks have sufficient free space in all tiers. The required number of blocks depends on the replication factor of the cluster. For example, if the replication factor of the cluster is two, then at least two blocks require sufficient free space in all tiers.

- A minimum of four blocks for replication factor 2 or six blocks for replication factor 3 is required to maintain block awareness if erasure coding is enabled on any storage container. (If the cluster has fewer blocks, block awareness is lost when erasure coding is enabled.)

**Note:** These conditions are not applicable for single-node replication target clusters. For more information about how single-node replication target clusters handle failures, see [Single-Node Replication Target Clusters](#) in the *Data Protection and Recovery with Prism Element* guide.

If the block fault tolerance conditions are met, the cluster can tolerate a specific number of block failures:

- A cluster with replication factor 2 or replication factor 3 with three or more blocks can tolerate a maximum failure of one block.
- A cluster with replication factor 3 and five or more blocks can tolerate a maximum failure of two blocks.

Block fault tolerance is one part of a resiliency strategy. It does not remove other constraints such as the availability of disk space and CPU or memory resources in situations where a significant proportion of the infrastructure is unavailable.

### Metadata Block Awareness Requirements for Block Fault Tolerance

Metadata block awareness is required for block fault tolerance. Metadata block awareness can be enabled for clusters with replication factor 2 and replication factor 3. To enable metadata block fault tolerance, your metadata must meet the following requirements.

**Table 7: Minimum Cluster Requirements**

Replication Factor	Minimum Number of Blocks and Nodes Per Block Required
Replication factor 2	<ul style="list-style-type: none"> <li>• 3 blocks</li> <li>• 1 node per block</li> </ul>
Replication factor 3	<ul style="list-style-type: none"> <li>• 5 blocks</li> <li>• 1 node per block</li> </ul>

**Table 8: Additional Requirements when Adding Nodes to an Existing Block Aware Cluster**

Replication Factor	Requirement	Example
<p><b>Note:</b> Be sure your cluster has met the previous minimum cluster requirements mentioned in <i>Minimum Cluster Requirements</i> table.</p>		

Replication Factor	Requirement	Example
Replication factor 2	There must be at least 3 blocks populated with a specific number of nodes to maintain block fault tolerance. To calculate the number of nodes required to maintain block fault tolerance when the cluster replication factor is 2, you need twice the number of nodes in the remaining blocks as there are in the block with the most or maximum number of nodes.	If $X = \text{number of nodes in the block with the most nodes}$ , and if there are 4 nodes in a block, you need $2X = 8$ nodes distributed across the remaining (non-failing) blocks to maintain block fault tolerance for that cluster.
Replication factor 3	There must be at least 5 blocks populated with a specific number of nodes to maintain block fault tolerance. To calculate the number of nodes required to maintain block fault tolerance when the cluster replication factor is 3 you need four times the number of nodes in the remaining blocks as there are in the block with the most or maximum number of nodes.	If $X = \text{number of nodes in the block with the most nodes}$ , and if there are 4 nodes in a block, you need $4X = 16$ nodes distributed across the remaining (non-failing) blocks to maintain block fault tolerance for that cluster.

## Mixing All-Flash and Hybrid Nodes

When you deploy a cluster that includes both All-Flash and Hybrid nodes, it is recommended to follow specific guidelines to prevent disproportionate allocation of data and ensure optimal disk usage. For more details on mixing All-Flash and Hybrid nodes, see [KB 17466](#).

## Block Fault Tolerant Data Placement

Stargate is responsible for placing data across blocks, and Curator makes data placement requests to Stargate to maintain block fault tolerance.

New and existing clusters can reach a block fault tolerant state. New clusters can be block fault tolerant immediately after being created if the configuration supports it. Existing clusters that were not previously block fault tolerant can be made tolerant by reconfiguring the cluster in a manner that supports block fault tolerance.

New data in a block fault tolerant cluster is placed to maintain block fault tolerance. Existing data that was not in a block fault tolerant state is moved and scanned by Curator to a block fault tolerant state.

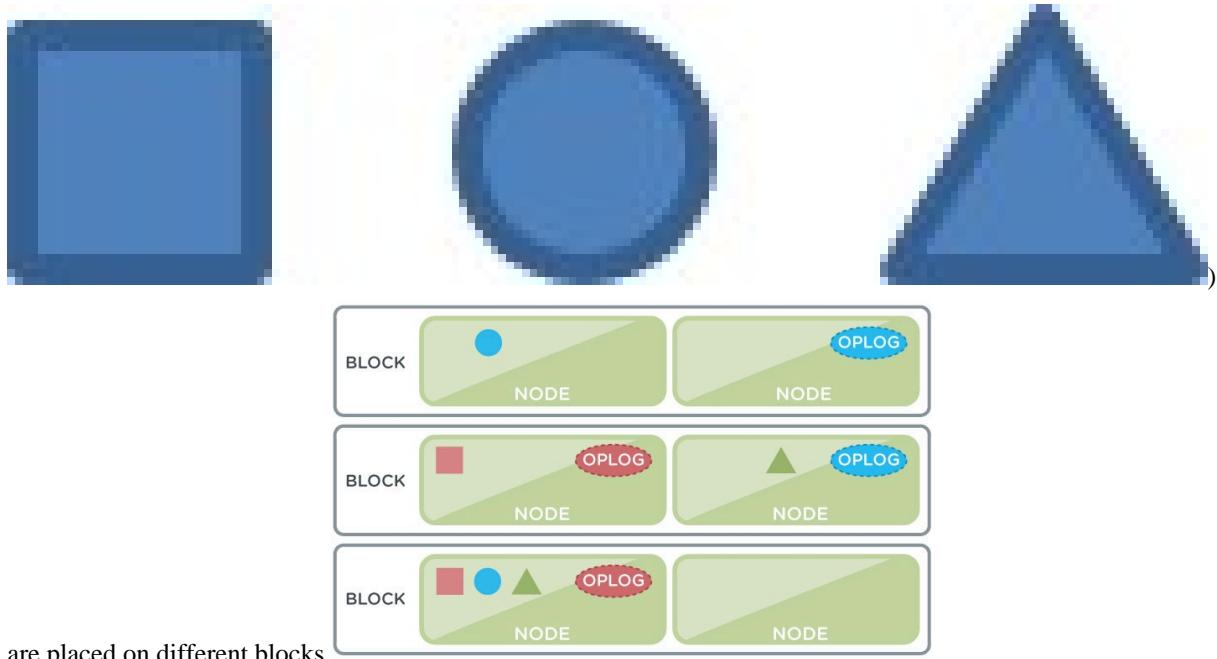
Depending on the volume of data that needs to be relocated, it might take Curator several scans over a period of hours to distribute data across the blocks.

Block fault tolerant data placement is on a commercially reasonable effort but is not guaranteed. Conditions such as high disk usage between blocks might prevent the cluster from placing guest VM redundant copy data on other blocks.

## Guest VM Data

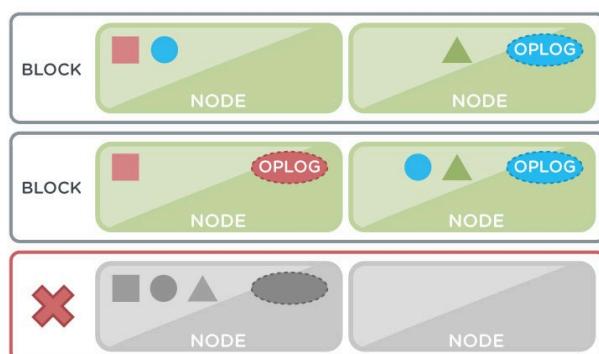
Redundant copies of guest VM data are written to different blocks from that block that the VM is running in. The cluster maintains two copies of each write in the oplog.

Redundant copies of the guest VM data (designated by



**Figure 12: Block-aware placement of guest VM data**

In the case of a block failure, the system copies the under-replicated guest VM data to other blocks in the cluster, and only one copy of the oplog contents becomes available.

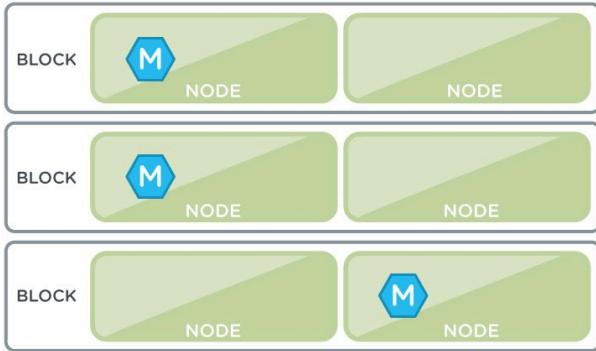


**Figure 13: Block-aware placement of guest VM data with block failure**

## Metadata

The Nutanix Medusa component uses Cassandra to store metadata. Cassandra uses a ring-like structure where data is copied to peers within the ring to ensure data consistency and availability. The cluster keeps at least three redundant copies of the metadata, at least half of which must be available to ensure consistency.

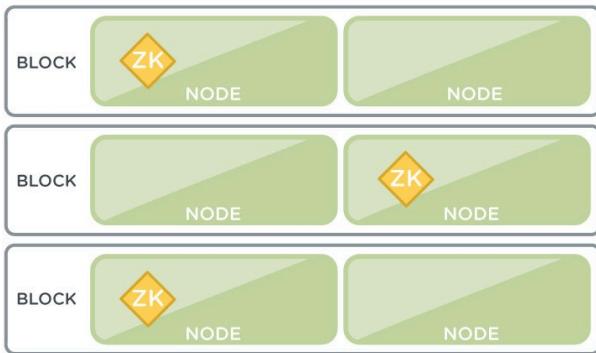
With block fault tolerance, the Cassandra peers are distributed among the blocks to ensure that no two peers are on the same block. In the event of a block failure, at least two copies of the metadata is present in the cluster.



**Figure 14: Block-aware placement of metadata**

### Configuration Data

The Nutanix Zeus component uses Zookeeper to store essential configuration data for the cluster. The Zookeeper role is distributed across blocks to ensure availability in the case of a block failure.



**Figure 15: Block-aware placement of configuration data**

### Data Resiliency Levels for Block Fault Tolerance

The following table shows the level of data resiliency (simultaneous failure) provided for the following combinations of replication factor, minimum number of nodes, and minimum number of blocks.

**Table 9: Data Resiliency Levels**

Replication Factor	Minimum Number of Nodes	Minimum Number of Blocks	Data Resiliency
2	3	1	1 node or 1 disk failure
2	3	3 (minimum 1 node each)	1 block or 1 node or 1 disk failure
3	5	2	2 nodes or 2 disk failures
3	5	5 (minimum 1 node each)	2 blocks or 2 nodes or 2 disks

Replication Factor	Minimum Number of Nodes	Minimum Number of Blocks	Data Resiliency
3	6	3 (minimum 2 nodes each)	1 block or 2 nodes or 2 disks
Metro Cluster (For more information, see <a href="#">Metro Availability (ESXi and Hyper-V 2016)</a> in the <i>Data Protection and Recovery with Prism Element</i> guide.)	3 nodes at each site	2	1 cluster failure

The state of block fault tolerance is available for viewing through the Prism Element web console and Nutanix CLI. Although administrators must set up the storage tiers or storage containers, they cannot determine where data is migrated. AOS determines where data is migrated.

Prism Element web **Cluster Resiliency / Fault Tolerance Status** widget on the **Home** screen console

nCLI

```
ncli> cluster get-domain-fault-tolerance-status type="rackable_unit"
```

### Rack Fault Tolerance

Rack fault tolerance is the ability to provide rack level availability domain. With rack fault tolerance, redundant copies of data are made and placed on the nodes that are not in the same rack.

Rack failure can occur in the following situations:

- All power supplies fail within a rack
- Top-of-rack (TOR) switch fails
- Network partition; where one of the racks becomes inaccessible from other racks

When rack fault tolerance is enabled, the cluster has rack awareness and the guest VMs can continue to run with failure of one rack (replication factor 2) or two racks (replication factor 3). The redundant copies of guest VM data and metadata exist on other racks when one rack fails.

#### Note:

- If a sufficient number of working racks are not present after a failure, the data is rebuilt in a non-rack-aware manner to get the node fault-tolerance level to one. The rack-fault-tolerance remains zero.
- Rack Fault Tolerance is supported for AHV, ESXi, and Hyper-V.
- Prism Central workflows are not applicable for rack fault tolerance using Hyper-V because Prism Central does not support Hyper-V.

### Configuring Rack Fault Tolerance

#### About this task

To enable rack fault tolerance, you must specify the mapping of the blocks to the racks based on the actual placement of the blocks in the datacenter.

To configure rack fault tolerance, do the following.

## Before you begin

- You must have information on the actual physical mapping of racks and blocks in the datacenter.
- Minimum cluster requirements:
  - Replication factor 2 - 3 racks (4 with Erasure Coding), 1 node in each rack
  - Replication factor 3 - 5 racks (6 with Erasure Coding), 1 node in each rack
- Network Latency Limit - The round trip latency for communication between Controller VMs in a Nutanix cluster should be less than or equal to 1 ms (millisecond).

## Procedure

1. Log in to the Prism Element web console.
2. Go to **Settings > Setup > Rack Configuration..**

**Note:** Directory List (AD and OpenLDAP) users can view and configure Rack Awareness only if a service account is configured for the directory service. For more information about how to configure a service account for the directory service, see [Configuring Authentication](#) in the *Security Guide*.

3. Select **Rack** as the fault tolerance domain, and click **Next**.
4. Click **+ Add New Rack**, and enter the name of the rack in the **Rack Name** field.
5. Click **Add Blocks** to assign the discovered blocks to the rack.
6. Click **+** to add the block to the rack based on the actual placement of the block in the datacenter, and click **Done**.  
Repeat steps 4 through 6 for adding more rack configurations. Verify the configuration and click **Save**.

The **Cluster Resiliency / Fault Tolerance Status** widget on the Prism dashboard shows the current state of the fault tolerance.

### Note:

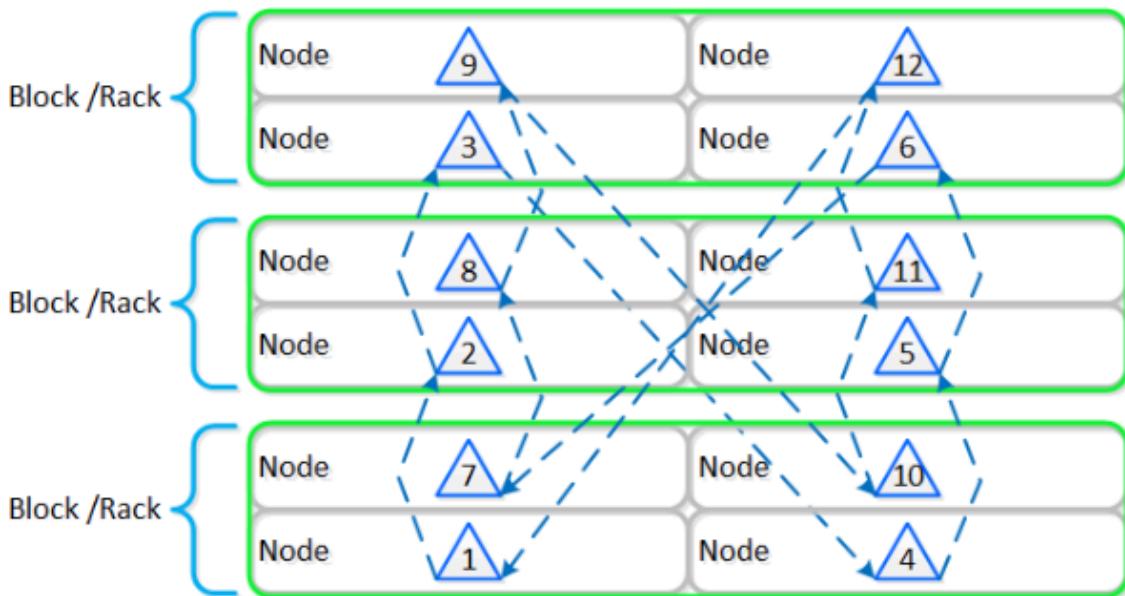
The fault tolerance has Four states.

- **OK:** This state indicates that the fault tolerance domain is highly resilient to safely handle a node or a disk (in single or two node clusters) failure.
- **Warning:** This state indicates that the fault tolerance level is almost reaching to 0. Warning state is displayed if the cluster is not fault tolerant at the configured domain, but is fault tolerant at a lower domain. For example, if you have configured rack as the configured domain and the cluster can no longer handle any rack failures due to some reason but can still handle node (lower domain) failures, then fault tolerance state is displayed as Warning.
- **Critical:** This state indicates that the fault tolerance level is 0, and the fault tolerance domain cannot handle a node or a disk (in single or two node clusters) failure.
- **Computing:** This state indicates that the new fault tolerance level is being calculated. This state is displayed soon after a node or disk failure, before rebuild is initiated.

**Note:** Once rack fault tolerance is enabled; create, edit, delete operations are not allowed. To make any new modifications, you must re-configure the fault tolerance level as **Node**. Enabling rack fault tolerance may trigger Cassandra ring change operations and trigger curator scans to redistribute replicas for rack fault tolerance. The time taken for these depend on existing data on cluster, workload on the cluster, and configurations. For more information, see [Configuring Node Fault Tolerance](#) on page 29.

## Rack Awareness Metadata Requirements for Rack Fault Tolerance

Nutanix stores essential metadata in a ring-like structure to provide data resiliency. Replication of metadata to all the nodes of a rack-aware configuration occurs in the form of a ring to ensure data consistency and availability. With this metadata placement, in the event of a rack failure, a minimum two copies of data are available as a backup.



**Figure 16: Node replication topology to form a ring-like structure in a rack-aware cluster**

Nutanix uses a data resiliency factor also known as replication factor to ensure data redundancy and availability, which is based upon the cluster fault tolerance (1N/1D, 1N&1D, and 2N/2D). The following table provides the metadata and data replication factor values for the corresponding FT level:

Cluster Fault Tolerance Level	Metadata Replication Factor	Data Replication Factor
1N/1D	3	2
1N&1D	3	3
2N/2D	5	3

## Rack Awareness Metadata Placement Requirements

Before you add nodes to or remove or move nodes from a rack-aware cluster, you must achieve rack-awareness resiliency by following the metadata placement requirements.

Use the following criteria to calculate the rack-aware metadata placement:

- Minimum number of metadata RF rack domains required:

$$\text{Metadata RF} = (\text{FT} \times 2) + 1$$

where RF is replication factor and FT is fault tolerance

- Total number of nodes required in a cluster:

$$\text{Nodes} \# N \times \text{Metadata RF}$$

where N is the maximum number of nodes in a rack domain

Example:

If a cluster has 1N/1D and 4 maximum nodes in a rack domain:

Minimum number of metadata RF rack domains required:

$$\text{Metadata RF} = (1 \times 2) + 1 = 3$$

Total number of nodes required in a cluster:

$$\text{Nodes} = 4 \times 3 = 12$$

Rack-aware resiliency is achieved from 3 racks and 12 nodes.

### Data Resiliency Levels for Rack Fault Tolerance

This topic provides information about the level of data resiliency (simultaneous failure) provided for various combinations of replication factor, minimum number of disks, minimum number of nodes, minimum number of blocks, and minimum number of racks when Erasure Coding (EC) is disabled or enabled in the containers.

**Table 10: Data Resiliency Levels with EC disabled**

Fault Domain	Replication Factor	Minimum number of Disks	Minimum Number of Nodes	Minimum Number of Blocks	Minimum Number of Racks	Data Resiliency
Disk	1*	1	1	1	1	None
	2	2	1	1	1	1 disk failure
Node	2	Not applicable	3	1	1	1 node or 1 disk failure
	3	Not applicable	5	2	1	2 nodes or 2 disk failures
Block	2	Not applicable	3	3	1	1 node or 1 block or 1 disk failure
	3	Not applicable	5	5	1	2 nodes or 2 blocks or 2 disk failures
Rack	2	Not applicable	3	3	3	1 node or 1 block or 1 rack or 1 disk failure
	3	Not applicable	5	5	5	2 nodes or 2 blocks or 2 racks or 2 disk failures

\* Before using replication factor 1, see [KB-11291](#) for replication factor 1 guidelines and limitations.

**Table 11: Data Resiliency Levels with EC enabled**

Fault Domain	Replication Factor	Minimum Number of Nodes	Minimum Number of Blocks	Minimum Number of Racks	Data Resiliency
Node	2	4*	1	1	1 node or 1 disk failure
	3	6*	2	1	2 nodes or 2 disk failures
Block	2	4	4*	1	1 node or 1 block or 1 disk failure
	3	6	6*	1	2 nodes or 2 blocks or 2 disk failures
Rack	2	4	4	4*	1 node or 1 block or 1 rack or 1 disk
	3	6	6	6*	2 nodes or 2 blocks or 2 racks or 2 disks

\* Minimums that are required to enable erasure coding on new containers in rack aware clusters.

**Caution:** If rack awareness is enabled on a cluster with EC functionality enabled, the cluster might need to reduce the EC strip size to comply with the new fault tolerance configuration. This leads to an increased usage of space in the cluster temporarily, due to the unpacking of EC strips. After the re-packing of EC strips is complete, some amount of savings will be lost (depending on initial and final EC strip sizes).

For example, an EC enabled 12-node cluster will have the EC strip size as 4/2 (4 data blocks and 2 parity blocks). If rack awareness is enabled on this cluster with 6 racks and 2 nodes in each rack, the EC strip size changes to 2/2 (2 data blocks and 2 parity blocks), leading to lesser savings to accommodate the new fault tolerance configuration.

For more information about EC strip sizes based on cluster size, see the [Nutanix Erasure Coding](#) solutions documentation.

## Cluster Rebuild Preference

Nutanix AOS provides cluster resilience capability to protect your clusters from failures. You can choose to reserve storage capacity within clusters for use in rebuilding failed disks, nodes, blocks, or racks. For more information, see [Rebuild Capacity Reservation](#) on page 107.

The rebuild operation requires additional storage on the cluster and might lead to space bloats during planned maintenance. These space bloats consume the free capacity on a cluster and might impact the cluster operations. For planned maintenance operations (such as software or firmware upgrades), you can set the rebuild preference to *Smart* using Prism Element or Prism Central. When the cluster rebuild preference is set as *Smart*, the system differentiates between a failure and a planned outage during an upgrade. During failure scenarios, the system initiates an immediate rebuild and during planned maintenance, the system optimizes the rebuild behavior to minimize the amount of data moved, rebuilt, and garbage collected.

**Note:** The *Delayed* cluster rebuild preference setting is deprecated from AOS 6.7 release. If you have the *Delayed* cluster rebuild preference configured in your setup, the system changes it to *Smart*.

Starting with AOS 6.8 release, the cluster rebuild preference is set as *Smart* by default. You can modify the cluster rebuild preference from Prism Element and Prism Central. For information on how to modify the cluster rebuild preference from Prism Element, see [Modifying Cluster Rebuild Preference](#) on page 77. For information on how to modify the cluster rebuild preference from Prism Central, see [Cluster Management](#) in the *Prism Central Infrastructure Guide*.

The following table describes the difference in cluster rebuild operation between *Smart* and *Immediate* preference:

**Table 12: Rebuild Preference for Upgrade**

Immediate	Smart
During an upgrade or failure, the rebuild process starts almost immediately (approximately 60 seconds) when Stargate of the node being upgraded is down.	During an upgrade, the system identifies the planned outage occurrence as a maintenance activity, and restricts unnecessary component rebuilds that might lead to space bloats on the cluster. However, if the upgrade extends beyond expected time or if any failure occurs in the cluster, the system triggers an immediate rebuild to restore cluster resiliency.

## Replication Factor

Replication factor refers to the number of copies of data maintained on a storage container in a cluster.

Nutanix clusters rely on replication factor for data protection and availability. This method provides the highest degree of availability because it does not require reading from multiple storage locations or data recomputation after a failure. However, this advantage comes at the cost of storage resources, as it requires full copies.

Following are the types of replication factor supported in a Nutanix cluster:

- [Replication Factor 1](#) on page 41
- [Replication Factor 2](#) on page 41
- [Replication Factor 3](#) on page 41

For information on how to configure replication factor on a storage container, see [Replication Factor Configuration](#) on page 137.

## Requirements

The following table lists the replication factor you can configure corresponding to the cluster fault tolerance configured in the cluster and the minimum number of nodes listed for the cluster fault tolerance.

**Table 13: Replication Factor Requirements**

Replication Factor	Cluster Fault Tolerance	Minimum Number of Nodes
2	1N/1D	3
3	1N&1D	3 (minimum number and maximum number of nodes are the same)
3	2N/2D	5

## Replication Factor 2

A replication factor of 2 means that the cluster maintains two copies of the data (the original data and a copy of the original data) for each replication factor 2 enabled storage container.

To configure replication factor 2 in a cluster, the cluster must have a minimum of 3 nodes. For more information, see [Requirements](#) on page 40.

For information on how to configure replication factor on a storage container, see [Replication Factor Configuration](#) on page 137.

## Replication Factor 3

A replication factor of 3 means that the cluster maintains three copies of the data (the original data and two copies of the original data) for each replication factor 3 enabled storage container.

Replication Factor 3 adds an extra layer of data protection at the cost of storing an additional copy of the data. To configure replication factor 3 in a cluster, the cluster must have a minimum of 5 nodes. For more information see [Requirements](#) on page 40. Nutanix recommends configuring replication factor 3 at sites with high protection requirements, but this requires more nodes and storage capacity.

For information on how to configure replication factor on a storage container, see [Replication Factor Configuration](#) on page 137.

## Replication Factor 1

A replication factor of 1 means that the cluster maintains only the original data without any copies.

Replication factor 1 does not guarantee data availability if a node or disk failure occurs. Therefore, Nutanix recommends that you enable replication factor 1 only when your cluster is running applications that provide their own data protection or high availability. When you enable replication factor 1, the cluster maintains a single copy of data for each replication factor 1 enabled storage container. The storage container contains multiple vDisks that you can directly attach to a VM or implement as part of a volume group. Each replication factor 1 enabled storage container is associated with a specific node that you choose. All the data in the replication factor 1 enabled storage container is associated with that node only.

Clusters with replication factor 1 enabled storage containers can improve I/O performance for write-intensive applications that do not need storage level data protection. Applications that provide their own data protection and applications that perform at high I/O rates on ephemeral data can benefit from this type of storage. Workloads that can benefit from storing data in a replication factor 1 enabled storage container include artificial intelligence (AI), machine learning (ML), and big data.

For information on how to enable replication factor 1, see [Enabling Replication Factor 1](#) on page 139.

### Recommendations

Nutanix recommends the following.

- For each cluster where you want to use replication factor 1, create one replication factor 1 enabled storage container per node. The replication factor 1 enabled storage container can contain multiple replication factor 1 enabled vDisks.
- For clusters running an ESXi hypervisor, ensure that you mount the replication factor 1 enabled storage container on a single host only. Mounting the replication factor 1 enabled storage container on multiple hosts is not supported.
- Do not enable replication factor 1 storage containers on clusters where SSD tier capacity is less than 6 percent of total cluster capacity.

### Limitations

**Table 14: Unsupported Software, Features, and Operations**

Nutanix Software	Description
Nutanix Database Service (NDB)	Using a replication factor 1 enabled storage container as part of configuration and deployment is not supported.
Nutanix Files	Using a replication factor 1 enabled storage container as part of configuration and deployment is not supported.
Nutanix Karbon	Using a replication factor 1 enabled storage container as part of configuration and deployment is not supported.
Nutanix Objects	Using a replication factor 1 enabled storage container as part of configuration and deployment is not supported.
Prism Central	Do not deploy Prism Central on replication factor 1 enabled storage containers. This configuration is not supported.
Cluster Hypervisor	Support or Limitation
Microsoft Hyper-V	Enabling replication factor 1 on clusters running Microsoft Hyper-V is not supported.
Mixed hypervisor cluster	For VMware ESXi and AHV mixed hypervisor clusters, replication factor 1 enabled storage containers and VMs with attached replication factor 1 enabled vDisks are not supported on the AHV storage-only nodes.
VMware ESXi	Using vSphere HA with Distributed Resource Scheduler (DRS) is not supported for any VM with at least one replication factor 1 enabled vDisk.  You can enable replication factor 1 on the nodes running the VMware ESXi hypervisor.
Feature or Operation	Support or Limitation
Snapshots and data protection/recovery	For vDisks in replication factor 1 enabled storage containers, disaster recovery operations like snapshots and replication are not supported.
In-place hypervisor conversion	Not supported when converting a cluster from AHV to ESXi.
Deduplication	Not supported for replication factor 1 enabled storage containers.
Erasure coding	Not supported for replication factor 1 enabled storage containers.
Degraded Node	Not supported for replication factor 1 enabled CVMs.

Feature or Operation	Support or Limitation
Metro availability	Not supported for replication factor 1 enabled storage containers and VMs with attached replication factor 1 enabled vDisks.
Recycle bin	Not supported. When you delete an replication factor 1 enabled vDisk, the vDisk is marked for deletion as soon as possible and bypasses the recycle bin.
Storage container settings or modification with replication factor 1 enabled	<p>These settings or modifications are not supported.</p> <ul style="list-style-type: none"> <li>• Increasing the replication factor</li> <li>• Enabling capacity reservation (Reserve Capacity setting) or Reserve Rebuild Capacity</li> <li>• Storage containers with Reserve Capacity or Reserve Rebuild Capacity already enabled</li> </ul>
Maintenance mode operations (planned)	<p>The following operations automatically shut down and restart replication factor 1 enabled VMs.</p> <ul style="list-style-type: none"> <li>• Controller VM shutdown</li> <li>• Memory update</li> <li>• Host boot disk replacement</li> <li>• Nutanix Flow microsegmentation work flows</li> <li>• Request Reboot (rolling reboot operation)</li> </ul>
ESXi hypervisor 1-click upgrade	Automatic VM shutdown is not supported. You must manually shut down replication factor 1 enabled VMs before upgrading and restart them after the upgrade is completed.
LCM upgrade operations	<p>The following LCM upgrade operations automatically shut down and restart replication factor 1 enabled VMs.</p> <ul style="list-style-type: none"> <li>• AOS upgrade</li> <li>• Firmware upgrades for ESXi and AHV clusters</li> <li>• AHV hypervisor upgrade</li> </ul>

Feature or Operation	Support or Limitation
Upgrade operations, VM with volume group access	<ul style="list-style-type: none"> <li>For any VM with a volume group directly attached to the VM (AHV clusters only), the cluster will automatically shut down and power on the VM as part of the upgrade operation.</li> <li>For any VM with volume group access provided by Nutanix Volumes (that is, connection to the volume group from the VM guest OS through an iSCSI target IP address), you must manually shut down the VM. You can power on the VM when the upgrade operation is completed.</li> </ul>
Unplanned event	<p>These unplanned events might affect I/O operations for VMs with vDisks in replication factor 1 enabled storage containers, as you cannot shut down these VMs in advance of these events.</p> <ul style="list-style-type: none"> <li>Disk or node failure</li> <li>Controller VM Stargate service failure</li> <li>Controller VM failure or restart</li> <li>Degraded node</li> </ul>
Node removal	<p>When you remove a node that contains an replication factor 1 enabled storage container, the storage container and its vDisks are marked for removal.</p> <p>The storage container is not automatically marked for deletion. As part of node removal (which first fails in this case), you are prompted to delete the storage container, including all data on the storage container. This is effectively the same as deleting the container.</p>
Disk removal or replacement	<p>When you remove or replace a node's disk in an RF1-enabled storage container, data in the RF1-enabled storage container is automatically migrated to other disks associated with the RF1 node. If the node has insufficient disk space, the disk removal fails with a message similar to Warning: no disk space for RF1 data.</p> <p>For a failed disk with RF1 data that has no extra replicas, the data cannot be rebuilt. Therefore, when logically removing a failed disk with RF1 data, the disk removal might get stuck. In order to unblock the disk removal, delete the RF1 data in the degraded disk for a thorough cleanup. For more information, see <a href="#">KB 11662</a>.</p>

## Degraded Node

A degraded node has a CVM that is partially unresponsive, preventing it from performing cluster operations as efficiently as fully functional nodes.

Nutanix clusters are designed to ensure fault tolerance using container settings like replication factor. However, fault tolerance alone does not guarantee protection against partial failures or degraded nodes. For instance, a single node with a disk experiencing high latency, even if partially responsive, can cause downtime for workloads in clusters with both replication factor 2 and replication factor 3 settings.

Degraded node events can occur because physical hardware can fail in many ways. While diagnostics can capture some of these events in software-defined failure scenarios, degradation can still lead to downtime for some or all production workloads on the cluster.

The following events might contribute to node degradation:

- Network bandwidth reduction
- Network packet drops
- Soft lockups
- Partly malfunctioning disks
- Hardware issues (such as unreliable DIMM with ECC errors)

## Degradation Effects

Nutanix clusters are designed to distribute the cluster services across the Controller VMs on all the constituent nodes to offer the best possible performance and resource allocation for the workloads. This distribution of services might cause a *degraded* (or partially available) node to adversely affect the performance of a cluster until you resolve the degradation.

## Degradation versus Complete Failure

The difference between complete and partial failures (leading to degradation) explains the possibility of downtime during a degradation event.

### Degradation

When a component such as a NIC or an SSD drive starts generating errors or drastically slows its throughput, the *Local Handler* service provides the first line of resolution.

For example, in an SSD drive, the *Local Handler* refers to either:

- The disk firmware deployed by the disk vendor.
- A Nutanix service on the Controller VM residing on the degraded node, such as the *Stargate* service, or the *Hades* disk manager.

When the *Local Handler* service recognizes that the SSD is producing a failure pattern that matches a harmful pattern, it marks the SSD as offline and Prism displays the SSD as a routine drive failure.

When the *Local Handler* encounters failure patterns that it does not recognize, the SSD continues to remain online. However, as a result of the failure pattern, the faulty device slows or halts the functioning of (or degrades) the distributed services throughout the cluster that depends on the device. This degradation of cluster services might lead to performance impact or storage unavailability for workload residing on nodes beyond the node with the SSD. This type of failure is termed as a *partial failure* of a component, where manual intervention is required to disable the degraded device and help the cluster services to recover. The *Local Handler* is unable to detect and mark the faulty device as faulty, resulting in the device remaining online and degrading the performance of the cluster.

### Complete Failure

A complete component failure occurs when a fault on a single node in the cluster is effectively managed. Examples include a node going offline due to AC power loss or network isolation. In these events, the Controller VM becomes unreachable from the rest of the cluster. The cluster then works to restore resiliency based on the fault tolerance configured in the cluster.

**Table 15: Fault-Response Matrix**

Type of fault	Local Handler*	Examples of response**
Disk error	Disk firmware	Update S.M.A.R.T. data to reflect that a disk has failed or could soon fail. For more information, see <a href="#">KB 8094</a> .
	HBA firmware	Multiple disks could be marked as offline.
	CentOS operating system	Mount disk as read-only.
		Register <i>udev</i> event for disk hot-plug
		Remove Controller VM boot disk partitions from RAID.
	Stargate Service	Mark disk as offline if read or write operation is not responding, send to Hades service to test.
	Cassandra Service	Controller VM is detached from the cluster metadata store, or a metadata repair is triggered, when Cassandra becomes unstable due to a failing disk.
	Curator Service	Stops using a particular disk during Curator scans if it produces I/O errors.
CPU error	BIOS firmware	Tests any drive that is marked offline by Stargate to check its S.M.A.R.T. health status and whether it is mountable.
		Monitors HBA error counters on disk interfaces. Raises alert if thresholds are exceeded.
		Correcting and logging recoverable errors
	Hypervisor OS	Throttle CPU if necessary
		Halting and logging unrecoverable errors
		Throttle performance
		Panic or halt
		Core dump
Memory error	BIOS	Restart or hang.
		Correcting and logging recoverable errors
		Online disabling of bad memory segments
		Decreasing the usable memory of a failing DIMM
	Hypervisor OS	Masking a failing DIMM and potentially others in that channel
		Throttle performance

Type of fault	Local Handler*	Examples of response**
		Logging errors
		Panic or halt
		Restart or hang.
Network error	NIC firmware	CVM/ host lost connection.
	Software virtual switch	Error disable of bonded interface (Link Aggregation Control Protocol (LACP) timer set to <i>fast</i> ) Failover to standby NIC (in active-standby bond modes)

**Note:**

\* Local handlers could have other dependencies on the cluster. Their failure-handling abilities might not be available during events where more than one node is impacted by a particular failure.

\*\*Response logic depends on the features available in the specific software or firmware versions deployed. It might be subject to change. Nutanix recommends that if you consider upgrading to the latest AOS release for the latest fault-tolerance capabilities.

## Degraded Node Detection

The Degraded Node Detection (DND) feature helps you limit the duration of impact or effects of a degraded node. In a Nutanix cluster, DND constitutes the second line of resolution against partial hardware and software failures that escape the current logic of *Local Handler* services.

DND consists of a global peer health database which monitors the services that run on each node of the cluster. Each node publishes health scores or votes for the services running on other peer nodes. The peer nodes health scores evaluate metrics such as:

- Remote Procedure Call (RPC) latency
- RPC failures or timeouts
- Network latency

If one node consistently receives poor health scores for approximately three minutes then the peer nodes mark that node as a degraded node. The cluster might experience unavailability of storage containers or data stores during this three minute period.

The DND feature acts only when all of the following conditions are met:

- The cluster was **Resilient** prior to the event and could tolerate a node failure.
- The partial failure occurs only on one node in the cluster.
- The adverse effects of the partial failure sustain for at least five minutes.

### Detection

DND works as follows:

- When a degraded node is detected, alerts are generated.

See the alerts in the **Alerts** page. For more information on these alerts, see [KB 3827](#) and [KB 9132](#).

The alerts trigger log collection to aid root cause analysis. See the **Log Collection for Alert XXXX** on the **Tasks** page. Click the **Succeeded** link to download the logs.

- If the degraded node had leadership of critical services including Prism, the leadership is revoked.
  - Insights Data Fabric (IDF) services do not run on the degraded node.
  - Cassandra services operate in Forwarding mode, meaning that the read and write requests from the Stargate service of a degraded node are handled by Cassandra services on other nodes.
- Until the degradation is resolved, the cluster cannot guarantee storage availability in the event of subsequent partial or complete failures on other nodes.
- Stargate of the degraded node stops placing Extent Group replicas on the degraded node.
  - If the degraded node hosts a Zookeeper server, that server is migrated to the Controller VM of another node.
  - The cluster is blocked from starting new upgrades or break-fix activities. If a node becomes degraded in the middle of an ongoing upgrade, an alert is generated.
  - DND includes an auto-resolve function that activates one day after a node is marked degraded. If the node remains degraded, the auto-resolve scan runs for about 60 minutes to check if the issue is resolved. If no issues are found, the node is automatically marked as normal. This prevents the metadata store on the node from being permanently marked offline if the cluster is healthy.

**Note:** Do not manually change the degraded status of a node (using the **Mark as Fixed** in the Prism Element web console) without confirming that the issue causing the node or CVM degradation has been fixed. Manually marking a degraded node as fixed can lead to significant production issues including downtime of the cluster. Contact Nutanix Support for assistance.

## Enabling or Disabling Degraded Node Detection

### About this task

To enable or disable the degraded node detection settings in the Prism Element web console, perform the following steps.

### Procedure

- From the dropdown menu on the left of the main menu, select **Settings**.  
The system displays the **Global Settings** page.
- From the **Data Resiliency** section in the left navigation pane, click **Degraded Node Settings**.  
The **Degraded Node Settings** page opens.
- Perform one of the following:
  - To enable DND, select the **Enable Degraded Node Detection** checkbox.
  - To disable DND, clear the **Enable Degraded Node Detection** checkbox.
- Click **Save** to confirm the settings.  
The **Degraded Node Settings** window closes and the Prism Element web console displays a pop-up confirming the changes.

## Managing a Degraded Node

Manage a node if it is marked as degraded.

### About this task

Once a node is detected as degraded, the leadership and critical services will not be hosted on that node.

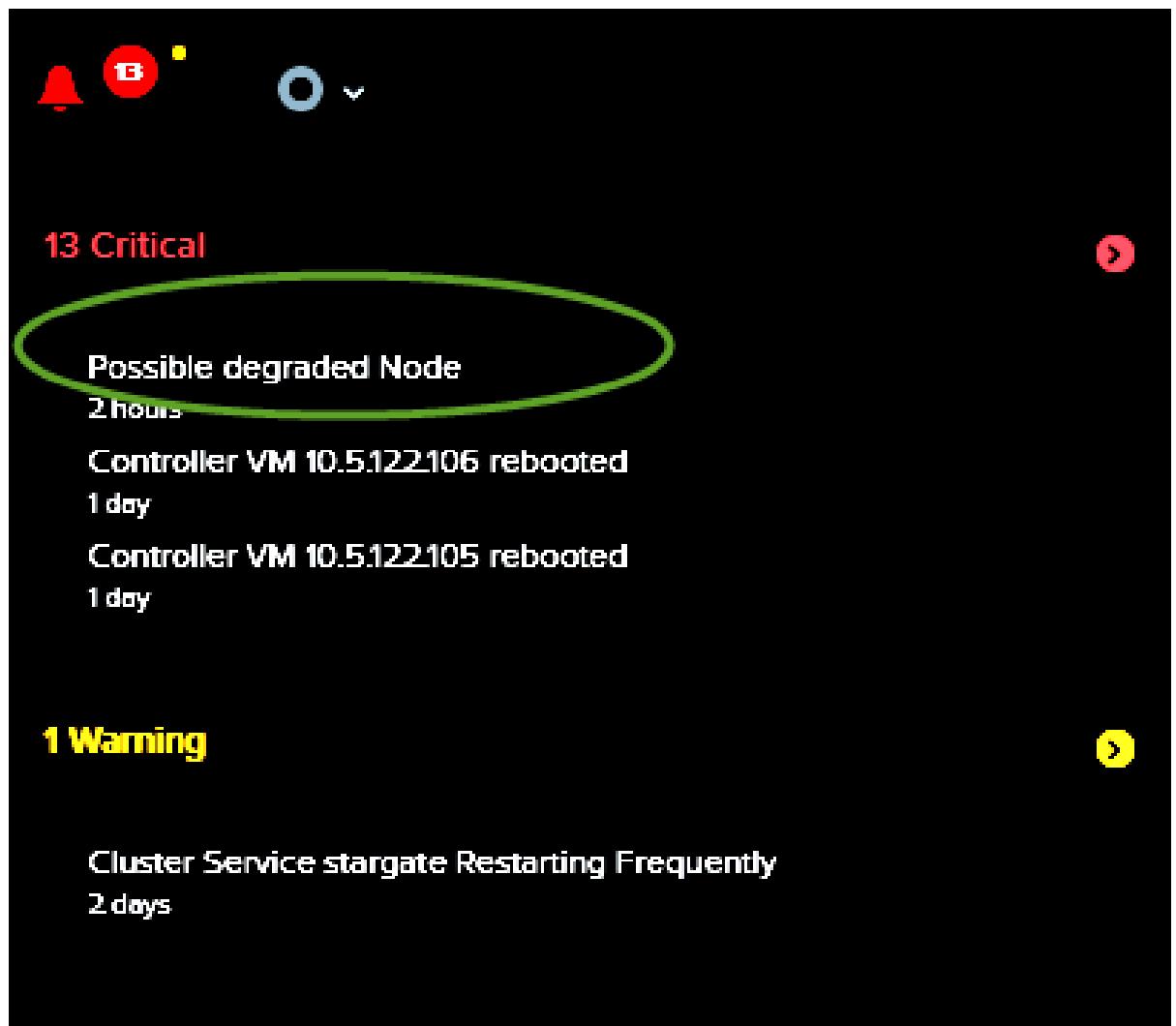
**Note:** When you set the degraded node operation to shut down or restart the CVM using `edit-degraded-node-policy`, the system places the CVM in maintenance mode before the action. If the node hosts replication factor 1 VMs, the system skips maintenance mode and ignores the shutdown or restart to keep those VMs available.

Until a degraded node is unmarked from the degraded state, Cassandra services remain in the forwarding state. For more information, see [Cluster Components](#) on page 12. Once the degraded node is marked as fixed in Prism, Cassandra restarts its services on the node.

The alert for a degraded node appears in the **Alerts** page of the Prism Element web console.

## Procedure

1. Open the degraded node window.
  - a. Click the **Alerts** icon at the top of the page.
  - b. Click the alert for the degraded node.



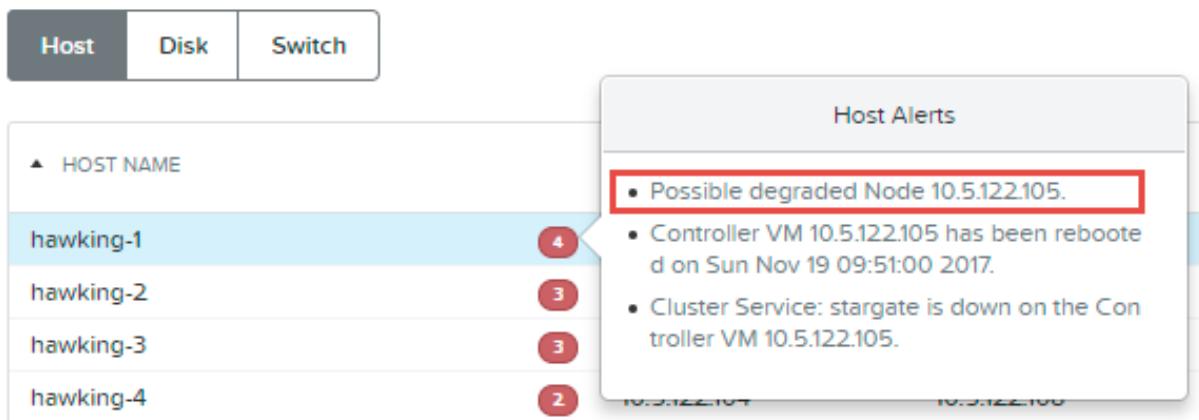
**Figure 17: Possible Degraded Node in Alerts**

The degraded node window is displayed.

2. Set the status for the degraded node.
  - a. **Resolve:** Select this option after you have fixed the underlying issue.

**Note:** Selecting **Resolve** does not resolve the degraded node issue. It merely marks the alert status as **Resolved**, indicating you or Nutanix Support have resolved the underlying issue that triggered the alert.
  - b. **Acknowledge:** Select this option to leave the degraded node in its current state, keep the alert unresolved, and mark the alert as acknowledged.

3. You can also view the degraded node in the **Hosts** table.
  - a. Go to **Home > Hardware > Host**.
  - b. Select the degraded node which displays a critical alert.



**Figure 18: Degraded Node Pop-up Alert**

4. To run an NCC check for the degraded node, go to the command line interface and enter

```
nutanix@cvm$ ncc health_checks system_checks degraded_node_check
```

The Prism Element web console does not remove the warning sign for the degraded node.

5. **Caution:** Do not unmark the degraded node if you have not confirmed that the issue causing the node or CVM degradation has been fixed. Unmarking a node can lead to production impacting issues in the cluster. Contact Nutanix Support for assistance.

To unmark the degraded node, in the **Summary** view, select the fixed node and click **Mark as Fixed**.

## Maximum System Values

Following are the considerations regarding the maximum number of hosts in a cluster:

- If you have a pure hypervisor cluster (cluster with only one type of hypervisor), you must adhere to the maximum number of hosts allowed by [Nutanix Configuration Maximums for AHV](#) or [Nutanix Configuration Maximums for ESXi](#) or [Nutanix Configuration Maximums for Hyper-V](#).
- If your cluster consists of multiple hypervisors (mixed hypervisor cluster), you must adhere to the minimum number of hosts specified for any of the hypervisors in your cluster. For example, if your cluster consists of AHV and ESXi, then you are allowed to have the number of hosts specified for either AHV or ESXi, whichever is less. For more information, see [Nutanix Configuration Maximums for AHV](#), [Nutanix Configuration Maximums for ESXi](#), and [Nutanix Configuration Maximums for Hyper-V](#).
- In a break-fix or generational upgrade (for example moving from NX G5 to G8 platform model) scenario, if you must exceed the number of hosts beyond the configuration maximum, contact Nutanix Support to temporarily allow the cluster extension beyond the limit. Clusters must always adhere to the size limits to ensure optimal performance and stability and you are allowed to exceed the limits only temporarily for these scenarios as an exception. You are expected to follow the size limits once the node is healthy or upgrades are complete. For more information, see [KB 12681](#).

Nutanix clusters are also subject to the vSphere maximum values documented by VMware. For more information about the list of the vSphere maximums, see [Configuration Maximums](#) for the version of vSphere you are running.

In case of contention of values between Nutanix and VMware, the Nutanix configuration maximum supersedes the VMware configuration maximum on Nutanix platforms.

Nutanix supports up to 50 VMs for each storage container if you are using Microsoft VSS-based backups in Hyper-V. If the number of VMs in each storage container exceeds 50, you might observe NFS timeouts when running backup jobs.

## Three Node Cluster Considerations

A Nutanix cluster requires a minimum of three nodes. This minimum configuration offers the same protections as larger clusters, allowing a three-node cluster to continue operating normally even after a node failure. However, there is a specific condition that applies only to three-node clusters.

In clusters with four or more nodes, if a node fails, you can dynamically remove the failed node to restore the cluster to full health. The cluster, now with at least three nodes, remains fully protected. You can then replace the failed hardware for that node and add the node back into the cluster as a new node.

In contrast, with a three-node cluster, the failed node cannot be dynamically removed. The cluster continues to run with two healthy nodes and one failed node, but the failed node cannot be removed when there are only two healthy nodes. Therefore, the cluster remains unprotected until you fix the problem with the failed node.

# CLUSTER MANAGEMENT

---

Managing a Nutanix cluster involves configuring and monitoring the entities within the cluster, including virtual machines, storage containers, and hardware components. You can manage a Nutanix cluster through the Prism Element web console or a command line interface (nCLI).

- The Prism Element web console allows you to monitor cluster operations and perform a variety of configuration tasks. For more information, see [Prism Element Web Console Overview](#) on page 53.
- Nutanix employs a license-based system to enable your entitled Nutanix features, and you can install or regenerate a license through the Prism Element web console. For more information, see [Prism Licensing](#) on page 73.
- You can upgrade a cluster when a new AOS release is available through the Prism Element web console. For more information, see the [Life Cycle Manager Guide](#).
- If you have multiple clusters, you can manage them all through a single web interface. For more information, see [Multi-Cluster Management](#) on page 91.

**Note:** You can perform most administrative actions using either the Prism Element web console or nCLI. However, some tasks are only supported in the nCLI either because a new feature has not yet been incorporated into the Prism Element web console or the task is part of an advanced feature that most administrators do not need to use. For more information about how to use the nCLI, see [Command Reference](#). For information about platform configuration and hypervisor-specific tasks that are not performed through the Prism Element web console, see [AHV Administration Guide](#) and hypervisor-specific guides.

## Prism Element Web Console Overview

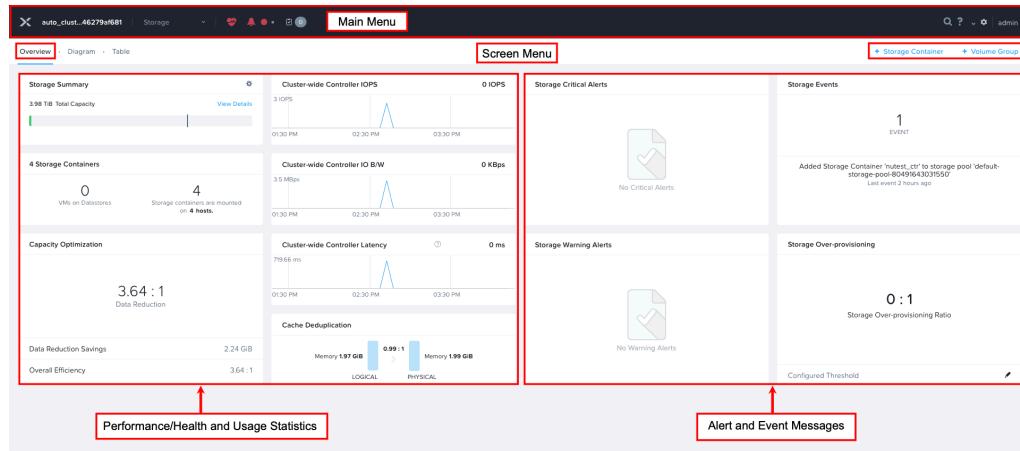
The Prism Element web console, provides a user interface to manage most activities in a Nutanix cluster.

### Display Features

The Prism Element web console screens are divided into the following sections:

- Main menu bar. The main menu bar appears at the top of every screen in the Prism Element web console. The cluster name appears on the far left of the main menu bar. To the right of the cluster name, you can select an entity from the dropdown menu (such as Home, Health, VM, Storage, Network, Hardware, File Server, Data Protection, Analysis, Alerts, Tasks, LCM and Settings) to display information about that entity. You can also search for specific topics or select various tasks from the dropdown menu on the right side of the main menu bar. In addition, the main menu bar includes status icons for quick access to health, alert, and event information. For more information, see [Main Menu](#) on page 56.
- Entity views. There is a dashboard view for each entity. Some entities (such as VM, Storage, Hardware, and Data Protection) include additional views such as a diagram or table view that you can select from the dashboard of that entity.
- Screen menu bar. Some entity dashboards include another menu bar below the main menu that provides options specific to that screen. In the following example from the **Storage** dashboard, three view tabs (**Overview**, **Diagram**, and **Table**) and three task buttons (**+ Storage Container**, **+ Volume Group**, and **+ Storage Pool**) appear on this menu bar.
- Usage and performance/health statistics. Most views include fields that provide usage and either performance or health (or both) statistics. The usage and performance/health statistics vary based on the entity that you are viewing. For example, virtual machine usage statistics are displayed in terms of CPU and memory, while disk usage statistics show disk capacity in TB. In most cases, performance statistics are displayed in IOPS, latency, and bandwidth.
- Alert and event messages. Several views include fields that list current event and alert messages. The listed messages are context specific, so for example only storage-related alerts and events appear on the Storage

screen. Clicking on a message opens the alert or event view at that message. For more information, see [Alerts Dashboard](#) in *Prism Element Alerts and Events Reference Guide*.



**Figure 19: Overview Screen Sections**

## Logging Into the Prism Element Web Console

### About this task

To log into the Prism Element web console, do the following.

For information about default cluster credentials, see [KB 1661](#)

### Procedure

1. Open a web browser.

**Note:**

Prism Element web console supports the latest version, and the two preceding major versions of Firefox, Chrome, Safari, and Microsoft Edge browsers.

2. Enter the cluster virtual IP address (if configured) or the IP address of any Nutanix Controller VM in the cluster.

**Note:** If you are logging into Prism Central, enter the Prism Central VM IP address.

The browser redirects to the encrypted port (9440) and might display an SSL certificate warning. Acknowledge the warning and proceed to the site. If user authentication is enabled and the browser does not have the correct certificate, a denied access message might appear. For more information, see [Configuring Authentication](#).

3. If a welcome screen appears, read the message, and then click the *Accept terms and conditions* bar at the bottom. For more information on the welcome screen, see [Configuring a Banner Page](#) on page 361.
4. In the login screen, enter your Nutanix login credentials and press **Enter** or click the right arrow icon.

**Note:**

- If you are using LDAP authentication, enter the user name in the `samAccountName@domain` format; the `domain\user` format is not supported. (Authentication does not use the user principle)

name [UPN]; *user@domain* is simply a concatenation of the user and domain names specified in [Configuring Authentication](#).)

- The login page includes background animation that is enabled by default. Click the **Freeze space time continuum!** link at the bottom right of the login screen to disable the animation (or the **Engage the warp drive!** link to enable the animation). For information on how to permanently disable (or enable) the animation, see [Modifying UI Settings](#) on page 70.

5. If you are logging in as an administrator (admin user name and password) for the first time, which requires that the default password (Nutanix/4u) be changed, enter a new password in the **password** and **re-type password** fields and then press **Enter** or click the right arrow icon.

The password must meet the following complexity requirements:

- At least 8 characters long
- At least 1 lowercase letter
- At least 1 uppercase letter
- At least 1 number
- At least 1 special character (allowed special characters are: "#\$%&()'\*+,.-/:;<=>@[]^\_`{|}~! )
- At least 4 characters different from the old password
- Must not be among the last 5 passwords
- Must not have more than 2 consecutive occurrences of a character
- Must not be longer than 199 characters

After you have successfully changed the password, the new password is synchronized across all Controller VMs and interfaces (Prism Element web console, nCLI, and SSH).

**Note:**

- You are prompted to change the password when logging in as the **admin** user for the first time after upgrading AOS. If the first login after upgrade is to the Controller VM through SSH (instead of Prism), you must log in using the default **admin** user password (Nutanix/4u) and then change the password when prompted.
- The default password expiration age for the **admin** user is 60 days. You can configure the minimum and maximum password expiration days based on your security requirement.
  - `nutanix@cvm$ sudo chage -M <MAX-DAYS> admin`
  - `nutanix@cvm$ sudo chage -m <MIN-DAYS> admin`
- When you change the **admin** user password, update any applications and scripts using the **admin** user credentials for authentication. Nutanix recommends that you create a user assigned with the **admin** role instead of using the **admin** user for authentication.

6. If a license agreement screen appears (typically on the first login or if the EULA changed since the last login), which indicates the current EULA has not been acknowledged yet, do the following:
  - a. Read the license agreement (on the left).
  - b. Enter appropriate information in the **Name**, **Company**, and **Job Title** fields (on the right).
  - c. Select the *I have read and agree to the terms and conditions* checkbox.
  - d. Click the **Accept** button.
7. If a *Pulse will be Enabled* screen appears (typically on the first login or after an upgrade), read the statement and then do one of the following. This screen refers to the Pulse feature that alerts Nutanix customer support regarding the health of the cluster. For more information, see [Pulse Health Monitoring](#) on page 381.
  - » Click **Continue** to enable the Pulse feature (recommended).
  - » Click **Disable Pulse (not recommended)** to disable the Pulse feature.

**Caution:** If Pulse is not enabled, alerting Nutanix customer support when problems occur is disabled.

Pulse provides Nutanix customer support with analytic information that allows them to dynamically monitor your cluster and identify potential issues before they become problems. For more information, see [Remote Diagnostics](#) on page 382. Enabling Pulse is recommended unless providing cluster information to Nutanix customer support violates your security policy.

8. If a screen about enhanced cluster health monitoring appears (typically either after enabling Pulse in the previous step or after upgrading a cluster), read the statement and then do one of the following:
  - » Click the **Yes (recommended)** button to enable enhanced cluster health monitoring.
  - » Click the **Not Now** button to disable this feature.

The enhanced (on top of standard Pulse) cluster health monitoring provides Nutanix customer support with more detailed (but more transparent) information that allows them to better monitor the health of your cluster. Enhanced cluster health monitoring is recommended unless providing information such as entity names violates your security policy.
9. [2-node clusters only] If a screen about registering with a Witness appears, see [Witness Option](#) in the *Data Protection and Recovery with Prism Element* guide.

## Logging Out of the Prism Element Web Console

### Procedure

1. Click the user menu that appears on the far right side of the Prism Element web console.
2. From the dropdown menu that appears, select **Sign Out**.  
The system logs you out immediately after selecting the option (no prompt or message).

## Main Menu

The main menu at the top of every screen provides access to all the features of the Prism Element web console. This section describes each of the main menu options.

### Cluster Information

The cluster name appears on the far left side of the main menu bar. Clicking the cluster name opens the **Cluster Details** window. This window displays cluster UUID, cluster ID, cluster incarnation ID, cluster subnet gateway IP address, cluster name, cluster virtual IP address (if set), iSCSI data services IP address (if set), and the cluster

encryption state. You can modify the name, FQDN, virtual IP address or iSCSI data services IP address. For more information, see [Modifying Cluster Details](#) on page 73.

## View Options

Selecting a view (entity name) from the dropdown menu on the left displays information about that entity. Select from the following options:

- **Home:** Displays the main dashboard (see [Home Dashboard](#)).
- **Health:** Displays the health dashboard (see [Health Dashboard](#) on page 252).
- **VM:** Displays a virtual machine information dashboard (see [VM Dashboard](#)).
- **Storage:** Displays a storage information dashboard (see [Storage Dashboard](#) on page 117).
- **Network** (AHV only): Displays the network visualiser.
- **Hardware:** Displays a hardware information dashboard (see [Hardware Dashboard](#) on page 182).
- **File Server:** Displays a file server dashboard (see [Nutanix Files Guide](#)).
- **Data Protection:** Displays a data protection information dashboard (see [Data Protection Dashboard](#)).
- **Analysis:** Displays a screen to create and run performance monitors (see [Analysis Dashboard](#) on page 330).
- **Alerts:** Displays a screen of alert and events messages (see [Alerts Dashboard](#) in *Prism Element Alerts and Events Reference Guide*).
- **Tasks:** Displays a screen of task messages (see [View Task Status](#) on page 87).
- **LCM:** Displays the life cycle manager (LCM) dashboard (see [Life Cycle Management \(LCM\)](#) on page 78).
- **Settings:** Displays the Settings menu, as does clicking the gear icon on the right of the main menu (see [Settings Menu](#) on page 59).

**Note:** These views reflect that Prism Element retains alerts and events, and raw metric values for 90 days.

## Informational and Search Features

There are multiple ways to access information from the main menu:

- A health (heart) icon appears on the left side of the main menu. It can be green (healthy), yellow (warning), or red (unhealthy) indicating the current health status. Clicking the icon displays the health details view. For more information, see [Health Dashboard](#) on page 252.
- An alerts (bell) icon appears on the left side of the main menu when critical (red), warning (yellow), or informational (gray) alert messages have been generated and have not been marked as resolved. The number of unresolved alerts is displayed in the icon. Click the icon to display a dropdown list of the most recent unresolved alerts. Click an alert or the right arrow link to open the alerts view. For more information, see [Alerts Dashboard](#) in *Prism Element Alerts and Events Reference Guide*.
- A tasks (circle) icon appears to the right of the alerts icon. The number of active tasks (running or completed within the last 48 hours) is displayed in the icon. Click the icon to display a dropdown list of the active tasks, and then click the **View All Tasks** button to open the tasks view. For more information, see [View Task Status](#) on page 87.
- A search (magnifying glass) icon appears on the right side of the main menu. Click this icon to display a search field. You can search for information about entities or actions by entering a string in this field. For example, you can enter an action name such as add that returns a list of add actions or an entity name such as MyVM that returns a list of links related to that entity.

## Help Menu

A question mark icon appears on the right side of the main menu. Clicking the question mark displays a list of help resource options that you can select. The following table describes each option in the dropdown menu.

**Table 16: Help Menu Options**

Name	Description
Help with this page	Opens the online help page that describes the specific screen from which you accessed this option. For more information, see <a href="#">Accessing Online Help</a> on page 396.
Health Tutorial	Opens the Health dashboard tutorial that takes you through a guided tour of the health analysis features. For more information, see <a href="#">Health Dashboard</a> on page 252.
General Help	Opens the online help at the introduction page.
Online Documentation	Opens the online help at the introductory page, providing an overview and essential information to help you get started.
Support Portal	Opens a new browser tab or window, directing you to the Nutanix support portal login page. For more information, see <a href="#">Accessing the Nutanix Support Portal</a> on page 392.
Nutanix Next Community	Opens a new browser tab or window, directing you to the Nutanix Next Community entry page. This is an online community site for customers and partners to exchange ideas, tips, and information about Nutanix technologies and related datacenter topics. For more information, see <a href="#">Accessing the Nutanix Next Community</a> on page 397.

## User Menu

A user icon appears on the far right side of the main menu with the current user login name. Clicking the user icon displays a dropdown menu of options described in the following table:

**Table 17: User Menu Options**

Name	Description
Update Profile	Opens the <b>Update Profile</b> window to update your user name and email address. For more information, see <a href="#">Updating My Account</a> .
Change Password	Opens the <b>Change Password</b> window to update your password. For more information, see <a href="#">Updating My Account</a> .
REST API Explorer	Opens a new browser tab or window, directing you to the Nutanix REST API Explorer web page. For more information, see <a href="#">Accessing the REST API Explorer</a> on page 394.
Download nCLI	Downloads the Nutanix command line interface (nCLI) as a zip file to your local system. The download occurs immediately after clicking this option. For more information about installing the nCLI locally and for nCLI command descriptions, see <a href="#">Nutanix Command Reference</a> .

Name	Description
Download Cmdlets Installer	Downloads the PowerShell installer for the Nutanix cmdlets. For more information about the cmdlets, see <a href="#">PowerShell Cmdlets Reference</a> .
Download Prism Central	Opens a new browser tab or window, directing you to the <b>Support Tools</b> page of the Nutanix support portal from which you can download the files to install Prism Central. If a login page appears, enter your Nutanix support portal credentials to access the portal. For more information, see <a href="#">Prism Central Infrastructure Guide</a> .
About Nutanix	Opens a window that displays the Nutanix AOS version, NCC version, and LCM version. It also includes a link to Nutanix patent information, and EULA. For more information, see <a href="#">Finding the AOS Version Using Prism Element</a> on page 72.
Nothing To Do?	Opens a game that is strictly for entertainment. To quit the game, click the X at the upper right of the screen.
Sign Out	Logs out the user from the Prism Element web console. For more information, see <a href="#">Logging Out of the Prism Element Web Console</a> on page 56.

## Settings Menu

The Prism Element web console includes a Settings page from which you can configure multiple system services.

You can access the **Settings** page by doing either of the following:

- Click the gear icon on the right of the main menu.  
For more information, see [Main Menu](#) on page 56.
- Select **Settings** from the dropdown list on the left of the main menu.

The **Settings** page displays a menu of tasks (on the left) you can perform. Click the task to open the window or page for that option in the pane to the right. The following table describes each menu option.

**Table 18: Settings Menu List**

Name	Description
General	
Cluster Details	Opens the <b>Cluster Details</b> window to view or modify certain cluster parameters. For more information, see <a href="#">Modifying Cluster Details</a> on page 73.
Configure CVM	Opens the <b>Configure CVM</b> window to increase the Controller VM memory size. For more information, see <a href="#">Increasing the Controller VM Memory Size</a> on page 100.
Convert Cluster	Opens the <b>Convert Cluster</b> window to convert the cluster from ESXi to AHV and then from AHV to ESXi. For more information, see <a href="#">In-Place Hypervisor Conversion</a> on page 365.
Expand Cluster	Opens the <b>Expand Cluster</b> window to add new nodes to the cluster . For more information, see <a href="#">Expanding a Cluster</a> on page 198.

Name	Description
Image Configuration [AHV only]	Opens the <b>Image Configuration</b> window to import and manage image files that can be used to create VMs. For more information, see <a href="#">Configuring Images</a> on page 292.
Licensing	Opens the <b>Licensing</b> window to install or update the cluster license that enables entitled Nutanix features. For more information, see <a href="#">Prism Licensing</a> on page 73.
Reboot [AHV]	Opens the <b>Request Reboot</b> window to gracefully restart the nodes in the cluster one after the other. You can select the nodes you want to restart. For more information, see <a href="#">Rebooting an AHV or ESXi Node in a Nutanix Cluster</a> on page 101.
Remote Support	Opens the <b>Remote Support Services</b> window, which enables (or disables) Nutanix remote support access. For more information, see <a href="#">Controlling Remote Connections</a> on page 390.
Upgrade Software	Opens the <b>Upgrade Software</b> window to upgrade the cluster to a newer AOS version, or update other upgradeable components. For more information, see <a href="#">Software and Firmware Upgrades</a> on page 77.
vCenter Registration [ESXi only]	Opens the <b>vCenter Registration</b> window to register (or unregister) the cluster with the vCenter instance. For more information, see <a href="#">Registering a Cluster to vCenter Server using Prism Element</a> on page 362.
Setup	
Connect to Citrix Cloud [AHV and XenServer only]	Opens the <b>Connect to Citrix Cloud</b> window to connect to the Citrix Workspace Cloud. For more information, see <a href="#">Connect to Citrix Cloud</a> on page 326.
Prism Central Registration	Opens the <b>Prism Central Registration</b> window to add the cluster into a central registration for multicluster connection and support. For more information, see <a href="#">Registering or Unregistering a Cluster with Prism Central</a> in <i>Prism Central Infrastructure Guide</i> .
Pulse	Opens the <b>Pulse</b> window to enable the sending of cluster information to Nutanix customer support for analysis. For more information, see <a href="#">Pulse Configuration</a> on page 383.
Rack Configuration	Opens the <b>Rack Configuration</b> page to configure the fault tolerant domain for node, block, and rack awareness. For more information, see <a href="#">Rack Fault Tolerance</a> on page 35.
Network	
HTTP Proxy	Opens the <b>HTTP Proxy</b> window to configure an HTTP proxy to which the Nutanix software can connect. For more information, see <a href="#">Configuring HTTP Proxy</a> on page 391.
Name Servers	Opens the <b>Name Servers</b> window to configure name servers for the cluster. For more information, see <a href="#">Configuring Name Servers</a> on page 349.
Network Configuration [AHV only]	Opens the <b>Network Configuration</b> window to configure network connections for the cluster. For more information, see <a href="#">Network Configuration for VM Interfaces</a> on page 162.

Name	Description
Network Switch	Opens the <b>Network Switch Configuration</b> window to configure network switch information needed for collecting network traffic statistics. For more information, see <a href="#">Configuring a Network Switch</a> on page 167. This option does not appear when running a hypervisor that does not support this feature.
NTP Servers	Opens the <b>NTP Servers</b> window to specify which NTP servers to access. For more information, see <a href="#">Configuring NTP Servers</a> on page 350.
SNMP	Opens the <b>SNMP Configuration</b> window to enable and configure SNMP for the cluster. For more information, see <a href="#">Configuring SNMP</a> on page 351.
Security	
Cluster Lockdown	Opens the <b>Cluster Lockdown</b> window, which allows you to delete (or add) public authentication keys used for SSH access into the cluster. Removing all public keys locks down the cluster from external access. For more information, see <a href="#">Controlling Cluster Access</a> .
Data at Rest Encryption [SEDs only]	Opens the <b>Data-at-Rest Encryption</b> screen to configure key management for self encrypting drives (SEDs) and enable data encryption across the cluster. This menu option appears only when the data drives in the cluster are SEDs. For more information, see <a href="#">Data-at-Rest Encryption</a> .
Filesystem Whitelists	Opens the <b>Filesystem Whitelist</b> window to specify whitelist addresses. For more information, see <a href="#">Configuring a Filesystem Whitelist</a> on page 348.
SSL Certificate	Opens the <b>SSL Certificates</b> window to create a self-signed certificate. For more information, see <a href="#">Certificate Management</a> .
Users and Roles	
Authentication	Opens the <b>Authentication Configuration</b> window to configure authentication for the cluster. For more information, see <a href="#">Configuring Authentication</a> .
Local User Management	Opens the <b>Local User Management</b> window. This window lists current users and allows you to add, update, and delete user accounts. For more information, see <a href="#">User Management</a> .
Role Mapping	Opens the <b>Role Mapping</b> window to configure role mappings that apply in the user authentication process. For more information, see <a href="#">Configuring Authentication</a> .
Email and Alerts	
Alert Email Configuration	Opens the <b>Alert Email Configuration</b> window, which enables (or disables) the e-mailing of alerts. For more information, see <a href="#">Configuring Alert Emails</a> in <i>Prism Element Alerts and Events Reference Guide</i> .
Alert Policies	Opens the <b>Alert Policies</b> window, which allows you to specify what events should generate an alert and how frequently the system should check for each event type. For more information, see <a href="#">Configuring Alert Policies</a> in <i>Prism Element Alerts and Events Reference Guide</i> .
SMTP Server	Opens the <b>SMTP Server Settings</b> window to configure an SMTP server. For more information, see <a href="#">Configuring an SMTP Server</a> on page 351.

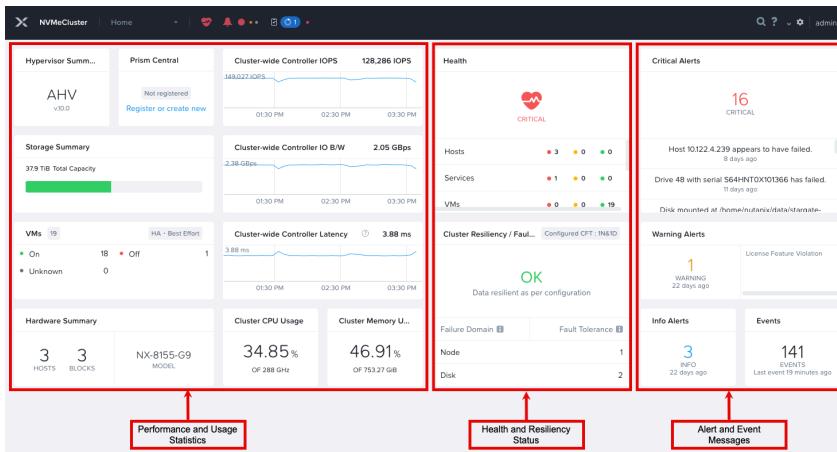
Name	Description
Data Resiliency	
Configure Witness [ESXi and AHV only]	Opens the <b>Configure Witness</b> window to add a witness VM for metro availability and two-node clusters. For more information, see <a href="#">Witness Option in Data Protection and Recovery with Prism Element Guide</a> .
Degraded Node Settings	Opens the <b>Degraded Node Settings</b> window to enable or disable Degraded Node Detection. For more information, see <a href="#">Degraded Node</a> on page 44.
Manage VM High Availability [AHV only]	Opens the <b>Manage VM High Availability</b> window to enable high availability for guest VMs in the cluster. For more information, see <a href="#">Enabling High Availability Reservations for the Cluster</a> on page 301.
Cluster Fault Tolerance	Opens the <b>Cluster Fault Tolerance</b> window to increase the fault tolerance of the cluster. For more information, see <a href="#">Increasing the Cluster Fault Tolerance Level</a> on page 75.
Appearance	
Language Settings	Opens the <b>Languages</b> window, which allows you to select the language of the Prism Element web console. For more information, see <a href="#">Localization (L10n)</a> on page 372.
UI Settings	Opens the <b>UI Settings</b> window to configure Prism UI background themes, disable (or re-enable) the login screen. For more information, see <a href="#">Modifying UI Settings</a> on page 70.
Welcome Banner	Opens the <b>Edit Welcome Banner</b> window to create a welcome banner message that appears before users log in to the Prism Element web console. For more information, see <a href="#">Configuring a Banner Page</a> on page 361.

## Home Dashboard

The Home dashboard is the opening screen that appears after logging into the Prism Element web console. It provides a dynamic summary view of the cluster status. To view the Home dashboard at any time, select **Home** from the dropdown menu on the far left side of the main menu.

### Home Screen Details

The Home dashboard contains widgets that display cluster-level performance and usage statistics on the left, health status information in the middle, and the most recent alert and event messages on the right. The following table describes each field in this screen. Several fields include a slide bar on the right to view additional information in that field. The displayed information is dynamically updated to remain current.



**Figure 20: Home Dashboard**

**Note:** These fields reflect that Prism Element retains alerts and events, and raw metric values for 90 days.

For information about how the statistics are derived, see [Understanding Displayed Statistics](#) on page 69.

**Table 19: Home Screen widgets**

Name	Description
Hypervisor Summary	Displays the name and version number of the hypervisor.
Prism Central	Displays whether you have registered the cluster to a Prism Central instance or not. Click <b>Register</b> to register the cluster to a Prism Central instance. If you have already registered, you can click the IP address of the Prism Central instance to launch the Prism Central instance in a new tab of your browser.
Storage Summary	<p>Displays information about the physical storage space utilization (in GiB or TiB) and resilient capacity of the cluster.</p> <p>Placing the cursor anywhere on the horizontal axis displays a breakdown view of the storage capacity usage.</p> <p>Click <b>View Details</b> to view the resiliency status and storage information of all the individual nodes in the cluster. For more information, see <a href="#">Storage Details Page</a> on page 119.</p> <p>You can also configure a threshold warning for the resilient capacity utilization in the cluster by clicking the gear icon. For more information, see <a href="#">Configuring a Warning Threshold for Resilient Capacity</a> on page 106.</p>
VMs	Displays the total number of VMs in the cluster categorized by their states: on, off, and suspended.
Hardware Summary	Displays the number of hosts and blocks in the cluster, along with one or more Nutanix block model numbers.

Name	Description
Cluster-wide Controller IOPS	Displays I/O operations per second (IOPS) in the cluster. The displayed time period is a rolling interval that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in-depth analysis, you can add this chart to the analysis page by clicking the <b>Add chart to analysis page</b> link in the upper left of the chart. For more information, see <a href="#">Analysis Dashboard</a> on page 330.
Cluster-wide Controller IO B/W	Displays I/O bandwidth used per second in the cluster. Depending on traffic volume, the value is displayed in an appropriate metric (MBps, KBps, and so on). Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in-depth analysis, you can add this chart to the analysis page by clicking the Add chart to analysis page link in the upper left of the chart. For more information, see <a href="#">Analysis Dashboard</a> on page 330.
Cluster-wide Controller Latency	Displays the average I/O latency (in milliseconds) in the cluster.
Cluster CPU Usage	Displays the current CPU utilization percentage along with the total available capacity (in GiB).
Cluster Memory Usage	Displays the total reserved memory, including memory assigned to user VMs, memory provisioned for CVMs, and memory reserved for HA, as a percentage of the total available capacity of the cluster (in GiB).
Health	Displays the health status of the cluster as a whole (good, warning, critical) and a summarized health status of the VMs, hosts, and disks in the cluster. Clicking an entity displays detailed information about that entity in the Health page. For more information, see <a href="#">Health Dashboard</a> on page 252.
Cluster Resiliency/Fault Tolerance Status	Displays the following: <ul style="list-style-type: none"> <li>Current failure domain of the cluster. An arrow indicates the upwards or downwards trend.</li> <li>Current fault tolerance status of the cluster.</li> </ul>
Critical Alerts	Displays the most recent unresolved critical alert messages. Click a message to open the Alert screen of that message. For more information, see <a href="#">Alerts Dashboard</a> in <i>Prism Element Alerts and Events Reference Guide</i> .
Warning Alerts	Displays the most recent unresolved warning alert messages. Click a message to open the Alert screen of that message.
Info Alerts	Displays a summary of informational alerts.
Events	Displays a summary of events.

### Cluster Resiliency/Fault Tolerance Status

The **Cluster Resiliency / Fault Tolerance Status** widget indicates whether the cluster can safely handle a node failure, that is, whether a copy of all data in any node exists somewhere in the cluster. The fault tolerance status of a cluster can have any one of the following states:

- **OK:** This state indicates that the fault tolerance domain is highly resilient and can safely handle a node or disk (in single or two-node clusters) failure.

- **Warning:** This state indicates that the fault tolerance level is almost reaching 0. A warning state is displayed if the cluster is not fault tolerant at the configured domain but is fault tolerant at a lower domain. For example, if you have configured rack as the configured domain and the cluster can no longer handle any rack failures due to some reason but can still handle node (lower domain) failures, then the fault tolerance state is displayed as **Warning**.
- **Critical:** This state indicates that the fault tolerance level is 0, and the fault tolerance domain cannot handle a node or disk (in single or two-node clusters) failure.
- **Computing:** This state indicates that the new fault tolerance level is being calculated.

Clicking anywhere in the widget displays the **Cluster Resiliency / Fault Tolerance Status** dialog box. This dialog box displays more detailed cluster resiliency status information. This window provides information about the number and type of failures the cluster can withstand safely. The **Failures Tolerable** column indicates the number of simultaneous failures of that component type that can be tolerated (0, 1, or 2). When no failure can be tolerated, a message is displayed to highlight the limitation, where there are not enough blocks in the cluster to support a block failure.

**Note:**

- The resiliency status for single-node backup cluster is at the disk level and not at the node level. For more information, see [Single-Node Replication Target Clusters](#) in the *Data Protection and Recovery with Prism Element Guide*.
- When a node goes down, the extent group (egroup) fault tolerance status remains unchanged as the node is assumed (initially) to be unavailable just temporarily. However, Stargate fault tolerance goes down by one until all data has been migrated off that node. The egroup fault tolerance status goes down only when a physical copy of the egroup replica is permanently bad. For more information on Stargate, see [Cluster Components](#) on page 12.

### Rebuild Progress (Cluster Resiliency/Fault Tolerance Status Widget)

You can monitor the data rebuild status of cluster entities like disks and nodes through the **Rebuild Progress** indicator. This rebuild progress bar reflects in the **Cluster Resiliency / Fault Tolerance Status** widget on the Prism Element **Home** page within a maximum duration of 90 seconds when a data rebuild event occurs due to a disk removal (or a node removal which triggers disk removals of the individual disks).

For example, if you mark a disk for removal, it takes a maximum of 90 seconds for its rebuild progress to appear in the **Cluster Resiliency / Fault Tolerance Status** widget.

The main objective of this feature is to provide the admin with information about the ongoing data rebuilds for disks and nodes. Along with the overall ETA and rebuild progress percentage for participating entities, you can also monitor the individual progress of the entities.

#### Data Rebuild Scenarios

You can monitor the data rebuild for the following scenarios.

- You mark a disk for removal.  
A disk is removed in any of the following cases.
  - You manually perform the **Remove Disk** operation.
  - A Stargate process internally encounters that a disk has gone down and marks it for removal.
- You mark a node offline.

The **Cluster Resiliency / Fault Tolerance Status** widget displays the data rebuild progress and ETA as an aggregate of all overlapping rebuilds. If a data rebuild operation intersects other rebuild operations, they are considered to belong to a single rebuild generation. In such a scenario, the Prism Element web console displays the

weighted average of the progress percentage of all the entities and maximum time of the ETA for all rebuilds in that generation.

For information on how to monitor the overall data rebuild ETA, overall progress percentage, and detailed progress information for nodes and disks respectively, see the [Monitoring Node Rebuild Progress](#) on page 68 and [Monitoring Disk Rebuild Progress](#) on page 67 sections.

**Note:** **Cluster Resiliency / Fault Tolerance Status** widget displays only a single generation data rebuild at any point in time.

## Rebuild Phases

A data rebuild has the following phases.

- **Rebuilding Data.** Indicates that the data rebuilt progress up to 100% . This includes time to rebuild data and also validate that all data has actually been rebuilt.
- **Data Rebuild Complete.** Indicates the success of the data rebuild operation.
- **Aborted.** Indicates an aborted rebuild operation. The rebuild operation aborts when a node that went offline comes back online.

## Data Rebuilt

The following data rebuilds when a rebuild scenario triggers.

**Note:** The data rebuild percentage does not account for metadata rebuild. For example, if the metadata rebuild is at 10% and the data rebuild is 100%, the **Cluster Resiliency / Fault Tolerance Status** widget displays the rebuild percentage as 100%. The metadata rebuild progress currently appears on the **Tasks** page of the Prism Element web console.

- Extent store data
  - Extent groups on victim disk.
- Oplog episodes
  - Unflushed oplog episodes on the victim disk.
- Near Sync LWS episodes.

**Note:** The progress percentage of the extent store data rebuild restricts to 95% until the rebuild completes for oplog and NearSync LWS episodes

## Keyboard Shortcuts in Prism Element Web Console

You can use the following keyboard shortcuts to invoke important menu options or views in Prism Element web console:

**Table 20: Keyboard Shortcuts for Prism Element web console**

Shortcut Key	Menu Option/View
m	Main Menu
s	Settings Menu
f or /	Spotlight (search bar)
u	User Menu

Shortcut Key	Menu Option/View
a	Alerts menu
h	Help menu (? menu)
p	Recent tasks

You can use the arrow keys to select a particular menu option.

If you are on a page with sub pages (such as Storage Dashboard), you can use the following keyboard shortcuts to navigate through the various view:

**Table 21: Keyboard Shortcuts for a dashboard**

Shortcut Key	Menu Option/View
o	Overview View
d	Diagram View
t	Table View

## Monitoring Disk Rebuild Progress

The Prism Element web console allows you to monitor the data rebuild progress and overall rebuild completion ETA for a disk.

### About this task

Curator periodically sends the data rebuild information to Insights. Prism Element queries this data rebuild information from the Insights database. The rebuild progress bar for the disk reflects in the **Cluster Resiliency / Fault Tolerance Status** widget within a maximum duration of 90 seconds. To monitor the data rebuild progress and overall rebuild completion ETA for a disk, follow these steps:

### Procedure

1. Log in to Prism Element web console.
2. Go to **Home > Cluster Resiliency / Fault Tolerance Status** widget.
3. Monitor the **Rebuild Progress** progress bar to view the rebuild completion percentage.
4. Hover over the (?) symbol to view the rebuild completion ETA for the current generation.

- To view the following rebuild metrics for the individual entities, click anywhere on the **Rebuild Progress** field.

The system opens the **Rebuild Progress Details** dialog box displaying the following rebuild metrics.

- Disk ID:** Displays the disk identification number (ID number).
- Serial No:** Displays the disk serial number (serial number).
- Slot No:** Displays the slot number associated with the disk (slot number).
- Node:** Displays the node name.
- Type:** Displays the disk type (tier name). The Nutanix platform can contain disk tiers for PCIe solid state disks (SSD-PCIe), SATA solid-state disks (SSD-SATA), and direct attach SATA hard disk drives (DAS-SATA) depending on the platform type [SSD-PCIe | SSDSATA | DAS-SATA].
- Rebuild Phase:** Displays the current data rebuild status. For information about the data rebuild phases, see [Home Dashboard](#) on page 62.
- Rebuild Progress:** Displays the rebuild progress percentage.
- Elapsed Time:** Displays the time elapsed since the data rebuild operation started.
- Estimated Time:** Displays the estimated time for the data rebuild operation to complete.

You can verify the rebuild event status through the **Tasks** option.

## Monitoring Node Rebuild Progress

The Prism Element web console allows you to monitor the data rebuild progress and overall rebuild completion ETA for a node.

### About this task

Curator periodically sends the data rebuild information to Insights. Prism Element queries this data rebuild trigger from the Insights DB. The rebuild progress bar for the node reflects in the **Cluster Resiliency / Fault Tolerance Status** widget within a maximum duration of 90 seconds. To monitor the data rebuild progress and overall rebuild completion ETA for a node, follow these steps:

**Note:** The offline node progress appears only if the Stargate health is down.

### Procedure

- Log in to Prism Element web console.
- Go to **Home > Cluster Resiliency / Fault Tolerance Status** widget.
- Monitor the **Rebuild Progress** progress bar to view the rebuild completion percentage.
- Hover on the (?) symbol to view the rebuild completion ETA for the current generation.

- Click anywhere on the **Rebuild Progress** field to view the following rebuild metrics for the individual entities. The system opens the **Rebuild Progress Details** dialog box displaying the following rebuild metrics.

- Node.** Displays the node name.
- Rebuild Phase.** Displays the current data rebuild status. For information about the data rebuild phases, see [Home Dashboard](#) on page 62.
- Rebuild Progress.** Displays the rebuild progress percentage.
- Elapsed Time.** Displays the time elapsed since the data rebuild operation started.
- Estimated Time.** Displays the estimated time for the data rebuild operation to complete.

You can verify the rebuild event status through the **Tasks** option.

## Understanding Displayed Statistics

The Prism Element web console and Prism Central web console display various statistics that are derived from the following sources:

**Note:** Most displayed statistics appear in 30 second intervals. The values in the tables represent the most recent data point within the last 30 seconds. Prism Central collects the statistical data from each registered cluster, so the process of collecting that data could result in a longer lag time for some statistics displayed in Prism Central.

- Hypervisor:* Hypervisor provides usage statistics only. The support to provide usage statistics is available only in ESXi, and not in Hyper-V and AHV hypervisors. If the cluster consists of Hyper-V or AHV hypervisor, the controller provides the usage statistics.

**Note:** Ensure that you consider the usage statistics reported from ESXi hypervisor in both Prism Central and Prism Element, only when it matches with the usage statistics in vCenter.

- Controller (Stargate):* When hypervisor statistics are unavailable or inappropriate, the Controller VM (CVM) provides the statistics from Stargate. For more information about Stargate, see [Nutanix Bible](#). The Controller-reported statistics might differ from those reported by the hypervisor for the following reasons:

- An NFS client might break up large I/O requests into smaller I/O units before issuing them to the NFS server, thus increasing the number of operations reported by the controller.
- The hypervisor might read I/O operations from the cache in the hypervisor which are not counted by the controller.

- Disk (Stargate):* Stargate can provide statistics from both controller and disk perspective. The controller perspective includes reading both I/O operations from memory and disk I/O operations, but the disk perspective includes only disk I/O operations.

**Note:** The difference in statistics derived from the sources: Hypervisor, Controller, and Disk, only applies to storage-related statistics such as IOPS, latency, and bandwidth.

The following field naming conventions are used in Prism Central to identify the information source:

- A field name with **Controller** word indicates the statistic is derived from the controller (for example *Controller IOPS*).
- A field name with **Disk** word indicates the statistic is derived from the disk (for example *Disk IOPS*).
- A field name without **Controller** or **Disk** word indicates the statistic is derived from the hypervisor. For example **IOPS**.

For VM statistics in a mixed ESXi/AHV cluster, the statistics source depends on the type of hypervisor that hosts the VM. If the Hypervisor is:

- ESXi - The hypervisor is the source for statistics.
- AHV - The controller is the source for statistics.

**Note:**

- The overview, VM, and storage statistics are derived from either the hypervisor or controller.
- Hardware statistics are derived from disk.
- Metrics in the analysis page are derived from any of the sources: hypervisor, controller, or disk, based on the type of metric.

The following table provides the information about the source for various statistics based on hypervisor type:

**Table 22: Source for Displayed Statistics**

Hypervisor Type	Statistics	Source	Analysis
ESXi	Overview, VM, and Storage	Both Hypervisor and controller	Metric dependent
	Hardware	Disk	<i>Controller for some storage statistics only</i>
Hyper-V	Overview, VM, and Storage	Controller	
	Hardware	Disk	
AHV	Overview, VM, and Storage	Controller	
	Hardware	Disk	
Citrix Hypervisor	Overview, VM, and Storage	Controller	
	Hardware	Disk	
Mixed (ESXi + AHV)	Overview, VM, and Storage	Hypervisor	
	Hardware	Disk	

## Modifying UI Settings

### About this task

By default, the logon page includes background animation, and Prism logs out the users automatically after the users have been idle for 15 minutes. You can disable the background animation, change the session timeout for users, and configure an override to the session timeout.

### Procedure

1. Log in to Prism Element web console.

- Click the gear icon in the main menu and then select **UI Settings** under **Appearance** in the **Settings** page. The **UI Settings** dialog box appears.
- To set different variations of the Prism UI background themes, select any of the following options from the **Prism Themes** drop-down menu. The UI changes cosmetically to reflect the selection.

**Important:**

- The Prism themes feature is currently in technical preview. You may encounter visual anomalies in few settings/views where the prism themes are not applied. For example, Licensing Settings. Nutanix recommends that you register a case on the support portal to report any anomalies
- You are required to save your selection and refresh any open Prism tabs after changing a background theme.
- The Prism themes setting is not a universal feature between Prism Central and Prism Element web console. The background themes need to be configured in Prism Central and Prism Element web console respectively.

- Select **Light Theme** for light background with high contrast view. This is the default Prism background theme.
  - Select **Dark Theme** for dark background with high contrast view. A pop-up appears prompting you to click **Continue** to proceed.
  - Select **Auto (OS defined)** to apply background themes defined in the OS. A pop-up appears prompting you to click **Continue** to proceed. For example, if you have defined **Dark** mode in the OS setting, the Prism UI honors the setting and sets a dark background theme.
- To disable the logon page background animation, clear the **Enable animated background particles** checkbox (or select it to enable).

Clearing the **Enable animated background particles** checkbox in the Prism **UI Settings** dialog box disables the creation or drawing of particles entirely. This action stops the drawing of the particles on the Prism Element logon page.

**Note:** This setting is not persistent. In other words, if the Prism service restarts, this setting is lost and must be disabled again.

Disabling the particles allows you to conserve critical CPU resources that are used in creating and maintaining the particles.

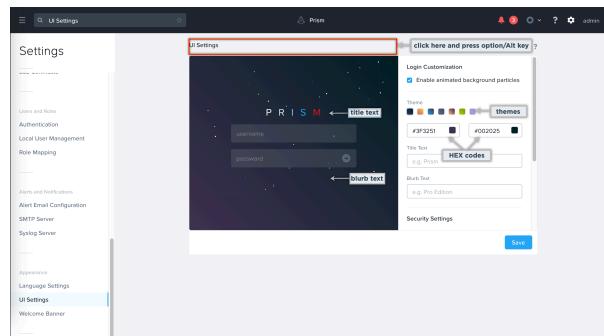
**Note:** Disabling or enabling this setting in Prism Element web console does not propagate to Prism Central or vice versa. The setting must be disabled in Prism Element web console and Prism Central UI separately.

You can disable the particle animation from the logon page by clicking **Freeze space-time continuum!** at the right bottom of the logon page. This action stores a setting in the local browser to stop the animation. However, this action does not stop creation or drawing of the particles itself.

**Note:** You can enable the particle animation by clicking **Engage the warp drive!**.

5. To customize the theme, background color, title text, or blurb text on the logon page, do the following:

- Click **UI Settings** dialog box and simultaneously press the option key on the MAC system or Alt key on the Windows system. Options for customizing the theme, title text, and blurb text are displayed.
- Select the theme from the options displayed for **Theme**. You can change the HEX codes to create your own custom gradient background color for the logon page.
- In the **Title Text** field, enter the text to create your custom title.
- In the **Blurb Text** field, enter the text to create your custom blurb text. This text is displayed below the password field.



**Figure 21: UI Settings Window for customizing the theme, title text, and blurb text**

6. To configure session timeout, do the following under **Security Settings**:

- Select the session timeout for the current user from the **Session Timeout For Current User** drop-down list.
- Select the default session timeout for all users (except an administrator) from the **DEFAULT SESSION TIMEOUT FOR NON-ADMIN USERS** drop-down list.
- Select the appropriate option from the **SESSION TIMEOUT OVERRIDE FOR NON-ADMIN USERS** drop-down list to override the session timeout.

**Note:** The timeout interval for an administrator cannot be set for longer than 1 hour.

7. Clear the **Disable 2048 game** checkbox to disable the 2048 game.

8. Click **Save** to save your changes.

## Finding the AHV Version on Prism Element

You can view the installed AHV version in the Prism Element web console.

### About this task

To view the AHV version installed on the host, follow these steps:

### Procedure

Log in to Prism Element web console.

The **Hypervisor Summary widget** widget on the top left side of the **Home** page displays the AHV version.

## Finding the AOS Version Using Prism Element

To view the Nutanix AOS version running in the cluster, follow these steps:

## Procedure

1. Log in to the Prism Element web console.
2. Click the user menu that appears on the far right side of the Prism Element web console.
3. From the dropdown menu that appears, select **About Nutanix** option.

The **About Nutanix** window displays the AOS version along with the Nutanix cluster check (NCC) and Life Cycle Manager (LCM) version numbers. It also includes a link to Nutanix patent information.

4. Click the **Close** button to close the window.

## Prism Licensing

Nutanix provides licenses you can apply to enable a variety of features.

The Prism Element web console and Nutanix Support Portal provide the most current information on your licenses. For more information on licenses, see the [License Manager Guide](#).

## Modifying Cluster Details

### About this task

You can add or modify cluster parameters such as cluster name, virtual IP address, and data services IP address through the **Settings** menu.

### Procedure

1. Log in to Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Settings**.  
The system displays the **Global Settings** page.
3. From the **General** section in the left navigation pane, click **Cluster Details**.  
It displays read-only fields for the Cluster UUID (universally unique identifier), Cluster ID, Cluster Incarnation ID, Cluster Subnet, and encryption status values. It also contains editable fields for cluster name, FQDN, virtual IP configuration, and iSCSI data services IP address.

**Note:** The cluster ID remains the same for the life of the cluster, but the incarnation ID is reset (typically to the wall time) each time the cluster is re-initialized.

4. In the **Cluster Name** field, enter (or update) a name for the cluster.  
The default name is simply Unnamed. Providing a custom name is optional but recommended.
5. In the **FQDN** field, enter the fully qualified domain name (FQDN) for the cluster.  
Ensure that you are logged on with SuperAdmin or Prism Admin role privileges to configure the domain name in the DNS server, enabling the DNS server to route the traffic between the domain name and the external IP addresses of the CVMs.
6. In the **Virtual IP** field, enter an IP address to be used as the virtual IP address for the cluster.  
A Controller VM runs on each node and has its own IP address. The Virtual IP address field sets a logical IP address that is always attached to the leader Controller VM in the cluster. The virtual IP address configuration removes the need to enter the IP address of a Controller VM in a cluster to log into the cluster. The virtual IP

address is normally set during the initial cluster configuration, but you can update the IP address at any time in this field. For more information, see [Field Installation Guide](#).

**Caution:** Changing the cluster virtual IP address impacts all the features that use the virtual IP address. For more information, see [Virtual IP Address Impact](#) on page 74.

**Note:** Configuring a virtual IP or a domain name is optional, but setting up both enhances addressing flexibility.

7. In the **Virtual IPv6** field, enter an IPv6 address to be used as a virtual IPv6 address for the cluster.

A Controller VM runs on each node and has its own IPv6 address. The Virtual IPv6 address field sets a logical IPv6 address that is always attached to the leader Controller VM in the cluster. The virtual IPv6 address configuration removes the need to enter the IPv6 address of a Controller VM in a cluster to log into the cluster. The virtual IPv6 address is normally set during the initial cluster configuration, but you can update the IPv6 address at any time in this field. For more information, see [Field Installation Guide](#).

8. In the **iSCSI Data Services IP Address** field, enter (or update) an IP address to be used with Nutanix Volumes and other data services applications.

**Caution:** For features, changing the external data services IP address can result in unavailable storage or other issues. The features in question include Volumes, Calm, Leap, Karbon, Objects, and Files. For more information, see [KB 8216](#) and [iSCSI Data Services IP Address Impact](#) on page 75.

9. Perform one of the following:

- a. To enable the Recycle Bin feature in the cluster, select the **Retain Deleted VMs for 24h** checkbox.

If you enable the Recycle Bin and then delete a guest VM or volume group vDisk, it retains its contents (deleted vDisks and configuration information) for up to 24 hours, unless the cluster free storage space reaches critical thresholds.

- b. To disable the Recycle Bin feature in the cluster, clear the **Retain Deleted VMs for 24h** checkbox.

When you disable the Recycle Bin, AOS automatically deletes any entities in the Recycle Bin after 24 hours. Any entities you delete after disabling the Recycle Bin are marked for deletion as soon as possible and are not stored in the storage container Recycle Bin folder. For more information, see [Recycle Bin](#) on page 146.

10. When the field entries are correct, click the **Save** button to save the values and close the window.

## Virtual IP Address Impact

Any Nutanix feature that uses the virtual IP address might be adversely affected if you change the virtual IP address of the cluster. Following are some of the features and functionalities that might be affected:

- You can no longer manage a Nutanix cluster running Hyper-V through the System Center Virtual Machine Manager (SCVMM).
- Nutanix data protection service might lose connection if you configured the remote site using the virtual IP address of that cluster.
- All the VMs running the NGT (Nutanix Guest Tools) instance will be affected. For information about NGT reconfiguration, see [Reconfiguring NGT](#) on page 318.
- External machines mounting shares from Nutanix might fail if the virtual IP address is used for HA functionality (as recommended).
- Some products such as Nutanix Objects use the virtual IP address for access. Check your product-specific documentation before changing the virtual IP address.

## iSCSI Data Services IP Address Impact

To provide access to cluster storage, Nutanix Volumes uses an iSCSI data services IP address for target discovery, simplifying external iSCSI configuration on clients. This IP address serves as the iSCSI target discovery portal and initial connection point.

Nutanix does not recommend configuring iSCSI client sessions to connect directly to Controller VM IP addresses. The data services address is owned by one Controller VM at a time. If the leader Controller VM becomes unavailable, the address moves to another Controller VM, ensuring that it is always available.

This IP address is also used as a cluster-wide address by clients configured as part of Nutanix Files and other products. This IP address:

- Must be in the same subnet as the cluster Controller VM IP `eth0` network interface addresses
- Helps load balance storage requests
- Enables path optimization in the cluster, preventing bottlenecks
- Eliminates the need for configuring a multipathing service such as Microsoft multipath I/O (MPIO)

Nutanix recommends setting the iSCSI data services IP address only one time for each cluster. However, if required, you can change it through the **Cluster Details** window in the Prism Element web console. For more information, see [Modifying Cluster Details](#) on page 73.

If you change the iSCSI data services IP address, you must perform the following to configure the clients and use the new IP address.

- Log out of or disconnect from existing iSCSI or Nutanix Files sessions.
- Delete the old IP address if necessary.
- Re-discover the new target or reestablish Nutanix Files sessions.

**Caution:** For certain features, changing the external data services IP address can result in unavailable storage or other issues. The features in question include Volumes, Calm, Leap, Karbon, Objects, and Files. For more information, see [KB 8216](#).

## Cluster Fault Tolerance Configuration

This section provides information on how to configure cluster fault tolerance.

You can configure cluster fault tolerance in the following ways:

- When you create a new cluster using Prism Central. For more information, see [Creating a Cluster](#) in the *Prism Central Infrastructure Guide*.
- When you configure a cluster using Foundation. For more information see [Configuring the Foundation GUI Automatically](#) and [Configuring Foundation VM by Using the Foundation GUI](#) in the *Field Installation Guide* or [Run Foundation Central](#) in the *Foundation Central Guide*.
- When you create a new cluster using nCLI. For more information, see [Command Reference Guide](#).

For information on the types of cluster fault tolerance, see [Cluster Fault Tolerance](#) on page 25.

## Increasing the Cluster Fault Tolerance Level

You can increase the fault tolerance of a cluster from 1N/1D to 2N/2D. This topic describes how to increase cluster fault tolerance.

## Before you begin

- Ensure that the cluster has a minimum of five nodes.
- You cannot increase the fault tolerance of a cluster from 1N/1D to 1N&1D. The 1N&1D cluster fault tolerance must be configured when you create the cluster.
- You cannot increase the fault tolerance of a cluster with 1N&1D fault tolerance.
- If you enable block fault tolerance in addition to increasing the cluster fault tolerance you need a minimum of 5 blocks.
- Increasing the cluster fault tolerance might require at least 30 percent of your disk space.
- You cannot revert the changes made to cluster fault tolerance or reduce the cluster fault tolerance. For example, you cannot reduce the cluster fault tolerance from 2N/2D to 1N/1D. If you attempt to reduce cluster fault tolerance, the Prism Element web console displays an error.
- For information on the types of cluster fault tolerance, see [Cluster Fault Tolerance](#) on page 25.

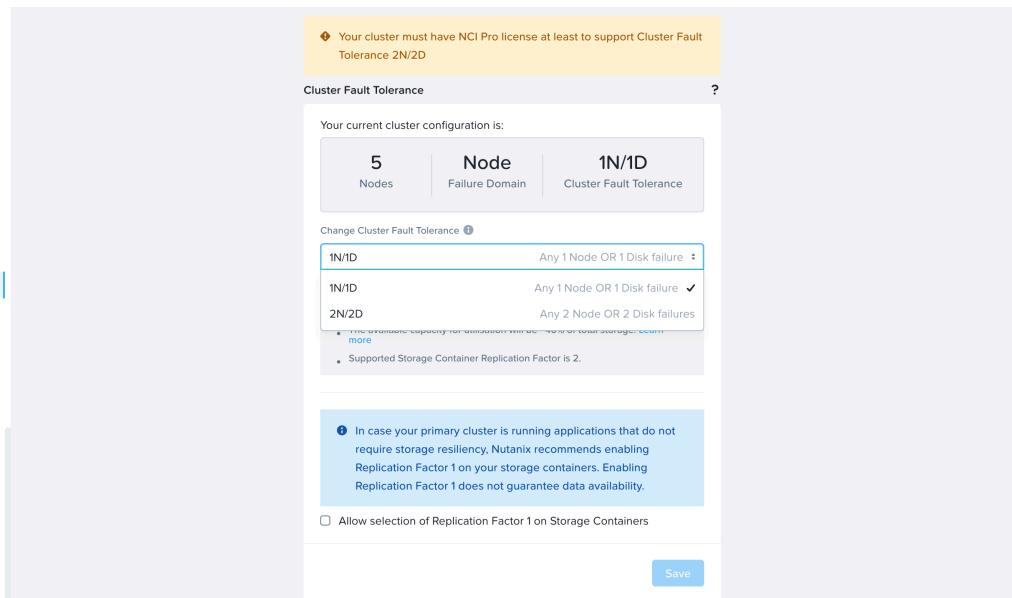
## About this task

To increase the cluster fault tolerance, follow these steps:

**Note:** A cluster with 2N/2D fault tolerance supports replication factor 3.

## Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Settings**.  
The system displays the **Global Settings** page.
3. From the **Data Resiliency** section in the left navigation pane, click **Cluster Fault Tolerance**.  
The system displays the **Cluster Fault Tolerance** page.



**Figure 22: Increasing Cluster Fault Tolerance**

- From the **Change Cluster Fault Tolerance** dropdown menu, select **2N/2D**.

The system increases the fault tolerance to 2N/2D and displays **Configured CFT : 2N/2D** in the **Cluster Resiliency / Fault Tolerance Status** widget in the dashboard of the Prism Element web console.

**Note:** The system might take a few hours to increase the cluster fault tolerance because it must replicate the metadata across the Cassandra ring.

### What to do next

Set the replication factor to 3, manually, for every storage container you want to have three copies of the data.

Increasing the cluster fault tolerance without any increase in the replication factor provides granular control for a container without incurring the overhead of a third copy. However, this also means no container has a third copy of the data until you explicitly increase the replication factor for that container to 3.

For more information, see [Increasing the Replication Factor using CLI](#) on page 137.

## Modifying Cluster Rebuild Preference

You can modify the cluster rebuild preference setting from the Prism Element web console.

### Before you begin

For information on the types of cluster rebuild preferences, see [Cluster Rebuild Preference](#) on page 39.

### About this task

To modify the cluster rebuild preference, follow these steps:

**Note:** By default, the cluster rebuild preference is set as *Smart*.

### Procedure

- Log in to the Prism Element web console.
- From the dropdown menu on the left of the main menu, select **Settings**.  
The system displays the **Global Settings** page.
- From the **Data Resiliency** section in the left navigation pane, click **Maintenance Resiliency**.  
The system displays the **Maintenance Resiliency** page.
- Perform one of the following:
  - Clear the **Smart Rebuild** checkbox to modify the cluster rebuild preference to **Immediate**.
  - If cleared, select the **Smart Rebuild** checkbox to modify the cluster rebuild preference to **Smart**.
- Click **Save**.  
The system updates the cluster rebuild preference based on your choice.

## Software and Firmware Upgrades

You can only upgrade ESXi and Hyper-V hypervisor, Files, and File Server through **Upgrade Software** feature (also known as 1-click upgrade) in the Prism Element web console..

For other firmware and software component upgrades, see [Life Cycle Manager Guide](#).

**Note:** Starting with LCM 2.7, Foundation upgrades are exclusively performed through LCM. The one-click upgrade for Foundation has been disabled; the Foundation tab under **Settings > Upgrade Software** is not present anymore.

## Life Cycle Management (LCM)

The life cycle manager (LCM) tracks software and firmware versions of the various components in a cluster. It allows you to view information about the current inventory and update the versions as needed. To view the LCM dashboard, select **LCM** from the drop-down list on the left of the main menu. For more information, see the [Life Cycle Manager Guide](#).

## Nutanix Cluster Check (NCC)

Before doing any upgrade procedure, run Nutanix Cluster Check from Prism Element and Prism Central.

### Run NCC on Prism Element Clusters

- For Prism Element clusters, run the NCC checks from the **Health** dashboard of the Prism Element web console or by logging on to a Controller VM and running NCC from the command line.

**Note:** In the Prism Element web console, you cannot run NCC checks and collect the logs at the same time.

### Run NCC on Prism Central

For Prism Central clusters, log on to the Prism Central VM through a secure shell session (SSH) and run the NCC checks using the ncc command line. For more information, see *Prism Central Infrastructure Guide*.

## Running NCC (Prism Element)

### About this task

Before doing any upgrade procedure, run Nutanix Cluster Check (NCC) from the Prism Element web console or ncc command line.

### Procedure

To run NCC from the Prism Element web console, follow these steps:

- Log in to the Prism Element web console.
- From the dropdown menu on the left of the main menu, select Health.

The system displays the Health dashboard.

- From the **Actions** dropdown menu, select Run NCC Checks
- Select one of the following options based on the the checks that you want to run for the cluster.

- All checks:** Select this option to run all the checks at once.
- Only Failed and Warning Checks:** Select this option to run only the checks that failed or triggered a warning during the health check runs.
- Specific Checks:** Select this option and type the checks name to run in the text box that appears.

This field gets auto-populated after you start typing the name of the check. The **Added Checks** box lists all the checks that you have selected for this run.

- To receive the report in your email after the cluster check is complete, **Send the cluster check report in the email** checkbox. To receive the report in your email, ensure that you have configured email notification for alerts. For more information, see the *Configuring Alert Emails*in the [Prism Element Alerts Reference Guide](#).

The **Tasks** dashboard displays the status of the check (succeeded or aborted). By default, the system marks all the event-triggered checks as passed. Also, the **Summary** page of the **Health** dashboard updates with the status according to health check runs.

## Run NCC from the Controller VM Command Line

### Procedure

Do these steps to run NCC by using the ncc command.

- a. Log on to a Controller VM.
- b. Run NCC.

```
nutanix@cvm$ ncc health_checks run_all
```

See [Displaying NCC Help](#) on page 79 to display NCC help.

If the check reports a status other than INFO or PASS, resolve the reported issues before proceeding. If you are unable to resolve the issues, contact Nutanix Support for assistance.

### Displaying NCC Help

Get help about NCC from the command line. You can also run the NCC checks from the **Health** dashboard of the Prism Element web console. Click **Actions > Manage Checks**, then select an NCC check. Click the link to the Knowledge Base article for more information about that check.

### Procedure

- Show top-level help about available health check categories.

```
nutanix@cvm$ $ ncc health_checks
```

- Show top-level help about a specific available health check category. For example, hypervisor\_checks.

```
nutanix@cvm$ ncc health_checks hypervisor_checks
```

- Show all NCC flags to set your NCC configuration. Use these flags under the direction of Nutanix Support.

```
nutanix@cvm$ ncc -help
```

## Use 1-Click Upgrade in the Prism Element Web Console

You can upgrade specific software using the **Upgrade Software** feature in the Prism Element web console, also known as the 1-click upgrade.

You can view the available upgrade options, start an upgrade, and monitor upgrade progress from the **Upgrade Software** page in the Prism Element web console.

This page enables you to upgrade the following software when you cannot or choose not to use Life Cycle Manager (LCM).

- File
- File Server
- VMware ESXi or Microsoft Hyper-V hypervisors

**Note:** You must use LCM to upgrade AHV.

### Options for Downloading Updates

**Note:** Ensure that the firewalls allow the ports required for communication to access each other. For information about the ports, see [Ports and Protocols](#).

Nutanix recommends performing most upgrades through Life Cycle Manager (LCM) in the Prism Element web console. If you choose to upgrade individual cluster software components using 1-click upgrade in the Prism Element

web console, follow the recommended upgrade order as described in [Recommended Upgrade Order for Dark Site Method](#) section in *Life Cycle Manager Guide*.

You can choose how to obtain the latest versions of the AOS or other software that Nutanix makes available on the Nutanix Support portals. You might need to download software from hypervisor vendor release web pages.

**Table 23: Software Download Options**

Downloadable Component	On-Demand 1-Click Upgrade	Manual 1-Click Upgrade
<ul style="list-style-type: none"><li>File Server</li><li>File</li></ul>	<ul style="list-style-type: none"><li>On demand: The Prism Element web console regularly checks for new software versions and notifies you through the <b>Upgrade Software</b> page when an update is available. Click <b>Download</b> to retrieve and install the software package.</li></ul>	<ul style="list-style-type: none"><li>The Nutanix Support portal lists File Server binaries, metadata, and checksums when available. You can download these files to your local machine or media and then upload them using 1-click upgrade to upgrade the cluster.</li></ul>
<ul style="list-style-type: none"><li>Hypervisor</li></ul>	<ul style="list-style-type: none"><li>AHV: Upgrade AHV by using the LCM, linked from the <b>Upgrade Software</b> page in the Prism Element web console.</li><li>ESXi: On-demand 1-click upgrade is not supported for ESXi hypervisor.</li><li>Hyper-V: On-demand 1-click upgrade is not supported for Hyper-V hypervisor.</li></ul>	<ul style="list-style-type: none"><li>The Nutanix Support portal lists ESXi and Hyper-V hypervisor binaries, metadata, and checksums when available. You can download these files to your local machine or media and then upload them using 1-click upgrade to upgrade the cluster. Hypervisor vendors such as VMware also provide upgrade packages. For example, you can download the metadata file from the Nutanix Support portal and the hypervisor binary package from the VMware portal and then upload the files using 1-click upgrade to upgrade the cluster. See <a href="#">Upgrading ESXi Hosts by Uploading Binary and Metadata Files</a> on page 82 or <a href="#">Upgrading Hyper-V Hosts by Uploading Binary and Metadata Files</a> on page 86 for more information.</li></ul>

## AOS Upgrade

To upgrade your cluster to AOS 6.8 or later versions, you must use Life Cycle Manager (LCM). However, you must upgrade LCM at your site to the latest version before you upgrade AOS. For more information, see [LCM Updates](#) in the *Life Cycle Manager Guide*.

**Note:** Starting with LCM 3.0, 1-click upgrade for AOS is deprecated.

## ESXi Upgrade

AOS supports upgrading the ESXi hypervisor using the 1-click upgrade feature in the Prism Element web console. You can view the available upgrade options, start an upgrade, and monitor upgrade progress from the Upgrade Software page in the Prism Element web console. For information on how to install or upgrade VMware vCenter server or other third-party software, see your vendor documentation.

## VMware ESXi Hypervisor Upgrade Recommendations and Limitations

This section provides the requirements, recommendations, and limitations to upgrade ESXi.

- To install or upgrade VMware vCenter Server or other VMware software, see VMware documentation.
- Always consult the VMware web site for any vCenter and hypervisor installation dependencies. For example, a hypervisor version might require that you upgrade vCenter first.
- Nutanix recommends that you enable fully automated DRS before upgrading the ESXi host using Life Cycle Manager (LCM) so that VM migrations can be done automatically. If you have not enabled fully automated DRS in your environment and want to upgrade the ESXi host, you must upgrade the ESXi host manually. For information on fully automated DRS, see *Set a Custom Automation Level for a Virtual Machine* in the *VMware vSphere Documentation*. For information on how to upgrade ESXi hosts manually, see [ESXi Host Manual Upgrade](#) in the *vSphere Administration Guide*.
- Ensure that you disable Admission Control before upgrading ESXi on AOS. If you enable Admission Control, the upgrade process fails. However, you can enable it for normal cluster operations.

### Nutanix Support for ESXi Upgrades

Nutanix qualifies specific VMware ESXi hypervisor updates and provides a related JSON metadata upgrade file on the [Nutanix Support Portal](#) for one-click upgrade through the Prism Element web console.

Nutanix does not provide ESXi binary files, only related JSON metadata upgrade files. Obtain ESXi offline bundles (not ISOs) from the VMware website.

Nutanix supports upgrading ESXi hosts with versions that were released after a Nutanix qualified version, but Nutanix might not have qualified those versions. For more information, see the Nutanix hypervisor support statement in our [Support FAQ](#). To upgrade ESXi hosts using VMware updates that do not have a Nutanix-provided JSON metadata upgrade file, obtain the offline bundle and md5sum checksum available from VMware, then upload them using the Prism Element web console. For more information, see [Upgrading ESXi by Uploading An Offline Bundle File and Checksum](#) on page 84.

### Trusted Platform Module (TPM) 2.0 enabled hosts

Before upgrading a Trusted Platform Module (TPM) 2.0 enabled host, in a cluster running ESXi 7.0U2 or later versions, Nutanix recommends that you backup the recovery key created when encrypting the host with TPM. For information on how to generate and backup the recovery key, see [KB 81661](#) in the *VMware documentation*. If the host fails to start after an upgrade, ensure that you use the recovery key to restore the host configuration encrypted by TPM 2.0. For information on how to restore an encrypted host, see [KB 81446](#) in the *VMware documentation*. If the recovery key is unavailable, and if the host fails to start after an upgrade, contact Nutanix Support.

### Mixing nodes with different processor (CPU) types in the same cluster

If you mix nodes with different processor (CPU) types in the same cluster, you must enable VMware enhanced vMotion compatibility (EVC) to allow vMotion/live migration of VMs during the hypervisor upgrade. For example, if your cluster includes a node with a Haswell CPU and other nodes with Broadwell CPUs, open vCenter and enable VMware enhanced vMotion compatibility (EVC) setting and specifically enable EVC for Intel hosts.

## CPU Level for Enhanced vMotion Compatibility (EVC)

Controller VMs and Prism Central VMs require a minimum CPU micro-architecture version of the Intel Sandy Bridge processor. For AOS clusters with ESXi hosts, or when deploying Prism Central VMs on any ESXi cluster: if you have set the vSphere cluster enhanced vMotion compatibility (EVC) level, the minimum level must be **L4 - Sandy Bridge**.

### vCenter Requirements and Limitations

**Note:** You might not be able to log in to vCenter Server if the /storage/seat partition for vCenter Server 7.0 and later versions become full due to an excessive number of SSH-related events. For information on the symptoms and solutions to this issue, see [KB 10830](#).

- If your ESXi cluster is managed by VMware vCenter, you must provide the vCenter administrator credentials and vCenter IP address before upgrading the ESXi hypervisor. Ensure that the ports 80 and 443 are open between the cluster and vCenter instance to successfully upgrade the ESXi hypervisor.
- After you register a cluster in vCenter, wait at least 1 hour before performing any cluster upgrades (AOS, Controller VM memory, hypervisor, and so on) to ensure that the cluster settings are updated. Additionally, do not register the cluster in vCenter and perform any upgrades at the same time.
- 1-click upgrade does not support configurations where a cluster is mapped to multiple vCenters or contains host-affinity rules for VMs.

Ensure that the cluster has sufficient resources to support live migration and to allow hosts to enter maintenance mode.

### Mixing Different Hypervisor Versions

For ESXi hosts, mixing different hypervisor versions in the same cluster is allowed for temporary operations such as deferring a hypervisor upgrade as part of an add-node/expand cluster operation, reimaging a node as part of a break-fix procedure and planned migrations.

## Upgrading ESXi Hosts by Uploading Binary and Metadata Files

### Before you begin

:

- Ensure that your ESXi cluster meets the recommendations mentioned in [VMware ESXi Hypervisor Upgrade Recommendations and Limitations](#).
- Ensure that your ESXi cluster meets the recommendations in the [General Hypervisor Upgrade Recommendations](#) section in *Life Cycle Manager Guide*.
- Ensure that you follow the recommended upgrade order mentioned in the [Recommended Upgrade Order for Dark Site Method](#) section in *Life Cycle Manager Guide*.
- For more information on how to install or upgrade VMware vCenter server or other third-party software, see your vendor documentation.
- Ensure that you are running the latest version of the Nutanix Cluster Check (NCC) health checks and upgrade NCC if necessary.

### About this task

To download Nutanix-qualified ESXi metadata (.JSON) files and upgrade the ESXi hosts using the 1-click upgrade feature in the Prism Element web console, perform the following steps. Nutanix provides only the related JSON metadata upgrade files, not the ESXi binary files.

## Procedure

1. Log in to the Prism Element web console.
2. Run NCC. For more information, see [Running NCC \(Prism Element\)](#) in the *Prism Element Web Console Guide*.
3. Log on to the Nutanix Support Portal. Click the menu icon and go to **Downloads > Hypervisors Support**. The system displays the Hypervisors Support page that lists the metadata files required for all supported third-party hypervisor upgrades.
  - a. From the dropdown menu that lists the supported hypervisor vendors, select **Nutanix - VMware ESXi**. The system displays all the available metadata files for upgrading the ESXi hypervisor.
  - b. From the dropdown menu that lists the supported ESXi versions, select the version you want to upgrade to. The system displays the metadata file required to upgrade to the selected version.
  - c. To download the metadata file to your local machine or media, click **Download**.
4. From the dropdown menu on the left of the main menu, select Settings. The system displays the Global Settings page.
5. From the General section in the left navigation pane, click Upgrade Software. The Upgrade Software page opens.
6. Click the Hypervisor tab.
7. Click the **upload a Hypervisor binary** link.
8. Click **Choose File** in the Hypervisor Metadata File section to select the metadata JSON file obtained from Nutanix. Then, browse to the file location and select the file.
9. Click **Choose File** in the Hypervisor Binary File (.zip file) section to select the binary file (offline bundle zip file for upgrades obtained from VMware). Then, browse to the file location and select the file.
10. Click **Upload Now**.
11. After the file upload is complete, click **Upgrade > Upgrade Now**, then click **Yes** to confirm.  
[Optional] To run the pre-upgrade installation checks only on the Controller VM where you are logged into, without proceeding with the upgrade, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.
12. Enter the IP address and credentials of the vCenter, then click **Upgrade**.  
Ensure that you are using your Active Directory or LDAP credentials in the format domain\username or username@domain.

**Note:** If AOS detects that the uploaded software is already installed or upgraded, the Upgrade option is not displayed.

The **Upgrade Software** dialog box displays the progress of your selection, including the status of pre-installation checks and uploads, through the **Progress Monitor**.

## What to do next

Perform and inventory using LCM to display the software and firmware versions of entities in the cluster. For more information, see the [Performing Inventory with the Life Cycle Manager](#) section in the *Life Cycle Manager Guide*.

## Upgrading ESXi by Uploading An Offline Bundle File and Checksum

### Before you begin

From the VMware website, download the offline bundle (for example, update-from-esxi6.0-6.0\_update02.zip) and copy the associated MD5 checksum. Ensure that this checksum is obtained from the VMware website and not manually generated from the bundle by you. Save the files to your local machine or media, such as a USB drive or other portable media.

### About this task

You can perform this procedure to upgrade an ESXi host in your cluster to a version not yet qualified by Nutanix. While Nutanix supports upgrading ESXi hosts to versions released after a Nutanix-qualified version, these versions might not have been qualified by Nutanix. For more information, see the Nutanix hypervisor support statement in our Support FAQ.

- Typically you perform this procedure to patch your version of ESXi and Nutanix has not yet officially qualified that new patch version. Nutanix supports the ability to patch upgrade ESXi hosts with versions that are greater than or released after the Nutanix qualified version, but Nutanix might not have qualified those releases.
- To download a non-Nutanix-qualified ESXi upgrade offline bundle from VMware and upgrade ESXi using the 1-click upgrade feature in the Prism Element web console, follow these steps:

### Procedure

1. From the VMware web site, download the offline bundle (for example, update-from-esxi6.0-6.0\_update02.zip) and copy the associated MD5 checksum. Ensure that this checksum is obtained from the VMware web site, not manually generated from the bundle by you.
2. Save the files to your local machine or media, such as a USB drive or other portable media.
3. Log in to the Prism Element web console.
4. From the dropdown menu on the left of the main menu, select **Settings**.  
The system displays the **Global Settings** page.
5. From the General section in the left navigation pane, click **Upgrade Software**.  
The **Upgrade Software** page opens.
6. Click the **Hypervisor** tab.
7. Click the **upload a Hypervisor binary** link.
8. Click **enter md5 checksum** and copy the MD5 checksum saved in your local machine or media into the **Hypervisor MD5 Checksum** field.
9. Scroll down and click **Choose File** in the Hypervisor Binary File (.zip file) section to select for the binary file (offline bundle zip file for upgrades obtained from VMware). Then, browse to the offline bundle file location, select the file.
10. Click **Upload Now**.
11. After the file upload is complete, click **Upgrade > Upgrade Now**, then click **Yes** to confirm.  
[Optional] To run the pre-upgrade installation checks only on the Controller VM where you are logged into, without proceeding with the upgrade, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.

12. Enter the vCenter IP address and credentials of the vCenter server, then click **Upgrade**.

Ensure that you are using your Active Directory or LDAP credentials in the format domain\username or username@domain.

**Note:** If AOS detects that the uploaded software is already installed or upgraded, the Upgrade option is not displayed.

The **Upgrade Software** dialog box displays the progress of your selection, including status of pre-installation checks and uploads, through the **Progress Monitor**.

## Hyper-V Upgrade

AOS supports upgrading the Hyper-V hypervisor using the 1-click upgrade feature in the Prism Element web console. You can view the available upgrade options, start an upgrade, and monitor upgrade progress from the **Upgrade Software** page in the Prism Element web console.

## Hyper-V Hypervisor Upgrade Recommendations, Requirements, and Limitations

This section provides the requirements, recommendations, and limitations to upgrade Hyper-V.

### Recommendations

Nutanix recommends that you schedule a sufficiently long maintenance window to upgrade your Hyper-V clusters.

The upgrade duration for a node in a cluster depends on the number of VMs running in the node. For example, upgrading a Hyper-V cluster from Hyper-V 2016 to Hyper-V 2019 takes approximately the time per node multiplied by the number of nodes. The upgrade process might take longer if an AOS upgrade is also required.

### Requirements

**Note:**

- You can only upgrade to a Windows Server 2022 Hyper-V cluster only from a Hyper-V 2019 cluster.
- Upgrading to Windows Server 2022 Hyper-V from an LACP-enabled Hyper-V 2019 cluster is not supported unless the Hyper-V vSwitch bound/team is set to Switch Embedded Teaming (SET). For more information, see [KB 11220](#).
- Upgrading directly to Windows Server 2022 Hyper-V from Hyper-V 2016 or Windows Server 2012 R2 is not supported.
- To upgrade to Windows Server 2022 Hyper-V, the cluster must have Foundation 5.2.2 or later versions.
- Windows Server 2022 Hyper-V is supported only on NX Series G6 and later models. Hyper-V 2019 is supported only on NX Series G5 and later models.
- For Windows Server 2022 Hyper-V, SET is the default teaming mode. LBFO teaming is not supported on Windows Server 2022 Hyper-V.
- For Hyper-V 2019, if you do not choose LACP/LAG, SET is the default teaming mode. For Hyper-V 2016, if you do not choose LACP/LAG, the teaming mode is Switch Independent LBFO teaming. For Hyper-V 2016 and 2019, if you choose LACP/LAG, the teaming mode is Switch Dependant LBFO teaming.

- Before upgrading, ensure that the Active Directory user account has the necessary permissions to add and remove Active Directory objects.
- The platform must not be a light-compute platform.

- Before upgrading, disable or uninstall third-party antivirus or security filter drivers that modify Windows firewall rules. Windows firewalls must accept inbound and outbound SSH traffic outside of the domain rules.
- Enable Kerberos when upgrading from Windows Server 2012 R2 to Windows Server 2016. For more information, see [Enabling Kerberos for Hyper-V](#).

**Note:** Kerberos is enabled by default when upgrading from Windows Server 2016 to Windows Server 2019.

- Enable virtual machine migration on the host. Upgrading reimages the hypervisor. Any custom or non-standard hypervisor configurations could be lost after the upgrade is completed.
- If you are using System Center for Virtual Machine Management (SCVMM) 2012, upgrade to SCVMM 2016 first before upgrading to Hyper-V 2016. Similarly, upgrade to SCVMM 2019 before upgrading to Hyper-V 2019 and upgrade to SCVMM 2022 before upgrading to Windows Server 2022 Hyper-V.

## Limitations

- When upgrading hosts to Hyper-V 2016, 2019, and later versions, the local administrator user name and password is reset to the default administrator name Administrator and password of nutanix/4u. Any previous changes to the administrator name or password are overwritten.
- VMs with any associated files on local storage are lost.
  - Logical networks are not restored immediately after upgrade. If you configure logical switches, the configuration is not retained and VMs could become unavailable.
  - Any VMs created during hypervisor upgrade (including as part of disaster recovery operations) and not marked as HA (High Availability) experiences unavailability.
  - Disaster recovery: VMs with the Automatic Stop Action property set to *Save* is marked as *CBR Not Capable* if they are upgraded to version 8.0 after upgrading the hypervisor. Change the value of Automatic Stop Action to *ShutDown* or *TurnOff* after you upgrade the VM so that it is not marked as *CBR Not Capable*
- Link Aggregation Control Protocol (LACP) is supported for cluster deployments when upgrading hypervisor hosts from Windows Server 2016 to Windows Server 2019.

## Upgrading Hyper-V Hosts by Uploading Binary and Metadata Files

You can upgrade Hyper-V using the 1-click upgrade feature in the Prism Element web console.

### Before you begin

Ensure that the following prerequisites are met before you upgrade the Hyper-V hosts:

- Check the [Hyper-V Hypervisor Upgrade Recommendations, Requirements, and Limitations](#) on page 85.
- Check the [General Hypervisor Upgrade Recommendations](#) section in *Life Cycle Manager Guide*.
- Follow the recommended upgrade order. For more information, see [Recommended Upgrade Order for Dark Site Method](#) section in *Life Cycle Manager Guide*.
- Ensure that the latest version of the Nutanix Cluster Check (NCC) health checks is installed and upgrade NCC if necessary.

### Procedure

1. Log in to Prism Element web console.

2. Run NCC. For more information, see [Running NCC \(Prism Element\)](#) on page 78.
3. From the dropdown menu on the left of the main menu, select **Settings**.  
The system displays the **Global Settings** page.
4. From the General section in the left navigation pane, click **Upgrade Software**.  
The **Upgrade Software** page opens.
5. Click the **Hypervisor** tab.
6. Click the **upload a Hypervisor binary** link.
7. Click **Choose File** in the Hypervisor Metadata File section to select the metadata JSON file obtained from Nutanix. Then, browse to the file location and select the file.
8. Click **Choose File** in the Hypervisor Binary File (.zip file) section to select the binary file (offline bundle zip file for upgrades obtained from VMware). Then, browse to the file location and select the file.
9. Click **Upload Now**.
10. After the file upload is complete, click **Upgrade > Upgrade Now**, then click **Yes** to confirm.  
[Optional] To run the pre-upgrade installation checks only on the Controller VM where you are logged into, without proceeding with the upgrade, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.
11. When the file upload is completed, click **Upgrade > Upgrade Now**, then click **Yes** to confirm.

**Note:** If AOS detects that the uploaded software is already installed or upgraded, the **Upgrade** option is not displayed.

The **Upgrade Software** dialog box shows the progress of your selection, including status of pre-installation checks and uploads, through the **Progress Monitor**.

### What to do next

Perform and inventory using LCM to display the software and firmware versions of entities in the cluster. For more information, see [Performing Inventory with Life Cycle Manager](#) section in the *Life Cycle Manager Guide*.

## View Task Status

The web console displays detailed information about all tasks that have been performed on the cluster.

### Task Page Navigation

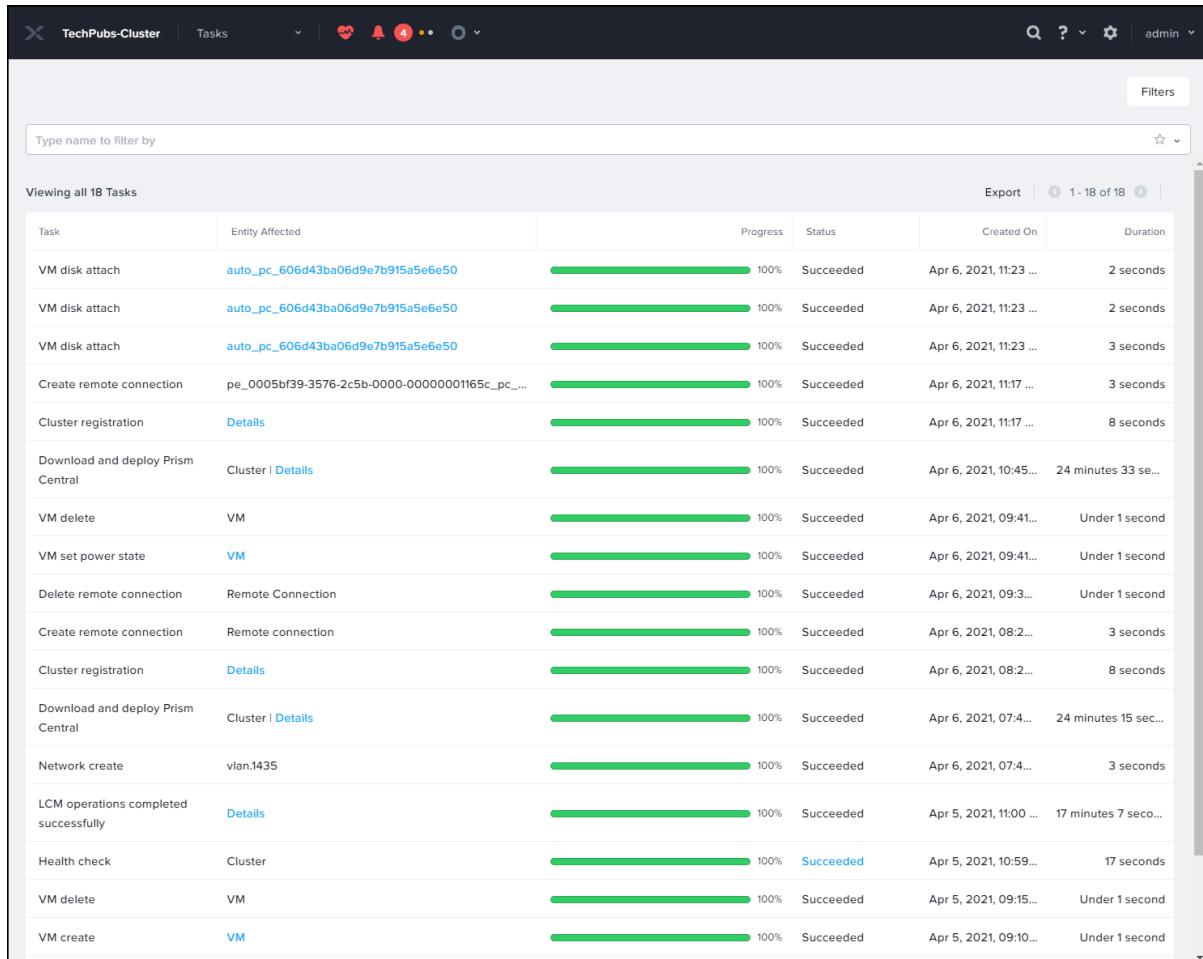
- To view the Task dashboard, log in to Prism Element web console, and select **Home > Tasks**.
- An icon also appears in the main menu when one or more tasks are active (running or completed within the last 48 hours). The icon appears blue when a task runs normally, yellow when it generates a warning, or red when it fails. Clicking the icon displays a drop-down list of active tasks; clicking the **View All Tasks** button at the bottom of that list displays a details screen with information about all tasks for this cluster.

**Note:** The drop-down list of active tasks may include a **Clean Up** button (top right). Clicking this button removes from the list any tasks that are no longer running. However, this applies to the current session only. The full active list (including the non-running tasks) appears when you open a new Prism Element web console session.

- When multiple tasks are active, you can filter the list by entering a name in the filter by field.
- You can also filter the list by clicking the **Filters** button and selecting the desired filter options

Each task appears in the list for a minimum of one hour after completion, but how long that task remains in the list depends on several factors. In general, the maximum duration is two weeks. However, tasks are rotated off the list as new tasks arrive, so a task might disappear from the list much sooner when activity is high. In some cases a task appears for longer than two weeks because the last task for each component is retained in the listing.

## View Task Status Dashboard



The screenshot shows a dashboard titled "TechPubs-Cluster | Tasks". The main area displays a table of 18 completed tasks, each with a green progress bar at 100%. The columns are: Task, Entity Affected, Progress, Status, Created On, and Duration. The tasks listed include VM disk attach, Create remote connection, Cluster registration, Download and deploy Prism Central, VM delete, VM set power state, Delete remote connection, Create remote connection, Cluster registration, Network create, LCM operations completed successfully, Health check, VM delete, and VM create. Most tasks were created on April 6, 2021, with a duration of under 1 second or up to 24 minutes and 33 seconds.

Task	Entity Affected	Progress	Status	Created On	Duration
VM disk attach	<a href="#">auto_pc_606d43ba06d9e7b915a5e6e50</a>	<div style="width: 100%;">100%</div>	Succeeded	Apr 6, 2021, 11:23 ...	2 seconds
VM disk attach	<a href="#">auto_pc_606d43ba06d9e7b915a5e6e50</a>	<div style="width: 100%;">100%</div>	Succeeded	Apr 6, 2021, 11:23 ...	2 seconds
VM disk attach	<a href="#">auto_pc_606d43ba06d9e7b915a5e6e50</a>	<div style="width: 100%;">100%</div>	Succeeded	Apr 6, 2021, 11:23 ...	3 seconds
Create remote connection	<a href="#">pe_0005bf39-3576-2c5b-0000-00000001165c_pc...</a>	<div style="width: 100%;">100%</div>	Succeeded	Apr 6, 2021, 11:17 ...	3 seconds
Cluster registration	<a href="#">Details</a>	<div style="width: 100%;">100%</div>	Succeeded	Apr 6, 2021, 11:17 ...	8 seconds
Download and deploy Prism Central	<a href="#">Cluster   Details</a>	<div style="width: 100%;">100%</div>	Succeeded	Apr 6, 2021, 10:45...	24 minutes 33 se...
VM delete	VM	<div style="width: 100%;">100%</div>	Succeeded	Apr 6, 2021, 09:41...	Under 1 second
VM set power state	VM	<div style="width: 100%;">100%</div>	Succeeded	Apr 6, 2021, 09:41...	Under 1 second
Delete remote connection	Remote Connection	<div style="width: 100%;">100%</div>	Succeeded	Apr 6, 2021, 09:3...	Under 1 second
Create remote connection	Remote connection	<div style="width: 100%;">100%</div>	Succeeded	Apr 6, 2021, 08:2...	3 seconds
Cluster registration	<a href="#">Details</a>	<div style="width: 100%;">100%</div>	Succeeded	Apr 6, 2021, 08:2...	8 seconds
Download and deploy Prism Central	<a href="#">Cluster   Details</a>	<div style="width: 100%;">100%</div>	Succeeded	Apr 6, 2021, 07:4...	24 minutes 15 sec...
Network create	vlan:1435	<div style="width: 100%;">100%</div>	Succeeded	Apr 6, 2021, 07:4...	3 seconds
LCM operations completed successfully	<a href="#">Details</a>	<div style="width: 100%;">100%</div>	Succeeded	Apr 5, 2021, 11:00 ...	17 minutes 7 seco...
Health check	Cluster	<div style="width: 100%;">100%</div>	<a href="#">Succeeded</a>	Apr 5, 2021, 10:59...	17 seconds
VM delete	VM	<div style="width: 100%;">100%</div>	Succeeded	Apr 5, 2021, 09:15...	Under 1 second
VM create	VM	<div style="width: 100%;">100%</div>	Succeeded	Apr 5, 2021, 09:10...	Under 1 second

**Figure 23: Task Dashboard**

**Table 24: Tasks List Fields**

Parameter	Description	Values
Task	Specifies which type of operation the task is performing.	Any cluster operation you can perform in the Prism Element web console
Entity Affected	Display the entity on which task has been performed. If the link appears on the entity, click it to display the details.	Entity description
Percent	Indicates the current percentage complete for the task.	0%-100%

Parameter	Description	Values
Status	Indicates the task status, which can be pending, running, completed, or failed.	pending, running, completed, failed
Created On	Displays when the task began.	seconds, minutes, hours
Duration	Displays how long the task took to complete.	seconds, minutes, hours

## Viewing the Progress of the Download or Upgrade Process

### About this task

**Note:** As part of the AOS upgrade, the node where you have logged on and initiated the upgrade restarts. The Prism Element web console appears unresponsive and might display the following message: Unable to reach server. Check for internet connectivity. Wait a few minutes and log on to the Prism Element web console again.

You can see the progress of the download or upgrade process through one of the following.

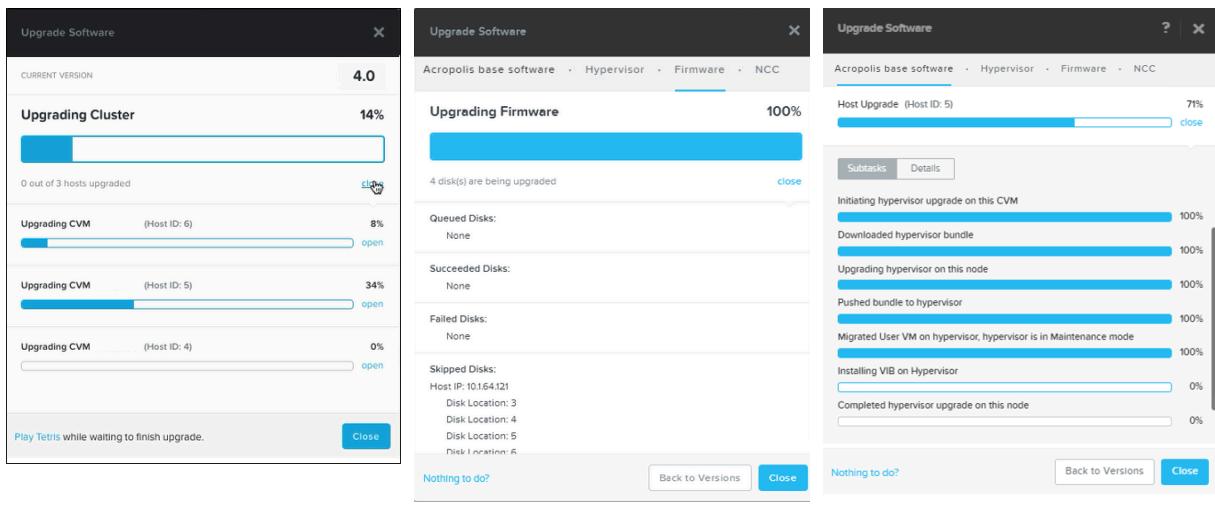
- **LCM Updates** page. For more information, see [Life Cycle Manager Guide](#).
- **Upgrade Software** dialog box in Prism Element web console.
- **Alerts** summary on the main menu

### Procedure

1. Log in to Prism Element web console.
2. Click the gear icon, and select **Upgrade Software**.
3. Under the **Upgrade Software** dialog box progress bar, click **Open**.

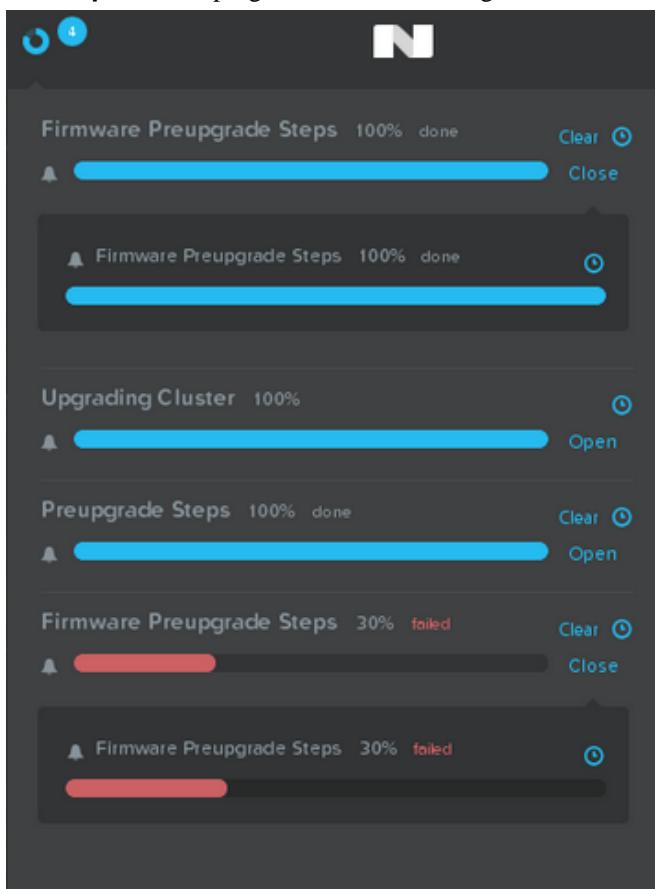
The dialog box displays each Controller VM or disk as it progresses through the upgrade. For example:

**Table 25: Upgrade Progress**



4. Click **open** to see progress including download, installation, and upgrade completion progress bars.
5. Click **Close** at any time; you can reopen the **Upgrade Software** dialog box from the main menu. If you click **Close**, the **Alerts** summary on the main menu also shows upgrade progress.

6. Click the **Alerts** summary on the main menu.
7. Click **Open** to see progress details, including download, installation, and upgrade completion progress bars.



8. Hover your mouse pointer over the clock icon to see timestamps related to the upgrade task.

## Pausing an In-Progress Download

### Procedure

1. If a software download is in progress, do one of the following:
  - » Open **Upgrade Software** from the **Settings** page in the Prism Element web console.
  - » Click the **Alerts** summary on the main menu.
2. Click **Open** near the download progress bar.
3. Click the **Pause** icon to temporarily stop the download.
4. Click the **Play** icon to resume.

## Deleting a Downloaded Image

### About this task

In some cases, you might need to delete a downloaded software image. A pre-upgrade check fails if a corrupted image exists (for example, corrupted as the result of a transient network glitch). You might also delete an image and download it again to clear a pre-upgrade check error message. Another example is

when you want to download the image again for any reason. The upgrade feature reports that you have already downloaded an image, preventing you from downloading it again.

### Procedure

1. Log on to the Controller VM where the image has been downloaded by using a secure shell session (SSH).
2. Change to the `/home/nutanix/software_downloads/download_type` directory, where `download_type` is software, hypervisor, or ncc.
3. Delete the image and retry to download it.

## Multi-Cluster Management

Nutanix provides an option to monitor and manage multiple clusters through a single web console, known as Prism Central. Prism Central is a centralized management tool that runs as a separate VM. From the Prism Element web console, you can either register the cluster with an existing Prism Central instance or deploy a Prism Central instance and register the cluster with it.

Prism Central provides the following features:

- Single sign-on for all registered clusters
- Summary dashboard across clusters that can be customized as desired
- Summary views for major entity types with options to view detailed information about individual entities
- Multi-cluster analytics capabilities
- Multi-cluster alerts summary with options to view information about possible causes and corrective actions for each alert
- Ability to configure individual clusters directly through Prism Central (for selected administrative tasks) or through one-click access to the Prism Element web console for a cluster
- Prism Central Intelligent Operations
- Ability to configure network and security settings, data protection and recovery settings, and Prism Central management settings
- Performance monitoring, application discovery and monitoring, and reports management

For more information about Prism Central, refer to the [Prism Central documentation](#). For information about how the Prism Central documentation is organized, see [Prism Central Documentation Portfolio](#).

For information on how to install Prism Central using 1-click method, see [Installing Prism Central Using 1-Click Method](#) on page 91.

For information on how to register or unregister a cluster with Prism Central, see [Registering a Cluster with Prism Central](#) on page 94.

For information on how to backup and migrate Prism Central, see [Prism Central Backup, Restore, and Migration](#) in the *Prism Central Infrastructure Guide*.

## Installing Prism Central Using 1-Click Method

This section describes how to install Prism Central in Nutanix environment with a connected site (with internet connectivity) or dark site (without internet connectivity) setup.

### Before you begin

Ensure that you meet the following prerequisites before you install Prism Central:

- Check the [Requirements for Prism Central Deployment](#) and [Limitations of Prism Central Deployment](#).
- Check the port requirements between Prism Central and Prism Element. For more information, see [Ports and Protocols](#).
- Check the following requirements for the connected site (with internet connectivity) and dark site (without internet connectivity) environment.

**Table 26: Prism Central Installation Requirements - Connected Site and Dark Site**

Connected site	Dark Site
<ul style="list-style-type: none"> <li>• The specified gateway must be reachable.</li> <li>• Ensure the port TCP port 2100 is open from the Prism Element cluster to the Prism Central VM IP address. For the complete list of required ports, see <a href="#">Ports and Protocols</a>.</li> <li>• Ensure network connectivity between the VM VLAN and portgroup of the Prism Element cluster Controller VM and the Prism Central VM VLAN and portgroup.</li> <li>• No duplicate IP addresses are used.</li> <li>• The storage container used for deployment is mounted on all hypervisor hosts.</li> <li>• When installing on an ESXi cluster: <ul style="list-style-type: none"> <li>• vCenter and the ESXi cluster must be configured properly. For more information, see <a href="#">vSphere Administration Guide for Acropolis</a>.</li> <li>• vCenter must be registered in Prism.</li> <li>• DRS must be enabled in vCenter.</li> <li>• vCenter is up and reachable during the deployment.</li> </ul> </li> </ul>	<p>Download Prism Central binary .TAR and metadata .JSON files from the Nutanix Support portal from a connected machine.</p> <ol style="list-style-type: none"> <li>1. Log in to the <a href="#">Downloads page for Prism Central</a>.</li> <li>2. Click <b>Download</b> and <b>Metadata</b> to save the <b>Prism Central 1-click deploy from Prism Element</b> binary .TAR and metadata .JSON files, respectively, to your local media.</li> </ol> <p>You can also copy these files to a USB stick, CD, or other media.</p> <p><b>Note:</b> Do not use the Prism Central OVA, ZIP, AHV image, or AOS binary .TAR.GZ and upgrade metadata JSON files from the Nutanix support portal to create this new Prism Central instance. Use the .TAR format binary and metadata .JSON files.</p> <p>The Prism Central OVA is used only to install or upgrade Prism Central in non-Nutanix ESXi environment. For more information, see <a href="#">Prism Central Installation in a Non-Nutanix ESXi Environment</a> and <a href="#">Prism Central Upgrade in a Non-Nutanix ESXi Environment without AOS</a>.</p>

## About this task

Perform this procedure for both connected site (with internet connectivity) and dark site (without internet connectivity).

## Procedure

1. Log in to the Prism Element web console as the user admin for your cluster.
2. Run NCC as described in [Run NCC Checks](#).

3. Do one of the following:

  - » On the **Home** dashboard, click **Deploy New Prism Central** from the **Prism Central** widget.
  - » Click the gear icon in the main menu, from the **Settings** menu, select **Prism Central Registration**, and then click **Deploy New Prism Central**.
4. In the **Prism Central (PC) Deployment** dialog box, in the **Version** section, enter the following information:

  - a. **PC Details:** Name for the Prism Central instance.
  - b. [Applicable to Dark site only] In **Available Versions**, click the **Upload Installation Binary** link, select the Prism Central Metadata File (.json) and Prism Central Installation Binary (.tar) files, and then click **Upload**.

If there is an image already uploaded, the system displays the available versions.
  - c. [Applicable to Connected site only] Select the required Prism Central version you intend to install.

Select **Only show compatible versions** checkbox to view the list of PC versions compatible with the AOS cluster.

**Note:** If the Prism Central version you want to install does not appear in the list, typically because the cluster does not have Internet access (such as at a dark site), you can click the **Upload Installation Binary** link to upload an image from your local media as described in Step **4.b** on page 93.
5. In the **Configuration** step, in **General Details** section, enter the IP address for Prism Central VM.

If you have selected **Enable High Availability (HA)** in the **Size and Scale** section, the IP addresses for the three PC VMs are populated automatically when you enter virtual IP. You can keep those addresses or change them as desired.
6. In the **Internal Network Configuration** section, do the following in the indicated fields:

  - a. **Use default settings (recommended)** : Select the checkbox to allows Prism Central to use the default values for **Subnet Mask**, **Gateway IP Address** and **IP Address Range**. Clear the checkbox if you want Prism Central to use the specific (non-default or custom) values for **Subnet Mask**, **Gateway IP Address** and **IP Address Range**.

The following three fields are enabled only if you choose not to use the default settings.
  - b. **Subnet Mask:** Enter the subnet mask.
  - c. **Gateway IP Address:** Enter the IP address for the gateway.
  - d. **Gateway IP Address:** Enter a range of IP addresses that the network can use.

Enter a range of at least 10 available (unreserved) addresses. For a managed network, the range of addresses for microservices infrastructure must be outside the range of reserved IP addresses (for example, DHCP IP Pool) in the selected network.
  - e. After you check that the values entered for all the fields are correct, click **Deploy**.

This begins the deployment process. On the **Home** page, the Prism Central widget displays **Deploying** until the installation is completed, then it displays **OK**. Click **OK** to launch the Prism Central web console in your browser.
7. Monitor the deployment progress from the **Tasks** page and view information about the deployed VMs through the **VM** dashboard. For more information, see [Tasks View](#).

#### What to do next

you can expand your cluster, remove nodes, and enable services such as Self-service, Flow Network Security, and Intelligent Operations without registering the hosting cluster with Prism Central.

Register this cluster with Prism Central, if you want to manage this cluster through Prism Central. For more information about how to connect to an existing Prism Central instance, see [Registering or Unregistering a Cluster with Prism Central](#).

## Registering a Cluster with Prism Central

You must register a cluster with Prism Central only if you want to manage the cluster through Prism Central.

### Before you begin

- If you have never logged into Prism Central as the admin user, you must log in and change the password before you attempt to register a cluster with Prism Central. For more information, see [Logging into Prism Central](#).
- Do not enable client authentication in combination with ECDSA certificates on a registered cluster because it causes interference when communicating with Prism Central.
- Port 9440 must be open in both directions between the Prism Central VM and all the Controller VMs (and the cluster virtual IP address if configured) in each registered cluster. For the complete list of required ports, see [Ports and Protocols](#).
- If you have a proxy server configured and you want the cluster communication between the cluster and Prism Central to go through the proxy, open the relevant ports on the proxy. If you do not want the communication to go through the proxy, add the Prism Central IP address to the proxy allowlist in the cluster settings. For more information about configuring proxy, see [Configuring HTTP Proxy](#) on page 391. For the complete list of required ports, see [Ports and Protocols](#).
- You can register a cluster with only one Prism Central instance at a time. To register with a different Prism Central instance, first unregister the cluster.
- If the cluster is dual stack enabled, the Prism Central instance must also be dual stack enabled to register it.

### About this task

To register a cluster with Prism Central, follow these steps:

**Note:** To perform this task, ensure that you log in to the Prism Element web console as an admin user.

### Procedure

1. Log in to the Prism Element web console on the target cluster.
2. To run Nutanix Cluster Checks, go to the **Health** dashboard, and from the **Actions** dropdown menu, click **Run Checks**.
3. From the dropdown menu on the left of the main menu, select **Settings**.  
The system displays the **Global Settings** page.
4. From the **Setup** section in the left navigation pane, click **Prism Central Registration**.  
The system displays the **Prism Central** page.
5. Click **Register** or deploy new Prism Central.  
The Prism Central dialog box opens displaying options to deploy a new Prism Central or connect to an existing Prism Central instance
6. Click **Connect**.  
The system displays the Connect Info tab outlining the services available through Prism Element and Prism Central

- After reviewing the message, click **Next**.  
The system displays the **Configuration** tab.

- Perform the following steps:

- In the **Prism Central IP/FQDN** field, enter the IP address or FQDN of the Prism Central VM.
- In the **Port** field, enter the port number to allow communication between Prism Element and Prism Central.  
For the complete list of required ports, see [Ports and Protocols](#).
- In the **Username** field, enter admin as the Prism Central user name.
- In the **Password** field, enter the password for the Prism Central user.

- Click **Connect** to save the details.

The cluster is now registered with the specified Prism Central VM. After successful registration, the specified cluster and Prism Central start communicating with each other.

**Note:**

- The user credentials provided when registering a cluster (Prism Element) with Prism Central are only used once. After registration, modifying the admin password would not impact any communication between Prism Central and the cluster.
- On small, large, and x-large Prism Central deployments, when you register a new cluster to Prism Central, Prism Central synchronises the past 90 days of data (including multiple metrics) from the cluster. On x-small Prism Central deployments, Prism Central synchronises the past 2 hours of data (including multiple metrics) from the cluster. To view the list of metrics that are synced during registration, see the file `/home/nutanix/config/arithmos/data_sender/arithmos_history.json` in the Controller VM. To view the list of metrics that are synced during a regular synchronisation between Prism Central and the cluster, see the file `/home/nutanix/config/arithmos/data_sender/arithmos.json` in the Controller VM.

### What to do next

After the cluster is registered with Prism Central, you can configure various settings for network, security, and alerts. For more information, see [Admin Center Settings Options](#).

## Restoring Prism Central (One-Click Recovery)

If you have protected or backed up your Prism Central instance, use an AHV or ESXi cluster to restore the Prism Central instance. For continuous backups (backups stored on on-prem Nutanix clusters), you can recover the Prism Central instance from a registered cluster only. For point-in-time backups (backups stored on AWS S3), you can recover the instance on a registered cluster, or you can recover it on a cluster that is not registered with any Prism Central instance.

### Before you begin

Ensure that the Nutanix cluster used to restore the Prism Central instance meets the following requirements:

- The cluster is registered to the protected Prism Central instance.
- To restore from a continuous backup, the cluster must run AOS 6.5.3.1 or later. For more information on the supported AOS versions, see [Compatibility and Interoperability Matrix](#).
- To restore from a point-in-time backup, the cluster must run AOS 6.8 or later. For more information on the supported AOS versions, see [Compatibility and Interoperability Matrix](#).

- The cluster is configured with iSCSI data service IP address for efficient recovery of Nutanix Disaster Recovery or NCM Self-Service configurations.

**Note:** After the recovery task on the Prism Element web console is displayed as complete, the Nutanix cluster takes approximately 10 minutes to stabilize the Prism Central instance. This is because Microservices Infrastructure causes the system to rotate certificates after the restoration and restart services like IAM and Flow Virtual Networking.

## About this task

### Important:

- After restoring your Prism Central instance, ensure that you manually restore Files to the pre-disaster version. For more information, see [Manually Failing Over to a Remote Site](#) in the *Files Manager User Guide*.
- Accessing Prism Central using APIs or any other alternative method is strongly discouraged until the restoration process is complete, as such actions might lead to locking of Prism Central username credentials resulting in subsequent login attempts.

To restore a Prism Central instance, follow these steps:

## Procedure

- Log in to a Prism Element web console registered to the Prism Central instance you plan to restore.  
The Prism Element dashboard shows the Prism Central widget, which contains Prism Central information (IP address and connection status). If this is a newly deployed Prism Element that has not yet been registered to a Prism Central, the **Register or Deploy Prism Central** option appears instead.
- From the dropdown menu on the left of the main menu, select **Settings**.  
The system displays the **Global Settings** page.
- From the **Data Resiliency** section in the left navigation pane, click **Restore Prism Central**.  
The system displays the **Restore Prism Central** page. This page provides you options to restore the Prism Central instance from a Prism Element cluster or S3-compatible object storage.
- Select whether you plan to restore the Prism Central instance from Prism Element or S3 compatible object storage, and click **Restore Now**.

**Note:** If you have configured only continuous backup, the system displays the **Restore Now** option only when Prism Central is in a disconnected state (shown as **Disconnected** in the Prism Element web console).

The **Restore Prism Central** window appears, displaying the service data that is recovered and the data that is not.

- Click **Continue** and specify the following information according to the source from where you plan to recover:
  - To recover from a continuous backup, see [Restoring Prism Central - Field Information for Continuous Backup](#) on page 98.
  - To recover from a point-in-time backup, see [Restoring Prism Central - Field Information for S3-based Object Storage](#) on page 98.

The Prism Central instance is restored in 60 to 90 minutes, depending on the configuration data of the hosts. The restoration involves the deployment of Prism Central and the restoration of its configuration data from the backup, which can take anywhere between 60 and 120 minutes, depending on the size of the data. The restored Prism Central instance takes an additional 30 to 40 minutes to show all the guest VMs, disks, and metrics. Wait to perform any actions on the restored Prism Central instance until all the recovery tasks are complete on the cluster. You can see the restoration status and the related processes in the **Tasks** window.

## What to do next

Consider the following after the Prism Central restoration:

- Use the newly restored Prism Central instance only.

If the old Prism Central instance becomes available, shut down or delete the old instance because running the old Prism Central instance can cause data corruption.

**Note:** If the Prism Central restoration fails, contact Nutanix Support. Do not restart the old Prism Central instance.

- Reset the credentials.

The Prism Central instance restores with the default credentials. Nutanix recommends changing the default credentials. For information about changing the default credentials, see [Logging Into Prism Central](#) in the *Prism Central Infrastructure Guide*.

**Note:** If you have both S3-compatible object storage and Nutanix on-prem clusters configured as backup targets and you restored the Prism Central instance using an on-prem cluster, you must reconfigure the S3 bucket credentials after recovery using the the Prism Central Backup and Restore widget in Prism Central. For more information, see [Backing up Prism Central](#).

- Reconfigure the proxy server. For more information, see [Configuring an HTTP Proxy](#) in the *Prism Central Admin Center Guide*

If the old Prism Central instance had a proxy server, reconfigure the proxy server so that the recovered Prism Central instance maps to the correct IP address.

- Reconfigure the fully qualified domain name (FQDN).

If the old Prism Central instance had an FQDN, reconfigure the FQDN so that the recovered Prism Central instance maps to the correct IP address.

- If you had recovery plan jobs (RPJ) in progress, perform the steps in [KB-10962](#).

If the old Prism Central instance had a failover task running (Nutanix Disaster Recovery) or protection policy with entities protected with synchronous replication schedule, perform the steps in [KB 10962](#) to ensure that all the failover tasks stuck in the running state are terminated and a script is executed for efficient recovery of the Prism Central instance.

- Restore the secret keys (for example, PCKMS) manually through nCLI on the newly restored Prism Central instance. For more information, see [Importing Keys](#) in the *Security Guide*.

First, back up the secret keys present on the old Prism Central instance to a text file:

```
ncli> data-at-rest-encryption backup-software-encryption-keys file-path=/path/
textfile.txt password=password
```

Replace `/path/textfile.txt` with the absolute path of the text file wherein you have backed up the secret keys.

Copy the text file to the newly restored Prism Central instance, then restore the secrets manually from the text file:

```
nutanix@pcvm$ mantle_recovery_util -backup_file_path /path/textfile.txt -password
<password>
```

Replace `/path/textfile.txt` with the absolute path of the text file wherein you have backed up the secret keys.

**Tip:** Run the following command to list the secret keys backed up in the text file:

```
nutanix@pcvm$ mantle_recovery_util -backup_file_path /path/textfile.txt -
list_key_ids -password <password>
```

Replace `/path/textfile.txt` with the absolute path of the text file wherein you have backed up the secret keys.

- Reconfigure Life Cycle Manager (LCM) if you do not use the Nutanix portal or if you use LCM in a dark site. For more information, see [LCM Settings for Dark Sites - No Internet Connectivity](#). For information on reconfiguration of LCM 3.1, see [KB 17966](#).

## Restoring Prism Central - Field Information for Continuous Backup

### Procedure

1. Select the cluster to restore the Prism Central instance.
2. Verify the version of the Prism Central instance to be restored on the selected cluster.
3. Select the network to restore and install the Prism Central instances.  
The **Subnet Mask**, **Gateway**, and **DNS Address(es)** fields show the relevant information associated with the selected network.
4. Enter the name and IP address of the Prism Central instance to restore and click **Save**.
5. Review the summary and click **Recover**.

## Restoring Prism Central - Field Information for S3-based Object Storage

### Procedure

1. In the **Connect** tab, specify the following details, then click **Next**:
  - a. **AWS Region Name:** Enter an AWS region name. For more information, see [AWS documentation](#).
  - b. **AWS Bucket Name:** Enter a bucket name. For more information, see [AWS documentation](#).
  - c. (Optional for NC2 environments) **Access Key:** Enter your access key.
  - d. (Optional for NC2 environments) **Secret Access Key:** Enter your secret access key.

2. In the **Source** tab, select the Prism Central backup you want to restore, and click **Next**.

You can use an S3 bucket to back up multiple Prism Central instances. The instances are listed as the **PC\_<IP\_ADDRESS>** or the FQDN if configured.

3. In the **Restore Point** tab, specify the date for the point-in-time backup, select one of the available restore points to restore the Prism Central instance and click **Next**.
4. In the **Installation** tab, verify the cluster IP address where the Prism Central instance was originally hosted and the version of your instance, then click **Next**.
5. In the **Configuration** tab, specify the networking details and click **Next**.

**Note:** If you are restoring the Prism Central instance from the same cluster (Prism Element) where the Prism Central instance was hosted, details like **vLAN**, **Subnet Mask**, **Gateway IP**, **DNS Address(es)**, **NTP Address(es)**, **Container**, and **Virtual IP** are populated automatically. You must configure these details if you are trying to restore the Prism Central instance from a different AZ or a cluster.

6. In the **Microservices** tab, specify the Prism Central service domain name, internal network, and the required input to enable Microservices Infrastructure (CMSP).

Nutanix recommends using the default settings for **Subnet Mask**, **Gateway IP Address**, and **IP Address Range**.

**Note:** Ensure that the IP address range does not conflict with the reserved DHCP IP address pool in your network.

7. In the **Summary** tab, review the information that you configured in the previous steps and click **Restore**.

## CVM Memory Configuration

When you create a cluster, Foundation provisions the default memory and vCPUs to each CVM (CVM) according to your platform category. After a CVM is created, you can increase the memory reserved for each CVM in your cluster by using the 1-click CVM Memory Upgrade feature available in the Prism Element web console. You might need to increase the CVM memory based on your cluster configuration.

### CVM Field Specifications

For information about the minimum CVM configurations (CVM logical cores, CPU physical cores per socket, and vRAM) based on your platform category, see [CVM \(CVM\) Field Specifications](#) topic in *Acropolis Advanced Administration Guide*.

Foundation allocates the maximum resources to Controller VM (CVM) of the SO node as follows:

- CVM vCPU = All CPU cores of the physical host minus 2, limited to a maximum of 22 vCPUs

**Note:** This is applicable till Foundation version 5.3.x. From Foundation version 5.4 onwards, the capping of maximum 22 vCPUs is not applicable.

- CVM memory = Available RAM minus 16 GiB, limited to a maximum of 256 GiB.

**Note:**

- This is applicable from Foundation version 5.3 and above. In the earlier Foundation versions, the memory allocation happens without capping to 256 GiB.
- A capping of maximum 256 GiB is applied, and Foundation allocates the maximum possible vRAM to CVM. For example, if the available RAM is 512 GiB, the system allocates a maximum of 256 GiB and never considers the  $512 - 16 = 496$  GiB value. However, if you change the system allocated vRAM, the vRAM gets overridden with the supplied value.

**Note:** Minimum Foundation version of 5.3 supports these limits with NUMA pinnings or alignments. Earlier Foundation versions with a minimum version of 5.0 support these limits but not NUMA pinnings or alignments.

## Increasing the Controller VM Memory Size

### Before you begin

See the CVM Field Specification in [CVM Memory Configuration](#) on page 99.

### About this task

**Note:**

- vCenter access details and credentials are required to update the CVM configuration. The details are encrypted on the CVM and removed after the update is complete.
- Nutanix does not support decreasing the CVM memory below the recommended minimum requirements.

To increase the CVM memory in the Prism Element web console, follow these steps:

### Procedure

1. Log in to the Prism Element web console.
2. Run NCC as described in [Running Checks by Using Prism Element Web Console](#) on page 257.
3. From the dropdown menu on the left of the main menu, select **Settings**.  
The system displays the **Global Settings** page.
4. From the **General** section in the left navigation pane, click **Configure CVM**.  
The system displays the **Configure CVM** page.
5. If you have an ESXi cluster managed by VMware vCenter Server, you must enter the vCenter authentication information to increase the CVM memory by performing the following steps:
  - a. In the **Configure CVM** dialog box, click **Add vCenter**.
  - b. Enter the vCenter Server IP address and administrator credentials.
  - c. Click **Add**.
6. Select the **Target CVM Memory Allocation** memory size and click **Apply**.

**Note:**

- You can allocate a maximum CVM memory of 64 GB through the Prism Element web console. To upgrade the CVM memory beyond 64 GB, contact Nutanix support.
- If a CVM was already allocated more memory than your choice, it remains at the allocated amount. For example, if a CVM is at 20 GB memory and you select 28 GB, the CVM memory is upgraded to 28 GB. However, if a CVM is at 48 GB memory and you select 28 GB, the CVM memory remains unchanged at 48 GB.

AOS allocates memory to each CVM that has less than the specified amount.. Resizing memory for a CVM requires a restart. Only one CVM restarts at a time, thus preventing any production impact.

## Resource Requirements Supporting Snapshot Frequency (Asynchronous, NearSync, and Metro)

For DR solutions with asynchronous, nearsync, and synchronous (using metro availability) replication schedules to succeed, the nodes must have certain resources.

For information on snapshot frequency requirements, see [Resource Requirements Supporting Snapshot Frequency \(Asynchronous, NearSync and Metro\)](#) information in the *Data Protection and Recovery with Prism Element Guide* or [On-Prem Hardware Resource Requirements](#) information in the *Nutanix Disaster Recovery Guide*.

**Note:** For metro availability, the synchronous replication is supported with snapshots generated every 6 hours. Any node that supports 6-hour snapshot retention can support synchronous replication with 0 seconds RPO. For more information, see [Synchronous \(0 seconds RPO\)](#) in *Nutanix Disaster Recovery Guide*.

## Rebooting an AHV or ESXI Node in a Nutanix Cluster

### About this task

The **Request Reboot** operation in the Prism Element web console gracefully restarts the selected nodes one after the other.

**Note:** Reboot host is a graceful restart workflow. Hosts are automatically put into maintenance mode and all the guest VMs are migrated to another host when you perform a reboot operation for a host. The reboot operation does not impact the user workload. Reboot fails if the ESXI node is already in maintenance mode.

### Procedure

To reboot the nodes in the cluster, perform the following steps:

1. Log on to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Settings**.  
The system displays the **Global Settings** page.
3. From the **General** section in the left navigation pane, click **Reboot**.  
The system displays a progress bar that indicates the restart status of each node.

# STORAGE MANAGEMENT

---

Storage in a Nutanix cluster is organized hierarchically into several components that allow you to manage capacity and performance. Following is a brief outline of the storage features of a Nutanix cluster and how to navigate these storage features.

- Nutanix clusters provide storage pool, storage container, volume group, and virtual disk components to organize storage. For more information see [Storage Components](#) on page 102.
- Nutanix clusters provide effective storage capacity management to ensure that containers have sufficient storage for optimal performance while maintaining cost-efficiency and avoiding disruptions. For more information, see [Capacity Management](#) on page 105.
- Nutanix clusters provide storage efficient capabilities that allows strategic management of storage resources. For more information, see [Storage Efficiency](#) on page 110.
- The Prism Element web console helps you monitor storage usage across the cluster. For more information see [Storage Dashboard](#) on page 117.
- The Prism Element web console helps you create storage containers and volume groups. For more information, see [Creating a Storage Container](#) on page 131 and [Creating a Volume Group](#) on page 141.
- The Prism Element web console helps you configure the replication factor of a storage container in a cluster. For more information, see [Replication Factor Configuration](#) on page 137.
- The Prism Element web console helps you configure a threshold warning for storage capacity available in the cluster after accounting for the storage space needed to rebuild and restore in case of any component failures. For more information, see [Configuring a Warning Threshold for Resilient Capacity](#) on page 106.
- The Prism Element web console helps you reserve storage capacity for rebuilding failed nodes, blocks or racks. For more information, see [Rebuild Capacity Reservation](#) on page 107.

## Storage Components

Storage in a Nutanix cluster is organized into the following components.

### Storage Tiers

Each type of storage hardware (SSD-PCIe (NVMe), SSD (SATA SSD), and HDD) is placed in a storage tier. You can determine the tier breakdown for disks in a storage pool through the web console . For more information, see [Storage Table View](#) on page 124 .

### Storage Pools

Storage pools consist of groups of physical disks from one or more tiers providing physical separation since each storage device belongs to only one storage pool at a time. Nutanix recommends creating a single storage pool per cluster to enable dynamic optimization of capacity and performance.

While isolating disks into separate storage pools ensures physical separation, it might lead to resource imbalances if the disks remain underutilized. When you expand a cluster by adding new nodes, their disks can also be seamlessly integrated into the existing storage pool. This scale-out architecture allows you to build a cluster that grows with your needs.

By default, when a cluster is created, a predefined storage pool is available. This pool includes the total capacity of all the disks on all the hosts in the cluster.

## Storage Containers

A storage container is a subset of available storage within a storage pool. Storage containers are created within a storage pool to hold virtual disks (vDisks) used by virtual machines. For more information, see [Creating a Storage Container](#). By default, storage is thinly provisioned, which means that the physical storage is allocated to a storage container as needed when data is written, rather than allocating the predefined capacity when the storage container is created. Storage efficiency features such as compression, deduplication, and erasure coding are enabled at the container level.

When you create a Nutanix cluster, the following storage containers are created by default:

- **NutanixManagementShare:** The NutanixManagementShare storage container is a built-in storage container designed for Nutanix clusters, specifically supporting Nutanix Files and the Self-Service Portal (SSP) features. This storage container is used for file storage, feature upgrades, and various operational tasks related to these features. To ensure proper functionality, do not delete this storage container. Nutanix recommends that you do not delete this storage container even if you are not using Nutanix Files or SSP. This storage container is not intended for vDisk storage, including Nutanix Volumes.
- **SelfServiceContainer:** SelfServiceContainer is a built-in storage container within a Nutanix cluster that is used for storage by VMs created using Image service features such as Self-Service and OpenShift. SelfServiceContainer can also be used like any other container for regular VMs, volume groups, and images. General requirements for using container-level configurations such as compression, deduplication, erasure coding, and replication factor in SelfServiceContainer are the same as any other container. Nutanix recommends that you do not delete this storage container.
- **Default-Container-XXXX:** Default-Container-XXXX is a built-in storage container used by VMs to store vDisks for guest VMs and applications. You can rename the Default-Container or delete it and create a new one according to your naming convention.

## Volume Groups

A volume group is a collection of logically related virtual disks (or volumes). A volume group is attached to a VM either directly or using iSCSI. You can add vDisks to a volume group, attach them to one or more consumers, include them in disaster recovery policies, and perform other management tasks. You can also detach a volume group from one VM and attach it to another, possibly at a remote location to which the volume group is replicated.

You manage a volume group as a single unit. When a volume group is attached to a VM, the VM can access all the vDisks in the volume group. You can add, remove, and resize the vDisks in a volume group at any time.

Each volume group is identified by a UUID, a name, and an iSCSI target name. Each disk in the volume group also has a UUID and an iSCSI index that specifies ordering within the volume group. A volume group can be configured for either exclusive or shared access.

You can backup, protect, restore, and migrate volume groups. You can include volume groups in a protection domains configured for asynchronous data replication (Async DR), either exclusively or with VMs. However, volume groups cannot be included in a protection domain configured for metro availability, in a protected vStore, or in a consistency group for which application consistent snapshots are enabled.

## vDisks

A vDisk is created within a storage container or volume group to provide storage to the virtual machines. A vDisk shows up as a SCSI device when it is mapped to a VM.

## Containers for VMware and Hyper-V (Datastores/SMB Shares)

In vSphere, a datastore is a logical container for files necessary for VM operations. Nutanix supports both iSCSI and NFS protocols when mounting a storage volume as a datastore within vSphere. NFS has many performance and scalability advantages over iSCSI, and is the recommended datastore type.

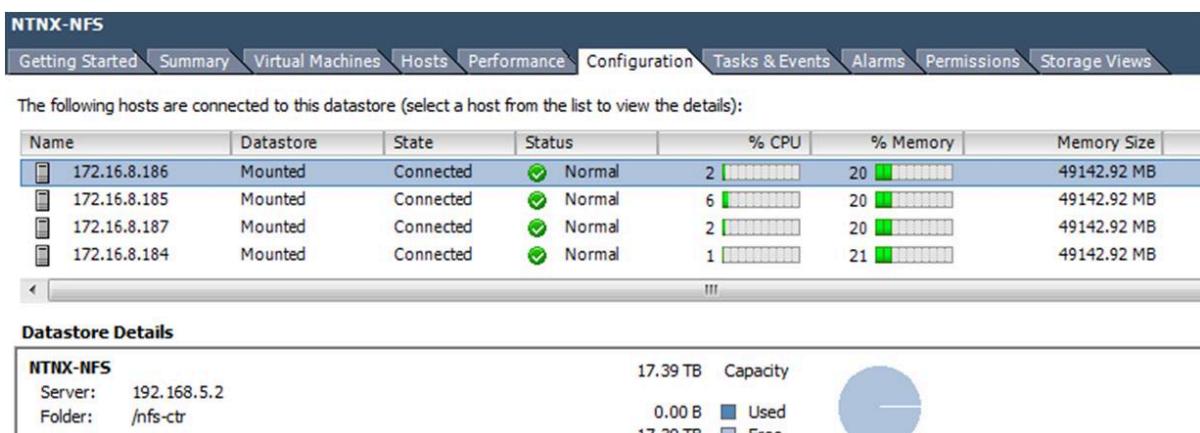
In Hyper-V environments, storage containers are mounted as an SMB share.

**Note:** Nutanix does not recommend using a Nutanix storage container as a general-purpose NFS or SMB share. For NFS and SMB file service, use Nutanix Files.

**NFS Datastores.** The Distributed Storage Fabric (DSF) reduces unnecessary network chatter by localizing the data path of guest VM traffic to its host. This boosts performance by eliminating unnecessary hops between remote storage devices that is common with the pairing of iSCSI and VMFS. To enable vMotion and related vSphere features (when using ESX as the hypervisor), each host in the cluster must mount an NFS volume using the same datastore name. The Nutanix web console and nCLI both have a function to create an NFS datastore on multiple hosts in a Nutanix cluster.

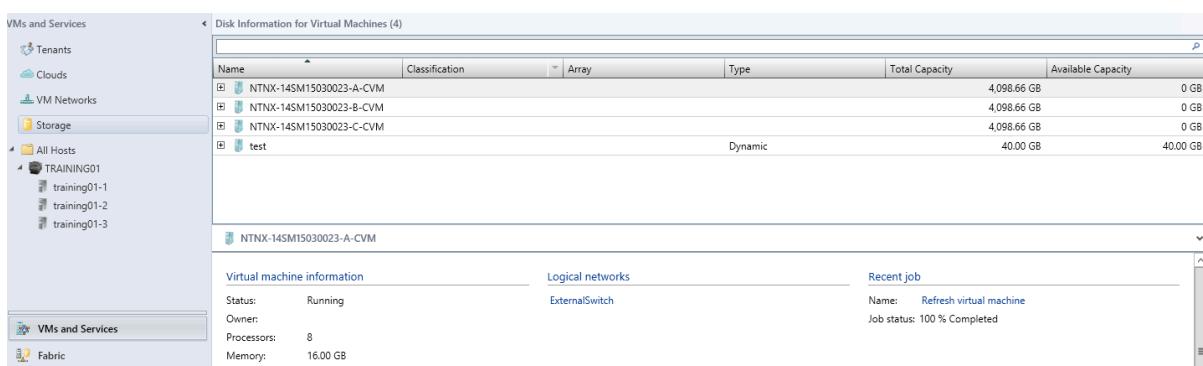
To correctly map the local ESXi datastore to the Nutanix container:

- Map the NFS share with 192.168.5.2 (internal IP address) and not the Controller VM IP address or cluster virtual IP address.
- The name of the datastore should be same as the name of the container.



**Figure 24: vSphere Configuration of NFS Datastore**

**SMB Library Share.** The Nutanix SMB share implementation is the Hyper-V equivalent of an NFS Datastore, offering feature and performance parity with a vSphere configuration. The registration of a Nutanix storage container as an SMB Library share can be accomplished through a single powershell script, or through the Virtual Machine Manager GUI.



**Figure 25: Hyper-V Configuration of an SMB Share**

# Capacity Management

Storage container capacity management involves monitoring and optimizing the allocation of storage resources within containers to ensure efficient utilization and prevent over-provisioning or resource exhaustion.

## Capacity Reservation Best Practices

Capacity reservation ensures that a storage container has a minimum allocated capacity, preventing other storage containers from using that reserved space.

By default, each storage container has access to all of the unused storage in the storage pool. If a storage pool consists of multiple storage containers, one storage container might take all the remaining storage space and leave others with no available space. To ensure that there is space available for a storage container, you can enable capacity reservation.

Nutanix recommends the following best practices to enable capacity reservation:

- Reserve capacity for a storage container only if the storage pool consists of multiple storage containers. Unless there is a specific reason to have multiple storage containers, Nutanix recommends you to configure a single storage pool with a single storage container.
- Do not reserve more than 90% of the total space in the storage pool.
- When you set an advertised capacity for a storage container, be aware that some extra space must be allocated beyond the projected size of any VMs placed in the container. This extra space is to allow room for data that is not yet garbage collected. The extra space is based on the workload and can be substantial, for example, 10% or more of the storage capacity in some cases.

## Cluster Resilient Capacity

Cluster resilient capacity is the storage capacity available in the cluster after accounting for the storage space needed to rebuild and restore the cluster in case of any component failures.

### Cluster Resilient Capacity Calculation with Homogeneous Capacity Entities in Failure Domains

For homogeneous capacity entities in a failure domain, the cluster resilient capacity is calculated as described in the following table:

**Table 27: Cluster Resilient Capacity Calculation - Homogenous Capacity Entities**

Cluster Fault Tolerance	Replication Factor	Failure Domain	Amount of space reserved (Reserve Capacity)
1N/1D	2	Node	1 node worth of capacity
		Block	1 block worth of capacity
		Rack	1 rack worth of capacity
1N&1D	3	Node	1 disk per node worth of capacity
		Block	1 disk per block worth of capacity
		Rack	1 disk per rack worth of capacity
2N/2D	3	Node	2 nodes worth of capacity
		Block	2 blocks worth of capacity
		Rack	2 racks worth of capacity

## Cluster Resilient Capacity Calculation with non-homogeneous Capacity Entities in Failure domains

For non-homogeneous capacity entities in a failure domain, the cluster resilient capacity is calculated as the maximum available capacity at the lowest supported failure domain that can meet the required replication factor after cluster fault tolerance failures at the configured failure domain.

The following table provides the examples for resilient capacity calculation when non-homogeneous capacity entities exist in failure domain:

**Table 28: Cluster Resilient Capacity Calculation - Non-homogenous Capacity Entities**

Cluster Fault Tolerance	Replication Factor	Failure Domain	Total Number of Nodes	Node Capacities	Failures
1N/1D	2	Node	5 nodes	10 TiB	Failure of capacity
				10 TiB	
				10 TiB	
				40 TiB	
				40 TiB	
1N&1D	3	Node	3 nodes	30TiB (3 disks of 10TiB each)	Failure of capacity any node
				30TiB (3 disks of 10TiB each)	
				40TiB (4 disks of 10TiB each)	
2N/2D	3	Node	5 nodes	10 TiB	Failure of capacity
				10 TiB	
				20 TiB	
				40 TiB	
				40 TiB	

## Configuring a Warning Threshold for Resilient Capacity

Resilient capacity is the storage capacity available in the cluster after accounting for the storage space required to rebuild and restore the cluster in case of any failures. The resilient capacity in a cluster depends on the cluster fault tolerance level and the configured cluster failure domain (node, block, or rack).

### About this task

You can configure a warning threshold to track the resilient capacity in the cluster. When the used capacity crosses the set threshold, the storage summary widget changes color as a warning.

To configure a warning threshold for resilient capacity, do the following.

### Procedure

- Log on to the Prism Element web console.
- From the dropdown menu on the left of the main menu, select **Storage**.  
The system opens the **Storage** dashboard displaying the **Overview** tab.

3. Click the settings icon in the **Storage Summary** widget.  
The system displays the **Configure Warning Threshold** dialog box.
  4. Select one of the following:
    - » **Use default** : Select this option to use the default 75% warning threshold limit for resilient capacity.
    - » **Set manually** : Select this option to manually enter a custom warning threshold limit for resilient capacity in the cluster.
- Threshold for warning limit** : If you select the **Use default** option, this field displays the default 75% warning threshold limit. If you select the **Set manually** option, enter the custom warning threshold limit for resilient capacity in the cluster.

5. Click **Save**.

The system sets a resilient capacity marker in the **Storage Summary** widget according to the warning threshold limit configured. Hover over the widget for more information.

## Rebuild Capacity Reservation

Rebuild capacity is the storage capacity reserved in the cluster to enable self-healing and rebuilding failed nodes, blocks or racks (depending on what is configured as cluster failure domain).

Nutanix recommends that you reserve rebuild capacity in a cluster to enhance the self-healing capabilities of the cluster. You can configure rebuild capacity reservations through the Prism Element web console.

When you enable the **Reserve Rebuild Capacity** option in the Prism Element web console, the system reserves the necessary capacity within the total cluster storage capacity based on *Failure Domain* and *Fault Tolerance* by removing the reserved capacity from the storage pool of the cluster. When there is a failure of the *Failure Domain* entity such as failure of a node, then the cluster rebuilds the data of the node by replicating the data on the remaining nodes.

For more information about *Failure Domain* and *Fault Tolerance*, see [Cluster Resiliency](#) on page 21.

For information on how to enable **Reserve Rebuild Capacity**, see [Reserving Rebuild Capacity](#) on page 109.

**Note:** The cluster stops accepting Write requests when the resilient capacity limit is reached. For information on cluster resilient capacity, see [Cluster Resilient Capacity](#) on page 105.

## Limitations

You can reserve rebuild capacity subject to the following limitations:

- Nutanix supports rebuild capacity reservation on a cluster with three or more nodes only.
- You cannot reserve rebuild capacity if you have enabled replication factor 1. You cannot enable replication factor 1 if you have reserved rebuild capacity.
- You cannot change the failure domain when rebuild capacity reservation is enabled. To change the failure domain, for example, from node to block you must first disable rebuild capacity reservation. After you change the failure domain you can enable rebuild capacity reservation again. You cannot change the failure domain when Rebuild Capacity Reservation is enabled.

Do not modify the failure domain using APIs when the Rebuild Capacity Reservation is enabled.

## Requirements

You can reserve rebuild capacity subject to the following requirements:

- Prism administrator must ensure that the manual container reservation is already configured on the cluster before configuring rebuild capacity reservation on it.

- Ensure that the cluster has only the default storage pool before you enable rebuild capacity reservation in a cluster. After you enable rebuild capacity reservation, do not create additional storage pools in the cluster.

For more information about storage pools, see [Storage Components](#) on page 102.

- Total capacity used capacity of the cluster must be less than the resilient capacity of the cluster.

If the used capacity approaches the resilient capacity and it increases due to large write operations, internal background jobs or migration tasks, then the used capacity might overshoot the resilient capacity. If rebuild capacity is already reserved on the cluster, the cluster stops accepting write requests.

Total Capacity in the cluster is the sum of resilient capacity and reserved rebuild capacity. Capacity usage, shown as the percentage of resilient capacity changes the color of the bar displaying the used capacity in the **Storage Summary** widget and generates alerts. For example, if the usage is 95 percent or more, then the cluster generates a critical alert after a specified number of NCC check iterations. When you have reserved rebuild capacity and the usage exceeds 95 percent (of the resilient capacity), the cluster stops accepting Write requests.

**Caution:** Enabling Rebuild Capacity Reservation on a cluster with total used space close to the resilient capacity threshold might result in a VM outage. To prevent this, ensure that total used space in the cluster does not exceed 90% of the calculated Resilient Capacity threshold.

- Ensure that features such as erasure coding, de-duplication and compression are not disabled after you enable rebuild capacity reservation. Disabling these features can cause a drastic increase in used capacity beyond 95 percent and put the cluster in read-only mode if the usage was close to the threshold before disabling these features.

**Note:**

Internal background jobs and migration tasks increases the used capacity in a cluster even without write operations running in the cluster. Additionally, heavy write operations on small containers also increases the used capacity. When the used capacity nears the resilient capacity threshold, increase the host capacity in the cluster to prevent the used capacity from reaching or exceeding 95% of the total capacity..

## General Conditions

You can reserve rebuild capacity subject to the following conditions:

- Enabling rebuild capacity reservation reduces the total usable capacity of the cluster from the total capacity to the resilient capacity. As a result, Recycle Bin usage, previously calculated as a percentage of the total usable capacity, is now calculated on the resilient capacity. For more information, see [Recycle Bin](#) on page 146.

For example, if Recycle Bin usage as a percentage of usable capacity is four percent before enabling rebuild capacity reservation, it could change to, 10% of the resilient capacity after enabling rebuild capacity reservation. When rebuild capacity reservation is enabled, Recycle Bin usage as a percentage of resilient capacity is used as the threshold to auto-disable Recycle Bin. This threshold percentage is five percent of the usable (whether Total or resilient) capacity. In the above example, when Curator identifies that the threshold percentage is exceeded during a full scan, the system auto-disables the Recycle Bin.

**Note:** Auto-disabling of Recycle Bin depends on full scans by Curator. Therefore, the excess usage condition of the Recycle Bin could continue for sometime between two full scans before Recycle Bin is disabled.

- Changes in the cluster storage capacity impacts Resilient, Rebuild, Used and Free capacities in the cluster.
  - When you try to remove a host or a disk after rebuild capacity reservation is enabled, the cluster calculates the potential post-removal used capacity and resilient capacity. If the used capacity exceeds the potential resilient capacity, then the host or disk removal fails.
- Therefore, when rebuild capacity reservation is enabled, Prism allows the removal of a node or disk only if the cluster can rebuild data after the removal while maintaining the configured domain's fault tolerance.
- When rebuild capacity reservation is enabled, the data consumption of failed nodes is excluded from the total usage. When rebuild capacity reservation is not enabled, the data consumption of failed nodes is included in the total usage thereby inflating it.
  - When rebuild capacity reservation is enabled, Oplog is accounted in the total usage. Oplog is a persistent write buffer that handles random write bursts. It is designed to provide fast write performance, especially for random I/O workloads.
  - The rebuild process is complete only when cluster fault tolerance is not exceeded. For example, if the failure domain is Node and fault tolerance is  $2N/2D$ , the rebuild process that starts after the first node failure completes successfully. The rebuild process that starts after a second (concurrent) node failure (concurrent) also completes successfully. However, if a third node fails at this stage, the rebuild process starts but does not complete.
  - The rebuild process does not complete if data replicas are unavailable due to reasons such as link failures or disk failures.

## Rebuild Capacity Display

When rebuild capacity is not reserved, the system displays a resilient capacity warning threshold in the **Storage Summary** widget on the **Storage** dashboard. For more information about Resilient Capacity and Warning Threshold configuration, see [Configuring a Warning Threshold for Resilient Capacity](#) on page 106.

For more information about *Resilient Capacity* and *Warning Threshold* configuration, see [Configuring a Warning Threshold for Resilient Capacity](#) on page 106.

To open the **Storage Details** page, click **View Details**. The **Storage Details** page displays a banner about rebuild capacity reservation, along with an **Enable Now** option that opens the **Rebuild Capacity Reservation** page, where you can reserve rebuild capacity.

For information on how to enable rebuild capacity reservation, see [Reserving Rebuild Capacity](#) on page 109.

When you enable rebuild capacity reservation, the cluster calculates the required rebuild capacity based on parameters such as fault tolerance, failure domain, and total storage capacity in the cluster. The reserved rebuild capacity is displayed on the **Rebuild Capacity Reservation** page.

After you reserve rebuild capacity, the system does not display a resilient capacity warning threshold in the **Storage Summary** widget on the **Storage** dashboard. Instead the **Storage Details** page displays a banner informing you that the cluster has reserved rebuild capacity. The details show an additional item - Rebuild Capacity with the capacity reserved in TiB. The capacity numbers change in the **Storage Details** page after the reservation.

## Reserving Rebuild Capacity

You can reserve rebuild capacity in a Nutanix cluster.

### About this task

To reserve rebuild capacity, follow these steps:

### Procedure

1. Log on to the Prism Element web console.

2. From the dropdown menu on the left of the main menu, select **Settings**.  
The system displays the **Global Settings** page.
3. From the **Data Resiliency** section in the left navigation pane, click **Rebuild Capacity Reservation**.  
The system displays the **Rebuild Capacity Reservation** page.
4. Select the **Reserve Rebuild Capacity** checkbox.
5. Click **Save**.  
The system reserves rebuild capacity in the cluster.

## Storage Efficiency

Nutanix provides storage efficient capabilities that allows strategic management of storage resources to maximize capacity utilization, enhance performance, and ensure reliability.

In a Nutanix cluster, where data is distributed across multiple nodes, achieving efficiency is critical to reducing costs, optimizing resource usage, and maintaining scalability.

To minimize redundancy, conserve space, and enhance fault tolerance, a Nutanix cluster supports the following storage efficiency capabilities:

- [Deduplication](#) on page 110
- [Compression](#) on page 111
- [Erasure Coding](#) on page 112

### Deduplication

Deduplication reduces space usage by consolidating duplicate data blocks on Nutanix storage when you enable capacity deduplication on a storage container.

**Important:**

- Deduplication is only supported on clusters with a minimum of three nodes.
- If you enable deduplication on storage containers with protected VMs, the system lowers the replication speed.
- Nutanix recommends that you do not enable deduplication for VAAI clone or linked clone environments.

### Capacity Deduplication

Capacity deduplication refers to deduplication performed on data stored in hard disk drives (HDDs). Enabling capacity deduplication for persistent data helps reduce storage usage.

**Note:**

- Capacity deduplication is not enabled by default.
- Capacity deduplication is available if you have purchased a Nutanix Cloud Infrastructure (NCI) Starter or higher license.

**Important:**

- The on-disk deduplication feature might be auto-disabled on fresh AOS 7.3 deployments having clusters eligible for certain Curator scans when the dense\_node capacity exceeds 92 TB per node.

- Nutanix recommends that you configure the Controller VMs with at least 32 GiB of RAM and 300 GiB SSDs for the metadata disk to enable capacity deduplication.

## How to enable Deduplication

The **Capacity** deduplication property is enabled at the storage container level. These storage container properties can be set in the Prism Element web console or through nCLI.

## Deduplication Best Practices

The following table provides the scenarios where deduplication is recommended and where it is not recommended:

Enable deduplication	Do not enable deduplication
<ul style="list-style-type: none"> <li>Full clones</li> <li>Physical-to-virtual (P2V) migration</li> <li>Persistent desktops</li> </ul>	<ul style="list-style-type: none"> <li><i>Linked clones or Nutanix VAAI clones:</i> Duplicate data is managed efficiently by DSF so deduplication has no additional benefit</li> <li><i>Server workloads:</i> Redundant data is minimal so may not see significant benefit from deduplication</li> </ul>

## Compression

You can enable compression on a storage container to save physical storage space, improve I/O bandwidth, and optimize memory usage thereby enhancing overall system performance.

**Note:** If the metadata usage is high, compression is automatically disabled. If compression is automatically disabled, an alert is generated.

A storage container in a Nutanix cluster supports the following types of compression:

### Post-process compression

Data is compressed after it is written. The delay time between write and compression is configurable, and Nutanix recommends a delay of 60 minutes.

### Inline compression

Data is compressed as it is written. When you create a new storage container, inline compression is enabled by default for all license tiers. It is set to a delay of 0, compressing data immediately as it is written.

## Viewing Compression Ratios

You can view compression ratios and usage savings in the Prism Element web console.

## Compression Ratios

- Cluster*

In the **Storage** dashboard, under **Capacity Optimization**, click the **After** bar, and hover your mouse over **Compression**.

- Storage container*

In the **Storage** dashboard **Table** view, on the **Storage Container** tab, click the storage container for which you want to view the compression ratio. You can see the compression ratio for the selected storage container under **Storage Container Details**.

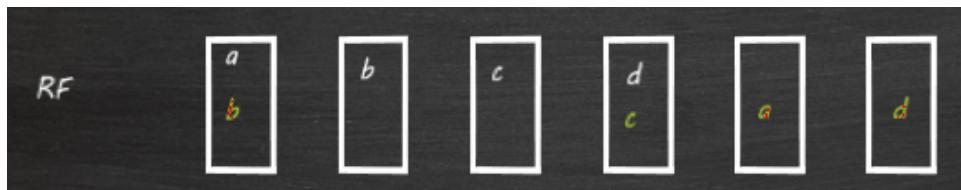
## Erasure Coding

Erasure coding increases the usable capacity of a cluster. Instead of replicating data, erasure coding uses parity information to rebuild data in the event of a disk failure. The capacity savings of erasure coding are in addition to deduplication and compression savings.

**Important:** Erasure coding is supported on clusters with a minimum of 4 nodes when using replication factor 2 and a minimum of 6 nodes when using replication factor 3.

If you have configured 1N/1D cluster fault tolerance, two data copies are maintained. For example, consider a 6-node cluster with 4 data blocks (a b c d). In this example, we start with 4 data blocks (a b c d) configured with 1N/1D cluster fault tolerance.

The white text represents the data blocks and the green text represents the copies.



**Figure 26: Data copies before Erasure Coding**

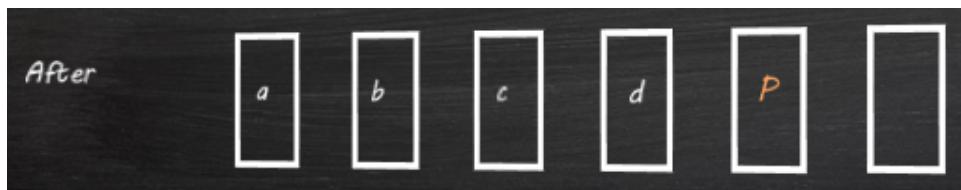
When the data becomes cold, the erasure code engine performs an exclusive OR operation to compute parity “P” for the data.

$$a \ b \ c \ d = P \text{ (parity)}$$

**Figure 27: During Computing Parity**

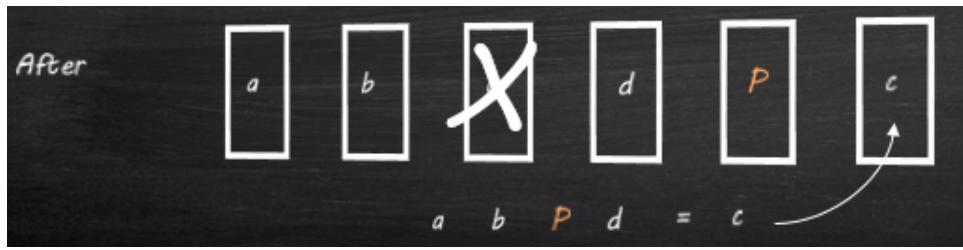
After parity is computed, the data block copies are removed and replaced with the parity information. Redundancy through parity results in data reduction because the total data on the system is now  $a+b+c+d+P$  instead of  $2 \times (a+b+c+d)$ .

**Note:** Each block in the stripe is placed on a separate node to protect from a single node failure.



**Figure 28: After Computation of Parity**

If the node that contains data block c fails, block c is rebuilt using the rest of the erasure coded stripe (a b d and P) as displayed in the following example:



**Figure 29: Post Node Failure**

Block c is then placed on a node that does not have any other members of this erasure coded stripe.

**Note:** When the cluster is configured with 2N/2D cluster fault tolerance, two parity blocks are maintained so that the erasure coded data has the same resiliency as the replicated data. An erasure coded stripe with two parity blocks can handle the failure of two nodes.

### Example of Data Reduction Savings from Erasure Coding

The space savings from the erasure coding depends on the cluster size, cluster fault tolerance setting, and percentage of cold data.

The sixth node in the cluster ensures that if a node fails, another node is available for rebuild.

STORAGE CONTAINER DETAILS	
Name	dp-cmp-inl-ec
Replication Factor	2
Free Capacity (Physical)	<b>58.08 TiB</b>
Used (Physical)	<b>12.21 GiB</b>
Snapshot	790.52 MiB
Max Capacity	<b>58.1 TiB</b>
Reserved	0 GiB
Data Reduction Ratio	<b>6.41 : 1</b>
Data Reduction Savings	44.03 GiB
Effective Free	<b>372.32 TiB</b>
Overall Efficiency	<b>26.95 : 1</b>
Compression	On
Capacity Deduplication	On
Erasure Coding	On
Filesystem Allowlists	None

Erasure Coding ratio: 1.13 : 1  
 Usage Savings: 1.06 GiB

**Figure 30: Storage Container Summary: Usage Savings Screen**

In a 6-node cluster configured with replication factor 2, erasure coding uses a stripe size of 5 where 4 nodes are for data and 1 node is for parity. The sixth node in the cluster ensures that if a node fails, another node is available for rebuild. You can view the erasure coding usage savings from the storage container summary.

Erasure coding stripe size adapts to the size of the cluster, starting with a minimum 4 nodes and a maximum stripe width of 5 nodes. The following is an example displaying the various configurations of cluster size, possible stripe widths, and approximate savings that might occur when erasure coding is enabled.

	Cluster Size	Raw	Usable	After Erasure
	4 nodes	80 TB	40 TB	$\sim 53 \text{ TB}$ $80/1.5 = \sim 53$
	5 nodes	100 TB	50 TB	$\sim 75 \text{ TB}$ $100/1.33 = 75$
	6 nodes	120 TB	60 TB	$\sim 96 \text{ TB}$ $120/1.25 = 96$
	7 nodes	140 TB	70 TB	$\sim 112 \text{ TB}$ $140/1.25 = 112$

Node avoided by Data or Parity
Node used for Parity
Node used for Data

**Figure 31: Example of Space Saving from Erasure Coding on 20 TiB Nodes**

### Erasure Coding Best Practices and Requirements

Nutanix recommends the following best practices and requirements to implement Erasure Coding:

- A cluster must have at least four nodes/blocks/racks to enable erasure coding. The cluster can have all four flash nodes or a combination of flash and hybrid nodes, or all hybrid nodes. If erasure coding is enabled on a storage container, a minimum of four blocks for replication factor 2 or six blocks for replication factor 3 is required to maintain block awareness.
- The following table provides the information about the recommended minimum configuration for multiple node removal operations:

**Table 29: Minimum Recommended Configuration for Erasure Coding**

Desired Awareness Type	Cluster Fault Tolerance	Min. Units	Simultaneous Failure Tolerance
Node	1N/1D	4 nodes	1 node
Node	2N/2D	6 nodes	2 nodes
Block	1N/1D	4 blocks	1 block
Block	2N/2D	6 blocks	2 blocks
Rack	1N/1D	4 racks	1 rack
Rack	2N/2D	6 racks	2 racks

**Note:** Ensure that you maintain a cluster size that is at least one node greater than the combined strip size (data + parity) to allow space to rebuild the strips if a node fails.

- AOS dynamically calculates the erasure coding strip sizes depending on the number of nodes, blocks, and racks. The maximum supported and recommended strip sizes are (4,1) or (4,2), depending on the nodes, blocks, and racks. Nutanix recommends that you do not change the strip size. Greater strip sizes increase the space savings; however, they also increase the cost of rebuild.
- Erasure coding effectiveness (data reduction savings) might reduce on workloads that have many overwrites outside of the erasure coding window. The default value for erasure coding window is seven days for write cold.
- Read performance is affected during rebuild and the amount depends on cluster strip size and read load on the system.

- Erasure coding is an asynchronous process, and hence the time taken to calculate and display space savings depends on the type and coldness of data. A minimum of two full Curator scans are required to calculate the data savings.
- Ensure that you have replication factor+1 storage heavy or storage only nodes for all-flash clusters with storage heavy nodes. For example, if you have a four-node replication factor 2 enabled cluster, then you must add a minimum of three storage heavy nodes for optimum performance.

## Inline Erasure Coding

Inline erasure coding creates erasure coding strips by erasure coding data without waiting for the data to become write cold.

There are two types of inline erasure coding:

- *Same vDisk strips*: Strips that are created using the data blocks from the same vDisk. Nutanix recommends that you configure inline erasure coding type as same vDisk strips for workloads that do not require data locality.
- *Cross vDisk strips*: Strips that are created using the data blocks across multiple vDisks. Nutanix recommends that you configure inline erasure coding type as cross vDisk strips for workloads that require data locality.

By default, same vDisk strips are created when you enable inline erasure coding.

**Note:** Inline erasure coding with same vDisk strips can be enabled for clusters running AOS version 5.18 or later; and with cross vDisk strips can be enabled for clusters running AOS version 6.6 or later versions.

## Enabling Inline Erasure Coding

Inline erasure coding can be enabled only using nCLI. Inline erasure coding is added as a storage container parameter in Zeus.

### Before you begin

**Caution:**

- Nutanix recommends that you enable inline erasure coding for Object storage containers only. To enable inline erasure coding for any other type of storage container, contact Nutanix Support.
- Erasure coding must be enabled on the container to enable inline erasure coding. For information about how to enable erasure coding, see [Creating a Storage Container](#).

### Procedure

To enable inline erasure coding, perform the following actions:

- Run the following nCLI command:

```
ncli> container create name=container_name sp-id=storage_pool_id erasure-code=on
      inline-ec-enabled=true
```

Replace `container_name` and `storage_pool_id` with the storage container name and storage pool ID on which you want to enable erasure coding.

- To explicitly configure inline erasure coding type, run the following nCLI commands:

- For inline erasure coding type: *Same vDisk strips*

```
ncli> container create name=container_name sp-id=storage_pool_id erasure-
      code=on inline-ec-enabled=true inline-ec-type=same-vdisk-strips
```

- For inline erasure coding type: *Cross vDisk strips*

```
ncli> container create name=container_name sp-id=storage_pool_id erasure-
      code=on inline-ec-enabled=true inline-ec-type=cross-vdisk-strips
```

Replace `container_name` and `storage_pool_id` with the storage container name and storage pool ID on which you want to enable erasure coding.

- To change an existing inline erasure coding type, run the following ncli commands:

- To change to *Same vDisk strips*:

```
ncli> container edit inline-ec-enabled=true inline-ec-type=same-vdisk-strips
      id=container_id
```

- To change to *Cross vDisk strips*:

```
ncli> container edit inline-ec-enabled=true inline-ec-type=cross-vdisk-strips
      id=container_id
```

Replace `container_id` with the ID of the storage container.

- To verify if inline erasure coding is enabled, run the following nCLI command:

```
ncli> container ls name=container_name
```

Replace `container_name` with the name of the storage container on which you enabled inline erasure coding.

The system displays `Inline EC Enabled : true` if inline erasure coding is enabled.

## Storage Dashboard

The Storage dashboard displays dynamically updated information about the storage configuration in a cluster.

### Storage Overview View

The Storage Overview dashboard provides a dynamic summary view of the performance and usage statistics, and alert and event messages of the containers in the cluster. For information about how the statistics are derived, see [Understanding Displayed Statistics](#) on page 69.

#### Table 30: Storage Overview Widgets

The following table describes the widgets that appear on the Storage Overview dashboard.

Name	Description
Storage Summary	<p>Displays information about the physical storage space utilization (in GiB or TiB) and resilient capacity of the cluster.</p> <p>Hovering over the green bar displays a detailed view of storage capacity usage.</p> <p>Click the <b>View Details</b> option to view the resiliency status and storage information of all the individual nodes in the cluster. For more information, see <a href="#">Storage Details Page</a> on page 119.</p> <p>Click the settings icon to configure a threshold warning for the resilient capacity utilization in the cluster. For more information, see <a href="#">Configuring a Warning Threshold for Resilient Capacity</a> on page 106.</p>
Storage Containers	Displays the number of storage containers, VMs, and hosts on which the storage containers are mounted in the cluster.
Capacity Optimization	Displays the data reduction ratio (compression, deduplication, and erasure coding), data reduction savings (compression, deduplication, and erasure coding), and the overall efficiency of the container gained by enabling compression, deduplication, and erasure coding features.
Cluster-wide Controller IOPS	<p>Displays I/O operations per second (IOPS) in the cluster.</p> <p>The time period displayed is a rolling interval that varies from one to several hours depending on activity moving from right to left. Hovering the cursor anywhere on the horizontal axis displays the value at that time. (These display features also apply to the I/O bandwidth and I/O latency monitors.)</p>
Cluster-wide Controller IO B/ W	<p>Displays I/O bandwidth used per second in the cluster.</p> <p>The value is displayed in an appropriate metric (MBps, KBps, and so on) depending on traffic volume. For more in depth analysis, you can add this chart (and any other charts on the page) to the analysis page by clicking the blue <b>Add chart to analysis page</b> link in the upper left of the chart. For more information, see <a href="#">Analysis Dashboard</a> on page 330.</p>
Cluster-wide Controller Latency	Displays the average I/O latency (in milliseconds) in the cluster.
Cache Deduplication	<p><b>Note:</b> Cache deduplication is not supported in AOS 6.6 and later versions.</p>
Storage Critical Alerts	Displays the five most recent unresolved storage-specific critical alert messages. Click a message to open the Alert screen of that message. You can also open the Alert screen by clicking the <b>view all alerts</b> button at the bottom of the list. For more information, see <a href="#">Alerts Dashboard</a> in <i>Prism Element Alerts and Events Reference Guide</i> .
Storage Warning Alerts	Displays the five most recent unresolved storage-specific warning alert messages. Click a message to open the Alert screen at that message. You can also open the Alert screen by clicking the <b>view all alerts</b> button at the bottom of the list.
Storage Events	Displays the ten most recent storage-specific event messages. Click a message to open the Event screen at that message. You can also open the Event screen by clicking the <b>view all events</b> button at the bottom of the list.

Name	Description
Storage Over-provisioning	Displays the storage over-provisioning ratio (calculated based on the provisioned storage and the available raw storage) in the cluster. Note that the time taken for the <b>Storage Over-provisioning Ratio</b> widget to reflect the changes made in the cluster varies according to the recent storage operations or activities performed.

### Storage Details Page

The Storage Details page displays the resiliency status and physical storage information of all the individual nodes in the cluster.

The Storage Details page is divided into two sections:

- The right section displays a diagrammatic representation of the number of nodes present in the cluster along with the respective storage capacity used.
- The left section provides detailed storage information of the cluster.

The following table describes the storage parameters that appear on the Storage Details page.

Parameter	Description	Values
Failure Domain	Displays the entity (node, block, or rack) the failure of which, the cluster can tolerate while still running guest VMs and responding to commands through the Prism Element web console.	node, block, or rack
Total Capacity	Displays the total capacity of all the disks on all the hosts in the cluster.	xxx [GiB TiB]
Resilient Capacity	Displays the total resilient capacity of the cluster.	xxx [GiB TiB]

Parameter	Description	Values
Total Usage	<p>Displays the sum of all the storage space used by the cluster.</p> <p>The total usage is calculated based on the following:</p> <ul style="list-style-type: none"> <li>• <b>Used Capacity:</b> The amount of used storage space in the cluster (by user data).</li> <li>• <b>Recovery Points:</b> The capacity occupied by images, clones and recovery points of VMs and volume groups.</li> <li>• <b>Recycle Bin:</b> The capacity is occupied by deleted VMs and volume groups, which are automatically purged after 24 hours. In the event of capacity constraints, this capacity is cleared by the system to service the incoming 10s.</li> <li>• <b>Others:</b> Capacity occupied by VM, VG Disks, and Images.</li> </ul>	xxx [GiB TiB]
Available Capacity	Displays the available storage capacity on all the disks on all the hosts in the cluster.	xxx [GiB TiB]

## Storage Diagram View

The Storage Diagram view displays information about the physical usage of storage pools and storage containers. The displayed information is dynamically updated to remain current.

The Storage Diagram view screen is divided into two sections:

- The top section is a cascading diagram of the storage units. Initially, a cluster bar appears with storage information about the cluster (used, provisioned, and available storage). You can configure a threshold warning for the resilient capacity utilization in the cluster by clicking the gear icon to the right of the cluster bar. For information, see [Configuring a Warning Threshold for Resilient Capacity](#) on page 106. Clicking on a cluster bar displays storage information about the physical usage of storage pool (used, provisioned, and available storage) and bar with colored blocks for each storage container in that storage pool. Clicking on a storage pool block displays storage information about the storage container and a bar for that storage container. You can edit a storage pool or storage container by clicking the pencil (edit) or X (delete) icon to the right of the name. Clicking the **close** link at the far right hides that storage pool or storage container bar from the display.
- The bottom **Summary** section provides additional information. It includes a details column on the left and a set of tabs on the right. The details column and tab content varies depending on what has been selected.

**Note:** For information about how the statistics are derived, see [Understanding Displayed Statistics](#) on page 69.

### Storage Container Details

Selecting a storage container in the diagram displays information about that storage container in the lower section of the screen.

- When a storage container is selected, **Summary: storage\_container\_name** appears below the diagram, and action links appear on the right of this line:
  - Click the **Update** link to update the settings for this storage container.
  - Click the **Delete** link to delete this storage container configuration.
 For more information about these actions, see [Modifying a Storage Container](#) on page 135.
- In the **Summary: storage\_container\_name** table, hover your mouse over the value to see additional details of that parameter.
- Four tabs appear that display information about the selected storage container (see following sections for details about each tab): **Storage Container Usage**, **Storage Container Performance**, **Storage Container Alerts**, **Storage Container Events**.

**Table 31: Storage Container Details Fields**

Parameter	Description	Values
Name	Displays the name of the storage container.	(name)
Replication Factor	Displays the replication factor, which is the number of maintained data copies. The replication factor is specified when the storage container is created.	[1,2,3]
Protection Domain	Displays the name of the protection domain if you have configured a protection domain for that storage container.	(name)
Datastore	Displays the name of the datastore.	(name)
VMs	Displays the number of VMs	(number)
Free Space (Physical)	Displays the amount of free physical storage space available to the storage container that is unreserved.	xxx [GB TB]
Used (Physical)	Displays the amount of used physical storage space in the storage container, including space used by Snapshots and Recycle Bin.	xxx [GB TB]
Max Capacity	Displays the total amount of storage capacity available to the storage container. Nutanix employs a <i>thin</i> provisioning model when allocating storage space, which means space is assigned to a storage container only when it is actually needed. The maximum capacity value reflects the total available storage regardless of how many storage containers are defined. Therefore, when you have two storage containers, it can appear that you have twice as much capacity because maximum capacity for both storage containers show the full amount. Maximum capacity is calculated as the total physical capacity in the storage pool, minus any reserved capacity, minus space used by other storage containers.	xxx [TB]
Reserved	Displays the amount of reserved physical storage space in the storage container.	xxx [GB TB]

Parameter	Description	Values
Data Reduction Ratio	Displays the ratio of how much the data size is reduced by enabling compression, deduplication, and erasure coding.	
Data Reduction Savings	Displays the data reduction savings by enabling compression, deduplication, and erasure coding.	
Effective Free	Displays the amount of usable free space after data reduction.	
Overall Efficiency	Displays the capacity optimization (as a ratio) that results from the combined effects of data reduction (deduplication, compression, and erasure coding), cloning, and thin provisioning.	
Compression	Displays whether compression is enabled.	[Off On]
Capacity Deduplication	Displays whether on disk deduplication is enabled on hard disks (HDD).	[Off On]
Erasure Coding	Displays whether erasure coding is enabled.	[On, Off]
Filesystem Whitelists	Displays whether you have configured filesystem whitelist for this storage container.	[None, On, Off]

### Storage Pool Details

Selecting a storage pool in the diagram displays information about that storage pool in the lower section of the screen.

- When a storage pool is selected, **Summary:** `storage_pool_name` appears below the diagram, and action links appear on the right of this line:
  - Click the **Update** link to update the settings for this storage pool.  
For more information about this action, see [Modifying a Storage Container](#) on page 135.
- Four tabs appear that display information about the selected storage pool (see following sections for details about each tab): **Storage Pool Usage**, **Storage Pool Performance**, **Storage Pool Alerts**, **Storage Pool Events**.

**Table 32: Storage Pool Details Fields**

Parameter	Description	Values
Name	Displays the name of the storage pool.	(name)
Free (Physical)	Displays the total amount of physical storage space that is available.	xxx [GB TB]
Used (Physical)	Displays the total amount of physical storage space used in the storage pool.	xxx [GB TB]
Capacity (Physical)	Displays the total physical storage space capacity in the storage pool.	xxx [TB]
Disk Count	Displays the number of disks in the storage pool.	(number)

## Cluster Summary Information

When a storage container or storage pool is not selected in the table (or when the word **Summary** is clicked), cluster-wide summary information appears in the lower part of the screen.

- The **Storage Summary** column (on the left) includes five fields:
  - **Free (Physical)**. Displays the amount of physical storage space still available in the cluster.
  - **Used (Physical)**. Displays the amount of physical storage space used currently in the cluster, including the Recycle Bin.
  - **Capacity (Physical)**. Displays the total physical storage capacity in the cluster.
  - **Storage Pool(s)**. Displays the names of the storage pool. Clicking on a name displays the detail information for that storage pool in this section.
  - **Storage Container(s)**. Displays the names of the storage containers. Clicking on a name displays the detail information for that storage container in this section.
- Four tabs appear that display cluster-wide information (see following sections for details about each tab): **Usage Summary**, **Performance Summary**, **Storage Alerts**, **Storage Events**.

### Usage Tab

The Usage tab displays graphs of storage usage. The tab label varies depending on what is selected in the table:

- **Usage Summary** (no storage pool or storage container selected). Displays usage statistics across the cluster.
- **Storage Container Usage** (storage container selected). Displays usage statistics for the selected storage container.
- **Storage Pool Usage** (storage pool selected). Displays usage statistics for the selected storage pool.

The Usage tab displays the following two graphs:

- **Cluster-wide Usage Summary**: Displays a rolling time interval usage monitor that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see [Analysis Dashboard](#) on page 330.
- **Tier-wise Usage**: Displays a pie chart divided into the percentage of storage space used by each disk tier in the cluster, storage pool, or storage container. Disk tiers can include DAS-SATA, SSD-SATA, and SSD-PCIe depending on the Nutanix model type.

### Performance Tab

The Performance tab displays graphs of performance metrics. The tab label varies depending on what is selected in the table:

- **Performance Summary** (no storage pool or storage container selected). Displays storage performance statistics across the cluster.
- **Storage Container Performance** (storage container selected). Displays storage performance statistics for the selected storage container.
- **Storage Pool Performance** (storage pool selected). Displays storage performance statistics for the selected storage pool.

The graphs are rolling time interval performance monitors that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time.

For more in depth analysis, you can add a monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see [Analysis Dashboard](#) on page 330. The Performance tab includes the following three graphs:

- **[Cluster-wide Hypervisor|Controller|Disk] IOPS:** Displays I/O operations per second (IOPS) for the cluster, selected storage container, or selected storage pool.
- **[Cluster-wide Hypervisor|Controller|Disk] I/O Bandwidth:** Displays I/O bandwidth used per second (MBps or KBps) for physical disk requests in the cluster, selected storage container, or selected storage pool.
- **[Cluster-wide Hypervisor|Controller|Disk] I/O Latency:** Displays the average I/O latency (in milliseconds) for physical disk requests in the cluster, selected storage container, or selected storage pool.

### Storage Alerts Tab

The Alerts tab displays the unresolved alert messages about storage pools or storage containers in the same form as the Alerts page. For more information, see [Alerts Summary View](#). Click the **Unresolved X** button in the filter field to also display resolved alerts.

### Storage Events Tab

The Events tab displays the unacknowledged event messages about storage pools or storage containers in the same form as the Events page. For more information, see [Events Summary View](#). Click the **Include Acknowledged** button to also display acknowledged events.

## Storage Table View

The Storage Table view displays information about storage pools and storage containers in a tabular form. Click the **Volume Group** tab to display volume group information; click the **Storage Pool** tab in the screen menu bar to display storage pool information; click the **Storage Container** tab to display storage container information. The displayed information is dynamically updated to remain current.

The Storage Table view is divided into two sections:

- The top section is a table. Each row represents a single volume group, storage pool, or storage container and includes basic information about that entity. Click a column header to order the rows by that column value (alphabetically or numerically as appropriate).
- The bottom **Summary** section provides additional information. It includes a details column on the left and a set of tabs on the right. The details column and tab content varies depending on what has been selected.

**Note:** For more information about how the statistics are derived, see [Understanding Displayed Statistics](#) on page 69.

### Volume Group tab

Clicking the Volume Group tab displays information about volume groups in the cluster.

- The table at the top of the screen displays information about all the configured volume groups, and the details column (lower left) displays additional information when a volume group is selected in the table. The following table describes the fields in the volume group table and detail column.

- When a volume group is selected, Summary: `volume_group_name` appears below the table, and action links appear on the right of this line:
  - Click the **Update** link to update the settings for this volume group.
  - Click the **Delete** link to delete this volume group.

For more information about these actions, see [Modifying a Volume Group](#) on page 142.

Five tabs appear that display information about the selected volume group (see following sections for details about each tab): Performance Metrics, Virtual Disks, Volume Group Tasks, Volume Group Alerts, and Volume Group Events.

**Table 33: Volume Group Table and Detail Fields**

Parameter	Description	Values
<i>Volume Group Table Fields</i> (upper screen)		
Name	Displays the name of the volume group.	(name)
Disks	Displays the number of disks in the volume group.	[0–256]
Controller IOPS	Displays the current I/O operations per second (IOPS) for the volume group. The controller IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by the Controller VM. The I/O can be served from memory, cache (SSD), or disk.	[0 - unlimited]
Controller IO B/W	Displays I/O bandwidth used per second for Controller VM-serviced requests in this volume group.	xxx [MBps KBps]
Controller IO Latency	Displays the average I/O latency for Controller VM-serviced requests in this volume group.	xxx [ms]
<i>Volume Group Details Fields</i> (lower screen)		
Name	Displays the name of the volume group.	(name)
Number of Virtual Disks	Displays the number of virtual disks in the volume group.	[0–256]
Total Size	Displays the total size of the volume group.	xxx [GB TB]
Flash Mode	Displays whether the flash mode is enabled.	
Shared	Indicates whether the volume group is shared across iSCSI initiators.	[Yes No]
Initiators	Displays the iSCSI initiators to which the volume group is attached.	(None List of names)
Storage Container	Displays the name of the storage container to which the volume group belongs.	(name)
Target IQN Prefix	Displays the IQN prefix of the target iSCSI.	

## Storage Container Tab

Clicking the **Storage Container** tab displays information about storage containers in the cluster (see [Creating a Storage Container](#) on page 131).

- The table at the top of the screen displays information about all the configured storage containers, and the details column (lower left) displays additional information when a storage container is selected in the table. The following table describes the fields in the storage container table and detail column.
- When a storage container is selected, **Summary: storage\_container\_name** appears below the table, and action links appear on the right of this line:
  - Click the **Update** link to update the settings for this storage container.
  - Click the **Delete** link to delete this storage container configuration.For more information about these actions, see [Modifying a Storage Container](#) on page 135.
- Four tabs appear that display information about the selected storage container (see following sections for details about each tab): **Storage Container Breakdown**, **Storage Container Usage**, **Storage Container Performance**, **Storage Container Alerts**, **Storage Container Events**.

**Table 34: Storage Container Table and Detail Fields**

Parameter	Description	Values
<i>Storage Container Table Fields</i> (upper screen)		
Name	Displays the name of the storage container.	(name)
Encrypted	Displays the encryption status of the storage container.	[Yes  No]
Replication Factor	Displays the replication factor, which is the number of maintained data copies. The replication factor is specified when the storage container is created.	[1,2,3]
Compression	Displays whether compression is enabled.	[Off On]
Capacity Deduplication	Displays whether on disk deduplication is enabled on hard disks (HDD).	[On, Off]
Erasure Coding	Displays whether erasure coding is enabled for the storage container or not	[On, Off]
Free Capacity (Physical)	Displays the amount of free physical storage space in the storage container.	xxx [GB TB]
Used Capacity (Physical)	Displays the amount of used physical storage space in the storage container, including space used by the Recycle Bin.	xxx [GB TB]
Reserved Capacity (Physical)	Displays the amount of reserved physical storage space in the storage container.	xxx [GB TB]

Parameter	Description	Values
Max Capacity (Physical)	Displays the total amount of physical storage capacity available to the storage container. Nutanix employs a <i>thin</i> provisioning model when allocating storage space, which means space is assigned to a storage container only when it is actually needed. The maximum capacity value reflects total available storage regardless of how many storage containers are defined. Therefore, when you have two storage containers, it can appear you have twice as much capacity because maximum capacity for both storage containers show the full amount. Maximum capacity is calculated as the total physical capacity in the storage pool, minus any reserved capacity, minus space used by other storage containers.	xxx [TB]
Controller IOPS	Displays the current I/O operations per second (IOPS) for the storage container. The controller IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by the Controller VM. The I/O can be served from memory, cache (SSD), or disk.	[0 - unlimited]
Controller IO B/W	Displays I/O bandwidth used per second for Controller VM-serviced requests in this storage container.	xxx [MBps KBps]
Controller IO Latency	Displays the average I/O latency for Controller VM-serviced requests in this storage container.	xxx [ms]
<i>Storage Container Details Fields</i> (lower screen)		
Name	Displays the name of the storage container.	(name)
Encrypted	Displays the encryption status of the storage container.	
Protection Domain	Displays the data protection domain used for the storage container.	(DR name)
VMs	Displays the number of VMs associated with the storage container.	xxx
Free Capacity (Physical)	Displays the amount of free physical storage space available to the storage container that is unreserved.	xxx [GB TB]
Used (Physical)	Displays the amount of used physical storage space for the storage container.	xxx [GB TB]
Snapshot	The total storage capacity in the cluster consumed by snapshots (sum of both local and remote).	xxx [GB TB]
Max Capacity	Displays the total amount of storage capacity available to the storage container (see the Max Capacity (Physical) for description).	xxx [TB]
Reserved	Displays the total reserved storage capacity in the storage container.	xxx [GB TB]
Replication Factor	Displays the replication factor, which is the number of maintained data copies. The replication factor is specified when the storage container is created.	[1, 2, 3]
Compression	Displays whether compression is enabled.	[Off On]

Parameter	Description	Values
Data Reduction Ratio	Displays the ratio of how much the data size is reduced by enabling compression, deduplication, and erasure coding.	x.xx : 1
Data Reduction Savings	Displays the data reduction savings by enabling compression, deduplication, and erasure coding.	xxx [GB TB]
Effective Free	Displays the amount of usable free space after data reduction.	xxx [GB TB]
Overall Efficiency	Displays the capacity optimization (as a ratio) that results from the combined effects of data reduction (deduplication, compression, and erasure coding), cloning, and thin provisioning.	xxx [GB TB]
Capacity Deduplication	Displays whether on disk deduplication is enabled, that is dedup compression applied to data on hard disks (HDD).	[On, Off]
Filesystem Allowlists	Displays whether you have configured filesystem allowlist for this storage container.	[None, On, Off]
Erasure Coding	Displays whether erasure coding is enabled or not.	[On, Off]

### Storage Pool Tab

Clicking the **Storage Pool** tab displays information about storage pools in the cluster.

- The table at the top of the screen displays information about the storage pool, and the details column (lower left) displays additional information when a storage pool is selected in the table. The following table describes the fields in the storage pool table and detail column.
- When a storage pool is selected, **Summary: *storage\_pool\_name*** appears below the table, and action links appear on the right of this line:
  - Click the **Update** link to update the settings for this storage pool.
 For more information about these actions, see [Modifying a Storage Pool](#) on page 131.
- Four tabs appear that display information about the selected storage pool (see following sections for details about each tab): **Storage Pool Usage**, **Storage Pool Performance**, **Storage Pool Alerts**, **Storage Pool Events**.

**Table 35: Storage Pool Table and Detail Fields**

Parameter	Description	Values
<i>Storage Pool Table Fields</i> (upper screen)		
Name	Displays the name of the storage pool.	(name)
Disks	Displays the number of disks in the storage pool.	(number)
Free (Physical)	Displays the total amount of physical storage space that is available.	xxx [GB TB]
Used (Physical)	Displays the total amount of physical storage space used in the storage pool.	xxx [GB TB]

Parameter	Description	Values
Max Capacity (Physical)	Displays the total physical storage space capacity in the storage pool.	xxx [TB]
Disk IOPS	Displays the current I/O operations per second (IOPS) for the storage pool. The IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by physical disks across the storage pool.	[0 - unlimited]
Disk IO B/W	Displays the I/O bandwidth used per second for physical disk requests in this storage pool.	xxx [MBps KBps]
Disk Avg IO Latency	Displays the average I/O latency for physical disk requests in this storage pool.	xxx [ms]
<i>Storage Pool Details Fields</i> (lower screen)		
Name	Displays the name of the storage pool.	(name)
Free (Physical)	Displays the total amount of physical storage space that is available.	xxx [GB TB]
Used (Physical)	Displays the total amount of physical storage space used in the storage pool.	xxx [GB TB]
Capacity (Physical)	Displays the total physical storage space capacity in the storage pool.	xxx [TB]
Disk Count	Displays the number of disks in the storage pool.	(number)

### Cluster Summary Information

When a storage pool, storage container, or volume group is not selected in the table (or when the word **Summary** is clicked), cluster-wide summary information appears in the lower part of the screen.

- The **Storage Summary** column (on the left) includes five fields:
  - Available (Physical)**. Displays the amount of physical storage space still available in the cluster.
  - Used (Physical)**. Displays the amount of physical storage space used currently in the cluster.
  - Capacity (Physical)**. Displays the total physical storage capacity in the cluster.
  - Storage Pool**. Displays the name of the storage pool in the cluster. Clicking the name displays detailed information about the storage pool in this section.
  - Storage Container(s)**. Displays the names of the storage containers. Clicking a name displays detailed information about that storage container in this section.
- Four tabs appear that display cluster-wide information (see following sections for details about each tab): **Usage Summary**, **Performance Summary**, **Storage Alerts**, **Storage Events**.

### Breakdown Tab

The **Breakdown** tab is displayed in the **Summary** section only when a storage container is selected from the storage container table.

The **Breakdown** tab displays the type (VM or VG), list of virtual disks, the amount of allocated space, and storage space utilized by each in the selected storage container.

## Usage Tab

The Usage tab displays graphs of storage usage. The tab label varies depending on what is selected in the table:

- **Usage Summary** (no storage pool, storage container, or volume group selected). Displays usage statistics across the cluster.
- **Storage Container Usage** (storage container selected). Displays usage statistics for the selected storage container.
- **Storage Pool Usage** (storage pool selected). Displays usage statistics for the selected storage pool.
- **Volume Group Usage** (volume group selected). Displays usage statistics for the selected volume group.

The Usage tab displays the following two graphs:

- **Usage Summary**: Displays a rolling time interval usage monitor that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see [Analysis Dashboard](#) on page 330.
- **Tier-wise Usage**: Displays a pie chart divided into the percentage of storage space used by each disk tier in the cluster, storage pool, or storage container. Disk tiers can include DAS-SATA, SSD-SATA, and SSD-PCIe depending on the Nutanix model type.

## Performance Tab

The Performance tab displays graphs of performance metrics. The tab label varies depending on what is selected in the table:

- **Performance Summary** (no storage pool, storage container, or volume group selected). Displays storage performance statistics across the cluster.
- **Storage Container Performance** (storage container selected). Displays storage performance statistics for the selected storage container.
- **Storage Pool Performance** (storage pool selected). Displays storage performance statistics for the selected storage pool.
- **Volume Group Performance** (volume group selected). Displays storage performance statistics for the selected volume group.

The graphs are rolling time interval performance monitors that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add a monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see [Analysis Dashboard](#) on page 330. The Performance tab includes the following three graphs:

- **[Cluster-wide Hypervisor|Controller|Disk] IOPS**: Displays I/O operations per second (IOPS) for the cluster, selected storage container, selected storage pool, or selected volume group.
- **[Cluster-wide Hypervisor|Controller|Disk] I/O Bandwidth**: Displays I/O bandwidth used per second (MBps or KBps) for physical disk requests in the cluster, selected storage container, selected storage pool, or selected volume group.
- **[Cluster-wide Hypervisor|Controller|Disk] I/O Latency**: Displays the average I/O latency (in milliseconds) for physical disk requests in the cluster, selected storage container, selected storage pool, or selected volume group.

## Alerts Tab

The Alerts tab displays the unresolved alert messages about storage pools, storage containers, or volume groups in the same form as the Alerts page. For more information, see [Alerts Summary View](#). Click the **Unresolved X** button in the filter field to also display resolved alerts.

## Events Tab

The Events tab displays the unacknowledged event messages about storage pools, storage containers, or volume groups in the same form as the Events page. For more information, see [Events Summary View](#). Click the **Include Acknowledged** button to also display acknowledged events.

# Modifying a Storage Pool

This section describes how to modify a storage pool in the cluster.

## About this task

You can only modify the name of the storage pool in the cluster. You cannot delete a storage pool.

To modify the name of the storage pool, perform the following steps:

## Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Storage**.  
The system opens the Storage dashboard displaying the **Overview** tab.
3. Click **Table > Storage Pool**.  
The system displays a list of storage pools in the cluster.
4. Select the storage pool to modify and click **Update**.  
The system displays the **Update Storage Pool** dialog box.
5. Enter the new name of the storage pool in the **Name** field.
6. Click **Save**.

# Creating a Storage Container

This section describes how to create a storage container in the cluster.

## Before you begin

- Ensure that you configure the cluster to synchronize time with NTP servers. For more information, see [Configuring NTP Servers](#) on page 350. Ensure that the time on the Controller VMs is properly synchronized and displays the current time. If the time on the Controller VMs is ahead of the current time, the files within the storage containers might also have timestamps ahead of the current time when viewed from the hypervisor, and the cluster services might fail to start.
- When you create a cluster, the system automatically creates a storage pool and a storage container in the cluster.
- To create a storage container, you must first configure a Controller VM with enough memory. Controller VM memory allocation requirements differ depending on the models and features that are being used. For more information, see [CVM Memory Configuration](#) on page 99.
- For replication factor 1 storage container recommendations and limitations, see [Replication Factor 1](#) on page 41.

## About this task

AOS automatically creates the correct type of access to the storage container for each hypervisor.

- Hyper-V: The storage container is accessible as an SMB share.

**Note:** You cannot create a replication factor 1 storage container on clusters running Hyper-V.

- vSphere: The storage container is accessible as an NFS datastore. This requires access to the vSphere APIs. Ensure that you have appropriate license of vSphere to access the APIs.

**Note:** Nutanix supports NFS version 3 with ESXi.

- AHV: The storage container is accessible transparently.

**Important:** To use cross cluster live migration (CCLM) and on-demand cross cluster live migration (OD-CCLM), ensure that both the source and the destination clusters have the same storage container name for the guest VMs. For example, if a SelfServiceContainer storage container exists on the source cluster, the destination cluster must also have a SelfServiceContainer storage container.

For more information on CCLM, see [Cross Cluster Live Migration](#) in *Nutanix Disaster Recovery Guide*.

For more information on OD-CCLM, see [On-Demand Cross-Cluster Live Migration](#) in *AHV Administration Guide*.

To create a storage container, follow these steps:

### Procedure

1. Log on to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Storage**.  
The system opens the Storage dashboard displaying the **Overview** tab.
3. Click **+ Storage Container**.

For more information on Storage dashboard, see [Storage Dashboard](#) on page 117.

The system displays the **Create Storage Container** dialog box.

**4.** Enter the following in the indicated fields:

- a. **Name:** Enter a name for the storage container.

**Note:** This entity has the following naming restrictions across hypervisors.

**Container Name Length:**

- AHV: Maximum length is 75 characters.
- ESXi: Maximum length is 42 characters.
- Hyper-V: Maximum length is 32 characters.

**Supported Characters:**

AHV, ESXi, and Hyper-V: Uppercase and lowercase standard Latin letters (A-Z and a-z), Simplified Chinese, decimal digits (0-9), dots (.), hyphens (-), hash (#), and underscores (\_).

**Case Sensitivity:**

- AHV and ESXi: Container names are case sensitive.
- Hyper-V: Container names are case insensitive. For example, if there is a container with name ABCD, then creating another container with name abcd is restricted.

- b. **Storage Pool:** Select a storage pool from the drop-down list.

The following field, **Max Capacity (Physical)**, displays the amount of free physical space available in the selected storage pool.

- c. (vSphere only) **NFS Datastore:** Perform one of the following:

- Mount on all ESXi hosts: Select this option to mount the storage container on all the hosts in the cluster.
- Mount on the following ESXi hosts: Select this option to mount the storage container on a specific set of hosts, with the host IP addresses displayed below this field. To choose a host, select the checkbox associated with the the host.

- d. (Hyper-V only) Set this storage container as default store for VMs on Hyper-V hosts.

Depending on your selection, the Create Virtual Machine Wizard of Hyper-V automatically populates the storage location with the relevant storage container.

Option	Description
<b>Make default on all Hyper-V hosts</b>	Makes this storage container a default location for storing virtual machine configuration and virtual hard disk files on all the Hyper-V hosts.
<b>Make default on particular Hyper-V hosts</b>	Provides you with an option to select the hosts to make this storage container a default location for storing virtual machine configuration and virtual hard disk files on all the Hyper-V hosts.

- To configure additional parameters, click the **Advanced Settings** button.

Enter the following in the indicated fields:

- Cluster Fault Tolerance (Read-Only)**: Displays the fault tolerance of the cluster that you configured when you created the cluster.

- Replication Factor**: Displays the number of copies of data in the container.

The default value is based on the cluster fault tolerance that you select when you create the cluster. For more information on cluster fault tolerance, see [Cluster Fault Tolerance](#) on page 25.

To modify the replication factor, select the value from the dropdown menu. You can set the replication factor to 1, 2, or 3 depending on the fault tolerance of the cluster. For more information on replication factor, see [Replication Factor](#) on page 40.

**Note:**

- You can modify the replication factor of a container in a cluster with 1N&1D or 2N/2D cluster fault tolerance. You cannot modify the replication factor of a container in a cluster with 1N/1D cluster fault tolerance; however, you can modify the replication factor of the container after you increase the fault tolerance of the cluster from 1N/1D to 2N/2D. For more information, see [Increasing the Cluster Fault Tolerance Level](#) on page 75.
- Nutanix supports a replication factor of 1, 2, or 3. Nutanix supports a replication factor of 1 if you enable the replication factor 1 setting only. For more information, see [Enabling Replication Factor 1](#) on page 139. If you do not enable the replication factor 1 setting, Nutanix supports a replication factor of 2 or 3 depending on the fault tolerance configured in the cluster. Setting the replication factor to 3 adds an extra layer of data protection at the cost of storing an additional copy of the data.

- Reserved Capacity (Logical)**: To reserve storage space for this storage container, enter the amount (in GiB) to reserve in this field.

**Reserved Capacity (Physical) (Read-Only)**: Displays the amount of physical capacity that is reserved based on the logical reserved capacity value.

You can reserve space for a storage container to ensure a minimum storage capacity is available. Reserving space for a storage container means that space is no longer available to other storage containers even if the reserved space is unused. For more information, see [Capacity Reservation Best Practices](#) on page 105.

- Advertised Capacity (Logical)**: To configure a maximum storage space for this storage container, enter the amount (in GiB) to reserve in this field.

**Advertised Capacity (Physical) (Read-Only)**: Displays shows the amount of physical capacity that is advertised based on the logical advertised capacity value.

This configures the *advertised* capacity, which is the maximum storage size that the storage container can use. You can configure any value, however if a reserved capacity is configured, the advertised capacity must be greater than or equal to the reserved capacity on the storage container. The hypervisor ensures that the storage container storage does not exceed the advertised capacity. When a storage container reaches a threshold percentage of the actual storage pool size, an alert is issued.

- Compression**: By default, this checkbox is selected.

Inline compression is enabled by default with the **Delay (In Minutes)** field set to 0. A value of 0 means that data is compressed immediately as it is written. The delay time between write and compression is configurable. For post-process compression, where data is compressed after it is written, Nutanix recommends a delay of 60 minutes. Compression is delayed for 60 minutes after the initial write operation. All data in the storage

container is compressed when you select **Compression**. For information about using compression, see [Compression](#) on page 111.

- f. **Deduplication:** Select the **Capacity** checkbox to perform post-process deduplication of persistent data.

Nutanix recommends this option primarily for full clone, persistent desktops, and physical to virtual migration use cases that need storage capacity savings (not just performance savings from deduplication). Nutanix recommends that the Controller VMs have at least 32GB of RAM and 300GB SSDs for the metadata disk to use this option.

**Note:** Deduplication is not available when you select **Replication Factor** as 1.

- g. **Erasure Coding:** Select the **Enable** checkbox to enable erasure coding.

Erasure coding increases the effective or usable capacity on a cluster. For more information about erasure coding, see [Erasure Coding](#) on page 112.

**Note:** Erasure coding is not available when you select **Replication Factor** as 1.

- h. **Filesystem Allowlists:** Enter the IP address and netmask value, separated by a comma (in the format ip\_address/netmask).

An allowlist is a set of addresses that are allowed access to a storage container. Allowlists allows legitimate traffic when while blocking unauthorized access from other sources. Configuring an allowlist at a storage container level overrides any global allowlist for that storage container.

Setting an allowlist enables access to the container via NFS. Some manual data migration workflows might require the allowlist to be configured temporarily, while some third-party backup vendors might require the allowlist to be configured permanently to access the container via NFS.

**Caution:**

- User authentication is not available for NFS access, and the IP address in the allowlist has full read or write access to the data on the container.
- Nutanix recommends to allow single IP addresses (with net mask such as 255.255.255.255) instead of allowing subnets (with netmask such as 255.255.255.0).

6. Click the **Save** button.

## Modifying a Storage Container

This section describes how to modify an existing storage container in the cluster.

### Before you begin

- The *NutanixManagementShare* container is an internal storage container for Nutanix products and services. To ensure seamless operations, external users must avoid accessing, modifying, or deleting this storage container. The *NutanixManagementShare* storage container is not intended to store user data and vDisks, including Nutanix Volumes.
- The Prism Element web console does not allow you to rename a storage container in an AHV cluster when modifying container details using this procedure.
- You cannot rename a storage container if it contains vdisks.

### About this task

Storage Containers can be modified to change how the data in that storage container is handled, for example to apply compression.

To modify a storage container, do the following:

### Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Storage**.  
The system opens the Storage dashboard displaying the **Overview** tab.
3. Click **Table > Storage Container**.  
The system displays a list of storage containers in the cluster.
4. Select the storage container to update, then click **Update**.  
The system displays the **Update Storage Container** dialog box.

#### Note:

- For ESXi clusters, if you make changes to any of the parameters that impact the storage container size (such as Advertised Capacity), the information does not get refreshed in the vCenter ESXi nodes by default. You must right-click the container in vCenter and select **Refresh Capacity Information** to refresh the capacity.
- If the compression policy is changed from compressed to uncompressed (or vice versa), the existing compressed (uncompressed) data in the storage container will be uncompressed (compressed) as a background process when the next data scan detects the data that needs this change.
- The Prism Element web console does not provide an option to change the container replication factor. This can only be done through the nCLI. For more information, see [Replication Factor Configuration](#) on page 137.

5. Enter the necessary values in the respective fields.

The fields in the **Update Storage Container** dialog box is identical to the fields in the **Create Storage Container** dialog box. For more information, see [Creating a Storage Container](#) on page 131.

## Deleting a Storage Container

This section describes how to delete an existing storage container in the cluster.

### Before you begin

- The *NutanixManagementShare* container is an internal storage container for Nutanix products and services. To ensure seamless operations, external users must avoid accessing, modifying, or deleting this storage container. The *NutanixManagementShare* storage container is not intended to store user data and vDisks, including Nutanix Volumes.

### About this task

To delete a storage container, do the following:

### Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Storage**.  
The system opens the Storage dashboard displaying the **Overview** tab.
3. Click **Table > Storage Container**.  
The system displays a list of storage containers in the cluster.

- To delete a storage container, select the target storage container, and click **Delete**.

## Replication Factor Configuration

This section describes how to configure the replication factor for a storage container in a Nutanix cluster.

The replication factor of a storage container depends on the fault tolerance of the cluster. The default replication factor of a container in a cluster is based on the cluster fault tolerance that you select when you create the cluster. For example, if you select the fault tolerance of a cluster as 1N&1D when you create the cluster, the system configures replication factor 3 for the storage containers in the cluster, by default.

You can modify the replication factor of a container in a cluster with 1N&1D or 2N/2D cluster fault tolerance. For more information, see [Creating a Storage Container](#) on page 131. You cannot modify the replication factor of a container in a cluster with 1N/1D cluster fault tolerance; however, you can modify the replication factor of the container after you increase the fault tolerance of the cluster from 1N/1D to 2N/2D. For more information, see [Increasing the Replication Factor using CLI](#).

To enable or disable replication factor 1, see [Enabling Replication Factor 1](#) on page 139 or [Disabling Replication Factor 1](#) on page 139.

### Increasing the Replication Factor using CLI

After you increase the fault tolerance in a cluster to 2N/2D, you must increase the replication factor for the storage containers in the cluster to ensure that all storage containers have three copies of the data. This topic describes how to increase the replication factor to 3.

#### Before you begin

Ensure that you have increased the cluster fault tolerance to 2N/2D. For more information, see [Increasing the Cluster Fault Tolerance Level](#) on page 75.

#### About this task

To increase the replication factor to 3 using CLI, follow these steps:

#### Procedure

- Log in to the Controller VM and type the following command.

```
nutanix@cvm$ ncli
```

- To locate the storage containers that require an update, run the following command.

```
ncli> ctr list
```

An output similar to the following is displayed.

Id	:	00052e5a-bc71-2112-0000-0000000261a::11	
	Uuid	:	c49eb9af-2eba-41b1-
bae5-08227f7cff13			
	Name	:	storage_container_name
bc71-2112-0000-0000000261a::10	Storage Pool Id	:	00052e5a-
bad7-3ac3587f2960	Storage Pool Uuid	:	b785ff57-9d53-4f05-
(11,316,325,361,581 bytes)	Free Space (Logical)	:	10.29 TiB
	Used Space (Logical)	:	0 bytes
	Allowed Max Capacity	:	10.29 TiB
(11,316,325,361,581 bytes)			
	Used by other Containers	:	0 bytes
	Explicit Reservation	:	0 bytes

	Thick Provisioned	:	0 bytes
	Replication Factor	:	2
	Oplog Replication Factor	:	2
	NFS Whitelist Inherited	:	true
	Container NFS Whitelist	:	
SATA	VStore Name(s)	:	default-container-9754
	Random I/O Pri Order	:	SSD-PCIe, SSD-SATA, DAS-
SATA	Sequential I/O Pri Order	:	SSD-PCIe, SSD-SATA, DAS-
	Compression	:	off
	Fingerprint On Write	:	off
	On-Disk Dedup	:	none
	Erasure Code	:	off

3. To set the replication factor to 3 for each target storage container, run the following command.

```
ncli> ctr edit name=storage_container_name rf=3
```

Replace `storage_container_name` with the name of the storage container.

Output similar to the following is displayed. This shows that the replication factor is now at the correct state (3) for the storage container.

	Id	:	00052e5a-bc71-2112-0000-00000000261a::1381
b356-4883-90c5-c37b2f3e0fad	Uuid	:	a567b66d-
	Name	:	<i>storage</i>
<i>container_name</i>	Storage Pool Id	:	00052e5a-
bc71-2112-0000-00000000261a::10	Storage Pool Uuid	:	b785ff57-9d53-4f05-
bad7-3ac3587f2960	Free Space (Logical)	:	6.86 TiB
(7,544,216,907,720 bytes)	Used Space (Logical)	:	0 bytes
	Allowed Max Capacity	:	6.86 TiB
(7,544,216,907,720 bytes)	Used by other Containers	:	0 bytes
	Explicit Reservation	:	0 bytes
	Thick Provisioned	:	0 bytes
	Replication Factor	:	3
	Oplog Replication Factor	:	3
	NFS Whitelist Inherited	:	true
	Container NFS Whitelist	:	
	VStore Name(s)	:	aaa
DAS-SATA	Random I/O Pri Order	:	SSD-PCIe, SSD-SATA,
	Sequential I/O Pri Order	:	SSD-PCIe, SSD-SATA,
DAS-SATA	Compression	:	off
	Fingerprint On Write	:	off
	On-Disk Dedup	:	none
	Erasure Code	:	off

**Important:** Ensure that you increase the replication factor to 3 for all target containers, including containers created by the system such as the SelfServiceContainer or NutanixManagementShare.

To set replication factor 3 for the system storage container NutanixManagementShare, run the following command:

```
ncli> ctr edit name=NutanixManagementShare rf=3 force=true
```

## What to do next

The system might take some time to increase the replication factor. Verify the status by viewing the **Cluster Resiliency / Fault Tolerance Status** widget in the dashboard of the Prism Element web console. When the value of **Failures Tolerable** for **Extent Group** (which reflects the container replication level) increases to 2, it confirms that the replication factor for the cluster is 3.

## Enabling Replication Factor 1

To enable replication factor 1, first enable the replication factor 1 setting, and then create a dedicated replication factor 1 enabled storage container and associate the replication factor 1 enabled storage container with one node.

### About this task

After the replication factor for a container is set to 1, you cannot increase the replication factor on that container.

### Before you begin

See [Replication Factor 1](#) on page 41.

### Procedure

1. Log on to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Settings**.  
The system displays the **Global Settings** page.
3. From the **Data Resiliency** section in the left navigation pane, click **Cluster Fault Tolerance**.  
The **Cluster Fault Tolerance** page opens, displaying the existing cluster fault tolerance.
4. Select the **Allow selection of Replication Factor 1 on Storage Containers** checkbox.  
The system prompts you to confirm the action.
5. Click **Yes** to confirm the action, and then click **Save**.

### What to do next

Create a replication factor 1 enabled storage container and assign it to a node. For more information, see [Creating a Storage Container](#) on page 131.

## Disabling Replication Factor 1

### About this task

Disabling replication factor 1 prevents you from creating a new replication factor 1 enabled storage container. Any existing replication factor 1 enabled containers with associated vDisks remain in place.

## Procedure

1. Log on to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Settings**.  
The system displays the **Global Settings** page.
3. From the **Data Resiliency** section in the left navigation pane, click **Cluster Fault Tolerance**.  
The **Cluster Fault Tolerance** page opens, displaying the existing cluster fault tolerance.
4. Clear the **Allow selection of Replication Factor 1 on Storage Containers** checkbox and then click **Save**.  
After disabling replication factor 1, if you create or modify a storage container, your replication factor choices are 2 or 3.

## Volume Group Configuration

A volume group is a collection of virtual disks (vDisks). Each volume group is identified by a name and UUID. Each vDisk has a UUID and a SCSI index to specify the ordering of disks within the volume group.

You can create a volume group on a storage container and enable access to the volume group in one of the following ways:

### iSCSI

iSCSI access to a volume group is provided through Nutanix Volumes. For more information, see the [Nutanix Volumes Guide](#).

### Attach Directly to a VM

In an AHV cluster, you can create a volume group and attach it to one or more VMs as a SCSI disk by using the Prism Element web console, the Nutanix REST API, or the nCLI or aCLI commands.

After the volume group is attached to a VM by using the Prism Element web console, vDisks appear as SCSI devices to the guest operating system. AOS transparently handles load balancing and path resiliency on the guest VM. Directly attached volume groups support Controller VM failover and do not impact VM migration.

Volume groups are managed independently of the VMs to which they are attached. You can configure a directly attached volume group for access by a single VM (exclusive access) or by multiple VMs (shared access).

**Caution:** Multiple VMs writing to a vDisk that belongs to a shared volume group and has no additional software to manage the access to the vDisk might lead to data corruption. Use shared access when you are configuring VMs for use with cluster aware software.

## Concurrent Access from Multiple Clients

Products, features, or solutions might require concurrent access to volume groups, either by multiple iSCSI initiators or multiple VM attachments.

### Multiple iSCSI Initiators

The following products, features, or solutions supports concurrent access to volume groups:

- Oracle RAC (bare-metal and virtualized environments)
- Linux VMs
- Windows Failover Clustering
- IBM Spectrum Scale (GPFS)
- Veritas InfoScale Storage

## Multiple Directly Attached VMs

The following products, features, or solutions supports concurrent access to volume groups:

- Oracle RAC
- Linux VMs
- IBM Spectrum Scale (GPFS)
- Veritas InfoScale Storage
- Windows Failover Clustering
- Linux guest VM clustering (also known as RHEL HA)

## Creating a Volume Group

Create a volume group in a storage container.

### About this task

To create a volume group, perform the following steps:

### Procedure

1. Log on to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Storage**.  
The system opens the Storage dashboard displaying the **Overview** tab.
3. Click the **+ Volume Group** button.  
The system displays the **Create Volume Group** dialog box.
4. In the **Storage** section, click **+ Add New Disk**.  
The system displays the **Add Disk** dialog box.
5. In **Name**, enter a name for the volume group.

**Note:** This entity has the following naming restrictions:

- The maximum length is 75 characters.
- Allowed characters are uppercase and lowercase standard Latin letters (A-Z and a-z), decimal digits (0-9), dots (.), and hyphens (-).

6. The **iSCSI Target Name Prefix** is auto-filled with the volume group **Name**. You can accept this prefix or enter your own target name prefix for the volume group. This entity has the same naming restrictions as **Name**.
7. In **Description**, enter a description for the volume group.
8. To add a disk to the volume group, do the following:
  - a. In the **Storage** section, click **Add New Disk**.
  - b. From the **Storage Container** dropdown menu, select the storage container
  - c. In **Logical Size (GiB)**, enter the disk size in GiBs.
  - d. Click **Add**.
9. Repeat these steps to add another disk for this volume group, if desired.

- To allow external clients such as bare-metal servers or VMs running outside the Nutanix cluster to access the volume group, select the **Enable external client access** checkbox if you are allowlisting clients that are external to or not residing in this cluster.

This selection remains enabled until you create a new volume group.

- If the cluster that hosts the volume group uses one-way CHAP security, select the **CHAP Authentication** checkbox and type a 12-character to 16-character password (also known as a CHAP secret) in the **Target Password** field.
- If you are using one-way CHAP security, select the **CHAP Authentication** checkbox and type a 12-character to 16-character password (also known as a CHAP secret) in the **Target Password** field.  
Initiators must use the same password to authenticate to the AOS cluster.
- To configure the iSCSI initiators, click **Add New Client**. The system displays the Add iSCSI Client dialog box. Perform the following in the indicated fields.

- Client IQN/IP Address:** Enter the client Initiator iSCSI Qualified Name (IQN) to create the allowlist.

**Note:** Ensure that you enter the client IQN in the **Client IQN/IP Address** field and not the IP address. AOS does not support an allowlist containing IP addresses in a volume group.

- CHAP Authentication:** Select this checkbox if you have configured mutual CHAP authentication on the client.
- Client Password:** Enter the iSCSI client password (secret).
- Click **Add**.

The **Client** section displays any configured clients. This list includes any clients attached to volume groups in the cluster. Repeat this step to add more initiators allowed to access this storage. For information on the products, features, or solutions that supports concurrent access to a volume group, see [Concurrent Access from Multiple Clients](#) on page 140.

- To enable the flash mode feature, select the **Enable Flash Mode** checkbox.

**Note:** Individual virtual disks of a volume group cannot be excluded from Flash Mode by using the Prism Element web console. However, you can exclude individual virtual disks from flash mode by using aCLI. For more information, see [Disabling Flash Mode from Virtual Disks of a Volume Group](#) on page 146.

- Click **Save**.

The system creates the volume group.

## What to do next

In an AHV cluster, you can attach the volume group to the VM and start using the vDisks. If you want to use iSCSI and you already allowlisted the host IP addresses, log on to the VMs, and configure iSCSI.

## Modifying a Volume Group

Modify a volume group in a storage container.

### About this task

To modify a volume group, do the following:

### Procedure

- Log in to the Prism Element web console.

2. From the dropdown menu on the left of the main menu, select **Storage**.  
The system opens the Storage dashboard displaying the **Overview** tab.
3. Click **Table > Volume Group**.  
The system displays a list of volume groups in the cluster.
4. Select the volume group to update, and then click **Update**.  
The system displays the Update Volume Group dialog box. Enter the necessary values in the respective fields. The fields in the Update Volume Group dialog box is identical to the fields in the Create Volume Group window. For more information, see [Creating a Volume Group](#) on page 141. You can change the volume group name, add and remove disks, configure the volume group for sharing, and add or remove (by clearing) entries from the initiator allowlist. On AHV clusters, you can attach the volume group to a VM as a SCSI disk (described later in this procedure).

You can increase the size of the volume group. Reducing the size of a volume group is not supported.  
Any unchecked initiator that remains unused by a volume group ultimately disappears from this list.
5. To attach a volume group to a VM, perform the following steps: , and then select the VM from the **Available VMs** list.
  - a. Click **Attach to a VM**.  
The systems diplays the **Attach to VM** dialog box.
  - b. From the **Available VMs** dropdown menu, select the VM to attach the volume group.
  - c. Click **Attach**.  
The system attaches the volume group to the VM.
6. To enable or disable CHAP authentication for an an iSCSI client, perform the following steps:
  - a. In the **Client** section, click the edit icon associated with the client.  
The system displays the **Edit iSCSI client** dialog box.
  - b. Select the **CHAP Authentication** checkbox to enable CHAP authentication on the client. Clear the **CHAP Authentication** checkbox to disable it. For more information, see the [Nutanix Volumes Guide](#).
  - c. Enter the iSCSI client password (secret) in the **Client Password** field.
  - d. Click **Add**.
7. After updating a volume group, click **Save**.

## Deleting a Volume Group

Delete a volume group from a storage container.

### Before you begin

If any iSCSI clients are attached to the volume group, first disconnect or detach the AOS cluster target for each iSCSI initiator from the iSCSI client (for example, from the Windows or Linux client). See your vendor documentation for specific disconnection procedures.

### About this task

To delete a volume group, perform these steps:

### Procedure

1. Log in to the Prism Element web console.

2. From the dropdown menu on the left of the main menu, select **Storage**.  
The system opens the Storage dashboard displaying the **Overview** tab.
3. Click **Table > Volume Group**.  
The system displays a list of volume groups in the cluster.
4. To detach any iSCSI clients attached to the volume group, perform the following steps:

**Note:** Before you delete a volume group, you must detach any iSCSI clients attached to the volume group. If no clients are attached, skip this step.

- a. Select the volume group to delete and click **Update**.  
The system displays the **Update Volume Group** dialog box
- b. Clear the **Enable External Client Access** checkbox and clear any clients listed in the **Clients** section.
- c. Click **Save**.
5. Select the volume group to delete, and click **Delete**.  
The system prompts you to confirm the delete action.
6. Click **Delete** to confirm.

## Cloning a Volume Group

Clone a volume group from an existing volume group in a storage container.

### About this task

To clone a volume group, perform the following steps.

### Procedure

1. Log on to the Prism Element web console.
2. From the dropdown menu on the left of the main menu, select **Storage**.  
The system opens the Storage dashboard displaying the **Overview** tab.
3. Click **Table > Volume Group**.  
The system displays a list of volume groups in the cluster.
4. Select the volume group to clone and click **Clone**.  
The system displays the **Clone Volume Group** dialog box.
5. Enter the necessary values in the respective fields.  
The fields in the **Clone Volume Group** dialog box is identical to the fields in the **Create Volume Group** dialog box. For more information, see [Creating a Volume Group](#) on page 141.
6. Click **Save**.

## Flash Mode for Virtual Machines, Disks, and Volume Groups

Flash mode for VM allows you to set the storage tier preference as SSD for a virtual machine or volume group. Flash mode allows latency sensitive workloads to remain on the SSD tier and avoid any potential performance impact of down migration of data. By default, flash mode is not enabled for all database deployments.

Flash Mode uses up to 25% of the SSD capacity of the cluster. If the size of the data of the flash mode-enabled entities exceeds 25% of the SSD capacity, the cluster moves the data to the cold tier. Before moving the data to the cold tier, flash mode attempts to preserve the excess data in the SSDs to enable corrective actions on the cluster such

as as SSD capacity expansion to stabilize the excess usage. To reduce flash mode usage, you can disable flash mode on some VMs or VGs or add SSDs.

**Note:** For information about minimum SSDs requirement for Hybrid HCI Node and All-Flash HCI Node, see [HCI Node Field Requirements](#) in *Acropolis Advanced Administration Guide*.

A node failure might reduce the SSD tier capacity causing the flash mode usage to exceed 25% of the tier capacity. In such cases, the system generates alerts to notify that flash usage exceeded the 25% threshold.

If you enable flash mode on a VM, all the virtual disks (vDisks) that are added or attached to the VM are automatically placed on the SSD tier. However, you can update the VM configuration to remove the flash mode from any vDisks.

You can enable flash mode on a VM and vDisks only when you update a VM from the Prism Element web console. For more information on how to enable flash mode on VMs, see [Step 11 in Managing a VM \(AHV\)](#). However, for VGs, you can enable the feature during the creation of VGs. For information on how to enable the feature on VGs, see [Creating a Volume Group](#) on page 141.

**Caution:** Enabling flash mode on a VM might negatively impact the performance of other VMs in the cluster that do not have flash mode enabled. Nutanix recommends that you evaluate the potential performance impact on these VMs before enabling flash mode. To mitigate any impact on the performance, you can remove the flash mode on individual vDisks. For example, you can enable flash mode on the application data disks and disable it on the log disks.

**Note:**

- Flash mode is supported on ESXi and AHV hypervisor for VMs and on all the hypervisors for VGs.
- For a cluster created using ESXi hosts, you must register your cluster with the vCenter Server before enabling flash mode. For more information, see [Registering a Cluster to vCenter Server using Prism Element](#) on page 362.

The system raises an alert

- When the flash usage exceeds 25% of the SSD tier.
- When the VM has the flash mode enabled but is in the powered off state.

## General Conditions

- When you clone a VM or VG with the Flash Mode feature enabled, the system automatically applies the Flash Mode policies to the cloned VM or VG.
- When you restore a VM or VG with the Flash Mode feature enabled from a DR snapshot, either locally or remotely, the system automatically applies the Flash Mode policies to the restored VM or VG.
- Flash mode restricts the movement of I/O data from the hot tier to the cold tier but does not restrict the usage of the hot tier by flash mode-enabled entities such as VMs, VGs, or vDisks. Based on the availability of memory in the hot tier, the data of the flash mode-enabled entities is placed in the hot tier.
- If you enable erasure coding on a cluster with flash mode enabled, the parity resides on the HDD tier.
- If you replicate a VM or VG to a remote site, the replicated VM or VG does not have flash mode enabled automatically. You must manually enable the flash mode in the VM or VG.
- Do not use flash mode feature with capacity tier deduplication. Enabling flash mode feature does not affect performance tier deduplication.
- If you perform a storage migration or storage vMotion, the new virtual disk created on the target datastore will not have the flash mode feature enabled. You need to manually enable the flash mode feature again.

- Flash mode is not supported if the cluster has more than one storage pool. If you delete and create a storage pool in your cluster, you cannot configure the flash mode for a short period because two storage pools exists in the cluster temporarily during this period, preventing flash mode from being enabled.

## Disabling Flash Mode from Virtual Disks of a Volume Group

You cannot disable flash mode from virtual disks in a volume group using the Prism Element web console. To disable flash mode from virtual disks in a volume group, use aCLI.

### Procedure

- Log in to the Controller VM using SSH.
- Disable flash mode on a particular disk by running the following command.

```
acli> vg.disk_update vg_name index_value flash_mode=false
```

Replace `vg_name` with the name of the VG and `index_value` with the index value of the VG. For example to disable flash mode for disk at index 0 with name `example_vg`, use the following command.

```
acli> vg.disk_update example_vg 0 flash_mode=false
```

## Recycle Bin

The Recycle bin helps you manage and restore deleted storage entities such as guest VMs or volume group vDisks. By default, the recycle bin is enabled when you create a cluster.

#### Note:

- To restore an entity from the recycle bin, contact Nutanix Support.
- When Replication Factor 1 is enabled for a storage container, the recycle bin is disabled for that storage container. When you delete a storage entity like a guest VM or volume group vDisk, it is marked for deletion as soon as possible and bypasses the recycle bin. For more information, see [Replication Factor](#) on page 40.

When the recycle bin is enabled, AOS creates a Recycle Bin associated with the storage container configured in your cluster. If you delete a storage entity, the Recycle Bin retains vDisk and configuration data files for up to 24 hours, unless the cluster free storage space reaches critical thresholds. After 24 hours, AOS automatically deletes these files. If the cluster lacks sufficient free disk space, AOS deletes the files in less than 24 hours and triggers free disk space alerts.

After you disable the recycle bin, AOS automatically deletes any entities in the recycle bin after 24 hours. Subsequent deletions of storage entities are not stored in the recycle bin but are marked for deletion immediately. After you delete one or more storage entities, the free storage space shown in the Prism Element web console might not update for 24 hours. To view the space used by the recycle bin, go to the **Storage** dashboard and and view the Storage Summary in the **Diagram** or **Table** view. For more information, see [Viewing Recycle Bin Space Usage](#) on page 148.

For more information about Recycle Bin behavior, see [Recycle Bin Guidelines and Limitations](#) on page 146.

## Recycle Bin Guidelines and Limitations

Limitations and guidelines to consider when you use the recycle bin.

- The recycle bin stores vDisk and configuration data for up to 24 hours. After 24 hours, these files are deleted. If the cluster lacks sufficient free disk space, the files are deleted in less than 24 hours.

The recycle bin is temporarily disabled when it uses more than five percent of cluster storage capacity. AOS triggers free disk space alerts when your cluster reaches critical thresholds. In this case, newly deleted entities are marked for deletion as soon as possible and are not stored in the recycle bin folder of the storage container.

When the recycle bin is cleared and uses two percent or less of cluster storage capacity, the system automatically re-enables the recycle bin after all Curator service scans are completed. (The Curator service controls the recycle bin and storage cleanup, among other cluster tasks.)

- If the recycle bin already contains more than 2,000 files, any storage entities subsequently deleted bypass the recycle bin. AOS marks these entities for immediate deletion and does not store them in the recycle bin folder of the storage container.
- The Prism Element web console displays the **Clear Recycle Bin** (available on the **Storage** dashboard in **Detail or Table** view) or **Clear Space** (available in **Storage Details**) options only if the recycle bin contains deleted files. If these options are available but the space used by the Recycle Bin shows as 0, it means AOS has detected the deleted files but not yet calculated the storage space used.
- After you empty the recycle bin using **Clear Recycle Bin** or **Clear Space** or when AOS empties the recycle bin, the system displays these options only after until you delete storage entities like guest VMs and volume group vDisks.
- The recycle bin is disabled for a container with Replication Factor 1. When you delete a storage entity, such as a guest VM or a vDisk, from a container with replication factor 1, the entity is marked for deletion as soon as possible and bypasses the recycle bin. For more information, see [Replication Factor](#) on page 40
- The recycle bin is not supported on storage containers with metro availability enabled.
- The recycle bin does not store deleted protection domain snapshots. Therefore, you cannot recover protection domain snapshots from the recycle bin.
- When you delete a VM with a thick provisioned vDisk reservation setting, the setting is removed. After recovering this VM, the reservation is not restored and defaults to thin provisioned.
- If you are using the X-Ray application, an automated testing framework and benchmarking application for enterprise-grade datacenters, you must disable the recycle bin on your cluster.

## Enabling Recycle Bin

By default, the recycle bin is enabled when you create a cluster. If you disable the recycle bin, you can enable it again from the Cluster Details window in the Prism Element web console.

### Before you begin

See [Recycle Bin Guidelines and Limitations](#) on page 146.

### Procedure

- Log in to the Prism Element web console.
- From the dropdown menu, select **Settings**.  
The systems displays the **Global Settings** page.
- From the **General** section in left navigation pane, select **Cluster Details**.  
The system displays the **Cluster Details** page.
- Select the **Retain Deleted VMs** checkbox.

**5. Click **Save**.**

The system enables the recycle bin for the cluster.

## Disabling Recycle Bin

By default, the recycle bin is enabled when you create a cluster. You can disable the recycle bin from the Cluster Details window in the Prism Element web console.

### Before you begin

See [Recycle Bin Guidelines and Limitations](#) on page 146.

### Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu, select **Settings**.  
The system displays the **Global Settings** page.
3. From the **General** section in left navigation pane, select **Cluster Details**.  
The system displays the **Cluster Details** page.
4. Clear the **Retain Deleted VMs** checkbox.
5. Click **Save**.  
The system disables the recycle bin for the cluster.

## Viewing Recycle Bin Space Usage

View the space used by the recycle bin in the Storage dasboard of the Prism Element web console

### Before you begin

See [Recycle Bin Guidelines and Limitations](#) on page 146.

### Procedure

1. Log on to the Prism Element web console.
2. From the **Storage Summary** widget, click **View Details**.  
The system opens the **Storage Details** dialog box displaying the space used by the recycle bin.

## Clearing Storage Space Used by the Recycle Bin

Clear the storage space used by the recycle bin from the Prism Element web console.

### Before you begin

See [Recycle Bin Guidelines and Limitations](#) on page 146.

### Procedure

1. Log in to the Prism Element web console.
2. From the **Storage Summary** widget, click **View Details**.  
The system opens the Storage Details dialog box displaying the space used by the recycle bin.
3. Click **Clear Space**.  
The system prompts you to confirm the delete action.

**4. Click **Delete**.**

The system immediately deletes the VMs and VGs in the recycle bin.

# NETWORK MANAGEMENT

---

Nutanix provides several features to manage and monitor network settings in the cluster.

- To configure network connections in an AHV cluster using Nutanix virtualization management, see [Network Configuration for Cluster](#) on page 150.
- To enable LAG and LACP on the T0R switch, see [Enabling LACP and LAG \(AHV Only\)](#) on page 169.
- To configure the network interfaces for a VM, see [Network Configuration for VM Interfaces](#) on page 162.
- To track and record networking statistics for a cluster, the cluster requires information about the first-hop network switches and the switch ports in use. You can configure one or more network switches for statistics collection. For more information, see [Configuring a Network Switch](#) on page 167.
- To present a consolidated graphical representation of the network formed by the VMs and hosts in the cluster and first-hop switches, the Prism Element web console has a network visualizer. You can use the visualizer to monitor the network and to obtain information that helps you troubleshoot network issues. For more information, see [Network Visualization](#) on page 174.

## Network Configuration for Cluster

You can view and configure network connections for the cluster from the **Network Configuration** page.

### Network Connections

Each VM network interface is bound to a virtual network, and each virtual network is bound to a single VLAN. Information about the virtual networks configured currently appears in the **Network Configuration** page.

The **Network Configuration** page includes three tabs.

- The **Subnets** tab displays a list of the configured networks.
- The **Internal Interfaces** tab displays a list of LAN interfaces.
- The **Virtual Switch** tab displays a list of virtual switches configured, including the default system-generated virtual switch vs0.

The following table describes the fields in each tab.

**Table 36: Network Configuration Fields**

Parameter	Description	Values
Networks Tab		
Subnet Name	Displays the name of the virtual network.	(name)
Virtual Switch	Displays the name of the virtual switch in the form vs#, for example vs0 for virtual switch 0 which is the default virtual switch.	(vs<number>)
VLAN ID	Displays the VLAN identification number for the network.	(ID number)

Parameter	Description	Values
Used IP Addresses	Displays the number of IP addresses in the subnet that are used, for example IP address of a VM or any other entity. This parameter is applicable only when you have configured a managed network or subnet.	(number of IP addresses)
Free IPs in Subnets	Displays the number of free or unused IP addresses in the subnet. This parameter is applicable only when you have configured a managed network or subnet.	(number of IP addresses)
Free IPs in Pool	Displays the number of free or unused IP addresses in the configured pool. This parameter is applicable only when you have configured a managed network or subnet.	(number of IP addresses)
Actions	Options to edit or delete a network configuration.	(Edit/Delete)
Internal Interfaces Tab		
Descriptive Name	Displays a name for the LAN.	(LAN name)
Subnet (Gateway IP / Prefix Length)	Displays the subnet that the internal interface belongs to in the form <IP Address>/<number (prefix)>	(IP Address/prefix number)
Features	Displays the features available on the internal interfaces.	
Interface	Displays the interface designation such as eth0 or eth1.	(interface name)
Virtual Switch		
Name	Displays the name of the switch in the form vs#	(vs<number>)
Bridge	Displays the name of the bridge associated with the virtual switch in the form br#, for example br0 for the default bridge.	(br<number>)
MTU (bytes)	Displays the MTU set for the virtual switch in bytes. The default MTU is 1500.	(number)
Bond Type	Displays the uplink bond type associated with the virtual switch. For example, Active-Backup. For more information, see <a href="#">Bond Types</a> on page 153.	(<bond_type>)

## LAG and LACP on the ToR Switch

For information on LAG and LACP on the ToR Switch, see [Enabling LACP and LAG \(AHV Only\)](#) on page 169.

## Creating a Virtual Switch

Create a virtual switch in the Nutanix cluster.

### About this task

For information about virtual switch, see [Layer 2 Network Management](#) in the *AHV Administration Guide*.

To create or update a virtual switch, follow these steps:

## Procedure

1. Log in to the Prism Element web console.
2. Perform one of the following:
  - » Go to **VM > Network Config**.
  - » Go to **Settings > Network > Network Configuration**.
3. On the **Network Configuration** page, click the **Virtual Switch** tab.
4. To create a virtual switch, click **+ Create VS** and perform the following steps in the **Create Virtual Switch** dialog box.
5. Click **+ Create VS**.  
The system displays the **Create Virtual Switch** page
6. In the **General** tab, provide the following information.
  - **Virtual Switch Name:** Enter a name for the virtual switch.
  - **Description:** Provide a description for the virtual switch that helps identify the virtual switch.
  - **Physical NIC MTU (bytes):** MTU must be a value in the range 1500 ~ 9000 inclusive.
  - **Select Configuration Method:**

**Standard (Recommended)** method: Select the **Standard (Recommended)** method to implement the virtual switch configuration. This method minimizes disruptions to the workloads by putting the hosts in maintenance mode and migrating the VMs out of the host before applying the configuration. This method deploys the virtual switch configuration through a rolling update process. However, it takes longer to complete, with the duration depending on the number and configuration of VMs.

**Note:** When you select the **Standard** method, the system reboots only the hosts updated with virtual switch configurations.

The virtual switch configuration is deployed in the rolling update process.

**Quick** method: This method is available only when you update an existing virtual switch.

**Important:** Nutanix recommends that you select the **Quick** method only on clusters that are not running production workloads. For limitations applicable to **Quick** method, see [Virtual Switch Limitations](#) in the *AHV Administration Guide*.

7. Click **Next**.  
The system displays the **Uplink Configuration** tab.

8. In the **Uplink Configuration** tab, provide the following information.

- **Bond Type:** Select an appropriate bond type. For more information about the bond types, see the *Bond Types* table for details about the bond types.
- **Select Hosts:** Select the hosts to host the VMs.
- **Select Uplink Ports:** (Port Type) Select one of the following:

**Connected and Unconnected Uplink Ports:** Select this option if you want to use the ports that are not currently connected but might be connected later.

**Only Connected Uplink Ports:** Select this option if you want to use only the connected ports. You must also select the switches with LLDP from the **On Switches (with LLDP)** dropdown menu.

- **Uplink Port Speeds:** Select a speed to display the ports that have the selected speed. You can select speeds such as **1G, 10G** or both (**All Speeds**). The speeds displayed depend on the NIC type that is installed on the host.

Based on your selection the columns in the (Host Port) table change dynamically to display the ports with the speeds you selected.

- **(Host Port) table:** Based on the selections you made in this Select Uplink Ports section, a table displays the hosts that have the uplink ports that satisfy the selected criteria. Select the ports you need for this configuration from the list. Click the down arrow on the right side of the table to display the ports listed for each host.

Select the checkbox of a port to select the port. Clear the checkbox to unselect the port. Clearing the checkbox removes the uplink port (NIC) from the virtual switch.

**Note:** A port listing is greyed out if it is unavailable because it is already associated with another virtual switch.

Click **Select All** to select all the ports available and listed.

Click **Clear All** to unselect all the ports available and listed.

**Note:** The Maximum VM NIC Throughput and Maximum Host Throughput values are not restricted to the value provided in this table. The values in the table are indicated for an assumption of 2 x 10 Gb adapters with simplex speed.

For more information about uplink configuration, see [Virtual Switch Workflow](#) in the *AHV Administration Guide*.

9. Click **Create** to create the virtual switch.

#### **Bond Types**

This section shows the bond types for a virtual switch.

**Table 37: Bond Types**

This table shows the Bond Types.

<b>Bond Type</b>	<b>Use Case</b>	<b>Maximum VM NIC Throughput</b>	<b>Maximum Host Throughput</b>
Active-Backup	Recommended. Default configuration, which transmits all traffic over a single active adapter.	10 Gb	10 Gb

Bond Type	Use Case	Maximum VM NIC Throughput	Maximum Host Throughput
Active-Active with MAC pinning  Also known as balance-slb	Works with caveats for multicast traffic. Increases host bandwidth utilization beyond a single 10 Gb adapter. Places each VM NIC on a single adapter at a time. Do not use this bond type with link aggregation protocols such as LACP.	10 Gb	20 Gb
Active-Active  Also known as LACP with balance-tcp	LACP and link aggregation required. Increases host and VM bandwidth utilization beyond a single 10 Gb adapter by balancing VM NIC TCP and UDP sessions among adapters. Also used when network switches require LACP negotiation.  The default LACP settings are: <ul style="list-style-type: none"> <li>• Speed—Fast (1s)</li> <li>• Mode—Active fallback-active-backup</li> <li>• Priority—Default. This is not configurable.</li> </ul>	20 Gb	20 Gb
No Uplink Bond	No uplink or a single uplink on each host.  Virtual switch configured with the No uplink bond bond type has 0 or 1 uplinks. When you configure a virtual switch with any other bond type, you must select at least two uplink ports on every node.	-	-

## Updating a Virtual Switch

Update an existing virtual switch in the Nutanix cluster.

### About this task

For information about virtual switch, see [Layer 2 Network Management](#) in the *AHV Administration Guide*.

To update a virtual switch, follow these steps:

### Procedure

1. Log in to the Prism Element web console.

2. Perform one of the following:
    - » Go to **VM > Network Config**.
    - » Go to **Settings > Network > Network Configuration**.
- The system displays the **Network Configuration** page.
3. Click the **Virtual Switch** tab.
  4. To update a virtual switch, click the edit icon associated with the switch.  
The system displays the **Edit Virtual Switch** page.
  5. Enter the necessary values in the respective fields.  
The fields in the **Edit Virtual Switch** page is identical to the fields in the **Create Virtual Switch** page. For more information, see [Creating a Virtual Switch](#) on page 151.
  6. Click **Save** to update an existing virtual switch.

## Deleting a Virtual Switch

Delete an existing virtual switch from a Nutanix cluster.

### About this task

For more information about virtual switch, see [Layer 2 Network Management](#) in the *AHV Administration Guide*.

When you delete a virtual switch, the bridge created by the virtual switch is also removed completely.

You can also disable all the virtual switches. However, you can do this only using CLI. The Prism Element web console does not support disabling virtual switches. Use the net.disable\_virtual\_switch command to disable the virtual switch functionality and remove all the virtual switches including the default virtual switch vs0. However, the bridge and uplink bond or interface configurations are not affected by this command. This action cannot be undone either.

To delete a virtual switch, follow these steps:

### Procedure

1. Log in to the Prism Element web console.
  2. Perform one of the following:
    - » Go to **VM > Network Config**.
    - » Go to **Settings > Network > Network Configuration**.
- The system displays the **Network Configuration** page.
3. Click the **Virtual Switch** tab.
  4. To delete a virtual switch, click the delete icon associated with the switch.  
The system prompts you to confirm the delete action.
  5. Click **Delete** to confirm.

### What to do next

Ensure if the virtual switch is deleted from the list on the **Virtual Switch** tab.

## Migrating Bridges after Upgrade

Migrate or convert a bridge in the cluster to virtual switches after you upgrade the minimum or compatible version of AOS and AHV.

### Before you begin

Ensure that the following prerequisites are met before migrating or converting a bridge to a virtual switch.

- The bridge to be converted to a virtual switch must have consistent configurations across all the nodes in the cluster in terms of bond-type, MTU and LACP parameters.
- The VLAN IDs in a virtual switch must be exclusive across networks, except when a network is IPAM enabled and the other network is not IPAM enabled. In a scenario where an existing bridge has duplicate VLAN IDs, only one network (per IPAM state) gets migrated under the virtual switch, while the additional networks remains unchanged with no impact to the functionality.

**Note:**

Networks with same VLAN IDs can exist across different virtual switches.

### About this task

You can migrate or convert bridges, other than br0, to virtual switches after you upgrade the minimum or compatible version of AOS and AHV. You can convert only one bridge at a time. You need to repeat the workflow for every bridge that you want to convert to a virtual switch.

**Note:** You cannot migrate any bridge using Prism Central. Use the Prism Element web console or aCLI to migrate or convert the bridges. The migration process creates new virtual switches that host the bridges that are being migrated or converted.

You can convert only one bridge at a time. You need to repeat the workflow for every bridge that you want to convert to a virtual switch.

**Note:** The migration process creates new virtual switches which host the bridges that are being migrated or converted.

To migrate the bridges after an upgrade, follow these steps:

### Procedure

- Log in to the Prism Element web console.
- From the dropdown menu, click **Network**.  
The system displays the **Network** dashboard.

- Click the **Convert Bridges to VS** option at the bottom left of the **Network** dashboard.

If there are no bridges to migrate, the system displays the There are no OVS bridges that can be converted to virtual switches message in the **Convert Bridges to VS** dialog box.

The system displays the **Convert Bridges to VS** dialog box.

- From the **Select a Bridge** dropdown menu, select the bridge to migrate.

The **Select a Bridge** drop down field provides a list of bridges you can migrate. Select the bridge you want to migrate and complete the following steps.

- Provide a name and a description for the virtual switch that you want to create by migrating the bridge.

For example, if you select *br1* in **Select a Bridge**, you can provide *vs1* as the name for the virtual switch.

## 5. Click **Convert**.

The system displays the converted virtual switch in the **Network** page of the Prism Element web console and in the **Virtual Switch** tab on the **Network Configuration** page in Prism Central.

### Re-Configuring Bonds Across Hosts Manually

Before upgrading AOS to the latest version, you must migrate the existing bridges to virtual switches. If bond configurations are inconsistent across hosts before migrating the bridges, the virtual switches might not deploy correctly after migration. To resolve this, manually configure the bonds to ensure consistency.

#### Before you begin

Ensure that cluster meets the following requirements before you reconfigure the bonds:

- Place the affected AHV host where you want to reconfigure the bonds into maintenance mode.

Log on to any CVM using SSH, and run the following command:

```
nutanix@cvm$ acli host.enter_maintenance_mode hypervisor-IP-address [wait="{ true | false }" ] [non_migratable_vm_action="{ acpi_shutdown | block }" ]
```

Replace *hypervisor-IP-address* with either the IP address or host name of the AHV host you want to shut down.

The following are optional parameters for running the `acli host.enter_maintenance_mode` command:

- wait:** Set the **wait** parameter to **true** to wait for the host evacuation attempt to finish.
- non\_migratable\_vm\_action:** By default the **non\_migratable\_vm\_action** parameter is set to **block**, that prevents the host from entering maintenance mode, if non-migratable VMs exist. For more information on non-migratable VMs, see [Non-Migratable VMs](#).

**Note:** VMs with host affinity policies are also not migrated to other hosts in the cluster, if any of the following condition is met:

- The hosts that are configured as part of VM-Host affinity policy are not available.
- The hosts that are part of VM-Host affinity policy does not have the sufficient resources to run the VM.

If you want to automatically shut down such VMs, set the **non\_migratable\_vm\_action** parameter to **acpi\_shutdown**.

For more information, see [Putting a Node into Maintenance Mode using CLI](#).

- Check the **Cluster Resiliency / Fault Tolerance Status** widget in the Prism Element web console dashboard to ensure that the cluster is healthy and resilient to any brief interruptions to network connectivity during uplink changes.

#### About this task

##### Important:

- Perform the bond changes only on one host at a time. Ensure that you get the completed host out of maintenance mode before you proceed to work on any other affected hosts.

- Use this procedure only to modify the inconsistent bonds in a migrated bridge across hosts in a cluster, that is preventing Acropolis (AOS) from deploying the virtual switch for the migrated bridge.

Do not use **nmcli** commands to make the bridge level changes. Use the **manage\_ovs** commands, instead.

The **manage\_ovs** command updates the cluster configuration, with changes applied and retained across host restarts. However, the **nmcli** command updates the live running host configuration but does not update the AOS cluster configuration causes the changes are lost at host restart. This behavior might lead to connectivity issues during maintenance, such as upgrades or hardware replacements.

The **nmcli** command is typically used in scenarios where a host might be isolated on the network and requires a workaround to gain connectivity before the cluster configuration can actually be updated using the **manage\_ovs** command.

**Note:** Disable the virtual switch before you attempt to change the bonds or bridge.

If you face an issue where the virtual switch is automatically re-created after it is disabled, follow steps 1 and 2 in this procedure to disable the automatically re-created virtual switch again before migrating the bridges. For more information, see [KB-3263](#).

Be cautious when you use the **disable\_virtual\_switch** command because it deletes all the configurations from IDF, not only for the default virtual switch **vs0**, but also any virtual switches that you may have created (such as **vs1** or **vs2**). Therefore, before you use the **disable\_virtual\_switch** command, ensure that you check a list of existing virtual switches, that you can get using the **acli net.get\_virtual\_switch** command.

Complete this procedure on each host Controller VM that is sharing the bridge that needs to be migrated to a virtual switch.

## Procedure

1. List the virtual switch.

```
nutanix@cvm$ acli net.list_virtual_switch
```

2. Disable all the virtual switches.

```
nutanix@cvm$ acli net.disable_virtual_switch
```

All the virtual switches in the cluster are disabled.

3. Change the bond type to ensure consistency across all the hosts for the specified virtual switch

```
nutanix@cvm$ manage_ovs --bridge_name bridge-name --bond_name bond_name --  
bond_mode bond-type update_uplinks
```

Where:

- *bridge-name*: Provide the name of the bridge, such as **br0** for the virtual switch on which to set the uplink bond mode.
- *bond-name*: Provide the name of the uplink port such as **br0-up** to set the bond mode.
- *bond-type*: Provide the bond mode that required to be used uniformly across the hosts on the named bridge.

Use the `manage_ovs --help` command for help on this command.

**Note:** To disable LACP, change the bond type from LACP Active-Active (balance-tcp) to Active-Backup/Active-Active with MAC pinning (balance-slb) by setting the *bond\_mode* using this command as active-backup or balance-slb.

Ensure that you turn off LACP on the connected ToR switch port. To avoid blocking of the bond uplinks during the bond type change on the host, ensure that you follow the ToR switch best practices to enable LACP fallback or passive mode.

To enable LACP, configure *bond-type* as balance-tcp (Active-Active) with additional variables `--lacp_mode fast` and `--lacp_fallback true`.

4. Exit the host from maintenance mode.

```
nutanix@cvm$ acli host.exit_maintenance_mode hypervisor-IP-address
```

Replace *hypervisor-IP-address* with the IP address of the AHV host.

This command migrates (live migration) all the VMs that were previously running on the host back to the host. For more information, see [Exiting a Node from the Maintenance Mode Using CLI](#) in the AHV Administration Guide.

5. Repeat the above steps for each host for which you intend to reconfigure bonds.

### What to do next

After you make the bonds consistent across all the hosts configured in the bridge, migrate the bridge or enable the virtual switch. For more information, see:

- [Re-Configuring Bonds Across Hosts Manually](#) on page 157.
- [Network Configuration](#) in the *Prism Central Infrastructure Guide*.

To check whether LACP is enabled or disabled, use the following command.

```
nutanix@cvm$ manage_ovs show_uplinks
```

## MAC Address Prefix

You can avoid duplicate IP addresses in a single-cluster or multi-cluster environment by implementing one of two possible configurations:

- Nutanix recommends that you assign a set of unique VLANs for guest VMs on each AHV cluster. Ensure these VLANs do not overlap with the VLANs on other AHV clusters. Assigning unique VLAN ranges for each cluster reduces the risk of MAC address conflicts and also ensures compliance with the general best practice of maintaining small Layer 2 broadcast domains with limited numbers of endpoints.

- If multiple AHV clusters need to share the same VLAN, or when guest VM MAC addresses needs to be globally unique among multiple AHV clusters, configure a predefined MAC address prefix for each AHV cluster.

By default, Nutanix does not guarantee unique MAC address assignment between Nutanix clusters with VLAN networks.

### Sample Design Scenario with Multiple Sites and Clusters

Using locally administered MAC addresses, you can ensure unique MAC addresses for VMs in an environment made up of multiple sites and clusters.

A MAC address is usually a 6-octet hexadecimal address block. The notation for a MAC address is **xx:xx:xx:xx:xx:xx**. In this 6-octet address, the first 3 octets are the organizationally unique identifier (OUI) octets or the MAC address prefix OUI. The second bit of the 1st octet (the first hexadecimal number **xx**) is set to 1 to make the MAC address a locally administered MAC address. The next 3 octets are NIC specific octets, **xx:xx:xx**, and it represents the useable hexadecimal range for endpoints within each AHV cluster.

**Note:** By default, AHV clusters use the MAC address prefix OUI 50:6B:8D.

By default, Acropolis leader generates MAC address for a VM on AHV. The first 24 bits of the MAC address (OUI) is set to 50-6b-8d (0101 0000 0110 1101 1000 1101) and are reserved by Nutanix, the 25th bit is set to 1 (reserved by Acropolis leader), the 26th bit to 48th bits are auto generated random numbers.

Consider this sample design of a deployment with three sites and five clusters in each site. Define a unique MAC address prefix for Site1-Cluster1 such as 02:01:01, where:

- 02—Defines the MAC address as a unicast address that is locally administered. This value could be a hexadecimal number defined by X2, X3, X6, X7, XA, XB, or XE series, where X is any valid hexadecimal value such that the second binary bit (binary bits being counted from right to left, right most is the first bit) of the binary equivalent of this hexadecimal number **xx** is set to 1 to make the MAC address a locally administered MAC address.
- 01—Used to identify, for example, the site number. This value could be any valid hexadecimal value.
- 01—Used to identify, for example, the AHV cluster within the site. This value could be any valid hexadecimal value

The NIC specific octets, **xx:xx:xx**, are auto-assigned to the VM NICs or the endpoints within each AHV cluster. Thus, for Site1, the clusters would have the following prefixes:

- Site1-Cluster1: 02:01:01
- Site1-Cluster2: 02:01:02
- Site1-Cluster3: 02:01:03
- Site1-Cluster4: 02:01:04
- Site1-Cluster5: 02:01:05

... and so on for the other clusters at Site1.

Similarly for Site2, if you define, for example 02:02:01 as the MAC address prefix for the first cluster - Cluster1, you get the series of predefined MAC address prefixes for the clusters and VMs or endpoints in Site2, Cluster1.

- Site2-Cluster1-VM1: 02:02:01:00:00:01
- Site2-Cluster1-VM2: 02:02:01:00:00:02
- ...
- Site2-Cluster1-VM10: 02:02:01:00:00:0A

... and so on for the other clusters at Site2.

## **Adding a MAC Address Prefix**

Add a MAC address prefix to a cluster.

### **Before you begin**

Ensure that the guest VMs in the cluster do not have any NICs that have MAC addresses with the default prefix before you add a MAC address prefix.

### **About this task**

Use aCLI to configure the MAC address prefix for a cluster.

### **Procedure**

1. Log in to a Controller VM in your cluster with SSH.

2. Access Acropolis CLI using the `acli` command.

```
nutanix@cvm$ acli
```

The prompt changes to `<acropolis>`.

3. Add the MAC address prefix for the cluster using the following command.

```
<acropolis> net.set_mac_prefix XX:XX:XX
```

#### **Warning:**

Ensure that you do not set the MAC address prefix to `52:6b:8d` as this might lead to a conflict due to one of the guest VMs acquiring `52:6b:8d:00:00:00` IP, which AHV uses internally for packet probing purposes.

Replace `XX:XX:XX` by the MAC address prefix for the cluster.

Using the example discussed in [MAC Address Prefix](#) on page 159, the following sample command adds the `02:01:01` as the MAC address prefix for Site1-Cluster1

```
<acropolis> net.set_mac_prefix 02:01:01
```

### **What to do next**

Verify if the MAC address prefix is configured using the `net.get_mac_prefix` command.

The output displays the hexadecimal prefix that you configured.

Using the configuration example, the output would show `"02:01:01"` as follows:

```
<acropolis> net.get_mac_prefix  
"02:01:01"  
<acropolis>
```

Repeat this procedure to add MAC address prefixes to other clusters that share the same VLAN (defining the common broadcast domain) to prevent duplicate MAC addresses.

## **Removing the MAC Address Prefix**

Remove the MAC address prefix of a cluster.

### **Before you begin**

Remove the MAC addresses with the configured prefix from the VM NICs in the cluster.

### **About this task**

Use aCLI commands to remove the MAC address prefix for a cluster. After removing the MAC address prefix added to a cluster manually, the cluster uses the default MAC prefix, "50:6b:8d".

## Procedure

1. Log on to a Controller VM in your cluster with SSH.
2. Access Acropolis CLI using the `acli` command.

```
nutanix@cvm$ acli
```

The prompt changes to `<acropolis>`.

3. Remove the MAC address prefix for the cluster using the following command.

```
<acropolis> net.clear_mac_prefix
```

## What to do next

Verify that the MAC address prefix is removed. When you use the `net.get_mac_prefix` command, the output displays the default MAC address prefix, `"50:6b:8d"`.

```
<acropolis> net.get_mac_prefix  
"50:6b:8d"  
<acropolis>
```

## Network Configuration for VM Interfaces

In clusters with Nutanix virtualization management (such as those running AHV), you can configure network connections through the web console. Each VM network interface is bound to a virtual network, and each virtual network is bound to a single VLAN. Additionally, on AHV, Hyper-V, and ESXi, you can secure intra-cluster communications by segmenting the virtual network on the cluster.

To configure a virtual network for VM interfaces, do one of the following:

- To configure virtual networks for user VM interfaces, see [Creating a Basic VLAN Subnet for Guest VM Interfaces](#) on page 162.
- To secure intra-cluster communications by configuring network segmentation, see [Securing Traffic Through Network Segmentation](#) in the *Nutanix Security Guide*.

## Creating a Basic VLAN Subnet for Guest VM Interfaces

Create a basic VLAN subnet for guest VMs using the Prism Element web console. You can associate the network with a VLAN and configure IP address management for VMs on the network.

### About this task

**Note:** Do not add any other device (including guest VMs) to the VLAN to which the CVM and hypervisor host are assigned. Isolate guest VMs on one or more separate VLANs.

To create a basic VLAN subnet for guest VM interfaces, follow these steps:

## Procedure

1. Log in to the Prism Element web console.

2. Perform one of the following:

- » Go to **VM > Network Config**.
- » Go to **Settings > Network > Network Configuration**.

**Note:** This option only appears in clusters that support this feature.

The **Network Configuration** window appears.

3. Click the **Subnets** tab and click **+ Create Subnet**.

In the Create Subnet dialog box that opens, perform the following in the indicated fields:

- Subnet Name:** Enter a name for the subnet or network.

Nutanix recommends assigning unique names to each VLAN subnet for easier identification. While using duplicate names is allowed, it results in multiple subnets with the same name but different UUIDs in the subnet list.

- Virtual Switch:** Select the virtual switch that you want to associate with the subnet.

- VLAN ID:** Enter the number of the VLAN.

Enter just the number in this field, for example 1 or 27. Enter 0 for the native VLAN. The system displays the value as vlan.1 or vlan.27.

- Enable IP Address Management:** Select the checkbox to enable cluster control IP addressing in the network.

Selecting this checkbox displays additional fields. If you do not select the checkbox, Nutanix Files does not attempt network management, assuming VLAN management is handled outside the cluster.

**Note:** If you do not select this checkbox while creating a network, you cannot enable or disable IP address management (IPAM).

For information on IP address management, see [IP Address Management](#) in the *AHV Administration Guide*.

- Network IP Prefix:** Enter the gateway IP address for the network, followed by the network prefix in CIDR notation (for example, 10.1.1.0/24).

- Gateway IP Address:** Enter the default gateway IP address of the VLAN subnet.

- DHCP Settings:** Select this checkbox to display the fields to define a domain.

- Domain Name Servers (Comma Separated):** Enter a comma-separated list of DNS servers.

- Domain Search (Comma Separated):** Enter a comma-separated list of domains.

- Domain Name:** Enter the VLAN domain name.

- TFTP Server Name:** Enter the host name or IP address of the TFTP server from which virtual machines can download a boot file.

Required in a Pre-boot eXecution Environment (PXE).

- Boot File Name:** Enter the name of the boot file to download from the TFTP server.

4. To define a IP range of addresses for automatic assignment to virtual NICs, click **Create Pool** and enter the following in the **Add IP Pool** dialog box:  
If you do not create a pool, you must assign IP addresses to VMs manually.
  - a. Enter the starting IP address of the range in the **Start Address** field.
  - b. Enter the ending IP address of the range in the **End Address** field.
  - c. Click **Submit** to save the changes and return to the **Create Subnet** dialog box.
5. To configure a DHCP server, select the **Override DHCP server** checkbox and enter an IP address in the **DHCP Server IP Address** field.  
This address (reserved IP address for the Acropolis DHCP server) is visible only to VMs on this network and responds only to DHCP requests. If you do not select the checkbox, the system does not display the **DHCP Server IP Address** field, and automatically generates the DHCP server IP address. The generated address is `network_IP_address_subnet.254`, or `network_IP_address_subnet.253` if the default gateway is using .254.
6. After entering all the information is correct, click **Save** to create the subnet.

**Note:**

- You can also specify network mapping to control network configuration for the VMs when they start on the remote site. For more information about configuring networking mapping on remote site, see [Configuring a Remote Site \(Physical Cluster\)](#) in the *Data Protection and Recovery with Prism Element Guide*.
- Verify (or update as needed) that the physical switch configuration allows traffic for the same VLAN's that are configured for the virtual networks.

### Verifying IPAM Address Pool for Sufficient IP Addresses

This procedure verifies the IPAM managed IP address pool for sufficient IP addresses and checks when the IP pool is close to running out of IP addresses.

#### About this task

To verify the IPAM managed IP address pool for sufficient IP addresses, do the following:

#### Procedure

1. Click the gear icon in the main menu and then select **Network Configuration** in the **Setting** page.

- Select the **Networks** tab (default) to view networks for the VMs in the **Network Configuration** dialog box. It consists of the following:
  - Network Name:** Displays the networks configured on the VM.
  - Virtual Switch:** Displays the virtual Switch configured on the VM.
  - VLAN ID:** Displays the VLAN ID configured on the VM.
  - Used IP Addresses:** Displays the number of IP addresses in use by the IPAM enabled network. Click on the value displayed to view which VM is using which IP addresses from the IPAM enabled network.

**Used IP Addresses for ipam network** X

---

Used IP Addresses			1 - 4 of 4	5 rows <span style="font-size: small;">▼</span>
IP Address <span style="font-size: small;">▼</span>	MAC Address <span style="font-size: small;">▼</span>	VM Name <span style="font-size: small;">▼</span>		
Search by IP Address, MAC Address or VM Name...				
192.168.123.0	-	-		
192.168.123.1	-	-		
192.168.123.254	-	-		
192.168.123.71	50:6b:8d:b8:1a:54	VM1		

---

1 - 4 of 4 ▼ | 5 rows ▼

Close

**Figure 32: Used IP Address for IPAM Network**

- Free IPs in Subnets:** Displays the number of IP addresses configured in the subnet.
- Free IPs in Pool:** Displays the number of free IPs available in the IP Pool configured for the subnet. The value in this field dynamically changes every time the network dynamically assigns a new IP to a VM.
- Actions:** You can select either the **Edit** or **Delete** actions to update the Network configuration.

## Modifying a Basic VLAN Subnet in Guest VM Interfaces

Modify a basic VLAN subnet in guest VMs using the Prism Element web console.

### About this task

To modify a VLAN subnet follow these steps:

### Procedure

1. Log in to the Prism Element web console.
2. Perform one of the following:

- » Go to **VM > Network Config**.
- » Go to **Settings > Network > Network Configuration**.

The system opens the **Network Configuration** page displaying the Subnets tab.

3. To modify a subnet, click the **Edit** option associated with the subnet.  
The system displays the **Update Subnet** dialog box.

4. Enter the necessary values in the respective fields.

The fields in the **Update Subnet** dialog box is identical to the fields in the **Create Subnet** dialog box. For more information, see [Creating a Basic VLAN Subnet for Guest VM Interfaces](#) on page 162.

**Note:** You cannot change the VLAN ID of an active network; only the name can be modified.

5. After entering all the information, click **Save** to modify the subnet.

## Deleting a Basic VLAN Subnet

Delete a basic VLAN subnet in a Nutanix cluster.

### About this task

To modify a VLAN subnet follow these steps:

### Procedure

1. Log in to the Prism Element web console.

2. Perform one of the following:

- » Go to **VM > Network Config**.
- » Go to **Settings > Network > Network Configuration**.

The system opens the **Network Configuration** page displaying the Subnets tab.

3. To delete a subnet, click the **Delete** option associated with the subnet.  
The system prompts you to confirm the delete action.

4. Click **Delete** to confirm.

## Network Segmentation

You can segment the network on a Nutanix cluster by using Prism Element.

For more information, see [Securing Traffic Through Network Segmentation](#) in the *Security Guide*.

# Configuring a Network Switch

Configure a new network switch using the Prism Element web console.

## About this task

To track and record networking statistics for a cluster, the cluster requires information about the first-hop network switches and the switch ports being used. RFC 2674-compliant switches support switch port discovery. Switch port discovery involves obtaining statistics from Q-BRIDGE-MIB on the switch and then identifying the MAC address that corresponds to the host. Such discovery is currently best-effort, so it is possible that, at times, an interface might not be discovered.

## Before you begin

Configure the corresponding SNMP settings on the first-hop network switch.

## About this task

To configure a network switch for statistics collection, follow these steps:

### Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu, select **Settings**.  
The system displays the **Global Settings** page.
3. From the Network section on the left navigation pane, select **Network Switch**.

**Note:** Network switch configuration is supported only for AHV clusters.

The system opens the **Network Switch Configuration** page displaying the **Switch Configuration** tab.

4. Click **+ Add Switch Configuration**.

5. Do the following in the indicated fields:

a. **Switch Management IP Address:** Enter the management IP address of the switch or the fully qualified switch name.

b. **Host IP Addresses or Host Name (Separated by Commas):** Enter the IP address or the fully qualified host name of each host in the cluster that uses the switch to route traffic.

If there are multiple hosts, enter the IP addresses in a comma separated list. Failing to add the host list might result in issues with switch port discovery.

c. **SNMP Profile:** Select the SNMP profile to apply (or **None**) from the dropdown menu.

The dropdown menu lists the SNMP profiles you have created.

**Note:** Selecting a profile populates the remaining fields automatically with the profile values. If you have not created a profile (or have selected **None**), you must enter the values in the remaining fields manually.

d. **SNMP Version:** Select the SNMP version to use from the dropdown menu.

e. **SNMP Security Level** (for SNMPv3 only): Select the security level to enforce from the drop-down list.

The options are **No Authorization No Privacy**, **Authorization But No Privacy**, and **Authorization and Privacy**. This field appears only when SNMPv3 is selected as the version.

f. **SNMP Community Name** (for SNMPv2c only): Enter the SNMP community name to use.

g. **SNMP Username:** Enter the SNMP user name.

h. **SNMP Authentication Type:** Select the authentication protocol to use from the drop-down list.

The options are **None** and **SHA**.

**Note:** This field and the following three fields are set to **None** or left blank (and read only) when the version is SNMPv2c or the security level is set to no authorization.

i. **SNMP Authentication Pass Phrase:** Enter the appropriate authentication pass phrase.

j. **SNMP Privacy Type:** Select the privacy protocol to use from the drop-down list.

The options are **None**, **AES**, and **DES**.

k. **SNMP Privacy Pass Phrase:** Enter the appropriate privacy pass phrase.

l. After entering all the information, click **Save**.

The system saves the profile and displays the new entry in the Switch Configuration tab.

**Note:** As a security protection, the **SNMP Authentication Pass Phrase** and **SNMP Privacy Pass Phrase** fields appear blank after saving (but the entered phrases are saved).

## Modifying a Network Switch Configuration

Modify an existing network switch in a Nutanix cluster.

### About this task

To modify a network switch, follow these steps:

### Procedure

1. Log in to the Prism Element web console.

2. From the dropdown menu, select **Settings**.

The system displays the **Global Settings** page.

- From the **Network** section on the left navigation pane, select **Network Switch**.

**Note:** Network switch configuration is supported only for AHV clusters.

The system opens the **Network Switch Configuration** page displaying the **Switch Configuration** tab.

- To modify a network switch configuration, click the **Edit** icon associated with the switch.  
The system displays the configuration fields.

- Enter the necessary values in the respective fields.

The configuration fields are identical to the fields in the procedure to configure a network switch. For more information, see [Configuring a Network Switch](#) on page 167.

## Deleting a Network Switch

Delete a network switch from a Nutanix cluster.

### About this task

To delete a network switch, follow these steps:

### Procedure

- Log in to the Prism Element web console.
- From the dropdown menu, select **Settings**.  
The system displays the **Global Settings** page.
- From the **Network** section on the left navigation pane, select **Network Switch**.

**Note:** Network switch configuration is supported only for AHV clusters.

The system opens the **Network Switch Configuration** page displaying the **Switch Configuration** tab.

- To delete a network switch, click the **Delete** icon associated with the switch.  
The system prompts you to confirm the delete action.
- Click **Yes** to confirm.

## Enabling LACP and LAG (AHV Only)

Enable LAG and LACP in AHV nodes and the Top-of-Rack (ToR) switch or any switch that is directly connected to the Nutanix node.

### Procedure

To enable LACP and LAG, follow these steps:

- Log in to the Prism Element web console.
- Perform one of the following:
  - Go to **VM > Network Config**.
  - Go to **Settings > Network > Network Configuration**.

The system opens the **Network Configuration** page displaying the Subnets tab.

- Click the **Virtual Switch** tab.

- To configure LACP and LAG on a virtual switch, click the **Edit** icon associated with the switch. The system opens the **Edit Virtual Switch** page displaying the **General** tab.
- Select the **Standard (Recommended)** option, and click **Next**.

**Important:** When you select the **Standard** method, only the hosts that have been updated are restarted.

The **Standard** configuration method puts each updated node in maintenance mode before applying the updated settings. After applying the updated settings, the node exits from maintenance mode. For more information, see [Virtual Switch Workflow](#).

The system displays the **Uplink Configuration** tab.

- From the **Bond Type** dropdown menu, select **Active-Active**, and click **Save**.

**Note:** The Active-Active bond type configures all AHV hosts with the fast setting for LACP speed, causing the AHV host to request LACP control packets at the rate of one per second from the physical switch. In addition, the Active-Active bond type configuration sets LACP fallback to Active-Backup on all AHV hosts. You cannot modify these default settings after you have configured them in Prism, even by using the CLI.

This completes the LAG and LACP configuration on the cluster. At this stage, cluster starts the rolling reboot operation for all the AHV hosts. Wait for the reboot operation to complete before you put the node and CVM in maintenance mode and change the switch ports.

For more information about how to manually perform the rolling reboot operation for an AHV host, see [Rebooting an AHV Node in a Nutanix Cluster](#).

Perform the following steps on each node, one at a time:

- Put the node and the Controller VM into maintenance mode.

**Note:** Before you put a node in maintenance mode, see [Verifying the Cluster Health](#) and carry out the necessary checks.

For more information, see [Putting a Node into Maintenance Mode using Web Console](#) in the AHV Administration Guide.

- Change the interface settings on the switch directly connected to the Nutanix node to match the LACP and LAG settings configured in the **Edit Virtual Switch** window.

For information on how to change the LACP settings, refer to the vendor-specific documentation of the deployed switch.

Nutanix recommends you perform the following configurations for LACP settings on the switch:

**Table 38: Nutanix Recommendations for LACP Settings**

Nutanix Recommendations	Description
Enable LACP fallback	<p>Nutanix recommends you enable LACP fallback to set up a workaround for the port, using which the port establishes a link before the switch receives the LACP Bridge Protocol Data Units (BPDUs).</p> <p>The LACP fallback helps avoid link failures if either AHV host or switch that is connected to the AHV node does not negotiate LACP.</p> <p>LACP fallback provides seamless discovery of new nodes in an active or passive capacity setup and reduces the impact on the node operation. When LACP fallback is enabled, you can have a minimal business impact as VMs and applications remain healthy in case of an LACP status mismatch between the AHV host and the ToR switch port.</p> <p>As LACP fallback ensures connectivity during initial deployment, so it is crucial when you do not have LACP in discoveryOS.</p>
Consider the LACP time options ( <i>slow and fast</i> )	<p>If the switch has a fast configuration, Nutanix recommends you set the LACP time to fast on AHV host.</p> <p>Nutanix recommends matching the LACP time on both the switch and the AHV host to ensure simultaneous L2 failure detection. This way, if an interface fails, both the switch and AHV host will detach it at the same time. It also helps to prevent an outage. When LACP time is set to fast, the failure detection occurs within 3 seconds, and if it is set to slow, failure detection takes up to 90 seconds.</p> <p><b>Caution:</b> When LACP fallback occurs, the port runs in fallback mode, and this might lead to an unbalanced utilization of ports and lack of redundancy in your site deployment. Based on your internal networking policies, you can decide whether LACP fallback is helpful for you, and enable or disable it.</p>

- 9.** Verify whether the LACP negotiation status displays as `Negotiated` in the output, by performing the following steps.

SSH to the CVM as a Nutanix user, and run the following commands:

```
nutanix@CVM$ ssh root@[AHV host IP] "ovs-appctl bond/show bond-name"
```

```
nutanix@CVM$ ssh root@[AHV host IP] "ovs-appctl lacp/show bond-name"
```

- Replace:
  - `bond-name` with the actual name of the uplink port such as `br0-up`.
  - `[AHV host IP]` with the actual AHV host IP at your site.
- Search for the string `negotiated` in the status lines.

- 10.** Remove the node and Controller VM from maintenance mode.

The Controller VM exits maintenance mode during the same process. For more information, see [Exiting a Node from the Maintenance Mode using Web Console](#).

## What to do next

- Verify that the status of all services on all the CVMs are Up. Run the following command and check if the status of the services is displayed as **Up** in the output:

```
nutanix@cvm$ cluster status
```

- Log in to the Prism Element web console of the node and ensure that the **Cluster Resiliency / Fault Tolerance Status** widget displays **OK**.

## Create an SNMP profile for the network switch

### About this task

If you need to configure multiple network switches, it might be useful to create one or more SNMP profiles that can be applied when configuring the switches. For information on configuring a network switch, see [Configuring a Network Switch](#) on page 167.

To create an SNMP profile, follow these steps:

### Procedure

- Log in to the Prism Element web console.
- From the dropdown menu, select **Settings**.  
The system displays the **Global Settings** page.
- From the **Network** section on the left navigation pane, select **Network Switch**.

**Note:** Network switch configuration is supported only for AHV clusters.

The system opens the **Network Switch Configuration** page displaying the **Switch Configuration** tab.

- Click the **SNMP Profile** tab and click **+ SNMP Profile**.

5. Do the following in the indicated fields:
  - a. **Profile Name:** Enter a name for the profile.
  - b. **SNMP Version:** Select the SNMP version to use from the dropdown menu.
  - c. **SNMP Security Level** (for SNMPv3 only): Select the security level to enforce from the dropdown menu.
  - d. **SNMP Community Name** (for SNMPv2c only): Enter the SNMP community name to use.
  - e. **SNMP Username:** Enter the SNMP user name.
  - f. **SNMP Authentication Type:** Select the authentication protocol to use from the pull-down list.  
The options are **None** and **SHA**.

**Note:** This field and the following three fields are set to **None** or left blank (and read only) when the version is SNMPv2c or the security level is set to no authorization.

- g. **SNMP Authentication Pass Phrase:** Enter the appropriate authentication pass phrase.
- h. **SNMP Privacy Type:** Select the privacy protocol to use from the pull-down list.  
The options are **None**, **AES**, and **DES**.
- i. **SNMP Privacy Pass Phrase:** Enter the appropriate privacy pass phrase.
- j. After entering all information, click **Save**.

The system saves the profile and displays the new entry in the SNMP Profile tab.

## Modifying an SNMP Profile

Modify an existing SNMP profile in the cluster.

### About this task

To modify a SNMP profile, follow these steps:

### Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu, select **Settings**.  
The system displays the **Global Settings** page.
3. From the **Network** section on the left navigation pane, select **Network Switch**.

**Note:** Network switch configuration is supported only for AHV clusters.

The system opens the **Network Switch Configuration** page displaying the **Switch Configuration** tab.

4. Click the **SNMP Profile** tab.
5. To modify an SNMP profile, click the **Edit** icon associated with the profile.  
The system displays the configuration fields.
6. Enter the necessary values in the respective fields.  
The configuration fields are identical to the fields in the procedure to create an SNMP profile. For more information, see [Create an SNMP profile for the network switch](#) on page 172.
7. After entering all information, click **Save** to modify the SNMP profile.

## Deleting an SNMP Profile

Delete an SNMP profile from a Nutanix cluster.

### About this task

To delete a SNMP profile, follow these steps:

### Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu, select **Settings**.  
The system displays the **Global Settings** page.
3. From the **Network** section on the left navigation pane, select **Network Switch**.

**Note:** Network switch configuration is supported only for AHV clusters.

The system opens the **Network Switch Configuration** page displaying the **Switch Configuration** tab.

4. Click the **SNMP Profile** tab.
5. To delete an SNMP profile, click the **Delete** icon associated with the profile.  
The system prompts you to confirm the delete action.
6. Click **Yes** to confirm.

## Network Visualization

The network visualizer is a consolidated graphical representation of the network formed by the VMs and hosts in a Nutanix cluster and first-hop switches. You can use the visualizer to monitor the network and to obtain information that helps you troubleshoot network issues.

You can use the visualizer to view the following:

- Physical and logical network topology.
- Summary of the number and types of devices in the network.
- Network configuration of the devices in the topology and of components such as physical and virtual NICs.
- Real-time usage graphs of physical and virtual interfaces.

**Note:**

- You cannot use the visualizer to configure a network.
- The network visualizer is available only on AHV clusters.

## Prerequisites

Before you use the network visualizer, do the following:

- Configure network switch information on the Nutanix cluster. For more information, see [Configuring a Network Switch](#) on page 167.
- Enable LLDP or CDP on the first-hop switches. The visualizer uses LLDP or CDP to determine which switch port is connected to a given host interface. If LLDP or CDP is unavailable, SNMP data is used on a commercially reasonable effort. For information about configuring LLDP or CDP, see the switch manufacturer's documentation.

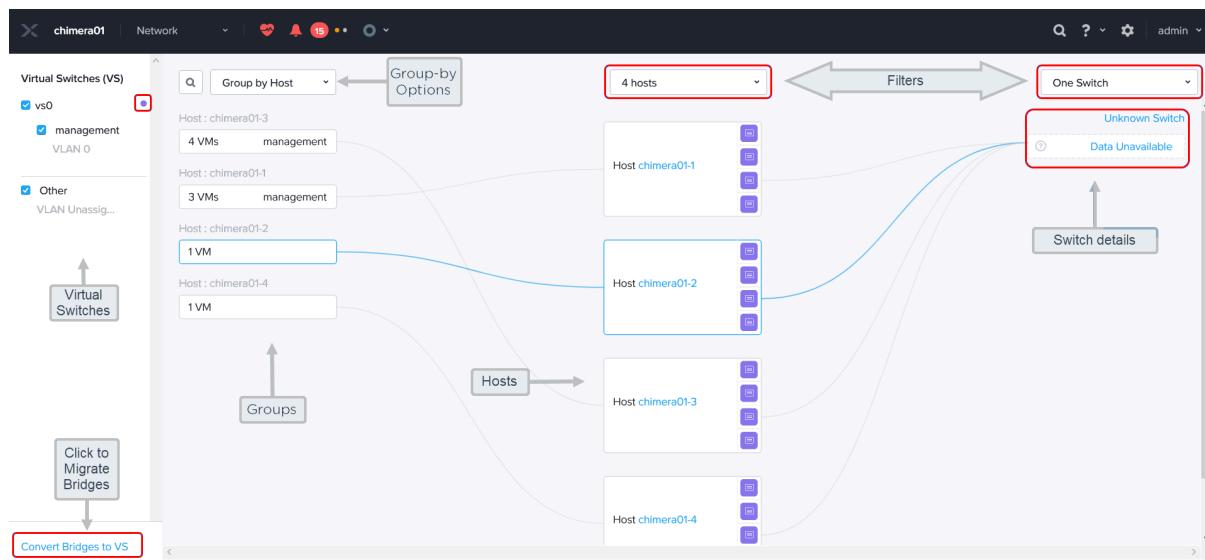
- (Optional) Configure SNMP v3 or SNMP v2c on the first-hop switches if you want the network visualizer to display the switch and switch interface statistics. The visualizer uses SNMP for discovery and to obtain real-time usage statistics from the switches. For information about configuring SNMP, see the switch manufacturer's documentation.

**Note:** This is not a mandatory requirement to use the network visualizer. This is a prerequisite only if you want the network visualizer to display the switch and switch interface statistics.

**Note:** Network visualization depends on a functional internal DNS system to map switch hostnames and IP addresses based on the LLDP responses. Incorrect or partial DNS configuration displays inaccurate network details in the UI. To troubleshoot the network visualization issues, see [KB-4085](#).

## Network Visualizer

The network visualizer displays interactive visual elements for the networked devices and for network components such as physical and logical interfaces. It also provides filtering and grouping capabilities that you can use to limit the display to a specific set of networked devices and connections.



**Figure 33: Network Visualizer**

The network visualizer includes the virtual networks pane and the topology view.

### Virtual Switches Pane

Lists the virtual switches configured on the Nutanix cluster. Selecting the checkbox associated with switch includes the VMs on that switch in the topology view. Conversely, clearing a checkbox excludes the VMs on that switch from the topology view. You can view up to five virtual switches at a time.

The **Other** checkbox corresponds to VMs that are not on any virtual switch. At a minimum, this checkbox is associated with the Controller VMs in the cluster.

### Topology View

Displays the network topology. The topology view shows the following entities:

### Virtual Switch (VS)

The visualizer displays the virtual switches configured on the cluster, with each virtual switch in a different color. It shows the switches associated with a VM or VM group and highlights which VSs are configured on a first-hop switch.

### VMs

The visualizer displays the VMs on the virtual switches that are selected in the virtual networks pane. Filter and group-by options allow you to customize the topology view.

### Hosts

The visualizer displays the hosts in the Nutanix cluster. The filter above the hosts allows you to specify the hosts to display in the topology view.

### Switches

The visualizer displays the first-hop switches and the virtual switches configured on each of them. The filter above the switches allows you to specify the switches to display in the topology view.

## Viewing the Network Visualizer

View the network visualizer for a Nutanix cluster.

### About this task

To view the network visualizer, follow these steps:

### Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu, click **Network**.

The system displays interactive visual elements for the networked devices and for network components such as physical and logical interfaces.

## Customizing the Topology View

Group VMs by a VM property or use a search filter to specify which network devices you want to show or exclude.

### About this task

To customize the topology view, follow these steps:

### Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu, click **Network**.  
The system displays interactive visuals for networked devices and components, including physical and logical interfaces.
3. Specify the virtual switches you want to show in the topology view:
  - In the **Virtual Switch** (VS) pane, select the checkboxes associated with the virtual switches and networks in each virtual switch to display in the topology view and clear those to exclude.
  - Select or clear the **Other** checkbox to include or exclude, respectively, the VMs not on any VLANs.

4. Specify the VMs you want to display in the topology view:
  - Select the group-by option from the menu at the top of the VMs. The following group-by options are available:
    - **Power State:** Groups VMs by states such as On and Off. By default, the VMs are grouped by power state.
    - **Host:** Groups VMs by the host on which they are running.
    - **VM Type:** Groups VMs into guest VMs and Controller VMs.
  - Enter a string in the search filter field to filter VMs that match the search string.
  - If the group-by and filter operations result in a VM group, click the VM group to show the VMs in the group. When you click a VM group, the visualizer displays ten VMs at first. To load ten more VMs, click **Load More VMs**.
- To group the VMs again or to clear the filter, click **Back** beside the group-by menu.
5. Specify the Nutanix hosts you want to display in the topology view:
  - a. Click the menu above the Nutanix hosts.
  - b. Select or clear the checkbox associated with the hosts to show or exclude, respectively.
6. Specify the switches to display in the topology view:
  - a. Click the menu above the switches.
  - b. Select or clear the checkbox associated with the switches to show or exclude, respectively.

## Viewing VM NIC Information

View the settings and real-time statistics of a virtual NIC in a VM from the visualizer.

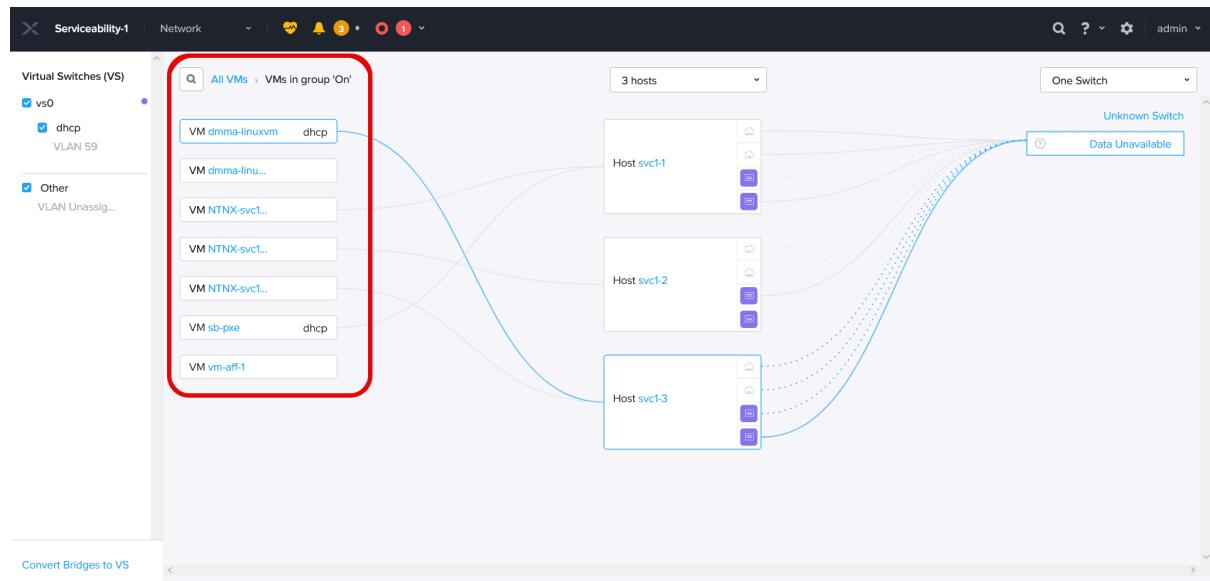
### About this task

To view the VM information, follow these steps:

### Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu, click **Network**.  
The system displays interactive visuals for networked devices and components, including physical and logical interfaces.

3. Use the group-by and filtering options in the visualizer to view the list of VMs in the cluster.



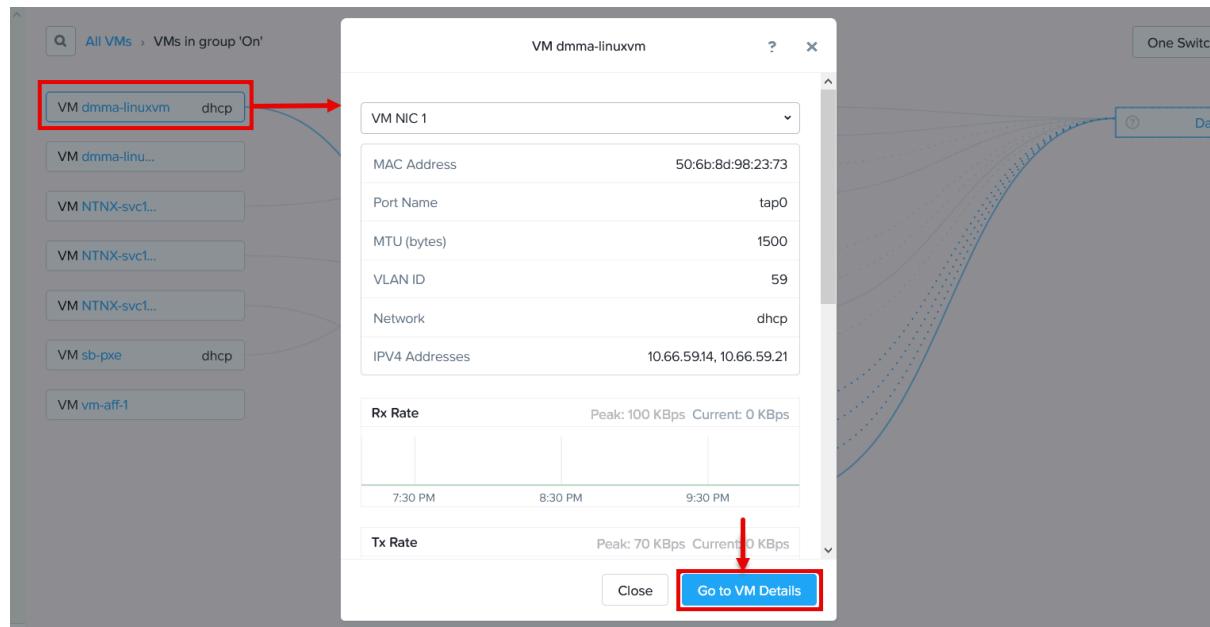
**Figure 34: VM Network**

4. To view the NIC information of a VM, click the name of the VM.

For information on how to group VMs or use a search filter, see [Customizing the Topology View](#) on page 176.

The system displays the network information dialog box of the VM.

5. From the VM NIC list at the top of the dialog box, select the NIC to show its settings and statistics.



**Figure 35: VM Details**

For information about the statistics that are displayed for the VM NICs, see [VM NICs Tab](#) on page 267.

6. To view additional information about the VM, click **Go to VM Details**.

The system displays the **VM** table view on the **VM** page.

**Tip:** You can return to the visualizer by pressing the back button in your browser.

## Viewing Host Information

View the internal network diagram of a Nutanix host and the settings and statistics of a network component.

### About this task

To view host information, follow these steps:

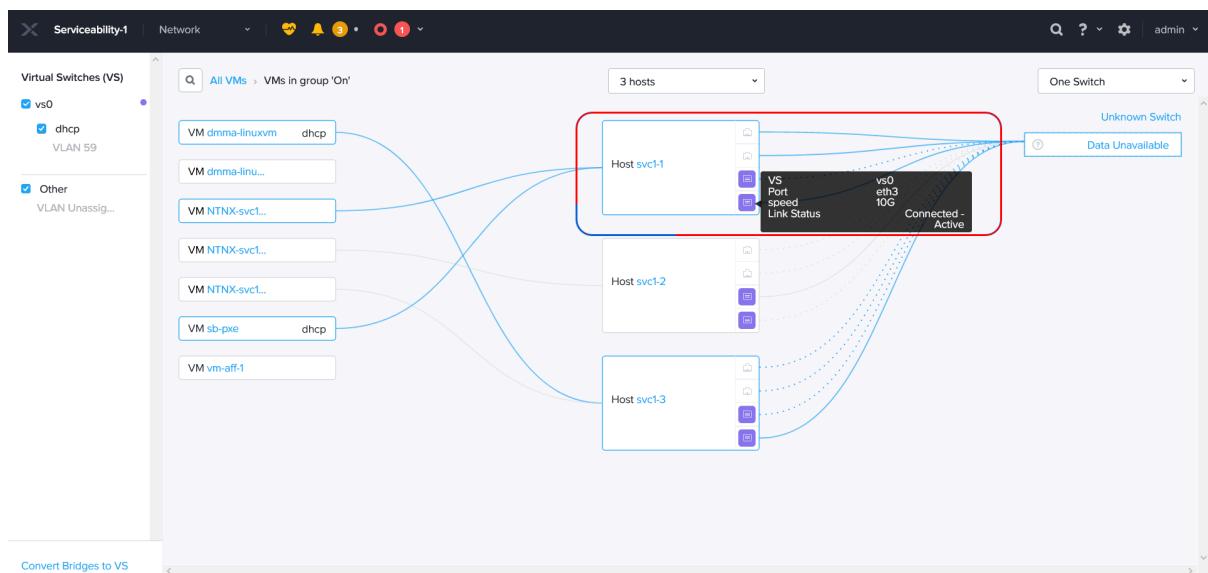
### Procedure

1. Log in to the Prism Element web console.

2. From the dropdown menu, click **Network**.

The system displays interactive visuals for networked devices and components, including physical and logical interfaces.

3. Hover over a host to view the host settings.



**Figure 36: Host Interface Information**

The network visualizer highlights lines to show VMs and virtual switches related to a selected host. A solid line from a bond to a host interface indicates an active uplink connection, while a dotted line represents a connected but unconfigured passive bond interface or an uplink on a virtual switch with the bond type set to **No Uplink Bond**.

4. To view the details of a host, click the name of the host.

The system opens a dialog box displaying the internal network diagram and the details of the host.

5. Click a network component in the diagram to view the network settings and statistics of the component in the right pane.

- » Click the Controller VM, and then, in the right pane, select a virtual NIC from the list to view settings and statistics of that virtual interface. Optionally, point to a location on a graph to view the value at that point in time.

For information about the statistics that are displayed for the virtual NICs, see [VM NICs Tab](#) on page 267.

- » Click a virtual switch to view the configuration details of the virtual switch.
- » Click a bridge to view the configuration details of the bridge.

A solid rectangle indicates an external bridge. A dotted rectangle indicates an internal bridge.

- » Click a bond to view the settings of the bond.

6. To additional information about the host, click **Go to Host Details**.

The system displays the **Host** table view on the **Hardware** page.

**Tip:** You can return to the visualizer by pressing the back button in your browser.

## View Switch Information

You can view both switch and switch port details from the network visualizer page.

### Viewing Switch Details

View the details of a switch such as switch name, vendor name, and management IP address.

#### About this task

To view the details of a switch, follow these steps:

#### Procedure

1. Log in to the Prism Element web console.

2. From the dropdown menu, click **Network**.

The system displays interactive visuals for networked devices and components, including physical and logical interfaces.

3. To view the details of a switch, click the name of the switch.

The system displays the switch information window that contains details about the switch.

4. For information about the details that are displayed for a switch, see [Hardware Table View](#) on page 191.

The system displays the **Switch** view on the **Hardware** page.

**Note:** When you open the network visualizer to view switch details, the Prism Element web console might take up to 30 seconds to load switch port statistics, causing a similar delay in the **Switch Details** table view.

**Tip:** You can return to the visualizer by pressing the back button in your browser.

### Viewing Switch Port Details

View switch port statistics and details, such as switch port name, physical address, and switch port type.

#### About this task

To view the details of a switch port, follow these steps:

## Procedure

1. Log in to the Prism Element web console.

2. From the dropdown menu, click **Network**.

The system displays interactive visuals for networked devices and components, including physical and logical interfaces.

3. To view the details of a switch port, click the name of the switch port.

The system displays the switch port information dialog box.

For information about the details that are displayed for a switch port, see [Switch Tab](#) on page 195.

# HARDWARE MANAGEMENT

---

A Nutanix block is a 1U or 2U chassis that contains one to four independent nodes, each optimized for high-performance compute, memory, and storage. Each node includes CPUs, DIMMs, SSD and HDD storage, fans, network connectors (multiple 10 and 1GbE ports), and other typical hardware components. Each block includes dual power supplies. For information about the number of nodes supported by a Nutanix cluster, see [Nutanix Configuration Maximums](#).

- You can monitor hardware configurations and status across the cluster through the Prism Element web console. For more information, see [Hardware Dashboard](#) on page 182.
- You can expand the cluster through the Prism Element web console. For more information, see [Expanding a Cluster](#) on page 198.

## Hardware Dashboard

The Hardware dashboard displays dynamically updated information about the hardware configuration in a cluster.

### Menu Options

In addition to the main menu, the Hardware screen includes a menu bar with the following options:

- **View selector:** The Hardware dashboard provides three viewing modes.
  - Click the **Overview** option on the left to display hardware information in a summary view. For more information, see [Hardware Overview View](#) on page 182.
  - Click the **Diagram** option to display a diagram of the cluster nodes from which you get detailed hardware information by clicking on a component of interest. For more information, see [Hardware Diagram View](#) on page 183.
  - Click the **Table** option to display hardware information in a tabular form. The Table screen is further divided into host, disk, and switch views; click the **Host** tab to view host information, the **Disk** tab to view disk information, or the **Switch** tab to view switch information. For more information, see [Hardware Table View](#) on page 191.
- **Add NVMe Devices:** Click this option to attach an NVMe drive to the cluster.

**Note:** This option appears only if your hardware supports NVMe software serviceability. For more information, see [Completing NVMe Drive Replacement \(Software Serviceability\)](#) in *Hardware Replacement Documentation*.

- **Expand Cluster:** Click this option to add nodes to the cluster. For more information on how to expand a cluster, see [Expanding a Cluster](#) on page 198.
- **Repair Host Boot Device:** Click this option to repair the boot drive of your hosts. For more information on how to repair the boot drives, see [Repair Boot Disks](#) on page 222.

## Hardware Overview View

The Overview page displays hardware-specific performance statistics, usage statistics, alerts and event messages.

**Note:** For information on how the statistics are derived, see [Understanding Displayed Statistics](#) on page 69.

**Table 39: Hardware Overview View Fields**

The following table describes the widgets that appear on the Overview page.

Name	Description
Hardware Summary	Displays the number of hosts and blocks in the cluster, along with the model number of the Nutanix hardware platform.
Hosts	Displays the number of hosts in the cluster categorized by discovered and monitored states, along with the number of discovered nodes that have not yet been added to the cluster.
Disks	Displays the total number of disks in the cluster categorized by tier type (SSD-PCIe, SSD-SATA, DAS-SATA, HDD).
CPU	Displays the total amount of CPU capacity (in GHz) of the cluster.
Memory	Displays the total amount of memory (in GBs) of the cluster.
Top Hosts by Disk IOPS	Displays I/O operations per host for the 10 most active hosts.
Top Hosts by Disk IO Bandwidth	Displays the I/O bandwidth used per host for the 10 most active hosts. The value is displayed in an appropriate metric (such as MBps, KBps, and so on) depending on the traffic volume.
Top Hosts by Memory Usage	Displays the percentage of memory capacity used per host for the 10 most active hosts.
Top Hosts by CPU Usage	Displays the percentage of CPU capacity used per host for the 10 most active hosts.
Hardware Critical Alerts	Displays the five most recent unresolved hardware-specific critical alert messages. Click a message to open the Alert screen for the message, or click view all alerts at the bottom to open the full Alert screen. For more information, see <a href="#">Alerts Dashboard</a> in <i>Prism Element Alerts and Events Reference Guide</i> .
Hardware Warning Alerts	Displays the five most recent unresolved hardware-specific warning alert messages. Click a message to open the Alert screen at that message. You can also open the Alert screen by clicking the <b>view all alerts</b> button at the bottom of the list.
Hardware Events	Displays the ten most recent hardware-specific event messages. Click a message to open the Event screen for the message, or click view all events at the bottom to open the full Event screen.

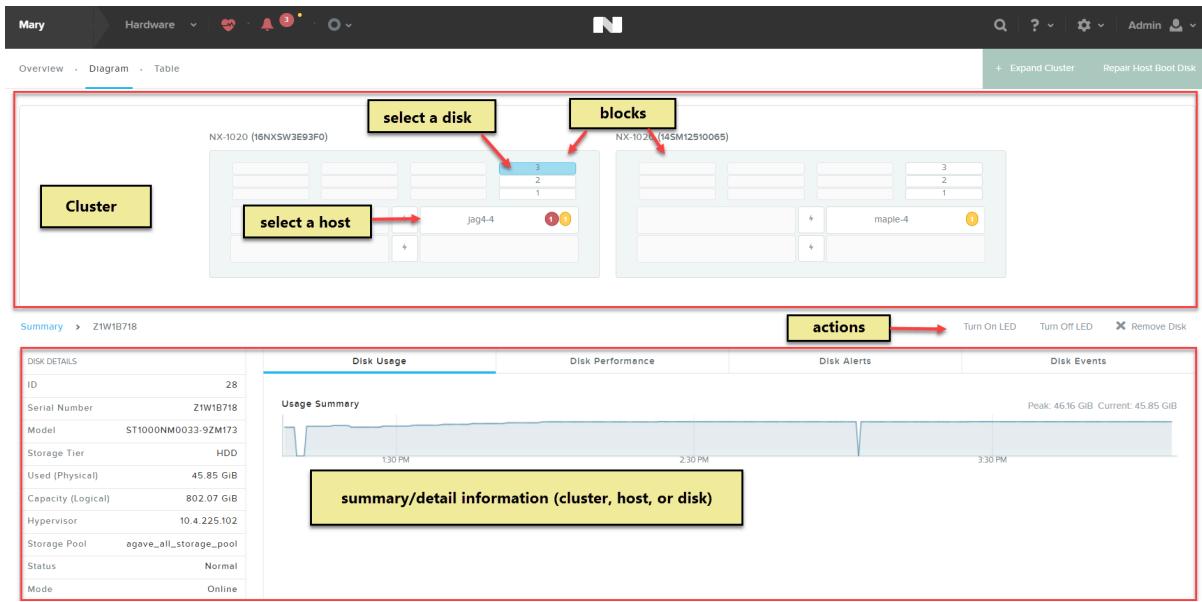
## Hardware Diagram View

The Hardware Diagram view displays information about hosts and disks.

The Hardware Diagram view screen is divided into two sections:

- The top section is an interactive diagram of the cluster blocks. Clicking on a disk or host (node) in the cluster diagram displays information about that disk or host in the summary section.
- The bottom **Summary** section provides additional information. It includes a details column on the left and a set of tabs on the right. The details column and tab content varies depending on what has been selected.

**Note:** For information about how the statistics are derived, see [Understanding Displayed Statistics](#) on page 69.



**Figure 37: Hardware Diagram View**

## Host Details

Selecting a host in the diagram displays information about that host in the lower section of the screen.

- When a host is selected, **Summary: host\_name** appears below the diagram, and action links appear to the right of this line:
  - Click the **Turn On LED** link to light up the host LED light on the chassis.
  - Click the **Turn Off LED** link to turn off the host LED light on the chassis.
  - Click the **Enter Maintenance Mode** link to place the host in maintenance mode
  - Click the **Repair Boot Disk Drive** link to repair the boot drive of the host.
  - Five tabs appear that display information about the selected host: **Host Performance**, **Host Usage**, **Host NICs**, **Host Alerts**, and **Host Events**.



**Figure 38: Hardware Diagram View: Hosts**

**Table 40: Host Detail Fields**

Parameter	Description	Values
Host Name	Displays the name of the host.	(host name)
Host Type	Displays the type of the host I Hyperconverged.	Storage-only
Hypervisor IP	Displays the IP address assigned to the hypervisor running on the host.	(IP address)
Controller VM IP	Displays the IP address assigned to the Controller VM.	(IP address)
IPMI IP	Displays the IP address of the Intelligent Platform Management Interface (IPMI) port. An IPMI port is used for the hypervisor host console. This field does not appear in Prism Central.	(IP address)
Node Serial	Displays the node serial number. The node serial is a unique number passed through from the manufacturer. (The form can vary because it is determined by each manufacturer.)	(manufacturer serial number)
Block Serial	Displays the block serial number.	(block serial number)
Block Model	Displays the block model number.	(model series number)
Storage Capacity	Displays the total storage capacity of the host.	xxx [GB TB]
Disks	Displays the number of disks in each storage tier in the host. Tier types vary depending on the Nutanix hardware platform model.	DAS-SATA: (number), SSD-SATA: (number), SSD-PCIe: (number), HDD: (number)
Memory	Displays the total memory capacity of the host.	xxx [MB GB]
CPU Capacity	Displays the total CPU capacity of the host.	xxx [GHz]
CPU Model	Displays the CPU model name	(CPU model name)
No. of CPU Cores	Displays the number of CPU cores on the host.	(number of CPU cores)
No. of Sockets	Displays the number of sockets.	(number of sockets)
No. of VMs	Displays the number of VMs running on the host.	(number)
Oplog Disk %	Displays the percentage of the operations log (oplog) capacity currently being used. The oplog resides on the metadata disk.	[0 - 100%]
Oplog Disk Size	Displays the current size of the operations log. (The oplog maintains a record of write requests in the cluster.) A portion of the metadata disk is reserved for the oplog, and you can change the size through nCLI.	xxx [GB]
Monitored	Displays whether the host is high availability (HA) protected. A <b>Yes</b> value indicates HA is active for the host. A <b>No</b> value indicates VMs on the host are not protected and will not restart if the host fails. Normally, this value must <b>Yes</b> ; a <b>No</b> value suggests an issue that must be investigated.	[Yes No]

Parameter	Description	Values
Hypervisor	Displays the name and version number of the hypervisor running on the host.	(name and version #)
Secure Boot Enabled	Displays whether secure boot is enabled in the host	Yes/No

## Disk Details

Selecting a disk in the diagram displays information about that disk in the lower section of the screen.

- When a disk is selected, **Summary: disk\_name** appears below the diagram, and action links appear to the right of this line:
  - Click the **Turn On LED** link to light up the LED light on the disk.
  - Click the **Turn Off LED** link to turn off the LED light on the disk.
  - Click the **Remove Disk** link to remove the disk from the cluster.
- Four tabs appear that display information about the selected storage container (see following sections for details about each tab): **Disk Usage**, **Disk Performance**, **Disk Alerts**, **Disk Events**.



**Figure 39: Storage Diagram View: Disks**

**Table 41: Disk Detail Fields**

Parameter	Description	Values
ID	Displays the disk identification number.	(ID number)
Serial Number	Displays the disk serial number.	(serial number)
Model	Displays the disk model number.	(model number)
Storage Tier	Displays the disk type (tier name). Nutanix models can contain disk tiers for PCIe solid state disks (SSD-PCIe), SATA solid state disks (SSD-SATA), and direct attach SATA hard disk drives (DAS-SATA) depending on the model type.	[SSD-PCIe   SSD-SATA   DAS-SATA]
Used (Physical)	Displays the used space on the drive.	xxx [GB TB]
Capacity (Physical)	Displays the total physical space on the drive.	xxx [GB TB]
Hypervisor	Displays the IP address of the hypervisor controlling the disk.	(IP address)

Parameter	Description	Values
Storage Pool	Displays the name of the storage pool that hosts the disk.	(name)
Status	Displays the operating status of the disk. Possible states include the following: <ul style="list-style-type: none"> <li>• <b>Normal:</b> Disk is operating normally.</li> <li>• <b>Data migration initiated:</b> Data is being migrated to other disks.</li> <li>• <b>Marked for removal, data migration is in progress:</b> Data is being migrated in preparation to remove disk.</li> <li>• <b>Detachable:</b> Disk is not being used and can be removed.</li> </ul>	Normal; Data migration initiated; Marked for removal, data migration is in progress; Detachable
Mode	Displays whether the disk is currently online or offline.	[online offline]
Self Encryption Drive	Displays whether the drive is a self encrypting drive (SED).	[present not present]
Password Protection Mode [SED only]	Displays whether data-at-rest encryption is enabled for the cluster. When it is enabled, a key is required to access (read or write) the data on the drive. This field appears only if the drive is a SED.	[protected not protected]

### Cluster Summary Information

When a host or disk is not selected in the diagram (or when the word **Summary** is clicked), cluster-wide summary information appears in the lower part of the screen.

- The **Hardware Summary** column (on the left) includes the following fields:
  - **Blocks:** Displays the number of blocks in the cluster.
  - **Hosts:** Displays the number of hosts in the cluster.
  - **Total Memory:** Displays the total memory capacity (GBs) of the cluster.
  - **Total CPU Capacity:** Displays the total CPU capacity (GHz) of the cluster.
  - **Disks:** Displays the number of disks in each storage tier (DAS-SATA, SSD-SATA, and SSD-PCIe) in the cluster. Tier types vary depending on the Nutanix model.
  - **Network Switches:** Displays the number of network switches being used in the cluster.
  - **GPUs:** (AHV only) Comma-separated list of GPUs installed on the host. GPU information includes the model name and a count in parentheses if multiple GPUs of the same type are installed on the host. If the firmware on the GPU is in compute mode, the string *compute* is appended to the model name. No string is appended if the GPU is in graphics mode.

The field is hidden if no GPUs are configured or if the hypervisor is not AHV.

- Three tabs appear that display cluster-wide information (see following sections for details about each tab): **Performance Summary**, **Hardware Alerts**, **Hardware Events**.

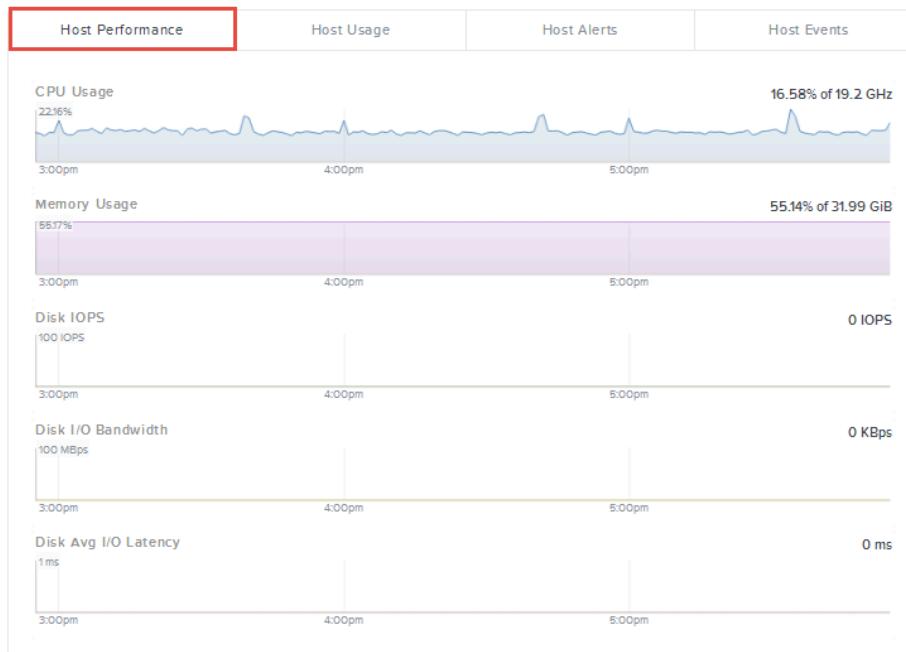
## Performance Tabs

The Performance tabs displays graphs of performance metrics. The tab label and number of graphs varies depending on what is selected in the diagram:

- **Performance Summary** (no host or disk selected): Displays resource performance statistics (CPU, memory, and disk) across the cluster.
- **Host Performance** (host selected): Displays resource performance statistics (CPU, memory, and disk) for the selected host.
- **Disk Performance** (disk selected): Displays disk performance statistics for the selected disk.

The graphs are rolling time interval performance monitors that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add a monitor to the analysis page by clicking the **Add chart to analysis** link in the upper right of the graph. For more information, see [Analysis Dashboard](#) on page 330. The Performance tab includes the following graphs:

- **[Cluster-wide] CPU Usage:** Displays the percentage of CPU capacity currently being used (0 - 100%) either across the cluster or for the selected host. (This graph does not appear when a disk is selected.)
- **[Cluster-wide] Memory Usage:** Displays the percentage of memory capacity currently being used (0 - 100%) either across the cluster or for the selected host. (This graph does not appear when a disk is selected.)
- **[Cluster-wide] IOPS:** Displays I/O operations per second (IOPS) for the cluster, selected host, or selected disk.
- **[Cluster-wide] I/O Bandwidth:** Displays I/O bandwidth used per second (MBps or KBps) for physical disk requests in the cluster, selected host, or selected disk.
- **[Cluster-wide] I/O Latency:** Displays the average I/O latency (in milliseconds) for physical disk requests in the cluster, selected host, or selected disk.



**Figure 40: Performance Tab**

## Usage Tabs

The Usage tabs display graphs of storage usage. This tab appears only when a host or disk is selected.

- **Host Usage:** Displays usage statistics for the selected host.
- **Disk Usage:** Displays usage statistics for the selected disk.

The Usage tab displays one or both of the following graphs:

- **Usage Summary:** Displays a rolling time interval usage monitor that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add the monitor to the analysis page by clicking the **Add chart to analysis** in the upper right of the graph. For more information, see [Analysis Dashboard](#) on page 330.
- **Tier-wise Usage** (host only): Displays a pie chart divided into the percentage of storage space used by each disk tier on the host. Disk tiers can include DAS-SATA, SSD-SATA, and SSD-PCIe depending on the Nutanix model type.

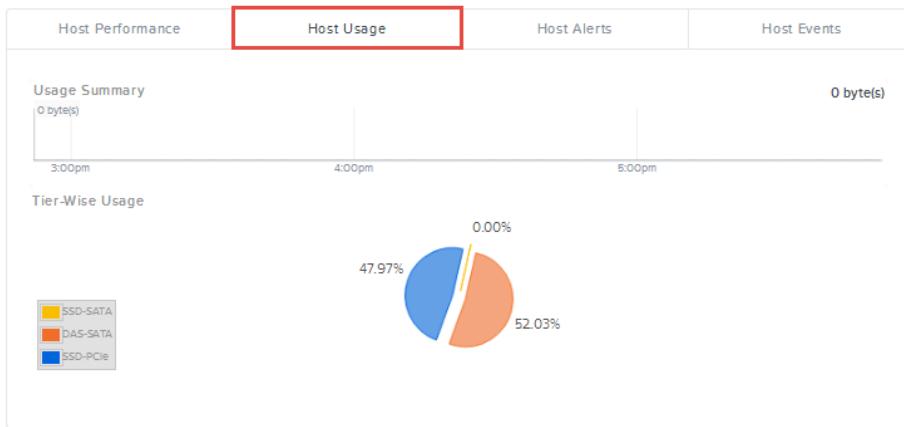


Figure 41: Usage Tab

## Alerts Tab

The Alerts tab displays the unresolved alert messages about hosts, disks, and other hardware in the same form as the Alerts page. The tab label and alerts depends on what is selected in the diagram. For more information, see [Alerts Summary View](#). Click the **Unresolved X** button in the filter field to also display resolved alerts.

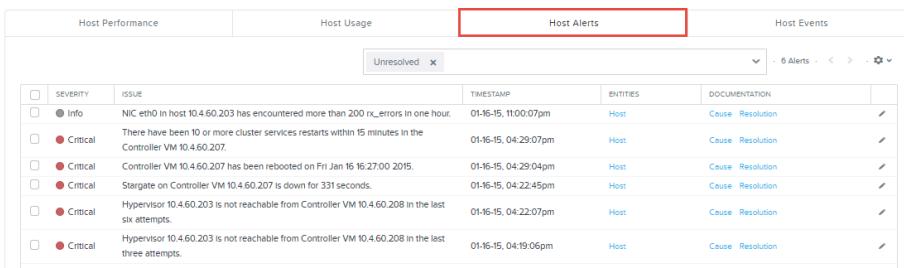


Figure 42: Alerts Tab

## Events Tab

The Events tab displays the unacknowledged event messages about hosts, disks, and other hardware in the same form as the Events page. The tab label and alerts depends on what is selected in the diagram. For more information, see [Events Summary View](#). Click the **Include Acknowledged** button to also display acknowledged events.

MESSAGE	ENTITIES	MODIFIED BY	TIMESTAMP

**Figure 43: Events Tab**

## Host NICs Tab

The Host NICs tab displays information in tabular form about the host NICs used to support traffic through the virtual NICs. (This tab appears only when a host is selected and the hypervisor is ESXi.) Each line represent a host NIC, and the following information is displayed for each NIC:

- **Host NIC:** Displays the host NIC name.
- **Speed (in KBps):** Displays the host NIC transmission speed.
- **MAC Address:** Displays the host NIC MAC address.
- **Rx Packets:** Displays the number of packets received by the host NIC.
- **Tx Packets:** Displays the number of packets transmitted by the host NIC.
- **Dropped Rx Packets:** Displays the number of received packets dropped by the host NIC.
- **Dropped Tx Packets:** Displays the number of transmitted packets dropped by the host NIC.
- **Rx Error Packets:** Displays the number of error packets that were received.
- **Tx Error Packets:** Displays the number of error packets that were transmitted.

When you click a host NIC entry, a set of usage graphs about that NIC appear below the table:

- **Rx Rate:** Displays a monitor of the total packets received over time. Place the cursor anywhere on the line to see the rate for that point in time. (This applies to all the monitors in this tab.)
- **Tx Rate:** Displays a monitor of the total packets that were transmitted.
- **Dropped Rx Packets:** Displays a monitor of received packets that were dropped.
- **Dropped Tx Packets:** Displays a monitor of transmitted packets that were dropped.
- **Error Rx Packets:** Displays a monitor of error packets that were received.



**Figure 44: Host NICs Tab**

## Hardware Table View

The Hardware Table view displays information about hosts, disks, and switches in a tabular form. Click the **Host** tab in the screen menu bar to display host information; click the **Disk** tab to display disk information; click the **Switch** tab to display switch information.

The Hardware table view is divided into two sections:

- The top section displays attributes that provides basic information the entity that you select.
- The bottom **Summary** section provides additional information about the selected entity. It includes a details column on the left and a set of tabs on the right. The details column and tab content varies depending on the entity that you select.

**Note:** For information about how the statistics are derived, see [Understanding Displayed Statistics](#) on page 69.

### Host Tab

Clicking the **Host** tab displays information about the hosts in the cluster.

- The table at the top of the screen displays information about all the hosts, and the details column (lower left) displays additional information when a host is selected in the table. The following table describes the fields in the host table and detail column.
- When a host is selected, **Summary: host\_name** appears below the table, and action links appear on the right of this line:
  - Click the **Turn On LED** link to light up the host LED light on the chassis.
  - Click the **Turn Off LED** link to turn off the host LED light on the chassis.
  - Click the **Enter Maintenance Mode** link to put the host in maintenance mode.
  - Click the **Repair Host Boot Device** link to repair the boot drive of the selected host.
- Five tabs appear that display information about the selected host: **Host Performance**, **Host Usage**, **Host NICs**, **Host Alerts**, and **Host Events**.

**Table 42: Host Table and Detail Fields**

Parameter	Description	Values
<i>Host Table Fields</i> (upper screen)		
Host Name	Displays the name of the host that hosts the disk.	(host name)
Host IP	Displays the IP address assigned to the hypervisor running on the host.	(IP address)
CVM IP	Displays the IP address assigned to the Controller VM.	(IP address)
Hypervisor	Displays the hypervisor type.	[ESXi AHV Hyper-V]
CPU Usage	Displays the percentage of CPU capacity currently being used.	0 - 100%
CPU Capacity	Displays the CPU capacity of the host.	xxx [GHz]
Memory Usage	Displays the percentage of memory capacity currently being used by the host.	0 - 100%
Memory Capacity	Displays the memory capacity of the host.	xxx [MiB GiB]
Total Disk Usage	Displays the storage space used and total disk capacity of the host.	xxx [MiB GiB TiB] of xxx [MiB GiB TiB]
Disk Usage	Displays the disk usage in percentage.	xx %
Disk IOPS	Displays I/O operations per second (IOPS) for the host.	[0 - unlimited]
Disk IO B/W	Displays I/O bandwidth used per second for the host.	xxx [MBps KBps]
Disk IO Latency	Displays the average I/O latency (in milliseconds) for the host.	xxx [ms]
<i>Host Detail Fields</i> (lower screen)		
Host Name	Displays the name of the host.	(host name)
Hypervisor IP	Displays the IP address assigned to the hypervisor running on the host.	(IP address)
Controller VM IP	Displays the IP address assigned to the Controller VM.	(IP address)
IPMI IP	Displays the IP address of the Intelligent Platform Management Interface (IPMI) port. An IPMI port is used for the hypervisor host console. This field does not appear in <i>Prism Central</i> .	(IP address)
Node Serial	Displays the node serial number. The node serial is a unique number passed through from the manufacturer. (The form can vary because it is determined by each manufacturer.)	(manufacturer serial number)
Block Serial	Displays the block serial number.	(block serial number)
Block Model	Displays the block model number.	(model series number)
Storage Capacity	Displays the total amount of storage capacity on the host.	xxx [GB TB]

Parameter	Description	Values
Disks	Displays the number of disks in each storage tier in the host. Tier types vary depending on the Nutanix model type.	DAS-SATA: (number), SSD-SATA: (number), SSD-PCIe: (number)
Memory	Displays the total memory capacity for the host.	xxx [MB GB]
CPU Capacity	Displays the total CPU capacity for the host.	xxx [GHz]
CPU Model	Displays the CPU model name	(CPU model name)
No. of CPU Cores	Displays the number of CPU cores on the host.	(number of CPU cores)
No. of Sockets	Displays the number of sockets.	(number of sockets)
No. of VMs	Displays the number of VMs running on the host.	(number)
Oplog Disk %	Displays the percentage of the operations log (oplog) capacity currently being used. The oplog resides on every SSD.	[0 - 100%]
Oplog Disk Size	Displays the current size of the operations log. (The oplog maintains a record of write requests in the cluster.) A portion of every SSD is reserved for the oplog.	xxx [GB]
Monitored	Displays whether the host is high availability (HA) protected. A <b>Yes</b> value means HA is active for the host. A <b>No</b> value means VMs on the host are not protected (will not be restarted on another host) if the host fails. Normally, this value should always be <b>Yes</b> . A <b>No</b> value is likely a sign of a problem situation that should be investigated.	[Yes No]
Hypervisor	Displays the name and version number of the hypervisor running on the host.	(name and version #)
Datastores	Displays the names of any datastores.	(name)
Secure Boot Enabled	Displays whether the host is secure boot enabled.	[Yes No]

## Disk Tab

Clicking the **Disk** tab displays information about disks in the cluster.

- The table at the top of the screen displays information about all the disks, and the details column (lower left) displays additional information when a disk is selected in the table. The following table describes the fields in the disk table and detail column.
- When a disk is selected, **Summary: disk\_name** appears below the table, and action links appear on the right of this line:
  - Click the **Turn On LED** link to light up the LED light on the disk.
  - Click the **Turn Off LED** link to turn off the LED light on the disk.
  - Click the **Remove Disk** link to remove this disk from the cluster.
- Four tabs appear that display information about the selected storage container (see following sections for details about each tab): **Disk Usage**, **Disk Performance**, **Disk Alerts**, **Disk Events**.

**Table 43: Disk Table and Detail Fields**

Parameter	Description	Values
<i>Disk Table Fields</i> (upper screen)		
Disk ID	Displays the disk identification number.	(ID number)
Serial Number	Displays the disk serial number.	(serial number)
Host Name	Displays the host name.	(host name)
Hypervisor IP	Displays the IP address assigned to the hypervisor running on the host.	(IP address)
Tier	Displays the disk type (tier name). Nutanix models can contain disk tiers for PCIe solid state disks (SSD-PCIe), SATA solid state disks (SSD-SATA), and direct attach SATA hard disk drives (DAS-SATA) depending on the model type.	[SSD-PCIe   SSD-SATA   DAS-SATA]
Status	Displays the operating state of the disk.	online, offline
Disk Usage	Displays the percentage of disk space used and total capacity of this disk.	[0 - 100%] of xxx [GB TB]
Disk IOPS	Displays I/O operations per second (IOPS) for this disk.	[0 - unlimited]
Disk IO B/W	Displays I/O bandwidth used per second for this disk.	xxx [MBps KBps]
Disk Avg IO Latency	Displays the average I/O latency for this disk.	xxx [ms]
<i>Disk Detail Fields</i> (lower screen)		
ID	Displays the disk identification number.	(ID number)
Serial Number	Displays the disk serial number.	(serial number)
Model	Displays the disk model number.	
Storage Tier	Displays the disk type (tier name). Nutanix models can contain disk tiers for PCIe solid state disks (SSD-PCIe), SATA solid state disks (SSD-SATA), and direct attach SATA hard disk drives (DAS-SATA) depending on the model type.	[SSD-PCIe   SSD-SATA   DAS-SATA]
Used (Physical)	Displays the amount of used space on the drive.	xxx [GB TB]
Capacity (Logical)	Displays the total physical space on the drive.	xxx [GB TB]
Hypervisor	Displays the IP address of the hypervisor controlling the disk.	(IP address)
Storage Pool	Displays the name of the storage pool in which the disk resides.	(name)

Parameter	Description	Values
Status	<p>Displays the operating status of the disk. Possible states include the following:</p> <ul style="list-style-type: none"> <li>• <b>Normal.</b> Disk is operating normally.</li> <li>• <b>Data migration initiated.</b> Data is being migrated to other disks.</li> <li>• <b>Marked for removal, data migration is in progress.</b> Data is being migrated in preparation to remove disk.</li> <li>• <b>Detachable.</b> Disk is not being used and can be removed.</li> </ul>	Normal; Data migration initiated; Marked for removal, data migration is in progress; Detachable
Mode	Displays whether the disk is currently online or offline.	[online offline]
Self Encryption Drive	Displays whether this is a self encrypting drive (SED).	[present not present]
Password Protection Mode [SED only]	Displays whether data-at-rest encryption is enabled for the cluster. When it is enabled, a key is required to access (read or write) data on the drive. This field appears only when the drive is a SED.	[protected not protected]

## Switch Tab

Clicking the **Switch** tab displays information about the physical switches used by the host NICs to support traffic through the virtual NICs. The table at the top of the screen displays information about the switches, and the lower portion of the screen displays additional information when a switch is selected in the table. You can configure any number of switches, but only the switches that are actually being used for virtual NIC traffic appear in this table. For more information on how to configure a switch, see [Configuring a Network Switch](#) on page 167. The following table describes the fields in the switch table, in the detail column (lower left), and in the Physical Switch Interfaces tab (lower right).

**Table 44: Switch Table and Detail Fields**

Parameter	Description	Values
<i>Switch Table Fields (upper screen)</i>		
Switch ID	Displays the switch identification number.	(ID value)
Switch Name	Displays the switch name.	(name)
Management Addresses	Displays the switch management IP address(es).	(IP address)
Vendor Name	Displays the name of the switch vendor.	(company name)
Location Info	Displays the switch vendor location.	(company address)
Contact Info	Displays the switch vendor contact information.	(company contact)
Description	Describes the switch model and type.	(switch description)
<i>Switch Detail Fields (lower left screen)</i>		
Name	Displays the switch name.	(name)

Parameter	Description	Values
Vendor Name	Displays the name of the switch vendor.	(company name)
Management Addresses	Displays the IP address(es) for the switch management ports.	(IP address)
Services	Displays the number of services being used.	(number)
<i>Physical Switch Interfaces Fields (lower right screen)</i>		
Physical Switch Interface	Displays the interface name.	(name)
Switch ID	Displays the switch identification number.	(ID value)
Index	Displays the index value.	(number)
MTU (in bytes)	Displays the size in bytes of the largest protocol data unit (maximum transmission unit) that the layer can pass onwards.	(number)
MAC Address	Displays the interface MAC address	(mac address)
Unicast Rx Pkts	Displays the number of unicast packets received.	(number)
Unicast Tx Pkts	Displays the number of unicast packets transmitted.	(number)
Error Rx Pkts	Displays the number of received packets with an error.	(number)
Error Tx Pkts	Displays the number of transmitted packets with an error.	(number)
Discard Rx Pkts	Displays the number of received packets that were discarded.	(number)
Discard Tx Pkts	Displays the number of transmitted packets that were discarded.	(number)

## Cluster Summary Information

The Cluster Summary information displayed when no host or disk is selected is the same as in the Diagram View. For more information, see Cluster Summary Information in Hardware Diagram View. The Performance, Usage, NICs, Alerts, and Events tabs display the same information as in the Diagram View. For more information, see the respective sections in Hardware Diagram View.

- The **Hardware Summary** column (on the left) includes the following fields:
  - **Blocks.** Displays the number of blocks in the cluster.
  - **Hosts.** Displays the number of hosts in the cluster.
  - **Total Memory.** Displays the total memory capacity (GBs) in the cluster.
  - **Total CPU Capacity.** Displays the total CPU capacity (GHz) in the cluster.
  - **Disks.** Displays the number of disks in each storage tier (DAS-SATA, SSD-SATA, and SSD-PCIe) in the cluster. Tier types vary depending on the Nutanix model type.
  - **Network Switches.** Displays the number of network switches being used in the cluster.
  - **GPUs.** (AHV only) Comma-separated list of GPUs installed on the host. GPU information includes the model name and a count in parentheses if multiple GPUs of the same type are installed on the host. If the firmware on

the GPU is in compute mode, the string *compute* is appended to the model name. No string is appended if the GPU is in graphics mode.

The field is hidden if no GPUs are configured or if the hypervisor is not AHV.

- Three tabs appear that display cluster-wide information (see following sections for details about each tab): **Performance Summary, Hardware Alerts, Hardware Events.**

### Host Performance Tab

The Host Performance tab displays graphs of performance metrics. The tab label and number of graphs varies depending on what is selected in the table:

- Performance Summary** (no host or disk selected). Displays resource performance statistics (CPU, memory, and disk) across the cluster.
- Host Performance** (host selected). Displays resource performance statistics (CPU, memory, and disk) for the selected host.
- Disk Performance** (disk selected). Displays disk performance statistics for the selected disk.

The graphs are rolling time interval performance monitors that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add a monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see [Analysis Dashboard](#) on page 330. The Performance tab includes the following graphs:

- [Cluster-wide] CPU Usage:** Displays the percentage of CPU capacity currently being used (0 - 100%) either across the cluster or for the selected host. (This graph does not appear when a disk is selected.)
- [Cluster-wide] Memory Usage:** Displays the percentage of memory capacity currently being used (0 - 100%) either across the cluster or for the selected host. (This graph does not appear when a disk is selected.)
- [Cluster-wide] IOPS:** Displays I/O operations per second (IOPS) for the cluster, selected host, or selected disk.
- [Cluster-wide] I/O Bandwidth:** Displays I/O bandwidth used per second (MBps or KBps) for physical disk requests in the cluster, selected host, or selected disk.
- [Cluster-wide] I/O Latency:** Displays the average I/O latency (in milliseconds) for physical disk requests in the cluster, selected host, or selected disk.

### Host Usage Tab

The Host Usage tab displays graphs of storage usage. This tab appears only when a host or disk is selected. The tab label varies depending on what is selected in the table:

- Host Usage** (host selected). Displays usage statistics for the selected host.
- Disk Usage** (disk selected). Displays usage statistics for the selected disk.

The Usage tab displays one or both of the following graphs:

- Usage Summary:** Displays a rolling time interval usage monitor that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see [Analysis Dashboard](#) on page 330)
- Tier-wise Usage** (host only): Displays a pie chart divided into the percentage of storage space used by each disk tier on the host. Disk tiers can include DAS-SATA, SSD-SATA, and SSD-PCIe depending on the Nutanix model type.

## Host Alerts Tab

The Host Alerts tab displays the unresolved alert messages about hosts, disks, and other hardware in the same form as the Alerts page. For more information, see [Alerts Summary View](#). Click the **Unresolved X** button in the filter field to also display resolved alerts.

## Host Events Tab

The Host Events tab displays the unacknowledged event messages about hosts, disks, and other hardware in the same form as the Events page. For more information, see [Events Summary View](#). Click the **Include Acknowledged** button to also display acknowledged events.

## Host NICs Tab

The Host NICs tab displays information in tabular form about the host NICs used to support traffic through the virtual NICs. (This tab appears only when a host is selected.) Each line represents a host NIC, and the following information is displayed for each NIC:

- **Host NIC.** Displays the host NIC name.
- **Speed (in KBps).** Displays the host NIC transmission speed.
- **MAC Address.** Displays the host NIC MAC address.
- **Received Packets.** Displays the number of packets received by the host NIC.
- **Transmitted Packets.** Displays the number of packets transmitted by the host NIC.
- **Dropped Rx Packets.** Displays the number of received packets dropped by the host NIC.
- **Dropped Tx Packets.** Displays the number of transmitted packets dropped by the host NIC.
- **Rx Packet Errors.** Displays the number of error packets received by the host NIC.
- **Tx Packet Errors.** Displays the number of error packets transmitted by the host NIC.

When you click a host NIC entry, a set of usage graphs about that NIC appear below the table:

- **Total Packets Received.** Displays a monitor of the total packets received by the host NIC (in KBs or MBs) over time. Place the cursor anywhere on the line to see the value for that point in time. (This applies to all the monitors in this tab.)
- **Total Packets Transmitted.** Displays a monitor of the total packets transmitted by the host NIC (in KBs or MBs).
- **Dropped Packets Received.** Displays a monitor of received packets that were dropped.
- **Dropped Packets Transmitted.** Displays a monitor of transmitted packets that were dropped.
- **Error Packets Received.** Displays a monitor for error packets received.

## Expanding a Cluster

Add new nodes to a cluster after physically installing and connecting them to the network on the same subnet as the cluster.

### Before you begin

Ensure that the following prerequisites are met before you expand the cluster:

- Review the [Prerequisites and Requirements](#) on page 204 before you add a node to the cluster. The process varies based on the AOS, hypervisor, encryption, and hardware configuration in the cluster.

- Check the **Health Dashboard**. If any health checks are failing, resolve them before adding new nodes. As a final check, run NCC to ensure that the cluster is healthy.
- Wait for any ongoing expand cluster operations to complete.
- Check the **Hardware** dashboard to ensure all nodes are in the correct metadata state. If any nodes show Metadata store disabled on the node or Node is removed from metadata store, enable the metadata store by clicking **Enable Metadata Store**.
- Observe the SSDs requirements for Hybrid HCI Node and All-Flash HCI Node specified in [HCI Node Field Requirements](#) of the *Acropolis Advanced Administration Guide*.
- The cluster expansion process compares the AOS version on the existing and new nodes and performs any upgrades necessary for all the nodes to have the same AOS version.

## About this task

To add one or more nodes to an existing cluster (you can add multiple nodes at the same time), follow these steps:

**Note:** Steps 10, 11, and 12 address special cases (rack fault tolerance, data-at-rest encryption, and Hyper-V) and are not in sequential order. Refer to these steps as needed during the procedure based on your specific requirements.

## Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu, click **Hardware**.  
The system displays the **Hardware Overview** page.
3. Click **+ Expand Cluster**.  
The system displays the **Expand Cluster** dialog box.
4. Select one of the following:
  - » **Expand Cluster** to begin the expansion immediately (after you complete the remaining configuration steps).
  - » **Prepare Now and Expand Later** to prepare the nodes now but delay adding them to the cluster until a later time. Preparing the nodes includes imaging the hypervisor (if needed), upgrading the AOS version (if needed), and configuring network settings for the new node (if needed).
5. Click **Next**.  
The cluster scans the network for Nutanix nodes, and the system displays the Select Host tab that shows a list of discovered blocks and nodes. Discovered blocks have one or more unassigned, factory-prepared nodes (hypervisor and Controller VM installed) on the same subnet as the cluster. Discovery requires IPv6 multicast packets to pass through the physical switch. If a failure occurs, review the [Prerequisites and Requirements](#) on page 204.

6. Do one of the following:
  - » If the list includes all the nodes to add, go to the next step.
  - » If the list does not include all the nodes to add or if IPv6 is not supported for the cluster, go to the bottom of the list, click **Discover Hosts Manually**, and do the following to retry discovering the nodes:
    1. In the **Manual Host Discovery** section, click the **+Add Host**.
    2. Enter the IP address of the Controller VM on the host (or the host IP address for compute-only nodes) and then click **Save**.
    3. Add more hosts as needed.
    4. After adding all the hosts, click **Discover and Add Hosts**.

**Note:** To manually discover a host in an ESXi or Hyper-V cluster, the target node must have the same hypervisor type and version as the cluster. Additionally, the AOS version on the node must be the same as, or earlier than, the version used in the cluster.

7. Select the checkbox associated with a block to add the block to the cluster. All the nodes in a selected block are also selected automatically. Clear the checkbox associated with the nodes to not add to the cluster.

When you select a block, more fields appear below the block diagram. A separate line for each node (host) in the block appears under each field name.

8. Do the following in the indicated fields for each selected block:

- a. **Host Name** (if present): Enter the name of the host.

Enter the host name, not the fully qualified domain name. The host name is mandatory for Hyper-V clusters, but not for ESXi and AHV clusters.

- b. **Controller VM [IPv4|IPv6]**: Review the Controller VM IP address assigned to each host and do one of the following:

**Note:** For the Controller VM, hypervisor, and IPMI, both IPv6 and IPv4 address fields appear to support either protocol. When entering addresses, ensure you enter each IP address in the correct field for the relevant protocol. Typically, you can leave the IPv6 field unchanged and only update the IPv4 address if necessary.

- If the address is correct, leave this field unchanged.
- If the address is not correct, either change the incorrect address or enter a starting address on the top line (for multiple hosts). The address you enter is assigned to the Controller VM of the first host, and consecutive IP addresses (sequentially from the entered address) are assigned automatically to the remaining hosts.

- c. **Hypervisor [IPv4|IPv6]**: Repeat the previous step for this field.

This field sets the hypervisor IP addresses for all the hosts to be added.

- d. **IPMI IP [IPv4|IPv6]**: Repeat the previous step for this field.

This field sets the IPMI port IP addresses for all the hosts to be added. An IPMI port is used for the hypervisor host console.

- e. When you enter all the node values, click **Next**.

The system validates the network addresses before proceeding and highlights the problematic addresses in red.

9. In the **Choose Node Type** tab, select the node type (**HCI Node** or **Storage-only**) for each node from the dropdown list and then click the **Next** button.

If you select **HCI Node**, the system adds the node as a standard node in the cluster. If you select **Storage-only** the system adds the node as a storage-only node. Storage-only nodes have specific requirements. Review [Storage-Only Nodes](#) on page 230 before adding a storage-only node.

10. In the **Host Networking** tab, configure the uplinks for each management bridge or vSwitch to be created or updated for the nodes.

The **Host Networking** tab displays a list of the target nodes where you can specify the status (active or standby) for each node's uplinks to the management bridge or vSwitch. The uplink list depends on the hypervisor of the node to be added, while the listed bridge or vSwitch is for the base cluster. The standard form for AHV uplinks is ethx (eth0, eth1, eth2, and so on); the standard form for ESXi uplinks is vmnicx (vmnic0, vmnic1, and so on.) For example, if the hypervisor is ESXi on the node but AHV on a three-node base cluster, each entry displays the AHV vSwitch name (br0 or br1), ESXi uplink name (vmnic0, vmnic1, or vmnic2), and status (active or standby). For hypervisor-specific information, see [Prerequisites and Requirements](#) on page 204.

**Note:** To skip network configuration, click **Skip Networking**.

- a. Click **Add Uplink** for the first node.
- b. Select the uplink from the dropdown list.
- c. Select **Active** or **Standby** from the dropdown list.
- d. Select the check mark icon to save the changes.
- e. Repeat steps b through d to configure all the uplinks in the node.
- f. Repeat steps a through e for each node.
- g. After configuring all the nodes in the list, click **Next**.

11. In the **Configure Host** tab, specify the hypervisor image and allowlist for nodes that require imaging.

- » If the system detects that the hypervisor and AOS version are the same as the version used in the cluster, no imaging is required and a message confirming this appears. Proceed to the next step.
- » If a hypervisor image is listed in the **Hypervisor: <type>** field and it is the correct one, proceed to the next step. If you previously uploaded a compatible hypervisor image when adding the nodes, that image appears here. You can use that image or upload a different one.
- » If no hypervisor image is listed or if the listed one is not the correct image, click **Browse** (no listed file) or **Change File** (file listed already). In the search window, find the image file, and then click **Open** (in the search window) to upload the image file.

You must provide an ISO file to image ESXi or Hyper-V. To obtain the required AHV image, visit the **Downloads > AHV** page of the Nutanix Support Portal. For information on how to access the portal, see [Accessing the Nutanix Support Portal](#) on page 392. Starting with AOS 6.8 version, AOS does not include the AHV installation bundle. You can find the AHV bundle on the portal, named as: AHV-DVD-x86\_64-e1x.nutanix.AHV-version.iso.

- Replace `e1x` with Enterprise Linux version as el7 or el8.

- Replace *AHV-version* with actual AHV version.

For example, AHV-DVD-x86\_64-el8.nutanix.20230302.1011.iso or AHV-DVD-x86\_64-el7.nutanix.20220304.478.iso.

- » If a message appears that the hypervisor image is not compatible, either select (choose and upload) a hypervisor image that is compatible or update the hypervisor ISO allowlist.

The cluster includes a hypervisor ISO allowlist, which lists the approved hypervisor images. You can only use an image that is in the approved list. For more information about the allowlist, see [Hypervisor ISO Images](#) in the *Field Installation Guide*. If your hypervisor image does not appear in the allowlist (because you created the cluster before the image was approved), you can update the allowlist as follows:

1. Download the latest hypervisor ISO whitelist from the **Downloads > Foundation** page of the Nutanix Support portal.
2. Click **Update** in the **Hypervisor ISO Whitelist** field.
3. Click **Browse** (which opens a search window), find and select the allowlist file, and click **Open**.
4. Click **Upload**.

The incompatible message disappears and you can continue provided the hypervisor image is on the uploaded allowlist.

12. [Rack fault tolerance only] In the **Assign Rack** tab, select the block and the rack to map the block placement in that rack. To add a rack to the list, click **Create Rack**.

This tab appears only when rack fault tolerance is enabled. For more information, see [Configuring Rack Fault Tolerance](#) on page 35.

13. [Data-at-rest encryption only] In the **Encrypt Host** tab, do the following.

This tab appears only when data-at-rest encryption is enabled with an external KMS. For more information, see [Data-At-Rest Encryption](#). You can apply encryption licenses after adding new nodes to the cluster.

- a. In the **Certificate Signing Request Information** field, click **Generate and Download** for each node to be added.

Clicking this option generates a certificate signing request (CSR) named csr\_for\_discovered\_node for the node, which you can download to your system.

- b. Get the CSRs signed by a certificate authority (CA).
- c. Click **Select files** for each key management server and upload the signed certificates for the nodes to be added.
- d. Click **Next**.

14. [Hyper-V only] Specify the credentials to join the new nodes to Active Directory and to a failover cluster.

- a. Specify the name of the Hyper-V failover cluster in the **Failover Cluster Name** text box.
- b. Specify the user name and password of the domain account that has the privileges to create a new or modify an existing computer account in the Active Directory domain. The user name must be in the DOMAIN\USERNAME format.

15. After you enter all the details, click **Run Checks** to verify if the nodes are ready.

The system runs a set of precheck tests on the nodes. Progress messages appear in the **Expand Cluster** window. You can also monitor progress from the **Tasks** dashboard. For more information, see [View Task Status](#) on page 87.

16. If the checks pass are successful, do one of the following:

  - » Click **Expand Cluster** to begin the cluster expansion process. (This option appears if you select **Expand Cluster** in step 2.)
  - » Click **Prepare Node(s)** to begin preparing the nodes. (This option appears if you select **Prepare Now and Expand Later** in step 2.)

The expand cluster or node preparation process begins. The progress messages appear in the **Expand Cluster** window, and you can also monitor the progress from the **Tasks** dashboard. Nodes are processed (upgraded or reimaged as needed) and added in parallel. Adding nodes can take some time. Imaging a node typically takes a half hour or more depending on the hypervisor.

17. If the cluster has multiple storage pools, assign the new storage capacity to a storage pool after the nodes are added successfully:

**Note:** When the cluster has only one storage pool, you can ignore this step because the new storage is added to that storage pool automatically.

- a. From the dropdown menu on the left of the main menu, select **Storage**.  
The System displays the **Storage Overview** page.
- b. Select **Table > Storage Container**
- c. Select the target storage pool (upper display) and click **Update**.
- d. In **Update Storage Pool**, check the **Use unallocated capacity** box in the **Capacity** line and then click the **Save** button.

This step adds all the unallocated capacity to the selected storage pool.

- e. Go to the **Tasks** dashboard and monitor progress until the node addition completes successfully.

Cluster expansion is not complete until the node is added to the metadata ring.

## What to do next

One or more of the following items might apply to the added nodes. Also, see [Prerequisites and Requirements](#) on page 204.

- Nondefault timezones are not updated on added nodes and must be reconfigured manually.
- If the password for the Controller VM in the cluster was changed from the default password, the password on any new nodes gets updated automatically to match the cluster password.
- To check Controller VM memory compatibility after cluster expansion, run the `cvm_same_mem_level_check` and `cvm_memory_check` NCC checks. For more information, see [Running Checks by Using Prism Element Web Console](#) on page 257.
  - If the `cvm_same_mem_level_check` result is FAIL, the memory size in the added nodes is not the same as the other Controller VMs in the cluster. If the memory is less than the common size, increase the memory to match.
  - If the `cvm_memory_check` result is FAIL, the Controller VM memory is less than the minimum required for the workload. Increase the memory to (at least) the minimum size.

For information about increasing the memory of the Controller VM, see [Increasing the Controller VM Memory Size](#) on page 100. For information about the Controller VM memory size recommendations, see [CVM Memory Configuration](#) on page 99.

## Prerequisites and Requirements

The process for adding a node varies depending on the AOS version, hypervisor host type, data-at-rest encryption status, and certain hardware configuration factors.

### AOS Considerations

The following apply to any cluster:

- Ensure that the total number of nodes per cluster does not exceed the Cluster Maximums defined in [Maximum System Values](#) on page 51. The maximum number of nodes per cluster depends on the hypervisor type and whether the cluster is a pure hypervisor cluster (only one hypervisor type) or a mixed hypervisor cluster (more than one hypervisor type).
- The expand cluster process does not support compute-only node preparation.
- In the cluster expansion process, discovering new nodes to add to a cluster requires IPv6 multicast packets to pass through the physical switch. If IPv6 is disabled on your network, the expand cluster process fails. If IPv6 is not enabled, do one of the following:
  - Enable IPv6 in your network and retry the expand cluster operation.
  - If you cannot enable IPv6 you can manually enter the IP addresses of nodes and run discovery using IPv4. Ensure that you have the IP addresses before starting the expand cluster operation.
- If the Controller VM memory on a new node is less than the current nodes in the cluster, the expand cluster process increases the memory on the new node to the same base value as the current nodes. The new Controller VM is upgraded to a maximum of 32 GB.

The Controller VM is upgraded to a maximum of 28 GB for ESXi nodes with 64 GB or less of total physical memory. With total physical memory greater than 64 GB, the existing Controller VM memory is increased by 4 GB.

- A new node is reimaged automatically before being added under certain conditions. The following table describes those conditions.

**Table 45: Node Imaging Criteria**

Configuration	Description
Same AOS and hypervisor versions	The node is added to the cluster without reimaging it.
Same hypervisor version but different AOS version	The node is automatically reimaged before it is added. However, if the AOS version on the node is higher than the version on the cluster, you can upgrade the cluster to the higher version. If you do not upgrade the base cluster to match the node AOS version, the node is reimaged automatically to match the lower AOS version of the cluster. For more information about how to upgrade your cluster, see the <a href="#">Life Cycle Manager Guide</a> .
Same AOS version but different hypervisor version	The node is automatically reimaged before it is added.

**Note:** If you are expanding a cluster which is segmented only by traffic type (management and backplane), see [Network Segmentation During Cluster Expansion](#) in the *Security Guide*.

## AHV Considerations

The following apply to AHV clusters:

- If the Controller VMs in the cluster are in a VLAN-configured network, the discovery process detects all factory-prepared nodes, regardless of their VLAN status.
- You cannot reimagine a node running discovery OS when Link Aggregation Control Protocol (LACP) is enabled on the cluster. Discovery OS is a pre-installed software on Nutanix nodes that allows the nodes to be discovered. Prepare the node with LACP using a Foundation VM.
- If you plan to use an NVIDIA host driver on a host you are adding to a cluster with GPU nodes, do not install the driver before adding the host to the cluster. First, add the host to the cluster, then run the `install_host_package` script to install the driver. For more information, see [Installing the NVIDIA GRID Driver](#).
- Network configuration has the following restrictions and requirements:
  - You cannot migrate management from br0 to other bridges.
  - You can only have the Controller VM management interface (eth0) and hypervisor management interface deployed on the br0 bridge.

## ESXi Considerations

The following apply to ESXi clusters:

- Before adding a host running ESXi 7.0U2 and later versions, with Trusted Platform Module (TPM) 2.0 enabled, to a cluster, Nutanix recommends that you backup the recovery key created when encrypting the host with TPM. For information on how to generate and backup the recovery key, see [KB 81661](#) in the *VMware documentation*. Ensure that you use this recovery key to restore the host configuration encrypted by TPM 2.0 if it fails to start after adding the host to your cluster. For information on how to restore an encrypted host, see [KB 81446](#) in the *VMware documentation*. If you do not have the recovery key, and if the host fails to start, contact Nutanix Support.
- If the ESXi root user password was changed from the default password, cluster expansion might fail. In this case, reset the ESXi root user password to the default password, and then retry the cluster expansion procedure. For default cluster credentials, see [KB 1661](#).
- While expanding a Nutanix cluster running NSX enabled ESXi hosts, add the newly imaged node to the Nutanix cluster where the host and CVM management network are configured with a standard vSwitch, and then add the node in NSX manager. Otherwise, the cluster expansion operation fails with the following error. For information on how to expand a cluster, see [Expanding a Cluster](#) on page 198.

`Failed to get VLAN tag of node <MAC Address of the node>`

- The expand cluster operation supports mixed node (ESXi + storage-only) clusters only if network segmentation is not enabled. If network segmentation is enabled for the mixed cluster, you cannot use the expand cluster operation. However, you can use the expand cluster operation for a mixed cluster that has backplane segmentation enabled and the storage-only nodes are hosted with AOS 6.1 or newer release.

- Network configuration has the following restrictions and requirements:
  - You cannot configure the network when either a target node or the base cluster has LACP enabled. Prepare LACP nodes offline using a Foundation VM.
  - You cannot migrate management from vSwitch0 to another standard vSwitch.
  - Management interfaces must either be on a VSS or a DVS; a mixed setup is not supported.
  - If on VSS, the Controller VM management interface (eth0) and the hypervisor management interface must be deployed on vSwitch0 and connected to port group VM Network and Management Network, respectively.
  - If on DVS, all Controller VM management interfaces and all host management interfaces must be connected to the same distributed virtual switch and same port group. (However, the Controller VM interfaces can be connected to a different DVS port group than the host management interfaces.)
  - Segmented network interfaces (backplane, volume, DR) must be on same vSwitch type (VSS or DVS) as the management.
  - If network segmentation is enabled on the base cluster and the backplane is deployed on a separate vSwitch than management, you can create vSwitches (VSS or DVS) and prepare the required Controller VM interfaces. (Manual switch configuration is required for expand now but is integrated into the expand later work flow.)
  - If the base cluster is on DVS and you are doing an expand later, you can migrate the target nodes from the default vSwitch0 to that DVS.
- If the Controller VMs in the cluster reside in a VLAN configured network, you must first configure the new nodes in the same VLAN before attempting to add them. Otherwise, the discovery process does not find these nodes. For more information about VLAN configuration instructions, see [Discovering Nodes in a VLAN-Segmented Network](#) in the *Field Installation Guide*.
- To expand a cluster configured with DVS for Controller VM external communication, ensure that you do the following:
  - Expand DVS with the new node.
  - Make sure both the host and the CVM are configured with DVS.
  - Make sure that host to CVM and CVM to CVM communications are working.
  - Follow the cluster expansion procedure.
- After adding the new nodes, note the following:
  - By default, the common Nutanix datastores are mounted on the new nodes after cluster expansion.
  - The target storage containers must be set to mount on the new hosts. You can check the mount status from the **Storage** dashboard. Click the **Storage Container** tab, select the target storage container, click the **Update** button, and ensure that **Mount on all ESXi Hosts** (or the new hosts are checked in **Mount/Unmount on the following ESXi Hosts**) is selected in the **NFS DATASTORE** field.
  - If a newly added node has an older processor class than the existing nodes in the cluster, cluster downtime is required to enable EVC (enhanced vMotion compatibility) with the lower feature set as the baseline. For an indication of the processor class of a node, see the **Block Serial** field in the **Hardware** dashboard. For more information, see [Hardware Diagram View](#) on page 183 or [Hardware Table View](#) on page 191. For more information on enabling EVC, see [vSphere EVC Settings](#) in the *vSphere Administration Guide for Acropolis*.

**Caution:** If you mix processor classes without enabling EVC, vMotion/live migration of VMs is not supported between processor classes. If you add the host with the newer processor class to vCenter Server before enabling

EVC, cluster downtime is required to enable EVC later because all VMs (including the Controller VM) must be shut down.

- Add the new nodes to the appropriate vCenter Server cluster. If an added node has a newer processor class (for example, Haswell) than the existing nodes in the cluster (Ivy Bridge or Sandy Bridge), enable EVC with the lower feature set as the baseline before adding the node to vCenter.
- If you are adding multiple nodes to an existing EVC-enabled vCenter cluster, which requires powering off the Controller VM for each node to complete the addition, add just one node at a time and wait for data resiliency to return to *OK* before adding the next node to vCenter.

**Caution:** Adding multiple nodes to vCenter simultaneously can cause a cluster outage when all the Controller VMs are powered off at the same time.

- If you are adding a node to a cluster where HA is enabled with APD and VMCP is enabled, you must enable APD and APD timeout on the new host.
- If you are adding new nodes to vCenter EVC configured cluster, ensure the following requirements.
  - Enabling EVC requires ESXi version 6.0 or above.
  - All ESXi nodes should be on same version and build.

## Hyper-V Considerations

The following apply to clusters running Hyper-V:

- Network preparation is not supported. To bypass this step and prepare the nodes otherwise, click the **Skip Networking** button when you get to the **Networking** tab. In addition, imaging to AHV or ESXi is not possible if the node or base cluster is Hyper-V.
- If the Controller VMs in the cluster reside in a VLAN configured network, you must first configure the new nodes in the same VLAN before attempting to add them. Otherwise, the discovery process does not find these nodes. For more information about VLAN configuration instructions, see [Discovering Nodes in a VLAN-Segmented Network](#) in the *Field Installation Guide*.
- After adding the new nodes, if you manage your Hyper-V cluster by using Microsoft System Center VM Manager (SCVMM), do not use the Prism Element web console or Microsoft Failover Cluster Manager to add the new node to the failover cluster. Instead, use SCVMM to add the node to the Hyper-V cluster and then perform the following steps in the SCVMM user interface.
  1. Open the SCVMM user interface.
  2. Refresh the cluster in SCVMM. The new node is displayed under the failover cluster in the **Pending** state.
  3. Right-click the node and select **Add to host cluster**.
  4. Choose a run-as account that has the local administrator permissions on the new node.
  5. Click **OK**. The SCVMM agent is installed on the node and file shares are registered to the new node.
  6. Update the networking and other settings of the node to match your standard configuration.

For Microsoft Windows Server 2012 R2 deployments, after adding the node to the cluster in SCVMM, ensure that node disks are not added as clustered resources. Open the Failover Cluster Manager and click **Storage > Disks** to check.

## Data-At-Rest Encryption Considerations

The following apply to clusters with data-at-rest encryption enabled. For more information, see [Data-At-Rest Encryption](#).

- Configure data-at-rest encryption for the new nodes. The new nodes must have self-encrypting disks or software-only encryption.

- If the cluster uses an external key manager server (KMS), either with self-encrypting drives or software only, then reimaging cannot be done through the expand cluster workflow. In this case, any nodes to add must already have the correct hypervisor and AOS version. Use Foundation to image the nodes (if needed) before attempting to add them to the cluster.
- If an encrypted cluster uses an external KMS, the new node might not be able to resolve the DNS name of the KMS. Therefore, you must manually update the resolv.conf file on the new node to enable communication between the node and the KMS.
- Adding a node to a cluster with self-encrypting drives (SED) where the added node is running a different hypervisor is not supported. In this case, image the node to the same hypervisor by using Foundation before adding it to the SED cluster. For more information, see [KB 4098](#).

## Nutanix Clusters Considerations

The following apply to clusters hosted on a cloud platform:

- When expanding a cluster on AWS, the nodes are not added to the Cassandra ring (wait in a queue) until there are enough nodes to extend the ring. In addition, new nodes are added to the Cassandra ring only when they are do not break domain awareness. (Other services remain unaffected.)

## Hardware Considerations

Note the following when it applies to the nodes you are adding:

- Ensure that you use the minimum version of Foundation required by your hardware platform. To determine whether Foundation needs an upgrade for a hardware platform, see the respective system specifications guide. If the nodes you want to include in the cluster are of different models, determine which of their minimum Foundation versions is the most recent version, and then upgrade Foundation on all the nodes to that version.
- When adding all-SSD nodes to an existing cluster, the minimum number of all-SSD nodes added must be equal to the maximum replication factor in the cluster.
- If you are adding a node with a different processor class to the cluster, ensure that there are no running VMs on the node and the host has the following configuration:
  - ESXi: Verify that EVC is enabled on the cluster.
  - Hyper-V: If you want to move the VMs between the nodes, ensure that you have selected the **Migrate to a physical computer with a different processor version** option for each VM by browsing to **Settings > Processor > Compatibility** in the **Action** pane of the Hyper-V Manager.

**Note:** Do not shut down more than one Controller VM at the same time.

- If you expand a cluster by adding a node with older generation hardware to a cluster that was initially created with later generation hardware, power cycle (do not reboot) any guest VMs before migrating them to the added older generation node or before upgrading the cluster.

Guest VMs are migrated during hypervisor and firmware upgrades (but not AOS upgrades).

For example, if you are adding a node with G4 Haswell CPUs to a cluster that also has newer G5 nodes with Broadwell CPUs, you must power cycle guest VMs hosted on the G5 nodes before you can migrate the VMs to the node with G4 CPUs. Power cycling the guest VMs enables them to discover a CPU set compatible with older G4 processors.

In rare cases, certain CPU features might be deprecated in the new generation of CPUs. For example, Intel introduced MPX in Skylake class of CPUs and deprecated it with Ice Lake. In such cases, introduction of Ice Lake

(newer) CPUs to an all-Skylake cluster can cause problems with existing VMs that are running with MPX. Such VMs must be power cycled.

Power cycle guest VMs from the Prism Element web console VM dashboard. Do not perform a Guest Reboot; a VM power cycle is required in this case.

- If you physically add a node to a block (for example, a single node shipped from Nutanix is placed into an empty slot in an existing chassis), log on to the Controller VM for that node, and update the following parameters in the /etc/nutanix/factory\_config.json file:
  - rackable\_unit\_serial: Set it to the same value as the other Controller VMs in the same block.
  - node\_position: Set it to the physical location of the node in the block (A, B, C, D).

After changing the configuration file, restart Genesis with the `genesis restart` command.

## Expand a Cluster with Flow Virtual Networking Enabled

### Check if the cluster uses non-default virtual switches

If you use non-default virtual switches for VPC (Flow Virtual Networking) traffic in an AHV cluster, prepare the new nodes and the existing AHV clusters accordingly. For information on how to check if the cluster uses non-default virtual switches for VPC traffic, see [Verifying if the Cluster uses Non-Default Virtual Switch](#) on page 209.

**Important:**

If the check result (output of the `acli atlas_config.get` command) shows the `vpc_east_west_traffic_config` section with `dvs_uuid` displaying the UUID of a non-default virtual switch, follow the procedure in this section.

If the `vpc_east_west_traffic_config` section does not exist, do not follow the procedure in this section.

### Cluster Network

This procedure assumes the following cluster network configuration:

- `vs0` is the default virtual switch for Controller VM and AHV communications.
  - All bridges are configured with Active-Active with LACP.
- 
- To prepare the new clusters for cluster expansion, see [Preparing the New Nodes for Addition to Existing AHV Cluster](#) on page 210.
  - To verify that the new node is adequately prepared for expansion of the existing cluster, see [Verifying the New Node Setup](#) on page 211.
  - To expand the cluster with the new node you prepared, see [Expanding a Cluster with Flow Virtual Networking Enabled](#) on page 212.

### Verifying if the Cluster uses Non-Default Virtual Switch

Verify if the cluster uses non-default virtual switches to route VPC traffic.

#### About this task

Use the `acli atlas_config.get` command to verify if the cluster uses non-default virtual switches to route VPC traffic.

#### Procedure

1. Log on to the CVM and run the following command.

```
nutanix@cvm$ acli
```

```
acli>
```

- Run the following command at the `acli` prompt.

```
acli> atlas_config.get
```

A sample output is as follows:

```
config {
    anc_domain_name_server_list: "10.xxx.xxx.xxx"
    dvs_physnet_mapping_list {
        dvs_uuid: "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
        physnet: "physnet1"
    }
    enable_atlas_networking: True
    logical_timestamp: 54
    minimum_ahv_version: "20201105.2016"
    ovn_cacert_path: "/home/certs/OvnController/ca.pem"
    ovn_certificate_path: "/home/certs/OvnController/OvnController.crt"
    ovn_privkey_path: "/home/certs/OvnController/OvnController.key"
    ovn_remote_address: "ssl:anc-ovn-external.default.xxxx.nutanix.com:6652"
    vpc_east_west_traffic_config {
        dvs_uuid: "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
        permit_all_traffic: True
    }
}
```

Verify if the `vpc_east_west_traffic_config` section is displayed in the output.

- Run the following command at the `acli` prompt to verify the UUIDs of all virtual switches.

```
acli> net.get_virtual_switch *
```

The sample output provides the UUIDs of all the virtual switches. Verify the virtual switch UUID that matches the value of `dvs_uuid` available in the output of the previous step. Verify if `default: True` attribute is not available for this virtual switch in the output, this virtual switch is the non-default virtual switch.

For information on commands for managed networks, see the [Command Reference](#).

## Preparing the New Nodes for Addition to Existing AHV Cluster

### About this task

Before imaging each new node with Foundation software, perform these steps to prepare all the new nodes you are adding to the existing cluster:

- (If Secure Boot is used in the cluster) Ensure that the node is booting with UEFI and not in Legacy BIOS. Ensure that Foundation does not change the node to boot mode back to Legacy BIOS. Change the Foundation settings if required.
- Ensure that the firmware on the new node is consistent with the firmware on the existing nodes in the cluster. If feasible, update the firmware on the new node to match the firmware version on the nodes in the cluster.
- Use the appropriate Foundation version to image the new node with the same AOS and AHW versions as those on *the cluster* to which you are adding the node. This is essential to prevent the cluster expansion process from running another Foundation imaging process and wiping out all prepared elements.

After imaging each node with Foundation software, perform these steps to prepare all the new nodes you are adding to the existing cluster:

### Procedure

- (If Secure Boot is used in the cluster) Enable Secure Boot for the node.

2. Check all physical-to-Ethernet port mappings to ensure that the physical connectivity matches the logical configuration. Verify that these mappings are consistent with the mappings in existing nodes to ensure AHV correctly enumerates Ethernet port numbering and maps Ethernet to the bridge (virtual switch) properly.
3. Configure the default virtual switch vs0 (and bridge br0) and the uplinks to match the existing nodes. You need not pre-create non-default virtual switches like vs1 and vs2 (with bridges br1 and br2) on new nodes if the switches were created after cluster expansion. Only pre-create and configure non-default virtual switches that already exist on the cluster nodes.

## What to do next

Verify the new node setup to ensure that it is adequately prepared for cluster expansion.

### Verifying the New Node Setup

#### About this task

Before you expand the existing cluster with the new node, verify that the new node is adequately prepared.

#### Procedure

1. Ensure that the new node is physically installed at the required location. To verify that the new node is physically installed correctly, do the following.
  - a. Ensure that redundant power cables are connected and power failover is tested after powering on the node.
  - b. Ensure that the node boots in AHV.
  - c. Ensure that the physical network connections are made in accordance with the physical connections on the existing nodes in the cluster.

Ensure that:

- Each virtual switch on the new node has dual redundant uplinks.
- The NICs have the same speed across all the nodes in the cluster.
- All the physical connections have the link lights on.

2. Log on to Controller VM on the new node and run the manage ovs show interfaces command to check if the necessary interfaces are up and displaying the necessary speed.
3. Perform network reachability tests to ensure that AHV, Controller VM and IPMI (management connectivity) are reachable over the network.

4. Perform NIC failover tests for the bridge (br0) on the default virtual switch vs0. Perform these tests from a local console that has access to the new AHV host.
  - a. Log on to AHV via a shell session.
  - b. Ping the default gateway of the network. Check the response for connectivity and latency. A good response would show low latency.
  - c. Disconnect both the uplinks for the default virtual switch. The ping responses display failure.
  - d. Reconnect only the first uplink and check the duration between the link light coming up and the positive ping response. Nutanix recommends a duration of less than two seconds.
  - e. Disconnect the first uplink. The pings fail again.
  - f. Reconnect only the second uplink and check the duration between the link light coming up and the positive ping response.
  - g. Reconnect the first uplink and check whether the pings fail. The pings must continue to display positive responses with low latencies.

Repeat these steps after logging on to the Controller VM on the new node.

If you find any issues with the failover, resolve the same before proceeding further with cluster expansion.

5. To check Secure Boot and vs0 configurations, do the following:

- a. Log on to the AHV host using a shell session and run the following command:

```
AHV# mokutil --sb-state
```

The output of the command indicates that Secure Boot is enabled.

- b. Check the LACP status on the AHV using the following command:

```
AHV# ovs-appctl lacp/show
```

The status of each uplink bond must be displays as **Negotiated** and not as **Active**.

- c. Log on to the Controller VM on the new node and run the following command to display the uplink status.

```
nutanix@cvm$ manage ovs show uplinks
```

Check the bridges, Ethernet and uplink bond configurations

Ensure that all issues found at this stage are resolved before proceeding to cluster expansion.

## **Expanding a Cluster with Flow Virtual Networking Enabled**

Use this procedure to expand an AHV cluster registered to Prism Central, where the Flow Virtual Networking Network Controller is enabled, and GENEVE traffic is moved to non-default virtual switches.

### **Before you begin**

For cluster network configuration used in this procedure, see [Expand a Cluster with Flow Virtual Networking Enabled](#) on page 209.

See [Prerequisites and Requirements](#) before expanding a cluster using Prism Element web console .

Before expanding the existing cluster, prepare the new nodes. For more information, see [Preparing the New Nodes for Addition to Existing AHV Cluster](#) on page 210 and [Verifying the New Node Setup](#) on page 211.

### **About this task**

The following steps can be implemented only if the new node is not re-imaged by Foundation during cluster expansion.

**Note:** The Flow Virtual Networking stack (Network Controller with brAtlas) is not present on the new node, causing VM migrations to the node to fail.

## Procedure

1. Log on to the CVM and run the following command to check the current status of Acropolis Dynamic Scheduling (ADS)

```
nutanix@cvm$ acli  
acli> ads.get
```

2. Check if ADS status is enabled or disabled.

If ADS is enabled, run the following command to disable ADS:

```
acli> ads.update enable=false
```

3. Repeat Step 1 to check the status of ADS and ensure that ADS is disabled. This step ensures that no VMs are migrated to the new node during the cluster expansion.

4. Log in to the Prism Element web console of the cluster.

You need a minimum of Cluster Admin privileges to run the cluster expansion workflow in the Prism Element web console.

5. From the dropdown menu, select **Hardware**.

The system displays the **Hardware Overview** page.

6. Click **+ Expand Cluster**.

The system displays the **Expand Cluster** dialog box.

7. Select the **Expand Cluster** option and click **Next**.

The system starts the discovery process to search for Nutanix nodes and blocks. The process generates a list of discovered nodes.

Discovery requires that IPv6 multicast packets are allowed through the physical switch. If you see a failure message, review the requirements in [Prerequisites and Requirements](#) on page 204.

8. Do one of the following:
  - » If the list includes all specified prepared nodes, go to the next step.
  - » If IPv6 is not supported for the cluster or the list does not include the correct nodes, click **Discover Hosts Manually**, and do the following to retry discovery using IPv4:
    - In the **Manual Host Discovery** window, click the **+Add Host** link. A line appears in the table below the link.
    - Enter the Controller VM IP address on that host (or the host IP address for compute-only nodes) and then click **Save**.
    - Add more hosts as desired.
    - When the list of hosts is complete, click the **Discover and Add Hosts** button. Manual discovery uses IPv4 to find and add the hosts to the list.

» If the list includes all specified prepared nodes, go to the next step.  
» If IPv6 is not supported for the cluster or the list does not include the correct nodes, click **Discover Hosts Manually**, and do the following to retry discovery using IPv4:

- In the **Manual Host Discovery** window, click the **+Add Host** link. A line appears in the table below the link.
- Enter the Controller VM IP address on that host (or the host IP address for compute-only nodes) and then click **Save**.
- Add more hosts as desired.
- When the list of hosts is complete, click the **Discover and Add Hosts** button. Manual discovery uses IPv4 to find and add the hosts to the list.

9. In the **Select Host** tab, select the check box for each node that you need to add to the cluster.

Check the **Host Name**, **Controller VM [IPv4|IPv6]**, **Hypervisor [IPv4|IPv6]**, and **IPMI IP [IPv4|IPv6]** fields. Ensure that the details are displayed correctly. Resolve any discrepancies before you proceed.

10. In the **Choose Node Type** tab, select the node type as **HCI Node**.
11. In the **Host Networking** tab, click **Skip Host Networking**.
12. In the **Configure Host** tab, if the detected AHV and AOS version on the selected new nodes are the same as versions on the existing nodes in the cluster, no imaging is required and a message acknowledging that fact appears. Skip to the next step.

Since the nodes were prepared with the correct AHV and AOS versions, this message is expected to be displayed, allowing you to skip to the next step.

13. When all the fields are correct, click the **Run Checks** button to verify that the nodes are ready.

This runs a set of precheck tests on the nodes. Progress messages appear in the **Expand Cluster** window. You can also monitor progress from the **Tasks** dashboard. For more information, see [View Task Status](#) on page 87.

14. Click the **Expand Cluster** button to begin the cluster expansion process.

After the first round of tasks is complete, a second round of tasks to add the nodes into the metadata ring automatically starts.

Check whether the nodes are added to the metadata ring by logging on to any Controller VM in the cluster and running the following commands:

```
nutanix@cvm$ nodetool -h 0 ring
```

The output lists all the controller VMs in the cluster and displays their status as Up.

15. Place all the new nodes in maintenance mode using aCLI. Do not use Prism Element web console.

Log on to any Controller VM in the cluster, enter `acli>` mode and run the aCLI command as follows:

```
acli> host.enter_maintenance_mode <host IP address>
```

Replace `<host IP address>` with the Controller VM IP address of the new node.

Run this command for each new node.

**16.** Update each virtual switch to include the new nodes.

- Update the uplinks of the virtual switches for the new nodes.

For information on how to update the uplink configuration, see [Creating a Virtual Switch](#) on page 151.

- Retrieve the UUID of the new node.

```
acli> host.list
```

Note the UUID of the new host in the aCLI command output.

- Run the following command at the `acli>` prompt to configure the IP addresses for new nodes.

```
acli> net.update_virtual_switch virtual-switch-name host_ip_addr_config='{<new-host-uuid1>:<new-host_ip_address/prefix>}'
```

Replace

- `<new-host-uuid1>` with the UUID of the new node noted in the previous step.
- `<new-host_ip_address/prefix>` with the IP address with prefix for new node.

To add the IP addresses of multiple new nodes to the host IP address configuration, use the following command format:

```
acli> net.update_virtual_switch vs1 host_ip_addr_config='{<new-host-uuid1>:<host_ip_address1/prefix>;<new-host-uuid2>:<host_ip_address2/prefix>;<new-host-uuid3>:<host_ip_address3/prefix>}'
```

- If the IP address of the new node does not belong to the default VLAN and the new node generates VPC traffic, tag the VLAN of the new node to the bridge of the non-default virtual switch. Log on to the new host with `root` privileges and run the following command.

```
root@ahv$ ovs-vsctl set port <brX> tag= <VLAN-ID>
```

Replace `<brX>` with the non-default bridge such as br1 or br2.

Replace `<VLAN-ID>` with the ID of the non-default VLAN that the new node IP address belongs to.

For more information, see [Assigning an AHV Host to a VLAN](#).

For information on how to update the virtual switches, see [Modifying Switch Information](#).

**17.** Reconfigure Flow Virtual Networking (Network Controller) on the new nodes.

- Ensure that the new node is placed to the maintenance mode (see [previous step](#)).

- Verify that the `Connected` status of the new node is True.

Run the aCLI `host.list` command and check the `Connection` status of the new node in the table in the output.

```
acli> host.list
```

A sample output of this command is as follows:

Hypervisor IP	Hypervisor DNS Name	Host UUID	Node		
state	Connected	Node type	Schedulable	Hypervisor Name	CVM
xx.xx.xx.1	xx.xx.xx.1	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx1			
AcropolisNormal	True	Hyperconverged	True	AHV	
xx.xx.xx.11					
xx.xx.xx.2	xx.xx.xx.2	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx1			
AcropolisNormal	True	Hyperconverged	True	AHV	
xx.xx.xx.12					

xx.xx.xx.3	xx.xx.xx.3	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx1
AcropolisNormal	True	Hyperconverged True AHV
xx.xx.xx.13		
xx.xx.xx.4	xx.xx.xx.4	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx1
EnteredMaintenanceMode	True	Hyperconverged False AHV
xx.xx.xx.14		

- c. Log on to the new host with `root` privileges and run the following command.

```
root@ahv# systemctl stop ahv-host-agent
```

After a few minutes, verify that the `Connected` status of the new node is False using the aCLI `host.list` command.

- d. Log on to the new host with `root` privileges and run the following command.

```
root@ahv# systemctl start ahv-host-agent
```

After a few minutes, verify that the `Connected` status of the new node is True using the aCLI `host.list` command.

Run this procedure on each new node.

**18.** Verify that no unresolved error exists.

- a. Run NCC checks and resolve any errors.

- b. In Prism Element web console of the cluster, click the **Settings** in the main menu and then select **Network Configuration > Virtual Switch**, and verify none of the virtual switches show a red warning icon.

If you see a red icon for any virtual switch, go to the **Alerts** page and check the alerts. The following alerts are not issued or are automatically resolved.

- Default Virtual Switch Error: This alert is not resolved automatically. Resolve it manually if you have verified that the virtual switch is healthy.
- Inconsistent Virtual Switch State Detected: This alert is resolved in the previous steps.
- Failed to configure host for Atlas networking: This alert is resolved in the previous steps.
- VPC east-west traffic configuration error: This alert is resolved in the previous steps.

Resolve all alerts. If you do not see any red icons for the virtual switches, go to the next step.

**19.** After the cluster health is validated as good, re-enable ADS using aCLI.

- a. Get the ADS status.

```
nutanix@cvm$ acli
acli> ads.get
```

- b. Enable ADS.

```
acli> ads.update enable=true
```

**20.** Remove the new nodes from maintenance mode using aCLI.

Log on to any Controller VM in the cluster, enter `acli>` mode and run the aCLI command as follows:

```
acli> host.exit_maintenance_mode <host IP address>
```

Replace `<host IP address>` with the Controller VM IP address of the new node.

Run this command for each new node.

## What to do next

Run network connectivity validations for guest VMs in the cluster, using test VMs. Create a test VM with appropriate IP address in the guest VM network and run ping tests from the test VM to the default gateway of the guest VM network and the IP addresses of the other guest VMs in the network. You need one test VM per guest VM network for this test.

# Node Maintenance

This section provides information about node maintenance in a Nutanix cluster.

## Node Maintenance Mode

You must place a node into the maintenance mode or non-operational state before making network configuration changes, upgrading or replacing firmware, performing CVM maintenance, or performing any other maintenance tasks.

### Placing a Node in Maintenance Mode

You can place only one node in maintenance mode at a time per cluster. You can place a node in maintenance mode using the Prism Element web console or using CLI.

When you place a node in maintenance mode using the Prism Element web console, the CVM automatically enters maintenance mode, and any replication factor 1-enabled VMs in the node are powered off. The cluster marks the node as unschedulable to prevent new VM instances from being created on it. The system also attempts to evacuate VMs from the node. If the evacuation fails, the node remains in the entering maintenance mode state, marked as unschedulable, and waits for user remediation. For information on how to place a node in maintenance mode using the Prism Element web console, see [Putting a Node into Maintenance Mode using Web Console](#) on page 218.

When you place a node in maintenance mode using the CLI, the system puts only the hypervisor (host) into maintenance mode, while the Controller VM (CVM) continues running. This means that VM workloads are migrated or powered off as expected, but the CVM remains operational. To place the entire node, including the CVM, into maintenance mode, you must run a separate command to shut down the CVM safely. This ensures that cluster services are fully paused on the node before performing maintenance tasks. For information on how to place a node in maintenance mode using CLI, see [Putting a Node into Maintenance Mode using Web Console](#) on page 218 using CLI in the AHV Administration Guide.

To place the entire node under maintenance, Nutanix recommends using Prism Element web console or Prism Central. When you place a node in maintenance mode, non-migratable VMs, such as pinned VMs or replication factor 1-enabled VMs with node affinity, are powered off. Live-migratable and high availability (HA) VMs are moved from the original host to other hosts in the cluster.

After the node exits maintenance mode, non-migratable VMs are powered on, and live-migrated VMs are automatically restored to the original host.

**Note:** VMs with CPU passthrough or PCI passthrough, pinned VMs (with host affinity policies), and replication factor 1 enabled VMs are not migrated to other hosts in the cluster when a node undergoes maintenance. Click the View these VMs option to view the list of VMs that cannot be live-migrated.

### Exiting a Node from Maintenance Mode

For information on how to remove a node from the maintenance mode using the Prism Element web console, see [Exiting a Node from the Maintenance Mode using Web Console](#) on page 219.

For information on how to remove a node from the maintenance mode using CLI, see [Exiting a Node from the Maintenance Mode using CLI](#) in the AHV Administration Guide.

## **Viewing a Node under Maintenance Mode**

For information on how to view the node under maintenance mode using the Prism Element web console, see [Viewing a Node that is in Maintenance Mode](#) on page 220.

## **UVM Status When Node under Maintenance Mode**

For information on how to view the status of UVMs when a node is undergoing maintenance operations, see [Guest VM Status when Node is in Maintenance Mode](#) on page 221.

## **Best Practices and Recommendations**

Nutanix strongly recommends using the **Enter Maintenance Mode** option on the Prism Element web console to place a node under maintenance.

## **Known Issues and Limitations**

- You can place one node at a time in maintenance mode for a cluster.
- Entering or exiting a node from maintenance mode using CLI is not equivalent to entering or exiting a node from maintenance mode using the Prism Element web console. When you place a node in maintenance mode using the Prism Element web console, both the hypervisor (host) and the CVM automatically enter maintenance mode. However, if you use the CLI, only the hypervisor (host) enters maintenance mode, while the CVM continues running.

**Warning:** You must exit the node from maintenance mode using the same method you used to put the node into maintenance mode. For example, if you put the node into maintenance mode using CLI, you must use CLI to exit the node from maintenance mode.

Switching the methods, such as using the CLI to enter maintenance mode and the Prism Element web console to exit or vice versa, disrupts the maintenance workflow. This might affect processes like node upgrades and the restart of CVM services after the node exists the maintenance mode.

## **Putting a Node into Maintenance Mode using Web Console**

Put a node into maintenance mode using Prism Element web console.

### **Before you begin**

- Check the cluster status and resiliency before putting a node in maintenance mode.
- Verify the status of the guest VMs. For more information, see [Guest VM Status when Node is in Maintenance Mode](#) on page 221.

### **About this task**

As the node enter the maintenance mode, the system performs the following high-level tasks internally.

- The AHV host initiates entering the maintenance mode.
- The HA VMs are live migrated.
- The pinned and replication factor 1 enabled VMs are powered-off.
- The AHV host completes entering the maintenance mode.

**Note:** At this stage, the AHV host is not shut down. For information on how to shut down the AHV host, see [Shutting Down a Node in a Cluster \(AHV\)](#). You can list all the hosts in the cluster by running `nutanix@cvm$ acli host.list` command, and note the value of *Hypervisor IP* for the node you want to shut down.

- The CVM enters the maintenance mode.

- The CVM is shut down.

Perform the following steps to put the node into maintenance mode.

## Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu, select **Hardware**.  
The system displays the **Overview** page.
3. Go to the **Table > Host** view.
4. Select the node to put in maintenance mode.
5. Click **Enter Maintenance Mode**.  
The system displays the **Host Maintenance**

**Note:** VMs with CPU passthrough, PCI passthrough, pinned VMs (with host affinity policies), and replication factor 1 are not migrated to other hosts in the cluster when a node undergoes maintenance. Click **View these VMs** link to view the list of VMs that cannot be live-migrated.

6. Select the **Power-off VMs that can not migrate** checkbox to enable the **Enter Maintenance Mode** button.
7. Click **Enter Maintenance Mode**.
  - A revolving icon appears as a tool tip beside the selected node and also in the Host Details view. This indicates that the host is entering the maintenance mode.
  - The revolving icon disappears and the **Exit Maintenance Mode** option is enabled after the node completely enters the maintenance mode.
  - You can also monitor the progress of the node maintenance operation through the newly created Host enter maintenance and Enter maintenance mode tasks which appear in the task tray.

**Note:** In case of a node maintenance failure, certain operations such as CVM reboot is rolled-back. But the live migrated VMs are not restored to the original host.

## What to do next

After the node is in maintenance mode, you can perform any of the following.

- View the nodes in maintenance mode. For more information, see [Viewing a Node that is in Maintenance Mode](#) on page 220.
- View the status of the guest VMs. For more information, see [Guest VM Status when Node is in Maintenance Mode](#) on page 221.
- Exit the node from the maintenance mode. For more information, see [Exiting a Node from the Maintenance Mode using Web Console](#) on page 219.

## Exiting a Node from the Maintenance Mode using Web Console

After you perform a maintenance activity, exit the node from the maintenance mode.

## About this task

**Warning:** You must exit the node from maintenance mode using the same method you used to put the node into maintenance mode. For example, if you put the node into maintenance mode using CLI, you must use CLI to exit the

node from maintenance mode. Switching the methods, such as using the CLI to enter maintenance mode and the Prism Element web console to exit or vice versa disrupts the maintenance workflow.

This might affect processes like node upgrades and the restart of CVM services after the node exists the maintenance mode.

As the node exits the maintenance mode, the following high-level tasks are performed internally.

- The CVM is powered on.
- The CVM is taken out of maintenance.
- The host is taken out of maintenance.

**Note:** The system shuts down the AHV host when you put a node in maintenance mode. You must power on the AHV host when you exit the node from maintenance mode. For information on how to power on the AHV host, see [Starting a Node in a Cluster \(AHV\)](#).

After the host exits the maintenance mode, the replication factor 1 enabled VMs continue to be powered on and the VMs migrate to restore host locality.

For more information, see [Guest VM Status when Node is in Maintenance Mode](#) on page 221 to view the status of the UVMs.

Perform the following steps to exit the node from maintenance mode.

### Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu, select **Hardware**.  
The system displays the **Overview** page.
3. Go to **Table > Host**.  
The system displays a list of hosts in the cluster.
4. Select the node to exit the maintenance mode.
5. Click **Exit Maintenance Mode**.  
The system displays the **Host Maintenance** window.
6. Click **Exit Maintenance Mode**.
  - A revolving icon appears as a tool tip beside the selected node and also in the Host Details view. This indicates that the host is exiting the maintenance mode.
  - The revolving icon disappears and the **Enter Maintenance Mode** option is enabled after the node completely exits the maintenance mode.
  - You can also monitor the progress of the exit node maintenance operation through the newly created Host exit maintenance and Exit maintenance mode tasks which appear in the task tray.

## Viewing a Node that is in Maintenance Mode

### About this task

**Note:** This procedure is the same for nodes in AHV and ESXi clusters.

Perform the following steps to view a node in maintenance mode.

## Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu, select **Hardware**.  
The system displays the **Overview** page.
3. Go to **Table > Host**.
4. The system displays a list of hosts in the cluster. The host in maintenance mode displays an alert icon along with a tool tip beside the host. You can also view this icon in the host details view.

## What to do next

You can:

- View the status of the guest VMs. For more information, see [Guest VM Status when Node is in Maintenance Mode](#) on page 221.
- Remove the node from the maintenance mode. For more information, see [Exiting a Node from the Maintenance Mode using Web Console](#) on page 219[Exiting a Node from the Maintenance Mode \(vSphere\)](#).

## Guest VM Status when Node is in Maintenance Mode

The following scenarios demonstrate the behavior of three guest VM types - high availability (HA) VMs, pinned VMs, and replication factor 1 enabled VMs, when a node enters and exits a maintenance mode. The HA VMs are live VMs that can migrate across nodes if the host server goes down or reboots. The pinned VMs have the host affinity set to a specific node. The replication factor 1 enabled VMs have affinity towards a specific node or a Controller VM (CVM). To view the status of the guest VMs, go to **VM > Table**.

**Note:** The following scenarios are the same for nodes in AHV and ESXi clusters.

### Scenario 1: Guest VMs before Node Entering Maintenance Mode

All the guest VMs are powered-on and reside on the same host.

### Scenario 2: Guest VMs during Node Maintenance Mode

As the node enters maintenance mode, the following high-level tasks are performed internally.

1. The host initiates entering the maintenance mode.
2. The HA VMs are live migrated.
3. The pinned and replication factor 1 enabled VMs are powered-off.
4. The AHV host completes entering the maintenance mode.
5. The CVM enters the maintenance mode.
6. The CVM is shut down.

### Scenario 3: Guest VMs after Node Exits Maintenance Mode

As the node exits the maintenance mode, the following high-level tasks are performed internally.

1. The CVM is powered on.
2. The CVM is taken out of maintenance.
3. The host is taken out of maintenance.

After the host exits the maintenance mode, the replication factor 1 enabled VMs continue to be powered on and the VMs migrate to restore host locality.

## Repair Boot Disks

Use the **Repair Host Boot Disk or SSD Repair** option in the Prism Element web console to perform both graceful and non-graceful repairs on the hypervisor and CVM when the boot disks in the hypervisor fail.

Use Repair Host Boot Disk to repair the boot disk on CO, SO, and HCI nodes. Use SSD Repair to repair boot disks on single SSD SO node platforms.

You can use the Repair Host Boot Disk option only if the nodes are deployed with the following cluster setup:

- Optimized Database Solution:

- AHV CO with AHV SO
- ESXi CO with AHV SO

For more information, see [Optimized Database Solution](#).

- AHV SO with AHV or ESXi HCI
- AHV CO with AHV HCI
- ESXi CO with ESXi HCI

For information on how to perform **Repair Host Boot Disk** see Starting Host Boot Disk Repair (Proactive or Graceful Replacement) in the [Proactive Hypervisor Boot Drive Replacement guide](#).

For **SSD Repair**, see Repairing a Drive (Single SSD Platforms) in the [Boot/Metadata Drive Replacement \(Single SSD Platforms\) guide](#).

Repair Host Boot Disk is not supported in the following cases:

- CO nodes hosted with Hyper-V.
- CO nodes hosted on non-NX platforms.
- Hyper-V HCI with AHV SO in a mixed hypervisor environment.
- Ungraceful host boot disk repairs when CO nodes are hosted on platforms with dual M.2 boot disks without a Redundant Array of Independent Disks (RAID) configuration.

### Limitations of SSD Repair Function

The **SSD Repair** function is not supported for the HyperV HCI and AHV SO mixed hypervisor case.

## Cluster Modifications

You can modify a cluster to remove or reconfigure hardware components, such as nodes and disks, when necessary.

### Adding a Disk

Add a disk to a node in Nutanix or non-Nutanix environments.

#### Before you begin

If Data-at-Rest Encryption is enabled in the cluster, test the node certificates and verify that the status displays Verified. For more information, see *Data-at-Rest Encryption* in the Security Guide.

#### About this task

- For a self-encrypting drive (SED) or node, failure to remove the drive or node as recommended results in the drive or node being locked.

- The process of adding a disk, except for an NVMe disk, is the same across all platforms, including Nutanix and third-party platforms, if the platform runs Nutanix AOS. The process for adding an NVMe disk varies by platform. For details, see [Completing NVMe Drive Replacement \(Software Serviceability\)](#).
- The types of disks you can add depends on your platform configuration. For supported disk configurations, see the [System Specifications](#) for your platform.
  - Hybrid:** A mixture of SSDs and HDDs. Hybrid configurations fill all available disk slots, so you can add a disk only if there is a disk missing.
  - All-flash:** All-flash nodes have fully and partially populated configurations and accept SSDs only. You can add new disks to the empty slots.
  - SSD with NVMe:** A mix of SSDs and NVMe drives is supported, but only specific drive slots can contain NVMe disks.
  - HDD with NVMe:** A mix of HDDs and NVMe drives is supported, but only specific drive slots can contain NVMe disks.
  - All NVMe:** All NVMe nodes support both fully populated and partially populated configurations. You can add drives to empty slots as needed. NVMe nodes accept only NVMe drives.
- Nutanix supports mixing disks of different capacities within a node. However, the node limits higher-capacity disks to the capacity of the smallest disk. This enables disk replacement when only higher-capacity disks are available. To increase the overall storage capacity of the node, replace all disks with higher-capacity ones.
- Adding multiple disks across several nodes in quick succession can cause Stargate restarts and potential cluster-wide downtime. Add disks to one node at a time and wait for at least two minutes before proceeding to the next node.

## Procedure

- Insert the disk in an empty slot of the node.
- Log in to the Prism Element web console.
- From the dropdown menu, select **Hardware**.  
The system displays the **Hardware Overview** page.
- Click the **Diagram** tab.  
The system displays the **Hardware Diagram** view.
- Select the disk you added in Step 1.
- If the disk appears in red with the label **Unmounted Disk**, select the disk and click **Repartition and Add**.

**Caution:** This action permanently deletes all data on the disk. Verify that the disk contains no essential data before proceeding with repartitioning.

This label and option appears only if the replacement disk contains data, preventing accidental use of a disk with existing data.

- Go to **Hardware > Disk**, and ensure that the disk has been added to the original storage pool.  
If the cluster has only one storage pool, the disk is automatically added to the storage pool.

8. If the cluster has multiple storage pools and the drive is not automatically added to the storage pool, perform the following steps to add the disk to a storage pool:
  - a. From the dropdown menu on the main menu, select **Storage**.  
The system displays the **Storage Overview** page.
  - b. Go to **Table > Storage Pool**.  
The system displays a list of storage pools in the cluster.
  - c. Select the storage pool to add the disk, and click **Update**.  
The system displays the **Update Storage Pool** window.
  - d. In the **Capacity** section, select the **Use unallocated capacity checkbox** to add the available unallocated capacity to the storage pool.
  - e. Click **Save**.
  - f. Go to **Hardware > Diagram**, select the drive, and confirm that it is in the correct storage pool.

## Removing a Disk

Remove a disk for tasks such as replacing a failed disk.

### About this task

Removing a disk from a node takes time because the system must migrate the data on the disk to other disks before you remove the disk. Removing multiple disks across several nodes in quick succession can cause Stargate restarts and potential cluster-wide downtime. Remove disks from one node at a time and wait for at least two minutes before proceeding to the next node. You can monitor the disk removal progress from the dashboard.

To remove a disk, follow these steps:

### Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu, select **Hardware**.  
The system displays the **Hardware Overview** page.
3. Go to **Table > Disk tab**.  
The system displays a list of disks in the cluster.
4. Select the disk to remove, and click **Remove Disk**.  
The system prompts you to confirm the action.
5. Click **Remove**.  
The system removes the disk from the node.
6. Click the **OK** button in the confirmation dialog box.

**Caution:** The status message that appears on completion of the steps in this procedure might indicate that the data migration is complete, but do not physically remove a disk until the disk status indicator in the diagram view turns red.

## Node Removal from a Cluster

You might need to remove a node:

- To replace a failed node
- If a node is either unreachable or powered off

- To deprecate old nodes for cluster expansion

You can remove a node using the Prism Element web console or nCLI.

## Prerequisites for Removing a Node

Consider the following before you remove a node:

- Removing a node takes time because the system must migrate the data on that node to other nodes before you remove the node from the cluster. You can monitor progress through the dashboard messages. Removing a node also removes all the disks in the node.
- (Hyper-V only) Initiating the removal of a node running Hyper-V fails if the node is running as a part of a Hyper-V failover cluster and the following message appears.

`Node node id is a part of a Hyper-V failover cluster failover cluster name. Please drain all the roles, remove the node from the failover cluster and then mark the node for removal.`

If this message appears in nCLI or in web interface, as a cluster administrator, use Microsoft management tools such as **Failover Cluster Manager**, to drain all highly available roles from the node. Then remove the node from the failover cluster followed by removing the node from the AOS cluster.

- (ESXi only) Before removing the node, ensure that there are no guest VMs running on the respective ESXi host. Also, the CVM must be running on the node to initiate the node removal.
- (ESXi only) Ensure that the vSphere Distributed Switch (VDS) does not have any references to the host in the Port mirroring and VM templates. Ensure that there are no remaining VMs, VMkernels, or VM NICs associated with the VDS on the host to remove.
- (ESXi only) Temporarily disable DRS on the cluster before the node removal. Ensure that you re-enable DRS after node removal. Update the HA configuration to exclude the node to remove.
- (ESXi only) As a cluster administrator, use the VMware management tools to migrate all the guest VMs off the node/host, before removing the node from the AOS cluster of ESXi hosts. Then, disconnect and remove the node or host from the vCenter server.

**Caution:** Always migrate guest VMs before removing a host or node. Ensure the target cluster has sufficient compute capacity before proceeding. Removing a node or host without migrating the guest VMs may cause service disruptions.

## Removing a Single Node

Remove a node from a cluster.

### About this task

Ensure that all the prerequisites are met. For more information, see [Prerequisites for Removing a Node](#).

To remove a single node (host) from the cluster, follow these steps:

### Procedure

1. Log in to the Prism Element web console.
2. From the dropdown menu, select **Hardware**.  
The system displays the **Hardware Overview** page.
3. Go to **Table > Host** tab.  
The system displays a list of nodes in the cluster.

**4.** Select the node to remove, and click **Remove Host**.

**Note:** The **Remove Host** option does not appear for a three-node cluster.

The system prompts you to confirm the action.

**5.** Click **Remove**.

The system removes the node from the cluster.

**6.** Click **OK** in the confirmation dialog box.

If the node that you are trying to remove is unreachable or powered off, the Prism Element web console triggers an alert notification indicating that the system cannot calculate the storage utilization for this node and warning of the possible impact of removing the node. If you choose to proceed use the force option to mark this node for removal.

**Caution:** Do not shut down the CVM or put the CVM into maintenance mode while the node removal is in progress.

### What to do next

- The Prism Element web console displays a warning message that you must reclaim the cluster license after you remove a node. For information about reclaiming or rebalancing your cluster licenses, see *License Manager Guide*.
- If you remove the last node with older-generation hardware from a cluster and the remaining nodes have newer-generation hardware, you must power cycle the guest VMs to allow them to detect a CPU set compatible with the new hardware. For example, if you remove the last node with a G4 Haswell CPU from a cluster where all remaining nodes are G5 Broadwell CPU nodes, the VMs recognize the newer G5 CPU set only after a power cycle.
- A power cycle is not required for normal cluster functionality, but guest VMs continue to use the older CPU set until you trigger a power cycle.
- After you remove a node, it goes into an unconfigured state. You can add such a node back to the cluster using the [Expanding a Cluster](#) on page 198 workflow.

**Caution:** After adding the removed node back into the cluster, the same cluster ID is applied to both clusters in the following circumstances:

- When the removed node is the first node (lowest IP address in the cluster)
- When you reuse the removed node in another cluster
- When the removed node again becomes the first node (lowest IP address) in the new cluster

To prevent this occurrence, reimage the node (using Foundation) before adding it to the new cluster.

For information about how to image a node, see [Prepare Bare-Metal Nodes for Imaging](#) in the *Field Installation Guide*.

### Remove Multiple Nodes

AOS supports removing multiple nodes from a cluster. The multinode removal process is sequential, allowing you to request the removal of only one node at a time. However, you can mark additional nodes for removal while data eviction occurs in the background for previously marked nodes.

The multinode removal process includes the following steps:

1. Request to remove multiple nodes (one at a time) through the Prism Element web console or nCLI.

2. The system runs prechecks on each node to validate the removal request. The node must pass all the prechecks to proceed with removal.
3. For more information, see [Prechecks to Allow Multiple Node Removal](#) on page 227.
4. The system removes nodes sequentially from Cassandra's metadata ring.
5. The system rebuilds the data in parallel in the background for all nodes marked for removal.

### Prechecks to Allow Multiple Node Removal

When you mark multiple nodes for removal, the system runs the following prechecks before accepting the node for removal.

- The cluster upgrade process is not in progress.
- The minimum number of nodes required by Cassandra and Zookeeper are available and are in healthy (kNormal status) state.
- No other nodes are pending to be added to the cluster.
- The cluster continues to meet the maximum replication factor requirements after removal of the node.
- The cluster has enough usable storage capacity to rebuild the data from the removed node.

The system does not allow multinode removal if a node fails any of the prechecks.

### Limitations for Multinode Removal

The following limitations apply to remove multiple nodes from a cluster:

- System allows a maximum of four nodes to be removed simultaneously from a cluster.
- For clusters with erasure coding (EC) enabled, the system computes the longest strip size possible on the cluster based on the EC parameters and fault tolerance of the container. The system does not allow multinode removal if there are not enough viable entities of the desired fault domain (node/rack/ru) to accommodate the largest EC strip possible on this cluster.
- In nCLI, multinode removal is not allowed if you skip the space usage check.

```
ncli> host rm-start skip-space-check=true
```

## Removing Multiple Nodes

### Before you begin

Ensure that all the are met. For more information, see [Prerequisites for Removing a Node](#) on page 225.

### About this task

**Note:** This feature is supported on a cluster with a minimum of four nodes (hosts).

To remove multiple nodes from the cluster, follow these steps:

### Procedure

1. Log on to the Prism Element web console.
2. From the dropdown menu, select **Hardware**.  
The systems displays the **Hardware Overview** page.
3. Go to **Table > Host** tab.  
The system displays a list of nodes in the cluster.

**4.** Select the node to remove, and click **Remove Host**.

**Note:** The **Remove Host** option does not appear for a three-node cluster.

The system prompts you to confirm the action.

**5.** Click **Remove**.

You can monitor the node removal progress in the **Tasks** menu.

**Caution:** Do not shut down the CVM or put the CVM into maintenance mode while the node removal is in progress.

The system removes the node from the cluster.

**6.** To remove multiple nodes, repeat Step 4 and Step 5 for each node.

The Tasks menu shows the progress of the node removal. The first node that was selected to be removed has two subtasks running:

- Transferring metadata to replacement replicas
- Extent store replication

The subsequent nodes have one subtask running in parallel.

You can also monitor the data rebuild progress in the **Cluster Resiliency / Fault Tolerance Status** widget that appears in the Prism Element web console dashboard.

### What to do next

- The Prism Element web console displays a warning message that you must reclaim the cluster license after you remove a node. For information about reclaiming or rebalancing your cluster licenses, see [License Manager Guide](#).
- If you remove the last node with older-generation hardware from a cluster and the remaining nodes have newer-generation hardware, you must power cycle the guest VMs to allow them to detect a CPU set compatible with the new hardware. For example, if you remove the last node with a G4 Haswell CPU from a cluster where all remaining nodes are G5 Broadwell CPU nodes, the VMs recognize the newer G5 CPU set only after a power cycle.
- After you remove a node, it goes into an unconfigured state. You can add such a node back into the cluster using the [Expanding a Cluster](#) on page 198 workflow.

**Caution:** After adding the removed node back into the cluster, the same cluster ID is applied to both clusters in the following circumstances:

- When the removed node is the first node (lowest IP address in the cluster)
- When you reuse the removed node in another cluster
- When the removed node again becomes the first node (lowest IP address) in the new cluster

To prevent this occurrence, reimage the node (using Foundation) before adding it to the new cluster.

For information about how to image a node, see [Prepare Bare-Metal Nodes for Imaging](#) in the *Field Installation Guide*.

## Adding a Node

Manually add a node or host to the metadata store after replacing a failed metadata disk.

## About this task

Each node contains a disk for metadata storage, and AOS maintains a metadata store across these disks to ensure resiliency in case of a metadata disk failure. If a metadata disk fails, the system removes the affected node from the metadata store group while the cluster continues operating seamlessly. Typically, the node is automatically reintroduced into the metadata store after the failed disk is replaced. However, in rare cases, this might not happen. If the node is ready but is not added back automatically, the following alert message is displayed, and you must manually add it back.

When the node is not added back automatically, the following alert message is displayed:

Node ready to be added to metadata store

To add a node into the metadata store, follow these steps:

### Procedure

1. Log in to the Prism Element web console.

2. From the dropdown menu, select **Hardware**.

The system displays the **Hardware Overview** page.

3. Go to **Table > Host** tab.

The system displays a list of nodes in the cluster.

4. Select the node to add, and click **Enable Metadata Store**

The **Enable Metadata Store** option appears only if the node is not added back automatically.

The system adds the node to the metadata store.

## Compute-Only and Storage-Only Nodes Management

This section provides information about the key features, deployment specifications, and deployment methods for compute-only and storage-only nodes in the HCI setup.

### Compute-Only Nodes

The Nutanix cluster uses the resources (CPUs and memory) of a compute-only (CO) node exclusively for computing purposes. A CO node allows you to seamlessly and efficiently expand the computing capacity (CPU and memory) of your cluster. CO nodes do not have a Controller VM (CVM) or local storage.

#### Characteristics of CO Nodes

CO nodes provide greater control and value by optimizing the use of restrictive licenses. Unlike traditional nodes, CO nodes do not run a CVM. Instead, VMs on CO nodes access storage disks through CVMs running on the Nutanix Hyperconverged Infrastructure (HCI) nodes within the cluster. When a CO node is part of HCI cluster, the licensed cores of the CO nodes are dedicated exclusively to application VMs.

Applications or databases licensed on a per CPU core basis require licensing for the entire node, including the cores used by the CVM. CO nodes help maximize ROI for database licenses, such as Oracle and Microsoft SQL Server, by eliminating the need to allocate compute resources to a CVM because CO nodes do not run a CVM.

CO nodes do not have local storage. Instead, CO nodes support the following two types of nodes for storage operation:

- AHV SO (Optimized Database Solution) nodes. For more information, see [Optimized Database Solution](#) on page 241
- HCI nodes. For more information, see [Deployment Specifications and Considerations for Compute-Only and Storage-Only Nodes](#) on page 231

For information on how to deploy a CO node, see [Deployment of Compute-Only Nodes](#) on page 238.

## Storage-Only Nodes

A storage-only (SO) node enables seamless expansion of storage capacity within a cluster. SO nodes always run the AHV hypervisor, regardless of the hypervisor used in the existing cluster. When you add an SO node to a cluster, it continues to operate on AHV, ensuring compatibility without requiring additional hypervisor licenses. This allows you to scale storage independently without incurring extra licensing costs.

Foundation allocates the maximum resources to Controller VM (CVM) of the SO node as follows:

- CVM vCPU = All CPU cores of the physical host minus 2, limited to a maximum of 22 vCPUs

**Note:** This is applicable till Foundation version 5.3.x. From Foundation version 5.4 onwards, the capping of maximum 22 vCPUs is not applicable.

- CVM memory = Available RAM minus 16 GiB, limited to a maximum of 256 GiB.

**Note:**

- This is applicable from Foundation version 5.3 and above. In the earlier Foundation versions, the memory allocation happens without capping to 256 GiB.
- A capping of maximum 256 GiB is applied, and Foundation allocates the maximum possible vRAM to CVM. For example, if the available RAM is 512 GiB, the system allocates a maximum of 256 GiB and never considers the  $512 - 16 = 496$  GiB value. However, if you change the system allocated vRAM, the vRAM gets overridden with the supplied value.

**Note:** Minimum Foundation version of 5.3 supports these limits with NUMA pinnings or alignments. Earlier Foundation versions with a minimum version of 5.0 support these limits but not NUMA pinnings or alignments.

### Characteristics of SO Nodes

The following characteristics apply to the storage-only nodes:

- A storage-only node includes an AHV hypervisor, a Controller VM (CVM), and memory and CPU resources enough to run only the CVM.
- A storage-only node always runs the AHV hypervisor. Therefore, if you add a storage-only node to an ESXi or Hyper-V cluster, the hypervisor on the storage-only node is always AHV.
- For hardware model support for storage-only node, see [Supported Hardware Platforms](#) on page 234.
- A storage-only node is supported on ESXi, Hyper-V, and AHV clusters. However, you cannot run guest VMs on the storage-only nodes.

**Note:** A storage-only node is not the same as a storage-heavy node. A storage-heavy node is a regular Nutanix hyperconverged node, but with a greater storage capacity. A storage-heavy node can run any hypervisor (AHV, ESXi, or Hyper-V) and can run guest VMs.

AHV SO nodes do not perform the compute operation, and they support the following two types of nodes for compute operation:

- AHV or ESXi CO nodes (Optimized Database Solution)
- AHV or ESXi HCI nodes

For more information, see [Supported Deployment Configurations](#) on page 231.

For information on how to deploy a storage-only node, see [Deployment of Storage-only Nodes](#) on page 240.

## Deployment Specifications and Considerations for Compute-Only and Storage-Only Nodes

This section provides information about specifications, requirements, and best practices for compute-only nodes and storage-only nodes deployment in the Hyperconverged Infrastructure (HCI) setup.

### Supported Deployment Configurations

This section provides information about the supported deployment configurations for compute-only (CO) nodes and storage-only (SO) nodes.

#### AHV Compute-only node with AHV HCI Nodes

You can deploy AHV CO nodes that use AHV hyperconverged (HCI) nodes for storage in a cluster.

#### AHV Storage-only node with AHV or ESXi HCI Nodes

You can deploy AHV SO nodes for storage in the cluster with AHV hyperconverged (HCI) nodes.

#### Optimized Database Solution

The CO and SO nodes can also be deployed in an optimized database solution setup. For more information, see [Optimized Database Solution](#) on page 241.

#### Operation Specifications

This section provides information about the operational attributes for the supported deployment configurations of compute-only (CO) and storage-only (SO) nodes in a Hyperconverged Infrastructure (HCI) setup.

**Table 46: Operation Mechanism - Supported Deployment Configurations**

Component / Operation Type	Deployment Configuration	
	AHV CO with AHV HCI	AHV SO with AHV or ESXi HCI
Storage source for vDisk/Volumes associated with guest VMs on the compute-only (CO) node	HCI nodes in the cluster	SO nodes in the cluster
Controller VM (CVM) and local storage	No CVM and local storage on CO nodes	No CVM and local storage on HCI nodes
VMs Management (CRUD operations, ADS, and HA)	Using Prism Element web console	
Hypervisor operation for CO node	Runs on the local storage media of the CO node	Runs on the local storage media of the HCI node
Network segmentation support	Not supported	
Hypervisor and firmware upgrade	Using Life Cycle Manager (LCM). For more information, see the <a href="#">LCM Updates</a> in the Life Cycle Manager Guide.	

#### Cluster Requirements

This section provides information about the minimum cluster requirements for compute-only (CO) and storage-only (SO) nodes in a Hyperconverged Infrastructure (HCI) setup.

**Table 47: Minimum Cluster Requirements for Compute-Only Nodes and Storage-Only Nodes**

Cluster Attributes	AHV CO with AHV HCI	AHV SO with AHV or ESXi HCI
AOS Version	AOS 5.11 or later for HCI nodes	AOS 5.11 or later for SO nodes
AHV Version	Compatible AHV version based on AOS release.	Compatible AHV version based on AOS release.
Number of nodes	Minimum 3 HCI nodes and minimum 2 CO nodes	Minimum 3 SO nodes and minimum 2 HCI nodes
Nodes Ratio	Nutanix recommends the following nodes ratio:  2 CO : 1 HCI, if CVM is allocated with 16 logical cores.	Nutanix recommends the following nodes ratio:  1 HCI : 2 SO
Storage node Specification	All the HCI nodes in the cluster must be All-flash nodes.	All the SO nodes in the cluster must be All-flash nodes.
CPU and memory assignment	The number of vCPUs assigned to Controller VMs on the HCI nodes must be greater than or equal to the total number of available cores on all the AHV CO nodes in the cluster. The Controller VM requires a minimum of 12 vCPUs. For more information about how Foundation allocates memory and vCPUs to your platform model, see <a href="#">Controller VM (CVM Field Specifications in the Acropolis Advanced Administration Guide</a> .	The number of vCPUs assigned to Controller VMs on the SO nodes must be greater than or equal to the total number of available cores on all the AHV HCI nodes in the cluster. The Controller VM requires a minimum of 12 vCPUs. For more information about how Foundation allocates memory and vCPUs to your platform model, see <a href="#">Controller VM (CVM Field Specifications in the Acropolis Advanced Administration Guide</a> .
Network Speed	Use dual 25 GbE on AHV CO nodes and quad 25 GbE on AHV HCI nodes.	Use dual 25 GbE on AHV HCI nodes and quad 25 GbE on AHV SO nodes.
Hypervisor specification	<ul style="list-style-type: none"> <li>• For HCI node: AHV only</li> <li>• For CO node: AHV</li> </ul> <p>AHV CO node must run the same AHV version as the AHV HCI nodes in the cluster.</p> <p>When you add an AHV CO node to the cluster, AOS checks if the AHV version of the node matches with the AHV version of the existing AHV nodes in the cluster. If there is a mismatch, the node addition fails.</p> <p>For general requirements about adding a node to a Nutanix cluster, see <a href="#">Expanding a Cluster</a>.</p>	<ul style="list-style-type: none"> <li>• For HCI node: AHV or ESXi</li> <li>• For SO node: AHV</li> </ul> <p>AHV HCI node must run the same AHV version as the AHV SO nodes in the cluster.</p> <p>When you add an AHV HCI node to the cluster, AOS checks if the AHV version of the node matches with the AHV version of the existing AHV nodes in the cluster. If there is a mismatch, the node addition fails.</p> <p>For general requirements about adding a node to a Nutanix cluster, see <a href="#">Expanding a Cluster</a>.</p>
NIC Bandwidth	Total amount of NIC bandwidth allocated to all the HCI nodes must be twice the amount of the total NIC bandwidth allocated to all the CO nodes in the cluster.	Total amount of NIC bandwidth allocated to all the SO nodes must be twice the amount of the total NIC bandwidth allocated to all the HCI nodes in the cluster.

Cluster Attributes	AHV CO with AHV HCI	AHV SO with AHV or ESXi HCI
CPU	See <a href="#">Controller VM (CVM) Specifications</a> in the <i>Acropolis Advanced Administration Guide</i> .	
Memory		
Drives	See <a href="#">HCI Node Field Requirements</a> in the <i>Acropolis Advanced Administration Guide</i> .	
Socket	For CO node: Single or Dual socket  For HCI node: Dual socket except ROBO setup	For SO node: Single socket  For HCI node: Dual socket except ROBO setup
Host interface	For CO node: iSCSI (boot and data drives)  For HCI node: iSCSI	For SO node: <ul style="list-style-type: none"><li>• iSCSI, if mixed with AHV HCI</li><li>• NFS, if mixed with ESXi HCI</li></ul> For HCI node: <ul style="list-style-type: none"><li>• NFS for ESXi HCI node</li><li>• iSCSI for AHV HCI node</li></ul>

## Licensing Requirements

This section provides information about the licensing requirements that apply to compute-only (CO) and storage-only (SO) nodes deployment at your site in a Hyperconverged Infrastructure (HCI) setup.

**Table 48: Licensing Requirements**

Deployment Configuration	Licensing
AHV CO with AHV HCI	Uses NCI licenses on a per-core basis. For more information about NCI licences, see <a href="#">NCI section in Nutanix Cloud Platform Software Options</a> .
AHV SO with AHV or ESXi HCI	

## Configuration and Operation Limits

This section provides information about the configuration and operation limits that apply to compute-only and storage-only nodes deployment in a Hyperconverged Infrastructure (HCI) setup.

**Table 49: Configuration and Operation Limits - CO and SO Nodes Deployment**

Cluster Attributes	Deployment Configuration	
	AHV CO with AHV HCI	AHV SO with AHV or ESXi HCI
Number of VMs	See <a href="#">Nutanix Configuration Maximums</a>	
Number of Nodes	Up to 32	
Addition of HCI Node	Supported	
Rolling Restart	Supported	

Cluster Attributes	Deployment Configuration	
	AHV CO with AHV HCI	AHV SO with AHV or ESXi HCI
RDMA	Not supported	
Host boot disk replacement for CO nodes	Not supported	
Virtual Switch configuration	Supported	
Network segmentation for disaster recovery	Not supported	
Automatic discovery of CO nodes as part of <i>Expand cluster</i> workflow (see <a href="#">Expanding a Cluster</a> )	Not supported  Initiate the manual host discovery workflow to add compute-only node when you use the <a href="#">Expanding a Cluster</a> workflow.	Not supported  Initiate the manual host discovery workflow to add HCI node when you use the <a href="#">Expanding a Cluster</a> workflow.
Cluster Conversion	Not supported	

### Supported Hardware Platforms

This section provides information about the supported hardware platforms for compute-only (CO) and storage-only (SO) nodes deployment at your site in a Hyperconverged Infrastructure (HCI) setup.

**Table 50: Supported Hardware Platforms**

Deployment Configuration	Supported Hardware Platforms
AHV CO with AHV HCI	<ul style="list-style-type: none"> <li>For HCI node: Any NX G8 or G9 model or Dell XC750/ XC650</li> <li>For CO node: NX8170-G8, NX1175S-G8, NX-8170-G9, NX-1175S-G9, NX-8155-G9, NX-8150-G9, NX-9151-G9, and Dell XC750/ XC650</li> </ul>
AHV SO with AHV or ESXi HCI	<ul style="list-style-type: none"> <li>For HCI node: Any NX and OEM model</li> <li>For SO node: Any NX and OEM model</li> </ul> <p>For more information on qualified models, see <a href="#">Hardware Platforms Spec Sheets</a>.</p> <p><b>Note:</b> The NX-8155A-G9 can only be included if all other nodes in the cluster are also hosted on NX-8155A-G9 platform.</p>

### Networking Configuration for Compute Nodes

This section provides information about how to perform the networking configurations for compute nodes based on the deployment configuration at your site in a Hyperconverged Infrastructure (HCI) setup.

**Table 51: Networking Configurations for Compute-Only Nodes**

Deployment Configuration	Method to perform networking configurations
AHV CO with AHV HCI	Use the <code>manage_ovs</code> commands and add the <code>--host</code> flag to the <code>manage_ovs</code> commands.
AHV SO with AHV HCI	<p>For example, to create or modify the bridges or uplink bonds or uplink load balancing, run the following command:</p> <pre data-bbox="633 432 1462 517">nutanix@cvm\$ manage_ovs --host IP_address_of_compute_node --bridge_name bridge_name create_single_bridge</pre> <p>Replace:</p> <ul style="list-style-type: none"> <li>• <code>IP_address_of_compute_node</code> with the IP address of the CO node in AHV CO with AHV HCI deployment configuration or IP address of the HCI node in AHV SO with AHV HCI deployment configuration.</li> <li>• <code>bridge_name</code> with the name of bridge you want to create.</li> </ul> <p><b>Note:</b> Run the <code>manage_ovs</code> commands for an AHV CO node from any Controller VM running on an AHV HCI node.</p>
AHV SO with ESXi HCI	<p>Perform the networking tasks for each AHV CO node in the cluster separately.</p> <p>For more information about networking configuration of the AHV hosts, see <a href="#">Host Network Management</a>.</p> <p>Perform the networking tasks for each ESXi HCI node in the cluster individually.</p> <p>For more information on vSphere network configuration, see <a href="#">vSphere Networking</a> in the <i>vSphere Administration Guide for Acropolis</i>.</p>

### Best Practices for SO Nodes

Consider the following best practice recommendations if you plan to include storage-only (SO) nodes in your cluster.

- Nutanix recommends ensuring that your cluster has enough capacity to handle a SO node failure and to support rolling upgrades, during which SO nodes must be restarted.

**Important:**

To achieve optimal cluster resiliency, deploy SO nodes in a replication factor plus one configuration. For example, if the replication factor of your cluster is two, deploy at least three SO nodes. If the replication factor of your cluster is three, deploy at least four SO nodes.

The replication factor configuration is crucial if you plan to configure SO nodes with higher storage capacity than regular hyper-converged nodes.

For example, in a cluster with four HCI nodes, each with 4 TB capacity (total 16 TB), if you add high capacity SO nodes of 30 TB capacity, add replication factor plus one number of nodes.

Since the fault tolerance value is applicable to the cluster as a whole, this value determines the usage until fault tolerance is reached and the cluster can still rebuild the data.

For example, you have configured Resiliency Factor 3 with four storage heavy nodes (say, `node_1`, `node_2`, `node_3`, and `node_4`). Assume that the capacities of the remaining smaller nodes do not add up to same amount of

storage as the capacity of a single storage heavy node. In such a case, to accommodate the failure of two storage heavy nodes AOS needs to be able to place all of their data on the remaining two storage heavy nodes in a node fault tolerant system. If extent group egroup\_1 resides on node\_1, node\_2, and node\_3 then, in an event of failure of node\_1 and node\_2, egroup\_1 may be placed on node\_4 or one of the smaller nodes that has enough space. Therefore, consider the Fault Tolerance capacity that you get based on the static configuration and ensure that the usage is maintained below Fault Tolerance value. This ensures that data can be rebuilt in a fault tolerant manner even in the event of Fault Tolerance number of simultaneous failures.

The following table provides details of the number of SO nodes for cluster fault tolerance with replication factor and fault tolerance settings.

<b>Configured Cluster Fault Tolerance</b>	<b>Resulting Cassandra/Zookeeper replication factor</b>	<b>Recommended Compute Cluster Settings</b>	<b>Configured Replication Factor ( for containers with user data)</b>	<b>Permitted SO Nodes (Replication Factor + 1 minimum number of nodes to add)</b>	<b>Possible Fault Tolerance Level for different components(for the node failure domain)</b>
1N/1D	3	N+1	2	3	<p>1 - when a cluster is healthy (can tolerate single node failure)</p> <p>0 - when a cluster is not healthy (cannot tolerate node failure)</p>
2N/2D	5	N+2	2	3	<p>2 - when a cluster is healthy (can tolerate a simultaneous failure of two nodes)</p> <p>1 - when a cluster is not healthy (still can tolerate single node failure)</p> <p>0 - when a cluster is not healthy (cannot tolerate node failure)</p>

Configured Cluster Fault Tolerance	Resulting Cassandra/Zookeeper replication factor	Recommended Compute Cluster Settings	Configured Replication Factor (for containers with user data)	Permitted SO Nodes (Replication Factor + 1 minimum number of nodes to add)	Possible Fault Tolerance Level for different components(for the node failure domain)
			3	4	<p>2 - when a cluster is healthy (can tolerate a simultaneous failure of two nodes)</p> <p>1 - when a cluster is not healthy (still can tolerate single node failure)</p> <p>0 - when a cluster is not healthy (cannot tolerate node failure)</p>

- **Recommended Compute Cluster Settings** refers to the number of compute (HCI or CO) nodes in the cluster for a given fault tolerance. **Permitted SO Nodes** refers to the number of SO nodes required for the given number of compute nodes. For example, for the minimum fault tolerance level of 1 in the first row of the table above, the **Recommended Compute Cluster Settings** number is N+1, and the **Permitted SO Nodes** number is 3.
- Nutanix recommends that the SSD capacity of the node must be at least 10% of the HDD capacity of the node. For example, if your cluster has 20 TB HDD capacity, the SSD capacity of the node must be at least 2 TB.

This recommendation does not apply to all-flash clusters.

- Nutanix recommends that you configure all CVMs in the cluster with the same resources.
- Nutanix recommends that a cluster with all SO nodes, has at least 3 nodes.

Nutanix recommends that you deploy a minimum 3 SO nodes to ensure a healthy and active cluster and 2 CO nodes to maintain high availability in case of upgrade or any other maintenance activities on the CO node

The following table shows the supported and unsupported configurations for a cluster with SO nodes.

Configuration	Supported	Description
A four-node cluster with 4 TB capacity on each node.	X	If the only SO node in the cluster fails, the cluster does not have the sufficient capacity of 30 TB.
One large capacity SO node of 30 TB capacity.		<b>Resolution:</b> Add the minimum number of SO nodes equal to the replication factor of your cluster.

Configuration	Supported	Description
A four-node cluster with 4 TB capacity on each node.	X	Four nodes of 4 TB = 16 TB capacity, that is 8 TB for each replication copy. If the 14 TB storage node fails, the remaining four nodes cannot accommodate 14 TB of replication data because 14 TB is greater than the 8 TB needed for second replication copy.
One large capacity SO node of 14 TB capacity.		<b>Resolution:</b> The number of SO nodes that you add must be equal to the replication factor of the cluster.
A four-node cluster with 4 TB capacity on each node.	#	If one SO node fails, the other can handle the required capacity.
Two large capacity SO nodes of 30 TB capacity each.		
A four-node cluster with 4 TB capacity on each node.	#	The cluster is able to handle the failure of any node in the cluster, because all nodes in the cluster are of the same capacity.
One same-capacity SO node as the rest of the cluster.		
Nutanix cluster with 2 TB SSD capacity and 20 TB HDD capacity.	#	The total SSD capacity is minimum 10% of the total HDD capacity.
Nutanix cluster with 2 TB SSD capacity and 40 TB HDD capacity.	X	The total SSD capacity is not minimum 10% of the total HDD capacity.

# = Supported configuration

X = Unsupported configuration

## Deployment of Compute-Only Nodes

This section provides information about how to deploy compute-only (CO) nodes in a AHV cluster.

The CO node can be deployed in the following ways:

### New Node as CO Node

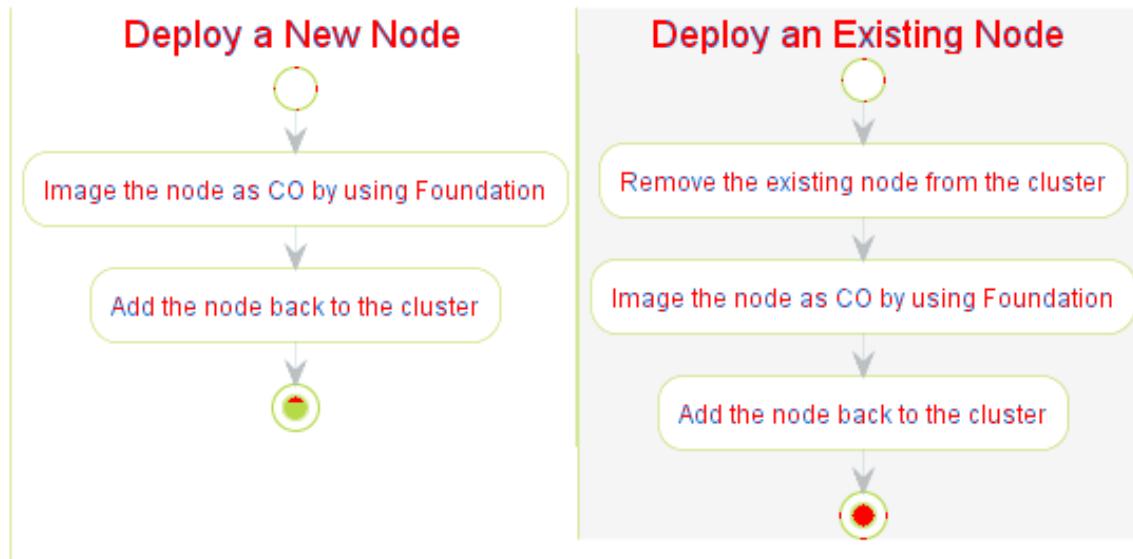
To add a new node as a CO node to the cluster, you must:

- Image the node as CO by using Foundation. For more information on how to image a node as a CO node, see the [Field Installation Guide](#).
- Add that node to the cluster by using the Prism Element web console. For more information, see [Adding an AHV Compute-Only Node to an AHV Cluster](#) on page 239 and [Adding an ESXi Compute-Only Node to an Optimized Database Solution Cluster](#) on page 247.

### Existing HCI Node as CO Node

To add an existing HCI node, that is already a part of the cluster, as a CO node to the cluster, you must:

- Remove that node from the cluster. For more information about how to remove a node, see [Cluster Modifications](#) on page 222.
- Image that node as CO by using Foundation.
- Add that node back to the cluster. For more information, see [Adding an AHV Compute-Only Node to an AHV Cluster](#) on page 239 and [Adding an ESXi Compute-Only Node to an Optimized Database Solution Cluster](#) on page 247.



**Figure 45:**

#### **Adding an AHV Compute-Only Node to an AHV Cluster**

This section provides information for adding an AHV compute-only (CO) node to an AHV cluster.

##### **Before you begin**

Ensure that you check the [Deployment Specifications and Considerations for Compute-Only and Storage-Only Nodes](#) on page 231 before you add a compute-only node to an AHV cluster.

##### **About this task**

To add a CO node to an AHV cluster, follow these steps:

##### **Procedure**

To add a CO node to an AHV cluster, perform the following steps:

1. Log in to the Prism Element web console.
2. From the dropdown menu, select **Hardware**.  
The system displays the **Hardware Overview** page.
3. Click **+ Expand Cluster**.  
The system displays the **Expand Cluster** dialog box.

4. Select **Expand Cluster** to expand the cluster with CO node.

**Note:** Do not select **Prepare Now and Expand Later**. This option is to only for preparing the nodes and expand the cluster at a later point in time. CO nodes do not support node preparation.

The system displays Compute only nodes cannot be prepared in the **Configure Host** tab error message, if you proceed with **Prepare Now and Expand Later** option:

5. In the **Select Host** tab, scroll down and, under **Manual Host Discovery**, click **Discover Hosts Manually**.
6. Click **Add Host**.
7. Under **Host or CVM IP**, type the IP address of the AHV host and click **Save**.

**Note:** The CO node does not have a Controller VM and you must therefore provide the IP address of the AHV host.

8. Click **Discover and Add Hosts**.

Prism Element discovers the CO node and the CO node appears in the list of nodes in the **Select Host** tab.

9. Select a CO node to view the node details, and click **Next**.  
The system displays the **Choose Node Type** tab.

10. Click **Next** in the **Choose Node Type** tab.  
The system prompts you to skip host networking.

11. Click **Skip Host Networking**.

The system prompts you to run checks and expand the cluster with the selected CO node.

12. In the **Configure Host** tab, select one of the following options:

- **Run Checks** - Used to only run pre-checks required for cluster expansion. Once all pre-checks are successful, you can click the **Expand Cluster** to add the CO node to the cluster.
- **Expand Cluster** - Used to run both; pre-checks required for cluster expansion and expand cluster operation together.

The add-node process begins, and Prism Element performs a set of checks before the node is added to the cluster. Once all checks are completed and the node is added successfully, the system displays the completion states for the tasks as 100%.

**Note:**

- You can check the progress of the operation in the **Tasks** menu of the Prism Element web console. The operation takes approximately five to seven minutes to complete.
- If you have not disabled the virtual switch as specified in [Prerequisites](#), the system displays multiple errors during cluster expansion.

13. Check the **Hardware Diagram** view to verify if the CO node is added to the cluster.

You can identify a node as a CO node if the Prism Element web console displays **N/A** in the **CVM IP** field.

## Deployment of Storage-only Nodes

You can image storage-only nodes when you create a cluster using Foundation. You can also expand your existing cluster to add a storage-only node.

- For information about imaging storage-only nodes when creating a cluster, see the [Field Installation Guide](#).
- For information on adding storage-only nodes to an existing cluster, see [Expanding a Cluster](#) on page 198.

## Optimized Database Solution

This section provides information about how to deploy compute-only (CO) nodes and storage-only (SO) nodes in an optimized database solution setup.

The optimized database solution provides a compartmentalized infrastructure for running databases. The compartmentalization separates the database instances and their storage, enables predictable performance, independent scalability, and isolated manageability for the database instances and their storage. It also provides dedicated resources within the Nutanix Cloud Infrastructure (NCI) cluster.

The optimized database solution uses the CO nodes and SO nodes features of NCI and Nutanix Database Service (NDB) in the following way:

- CO nodes are hosted with AHV or ESXi and no CVM
- SO nodes are hosted with AHV and CVM

In an optimized database solution cluster, the database instances are deployed on the guest VMs that are scheduled only on the CO nodes and not on the SO nodes. A different set of SO nodes serves the storage for the database instances in the cluster. NDB automates the provisioning of the storage on the SO nodes and maps them to the database instances on the CO nodes.

To preserve compartmentalization, the optimized database solution implements a fencing mechanism that prevents the guest VMs (including the guest VMs that host the database instances in the cluster) from being scheduled (automatically or manually) on SO nodes at any time. This fencing mechanism disables all the SO nodes in the cluster to host any guest VM at the time of the cluster creation. So, the database instances runs only on CO nodes and never on SO nodes.

The database software licensing on CO nodes and SO nodes is based on the end user licensing agreement of the database software vendor.

The optimized database solution can be deployed in the following two methods based on the hypervisor used on the CO nodes:

- AHV CO node with AHV SO node.
- ESXi CO node with AHV SO node.

**Note:** Starting with AOS 6.8, ESXi CO nodes support ESXi 8.0 and later versions.

**Note:** Nutanix does not support the following deployments:

- A combination of AHV CO and ESXi CO nodes within a cluster.
- ESXi SO nodes, or a combination of ESXi CO nodes and AHV HCI nodes.

An ESXi CO node allows you to seamlessly and efficiently expand the computing capacity (CPU and memory) of your AHV cluster. The Nutanix cluster uses the resources (CPUs and memory) of an ESXi CO node exclusively for computing purposes.

You can use a supported server or re-image an existing hyperconverged (HCI) node as an ESXi CO node.

To use a node as a CO node, image the node as a CO node using Foundation and then add that node to the cluster using the Prism Element web console. For more information on how to image a node as a CO node, see the [Field Installation Guide](#).

**Note:** If you want an existing HCI node that is already a part of the cluster to work as a CO node, remove that node from the cluster, image that node as a CO node by using Foundation, and add that node back to the cluster. For more information on how to remove a node, see [Modifying a Cluster](#).

## Operation Specifications for Optimized Database Solution

This section describes the operation specifications of compute-only (CO) and storage-only (SO) nodes in an optimized database solution setup.

**Table 52: Operation Specifications - Optimized Database Solution**

Component / Operation Type	Optimized Database Solution	
	AHV CO with AHV SO	ESXi CO with AHV SO
Storage source for vDisk/Volumes associated with guest VMs on the compute-only (CO) node	SO nodes in the cluster	
Controller VM (CVM) and local storage	No CVM and local storage on CO nodes	
VMs Management (CRUD operations, ADS, and HA) for CO node	Using Prism Element web console	
Hypervisor operation for CO node	Runs on the local storage media of the CO node	
Network segmentation support for CO node	Only for Controller VM backplane network and volume networks.	
Hypervisor and firmware upgrade for CO node	Using Life Cycle Manager (LCM). For more information, see the <a href="#">LCM Updates</a> topic in Life Cycle Manager Guide.	

## Cluster Requirements for Optimized Database Solution

This section provides information about the minimum cluster requirements for compute-only (CO) and storage-only (SO) nodes in an optimized database solution setup.

**Table 53: Minimum Cluster Requirements for Compute-Only Nodes and Storage-Only Nodes in Optimized Database Solution**

Cluster Attributes	Optimized Database Solution	
	AHV CO with AHV SO	ESXi CO with AHV SO
AOS Version for SO nodes	AOS 6.7 or later	AOS 6.6.2 or later
AHV Version for SO nodes	20230302.204 or later	Compatible AHV version based on AOS release
Number of nodes	Minimum 3 SO Nodes and minimum 2 CO nodes	

Cluster Attributes	Optimized Database Solution	
	AHV CO with AHV SO	ESXi CO with AHV SO
Nodes Ratio	<p>Nutanix recommends the following nodes ratio:</p> <ul style="list-style-type: none"> <li>• Even nodes - 1 CO : 1 SO</li> <li>• Odd Nodes - Recommended difference between CO and SO nodes is 1.</li> </ul> <p>However, you can deploy different combination of CO and SO nodes, provided the combinations comply with minimum 5 nodes and maximum 32 nodes in a cluster and meet your workload requirements.</p> <p><b>Note:</b> Use minimum 3 SO nodes to ensure a healthy and active cluster and minimum 2 CO nodes to maintain high availability in case of upgrade or any other maintenance activities on the CO node</p>	
Storage node Specification	All the SO nodes in the cluster must be NVMe nodes.	
CPU and memory assignment	No balancing required for the vCPU assignment between the CO and SO nodes as all the CPUs and memory are allocated to the SO node.	No balancing required for the vCPU assignment between the CO and SO nodes as all the CPUs and memory are allocated to the SO node.
Network Speed	Use dual 25 GbE or above on CO and AHV SO nodes.	Use dual 25 GbE or above on CO and AHV SO nodes.
Hypervisor specification	<ul style="list-style-type: none"> <li>• For SO node: AHV only</li> <li>• For CO node: AHV</li> </ul> <p>AHV CO node must run the same AHV version as the AHV SO nodes in the cluster.</p> <p>When you add an AHV CO node to the cluster, AOS checks if the AHV version of the node matches with the AHV version of the existing AHV nodes in the cluster. If there is a mismatch, the node addition fails.</p> <p>For general requirements about adding a node to a Nutanix cluster, see <a href="#">Expanding a Cluster</a>.</p>	<ul style="list-style-type: none"> <li>• For SO node: AHV only</li> <li>• For CO node: ESXi</li> </ul> <p>ESXi version of the ESXi compute-only nodes must be the same across the cluster. Nutanix supports the minimum ESXi version of 7.0 for ESXi CO node deployments in a Nutanix SO node cluster.</p> <p>When you add an ESXi CO node to the cluster, AOS checks if the ESXi version of the node matches with the ESXi version of the existing CO nodes in the cluster. If there is a mismatch, the node addition fails.</p> <p>For general requirements about adding a node to a Nutanix cluster, see <a href="#">Expanding a Cluster</a>.</p>
NIC Bandwidth	Uniform NIC bandwidth between CO and SO nodes.	

Cluster Attributes	Optimized Database Solution	
	AHV CO with AHV SO	ESXi CO with AHV SO
CPU	<p>For SO node:</p> <ul style="list-style-type: none"> <li>• Minimum 24 cores (12 cores per socket)</li> <li>• Minimum 2.5 GHz clock speed</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• 1: 1 mapping between Cores and vCPU for CVM</li> <li>• CVM picks all the cores minus 2 given to the SO node</li> </ul>	
	<p>For CO node:</p> <ul style="list-style-type: none"> <li>• Single socket: Minimum 8 cores per node/socket</li> <li>• Dual socket: Minimum 16 cores per node (8 cores per socket)</li> <li>• Minimum 2.5 GHz clock speed</li> </ul> <p><b>Note:</b> See the <a href="#">NDB Control Plane Configuration and Scalability</a> section of <i>Nutanix Database Service Administration Guide</i> to review the additional CPUs that may be used by NDB Agent VMs running on the Compute Only Nodes.</p>	
Memory	For SO node: Minimum 128 GB	
	For CO node: Based on customer requirements	
Drives	<p>For SO node: Minimum 8 drives, minimum 3.84 TB each Drives ( NVMe only)</p> <p>For CO node: The minimum number of drives differs based on the platforms. For example, the NX-G9 platforms can be shipped without any drives when used as compute-only nodes; however, for Dell platforms, there is a factory limitation of shipping with a minimum of 2 drives.</p>	
Socket	<p>For SO node: Dual socket</p> <p>For CO node: Single or dual socket</p>	
Host interface	<p>For SO node: iSCSI</p> <p>For CO node: iSCSI (boot and data drives)</p>	<p>For SO node: NFS, iSCSI</p> <p>For CO node: NFS (boot drive), iSCSI (data drives)</p>

## Licensing Requirements for Optimized Database Solution

This section provides information about the licensing requirements that apply to compute-only (CO) and storage-only (SO) nodes deployment in an optimized database solution setup.

**Table 54: Licensing Requirements for Optimized Database Solution**

Deployment Configuration		Licensing
Optimized Database Solution	AHV CO with AHV SO ESXi CO with AHV SO	Uses a combination of NCI Ultimate or NCI Pro licenses for AHV storage-only nodes and NDB Platform licenses for AHV compute-only nodes. Both NCI and NDB platforms are licensed on a per-core basis.  NCI Ultimate on storage-only AHV nodes is the preferred licensing model to get the most functional Optimized DB Solution. When you use the NCI Pro license on the storage-only AHV nodes, the entire cluster functions at the Pro level feature set, and the NDB disaster recovery feature and other advanced functionalities are not available.  For more information about NCI Ultimate and NDB feature set licenses, see <a href="#">Nutanix Cloud Platform Software Options</a> .
<b>Note:</b> The database instances can run only on CO nodes and not on SO nodes. The database software licensing on CO nodes and SO nodes is based on the end user licensing agreement of the database software vendor.		

## Configuration and Operation Limits for Optimized Database Solution

This section provides information about the configuration and operation limits that apply to compute-only and storage-only nodes deployment in an optimized database solution setup.

**Table 55: Configuration Limits - CO and SO Nodes Deployment**

Cluster Attributes	Optimized Database Solution	
	AHV CO with AHV SO	ESXi CO with AHV SO
Number of VMs	Up to 500	Up to 500
Number of Nodes	Up to 32	Up to 32
Addition of HCI Node	Not supported	Not supported
Rolling Restart	Supported	Supported
RDMA	Not supported	Not supported
Host boot disk replacement for CO nodes	Not supported	Not supported
Virtual Switch configuration	Supported	Supported
Network segmentation for disaster recovery	Supported on SO node	Not supported

Cluster Attributes	Optimized Database Solution	
	AHV CO with AHV SO	ESXi CO with AHV SO
Automatic discovery of CO nodes as part of <i>Expand cluster</i> workflow (see <a href="#">Expanding a Cluster</a> )	Not supported  Initiate the manual host discovery workflow to add compute-only node when you use the <a href="#">Expanding a Cluster</a> workflow.	Not supported  Initiate the manual host discovery workflow to add compute-only node when you use the <a href="#">Expanding a Cluster</a> workflow.
Cluster Conversion	Not supported	Not supported

## Supported Hardware Platforms for Optimized Database Solution

This section provides information about the supported hardware platforms for compute-only (CO) and storage-only (SO) nodes deployment in an optimized database solution setup.

**Table 56: Supported Hardware Platforms - Optimized Database Solution**

Optimized Database Solution	Supported Hardware Platforms
AHV CO with AHV SO	
ESXi CO with AHV SO	<ul style="list-style-type: none"> <li>For SO node: NX8170-G8, NX-8170-G9, NX-8155-G9, NX-8150-G9, Dell XC650-10N, Dell XC750-16N, Dell XC660-12N, and Dell XC760-24N</li> <li>For CO node: NX8170-G8, NX1175S-G8, NX-8170-G9, NX-1175S-G9, NX-8155-G9, NX-8150-G9, NX-9151-G9, Dell XC650-10N, Dell XC750-16N, Dell XC660xs-4S, Dell XC660-12N, and Dell XC760-24N</li> </ul>
<p><b>Note:</b> In case of any queries regarding the supported hardware models, contact Nutanix Support.</p>	

## Networking Configurations for Compute-Only Nodes in Optimized Database Solution

This section provides information about how to perform the networking configurations for compute-only nodes based on the deployment configuration in an optimized database solution setup.

**Table 57: Networking Configurations for Compute-Only Nodes in Optimized Database Solution**

Optimized Database Solution	Method to perform networking configurations
AHV CO with AHV SO	<p>Use the <code>manage_ovs</code> commands and add the <code>--host</code> flag to the <code>manage_ovs</code> commands.</p> <p>For example, to create or modify the bridges or uplink bonds or uplink load balancing, run the following command:</p> <pre>nutanix@cvm\$ manage_ovs --host IP_address_of_co_node --bridge_name bridge_name create_single_bridge</pre> <p>Replace <code>IP_address_of_co_node</code> with the IP address of the CO node and <code>bridge_name</code> with the name of bridge you want to create.</p> <p><b>Note:</b> Run the <code>manage_ovs</code> commands for an AHV CO node from any Controller VM running on an AHV SO node.</p> <p>Perform the networking tasks for each AHV CO node in the cluster separately.</p> <p>For more information about networking configuration of the AHV hosts, see <a href="#">Host Network Management</a>.</p>
ESXi CO with AHV SO	<p>Perform the networking tasks for each ESXi CO node in the cluster individually.</p> <p>For more information on vSphere network configuration, see <a href="#">vSphere Networking</a> in the <i>vSphere Administration Guide for Acropolis</i>.</p>

## Deployment of Compute-Only and Storage-Only nodes in Optimized Database Solution

This section describes how to deploy compute-only and storage-only nodes in an optimized database solution setup.

For information on how to deploy AHV compute-only node in an optimized database solution, see [Adding an AHV Compute-Only Node to an AHV Cluster](#) on page 239.

For information on how to deploy ESXi compute-only node in an optimized database solution, see [Adding an ESXi Compute-Only Node to an Optimized Database Solution Cluster](#) on page 247.

For information on how to deploy storage-only nodes in an optimized database solution, see [Deployment of Storage-only Nodes](#) on page 240.

### Adding an ESXi Compute-Only Node to an Optimized Database Solution Cluster

This section provides information for adding an ESXi compute-only (CO) node to an optimized database solution cluster

#### Before you begin

Check the [Cluster Requirements for Optimized Database Solution](#) on page 242.

#### About this task

To add an ESXi compute-only node to an optimized database solution cluster setup with ESXi compute-only and AHV storage-only nodes.

#### Procedure

1. Log in to the Prism Element web console.

2. From the dropdown menu, select **Hardware**.  
The system displays the **Hardware Overview** page.
3. Click **+ Expand Cluster**.  
The system displays the **Expand Cluster** dialog box.
4. Select **Expand Cluster** to expand the cluster with CO node.

**Note:** Do not select **Prepare Now and Expand Later**. This option is to only for preparing the nodes and expand the cluster at a later point in time. CO nodes do not support node preparation.

The system displays Compute only nodes cannot be prepared in the **Configure Host** tab error message, if you proceed with **Prepare Now and Expand Later** option:

5. In the **Select Host** screen, scroll down and, under **Manual Host Discovery**, click **Discover Hosts Manually**.
6. Click **Add Host**.
7. Under **Host or CVM IP**, type the IP address of the ESXi CO node and click **Save**.  
This node does not have a Controller VM and you must therefore provide the IP address of the ESXI CO node.
8. Click **Discover and Add Hosts**.  
Prism Element discovers this node and the node appears in the list of nodes in the **Select Host** screen.
9. Select the node to display the details of the compute-only node.
10. Click **Next**.
11. In the **Configure Host** screen, click **Expand Cluster**.  
The add node process begins and Prism Element performs a set of checks before the node is added to the cluster.  
Check the progress of the operation in the **Tasks** menu of the Prism Element web console. The operation takes approximately five to seven minutes to complete.
12. Check the **Hardware Diagram** view to verify if the node is added to the cluster.  
You can identify a node as a CO node if the Prism Element web console does not display the IP address for the Controller VM.

# NUTANIX VOLUMES

---

Nutanix Volumes acts as one or more targets for client Windows or Linux operating systems running on a bare metal server or as guest VMs using iSCSI initiators. You can use storage from any new or existing Nutanix cluster for Volumes.

For more information, see the [Nutanix Volumes Guide](#). For best practice information, see [Nutanix Volumes Solutions Documentation](#).

# FILE SERVER MANAGEMENT

---

Nutanix Files enables files sharing across user workstations in a centralized and secure location eliminating the need for a third-party file server. The **File Server** dashboard displays real time information about the file servers and shares/exports in a cluster. For more information, see the [Nutanix Files Guide](#).

# DATA PROTECTION

---

Nutanix offers data protection solutions for virtual datacenters. Nutanix provides data protection functions at the VM, file, and volume group level, ensuring VMs and data remain safe in a crash-consistent environment.

**Note:** For more information about the data protection solutions available from Nutanix, see [Nutanix DR Solutions Workflow](#) in the *Data Protection and Recovery with Prism Element Guide*.

- Nutanix supports several types of protection strategies including one-to-one or one-to-many replication. For more information, see [Protection Strategies](#) in the *Data Protection and Recovery with Prism Element Guide*.
- Nutanix supports configuring asynchronous replication. For more information, see [Data Protection with Asynchronous Replication \(One-hour or Greater RPO\)](#) in the *Data Protection and Recovery with Prism Element Guide*.
- The Cloud Connect feature gives you the option to asynchronously back up data on the Amazon Web Service (AWS) cloud. For more information, see [Asynchronous Replication With Cloud Connect \(On-Premises To Cloud\)](#) in the *Data Protection and Recovery with Prism Element Guide*.
- Nutanix supports configuring synchronous replication. There are two options:
  - For environments that support metro availability, you can configure a metro availability protection domain. For more information, see [Metro Availability \(ESXi and Hyper-V 2016\)](#) in the *Data Protection and Recovery with Prism Element Guide*.
  - For other environments, you can configure synchronous replication. For more information, see [Synchronous Replication \(ESXi and Hyper-V 2012\)](#) in the *Data Protection and Recovery with Prism Element Guide*.

# HEALTH MONITORING

---

Nutanix provides a range of status checks to monitor the health of a cluster.

- Summary health status information for VMs, hosts, and disks appears on the home dashboard. For more information, see [Home Dashboard](#) on page 62.
- In depth health status information for VMs, hosts, and disks is available through the Health dashboard. For more information, see [Health Dashboard](#) on page 252.
- You can customize the frequency of the scheduled health checks and how frequently to run them. For more information, see [Configuring Health Checks](#) on page 255.
- You can run NCC health checks directly from the Prism. For more information, see [Running Checks by Using Prism Element Web Console](#) on page 257.
- You can collect logs for all the nodes and components. For more information, see [Collecting Logs by Using Prism Element Web Console](#) on page 257.
- For a description of each available health check. For more information, see [Alerts/Health checks](#).

**Note:** If the Cluster Health service status is DOWN for more than 15 minutes, an alert email is sent by the AOS cluster to configured addresses and Nutanix support (if selected). In this case, no alert is generated in the Prism Element web console. The email is sent once per 24 hours. You can run the NCC check cluster\_services\_down\_check to see the service status.

## Health Dashboard

The Health dashboard displays dynamically updated health information about VMs, hosts, and disks in the cluster. To view the Health dashboard, select **Health** from the pull-down list on the left of the main menu.

### Menu Options

The Health dashboard does not include menu options other than those available from the main menu.

**Note:** When you first visit the Health dashboard, a tutorial opens that takes you through a guided tour of the health analysis features. Read the message and then click the **Next** button in the text box to continue the tutorial (or click the **X** in the upper right to close the text box and end the tutorial.) You can view this tutorial at any time by selecting the **Health Tutorial** option in the user menu. For more information, see [Main Menu](#) on page 56.

### Screen Details

The Health dashboard is divided into three columns:

- The left column displays tabs for each entity type (VMs, hosts, disks, storage pools, storage containers, cluster services, and [when configured] protection domains and remote sites). Each tab displays the entity total for the cluster (such as the total number of disks) and the number in each health state. Clicking a tab expands the displayed information (see following section).
- The middle column displays more detailed information about whatever is selected in the left column.

- The right column displays summary of all the health checks. You also have an option to view individual checks from the **Checks** button (success, warning, failure, or disabled).
- The **Summary** tab provides summarized view of all the health checks according to check status and check type.
- The **Checks** tab provides information about individual checks. Hovering the cursor over an entry displays more information about that health check. You can filter the checks by clicking appropriate field type and clicking **Apply**. The checks are categorized as follows.

**Filter by Status**

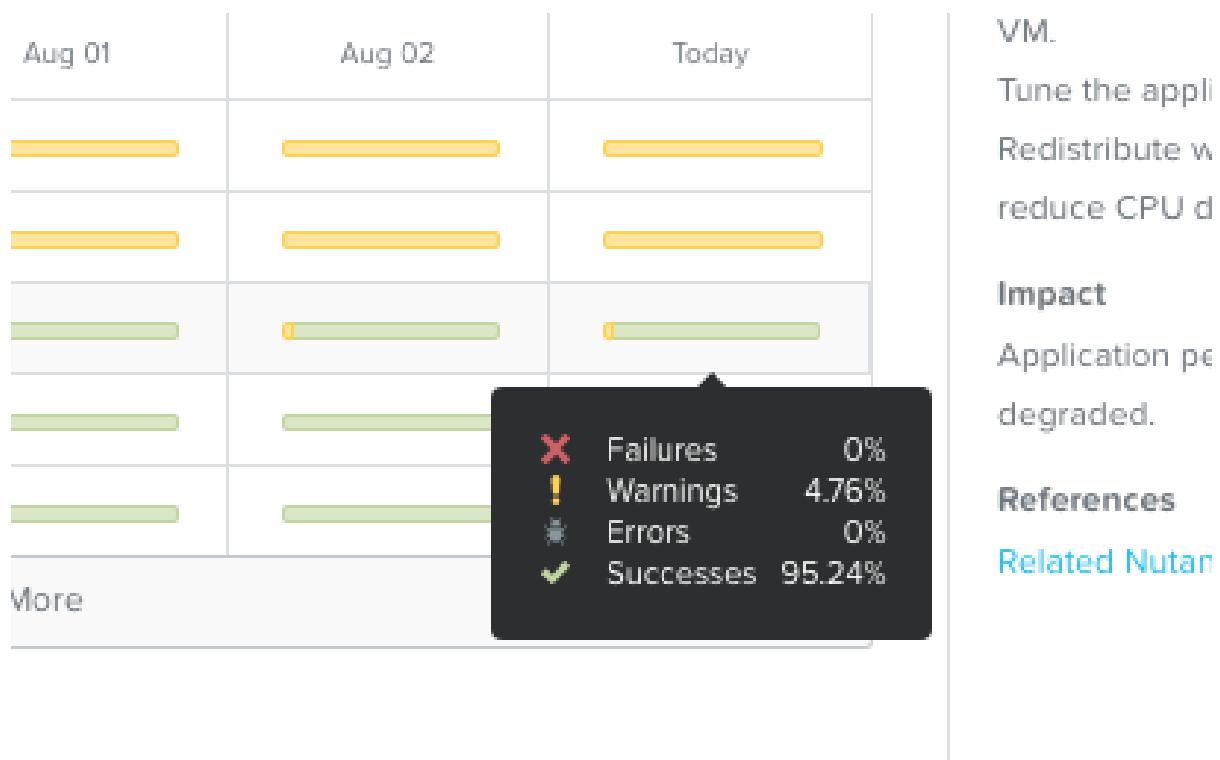
Passed, Failed, Warning, Error, Off, or All

**Filter by Type**

Scheduled, Not Scheduled, Event Triggered, or All

**Filter by Entity Type**

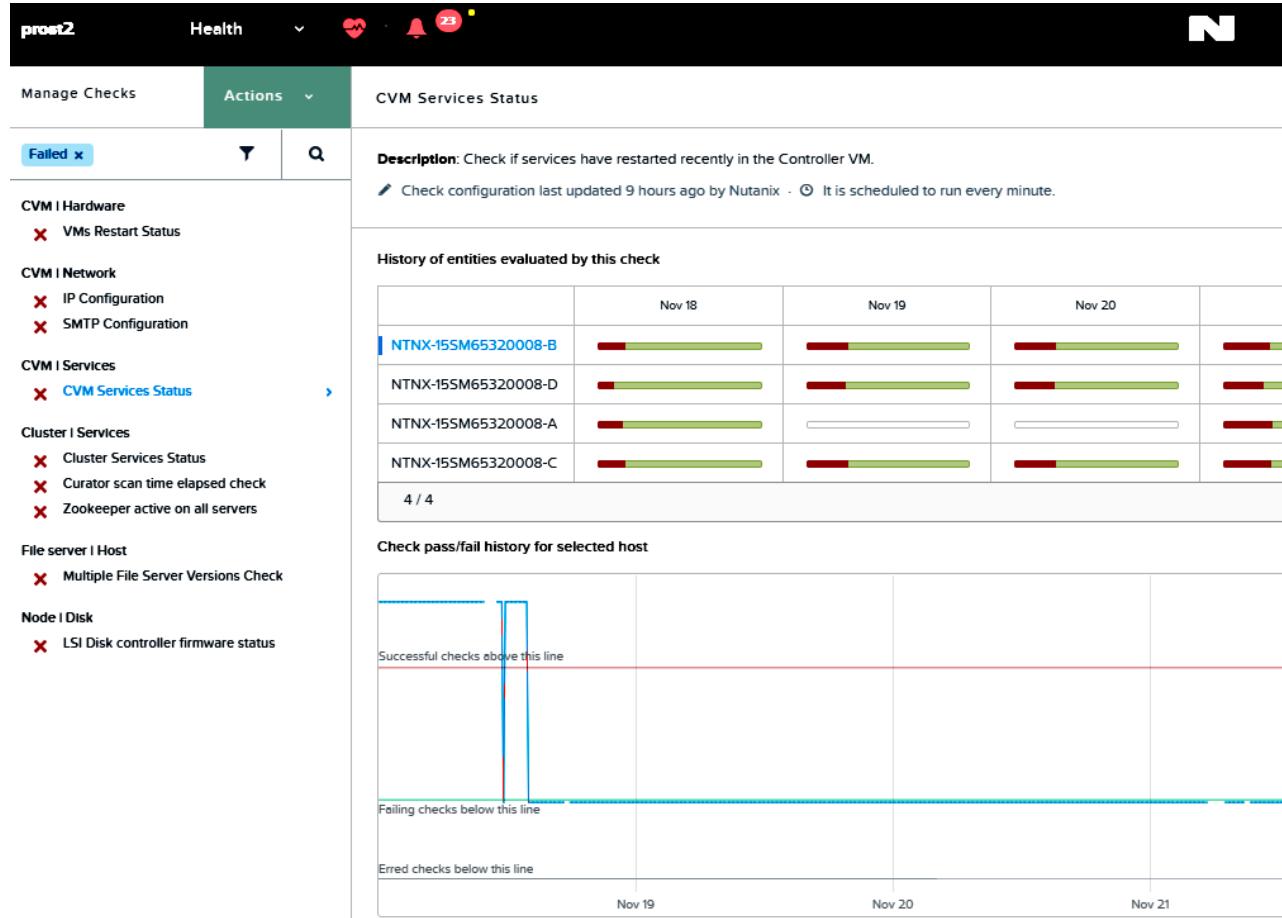
VM, Host, Disk, Storage Pool, Storage Container, Cluster Service, or All



**Figure 46: Hover Information**

For example, if you want to see only the failed checks, filter the checks by selecting the **Failed** option. If you click on the specific check, the middle column will provide the detailed history of when the checks failed and what is the percentage of the check failure. If you click the bar, a detailed graph of the pass and fail history is

displayed (as shown below). Hovering the mouse along the graph line displays information about that point in time.



**Figure 47: Filter Categorization**

**Note:** For the checks with status as error, follow the similar process as described above to get detailed information about the errors.

You can also search for specific checks by clicking the health search icon and then entering a string in the search box.

- The **Actions** tab provides you with an option to manage checks, run checks, and collect logs.

### Focus and Filtering Options

The Health dashboard allows you to display entity health information through various views. Clicking a left column tab expands that tab to display grouping categories for that entity type (VMs, hosts, or disks). The middle section also expands with additional detail. The **Checks** tab of the right column displays the health checks that are relevant for that entity type.

Clicking on a grouping category displays detailed information about that grouping:

- The left column expands to display a set of grouping and filter options. The selected grouping is highlighted. You can select a different grouping by clicking on that grouping. Each grouping entry lists how many categories are in that grouping, and the middle section displays information about those categories. In the following example, the disks storage tier is selected, and there are two categories (SSD and HDD) in that grouping. By default, all entities

(in this example, all disks) are included in the category information. You can narrow the included list by clicking one or more of the filters.

- The middle column displays a field for each category in the selected grouping. Each field provides details about that category. You can see additional information by hovering the cursor over a specific entry. There is a drop-down select list for filtering (same as the grouping filters) and a drop-down sort by list for ordering the information.
- The right column continues to display the health checks that are relevant for that entity type.

The middle column provides two viewing options: a diagram view and a table view. The table view provides more detailed information in tabular form. You can sort the entries by clicking a column header.

The middle column also includes watch list information at the top (*Currently watching xx entities* or *Currently watching x / xx total entity\_type*). The Health dashboard is dynamically adjusted to reflect information about the entities in the current watch list. In this example, all disks are currently selected for the watch list (*Currently watching 18 / 18 total disks*), so the status information (middle column) and relevant health checks (right column) reflect the 18 disks. When you change the watch list to a subset of the current entity type (such as a single disk) or a different entity type (such as hosts), the status information and relevant health checks are customized accordingly for the new watch list.

## Configuring Health Checks

A set of health checks are run regularly that provide a range of clusters health indicators. You can specify which checks to run and configure the schedulable checks and other parameters for each health check.

### About this task

The cluster health checks cover a range of entities including AOS, hypervisor, and hardware components. A set of checks are enabled by default, but you can run, disable, or reconfigure any of the checks at any time. To reconfigure one or more health checks, do the following:

### Procedure

1. Log on to the Prism Element web console.
2. In the Health dashboard, click **Actions > Manage Checks**.  
The Health dashboard redisplays with information about the health checks. If you clicked on a specific health check, that check is highlighted. Either you are prompted to select a health check (first time) or the previously selected health check is highlighted.
3. Select a check.
  - a. The left column lists the health checks with the selected check highlighted. Click any of the entries to select and highlight that health check.
  - b. The middle column describes what this health check does, and it provides the run schedule and history across affected entities (hosts, disks, or VMs).
  - c. The right column describes what failing this health check means (cause, resolution, and impact).
4. To run a particular check, click **Run Check**.
5. To turn off (or turn on) a health check, click the **Turn Check Off** (or **Turn Check On**) link at the top of the middle column and then click the **Yes** button in the dialog box.

6. To change the alert policy for those health checks that have a configurable policy, click Alert Policy at the top of the middle column, change one or more of the parameter values in the drop-down window, and then click **Save**.

- a. Depending on the alert condition (**Info**, **Critical**, and so on), unselect the condition to disable these alert condition messages.

All the alerts are enabled by default (box checked). In most cases this field includes just a single box with the word Critical, Warning, or Info indicating the severity level. Checking the box means this event will trigger an alert of that severity. Unchecking the box means an alert will not be issued when the event occurs. In some cases, such as in the example figure about disk space usage, the event can trigger two alerts, a warning alert when one threshold is reached (in this example 90%) and a critical alert when a second threshold is reached (95%). In these cases you can specify whether the alert should be triggered (check/uncheck the box) and at what threshold (enter a percentage in the box).

- b. **Auto Resolve These Alerts:** Uncheck (or check) the box to disable (or re-enable) automatic alert resolution.

Automatic alert resolution is enabled for all alert types (where applicable) by default. When this is enabled, the system will automatically resolve alerts under certain conditions such as when the system recognizes that the error has been resolved or when the initiating event has not reoccurred for 48 hours. (Automatic resolution is not allowed for some alert types, and this is noted in the policy window for those types.)

7. To change a parameter setting for those health checks that have configurable parameters, click the **Parameters** link at the top of the middle column, change one or more of the parameter values in the drop-down window, and then click the **Update** button.

This link appears only when the health check includes configurable parameters. The configurable parameters are specific to that health check. For example, the *CPU Utilization* health check includes parameters to specify the host average CPU utilization threshold percentage and host peak CPU utilization threshold percentage.

8. To change the schedule for running a health check, select an interval from the **Schedule** drop-down list for the schedulable checks at the top of the middle column.

Each check has a default interval, which varies from as short as once a minute to as long as once a day depending on the health check. The default intervals are optimal in most cases, and changing the interval is not recommended (unless requested to do so by Nutanix customer support).

## Configuring NCC Frequency

Perform the following procedure to configure NCC to run automatically after the specified period of time from Prism.

### Procedure

1. Log on to the Prism Element web console.
2. In the Health dashboard, from the **Actions** drop-down menu select **Set NCC Frequency**.

3. Select the configuration schedule.
  - » **Every 4 hours:** Select this option to run the NCC checks at four hours interval.
  - » **Every Day:** Select this option to run the NCC checks on a daily basis.  
Select the time of the day when you want to run the checks from **Start Time** field.
  - » **Every Week:** Select this option to run the NCC checks on a weekly basis.  
Select the day and time of the week when you want to run the checks from the **On** and **Start Time** fields. For example, if you select Sunday and Monday from the **On** field and select 3:00 p.m. from the **Start Time** field, every Sunday and Monday at 3 p.m. the NCC checks are run automatically.

The Email address that you have configured by using alert emails is also displayed. A report will be sent as an email to all the recipients. For more information on how to configure alert emails, see [Configuring Alert Emails](#) in *Prism Element Alerts and Events Reference Guide*.

4. Click **Save**.

## Running Checks by Using Prism Element Web Console

You can now run the NCC checks from the **Health** dashboard of the Prism Element web console. You can select to run all the checks at once, the checks that have failed or displayed some warning, or even specific checks of your choice.

### About this task

**Note:** If you are running checks by using Prism Element web console, you will not be able to collect the logs at the same time.

### Procedure

1. In the Health dashboard, from the **Actions** drop-down menu select **Run NCC Checks**.
2. Select the checks that you want to run for the cluster.
  - a. **All checks:** Select this option to run all the checks at once.
  - b. **Only Failed and Warning Checks:** Select this option to run only the checks that were failed or gave warning during the health check runs.
  - c. **Specific Checks:** Select this option and type the check or checks name in the text box that appears that you want to run.  
This field gets auto-populated once you start typing the name of the check. All the checks that you have selected for this run are listed in the **Added Checks** box.
3. Select the **Send the cluster check report in the email** option to receive the report after the cluster check. To receive the email configuration ensure that you have configured email configuration for alerts. For more information, see [Configuring Alert Emails](#) in *Prism Element Alerts and Events Reference Guide*.  
The status of the run (succeeded or aborted) is available in the **Tasks** dashboard. By default, all the event triggered checks are passed. Also, the **Summary** page of the **Health** dashboard will be updated with the status according to health check runs.

## Collecting Logs by Using Prism Element Web Console

You can collect logs for Controller VMs, file server, hardware, alerts, hypervisor, and for the system. After the task finishes, the log bundle is available for download purpose from the **Tasks** dashboard.

## About this task

Log bundle includes logs and configuration information from one or more Controller VMs, configuration information for hypervisors, and information about alerts and so on. To collect the logs and download the log bundle, perform the following procedure.

### Note:

- While this method works, the preferred method for collecting logs is through a CLI tool called logbay. For more information about logbay, see the [Nutanix Cluster Check \(NCC\) Guide](#).
- The timestamps for all Nutanix service logs are moved to UTC (in ISO 8601:2020-01-01 T00:00:00Z) from Prism version 5.18.
- All operating system logs will not be moved to UTC, hence Nutanix recommends that you set the server local time to UTC.

## Procedure

1. Log on to the Prism Element web console.
2. In the **Health** dashboard, from the **Actions** drop-down menu, select **Collect Logs**.
3. In **Node Selection**, click **+ Select Nodes**. Select the nodes for which you want to collect the logs and click **Done**.
4. Click **Next**.
5. In **Log Settings**, select one of the following:
  - » **All**. Select this option if you want to collect the logs for all the tags.
  - » **Specific (by tags)**. Select this option, click **+ Select Tags** if you want to collect the logs only for the selected tags and then click **Done**.
6. In **Output Preferences**, do the following in the indicated fields.
  - 1. **Select Duration**. Select the duration for which you want to collect the logs. You can collect the logs either in hours or days. Click the drop-down list to select the required option.
  - 2. **Cluster Date**. Select the date from which you want to start the log collection operation. Click the drop-down list to select either **Before** or **After** to collect logs before or after a selected date.
  - 3. **Cluster Time**. Select the time from when you want to start the log collection operation.
  - 4. **Select Destination for the collected logs**. Click the drop-down list to select the server where you want the logs to be collected.
    - **Download Locally**
    - **Nutanix Support FTP**. If you select this option, enter the case number in the **Case Number** field.
    - **Nutanix Support SFTP**. If you select this option, enter the case number in the **Case Number** field.
    - **Custom Server**. Enter server name, port, username, password, and archive path if you select this option.
  - 5. **Anonymize Output**. Select this checkbox if you want to mask all the sensitive information like the IP addresses.
7. To start the operation, click **Collect**.

8. After the operation completes, you can download the log bundle for the last two runs and (as needed) add it to a support case as follows:
  - a. Go to the **Task** dashboard, find the log bundle task entry, and click the **Succeeded** link for that task (in the Status column) to download the log bundle. For more information, see [View Task Status](#) on page 87.

**Note:** If a pop-up blocker in your browser stops the download, turn off the pop-up blocker and try again.
  - b. Log in to the support portal, click on the target case in the **360 View** widget on the dashboard (or click the **Create a New Case** button to create a new case), and upload the log bundle to the case (click the **Choose Files** button in the **Attach Files** section to select the file to upload).

# VIRTUAL MACHINE MANAGEMENT

Each node in a cluster includes local storage (flash and hard disk), a Controller VM, a hypervisor, and any number of host VMs running on that hypervisor.

- The web console allows you to monitor status of the VMs across the cluster. For more information, see [VM Dashboard](#) on page 260.
- In Acropolis managed clusters, the web console also allows you to do the following:
  - Create VMs. For more information, see [Creating a VM \(AHV\)](#) on page 270.
  - Manage VMs. For more information, see [Managing a VM \(AHV\)](#) on page 276.
  - Enable VM high availability. For more information, see [Enabling High Availability Reservations for the Cluster](#) on page 301.
  - Configure network connections. For more information, see [Network Configuration for VM Interfaces](#) on page 162.
- You can create and manage VMs directly from Prism Element when the hypervisor is ESXi.
  - Create VMs. For more information, see [Creating a VM \(ESXi\)](#) on page 286.
  - Manage VMs. For more information, see [Managing a VM \(ESXi\)](#) on page 288.

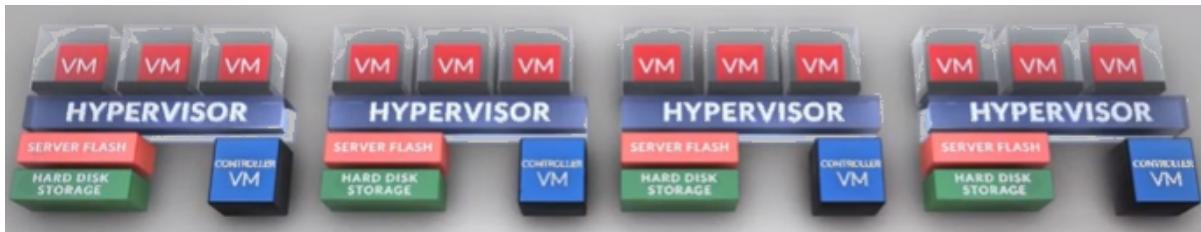


Figure 48: Node Architecture

## VM Dashboard

The virtual machine (VM) dashboard displays dynamically updated information about virtual machines in the cluster. To view the VM dashboard, select **VM** from the pull-down list on the left of the main menu.

### Menu Options

In addition to the main menu, the VM screen includes a menu bar with the following options:

- *View selector.* Click the **Overview** button on the left to display the VM dashboard. For more information, see [VM Overview View](#) on page 261. Click the **Table** button to display VM information in a tabular form. For more information, see [VM Table View](#) on page 262.
- *Action buttons.* Click the **Create VM** button on the right to create a virtual machine. For more information, see [Creating a VM \(AHV\)](#) on page 270. Click the **Network Config** button to configure a network connection. For more information, see [Network Configuration for VM Interfaces](#) on page 162.

**Note:** The action buttons appear only in Acropolis managed clusters.

- *CVM filter.* In the Table view, the Controller VMs are not listed by default. To include them in the table list, check the **Include Controller VMs** box.
- *Page selector.* In the Table view, VMs are listed 10 per page. When there are more than 10 VMs, left and right paging arrows appear on the right, along with the total VM count and the VM numbers for the current page.
- *Export VM information.* In the Table view, you can export the table containing the list of VMs and their information to a file in either CSV or JSON format by clicking the gear icon  on the right and selecting either **Export CSV** or **Export JSON** from the drop-down menu. (The browser must allow a dialog box for export to work.) Chrome, Internet Explorer, and Firefox download the data into a file; Safari opens the data in the current window.
- *Search box.* In the Table view, you can search for entries in the table by entering a search string in the box.

## VM Overview View

The VM Overview view displays VM-specific performance and usage statistics on the left plus the most recent VM-specific alert and event messages on the right.

The following table describes each field in the VM Overview view. Several fields include a slide bar on the right to view additional information in that field. The displayed information is dynamically updated to remain current.

**Note:** For information about how the statistics are derived, see [Understanding Displayed Statistics](#) on page 69.

**Table 58: VM Overview View Fields**

Name	Description
Hypervisor Summary	Displays the name and version number of the hypervisor.
VM Summary	Displays the total number of VMs in the cluster broken down by on, off, and suspended states.
CPU	Displays the total number of provisioned virtual CPUs and the total amount of reserved CPU capacity in GHz for the VMs.
Memory	Displays the total amount of provisioned and reserved memory in GBs for the VMs.
Top User VMs by Controller IOPS	Displays I/O operations per VM for the 10 most active VMs.
Top User VMs by Controller IO Latency	Displays I/O bandwidth used per VM for the 10 most active VMs. The value is displayed in an appropriate metric (MBps, KBps, and so on) depending on traffic volume.
Top User VMs by Memory Usage	Displays the percentage of reserved memory capacity used per VM for the 10 most active VMs.
Top User VMs by CPU Usage	Displays the percentage of reserved CPU capacity used per VM for the 10 most active VMs.
VM Critical Alerts	Displays the five most recent unresolved VM-specific critical alert messages. Click a message to open the Alert screen at that message. You can also open the Alert screen by clicking the <i>view all alerts</i> button at the bottom of the list. For more information, see <a href="#">Alerts Dashboard</a> in <i>Prism Element Alerts and Events Reference Guide</i> .

Name	Description
VM Warning Alerts	Displays the five most recent unresolved VM-specific warning alert messages. Click a message to open the Alert screen at that message. You can also open the Alert screen by clicking the <i>view all alerts</i> button at the bottom of the list.
VM Events	Displays the ten most recent VM-specific event messages. Click a message to open the Event screen at that message. You can also open the Event screen by clicking the <i>view all events</i> button at the bottom of the list.

## VM Table View

The VM Table view displays information about each VM in a tabular form. The displayed information is dynamically updated to remain current. In Acropolis managed clusters, you can both monitor and manage VMs through the VM Table view.

### Table View Fields

The VM Table view is divided into two sections:

- The top section is a table. Each row represents a single VM and includes basic information about that VM. Click a column header to order the rows by that column value (alphabetically or numerically as appropriate).
- The bottom **Summary** section provides additional information. It includes a summary or details column on the left and a set of tabs on the right. The details column and tab content varies depending on what has been selected.

The following table describes each field in the table portion of the view. The details portion and tab contents are described in the subsequent sections.

**Note:** For information about how the statistics are derived, see [Understanding Displayed Statistics](#) on page 69. VirtIO must be installed in a VM for AHV to display correct VM memory statistics. For more information about VirtIO drivers, see [Nutanix VirtIO for Windows](#) in *AHV Administration Guide*.

**Table 59: VM Table View: Table Fields**

Parameter	Description	Values
VM Name	Displays the name given to the VM.	(VM name)
ID	Displays the UUID of the VM.	(VM UUID)
Host	Displays the name of the host.	(Host name)
IP Addresses	Displays the IP address assigned to the VM.	(IP address)
Cores	Displays the number of CPU cores being used by the VM.	(number)
Memory Capacity	Displays the total amount of memory available to the VM.	xxx [MB   GB]
Storage	Displays the used capacity (utilised capacity of the VM disk(s)) in relation to the total capacity (the total storage capacity of all the disks provisioned to the VM). For example, 1.9 GiB/ 5 GiB.	xxx / xxx [MiB   GiB]

Parameter	Description	Values
CPU Usage	Displays the percentage of allocated CPU capacity currently being used by the VM.	0 - 100%
Memory Usage	Displays the percentage of allocated memory capacity currently being used by the VM.	0 - 100%
[Controller] Read IOPS	Displays read I/O operations per second (IOPS) for the VM.	(number)
	<p><b>Note:</b> In this and the following three fields, the column name includes the word <i>Controller</i> if the information comes from the Controller VM instead of the hypervisor. For ESXi, the information comes from the hypervisor; for Hyper-V and AHV, the information comes from the Controller VM.</p>	
[Controller] Write IOPS	Displays write I/O operations per second for the VM.	(number)
[Controller] IO Bandwidth	Displays I/O bandwidth used per second by the VM.	xxx [MBps KBps]
[Controller] Avg IO Latency	Displays the average I/O latency of the VM.	xxx [ms]
Backup and Recovery Capable	Indicates (Yes or No) whether the VM can be protected (create backup snapshots) and recovered if needed. When the value is No, click the question mark icon for an explanation.	[Yes No]
Flash Mode	Displays whether flash mode feature is enabled or not for the VM.	[Yes No]

### VM Detail Information

When a VM is selected in the table, information about that VM appears in the lower part of the screen.

- **Summary:** `vm_name` appears below the table and **VM Details** fields appear in the lower left column. The following table describes the fields in this column.

- For VMs in Acropolis managed clusters, action links appear on the right of the **Summary: vm\_name** line. For more information about these actions, see [Managing a VM \(AHV\)](#) on page 276.

- Click **Manage NGT** to enable and mount Nutanix guest tools for this VM.
- Click the **Launch Console** link to open a console window for this VM.
- Click the **Power on** (or **Power Off Actions**) link to start (or shut down) this VM.
- Click the **Take Snapshot** link to create a backup snapshot on demand.
- Click the **Migrate** link to migrate the VM onto a different host.
- Click the **Pause** (or **Resume**) link to pause (or resume) this VM.

**Note:** VM pause and resume feature is not supported on AHV.

- Click the **Clone** link to clone a copy of the VM.
- Click the **Update** link to update the VM configuration.
- Click the **Delete** link to delete the VM. (A VM must be powered off before it can be deleted.)

**Note:** If the VM is a Prism Central VM, all Actions except **Launch Console**, **Take Snapshot**, and **Migrate** are disabled as a protective measure.

- A set of tabs appear to the right of the details section that display information about the selected VM. The set of tabs varies depending on whether the VM is an Acropolis managed VM or not. The following sections describe each tab.
  - Standard VM tabs: **VM Performance**, **Virtual Disks**, **VM NICs**, **VM Alerts**, **VM Events**, **I/O Metrics**, and **Console**.
  - Acropolis managed VM tabs: **VM Performance**, **Virtual Disks**, **VM NICs**, **VM Snapshots**, **VM Tasks**, **I/O Metrics**, and **Console**.

**Table 60: VM Detail Fields**

Parameter	Description	Values
Name	Displays the name given the VM.	(VM name)
Host	Displays the host name on which this VM is running.	(IP address)
Host IP	Displays the host IP address for this VM.	(IP address)
Guest OS	Displays the operating system running on this VM, such as Windows 7 or Ubuntu Linux. (This information is not available when running AHV.)	(operating system name)
Memory	Displays the amount of memory available to this VM.	xxx [MB GB]
Reserved Memory	Displays the amount of memory reserved for this VM (by the hypervisor).	xxx [MB GB]
Assigned Memory (Hyper-V only)	Displays the amount of dynamic memory currently assigned to the VM by the hypervisor.	xxx [MB GB]

Parameter	Description	Values
Cores	Displays the number of CPU cores being used by this VM.	(number)
Reserved CPU	Displays the amount of CPU power reserved for this VM (by the hypervisor).	xxx [GHz]
Disk Capacity	Displays the total disk capacity available to this VM.	xxx [GB TB]
Network Adapters	Displays the number of network adapters available to this VM.	(# of adapter ports)
IP Addresses	Displays the IP address assigned to the VM.	(IP address)
Storage Container	Displays the name of the storage container in which the VM resides.	(storage container name)
Virtual Disks	Displays the number of virtual disks in the VM.	(number)
NGT Enabled	Displays whether NGT is enabled or not for the VM.	[Yes No]
NGT Mounted	Displays whether NGT is mounted or not for the VM.	[Yes No]
GPU Configuration	(AHV only) Comma-separated list of GPUs configured for the VM. GPU information includes the model name and a count in parentheses if multiple GPUs of the same type are configured for the VM. If the firmware on the GPU is in compute mode, the string <code>compute</code> is appended to the model name.  The field is hidden if no GPUs are configured or if the hypervisor is not AHV.	(list of GPUs)
GPUs in Use	(AHV only) Number of GPUs in use by a VM.  The field is hidden if no GPUs are configured or if the hypervisor is not AHV.	(number)
VMware Guest Tools Mounted	Displays whether VMware guest tools are mounted or not on the VM	[Yes No]
VMware Guest Tools Running Status	Displays whether VMware guest tools are running or not on the VM.	[Yes No]

## Cluster Summary Information

When a VM is not selected in the table (or when the word **Summary** is clicked), summary information across all VMs in the cluster appears in the lower part of the screen.

- The **VM Summary** fields appear in the lower left column. The following table describes the fields in this column.
- Three tabs appear that display cluster-wide information (see following sections for details about each tab): **Performance Summary**, **All VM Alerts**, **All VM Events**.

**Table 61: VM Summary Fields**

Parameter	Description	Values
Total VMs	Displays the total number of VMs in the cluster.	(number)
VM State	Displays the number of powered on, powered off, and suspended VMs in the cluster.	[number] powered on, powered off, suspended
Total Provisioned vCPU	Displays the total number of provisioned virtual CPUs in the cluster.	(number)
Total Reserved CPU	Displays the total amount of CPU power reserved for the VMs (by the hypervisor).	xxx [GHz]
Total Provisioned Memory	Displays the total amount of memory provisioned for all VMs.	xxx [GB]
Total Reserved Memory	Displays the total amount of memory reserved for all VMs (by the hypervisor).	xxx [GB]

## VM Performance Tab

The VM Performance tab displays graphs of performance metrics. The tab label varies depending on what is selected in the table:

- **Performance Summary** (no VM selected). Displays resource performance statistics (CPU, memory, and I/O) across all VMs in the cluster.
- **VM Performance** (VM selected). Displays resource performance statistics (CPU, memory, and I/O) for the selected VM.

The graphs are rolling time interval performance monitors that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add a monitor to the analysis page by clicking the blue link in the upper right of the graph. For more information, see [Analysis Dashboard](#) on page 330. The Performance tab includes the following graphs:

- **[Cluster-wide] CPU Usage:** Displays the percentage of CPU capacity currently being used (0 - 100%) across all VMs or for the selected VM.
- **[Cluster-wide] Memory Usage:** Displays the percentage of memory capacity currently being used (0 - 100%) across all VMs or for the selected VM. (This field does not appear when the hypervisor is Hyper-V.)
- **[Cluster-wide] {Hypervisor|Controller} IOPS:** Displays I/O operations per second (IOPS) across all VMs or for the selected VM.

**Note:** In this and the following two fields, the field name is either *Controller* or *Hypervisor* to indicate where the information comes from. For ESXi, the information comes from the hypervisor; for Hyper-V and AHV, the information comes from the Controller VM.

- **[Cluster-wide] {Hypervisor|Controller} I/O Bandwidth:** Displays I/O bandwidth used per second (MBps or KBps) across all VMs or for the selected VM.
- **[Cluster-wide] {Hypervisor|Controller} Avg I/O Latency:** Displays the average I/O latency (in milliseconds) across all VMs or for the selected VM.

## Virtual Disks Tab

The Virtual Disks tab displays information in tabular form about the virtual disks in a selected VM. (This tab appears only when a VM is selected.) Each line represents a virtual disk, and the following information is displayed for each disk organized under *Default* and *Additional Stats* subtabs.

### Default Tab:

**Note:** Clicking on a virtual disk (line) displays subtabs for total, read, and write IOPS, I/O bandwidth, and I/O latency performance graphs for the virtual disk (see the *Performance Tab* section for more information about the graphs).

- **Virtual Disk.** Displays the virtual disk identification number.
- **Total Capacity.** Displays the total capacity of the virtual disk (in GiBs).
- **Physical Usage.** Displays the used space of the virtual disks (in GiBs).
- **Read IOPS.** Displays the read IOPS for the virtual disk.
- **Read BW.** Displays the bandwidth used by the virtual disk for read operations.
- **Read Latency.** Displays the average I/O latency for read requests to this virtual disk.
- **Write IOPS.** Displays the write IOPS for the virtual disk.
- **Write BW.** Displays the bandwidth used by the virtual disk for write operations.
- **Write Latency.** Displays the average I/O latency for write requests to this virtual disk.
- **Flash Mode.** Displays whether flash mode is enabled for the virtual disk or not.

### Additional Stats Tab:

- **Total IOPS.** Displays the total (both read and write) I/O operations per second (IOPS) for the virtual disk.
- **Random IO.** Displays the percentage of I/O that is random (not sequential).
- **Read Source Cache.** Displays the amount of cache data accessed for read requests.
- **Read Source SSD.** Displays the amount of SSD data accessed for read requests.
- **Read Source HDD.** Displays the amount of HDD data accessed for read requests.
- **Read Working Size Set.** Displays the amount of data actively being read by applications in the VM that are using this virtual disk.
- **Write Working Size Set.** Displays the amount of data actively being written by applications in the VM that are using this virtual disk.
- **Union Working Size Set.** Displays the total amount of data used by the VM for either reads or writes.

## VM NICs Tab

The VM NICs tab displays information in tabular form about the virtual NICs in a selected VM. (This tab appears only when a VM is selected.) Each line represents a virtual NIC, and the following information is displayed for each NIC:

- **Virtual NIC.** Displays the virtual NIC identification number.
- **Adapter Type.** Displays the adaptor type defined for the virtual NIC.
- **MAC Address.** Displays the virtual NIC MAC address
- **IPv4 Addresses.** Displays the virtual NIC IPv4 address(es).

- **IPv6 Addresses.** Displays the virtual NIC IPv6 address(es).
- **Received Packets.** Displays the number of packets received by the virtual NIC.
- **Transmitted Packets.** Displays the number of packets transmitted by the virtual NIC.
- **Dropped Rx Packets.** Displays the number of received packets dropped by the virtual NIC.
- **Dropped Tx Packets.** Displays the number of transmitted packets dropped by the virtual NIC.

When you click a virtual NIC entry, three more tabs appear below the list of virtual NICs. Clicking the **Virtual NICs Stats** tab displays the following statistics for that virtual NIC:

- **Total Packets Received.** Displays a monitor of the total packets received (in KB or MB) over time. Place the cursor anywhere on the line to see the value for that point in time. (This applies to all the monitors on this tab.)
- **Total Packets Transmitted.** Displays a monitor of the transmitted data rate.
- **Dropped Packets Received.** Displays a monitor of received packets that were dropped.
- **Dropped Packets Transmitted.** Displays a monitor of transmitted packets that were dropped.
- **Error Packets Received.** Displays a monitor for error packets received.

Clicking the **Host NICs Stats** tab displays the following statistics for each host NIC (one per line) that is used by the selected virtual NIC to send the traffic:

- **Host NIC.** Displays the host NIC name.
- **Speed (in KBps).** Displays the host NIC transmission speed.
- **MAC Address.** Displays the host NIC MAC address.
- **Received Packets.** Displays the number of packets received by the host NIC.
- **Transmitted Packets.** Displays the number of packets transmitted by the host NIC.
- **Dropped Rx Packets.** Displays the number of received packets dropped by the host NIC.
- **Dropped Tx Packets.** Displays the number of transmitted packets dropped by the host NIC.
- **Rx Packet Errors.** Displays the number of error packets received by the host NIC.
- **Tx Packet Errors.** Displays the number of error packets transmitted by the host NIC.

Clicking the **Physical Switch Interface Stats** tab displays the following statistics for each physical switch interface (one per line) used by the selected virtual NIC to send the traffic:

- **Physical Switch Interface.** Displays the switch interface name.
- **Switch ID.** Displays the switch interface ID value.
- **Index.** Displays the switch interface index number.
- **MTU (in Bytes).** Displays the size in bytes of the largest protocol data unit (maximum transmission unit) that the layer can pass onwards.
- **MAC Address.** Displays the interface MAC address.
- **Unicast Rx Pkts.** Displays the number of unicast packets received.
- **Unicast Tx Pkts.** Displays the number of unicast packets transmitted.
- **Error Rx Pkts.** Displays the number of received packets with an error.

- **Error Tx Pkts.** Displays the number of transmitted packets with an error.
- **Discard Rx Pkts.** Displays the number of received packets that were discarded.
- **Discard Tx Pkts.** Displays the number of transmitted packets that were discarded.

### VM Alerts Tab

The VM Alerts tab displays the unresolved alert messages about all VMs or the selected VM in the same form as the Alerts page. For more information, see [Alerts Summary View](#). Click the **Unresolved X** button in the filter field to also display resolved alerts.

### VM Events Tab

The VM Events tab displays the unacknowledged event messages about all VMs or the selected VM in the same form as the Events page. For more information, see [Events Summary View](#). Click the **Include Acknowledged** button to also display acknowledged events.

### VM Snapshots Tab (Acropolis only)

The VM Snapshots tab displays information in tabular form about backup snapshots of the VM. (This tab appears only when a VM is selected.) Each line represents a snapshot, and the following information is displayed for each snapshot:

- **Create Time.** Displays the time the backup snapshot was created (completed).
- **Name.** Displays a name for the backup if one was created.
- **Actions.** Displays four action links:
  - Click the **Details** link to open a window that displays the VM configuration plus a creation time stamp field.
  - Click the **Clone** link to clone a VM from the snapshot.
  - Click the **Restore** link to restore the VM from the snapshot. This restores the VM back to the state of the selected snapshot.
  - Click the **Delete** link to delete the snapshot.

### VM Tasks Tab (Acropolis only)

The VM Tasks (selected VM) or All VM Tasks (cluster-wide) tab displays a log in tabular form of the running and completed tasks for the selected VM or across the cluster. Each line represents a task, and the following information is displayed for each task:

- **Operation.** Describes the type of task.
- **Entities.** Lists the affected VM and node.
- **Percent Complete.** Displays the run status (0-100%) of the task.
- **Progress Status.** Displays the completion status of the task (succeeded, in progress, failed).
- **Create Time.** Displays when the task began.
- **Duration.** Displays how long the task took to complete.

### I/O Metrics

The I/O Metrics tab displays information about different I/O metrics for the VM (latency and performance distribution).

- Average I/O latency for the VM. Displays a graph of average I/O latency (in milliseconds) for reads and writes over a period of time. If you hover the cursor over the graph, the read and write latency at that particular time is displayed.
- Performance distribution. Displays a bar chart for the performance distribution of read and write size (in bytes) and read and write latency (in milliseconds). This widget also provides information on the read source (HDD, SSD, or DRAM), random vs sequential read and writes in a pie chart format. This information changes according to the time that you select in the **Avg I/O Latency** widget.

## Console Tab

The Console tab displays a live console window. (This tab appears only when a VM is selected.) In addition to entering commands in the console window, you can invoke several options from this tab:

- Click the language (left-most) button and select the desired language from the pull-down list to set the language key mapping for the console keyboard.
- Click the **Send CtrlAltDel** button to send a Ctrl+Alt+Delete key signal. This is the same as pressing Ctrl+Alt +Delete from the console keyboard.
- Click the **Take Screenshot** button to take a screen shot of the console display that you can save for future reference.
- Click the **New Window** button to open a new console window. This is the same as clicking the **Launch Console** link on the Summary line.

## VM Management

You can create and manage VMs directly from *Prism Element* when the hypervisor is either AHV or ESXi. The following topics provide more information on creating and managing VM configuration on AHV and ESXi.

- AHV
  - To create a VM, see [Creating a VM \(AHV\)](#) on page 270.
  - To manage guest tools, launch console, power actions, take snapshot, migrate, power operations, clone, update, or delete operations, see [Managing a VM \(AHV\)](#) on page 276.
- ESXi
  - To create a VM, see [Creating a VM \(ESXi\)](#) on page 286.
  - To manage guest tools, launch VM console, power actions, clone, update, or delete operations, see [Managing a VM \(ESXi\)](#) on page 288.

### Creating a VM (AHV)

In AHV clusters, you can create a new virtual machine (VM) through the Prism Element web console.

#### About this task

**Note:** Use Prism Central to create a VM with the memory overcommit feature enabled. Prism Element web console does not allow you to enable memory overcommit while creating a VM. If you create a VM using the Prism Element web console and want to enable memory overcommit for it, update the VM using Prism Central and enable memory overcommit in the **Update VM** page in Prism Central. For more information, see [Updating a VM through Prism Central](#) information in *Prism Central Infrastructure Guide*.

When creating a VM, you can configure all of its components, such as number of vCPUs and memory, but you cannot attach a volume group to the VM. Attaching a volume group is possible only when you are modifying a VM.

To create a VM, do the following:

## Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Create VM** button.

**Note:** This option does not appear in clusters that do not support this feature.

The **Create VM** dialog box appears.

3. Do the following in the indicated fields:

- a. **Name:** Enter a name for the VM.
- b. **Description** (optional): Enter a description for the VM.
- c. **Timezone:** Select the timezone that you want the VM to use. If you are creating a Linux VM, select **(UTC) UTC**.

**Note:**

The RTC of Linux VMs must be in UTC, so select the UTC timezone if you are creating a Linux VM.

Windows VMs preserve the RTC in the local timezone, so set up the Windows VM with the hardware clock pointing to the desired timezone.

- d. **Use this VM as an agent VM:** Select this option to make this VM as an agent VM.

You can use this option for the VMs that must be powered on before the rest of the VMs (for example, to provide network functions before the rest of the VMs are powered on the host) and must be powered off after the rest of the VMs are powered off (for example, during maintenance mode operations). Agent VMs are never migrated to any other host in the cluster. If an HA event occurs or the host is put in maintenance mode, agent VMs are powered off and are powered on the same host once that host comes back to a normal state.

If an agent VM is powered off, you can manually start that agent VM on another host and the agent VM now permanently resides on the new host. The agent VM is never migrated back to the original host. Note that you cannot migrate an agent VM to another host while the agent VM is powered on.

- e. **vCPU(s):** Enter the number of virtual CPUs to allocate to this VM.
- f. **Number of Cores per vCPU:** Enter the number of cores assigned to each virtual CPU.
- g. **Memory:** Enter the amount of memory (in GiB) to allocate to this VM.

4. (For GPU-enabled AHV clusters only) To configure GPU access, click **Add GPU** in the **Graphics** section, and then do the following in the **Add GPU** dialog box:

For more information, see [GPU and vGPU Support](#) in the *AHV Administration Guide*.

- a. To configure GPU pass-through, in **GPU Mode**, click **Passthrough**, select the GPU that you want to allocate, and then click **Add**.

If you want to allocate additional GPUs to the VM, repeat the procedure as many times as you need to. Make sure that all the allocated pass-through GPUs are on the same host. If all specified GPUs of the type that you

want to allocate are in use, you can proceed to allocate the GPU to the VM, but you cannot power on the VM until a VM that is using the specified GPU type is powered off.

For more information, see [GPU and vGPU Support](#) in the *AHV Administration Guide*.

- b. To configure virtual GPU (vGPU) access, in **GPU Mode**, click **virtual GPU**, select a GRID license, and then select a virtual GPU (vGPU) profile from the list.

**Note:** This option is available only if you have installed the GRID host driver on the GPU hosts in the cluster.

For more information about the NVIDIA GRID host driver installation instructions, see the [NVIDIA Grid Host Driver for Nutanix AHV Installation Guide](#).

You can assign multiple virtual GPU (vGPU) to a VM. A vGPU is assigned to the VM only if a vGPU is available when the VM is starting up.

Before you add multiple vGPUs to the VM, see [Multiple Virtual GPU Support](#) and [Restrictions for Multiple vGPU Support](#) in the *AHV Administration Guide*.

**Note:** Multiple vGPUs are supported on the same VM only if you select the highest vGPU profile type.

After you add the first vGPU, to add multiple vGPUs, see [Adding Multiple vGPUs to the Same VM](#) in the *AHV Administration Guide*.

5. Select one of the following firmware to boot the VM.

- » **Legacy BIOS:** Select legacy BIOS to boot the VM with legacy BIOS firmware.
- » **UEFI:** Select UEFI to boot the VM with UEFI firmware. UEFI firmware supports larger hard drives, faster boot time, and provides more security features. For more information about UEFI firmware, see [UEFI Support for VM](#) in the *AHV Administration Guide*.

If you select UEFI, you can enable the following features:

- **Secure Boot:** Select this option to enable UEFI secure boot policies for your guest VMs. For more information about Secure Boot, see [Secure Boot Support for VMs](#) in the *AHV Administration Guide*.
- **Windows Defender Credential Guard:** Select this option to enable the Windows Defender Credential Guard feature of Microsoft Windows operating systems that allows you to securely isolate user credentials from the rest of the operating system. Follow the detailed instructions described in [Windows Defender Credential Guard Support in AHV](#) in the *AHV Administration Guide* to enable this feature.

**Note:** For information on how to add the virtual TPM, see [Securing AHV VMs with Virtual Trusted Platform Module](#).

6. To attach a disk to the VM, click the **Add New Disk** button.

The **Add Disk** dialog box appears. Do the following in the indicated fields:

- a. **Type:** Select the type of storage device, **DISK** or **CD-ROM**, from the drop-down list.

The following fields and options vary depending on whether you choose **DISK** or **CD-ROM**.

- b. **Operation:** Specify the device contents from the drop-down list.

- Select **Clone from ADSF file** to copy any file from the cluster that can be used as an image onto the disk.
- Select **Empty CD-ROM** to create a blank CD-ROM device. (This option appears only when **CD-ROM** is selected in the previous field.) A CD-ROM device is needed when you intend to provide a system image from CD-ROM.
- Select **Allocate on Storage Container** to allocate space without specifying an image. (This option appears only when **DISK** is selected in the previous field.) Selecting this option means you are allocating space only. You have to provide a system image later from a CD-ROM or other source.
- Select **Clone from Image Service** to copy an image that you have imported by using image service feature onto the disk. For more information about the Image Service feature, see [Configuring Images](#) and [Image Management](#) in the *Prism Self Service Administration Guide*.

- c. **Bus Type:** Select the bus type from the dropdown list.

The options displayed in the **Bus Type** dropdown list varies based on the storage device **Type** selected in Step a.

- For device **Disk**, select from **SCSI**, **SATA**, **PCI**, or **IDE** bus type.
- For device **CD-ROM**, you can select either **IDE** or **SATA** bus type.

**Note:**

- SCSI bus is the preferred bus type and it is used in most cases. Ensure you have installed the VirtIO drivers in the guest OS. For more information about VirtIO drivers, see [Nutanix VirtIO for Windows](#) in *AHV Administration Guide*.
- For AHV 5.16 and later, you cannot use an IDE device if **Secured Boot** is enabled for **UEFI Mode** boot configuration.

**Caution:** Use SATA, PCI, IDE for compatibility purpose when the guest OS does not have VirtIO drivers to support SCSI devices. This may have performance implications. For more information about VirtIO drivers, see [Nutanix VirtIO for Windows](#) in *AHV Administration Guide*.

- d. **ADSF Path:** Enter the path to the desired system image.

This field appears only when **Clone from ADSF file** is selected. It specifies the image to copy. Enter the path name as `/storage_container_name/iso_name.iso`. For example to clone an image from myos.iso in a storage container named crt1, enter /crt1/myos.iso. When a user types the storage container

name (*/storage\_container\_name*), a list appears of the ISO files in that storage container (assuming one or more ISO files had previously been copied to that storage container).

- e. **Image:** Select the image that you have created by using the image service feature.  
This field appears only when **Clone from Image Service** is selected. It specifies the image to copy.
  - f. **Storage Container:** Select the storage container to use from the drop-down list.  
This field appears only when **Allocate on Storage Container** is selected. The list includes all storage containers created for this cluster.
  - g. **Logical Size (GiB):** Enter the disk size in GiB.
  - h. **Index:** Displays **Next Available** by default.
  - i. When all the field entries are correct, click the **Add** button to attach the disk to the VM and return to the **Create VM** dialog box.
  - j. Repeat this step to attach additional devices to the VM.
7. To create a network interface for the VM, click the **Add New NIC** button.  
The Prism Element console displays the **Create NIC** dialog box.

**Note:**

- All virtual network interface cards (vNICs) on a single virtual machine (VM) must be configured with the same subnet and VLAN configurations. If the first vNIC uses basic VLAN, all subsequent vNICs must also use basic VLAN. Similarly, if the first vNIC uses overlay VLAN, all additional

vNICs must match this type. The system will reject any configuration that includes a mismatch subnet types.

- Multiple NIC types are supported only for Traffic Mirroring destination vNICs. For more information, see [Traffic Mirroring on AHV Hosts](#) in the *AHV Administration Guide*.
- To create or update a Traffic Mirroring destination type VM or vNIC, use command line interface. For more information, see [Traffic Mirroring on AHV Hosts](#) in the *AHV Administration Guide*.

Do the following in the indicated fields:

- a. **Subnet Name:** Select the target virtual LAN from the drop-down list.

The list includes all defined networks.

**Note:** Selecting IPAM enabled subnet from the drop-down list displays the **Private IP Assignment** information that provides information about the number of free IP addresses available in the subnet and in the IP pool.

- b. **Network Connection State:** Select the state for the network that you want it to operate in after VM creation. The options are *Connected* or *Disconnected*.
- c. **Private IP Assignment:** This is a read-only field and displays the following:
  - **Network Address/Prefix:** The network IP address and prefix.
  - **Free IPs (Subnet):** The number of free IP addresses in the subnet.
  - **Free IPs (Pool):** The number of free IP addresses available in the IP pools for the subnet.
- d. **Assignment Type:** This is for IPAM enabled network. Select **Assign with DHCP** to assign IP address automatically to the VM using DHCP. For more information, see [IP Address Management](#) in the *AHV Administration Guide*.
- e. When all the field entries are correct, click the **Add** button to create a network interface for the VM and return to the **Create VM** dialog box.
- f. Repeat this step to create additional network interfaces for the VM.

**Note:**

- Nutanix does not recommend configuring multiple clusters to use the same broadcast domain (the same VLAN network), but if you do, configure MAC address prefixes for each cluster to avoid duplicate MAC addresses. For information on configuring or removing pre-defined prefix of MAC addresses for each cluster, see [MAC Address Prefix](#) on page 159
- Nutanix AHV clusters use the MAC address prefix OUI 50:6B:8D by default.

8. To configure affinity policy for this VM, click **Set Affinity**.

The **Set VM Host Affinity** dialog box appears.

- a. Select the host or hosts on which you want configure the affinity for this VM.
- b. Click **Save**.

The selected host or hosts are listed. This configuration is permanent. The VM will not be moved from this host or hosts even in case of HA event and will take effect once the VM starts.

9. To customize the VM by using Cloud-init (for Linux VMs) or Sysprep (for Windows VMs), select the **Custom Script** check box.  
Fields required for configuring Cloud-init and Sysprep, such as options for specifying a configuration script or answer file and text boxes for specifying paths to required files, appear below the check box.
  10. To specify a user data file (Linux VMs) or answer file (Windows VMs) for unattended provisioning, do one of the following:
    - » If you uploaded the file to a storage container on the cluster, click **ADSF path**, and then enter the path to the file.  
Enter the ADSF prefix (adsf://) followed by the absolute path to the file. For example, if the user data is in /home/my\_dir/cloud.cfg, enter adsf:///home/my\_dir/cloud.cfg. Note the use of three slashes.
    - » If the file is available on your local computer, click **Upload a file**, click **Choose File**, and then upload the file.
    - » If you want to create or paste the contents of the file, click **Type or paste script**, and then use the text box that is provided.
  11. To copy one or more files to a location on the VM (Linux VMs) or to a location in the ISO file (Windows VMs) during initialization, do the following:
    - a. In **Source File ADSF Path**, enter the absolute path to the file.
    - b. In **Destination Path in VM**, enter the absolute path to the target directory and the file name.  
For example, if the source file entry is /home/my\_dir/myfile.txt then the entry for the **Destination Path in VM** should be /<directory\_name>/copy\_destination> i.e. /mnt/myfile.txt.
    - c. To add another file or directory, click the button beside the destination path field. In the new row that appears, specify the source and target details.
  12. When all the field entries are correct, click the **Save** button to create the VM and close the **Create VM** dialog box.
- The new VM appears in the VM table view.

## Managing a VM (AHV)

You can use the web console to manage virtual machines (VMs) in AHV managed clusters.

### About this task

**Note:** Use Prism Central to update a VM if you want to enable memory overcommit for it. Prism Element web console does not allow you to enable memory overcommit while updating a VM. You can enable memory overcommit in the **Update VM** page in Prism Central. For more information, see [Updating a VM through Prism Central](#) information in *Prism Central Infrastructure Guide*.

After creating a VM, you can use the web console to start or shut down the VM, launch a console window, update the VM configuration, take a snapshot, attach a volume group, migrate the VM, clone the VM, or delete the VM.

**Note:** Your available options depend on the VM status, type, and permissions. Unavailable options are grayed out.

To accomplish one or more of these tasks, do the following:

### Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Table** view.

3. Select the target VM in the table (top section of screen).

The Summary line (middle of screen) displays the VM name with a set of relevant action links on the right. You can also right-click on a VM to select a relevant action.

The possible actions are **Manage Guest Tools**, **Launch Console**, **Power on** (or **Power off**), **Take Snapshot**, **Migrate**, **Clone**, **Update**, and **Delete**.

**Note:** VM pause and resume feature is not supported on AHV.

The following steps describe how to perform each action.

- To manage guest tools as follows, click **Manage Guest Tools**.

You can also enable NGT applications (self-service restore, Volume Snapshot Service and application-consistent snapshots) also as part of manage guest tools.

- Select the **Enable Nutanix Guest Tools** checkbox to enable NGT on the selected VM.

- Select the **Mount Nutanix Guest Tools** checkbox to mount NGT on the selected VM.

Ensure that VM must have at least one empty IDE CD-ROM slot to attach the ISO.

The VM is registered with the NGT service. NGT is enabled and mounted on the selected virtual machine. A CD with volume label NUTANIX\_TOOLS gets attached to the VM.

- To enable self-service restore feature for Windows VMs, select the **Self Service Restore (SSR)** checkbox.

The Self-Service Restore feature is enabled on the VM. The guest VM administrator can restore the desired file or files from the VM. For more information about self-service restore feature, see [Self-Service Restore](#) in the *Data Protection and Recovery with Prism Element* guide.

- After you select the **Enable Nutanix Guest Tools** checkbox the VSS snapshot feature is enabled by default.

After this feature is enabled, Nutanix native in-guest VmQuiesced Snapshot Service (VSS) agent takes snapshots for VMs that support VSS.

**Note:** The AHV VM snapshots are not application consistent. The AHV snapshots are taken from the **VM** entity menu by selecting a VM and clicking **Take Snapshot**.

The application consistent snapshots feature is available with Protection Domain based snapshots and Recovery Points in Prism Central. For more information, see [Conditions for Application-consistent Snapshots](#) in the *Data Protection and Recovery with Prism Element* guide.

- Click **Submit**.

The VM is registered with the NGT service. NGT is enabled and mounted on the selected virtual machine. A CD with volume label NUTANIX\_TOOLS gets attached to the VM.

**Note:**

- If you clone a VM, by default NGT is not enabled on the cloned VM. If the cloned VM is powered off, enable NGT from the UI and power on the VM. If cloned VM is powered on, enable NGT from the UI and restart the nutanix guest agent service.
- You can enable NGT on multiple VMs simultaneously. For more information, see [Enabling NGT and Mounting the NGT Installer Simultaneously on Multiple Cloned VMs](#).

If you eject the CD, you can mount the CD back again by logging into the Controller VM and running the following nCLI command.

```
nutanix@cvm$ ncli ngt mount vm-id=virtual_machine_id
```

For example, to mount the NGT on the VM with

VM\_ID=00051a34-066f-72ed-0000-000000005400::38dc7bf2-a345-4e52-9af6-c1601e759987, type the following command.

```
nutanix@cvm$ ncli ngt mount vm-id=00051a34-066f-72ed-0000-000000005400::38dc7bf2-a345-4e52-9af6-c1601e759987
```

- To launch a console window, click the **Launch Console** action link.

This opens a Virtual Network Computing (VNC) client and displays the console in a new tab or window. This option is available only when the VM is powered on. The console window includes the following menu options (top right):

- Clicking the **Mount ISO** button displays a window that allows you to mount an ISO image to the VM. To mount an image, select the desired image and CD-ROM drive from the drop-down lists and then click the **Mount** button.

**Note:** For information on how to select CD-ROM as the storage device when you intent to provide a system image from CD-ROM, see *Add New Disk* in [Creating a VM \(AHV\)](#) on page 270.

- Clicking the **Unmount ISO** button unmounts the ISO from the console.
- Clicking the **C-A-D** icon button sends a **CtrlAltDel** command to the VM.
- Clicking the camera icon button takes a screenshot of the console window.
- Clicking the power icon button allows you to power on/off the VM. These are the same options that you can access from the **Power On Actions** or **Power Off Actions** action link below the VM table (see next step).

- To start or shut down the VM, click the **Power on** (or **Power off**) action link.

Power on begins immediately. If you want to power off the VMs, you are prompted to select one of the following options:

- Power Off:** Hypervisor performs a hard power off action on the VM.
- Power Cycle:** Hypervisor performs a hard restart action on the VM.
- Reset:** Hypervisor performs an ACPI reset action through the BIOS on the VM.
- Guest Shutdown:** Operating system of the VM performs a graceful shutdown.
- Guest Reboot:** Operating system of the VM performs a graceful restart.

Select the option you want and click **Submit**.

**Note:** If you perform power operations such as Guest Reboot or Guest Shutdown by using the Prism Element web console or API on Windows VMs, these operations might silently fail without any error messages if at that time a screen saver is running in the Windows VM. Perform the same power operations again immediately, so that they succeed.

- To make a snapshot of the VM, click the **Take Snapshot** action link.

For more information, see [Virtual Machine Snapshots](#) on page 282.

- To migrate the VM to another host, click the **Migrate** action link.

This displays the **Migrate VM** dialog box. Select the target host from the drop-down list (or select the **System will automatically select a host** option to let the system choose the host) and then click the **Migrate** button to start the migration.

**Note:** Nutanix recommends to live migrate VMs when they are under light load. If they are migrated while heavily utilized, migration may fail because of limited bandwidth.

- To clone the VM, click the **Clone** action link.

This displays the **Clone VM** dialog box, which includes the same fields as the **Create VM** dialog box. A cloned VM inherits the most the configurations (except the name) of the source VM. Enter a name for the clone and

then click the **Save** button to create the clone. You can optionally override some of the configurations before clicking the **Save** button. For example, you can override the number of vCPUs, memory size, boot priority, NICs, or the guest customization.

**Note:**

- You can clone up to 250 VMs at a time.
- You cannot override the secure boot setting while cloning a VM, unless the source VM already had secure boot setting enabled.

**10.** To modify the VM configuration, click the **Update** action link.

The **Update VM** dialog box appears, which includes the same fields as the **Create VM** dialog box. Modify the configuration as needed, and then save the configuration. In addition to modifying the configuration, you can attach a volume group to the VM and enable flash mode on the VM. If you attach a volume group to a VM that is part of a protection domain, the VM is not protected automatically. Add the VM to the same Consistency Group manually.

(For GPU-enabled AHV clusters only) You can add pass-through GPUs if a VM is already using GPU pass-through. You can also change the GPU configuration from pass-through to vGPU or vGPU to pass-through, change the vGPU profile, add more vGPUs, and change the specified vGPU license. However, you need to power off the VM before you perform these operations.

- Before you add multiple vGPUs to the VM, see [Multiple Virtual GPU Support](#) and [Restrictions for Multiple vGPU Support](#) in the *AHV Administration Guide*.
- Multiple vGPUs are supported on the same VM only if you select the highest vGPU profile type.
- For more information on vGPU profile selection, see:
  - *Virtual GPU Types for Supported GPUs* in the *NVIDIA Virtual GPU Software User Guide* in the NVIDIA's *Virtual GPU Software Documentation* web-page, and
  - [GPU and vGPU Support](#) in the *AHV Administration Guide*.

- After you add the first vGPU, to add multiple vGPUs, see [Adding Multiple vGPUs to the Same VM](#) in the *AHV Administration Guide*.

You can add new network adapters or NICs using the **Add New NIC** option. For more information, see Step 7 in [Creating a VM \(AHV\)](#) on page 270.

You can also modify the network used by an existing NIC. Before you modify the NIC network observe the limitations in [Limitation for vNIC Hot-Unplugging](#) in the *AHV Administration Guide*.

**Note:**

- To create or update a Traffic Mirroring destination type VM or vNIC, use command line interface. For more information, see [Traffic Mirroring on AHV Hosts](#) in the *AHV Administration Guide*.
- If you delete a vDisk attached to a VM and snapshots associated with this VM exist, space associated with that vDisk is not reclaimed unless you also delete the VM snapshots.

To increase the memory allocation and the number of vCPUs on your VMs while the VMs are powered on (hot-pluggable), do the following:

- a. In the **vCPUs** field, you can increase the number of vCPUs on your VMs while the VMs are powered on.
- b. In the **Number of Cores Per vCPU** field, you can change the number of cores per vCPU only if the VMs are powered off.

**Note:** This is not a hot-pluggable feature.

- c. In the **Memory** field, you can increase the memory allocation on your VMs while the VMs are powered on. For more information about hot-pluggable vCPUs and memory, see [Virtual Machine Memory and CPU Hot-Plug Configurations](#).

To attach a volume group to the VM, do the following:

- a. In the **Volume Groups** section, click **Add volume group**, and then do one of the following:
    - » From the **Available Volume Groups** list, select the volume group that you want to attach to the VM.
    - » Click **Create new volume group**, and then, in the **Create Volume Group** dialog box, create a volume group. After you create a volume group, select it from the **Available Volume Groups** list.

Repeat these steps until you have added all the volume groups that you want to attach to the VM.
  - b. Click **Add**.
11. To enable flash mode on the VM, click the **Enable Flash Mode** check box.
    - » After you enable this feature on the VM, the status is updated in the VM table view. To view the status of individual virtual disks (disks that are flashed to the SSD), click the update disk icon in the **Disks** pane in the **Update VM** window.
    - » You can disable the flash mode feature for individual virtual disks. To update the flash mode for individual virtual disks, click the update disk icon in the **Disks** pane and deselect the **Enable Flash Mode** check box.
  12. To delete the VM, click the **Delete** action link. A window prompt appears; click the **OK** button to delete the VM.
- The deleted VM disappears from the list of VMs in the table.

## Virtual Machine Snapshots

You can generate snapshots of virtual machines or VMs. You can generate snapshots of VMs manually or automatically. Some of the purposes that VM snapshots serve are as follows:

- Disaster recovery
- Testing - as a safe restoration point in case something went wrong during testing.
- Migrate VMs
- Create multiple instances of a VM.

Snapshot is a point-in-time state of entities such as VM and Volume Groups, and used for restoration and replication of data. You can generate snapshots and store them locally or remotely. Snapshots are mechanism to capture the delta changes that has occurred over time. Snapshots are primarily used for data protection and disaster recovery. Snapshots are not autonomous like backup, in the sense that they depend on the underlying VM infrastructure and other snapshots to restore the VM. Snapshots consume less resources compared to a full autonomous backup. Typically, a VM snapshot captures the following:

- The state including the power state (for example, powered-on, powered-off, suspended) of the VMs.
- The data includes all the files that make up the VM. This data also includes the data from disks, configurations, and devices, such as virtual network interface cards.

### VM Snapshots and Snapshots for Disaster Recovery

The **VM** Dashboard only allows you to generate VM snapshots manually. You cannot select VMs and schedule snapshots of the VMs using the VM dashboard. The snapshots generated manually have very limited utility.

**Note:** These snapshots (stored locally) cannot be replicated to other sites.

You can schedule and generate snapshots as a part of the disaster recovery process using Nutanix DR solutions. AOS generates snapshots when you protect a VM with a protection domain using the **Data Protection** dashboard in Prism Element web console. For more information, see [Snapshots](#) in the *Data Protection and Recovery with Prism Element Guide*. Similarly, AOS generates recovery points (snapshots are called recovery points in Prism Central) when you protect a VM with a protection policy. For more information about protection policies, see [Protection Policies View](#) in *Nutanix Disaster Recovery Guide*.

For example, in the **Data Protection** dashboard in Prism Element web console, you can create schedules to generate snapshots using various RPO schemes such as asynchronous replication with frequency intervals of 60 minutes or more, or NearSync replication with frequency intervals of as less as 20 seconds up to 15 minutes. These schemes create snapshots in addition to the ones generated by the schedules, for example, asynchronous replication schedules generate snapshots according to the configured schedule and, in addition, an extra snapshot every 6 hours. Similarly, NearSync generates snapshots according to the configured schedule and also generates one extra snapshot every hour.

Similarly, you can use the options in the **Data Protection** entity of Prism Central to generate recovery points using the same RPO schemes.

### Creating a VM Snapshot Manually

You can create or generate a VM snapshot manually in Prism Element web console.

#### Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Table** view.
3. Click the VM you want to take a snapshot of.

4. In the **Take Snapshot** dialog box, provide a name for the snapshot and click **Submit**.

Ensure that the name contains only alphanumeric, dot, dash, or underscore characters.

The snapshot is listed with the name you provided in the **VM Snapshots** tab in the **Summary** section of the **VM Table** view.

## What to do next

You can **Delete** the snapshot. For more information, see [Deleting a VM Snapshot Manually](#) on page 283.

You can clone a VM by clicking the **Clone** action link for the snapshot of the VM.

You can use the VM snapshot to **Restore** the VM to the previous state captured in the snapshot.

Click **Details** to view the details of the snapshot.

### Deleting a VM Snapshot Manually

You can delete a snapshot for any VM.

## Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Table** view.
3. Click the VM you want to delete a snapshot of.
4. Click the **VM Snapshots** tab in the **Summary** section of the **VM Table** view.
5. Click the **Delete** action link for the snapshot that you want to delete in the list of snapshots.
6. On the confirmation box,
  - » Click **Yes** to delete the snapshot.
  - » Click **Cancel** to close the confirmation box without deleting the snapshot.

## What to do next

To create a snapshot manually, see [Creating a VM Snapshot Manually](#) on page 282.

## Adding Multiple vGPUs to the Same VM

### About this task

You can add multiple vGPUs of the same vGPU type when you create a new VM or update an existing VM.

- For information on how to create a VM, see [Creating a VM through Prism Central \(AHV\)](#).
- For information on how to update an existing VM, see [Updating a VM through Prism Central \(AHV\)](#).

For more information on multiple vGPU support, see [Multiple Virtual GPU Support](#).

### Before you begin

Ensure that the following prerequisites are met before you add multiple vGPUs to the VM:

- Select the license for NVIDIA Virtual GPU (vGPU) software version 10.1 (440.53) or later.
- Observe the guidelines and restrictions specified in [Multiple Virtual GPU Support](#) and [Restrictions for Multiple vGPU Support](#).

## Procedure

To add multiple vGPUs to the same VM, perform the following steps:

1. Click **Add GPU** in the **Resources** step of create VM workflow or update VM workflow. For more information, see [Creating a VM through Prism Central \(AHV\)](#) or [Updating a VM through Prism Central \(AHV\)](#)

2. In the **Add GPU** window, click **Add**.

The License field is grayed out and you cannot select a different license when you add a vGPU for the same VM.

The **VGPU Profile** is auto-selected. The system allows you to select additional vGPU of the same vGPU type as indicated by the message at the top of the **Add GPU** window.

The newly added vGPU appears in the **Create VM** or **Update VM** window.

3. Repeat the steps for each vGPU addition to the VM.

## Migrating Live a vGPU-enabled VM Within the Cluster

You can migrate a vGPU-enabled VM only to another host in the same cluster on Prism Element.

### About this task

You can perform live migration of VMs enabled with virtual GPUs (vGPU-enabled VMs) only on commercially reasonable effort, if the destination node is equipped to provide enough resources to the vGPU- enabled VMs. However, if the destination node is not equipped with the enough resources, the vGPU-enabled VMs are shut down and you might experience a downtime.

In a successful migration case, the vGPUs can continue to run while the VMs that are running the vGPUs are seamlessly migrated in the background.

When you perform the LCM update, the vGPU-enabled VMs are listed as Non-HA-protected VMs. LCM also migrates the Non-HA-protected VMs on commercially reasonable effort to the destination node if the following requirements are met:

- Destination node is equipped with the required resources for the VM.
- The VM GPU drivers are compatible with the AHV host GPU drivers.

If the destination node is not equipped with the enough resources or there is any compatibility issue between the VM GPU drivers and AHV host GPU drivers, the LCM forcibly shuts down the Non-HA-protected VMs.

### Before you begin

Ensure the following prerequisites are met before you live migrate the vGPU-enabled VMs:

- The VM is not powered off.
- The host affinity is not set for the VM.

If the host affinity of the VM is set to only one host, you cannot live migrate the VM. However, based on the GPU resources required, if the host affinity is set to multiple hosts with the same or similar GPU resources, you can migrate the VM among the hosts with which the affinity is set.

- You have another host in the same cluster to migrate the VM.

For limitations applicable to live migration of vGPU-enabled VMs, see [Limitations of Live Migration Support](#) in the [AHV Administration Guide](#).

**Table 62: Minimum Versions**

Component	Supports	With Minimum Version
AOS	Live migration within the same cluster	5.18.1
AHV	Live migration within the same cluster	20190916.294
AOS	Live migration across cluster	6.1
AHV	Live migration across cluster	20201105.30142

### Procedure

To migrate the vGPU-enabled VM to another host within the same cluster on Prism Element, perform the following steps:

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Table** view.
3. To migrate the VM, go to the **VM > Table**.
4. Select the VM you want to migrate live. Click **Migrate**.
5. In the **Migrate VM** dialog box, do the following:
  - a. In the **Host** drop-down list, do one of the following:
    - » Retain the *System will automatically select a host* option if you want to migrate the VM to a host selected by the system.  
The system selects a host based on the GPU resources available with the host as appropriate for the VM to be migrated live.
    - » Select the host listed in the drop-down list that you want to migrate the VM to.

6. Click **Migrate**.

Prism submits the task and displays the following message:

Successfully submitted migrate operation.  
Task details

**Task details** is a link to the **Tasks** page. Click the link to monitor the migration task on the **Tasks** page.

When the migration is complete, the host name of the VM in the **List** view changes to the host name to which you migrated the VM.

## VM Management through Prism Element (ESXi)

You can perform your core VM management operations directly from Prism without using any hypervisor management interface (for example, vCenter Server). The VM Management through Prism for ESXi feature provides an unified management interface for all of the ESXi hypervisors. For this functionality to work, you need to register vCenter Server with the Prism Element or multiple vCenter Servers with the Prism Central. For more information about registering vCenter Server to your cluster, see [Registering a Cluster to vCenter Server using Prism Element](#) on page 362.

By using this feature you can perform following operations directly through Prism.

- Create, clone, update, and delete VMs.
- Create and delete NICs.

- Attach and delete disks.
- Power operations: Power on or off, reset, suspend, resume, guest shutdown, and guest restart.
- Open and launch VM console.
- Manage VM guest tools (mounting VMware guest tools, mounting NGT).

**Note:**

- You can perform the power operations and launching of VM console even when vCenter Server is not registered.
- If you are creating VM through Prism, configuration changes to the VM when it is powered on is enabled by default and it depends on the guest operating system that is deployed on the VM.

## Rules and Guidelines

- Ensure that all the hosts in the cluster is managed by a single vCenter Server.
- Ensure that DRS is enabled on the vCenter Server.
- Ensure that you are running ESXi and vCenter Server 5.5 or later releases.
- Ensure that you have homogeneous network configuration. For example, network should have either 1G or 10G NICs.
- Ensure that you unregister the vCenter Server from the cluster before changing the IP address of the vCenter Server. After you change the IP address of the vCenter Server, you must register the vCenter Server again with the new IP address.
- The vCenter Server Registration page displays the registered vCenter Server. If for some reason the Host Connection field changes to **Not Connected**, it implies that the hosts are being managed by a different vCenter Server. In this case, there will be new vCenter entry with host connection status as Connected and you need to register to this vCenter Server. For more information about registering vCenter Server again, see [Migrating a Nutanix Cluster between Two vCenter Servers using Prism Element](#) on page 364.

**Caution:** If multiple vCenter Servers are managing the hosts, you will not be able to perform the VM management operations. Move all the hosts into one vCenter Server.

## Requirements and Limitations

- SCSI, IDE, and SATA disks are supported. PCI disks are not supported.
- The E1000, E1000e, PCnet32, VMXNET, VMXNET 2, VMXNET 3 network adapter types (NICs) are supported.
- Creating a VM by using a template is not supported.
- Creating a VM by using image service is not supported.
- If a VM is deleted, all the disks that are attached to the VM gets deleted.
- Network configuration (creation of port groups or VLANs) is not supported.

## Creating a VM (ESXi)

In ESXi clusters, you can create a new virtual machine (VM) through the web console.

## Before you begin

- Ensure that you refer requirements and limitations. For more information, see the requirements and limitations section in [VM Management through Prism Element \(ESXi\)](#) before proceeding.
- Register the vCenter Server with your cluster. For more information, see [Registering a Cluster to vCenter Server using Prism Element](#) on page 362.

## About this task

When creating a VM, you can configure all of its components, such as number of vCPUs and memory, but you cannot attach a volume group to the VM.

To create a VM, do the following:

### Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Create VM** button.  
The **Create VM** dialog box appears.
3. Do the following in the indicated fields:
  - a. **Name**: Enter a name for the VM.
  - b. **Description** (optional): Enter a description for the VM.
  - c. **Guest OS**: Type and select the guest operating system.  
The guest operating system that you select affects the supported devices and number of virtual CPUs available for the virtual machine. The **Create VM** wizard does not install the guest operating system. For information on the list of supported operating systems, see [VM Management through Prism Element \(ESXi\)](#).
  - d. **vCPU(s)**: Enter the number of virtual CPUs to allocate to this VM.
  - e. **Number of Cores per vCPU**: Enter the number of cores assigned to each virtual CPU.
  - f. **Memory**: Enter the amount of memory (in GiBs) to allocate to this VM.
4. To attach a disk to the VM, click the **Add New Disk** button.  
The Add Disks dialog box appears. Do the following in the indicated fields:
  - a. **Type**: Select the type of storage device, **DISK** or **CD-ROM**, from the drop-down list.  
The following fields and options vary depending on whether you choose **DISK** or **CD-ROM**.
  - b. **Operation**: Specify the device contents from the drop-down list.
    - Select **Clone from ADSF file** to copy any file from the cluster that can be used as an image onto the disk.
    - Select **Allocate on Storage Container** to allocate space without specifying an image. (This option appears only when **DISK** is selected in the previous field.) Selecting this option means you are allocating space only. You have to provide a system image later from a CD-ROM or other source.
  - c. **Bus Type**: Select the bus type from the drop-down list. The choices are **IDE** or **SCSI**.
  - d. **ADSF Path**: Enter the path to the desired system image.  
This field appears only when **Clone from ADSF file** is selected. It specifies the image to copy. Enter the path name as `/storage_container_name/vmdk_name.vmdk`. For example to clone an image from myvm-flat.vmdk in a storage container named crt1, enter `/crt1/myvm-flat.vmdk`. When a user types the storage

container name (`/storage_container_name/`), a list appears of the VMDK files in that storage container (assuming one or more VMDK files had previously been copied to that storage container).

**Note:** Make sure you are copying from a flat file.

- e. **Storage Container:** Select the storage container to use from the drop-down list.

This field appears only when **Allocate on Storage Container** is selected. The list includes all storage containers created for this cluster.

- f. **Size:** Enter the disk size in GiBs.

- g. When all the field entries are correct, click the **Add** button to attach the disk to the VM and return to the **Create VM** dialog box.

- h. Repeat this step to attach more devices to the VM.

5. To create a network interface for the VM, click the **Add New NIC** button.

The Create NIC dialog box appears. Do the following in the indicated fields:

- a. **VLAN Name:** Select the target virtual LAN from the drop-down list.

The list includes all defined networks. For more information, see [Network Configuration for VM Interfaces](#).

- b. **Network Adapter Type:** Select the network adapter type from the drop-down list.

For information on the list of supported adapter types, see [VM Management through Prism Element \(ESXi\)](#).

- c. **Network UUID:** This is a read-only field that displays the network UUID.

- d. **Network Address/Prefix:** This is a read-only field that displays the network IP address and prefix.

- e. When all the field entries are correct, click the **Add** button to create a network interface for the VM and return to the **Create VM** dialog box.

- f. Repeat this step to create more network interfaces for the VM.

6. When all the field entries are correct, click the **Save** button to create the VM and close the **Create VM** dialog box.

The new VM appears in the VM table view. For more information, see [VM Table View](#).

## Managing a VM (ESXi)

You can use the web console to manage virtual machines (VMs) in the ESXi clusters.

### Before you begin

- Ensure that you refer the requirements and limitations. For more information, see the requirements and limitations section in [VM Management through Prism Element \(ESXi\)](#) before proceeding.
- Ensure that you have registered the vCenter Server with your cluster. For more information, see [Registering a Cluster to vCenter Server using Prism Element](#) on page 362.

### About this task

After creating a VM, you can use the web console to manage guest tools, power operations, suspend, launch a VM console window, update the VM configuration, clone the VM, or delete the VM. To accomplish one or more of these tasks, do the following:

**Note:** Your available options depend on the VM status, type, and permissions. Unavailable options are unavailable.

## Procedure

1. Log in to Prism Element web console.
2. In the VM dashboard, click the **Table** view.
3. Select the target VM in the table (top section of screen).

The summary line (middle of screen) displays the VM name with a set of relevant action links on the right. You can also right-click on a VM to select a relevant action.

The possible actions are **Manage Guest Tools**, **Launch Console**, **Power on** (or **Power off actions**), **Suspend** (or **Resume**), **Clone**, **Update**, and **Delete**. The following steps describe how to perform each action.

4. To manage guest tools as follows, click **Manage Guest Tools**.

You can also enable NGT applications (self-service restore, volume snapshot service and application-consistent snapshots) as part of manage guest tools.

- a. Select the **Enable Nutanix Guest Tools** checkbox to enable NGT on the selected VM.
- b. Select the **Mount Nutanix Guest Tools** checkbox to mount NGT on the selected VM.

Ensure that VM has at least one empty IDE CD-ROM or SATA slot to attach the ISO.

The VM is registered with the NGT service. NGT is enabled and mounted on the selected virtual machine. A CD with volume label NUTANIX\_TOOLS gets attached to the VM.

- c. To enable self-service restore feature for Windows VMs, select the **Self Service Restore (SSR)** checkbox.

The self-service restore feature is enabled of the VM. The guest VM administrator can restore the desired file or files from the VM. For information on the self-service restore feature, see [Self-Service Restore](#) in the *Data Protection and Recovery with Prism Element* guide.

- d. After you select the **Enable Nutanix Guest Tools** checkbox the VSS and application-consistent snapshot feature is enabled by default.

After this feature is enabled, Nutanix native in-guest VmQuiesced snapshot service (VSS) agent is used to take application-consistent snapshots for all the VMs that support VSS. This mechanism takes application-consistent snapshots without any VM stuns (temporary unresponsive VMs) and also enables third-party backup providers like Commvault and Rubrik to take application-consistent snapshots on Nutanix platform

in a hypervisor-agnostic manner. For more information, see [Conditions for Application-consistent Snapshots](#) in the *Data Protection and Recovery with Prism Element* guide.

- e. To mount VMware guest tools, select the **Mount VMware Guest Tools** checkbox.

The VMware guest tools are mounted on the VM.

**Note:** You can mount both VMware guest tools and Nutanix Guest Tools at the same time on a particular VM provided the VM has sufficient empty CD-ROM slots.

- f. Click **Submit**.

The VM is registered with the NGT service. NGT is enabled and mounted on the selected virtual machine. A CD with volume label NUTANIX\_TOOLS gets attached to the VM.

**Note:**

- If you clone a VM, by default NGT is not enabled on the cloned VM. If the cloned VM is powered off, enable NGT from the UI and start the VM. If cloned VM is powered on, enable NGT from the UI and restart the Nutanix guest agent service.
- For information on how to enable NGT on multiple VMs simultaneously, see [Enabling NGT and Mounting the NGT Installer on Cloned VMs](#).

If you eject the CD, you can mount the CD back again by logging into the Controller VM and running the following nCLI command.

```
ncli> ngt mount vm-id=virtual_machine_id
```

For example, to mount the NGT on the VM with VM\_ID=00051a34-066f-72ed-0000-000000005400::38dc7bf2-a345-4e52-9af6-c1601e759987, type the following command.

```
ncli> ngt mount vm-id=00051a34-066f-72ed-0000-000000005400::38dc7bf2-a345-4e52-9af6-c1601e759987
```

**Caution:** In AOS 4.6, for the powered-on Linux VMs on AHV, ensure that the NGT ISO is ejected or unmounted within the guest VM before disabling NGT by using the web console. This issue is specific for 4.6 version and does not occur from AOS 4.6.x or later releases.

**Note:** If you have created the NGT ISO CD-ROMs prior to AOS 4.6 or later releases, the NGT functionality will not work even if you upgrade your cluster because REST APIs have been disabled. You must unmount the ISO, remount the ISO, install the NGT software again, and then upgrade to 4.6 or later version.

5. To launch a VM console window, click the **Launch Console** action link.

This opens a virtual network computing (VNC) client and displays the console in a new tab or window. This option is available only when the VM is powered on. The VM power options that you access from the **Power Off Actions** action link below the VM table can also be accessed from the VNC console window. To access the VM power options, click the **Power** button at the top-right corner of the console window.

**Note:** A VNC client may not function properly on all browsers. Some keys are not recognized when the browser is Google Chrome. (Firefox typically works best.)

- To start (or shut down) the VM, click the **Power on** (or **Power off**) action link.

Power on begins immediately. If you want to shut down the VMs, you are prompted to select one of the following options:

- Power Off.** Hypervisor performs a hard shut down action on the VM.
- Reset.** Hypervisor performs an ACPI reset action through the BIOS on the VM.
- Guest Shutdown.** Operating system of the VM performs a graceful shutdown.
- Guest Reboot.** Operating system of the VM performs a graceful restart.

**Note:** The **Guest Shutdown** and **Guest Reboot** options are available only when VMware guest tools are installed.

- To pause (or resume) the VM, click the **Suspend** (or **Resume**) action link. This option is available only when the VM is powered on.

- To clone the VM, click the **Clone** action link.

This displays the **Clone VM** dialog box, which includes the same fields as the **Create VM** dialog box. A cloned VM inherits the most configurations (except the name) of the source VM. Enter a name for the clone and then click the **Save** button to create the clone. You can optionally override some of the configurations before clicking the **Save** button. For example, you can override the number of vCPUs, memory size, boot priority, NICs, or the guest customization.

**Note:**

- You can clone up to 250 VMs at a time.
- In the Clone window, you cannot update the disks.

- To modify the VM configuration, click the **Update** action link.

The **Update VM** dialog box appears, which includes the same fields as the **Create VM** dialog box. Modify the configuration as needed, and in addition you can enable Flash Mode for the VM.

**Note:** If you delete a vDisk attached to a VM and snapshots associated with this VM exist, space associated with that vDisk is not reclaimed unless you also delete the VM snapshots.

- Select the **Enable Flash Mode** checkbox.

- » After you enable this feature on the VM, the status is updated in the VM table view. To view the status of individual virtual disks (disks that are flashed to the SSD), go the **Virtual Disks** tab in the VM table view.
- » You can disable the Flash Mode feature for individual virtual disks. To update the Flash Mode for individual virtual disks, click the update disk icon in the **Disks** pane and clear the **Enable Flash Mode** checkbox.

- To delete the VM, click the **Delete** action link. A window prompt appears; click the **OK** button to delete the VM.

The deleted VM disappears from the list of VMs in the table. You can also delete a VM that is already powered on.

# Configuring Images

In AHV clusters, you can import and configure operating system ISO and disk image files through the web console. You can also convert previously imported files to the format that AHV uses.

## About this task

You can use the image service feature to build a store of imported files that you can use to create a CD-ROM from an ISO image or an operating system disk from a disk image when creating a VM. The image service supports raw, VHD, VHDX, VMDK, ISO, and QCOW2 disk formats. Port 2007 must be open, since the image service uses port 2007. For the complete list of required ports, see [Port Reference](#).

Image create, update, and delete (CUD) behavior depends on whether a cluster (also known as Prism Element) is registered to Prism Central.

- Images created on a Prism Element reside on Prism Element and can be managed from Prism Element.
- For better centralized management, you can migrate images manually to Prism Central by using the image import feature in Prism Central. An image migrated to Prism Central in this way remains on Prism Element, but you can manage the image only from Prism Central. Migrated images cannot be updated from the Prism Element.
- In the case of a local image upload, with more than one Prism Element cluster managed by Prism Central, the image state is active on that Prism Element cluster. All other Prism Element clusters show the image as inactive. If you create a VM from that image, the image bits are copied to the other Prism Element clusters. The image then appears in an active state on all managed Prism Element clusters.

**Note:** After you upload a disk image file, the storage size of the image file in the cluster appears higher than the actual size of the image. This is because the image service in the cluster converts the image file to raw format which is required by AHV to create a VM from an image.

To import and configure an image file, follow these steps:

## Procedure

1. Log on to the Prism Element web console.
2. Click the gear icon in the main menu and then select **Image Configuration** in the **Settings** page.  
The **Image Configuration** window appears.
3. To upload an image file to the cluster, click the **Upload Image** button.  
The **Create Image** window appears. Do the following in the indicated fields:
  - a. **Name:** Enter a name for the image.
  - b. **Annotation** (optional): Enter a description for the image.
  - c. **Image Type** (optional): Select the image type, either **ISO** or **Disk**, from the pull-down list.
  - d. **Storage Container:** Select the storage container to use from the pull-down list.  
The list includes all storage containers created for this cluster. If there are no storage containers currently, a **Create Storage Container** link appears to create a storage container.
- e. **Image Source:** Do one of the following:
  - Click the **From URL** option to import the image from the Internet. Enter the appropriate URL address in the field using the following syntax for either NFS or HTTP. (NFS and HTTP are the only supported protocols.)  
`nfs://[hostname|IP_addr]/path`

```
http://[hostname|IP_addr]/path
```

Enter either the name of the host (*hostname*) or the host IP address (*IP\_addr*) and the path to the file. If you use a *hostname*, the cluster must be configured to point at a DNS server that can resolve that name. A file uploaded through NFS must have 644 permissions. For more information, see [Configuring Name Servers](#) on page 349.

If the image files have been copied to a container on the cluster, replace *IP\_addr* with CVM IP address.

For example, enter nfs://*CVM\_IP\_addr*/*container\_name*/*file\_name*.

Replace *CVM\_IP\_addr* with the CVM IP address, *container\_name* with the name of the container where the image is placed, and *file\_name* with the image file name.

To identify the NFS path to the VM disks of a VM, log on to any CVM in a cluster as Nutanix user. Run the following command to find the associated disk UUID.

```
nutanix@cvm$ accli vm.get <VM name> include_vmdisk_paths=1 | grep -E 'disk_list|vmdisk_nfs_path|vmdisk_size|vmdisk_uuid'
```

To construct the NFS path, append the VM disk path returned by the command to nfs://*CVM\_IP\_addr*. For example, if the command returns the path ContainerA.acropolis/vmdisk/9365b2eb-a3fd-45ee-b9e5-64b87f64a2df, then your NFS path is nfs://*CVM\_IP\_addr*/ContainerA.acropolis/vmdisk/9365b2eb-a3fd-45ee-b9e5-64b87f64a2df.

Replace *CVM\_IP\_addr* with the CVM IP address.

- Click the **Upload a file** option to upload a file from your workstation. Click the **Choose File** button and then select the file to upload from the file search window.

- f. When all the fields are correct, click the **Save** button.

The **Create Image** window closes and the **Image Configuration** window reappears with the new image appearing in the list.

4. To update the image information, click the pencil icon for that image.

The **Update Image** window appears. Update the fields as desired and then click the **Save** button.

**Note:** The pencil icon is unavailable for images imported to Prism Central. Use Prism Central to manage such images.

5. To delete an image file from the store, click the X icon for that image.

The image file is deleted and that entry disappears from the list.

## Virtual Machine Customization

In an Acropolis cluster, you can use Cloud-init to customize Linux VMs and the System Preparation (Sysprep) tool to customize Windows VMs.

### About Cloud-Init

Cloud-init is a utility that is used to customize Linux VMs during first-boot initialization. The utility must be pre-installed in the operating system image used to create VMs. Cloud-init runs early in the boot process and configures the operating system on the basis of data that you provide (user data). You can use Cloud-init to automate tasks such as setting a host name and locale, creating users and groups, generating and adding SSH keys so that users can log in, installing packages, copying files, and bootstrapping other configuration management tools such as Chef, Puppet, and Salt. For more information about Cloud-init, see <https://cloudinit.readthedocs.org/>.

### About Sysprep

Sysprep is a utility that prepares a Windows installation for duplication (imaging) across multiple systems. Sysprep is most often used to generalize a Windows installation. During generalization, Sysprep removes system-specific information and settings such as the security identifier (SID) and leaves installed applications untouched. You can

capture an image of the generalized installation and use the image with an answer file to customize the installation of Windows on other systems. The answer file contains the information that Sysprep needs to complete an unattended installation. For more information about Sysprep and answer files, see the Microsoft Sysprep documentation.

### The Customization Process in a Nutanix Cluster

You can use Cloud-init or Sysprep both when creating and when cloning VMs in a Nutanix cluster. For unattended provisioning, you can specify a user data file for Cloud-init and an answer file for Sysprep. All Cloud-init user-data formats are supported. For example, you can use the Cloud Config format, which is written in YAML, or you can provide a multi-part archive. To enable Cloud-init or Sysprep to access the script, AOS creates a temporary ISO image that includes the script and attaches the ISO image to the VM when you power on the VM.

**Note:** The ISO image is mounted on bus IDE 3, so ensure that no other device is mounted on that bus.

You can also specify source paths to the files or directories that you want to copy to the VM, and you can specify the target directories for those files. This is particularly useful if you need to copy software that is needed at start time, such as software libraries and device drivers. For Linux VMs, AOS can copy files to the VM. For Windows VMs, AOS can copy files to the ISO image that it creates for the answer file.

After customizing a VM, you can copy the VDisk of the VM to Image Service for backup and duplication.

## Customizing Linux Virtual Machines with Cloud-Init

Keep the user data file ready, either saved locally or uploaded to a storage container on the cluster. Alternatively, you can create or paste the script in the web console. If you want files copied to the VM during initialization, upload the files to a storage container on the cluster.

### About this task

To customize a Linux VM by using Cloud-init, do the following:

### Procedure

1. Log in to the web console by using the Nutanix credentials.
2. In the VM dashboard, do one of the following:
  - » To create a VM, click **Create VM**.
  - » To clone a VM, click the VM that you want to clone, and then click **Clone**.
3. In the **Create VM** or **Clone VM** dialog box, specify a name for the VM and allocate resources such as vCPUs, memory, and storage. Select the **Custom Script** check box and specify how you want to customize the VM.

For information about creating a VM and specifying customization options, see [Creating a VM \(AHV\)](#) on page 270. For information about cloning a VM, see [Managing a VM \(AHV\)](#) on page 276.

For information about using cloud-init custom script, see [Cloud-Init Limitations and Guidelines](#) on page 294 and [Cloud-init Sample Scripts](#) on page 295.

4. In the VM dashboard, select the VM, and then click **Power On**.

The VM is powered on and initialized based on the directives in the user data file. To create a reference image from the VM, use Image Service. For more information about Image Service, see [Configuring Images](#).

### Cloud-Init Limitations and Guidelines

- Nutanix supports a maximum of 32 KB for the size of a VM guest customization script.
- AHV supports guest customization through cloud-init using Config Drive v2 datasource (see [Cloud-init documentation](#)). For more information, see the example cloud-init scripts for network configuration.

## Cloud-init Sample Scripts

The following are a few sample cloud-init scripts that you can use to customize the VMs.

### Script for setting up a static IP configuration (CentOS)

On CentOS, you can inject the static IP configuration in the cloud-init script by editing the network interface configuration file located in /etc/sysconfig/network-scripts directory with a *write\_files* block as shown in the following example:

```
#cloud-config

disable_root: False
cloud_config_modules:
- resolv_conf

# Set the hostname
hostname: host_name
fqdn: host_name.domain_name

# User Authentication
users:
- default
- name: linux.username
  ssh-authorized-keys:
  - public_key
  sudo: ['ALL=(ALL) NOPASSWD:ALL']

# Assign static IP address
write_files:
- path: /etc/sysconfig/network-scripts/ifcfg-eth0
  content: |
    IPADDR=vm_ip
    NETMASK=vm_subnet_mask
    GATEWAY=vm_gateway
    BOOTPROTO=static
    ONBOOT=yes
    DEVICE=eth0

# Configure resolv.conf
manage_resolv_conf: true
resolv_conf:
  nameservers: ['dns1','dns2']
  domain: 'domain_name'
  options:
    attempts: 5
    timeout: 15

# Run the boot commands
runcmd:
- [sudo, ifdown, eth0]
- [sudo, ifup, eth0]
- [sudo, systemctl, restart, network]
- [sudo, systemctl, mask, cloud-init-local, cloud-init, cloud-config, cloud-final]
- [eject]

# Enable automatic package upgrade
package_upgrade: true

# Specify power state
power_state:
  delay: "+1"
```

```

mode: reboot
message: Rebooting after cloud-init
timeout: 30
condition: True

```

Variable used in the script	Value
<code>host_name</code>	hostname of the VM
<code>host_name.domain_name</code>	host name of the VM and domain name joined by a dot (.)
<code>linux.username</code>	Linux username
<code>public_key</code>	Public Key
<code>vm_ip</code>	IP address of the VM
<code>vm_subnet_mask</code>	Subnet mask of the VM
<code>vm_gateway</code>	Default gateway of the VM
<code>dns1</code>	Primary DNS address
<code>dns2</code>	Secondary DNS address
<code>domain_name</code>	Domain name

### Script for setting up a static IP configuration (Ubuntu)

Unlike CentOS, Ubuntu uses *netplan* for network interface configuration, so you need to edit the /etc/netplan/50-cloud-init.yaml file and then run the netplan apply command through cloud-init script as shown in the following example:

```

#cloud-config
apt_upgrade: true
repo_update: true
repo_upgrade: all

# Set the hostname
hostname: host_name

# User Authentication
users:
  - default
  - name: ubuntu
    groups: sudo
    shell: /bin/bash
    lock_passwd: false
    ssh-authorized-keys:
      - public_key
    sudo: [ "ALL=(ALL) NOPASSWD:ALL" ]
chpasswd:
  list: |
    ubuntu:user_password
  expire: false

# Assign static IP address
write_files:
  - path: /etc/netplan/50-cloud-init.yaml
    content: |
      network: |
        version: 2
        renderer: networkd

```

```

ethernets:
    ens3:
        addresses: [vm_ip/netmask_bit]
        gateway4: vm_gateway
        nameservers:
            addresses: [dns1,dns2]

# Run the commands to add packages and resize the root partition
runcmd:
    - netplan apply
packages:
    - git
    - wget
    - curl
    - unzip
    - tar
    - python3
    - cloud-guest-utils
growpart:
    mode: auto
    devices: ['/']
    ignore_growroot_disabled: false

# Specify power state
power_state:
    delay: "+1"
    mode: reboot
    message: Rebooting after cloud-init
    timeout: 30
    condition: True

```

Variable used in the script	Value
host_name	hostname of the VM
public_key	Public Key
user_password	Password for the user
vm_ip	IP address of the VM
netmask_bit	Netmask bit such as 24 or 32
vm_gateway	Default gateway of the VM
dns1	Primary DNS address
dns2	Secondary DNS address

### Script for setting up a static IP configuration (RHEL 9)

If your Linux distribution is using *NetworkManager* (as is the case with RHEL9), you need to use several nmcli commands in the cloud-init *runcmd* block to configure the static IPV 4 on your network interface as shown in the following example:

```

#cloud-config
apt_upgrade: true
repo_update: true
repo_upgrade: all

# Set the hostname
hostname: host_name

```

```

# User Authentication
users:
  - default
  - name: rhel
    groups: sudo
    shell: /bin/bash
    lock_passwd: false
    ssh-authorized-keys:
      - public_key
    sudo: [ "ALL=(ALL) NOPASSWD:ALL" ]
chpasswd:
  list: |
    rhel: user_password
  expire: false

# Assign static IP address
runcmd:
  - nmcli connection migrate
  - nmcli con down "System eth0"
  - nmcli con del "System eth0"
  - nmcli con add con-name "System eth0" ifname eth0 type ethernet
  ip4 vm_ip/netmask_bit gw4 vm_gateway ipv4.dns "dns1 dns2"
  - nmcli con up "System eth0"
  - nmcli general reload
  - nmcli connection reload

# Run the commands to add packages and resize the root partition
packages:
  - git
  - wget
  - curl
  - unzip
  - tar
  - python3
  - cloud-guest-utils
growpart:
  mode: auto
  devices: ['/']
  ignore_growroot_disabled: false

# Specify power state
power_state:
  delay: "+1"
  mode: reboot
  message: Rebooting after cloud-init
  timeout: 30
  condition: True

```

#### Variable used in the script

#### Value

<code>host_name</code>	hostname of the VM
<code>public_key</code>	Public Key
<code>user_password</code>	Password for the user
<code>vm_ip</code>	IP address of the VM
<code>netmask_bit</code>	Netmask bit such as 24 or 32
<code>vm_gateway</code>	Default gateway of the VM

Variable used in the script	Value
<code>dns1</code>	Primary DNS address
<code>dns2</code>	Secondary DNS address

## Customization of Windows Virtual Machines with System Preparation

To customize a Windows VM by using Sysprep, follow these steps:

- Create a reference image by using Sysprep.

**Note:** Starting with AOS 7.0, the network adapter name of the vNIC on a Windows VM is **Ethernet Instance 0**. Apply this change when creating or customizing a new VM using the reference image.

- Create a VM from the reference image.

You can also customize a VM when performing a fresh installation of Windows with an ISO file.

If you require unattended provisioning, keep the answer file ready, either saved locally or uploaded to a storage container on the cluster. Alternatively, you can create or paste the script in the Prism Element web console. If you have files that must be copied to a temporary ISO image, upload the files to a storage container on the cluster.

### Preparing a VM to Create a Reference Image

Creating a reference image requires knowledge of Sysprep. For information about how to use Sysprep, see the Sysprep documentation on the Microsoft TechNet website.

### About this task

To create a reference image, follow these steps:

#### Procedure

1. Log in to the web console by using the Nutanix credentials, and then browse to the VM dashboard.
2. Select the VM that you want to clone, click **Launch Console**, and then log in to the VM with administrator credentials.
3. Configure Sysprep with the system cleanup action of your choice, specify whether or not you want to generalize the installation, and then choose to shut down the VM.

- Open the command prompt as an administrator and navigate to the sysprep folder.

```
cd C:\windows\system32\sysprep
```

- Generalize the installation and then shut down the VM.

```
C:\Windows\system32\sysprep>sysprep /generalize /shutdown /oobe
```

The VM shuts down automatically.

**Note:** Make sure to shut down the VM. Restarting the VM results in the VM losing its generalized state and in Sysprep attempting to find an answer file that has not been provided yet. For the same reasons, until you have completed this procedure, do not start the VM.

4. Create a reference image from the VM by using Image Service. For more information, see [Configuring Images](#) on page 292.

## **Creating a Customized Virtual Machine from a Reference Image**

### **About this task**

To use a reference image, follow these steps:

### **Procedure**

1. Log in to the web console by using the Nutanix credentials, and then browse to the VM dashboard.
2. Click **Create VM**, and then, in the **Create VM** dialog box, follow these steps:
  - a. Specify a name for the VM and allocate resources such as vCPUs, memory, and storage.
  - b. Click **Add new disk**, select the **Clone from Image Service** operation, and select the Windows reference image that you copied to Image Service.
  - c. Click the **Custom Script** check box and specify how you want to customize the VM.
- For more information about creating a VM, see [Creating a VM \(AHV\)](#) on page 270.

3. In the VM dashboard, select the VM, and then click **Power On**.

The VM is powered on and initialized based on the directives in the answer file. To create a reference image from the VM, use Image Service. For more information about Image Service, see [Configuring Images](#).

### **Customizing a Fresh Installation**

You can perform a fresh installation only if you attach an empty vDisk and an installation CD-ROM to the VM. If you specify an image from Image Service or ADSF, for use as a vDisk, the VM is created from that image, and the install is no longer a fresh install.

### **About this task**

To customize a fresh installation of Windows by using Sysprep, follow these steps:

### **Procedure**

1. Log in to the web console by using the Nutanix credentials, and then browse to the VM dashboard.
2. Click **Create VM**, specify the details that are required for installing Windows on the new VM, and then follow these steps:
  - a. Specify a name for the VM and allocate resources such as vCPUs, memory, and storage.
  - b. In the **Disks** area, click the edit button that is provided against the default CD-ROM entry. In the **Update Disk** dialog box, select the operation (**Clone from ADSF File** or **Clone from Image Service**), and then specify the image that you want to use. Click **Update**.
  - c. Click **Add new disk**. Allocate space for a new disk on a storage container, and then click **Add**.
  - d. Click the **Custom Script** check box and specify how you want to customize the VM.
- For more information on creating a VM, see [Creating a VM \(AHV\)](#) on page 270.

3. In the VM dashboard, select the VM, and then click **Power On**.

The VM is powered on and initialized based on the directives in the answer file. To create a reference image from the VM, use **Image Service**. For more information on **Image Service**, see [Configuring Images](#).

## **VM High Availability in Acropolis**

Acropolis uses the segment-based reservation method to enable guaranteed VM High Availability (HA). Acropolis no longer supports the deprecated host-based reservation method.

By default, AHV provides best-effort HA where it does not reserve resources. In case of a host failure, Acropolis attempts to restart the affected VMs on any available space on the other hosts in the cluster. Once the failed host restores and rejoins the cluster, Acropolis migrates the VMs back. This mode does not enforce admission control and therefore cannot guarantee that sufficient capacity is available to start all VMs.

**Note:**

- For HA to protect a VM, it must have at least one virtual disk (vDisk) present in a Nutanix storage container.
- The VM HA does not reserve memory for non-migratable VMs. For information on how to check the non-migratable VMs, see [Checking Live Migration Status of a VM](#) in the *Prism Central Infrastructure Guide*.

To provide guaranteed restarts when you enable HA, Acropolis uses the segment-based reservation method (Guarantee mode).

In segment-based reservation, the scheduler divides the cluster into segments to ensure that it reserves enough space for any host failure. Each segment corresponds to the largest VM that it guarantees to restart in case a failure occurs. The other factor is the number of host failures that the cluster can tolerate. Using these inputs, the scheduler implements admission control to always have enough resources reserved so that it can restart the VMs upon failure of any host in the cluster.

The segment size ensures that Acropolis can power on the largest VM in an HA failover when the cluster is fully loaded (except for the reserved segments). Acropolis reserves enough segments to ensure it can tolerate the failure of any host in the cluster. Multiple VMs may fit into a segment. If anything changes in the cluster, Acropolis recomputes the reservation. The total resources reserved for segments can be more than the resources used by running VMs.

This implementation guarantees successful failover even in the case of segment fragmentation. The actual number of reserved resources depends on the current load of the cluster, but it is typically at 1 to 1.25 times the resource usage on the most loaded host.

If the host enters maintenance mode (for a host upgrade), the cluster might not be protected against further host failures. Maintenance mode uses the HA reservation to migrate VMs from the host. Although the cluster is not protected against a host failure during this time, a hypervisor upgrade occurs without any difficulty because Acropolis migrates the VMs instead of restarting them, which preserves their runtime state. The HA status goes through the same states as it would during an actual host failure.

### Fault Detection for High Availability

Acropolis version 6.1 (with minimum supported AHV version 20201105.2229) onwards, the fault detection mechanism for High Availability checks for the heartbeat of the management services on the host. If any one of the services are down, then the host is marked as disconnected.

In addition to this, the fault detection mechanism also performs the following health checks for the host:

- Root file system corruption
- Read-only root file system

If any of the above-mentioned health checks are affirmative, then the host is marked as disconnected.

If the host remains in the disconnected status for 40 seconds, the VMs running on the affected host are automatically restarted (based on the resource availability) .

You can view the alerts raised for any of the above-mentioned checks in the **Activity > Alerts** view in Prism UI.

### Enabling High Availability Reservations for the Cluster

In Acropolis managed clusters, you can enable high availability reservations for the cluster to ensure that VMs can be migrated and restarted on another host in case of failure.

## About this task

After you enable high availability for the cluster, if a host failure occurs the cluster goes through following changes.

- OK: This state implies that the cluster is protected against a host failure.
- Healing: Healing period is the time that Acropolis brings the cluster to the protected state. There are two phases to this state. The first phase occurs when the host fails. The VMs are restarted on the available host. After restarting all the VMs if there are enough resources to protect the VM, the HA status of the cluster comes back to OK state. If this does not occur, the cluster goes into critical state. The second phase occurs when the host comes back from the failure. Once the host comes back from failure, no VMs are present on the host and hence during this healing phase restore locality task occurs (VMs are migrated back). Apart from restoring the locality of the VMs, the restore locality task ensures that the cluster is back to the same state before the HA failure. Once it is finished, the HA status is back to OK state.
- Critical: If the host is down, the HA status of the cluster goes into Critical state. This happens because the cluster cannot tolerate any more host failures. You have to ensure that you bring back the host so that your cluster is protected against any further host failures.

**Note:** On a less loaded cluster, it is possible for HA to go directly back to OK state if enough resources are reserved to protect another host failure. The start and migrate operations on the VMs are restricted in the Critical state because Acropolis continuously tries to ensure that the HA status is back to the OK state.

## Procedure

1. Log in to the Prism Element web console.
2. Click the gear icon in the main menu and then select **Manage VM High Availability** in the **Settings** page.

**Note:** This option does not appear in clusters that do not support this feature.

The **Manage VM High Availability** dialog box appears.

3. Check the **Enable HA Reservation** box and then click the **Save** button to enable.

## Nutanix Guest Tools

Nutanix Guest Tools (NGT) is a software package that comes bundled with AOS. You can install NGT in a guest virtual machine (VM) to enable advanced VM management functionalities provided by Nutanix.

For more information about NGT and the various NGT features, see [Nutanix Guest Tools Overview](#) in the *Prism Central Guide*.

Prism Element web console does not support automatic installation of NGT. You must log in to a VM to manually install NGT in that VM. Nutanix recommends that you use Prism Central to install NGT automatically in the VMs. For more information, see [Installing NGT](#) in the *Prism Central Guide*.

To set up NGT through the Prism Element web console, you must do the following:

1. Enable NGT for a VM in the Prism Element web console.

When you enable NGT for a VM, Prism Element prepares the VM so that you can successfully install NGT and use the NGT features in that VM.

2. Mount the NGT installer (ISO disk file) in a VM.
3. Install NGT in a VM.

## Enabling NGT and Mounting the NGT Installer in a VM

By default, the NGT feature is disabled for a guest VM running in a Nutanix cluster. To install and use the NGT feature in a VM, you must first enable the NGT feature (allow the installation and usage of NGT) for the VM, then mount the NGT installer in that VM using the Prism Element web console.

### Before you begin

Ensure that all the NGT requirements are met. For more information, see [Nutanix Guest Tools Requirements](#) in the *Prism Central Guide*.

### About this task

When you are enabling the NGT feature and mounting the NGT installer in a VM, you must also select the NGT applications (self-service restore, volume snapshot service, and application-consistent snapshots) that you want to use in that VM.

Perform the following steps to enable the NGT feature, mount the NGT installer, and select the NGT applications that you want to use in a VM using the Prism Element web console.

**Note:** You can install both VMware guest tools and NGT in a VM because NGT is designed to install alongside VMware guest tools.

### Procedure

1. Log in to the Prism Element web console.
2. In the dropdown list of the main menu, select **VM**.
3. From the VM page, select the **Table** view.
4. Select the VM for which you want to enable NGT and click **Manage Guest Tools**.
5. In the **Manage VM Guest Tools** window, select the **Enable Nutanix Guest Tools** checkbox.  
Selecting this checkbox displays the options to mount the NGT installer, and to select the NGT applications that you want to use in the VM.
6. Perform the following in the indicated fields:
  - a. **Mount Nutanix Guest Tools**: Select this checkbox to mount the NGT installer in the selected VM.
  - b. **Self Service Restore (SSR)**: Select this checkbox to enable the self-service restore feature for Windows VMs.  
For more information about the self-service restore feature, see [Self-Service Restore](#) in the *Data Protection and Recovery with Prism Element* guide.
  - c. **Volume Snapshot Service / Application Consistent Snapshots (VSS)**: This checkbox is selected by default when you select the **Enable Nutanix Guest Tools** checkbox.  
This feature enables the Nutanix native in-guest Volume Snapshot Service (VSS) agent to take application-consistent snapshots for all the VMs that support VSS. For more information, see [Conditions for Application-consistent Snapshots](#) in the *Data Protection and Recovery with Prism Element* guide.
- d. Click **Submit**.  
Prism Element enables the NGT feature, mounts the NGT installer, and attaches the NGT installation media with the volume label NUTANIX\_TOOLS to the selected VM.

7. To verify whether NGT is enabled and the NGT installer is mounted successfully on a guest VM, do the following from the Prism Element web console:
  - a. In the dropdown list of the main menu, select **VM**.
  - b. From the VM page, select the **Table** view.
  - c. Select the desired VM.
  - d. Under **VM DETAILS**, check the **NGT Enabled**, and **NGT Mounted** fields.

If NGT is enabled and the NGT installer is mounted successfully, the respective fields display the status **Yes**.

**Note:**

- NGT is not enabled on a cloned VM by default. For more information, see [Enabling NGT and Mounting the NGT Installer on Cloned VMs](#).
- For information about troubleshooting any NGT-related issues, see [KB-3741](#).

### What to do next

Install NGT in the guest VM by following the instructions in [NGT Installation](#).

## NGT Installation

Prism Element web console does not support automatic installation of NGT. You must log in to a VM to manually install NGT in that VM.

**Note:**

- You can install NGT on up to 1,500 VMs in a cluster. If you exceed this limit, migrate or delete the extra VMs to return to the supported limits.
- You cannot install NGT on VMs created on storage containers with replication factor 1.

### Installing NGT on a Windows VM

#### Before you begin

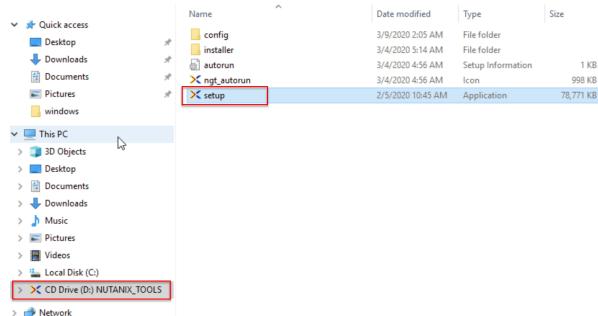
Ensure that the following prerequisites are met:

- All the NGT requirements are met. For more information, see [Nutanix Guest Tools Requirements](#) in the *Prism Central Guide*.
- NGT is enabled in the selected VM and the NGT installer is mounted on the selected VM. For more information, see [Enabling NGT and Mounting the NGT Installer in a VM](#).

#### Procedure

1. Log in to the Windows VM.
2. Open File Explorer and click the CD drive with the `NUTANIX_TOOLS` label from the left navigation pane.

- From the right pane that displays all the files and sub-folders in the drive, double-click the setup.exe file.



**Figure 49: Start NGT Installation on Windows**

**Note:** If you mount the NGT installer while the VM is powered off, the CD drive might not display the NUTANIX\_TOOLS label after you power on the VM. You must open the CD drive, and double-click the setup.exe file.

- Accept the license agreement and follow the prompts to install NGT in the virtual machine.  
A Setup Successful message appears if NGT is successfully installed.
- After you install NGT in a Windows VM, the Nutanix Guest Agent (NGA) service in the VM starts periodic communication with the CVM. To verify whether the NGA service is communicating with the CVM, log in to the CVM and run the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true  
vm_name=vm-name
```

Replace `vm-name` with the name of the Windows VM.

In the command output, `communication_link_active = true` indicates that the NGA is communicating with the CVM.

**Note:** For information about troubleshooting any NGT-related issues, see [KB-3741](#).

### Installing NGT on a Windows VM (Silent Install)

The NGT installer package allows you to manually install NGT on a Windows VM, in the background, without affecting normal VM operations.

#### Before you begin

Ensure that the following prerequisites are met:

- All the NGT requirements are met. For more information, see [Nutanix Guest Tools Requirements](#) in the *Prism Central Guide*.
- NGT is enabled in the selected VM and the NGT installer is mounted on the selected VM. For more information, see [Enabling NGT and Mounting the NGT Installer in a VM](#).

#### About this task

Perform the following procedure to install NGT using the NGT silent installer package.

**Note:**

- Add the commands mentioned in the following procedure to a custom script and run the script to install NGT on multiple Windows VMs. However, you might need to restart the VM after NGT is installed for the updated functionalities to be available in the VM.
- For information about the contents included in the NGT silent installer package, see [Nutanix Guest Tools Overview](#) in the *Prism Central Guide*.

## Procedure

1. Open the command prompt and go to the drive on which the NGT installer is mounted.
2. Install NGT using the installer package by running either of the following commands:

```
» $ setup.exe /quiet ACCEPTEULA=yes /norestart
```

Use this command to ensure that VMs are not restarted after installing NGT.

**Note:** This command updates the Nutanix VirtIO drivers to the latest version, but the updated functionality of the VirtIO drivers is available only after a VM restart. For more information about VirtIO drivers, see [Nutanix VirtIO for Windows](#) in *AHV Administration Guide*.

```
» $ setup.exe /quiet ACCEPTEULA=yes
```

Use this command to restart the VM and for all the updated VirtIO driver functionalities to be available in the VM. For more information about VirtIO drivers, see [Nutanix VirtIO for Windows](#) in *AHV Administration Guide*.

By default, NGT logs are generated in **Event Viewer** and in the %TEMP% directory starting with *Nutanix\_Guest\_Tools\_timestamp*. Event Viewer log files are created for all the components as part of the NGT installation.

### Note:

- NGT installation on guest VMs running on AHV might require a VM restart if the VirtIO drivers are updated during the installation whereas NGT installation on guest VMs running on ESXi does not require a VM restart because the installed VirtIO drivers are not active until the VM moves to AHV. For more information about VirtIO drivers, see [Nutanix VirtIO for Windows](#) in *AHV Administration Guide*.
- The NGT installer has some built-in checks (for example, if the VSS service is disabled or if KB2921916 Windows update is installed inside Windows 7/Windows Server 2008R2) that are treated as warnings during an interactive installation of NGT. However, these checks are deemed as errors during a silent installation. To ignore these errors and proceed with the silent installation, use the IGNOREALLWARNINGS=yes flag. For example, drive:> setup.exe /quiet ACCEPTEULA=yes IGNOREALLWARNINGS=yes.

3. (Optional) If you want the NGT logs to be generated in a location other than the %TEMP% directory, install NGT by running the following command.

```
$ setup.exe /quiet ACCEPTEULA=yes -log log_path
```

Replace *log\_path* with the path where you want to create the log files.

Logs are generated in the path that you provide. Ensure that the path you provide has the necessary write permissions. Also, some events are added to the Windows Application Event Log.

**Note:** For information on troubleshooting any NGT related issues, see [KB-3741](#) available on the Nutanix support portal.

- After you install NGT in a Windows VM, the Nutanix Guest Agent (NGA) service in the VM starts periodic communication with the CVM. To verify whether the NGA service is communicating with the CVM, log in to the CVM and run the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true  
vm_name=vm-name
```

Replace `vm-name` with the name of the Windows VM.

In the command output, `communication_link_active = true` indicates that the NGA is communicating with the CVM.

**Note:** For information about troubleshooting any NGT-related issues, see [KB-3741](#).

## Installing NGT on a Linux VM

### Before you begin

Ensure that the following prerequisites are met:

- All the NGT requirements are met. For more information, see [Nutanix Guest Tools Requirements](#) in the *Prism Central Guide*.
- NGT is enabled in the selected VM and the NGT installer is mounted on the selected VM. For more information, see [Enabling NGT and Mounting the NGT Installer in a VM](#).

### About this task

Some Linux deployments auto-discover the CD-ROM and mount the CD-ROM appropriately. Some of the following steps might be optional for your VM.

### Procedure

- Log in to the Linux VM.
- Run one of the following to determine the device in which the NUTANIX\_TOOLS CD is inserted:

- `$ blkid -L NUTANIX_TOOLS`
- `$ lsblk -o NAME,LABEL`

The second command displays a list of directories. You must look for a directory with the label `NUTANIX_TOOLS`.

- Create a temporary directory if a target mount point does not exist and mount the content of the CD in the temporary directory that you created by running the following command:

```
$ sudo mount /dev/device target-mount-point /mnt
```

Replace `device` with the device that you determined in Step 2, for example, `sr0` or `sr1`, and replace `target-mount-point` with the name of the directory where the content of the CD should be mounted.

**Note:** On some Linux distributions, it is appropriate to use `/mnt` or a specific directory created under `/mnt`.

4. Install NGT by running the following command:

```
$ sudo python target-mount-point/installer/linux/install_ngt.py --operation install
```

Replace *target-mount-point* with the name of the directory where the content of the CD is mounted.

Output similar to the following is displayed.

```
[root@localhost linux]# python install_ngt.py --operation install
Downloading packages:
Public key for nutanix-guest-agent-4.0-1.x86_64.rpm is not installed
Retrieving key from file:///tmp/cdrom/installer/linux/ngt_rpm_installer/RPM-GPG-
PUBLIC-KEY
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Pre: RPM is getting installed
Installing : nutanix-guest-agent-4.0-1.x86_64 1/1
Post: RPM is getting installed.
Running installer utility script.
INFO: Setting up Nutanix Guest Tools - VM mobility drivers.
INFO: Successfully set up Nutanix Guest Tools - VM mobility drivers.
INFO: Creating desktop shortcuts...
Restarting ngt_guest_agent.service systemctl service...
ngt_guest_agent.service service restart done.
Restarting ngt_self_service_restore.service systemctl service...
ngt_self_service_restore.service service restart done.
    Verifying: nutanix-guest-agent-4.0-1.x86_64 1/1
Installed:
  nutanix-guest-agent.x86_64 0:4.0-1
[root@localhost linux]#
```

5. Verify whether the Nutanix Guest Agent (NGA) service is installed in the VM by running the command based on your package management tool.

The following is an example of the command for the YUM package management tool.

```
$ sudo yum list installed | grep 'nutanix-guest-agent'
```

Output similar to the following is displayed.

```
[root@localhost linux]# sudo yum list installed | grep 'nutanix-guest-agent'
Failed to set locale, defaulting to C
nutanix-guest-agent.x86_64           4.0-1                               @nutanix-
ngt-20230524223422
[root@localhost linux]#
```

6. After you install NGT in a Linux VM, the Nutanix Guest Agent (NGA) service in the VM starts periodic communication with the CVM. To verify whether the NGA service is communicating with the CVM, log in to the CVM and run the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true
  vm_name=vm-name
```

Replace *vm-name* with the name of the Linux VM.

In the command output, *communication\_link\_active = true* indicates that the NGA communicates with the CVM.

**Note:** For information about troubleshooting any NGT-related issues, see [KB-3741](#).

## Manage Bulk Operations for NGT

You can install or upgrade NGT in bulk on multiple guest virtual machines (VMs) using third-party endpoint management tools, such as Microsoft Intune or HCL BigFix, or automation tools, such as Ansible. Using these management tools, you can also remove NGT in bulk from guest VMs.

Bulk installation of NGT is supported on guest VMs running AOS 6.7 or later versions only.

The [Nutanix Support portal](#) lists the following NGT installer files:

- EXE file for Windows OS
- TGZ file for RPM-based Linux OS
- TGZ file for DEB-based Linux OS
- Nutanix NGT GnuPG public key

Download the latest installer files to install or upgrade NGT in bulk.

**Note:** Bulk installation of NGT using third-party endpoint management tools does not require Prism Element web console. However, you must enable and mount NGT in guest VMs using Prism Element web console after installing NGT in VMs. For more information, see [Enable and Configure NGT](#).

### Prepare the NGT installation files for Distribution

You can install NGT using the installer files available in the [Nutanix Support portal](#) in a single VM or, in bulk, on multiple VMs. When you prepare to install NGT in bulk on multiple VMs, download the installer files and make them available for use by the third-party endpoint management tool deployed at your site. The instructions in this document assume that the third-party endpoint management tool deployed at your site requires that you host the NGT installer files on a web server.

#### Hosting the files for Windows VMs

##### Before you begin

Ensure that the NGT version is compatible with the AOS version installed in your cluster.

##### Procedure

1. Go to the Nutanix Support portal, select **Downloads > NGT**, and download the *nutanix-guest-agent-<version>.exe* installer file for Windows, which matches the AOS version installed in your clusters.
2. Host this installation file directly on the web server.

#### Hosting the files for Red Hat Package Manager (RPM) based VMs

##### Before you begin

Ensure that the NGT version is compatible with the AOS version installed in your cluster.

##### Procedure

1. Go to the Nutanix Support portal, select **Downloads > NGT**, and download the *nutanix-guest-agent-rpm-<version>.tar.gz* installer file for RPM-based distributions, which matches the AOS version installed in your clusters.
2. Extract the *nutanix-guest-agent-rpm-<version>.tar.gz* file, and host the *NUTANIX-NGT-GPG-KEY* file and the *ngt\_repo* directory on the web server.

## Hosting the files for Debian (DEB) based VMs

### Before you begin

Ensure that the NGT version is compatible with the AOS version installed in your cluster.

### Procedure

1. Go to the Nutanix Support portal, select **Downloads > NGT**, and download the *nutanix-guest-agent-deb-<version>.tar.gz* installer file for DEB-based distributions, which matches the AOS version installed in your clusters.
2. Extract the *nutanix-guest-agent-deb-<version>.tar.gz* file, and host the i386 and amd64 directories on the web server.
3. (Optional) Perform the following steps to verify the DEB installer packages against the detached signatures using the *NUTANIX-NGT-GPG-KEY* file:
  - a. Run the following command to import the public key:

```
$ gpg --import NUTANIX-NGT-GPG-KEY
```

The following is an example.

```
$ gpg --import NUTANIX-NGT-GPG-KEY
gpg: key 42DBF8BB: public key "Nutanix, Inc. (NGT Packaging)
<security@nutanix.com>" imported
gpg: Total number processed: 1
gpg:                      imported: 1 (RSA: 1)
```

- b. Run the following command to verify the DEB installer packages against the detached signatures:

```
$ gpg --verify os-arch/nutanix-guest-agent.deb.asc os-arch/nutanix-guest-
agent_version-1_os-arch.de
```

Replace *os-arch* with the architecture of the OS of guest VM, and *version* with the NGA version.

The following is an example.

```
$ gpg --verify i386/nutanix-guest-agent.deb.asc i386/nutanix-guest-
agent_4.0-1_i386.deb
gpg: Signature made Wed 24 May 2023 01:46:29 PM UTC using RSA key ID 42DBF8BB
gpg: Good signature from "Nutanix, Inc. (NGT Packaging) <security@nutanix.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:                 There is no indication that the signature belongs to the owner.
Primary key fingerprint: D8B0 18BD CFEB 774C D157 F0A5 11B1 600F 42DB F8BB
```

## Install NGT in Bulk on Multiple VMs

You can install NGT in bulk on multiple Windows and Linux guest VMs using the NGT installer files available in the [Nutanix Support portal](#).

### Installing NGT in Bulk on Windows VMs

#### Before you begin

- Ensure that the cluster meets all NGT requirements. For more information, see [Nutanix Guest Tools Requirements](#) in the *Prism Central Infrastructure Guide*.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

- Review the end user license agreement (EULA) for Nutanix Guest Tools using a manual installation because the following installation procedure requires you to accept the EULA automatically.

## Procedure

1. Configure the third-party endpoint management tool deployed at your site to distribute the *nutanix-guest-agent-<version>.exe* file to the VMs where NGT is installed.

For more information, see the tool-specific documentation.

2. Configure the third-party endpoint management tool to install NGT by running one of the following commands:

```
» C:\ngtinstaller> nutanix-guest-agent-<version>.exe /quiet ACCEPTEULA=yes /norestart
```

Replace *version* with the NGA version.

Use this command to ensure that VMs do not restart after you install NGT.

**Note:** This command might update the Nutanix VirtIO drivers if no Nutanix VirtIO drivers are installed or if a newer version is available, but the updated functionality of the VirtIO drivers is available only after a VM restart.

```
» C:\ngtinstaller> nutanix-guest-agent-<version>.exe /quiet ACCEPTEULA=yes
```

Replace *version* with the NGA version.

Use this command to automatically restart the VM and to make all the updated VirtIO driver functionalities to be available in the VM.

3. (Optional) To generate the NGT logs in a location other than the %TEMP% directory, install NGT by running the following command.

```
C:\ngtinstaller> nutanix-guest-agent-<version>.exe /quiet ACCEPTEULA=yes /log log_file
```

Replace *version* with the NGA version, and *log\_file* with the filename to write the logs.

Ensure that the directory containing the filename that you provide has the necessary write permissions. Also, the installation process adds some events to the Windows application event log.

## What to do next

After successful installation, enable and configure NGT in guest VMs. For more information, see [Enable and Configure NGT](#).

## Installing NGT in Bulk on Linux VMs

### About this task

This sample procedure provides steps to install NGT on Red Hat Package Manager (RPM) based operating systems. Use this procedure as a template to install NGT on Debian-based operating systems.

### Before you begin

- Ensure that the cluster meets all NGT requirements. For more information, see [Nutanix Guest Tools Requirements](#) in the *Prism Central Infrastructure Guide*.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

## Procedure

1. To verify the package signatures, configure the third-party endpoint management tool deployed at your site to install the NUTANIX-NGT-GPG-KEY file on RPM-based operating systems.

For more information, see the tool-specific documentation.

2. Configure the third-party endpoint management tool to set up the repositories.

For more information, see the tool-specific documentation.

For example, guest VMs running RedHat 8.x distribution might need a repository configuration in /etc/yum.repos.d/nutanix-guest-tools.repo similar to the following configuration:

```
[NutanixGuestTools]
name=Nutanix Guest Tools
baseurl=http://local-web-server/ngt_repo
enabled=1
gpgcheck=1
gpgkey=http://local-web-server/RPM-GPG-PUBLIC-KEY
repo_gpgcheck=0
```

Replace *local-web-server* with the name of the web server used to distribute the NGT installer files as described in [Preparing the NGT installation files for the Distribution](#).

3. Configure the third-party endpoint management tool to install the Nutanix guest agent package by running the package manager-specific install command.

For example, the yum install -y nutanix-guest-agent command installs Nutanix guest agent package using the yum package manager for RedHat-based distributions.

```
[nutanix@localhost ~]$ yum install -y nutanix-guest-agent
```

For information about the install command specific to the package manager at your site, see the package manager-specific documentation.

## What to do next

After successful installation, enable and configure NGT in guest VMs. For more information, see [Enable and Configure NGT](#).

## Enable and Configure NGT

Use Prism Element web console to enable and configure NGT in VMs so that you can use the NGT applications such as self-service restore, volume snapshot service, and application-consistent snapshots. The initial configuration of NGT requires mounting an ISO into the CD-ROM drive of guest VMs. The NGT agent detects the ISO and performs the initial configuration, making connections to the CVM.

### Enabling and Configuring NGT using the Prism Element Web Console

## Procedure

- Mount NGT on guest VMs by performing Step 1 to Step 6 in [Enabling NGT and Mounting the NGT Installer in a VM](#) on page 303.

## What to do next

The Nutanix Guest Agent (NGA) service in the VMs starts periodic communication with the CVM. To verify whether the NGA service is communicating with the CVM, log in to the CVM and run the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true
vm_name=vm-name
```

Replace `vm-name` with the name of one of the VMs.

## Enabling and Configuring NGT using CVM (Config-only Mount)

The config-only mount method reduces the size of the NGT ISO mounted on the guest VM by not including the NGT installers. Therefore, it is less prone to scalability issues (for example, the ISO stored on disk is smaller) and might attach faster to the guest VM.

### About this task

Nutanix recommends config-only mount when you enable NGT on a large number of VMs.

### Procedure

1. Log in to the CVM using SSH and (admin, nutanix, or root) access.
2. Run the following command to enable NGT in the guest VM.

```
nutanix@cvm$ nutanix_guest_tools_cli create_vm_tools_entity vm_uuid  
guest_tools_enabled=true
```

Replace `vm_uuid` with the UUID of the VM.

**Note:** To enable SSR and VSS while enabling NGT, use the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli create_vm_tools_entity vm_uuid  
guest_tools_enabled=true file_level_restore=true vss_snapshot=true
```

Replace `vm_uuid` with the UUID of the VM.

3. Run the following command to mount the NGT configuration updates in the guest VM.

```
nutanix@cvm$ nutanix_guest_tools_cli mount_guest_tools vm_uuid config_only=true
```

Replace `vm_uuid` with the UUID of the VM.

Output similar to the following is displayed.

```
nutanix@cvm$ nutanix_guest_tools_cli mount_guest_tools aca91d9b-8a31-47ec-a9b7-  
dfc613115748 config_only=true  
2023-05-26 06:11:51,809Z:30612(0x7f33d60d4340):ZOO_INFO@zookeeper_init@994:  
    Initiating client connection, host=zk1:9876 sessionTimeout=20000  
    watcher=0x7f33e59dec10 sessionId=0 sessionPasswd=<null> context=0x7ffd1271ba00  
    flags=0  
2023-05-26 06:11:51,813Z:30612(0x7f33d57ff700):ZOO_INFO@zookeeper_interest@1941:  
    Connecting to server 10.46.27.73:9876  
2023-05-26 06:11:51,813Z:30612(0x7f33d57ff700):ZOO_INFO@zookeeper_interest@1978:  
    Zookeeper handle state changed to ZOO_CONNECTING_STATE for socket [10.46.27.73:9876]  
2023-05-26 06:11:51,814Z:30612(0x7f33d57ff700):ZOO_INFO@check_events@2187: initiated  
    connection to server [10.46.27.73:9876]  
2023-05-26 06:11:51,814Z:30612(0x7f33d57ff700):ZOO_INFO@check_events@2235: session  
    establishment complete on server [10.46.27.73:9876], sessionId=0x188458c12d08959,  
    negotiated timeout=20000  
2023-05-26 06:11:51,919Z:30612(0x7f33d60d4340):ZOO_INFO@zookeeper_close@3108: Closing  
    zookeeper sessionId=0x188458c12d08959 to [10.46.27.73:9876]  
  
mount_result : kNoError  
task_uuid : d5f7eb25-9e3d-4c7d-ade9-5d25e1e737d5  
nutanix@cvm$
```

## What to do next

The Nutanix Guest Agent (NGA) service in the VMs starts periodic communication with the CVM. To verify whether the NGA service is communicating with the CVM, log in to the CVM and run the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true  
vm_name=vm-name
```

Replace `vm-name` with the name of one of the VMs.

## Upgrade NGT in Bulk on Multiple VMs

You can upgrade NGT in bulk on multiple Windows and Linux guest VMs using the NGT installer file available in the [Nutanix Support portal](#).

### Upgrading NGT in Bulk on Windows VMs

#### Before you begin

- Ensure that the NGT version is compatible with the AOS version installed in your cluster. For more information, see the [NGT](#) section in the *Compatibility and Interoperability Matrix*.
- Ensure that the cluster meets all NGT requirements. For more information, see [Nutanix Guest Tools Requirements](#) in the *Prism Central Infrastructure Guide*.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

#### Procedure

- Perform Step 1 to Step 3 in [Installing NGT in Bulk on Windows VMs](#).

The installer detects that an existing NGT version is already present on the VM and performs an upgrade.

### Upgrading NGT in Bulk on Linux VMs

#### About this task

This sample procedure provides steps to upgrade NGT on Red Hat Package Manager (RPM) based operating systems. Use this procedure as a template to upgrade NGT on Debian-based operating systems.

#### Before you begin

- Ensure that the NGT version is compatible with the AOS version installed in your cluster. For more information, see the [NGT](#) section in the *Compatibility and Interoperability Matrix*.
- Ensure that the cluster meets all NGT requirements. For more information, see [Nutanix Guest Tools Requirements](#) in the *Prism Central Infrastructure Guide*.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

#### Procedure

1. To verify the package signatures, configure the third-party endpoint management tool deployed at your site to install the NUTANIX-NGT-GPG-KEY file on RPM-based operating systems.

For more information, see the tool-specific documentation.

- Configure the third-party endpoint management tool to set up the repositories.

For more information, see the tool-specific documentation.

For example, guest VMs running RedHat 8.x distribution might need a repository configuration in /etc/yum.repos.d/nutanix-guest-tools.repo similar to the following configuration:

```
[NutanixGuestTools]
name=Nutanix Guest Tools
baseurl=http://local-web-server/ngt_repo
enabled=1
gpgcheck=1
gpgkey=http://local-web-server/RPM-GPG-PUBLIC-KEY
repo_gpgcheck=0
```

Replace *local-web-server* with the name of the web server used to distribute the NGT installer files as described in [Preparing the NGT installation files for the Distribution](#).

- Configure the third-party endpoint management tool to upgrade the Nutanix guest agent package by running the package manager-specific upgrade command.

For example, the yum update -y nutanix-guest-agent command upgrades Nutanix guest agent package using the yum package manager for RedHat-based distributions.

```
[nutanix@localhost ~]$ yum update -y nutanix-guest-agent
```

For information about the upgrade command specific to the package manager at your site, see the package manager-specific documentation.

## Uninstall NGT in Bulk from Multiple VMs

You can uninstall NGT in bulk from guest VMs using the third-party management tool deployed at your site.

**Note:** Before uninstalling NGT from a guest VM, ensure the communication link between guest VM and CVM remains active. The CVM displays that NGT is uninstalled only if the communication between CVM and guest VM is active during the uninstallation. If the communication link is down, CVM continues to display that NGT is installed on the guest VM even after the successful uninstallation of NGT. For information about how to verify that the communication link is active, see Step 4 in [Enabling NGT and Mounting the NGT Installer on Cloned VMs](#) on page 316.

## Uninstalling NGT from Windows VMs

### About this task

When you install NGT in a Windows VM, NGT registers an uninstaller in the VM that can be accessed manually using Add/Remove Programs in the Windows Control Panel. This uninstaller can also be used by a third-party endpoint management tool to remove NGT from the VM.

### Before you begin

Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

### Procedure

- Configure the third-party endpoint management tool to uninstall the Nutanix Guest Agent package using the uninstaller registered with Add/Remove Programs in the Windows Control Panel.

For more information, see the tool-specific documentation or Microsoft Windows documentation.

## Uninstalling NGT from Linux VMs

### About this task

This sample procedure provides steps to remove NGT on Red Hat Package Manager (RPM) based operating systems. Use this procedure as a template to remove NGT on Debian-based operating systems.

### Before you begin

Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

### Procedure

- Configure the third-party endpoint management tool to uninstall the Nutanix guest agent package in bulk by running the package manager-specific removal command.

For example, the `yum remove -y nutanix-guest-agent` command uninstalls Nutanix guest agent package using the yum package manager for RedHat-based distributions.

```
[nutanix@localhost ~]$ yum remove -y nutanix-guest-agent
```

For information about the removal command specific to the package manager at your site, see the package manager-specific documentation.

## Enabling NGT and Mounting the NGT Installer on Cloned VMs

If you cloned a VM or multiple VMs from a single VM (master VM), you must enable NGT and mount the NGT installer on the cloned VM to use the NGT feature in the VM.

### Before you begin

Ensure the following before you perform this task:

- NGT is installed in the master VM.
- The required number of VMs were cloned from the master VM.

### About this task

Perform the following steps to enable NGT and mount the NGT installer on cloned VMs.

**Note:** After you perform the following steps, you do not need to separately install NGT on the cloned VMs.

### Procedure

- Enable NGT and mount the NGT installer on the cloned VM by following the instructions mentioned in Steps 1 through 6 of [Enabling NGT and Mounting the NGT Installer in a VM](#).
- Power on the cloned VM.
- (Optional) If you enable NGT and mount the NGT installer while the cloned VMs are powered on, do either of the following:
  - » Restart the Nutanix Guest Agent (NGA) service.  
For Linux VMs – Run the `$ sudo service ngt_guest_agent restart` command or the `$ sudo systemctl restart ngt_guest_agent` command.  
For Windows VMs – Run the `$ net stop "Nutanix Guest Agent"` and `$ net start "Nutanix Guest Agent"` commands.
  - » Power cycle the cloned guest VMs.

- Verify whether the NGA service is communicating with the CVM by logging in to the CVM and running the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true  
vm_name=vm-name
```

Replace `vm-name` with the name of the guest VM.

In the command output, `communication_link_active = true` indicates that the NGA is communicating with the CVM.

**Note:** For information on troubleshooting any NGT related issues, see [KB-3741](#) available on the Nutanix support portal.

## Automatic Regeneration of NGT Certificates

The NGT service inside the controller VM (CVM) automatically reissues an updated NGT client certificate to the guest VM before its expiry date.

NGT client certificates have a fixed expiry of less than three years. The guest VM stops communicating with the CVM when the client certificate expires. When the certificate has less than a year remaining until the expiry date, the guest VM connects to the CVM, updates the certificates and continues IP-based communication with the CVM using the new or updated certificates.

### Requirements

Following are the requirements for automatic regeneration of NGT client certificates:

- Ensure that the cluster is running AOS 7.0 or later and the guest VM is running NGT 4.2 or later versions.
- Ensure that the guest VM is powered on and the connection between the CVM and the guest VM is active.

The NGT client certificates are not automatically regenerated if the guest VM is powered off or if the communication link between CVM and guest VM is down. For information on how to regenerate the client certificates manually, see [Manually Regenerating NGT Certificates for Guest VMs](#) on page 317. To view the list of certificates that are not regenerated, see Step 3 in [Manually Regenerating NGT Certificates for Guest VMs](#) on page 317.

### Manually Regenerating NGT Certificates for Guest VMs

Regenerate NGT client certificates manually if the guest VM cannot regenerate the certificates automatically.

#### About this task

To regenerate the client certificates, follow these steps:

#### Procedure

- Log in to the Prism Element web console.
- Select **Alerts** from the drop-down list on the left of the main menu.  
The **Alerts** dashboard opens displaying all the alerts in the cluster.
- Identify the alert that has **NGT client certificates expiring** in the **Title** with the **Severity** status as **Critical** or **Warning**.  
The **Alerts** dashboard displays the severity status as **Critical** if the certificate is expiring in less than seven days and as **Warning** if the certificate is expiring in less than 45 days. It also displays the name and UUID of the guest VMs for which the certificates are expiring in the **Source Entity** field.
- Click the name of the guest VM in the **Source Entity** field.  
The system opens the **VM** dashboard displaying the details of the guest VM.

**5. Click **Manage Guest Tools**.**

The system displays the **Manage Guest Tools** dialog box.

**6. Select the **Mount Nutanix Guest Tools** checkbox.**

**7. Click **Submit**.**

The system generates a new certificate for the guest VM.

**Note:** After regenerating the NGT client certificates, the guest VM might take a few minutes to communicate with the CVM. To force the guest VM to communicate with the CVM immediately, restart the NGA service.

### What to do next

Check the **Alerts** dashboard in the Prism Element web console and ensure that there are no guest VMs with expired certificates.

## Upgrading NGT

After you upgrade AOS, you must reinstall NGT to upgrade NGT to the latest version.

Perform the following steps to upgrade NGT.

**Note:**

- You can install NGT on up to 1,500 VMs in a cluster. If you exceed this limit, migrate or delete the extra VMs to return to the supported limits.
- Unless you upgrade AOS, you cannot upgrade NGT.

**1. Mount the NGT installer.**

For more information, see [Enabling NGT and Mounting the NGT Installer in a VM](#) on page 303.

**2. Install NGT.**

For more information, see [NGT Installation](#) on page 304.

## Reconfiguring NGT

If you reconfigure the cluster IP address, NGT loses connection with the CVM. You must reconfigure NGT to reestablish the connection.

To reconfigure NGT, mount the NGT installer. For more information, see [Enabling NGT and Mounting the NGT Installer in a VM](#) on page 303.

After you mount the NGT ISO, NGA fetches the latest configuration (new cluster IP address) mounted in the guest VM. The guest VM can now use the new IP address to communicate with the cluster.

**Note:**

- It takes a few minutes for the guest VM to communicate with the cluster because this is an asynchronous operation.
- For information about troubleshooting any NGT-related issues, see [KB-3741](#).

## Uninstalling and Removing Nutanix Guest Tools

### About this task

Do the following to remove NGT from the VM completely.

- Uninstall NGT from the guest VM.
- Verify whether the NGT information of the guest VM is removed from the CVM.
- If the NGT information of the guest VM is not removed from the CVM, remove it from the CVM using nCLI.

## Procedure

### 1. Uninstall NGT.

**Note:** Before you uninstall NGT from a guest VM, ensure that the communication link between the guest VM and the CVM is active. If the communication link is down, the CVM continues to display that NGT is installed on the guest VM even after the successful uninstallation of NGT. The CVM displays that NGT is uninstalled only after the communication between the CVM and the guest VM is restored. For information about how to verify that the communication link is active, see Step 4 in [Enabling NGT and Mounting the NGT Installer on Cloned VMs](#).

- **Windows VM**

You can uninstall NGT from a Windows VM through Control Panel. Log in to the Windows VM and perform the following.

1. Navigate to **Control Panel > Programs > Programs and Features**.
2. Select the **Nutanix Guest Tools** service.
3. Click **Uninstall**.

An Uninstall Successfully Completed message appears on successfully uninstalling NGT.

(Optional) You can uninstall NGT from a Windows VM using the PowerShell command. Log in to the Windows VM and perform the following.

1. Run the following command from Windows PowerShell to generate the output string required to uninstall NGT.

```
$ Get-ChildItem -Path HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion
\Uninstall, HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion
\Uninstall | Get-ItemProperty | Where-Object {$_DisplayName -match "Nutanix
Guest Tools" } | Select-Object -Property QuietUninstallString | Out-String -
Width 4096
```

**Result:** An output string appears on the console. For example, "`C:\ProgramData\Package Cache\{3cfa83ac-a36f-49f1-ad23-3a51c0e6964a}\NutanixGuestTools.exe" /uninstall /quiet`.

2. Run the output string that is generated to uninstall NGT.

```
"C:\ProgramData\Package Cache\{3cfa83ac-a36f-49f1-
ad23-3a51c0e6964a}\NutanixGuestTools.exe" /uninstall /quiet
```

**Note:** If you do not want to restart the guest VM after uninstalling NGT, append /norestart to the generated output string, and run the updated output string. For example,

```
"C:\ProgramData\Package Cache\{3cfa83ac-a36f-49f1-
ad23-3a51c0e6964a}\NutanixGuestTools.exe" /uninstall /quiet /norestart
```

**Tip:** After uninstalling NGT from a Windows VM, ensure the following entries that are created during NGT installation, are removed from the VM registry.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Nutanix HKEY_LOCAL_MACHINE\SOFTWARE\Nutanix
\VSS\1.0 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nutanix
Guest Agent HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nutanix
Self Service Restore Gateway HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
```

```
\Services\EventLog\Application\Nutanix HKEY_LOCAL_MACHINE\SYSTEM  
\CurrentControlSet\Services\EventLog\Application\Nutanix Guest Agent  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application  
\Nutanix Self Service Restore Gateway HKEY_LOCAL_MACHINE\SYSTEM  
\CurrentControlSet\Services\VSS
```

- **Linux VM**

Log in to the Linux VM and run the following command.

```
$ sudo sh /usr/local/nutanix/ngt/python/bin/uninstall_ngt.sh
```

Output similar to the following is displayed.

```
$ sudo sh /usr/local/nutanix/ngt/python/bin/uninstall_ngt.sh  
Stopping ngt_guest_agent.service systemctl service...  
ngt_guest_agent.service service stopped.  
Stopping ngt_self_service_restore.service systemctl service...  
ngt_self_service_restore.service service stopped.  
NGA is getting uninstalled.  
Removing Desktop icon and shortcuts.  
Notify CVM of agent uninstallation.  
Successfully notified CVM of agent uninstallation.  
    Erasing      : nutanix-guest-agent-4.0-1.x86_64  
  
1/1  
warning: /usr/local/nutanix/ngt/config/ngt_config.json saved as /usr/local/  
nutanix/ngt/config/ngt_config.json.rpmsave  
RPM is getting removed/uninstalled.  
Successfully uninstalled Nutanix Guest Tools.  
    Verifying     : nutanix-guest-agent-4.0-1.x86_64  
  
1/1  
Removed:  
    nutanix-guest-agent.x86_64 0:4.0-1  
  
Complete!
```

Additionally, clear the /usr/local/nutanix/ngt directory.

2. Verify whether the NGT information of the guest VM is removed from the CVM.

- a. Log in to the CVM with SSH.

- b. Check the NGT information status in the CVM by running the following command.

```
nutanix@cvm$ ncli ngt list
```

An output similar to the following is displayed if the NGT information of the guest VM is not removed from the CVM.

```
nutanix@cvm$ ncli ngt list  
  
          VM Id : 0005b6a7-6bcc-03f2-0000-000000097fe::e4a1216a-  
a287-43c2-bbbf-28951elbf615  
          VM Name : win 2012  
          NGT Enabled : true  
          Tools ISO Mounted : false  
          Vss Snapshot : false  
          File Level Restore : false  
          Communication Link Active : true
```

In the VM ID column, the text after ":" is the ID of the VM as shown in the example.

- If the NGT information of the guest VM appears when you run the command in Step 2b, remove the NGT information from the CVM by running the following command.

```
nutanix@cvm$ ncli ngt delete vm-id=virtual_machine_id
```

Replace *virtual\_machine\_id* with the ID of the VM displayed in the output of Step b.

**Note:** For information about troubleshooting any NGT-related issues, see [KB-3741](#).

## NGT Metrics Collection for Windows Performance Monitor

You can monitor host-specific metrics for a VM in a guest VM running Windows OS. The supported metrics are fetched from the controller VM (CVM) and are published to the Microsoft Windows Performance Monitor on the guest VM.

### Managing Metrics Collection in a Guest VM

Nutanix publishes VM-specific metrics in the NGT Metrics performance counter object in the Windows Performance Monitor. You can leverage all Perfmon functionalities to view the metrics data in different ways. For example, you can view the metrics in different graph formats. The options available for graphs are line, histogram, and report.

**Important:** By default, NGT metrics collection is disabled in a guest VM. Contact Nutanix Support to enable metrics collection in a guest VM.

The guest VM makes an RPC call to the CVM every 30 seconds to fetch the metrics data. Once the data is fetched successfully, it internally checks if this counter is already registered in the Perfmon utility. If the counter is not registered, it first registers the counter and then publishes this data to the Performance Monitor. By default, the following metrics are collected from the CVM after enabling NGT metrics collection in the guest VM.

- hypervisor\_cpu\_usage\_ppm**: Indicates the VM processor time in parts per million.
- hypervisor\_cpu\_ready\_time\_ppm**: Indicates the VM stolen time in parts per million.

For information about monitoring or viewing NGT metrics in the guest VM, see [Monitoring NGT Metrics for System Performance in Guest VM](#) on page 322.

### Managing Metrics Collection from CVM

Although the NGT metrics collection is enabled by default on CVMs, you can monitor the NGT metrics in the Performance Monitor only in the guest VM.

**Important:** Contact Nutanix Support to enable or disable NGT metrics collection in a CVM.

The default metrics available in the CVM are `hypervisor_cpu_usage_ppm` and `hypervisor.cpu_ready_time_ppm`. You can modify the metrics list from the CVM by editing the `~/config/nutanix_guest_tools/ngt_metrics_info.json` file to add or remove the metrics to be published on the guest VMs.

For example, in the `ngt_metrics_info.json` file you can modify the array list to add or remove metrics in the metrics info block. Any changes in the metrics list reflect after you restart the NGA service on the CVM.

```
{  
    "metrics_info" : [  
        "hypervisor_cpu_usage_ppm",  
        "hypervisor.cpu_ready_time_ppm"  
    ]  
}
```

After you modify the metrics list, you must restart the NGT service on the CVM by running the `$ allssh "genesis stop nutanix_guest_tools && cluster start"` command for the updated metrics data to reflect in the guest VM. After the guest VM fetches the metrics, it updates this data in the Perfmon utility without manual intervention (like service restart) in the guest VM.

**Note:** The metrics list must be modified for all the nodes.

## Known Issues and Limitations

- Any failure in registering a counter or in publishing the metrics data is logged in the Nutanix Guest Agent logs in the guest VM. Currently, you are not alerted if such an event occurs.
- In Windows Performance monitor, the NGT hypervisor CPU metrics is collected in parts per million. Because the default scale is 1, it gives values over 100%. Nutanix recommends to adjust the scale in the **Performance Monitor Properties > Data** tab to .0001.

## Monitoring NGT Metrics for System Performance in Guest VM

### Before you begin

- Verify that the guest VM has Microsoft Windows OS and NGT installed.
- Verify that the guest VM has Microsoft Windows Perfmon utility installed.
- Verify that the NGT metric collection is enabled in the guest VM. You can do this by checking if the Ngt Metrics collection capabilities got enabled message is logged in C:\Program Files\Nutanix\logs \guest\_agent\_service.INFO.
- Ensure that the CVM and the guest VM system clocks are in sync with the actual time to ensure that accurate metrics are generated.

### About this task

Perform the following steps to view the NGT metrics in the guest VM.

### Procedure

1. Log in to the Prism Element web console.
2. In the dropdown list of the main menu, select **VM**.
3. From the VM page that opens, select the **Table** view.
4. Select the target VM in the table, and click **Launch Console**.
5. Log in to the guest VM.
6. Navigate to **Start > Run**.
7. Type perfmon and click **OK**.  
This launches the **Performance Monitor** utility.
8. Under **Monitoring Tools**, select **Performance Monitor**.

9. Click the **Add** icon.

The **Add Counters** window appears. NGT metrics is listed in the counter list.

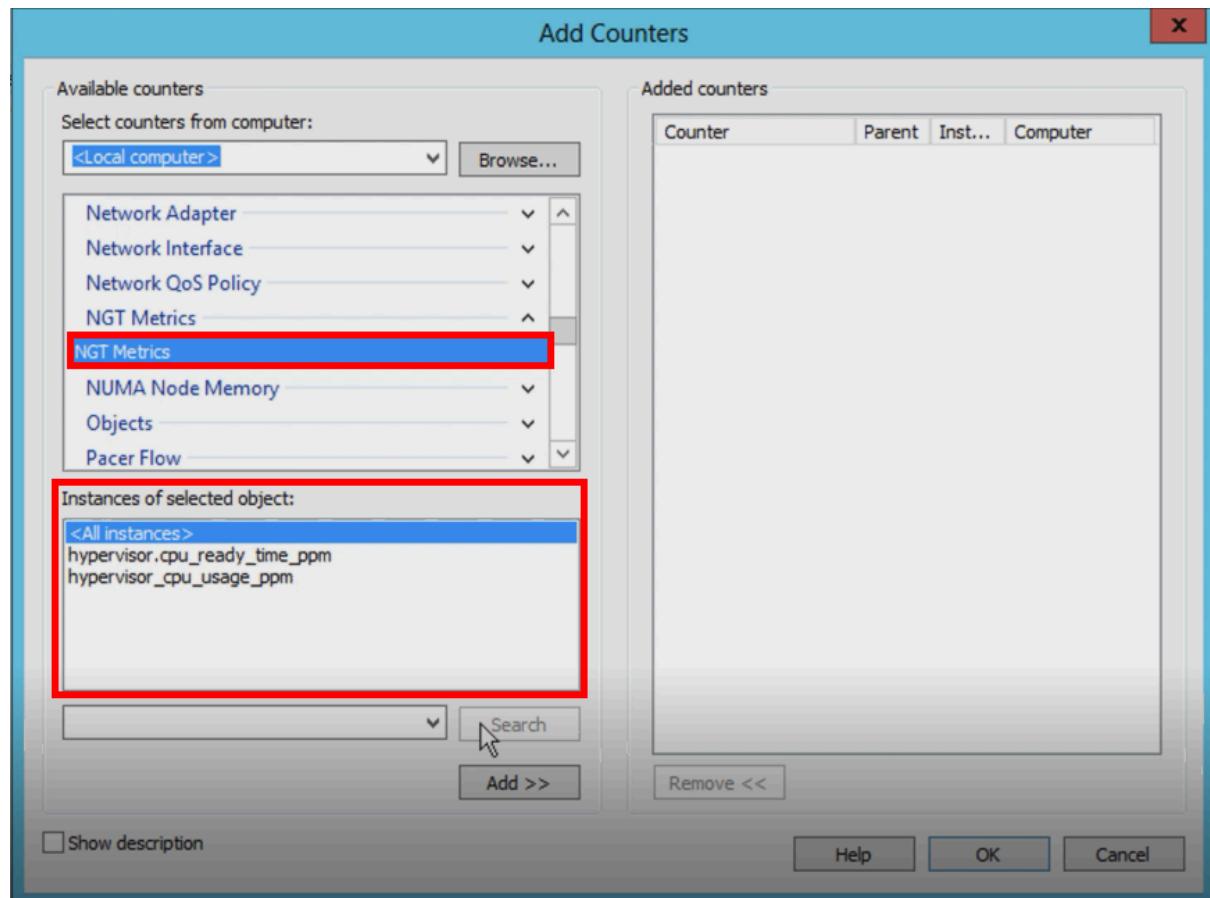
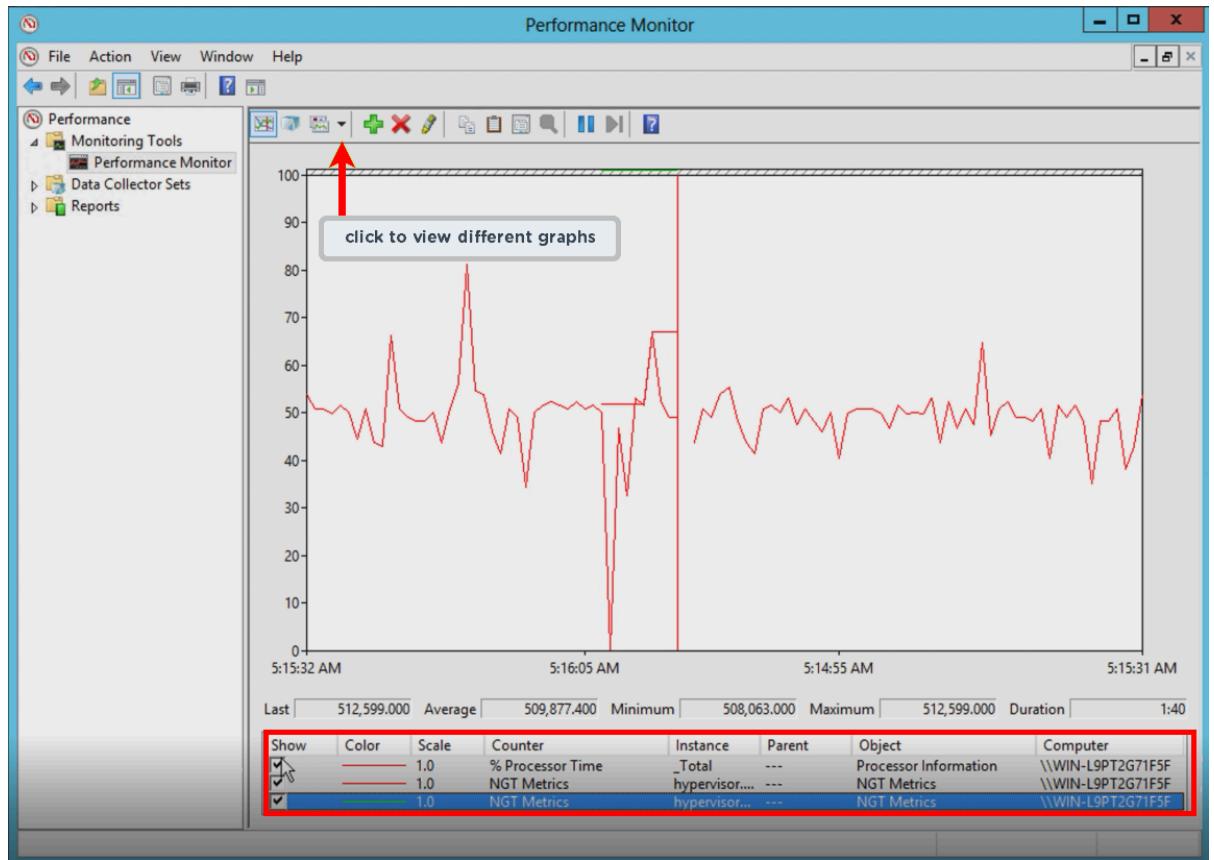


Figure 50: Performance Monitor (Add Counters)



**Figure 51: NGT Metrics (Graphical View)**

#### What to do next

After metrics are collected, you can leverage all the Windows Performance Monitor functionalities like generating reports, viewing metrics graphically.

## VM-Host Affinity Policies Defined in Prism Element

In Prism Element, you can define scheduling policies for virtual machines on an AHV cluster at a VM level. By defining these policies, you can control the placement of a virtual machine on specific hosts within a cluster.

You can define the VM-Host affinity policies by using Prism Element during the VM create or update operation. For more information, see [Creating a VM \(AHV\)](#).

For information on how the protection domain-based VM-Host affinity policies are handled during disaster recovery, see [Affinity Policies Handling - Protection-Domain Based DR Solution with On-prem Clusters Only](#).

#### Limitations of Affinity Rules

Even though if a host is removed from a cluster, the host UUID is not removed from the host-affinity list for a VM.

## Configuring Legacy VM-VM Anti-Affinity Policy

To configure the legacy VM-VM anti-affinity policies, you must first define a group and then add all the VMs on which you want to define the legacy VM-VM anti-affinity policy.

## About this task

**Important:** Starting with the AOS 7.0 and pc.2024.3 release, you can create category based VM-VM anti-affinity policies from Prism Central. For more information, see [VM-VM Anti-Affinity Policies Defined in Prism Central](#).

To configure the legacy VM-VM anti-affinity policy, follow these steps:

### Procedure

1. Log on to the Controller VM with SSH session.

2. Create a group:

```
nutanix@cvm$ acli vm_group.create group_name
```

Replace *group\_name* with the name of the group.

3. Add the VMs on which you want to define the legacy anti-affinity to the group:

```
nutanix@cvm$ acli vm_group.add_vms group_name vm_list=vm_name
```

Replace *group\_name* with the name of the group. Replace *vm\_name* with the name of the VMs that you want to define anti-affinity on. In case of multiple VMs, you can specify comma-separated list of VM names.

4. Create the legacy VM-VM anti-affinity policy.

```
nutanix@cvm$ acli vm_group.antiaffinity_set group_name
```

Replace *group\_name* with the name of the group.

After you configure the group and then power on the VMs, the VMs that are part of the group are started (attempt to start) on the different hosts.

#### Important:

The legacy VM-VM anti-affinity policy is a preferential policy. The system does not block any VM operation, such as VM maintenance mode or manual live migration of the VM, even if there is a policy violation. For example, when you manually migrate one VM of a VM-VM pair with an anti-affinity policy, the policy is applied on a commercially reasonable effort only.

The Acropolis Dynamic Scheduling (ADS) always attempts to maintain compliance with the VM-VM anti-affinity policy and ensures that the legacy VM-VM anti-affinity policy is enforced on a commercially reasonable effort. For example, if you manually migrate a VM and the migration leads to non-compliance with the legacy VM-VM anti-affinity policy, the ADS checks if the host is specified in manual migration, and performs the following actions:

- Ignores compliance to the legacy VM-VM anti-affinity policy, if a host is specified during manual migration.
- Attempts to enforce the policy back into compliance on a best-effort basis, if a host is not specified during manual migration.

For more information on ADS, see [Acropolis Dynamic Scheduling in AHV](#) section in AHV Administration Guide.

## Removing Legacy VM-VM Anti-Affinity Policy

Perform the following procedure to remove the legacy VM-VM anti-affinity policy.

### Procedure

1. Log on to the Controller VM with SSH session.

- Remove the legacy VM-VM anti-affinity policy.

```
nutanix@cvm$ acli vm_group.antiaffinity_unset group_name
```

Replace `group_name` with the name of the group.

The legacy VM-VM anti-affinity policy is removed for the VMs that are present in the group, and they can start on any host during the next power on operation (as necessitated by the ADS feature).

## Connect to Citrix Cloud

The **Connect to Citrix Cloud** feature leverages the automated installer functionality of the Citrix Cloud connector to establish a secure communication channel between Nutanix and Citrix Cloud. This feature provides single-click integration of the on-premise Nutanix clusters as a resource location with the Citrix Cloud environment.

**Note:** This feature is supported on AHV only.

This feature helps you configure the Citrix Cloud integration settings in the following way:

- Establishes the connection to the Citrix Cloud workspace.
- Configures Nutanix cluster as resource location in the Citrix cloud.
- Configures the Citrix Cloud connector VM.
- Registers the Citrix Cloud connector VM to the Active Directory (AD) domain on the Citrix cloud.

Once the integration is complete, VDIs can be created using the *Nutanix AHV MCS Plug-in for Citrix XenDesktop* 1.1.1.0 or later. The AHV MCS Plug-in is designed to create and manage VDIs in a Nutanix Acropolis infrastructure environment. For more information, see [AHV Plug-in for Citrix](#) install guide and release notes.

Thus, to begin deploying your VMs and applications, you must perform the following:

- Configure the Citrix cloud integration settings using the **Connect to Citrix Cloud** feature.
- Install the *Nutanix CWA Plug-In for Citrix Cloud Connector*.

Refer to the *Citrix documentation* for details on Citrix Cloud connector.

## Connecting to the Citrix Cloud

To integrate with the Citrix Cloud workspace, perform the following procedure.

### Before you begin

Ensure that you have created a Sysprep (System Preparation) VM with Windows 2012 R2 server or newer versions of Windows server 2016, 2019 and 2022 as the base image and the VM should be available on the Nutanix cluster.

**Caution:** The Sysprep VM must be in the powered-off state. If you power on the VM, you will lose the Sysprep state and the configuration will fail.

For more information, see *Microsoft documentation on Sysprep (Generalize) a Windows installation*.

### Procedure

- Log on to the Prism Element web console using your Nutanix administrator credentials.

**Note:** The procedure does not work if Prism Element is launched from Prism Central web console.

- Click the gear icon in the main menu and then select **Connect to Citrix Cloud** from the **Setup** section in the **Settings** page.

The **Connect to Citrix Cloud** dialog box opens.

3. Authenticate your connection to the Citrix cloud by using one of the following methods:

- **Enter Manually**

1. Enter your **Customer ID** for the Citrix Cloud.
2. Enter your secure **Client ID** for the Citrix Cloud.
3. Enter the downloaded secure client **Secret Key**.

**Note:** You can find the **Customer ID**, **Client ID**, and **Secret Key** from the *API Access* page in the Citrix Cloud console.

4. Click **Connect**.

- **Upload Credential Key**

1. Click **Upload Key File** to browse and select the key file in the CSV format.

You can create or download the key file from the *API Access* page in the Citrix Cloud console (within *Identity and Access Management*). This key file is used for the Citrix Cloud connector installation.

2. Enter your **Customer ID** for the Citrix Cloud.
3. Click **Connect**.

4. Select the **Resource Location** from the drop-down menu.

The drop-down menu displays the resource locations that are created on the Citrix Cloud. If you have not previously created any resource locations, enter a name for the resource location that you want to create in the **Resource location** field.

5. (Optional) Review the **Citrix Cloud** details. If any change is required, click the **Change** hyperlink to edit the connection details.
6. (Optional) Select the **High Availability** check-box to enable or disable high availability for the connector nodes.

By default, high availability is enabled. On enabling high availability, two connector nodes are created for the redundancy purpose.

**Note:** Citrix Cloud recommends that you install two connectors for redundancy and high availability.

7. In the **VM Master Image** search box, start typing the initial letters of the previously created Sysprep VM image and select the auto-completed option.
8. Enter the **Connector VM Name**.
9. If high availability is enabled, enter the **Secondary Connector VM Name (for high availability)**.
10. Enter the **Connector VM Password**.
11. Enter the **Domain Credentials** to join your enterprise domain to the resource location.
  - a. Enter the **Domain Username** in the format USERDOMAIN\USERNAME.
  - b. Enter the **Domain Password**.
  - c. Enter the **Machine Domain Name**.
  - d. Enter the **DNS Gateway**.
12. Click **Save and Continue**.

The connector VM or VMs are configured successfully.

## What to do next

- Verify the connection status. For more information, see [Viewing Citrix Connection Status](#) on page 328.
- Verify if the connector VM or VMs are created from the **VM Dashboard**.
- Wait for the state of the connector VM or VMs to change from powered off to powered on and then click **Launch Console**. The VM preparation process starts.
- Once the VM starts, install the *Nutanix CWA Plug-In for Citrix Cloud Connector* to start the application deployment.

## Viewing Citrix Connection Status

You can view the current status of your Citrix Cloud connection. This helps to verify the registration of the connector VM to the Citrix cloud.

To view details of the Citrix connection, click the gear icon and select **Connect to Citrix Cloud**. If the connector VM is configured, the connector VM name and the status are listed under Connector VMs. It might take some time for the connection status to refresh.

The Connection Status shows the following statuses:

- Connected - The connector VM is successfully registered with Citrix cloud.
- Connection in progress - The connector VM is registration with Citrix cloud is in progress.
- Not Connected - The connector VM is not registered with the Citrix cloud or the Citrix registration has failed. In this case, wait for the connection status to refresh, it may take several minutes depending on your environment. Otherwise, click **Delete Connection** to delete the Citrix cloud connection and configure it again. The **Delete Connection** option deletes the connector VM and unregisters the account from the Citrix Cloud.

**Note:** For XenServer, the **Delete Connection** option does not delete the connector VMs. You must delete the connector VMs manually.

## Guest VM Cluster Configuration (AHV Only)

In AHV clusters, you can create guest VM clusters by either directly attaching volume groups to guests VMs or by using iSCSI. Follow this document if you want to create guest VM clusters by directly attaching volume groups to guests VMs.

For information on how to create guest VM clusters by using iSCSI, see the [Nutanix Volumes Guide](#).

### Creating a Guest VM Cluster by Directly Attaching a Volume Group (AHV Only)

In AHV clusters, you can create a guest VM cluster by directly attaching a volume group to guest VMs. After you attach a volume group to guest VMs, vDisks appear as SCSI devices to the guest operating system and you do not need to set up any in-guest connections when you are creating a guest cluster. If you directly attach volume groups to guest VMs, you can seamlessly share vDisks across VMs in the guest cluster.

#### About this task

You can directly attach a volume group to guest VMs to create the following guest clusters:

- Windows Server Failover Clusters (WSFC)
- Red Hat Enterprise Linux (RHEL) Cluster

**Note:** To create an WSFC cluster, ensure that the minimum Nutanix VirtIO version installed on the guest VM is 1.1.4. For more information about VirtIO drivers, see [Nutanix VirtIO for Windows](#) in *AHV Administration Guide*.

You cannot create a guest VM cluster by directly attaching a volume group to guest VMs in ESXi and Hyper-V clusters.

Perform the following sequence of tasks to create a guest cluster by directly attaching a volume group to guest VMs.

### Procedure

1. Log in to the Prism Element web console.

2. Create the number of VMs you want in the guest cluster.

For information on how to create a VM in an AHV cluster, see [Creating a VM \(AHV\)](#).

3. Create a volume group for the guest cluster.

For information on how to create a volume group, see [Creating a Volume Group](#).

4. Attach the volume group you created to each VM in the guest cluster.

For information on how to attach a volume group to a VM, see [Managing a VM \(AHV\)](#).

5. Create a guest cluster.

For information on how to create a guest cluster, see the documentation of your guest operating system.

# PERFORMANCE MONITORING

---

Nutanix provides several mechanisms to maximize performance in the cluster. The converged Distributed Storage Fabric (DSF) architecture is designed to service the VM requests locally on each node whenever possible. Each node employs data tiers so that frequently accessed (*hot*) data is retained in memory or solid state disk (SSD) storage while seldom accessed (*cold*) data is moved to hard disk drive (HDD) storage. Each Controller VM has an in-memory read cache to access highly requested data directly from memory.

The web console allows you to monitor and analyze performance across the cluster. For more information, see [Analysis Dashboard](#) on page 330.

## Analysis Dashboard

The Analysis dashboard allows you to create charts that can monitor dynamically a variety of performance measures. To view the Analysis dashboard, select **Analysis** from the pull-down list on the left of the main menu.

### Menu Options

The Analysis dashboard does not include menu options other than those available from the main menu.

### Analysis Screen Details

The Analysis dashboard includes three sections.

- *Chart definitions.* The pane on the left lists the charts that can be run. No charts are provided by default, but you can create any number of charts. A chart defines the metrics to monitor. There are two types of charts, metric and entity. A metric chart monitors a single metric for one or more entities. An entity chart monitors one or more metrics for a single entity.

**Note:** You can change the color assigned to a metric or entity by clicking that color box in the chart (left pane) and then selecting a different color from the displayed palette.

- *Chart monitors.* When a chart definition is checked, the monitor appears in the middle pane. An Alerts & Events monitor always appears first. The remaining monitors are determined by which charts are checked in the left pane. You can customize the display by selecting a time interval (from 3 hours to a month) from the **Range** drop-down (above the charts) and then refining the monitored period by moving the time interval end points to the desired length.
- *Alerts and events.* Any alerts and events that occur during the interval specified by the time line in the middle pane appear in the pane on the right. For more information, see [Prism Element Alerts and Events Reference Guide](#).

The following table describes each field in the Analysis dashboard. Some fields can include a slide bar on the right to view additional information in that field. The displayed information is dynamically updated to remain current.

**Note:** For information about how the metrics are measured, see [Understanding Displayed Statistics](#) on page 69.

**Table 63: Analysis Screen Fields**

Name	Description
Charts	Displays the set of defined charts. Check the box next to a chart name to run that chart in the middle pane. The chart monitor appears in the middle pane shortly after checking the box. Uncheck the box to stop that monitor and remove it from the middle pane. To edit a chart definition, click the pencil icon to the right of the name. This opens the edit chart window, which is the same as the new chart window except for the title. To delete a chart, click the cross icon on the right.
New Metric Chart	Allows you to create a chart that tracks a single metric for one or more entities. For more information, see <a href="#">Creating a Metric Chart</a> on page 332.
New Entity Chart	Allows you to create a chart that tracks one or more metrics for a single entity. For more information, see <a href="#">Creating an Entity Chart</a> on page 332.
(range time line and monitor period)	<p>Displays a time line that sets the duration for the monitor displays. To set the time interval, select the time period (3 hour, 6 hour, 1 day, 1 week, WTD [week to date], 1 month) from the <b>Range</b> field pull-down menu (far right of time line). To customize the monitor period, you may move through the timeline by manipulating the translucent blue bar on the top of the Analysis pane. To reach a specific point in time, use the solid blue bar at the bottom of the Analysis pane.</p> <ul style="list-style-type: none"><li>• By default, if you select a scale that is greater than the current, the translucent time scrubber tends to jump to the most recent record.</li><li>• If you need to move further back in time than the scrubber allows at the current scale, increase the scale of the scrubber.</li><li>• After you have the scale of your choice, move the translucent scrubber across the timeline to the period in time that you wish to examine.</li><li>• After you have a time period selected, slide the solid blue time slider to a specific point in time.</li><li>• To move down further into the time period, lower the scale and move the scrubber accordingly.</li><li>• The lowest choice for scale is 3 hours, but you can shrink the translucent scrubber down to approximately five minutes within the UI.</li><li>• When exporting the charts, the selected scale is used for the file regardless of whether the scrubber has been resized to a custom value.</li></ul>
Alerts & Events Monitor  (defined chart monitors)	<p>Displays a monitor of alert and event messages that were generated during the time interval. Alerts and events are tracked by a moving histogram with each bar indicating the number of messages generated during that time. The message types are color coded in the histogram bars (critical alert = red, warning alert = orange, informational alert = blue, event = gray).</p> <p>Displays monitors for any enabled (checked) charts. In the figure above, three charts are enabled (memory usage, CPU/memory, and disk IOPS). You can export the chart data by clicking on the chart header. This displays a drop-down menu (below) to save the data in CSV or JSON format. It also includes a chart link option that displays the URL to that chart, which you can copy to a clipboard and use to import the chart.</p>

Name	Description
Alerts	Displays the alert messages that occurred during the time interval. For more information, see <a href="#">Alerts Dashboard</a> in <i>Prism Element Alerts and Events Reference Guide</i> . Clicking a message causes the monitor line to move to the time when that alert occurred.
Events	Displays the event messages that occurred during the time interval. Clicking a message causes the monitor line to move to the time when that event occurred.

## Creating an Entity Chart

### About this task

An entity chart monitors the performance of one or more metrics for a single entity. To create an entity chart definition, do the following:

### Procedure

1. Log in to the Prism Element web console.
2. In the [Analysis Dashboard](#) on page 330, click **New > New Entity Chart**.  
The **New Entity Chart** dialog box appears.
3. Do the following in the indicated fields:
  - a. **Chart Title:** Enter a title for this chart.
  - b. **Entity type:** Select an entity from the pull-down list.  
The entity types include host, disk, storage pool, storage container, virtual machine, volume group, remote site, protection domain, replication link, virtual disk, and cluster.
  - c. **Entity:** Enter the name of the target entity.  
As you enter characters in this field, it displays a list of matching entries of that entity type. Click the name when it appears in the search list.

**Note:** If you are creating this chart for *Prism Central*, the list spans the registered clusters. Otherwise, the list is limited to the current cluster.
- d. **Metric:** Select a metric from the drop-down list. (Repeat to include additional metrics.)  
For descriptions of the available metrics, see [Chart Metrics](#) on page 333.
4. When all the field entries are correct, click the **Save** button.  
The Analysis dashboard reappears with the new chart appearing in the list of charts on the left of the screen.

## Creating a Metric Chart

### About this task

A metric chart monitors the performance of a single metric for one or more entities. To create a metric chart definition, do the following:

### Procedure

1. Log in to the Prism Element web console.

- In the [Analysis Dashboard](#) on page 330, click **New > New Metric Chart**.

The **New Metric Chart** dialog box appears.

- Do the following in the indicated fields:

a. **Chart Title:** Enter a title for this chart.

b. **Metric:** Select a metric to monitor from the pull-down list.

For descriptions of the available metrics, see [Chart Metrics](#) on page 333.

c. **Entity Type:** Select an entity type from the pull-down list. (Repeat to include additional entities.)

The entity types include host and cluster.

d. **Entity:** Enter the name of the target entity.

As you enter characters in this field, it displays a list of matches of the entity type. Click the name when it appears in the search list. (Repeat to include additional names.)

**Note:** If you are creating this chart for *Prism Central* the list spans the registered clusters. Otherwise, the list is limited to the current cluster.

- When all the field entries are correct, click the **Save** button.

The Analysis dashboard reappears with the new chart appearing in the list of charts on the left of the screen.

## Chart Metrics

The following metrics can be added to charts.

**Note:** The mapping between a metric and an entity type is hypervisor dependent.

Memory Usage	Entity Type(s)	Description
<b>Metric</b>		
Content Cache Hit Rate (%)	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> </ul>	Content cache hits over all lookups. ID: <code>CONTENT_CACHE_HIT_PPM</code>
Content Cache Hits	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> </ul>	Number of hits on the content cache. ID: <code>CONTENT_CACHE_NUM_HITS</code>
Content Cache Logical Memory Usage	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> </ul>	Logical memory (in bytes) used to cache data without deduplication. ID: <code>CONTENT_CACHE_LOGICAL_MEMORY_USAGE_BYTES</code>
Content Cache Logical SSD Usage	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> </ul>	Logical SSD memory (in bytes) used to cache data without deduplication. ID: <code>CONTENT_CACHE_LOGICAL_SSD_USAGE_BYTES</code>
Content Cache Lookups	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> </ul>	Number of lookups on the content cache. ID: <code>CONTENT_CACHE_NUM_LOOKUPS</code>

Memory Usage	Entity Type(s)	Description
Metric		
Content Cache Physical Memory Usage	<ul style="list-style-type: none"> <li>Host</li> <li>Cluster</li> </ul>	Real memory (in bytes) used to cache data by the content cache. ID: <code>CONTENT_CACHE_PHYSICAL_MEMORY_USAGE_BYTES</code>
Content Cache Reference Count	<ul style="list-style-type: none"> <li>Host</li> <li>Cluster</li> </ul>	Average number of content cache references. ID: <code>CONTENT_CACHE_NUMDEDUP_REF_COUNT_PPH</code>
Content Cache SSD Usage	<ul style="list-style-type: none"> <li>Host</li> <li>Cluster</li> </ul>	Real SSD usage (in bytes) used to cache data by the content cache. ID: <code>CONTENT_CACHE_PHYSICAL_SSD_USAGE_BYTES</code>
Deduplication Fingerprints Cleared	<ul style="list-style-type: none"> <li>Host</li> <li>Cluster</li> </ul>	Number of written bytes for which fingerprints have been cleared. ID: <code>DEDUP_FINGERPRINT_CLEARED_BYTES</code>
Deduplication Fingerprints Written	<ul style="list-style-type: none"> <li>Host</li> <li>Cluster</li> </ul>	Number of written bytes for which fingerprints have been added. ID: <code>DEDUP_FINGERPRINT_ADDED_BYTES</code>
Disk I/O Bandwidth	<ul style="list-style-type: none"> <li>Host</li> <li>Cluster</li> <li>Disk</li> <li>Storage Pool</li> </ul>	Data transferred per second in KB/second from disk. ID: <code>STATS_BANDWIDTH</code>
Disk I/O Bandwidth - Read	<ul style="list-style-type: none"> <li>Host</li> <li>Cluster</li> <li>Disk</li> <li>Storage Pool</li> </ul>	Read data transferred per second in KB/second from disk. ID: <code>STATS_READ_BANDWIDTH</code>
Disk I/O Bandwidth - Write	<ul style="list-style-type: none"> <li>Host</li> <li>Cluster</li> <li>Disk</li> <li>Storage Pool</li> </ul>	Write data transferred per second in KB/second from disk. ID: <code>STATS_WRITE_BANDWIDTH</code>
Disk I/O Latency	<ul style="list-style-type: none"> <li>Host</li> <li>Cluster</li> <li>Disk</li> <li>Storage Pool</li> </ul>	I/O latency in milliseconds from disk. ID: <code>STATS_AVG_IO_LATENCY</code>

Memory Usage	Entity Type(s)	Description
Metric		
Disk IOPS	<ul style="list-style-type: none"> <li>Host</li> <li>Cluster</li> <li>Disk</li> <li>Storage Pool</li> </ul>	Input/Output operations per second from disk. ID: <code>STATS_NUM_IOPS</code>
Disk IOPS - Read	<ul style="list-style-type: none"> <li>Host</li> <li>Cluster</li> <li>Disk</li> <li>Storage Pool</li> </ul>	Input/Output read operations per second from disk. ID: <code>STATS_NUM_READ_IOPS</code>
Disk IOPS - Write	<ul style="list-style-type: none"> <li>Host</li> <li>Cluster</li> <li>Disk</li> <li>Storage Pool</li> </ul>	Input/Output write operations per second from disk. ID: <code>STATS_NUM_WRITE_IOPS</code>
GPU Framebuffer Usage	Virtual Machine	Framebuffer usage in percentage. ID: <code>FRAMEBUFFER_USAGE_PPM</code> <p><b>Note:</b> The Virtual Machine entity is applicable for AHV hypervisor.</p>
GPU Usage	Virtual Machine	GPU compute usage in percentage. ID: <code>GPU_USAGE_PPM</code> <p><b>Note:</b> The Virtual Machine entity is applicable for AHV hypervisor.</p>
GPU video decoder Usage	Virtual Machine	GPU video decoder usage in percentage. ID: <code>DECODER_USAGE_PPM</code> <p><b>Note:</b> The Virtual Machine entity is applicable for AHV hypervisor.</p>
GPU video encoder usage	Virtual Machine	GPU video encoder usage in percentage ID: <code>ENCODER_USAGE_PPM</code> <p><b>Note:</b> The Virtual Machine entity is applicable to AHV hypervisor.</p>

Memory Usage	Entity Type(s)	Description
Metric		
Hypervisor CPU Ready Time (%)	Virtual Machine	Percentage of time that the virtual machine was ready, but could not get scheduled to run.  ID: <code>STATS_HYP_CPU_READY_TIME</code>
Hypervisor CPU Usage (%)	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Virtual Machine</li> </ul>	Percent of CPU used by the hypervisor.  ID: <code>STATS_HYP_CPU_USAGE</code>
Hypervisor I/O Bandwidth	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Virtual Machine</li> </ul>	Data transferred per second in KB/second from Hypervisor.  ID: <code>STATS_HYP_BANDWIDTH</code>  <div style="background-color: #f0f0f0; padding: 5px;"> <b>Note:</b> Virtual Machine entity is applicable for ESXi hypervisor.         </div>
Hypervisor I/O Bandwidth - Read	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Virtual Machine</li> </ul>	Read data transferred per second in KB/second from Hypervisor.  ID: <code>STATS_HYP_READ_BANDWIDTH</code>  <div style="background-color: #f0f0f0; padding: 5px;"> <b>Note:</b> Virtual Machine entity is applicable for ESXi hypervisor.         </div>
Hypervisor I/O Bandwidth - Write	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Virtual Machine</li> </ul>	Write data transferred per second in KB/second from Hypervisor.  ID: <code>STATS_HYP_WRITE_BANDWIDTH</code>  <div style="background-color: #f0f0f0; padding: 5px;"> <b>Note:</b> Virtual Machine entity is applicable for ESXi hypervisor.         </div>
Hypervisor I/O Latency	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Virtual Machine</li> </ul>	I/O latency in milliseconds from Hypervisor.  ID: <code>STATS_HYP_AVG_IO_LATENCY</code>  <div style="background-color: #f0f0f0; padding: 5px;"> <b>Note:</b> Virtual Machine entity is applicable for ESXi hypervisor.         </div>
Hypervisor I/O Latency - Read	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> </ul>	I/O read latency in milliseconds from Hypervisor.  ID: <code>STATS_HYP_AVG_READ_IO_LATENCY</code>  <div style="background-color: #f0f0f0; padding: 5px;"> <b>Note:</b> Cluster entity is applicable only for AHV hypervisor.         </div>
Hypervisor I/O Latency - Write	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> </ul>	I/O write latency in milliseconds from Hypervisor.  ID: <code>STATS_HYP_AVG_WRITE_IO_LATENCY</code>  <div style="background-color: #f0f0f0; padding: 5px;"> <b>Note:</b> Cluster entity is applicable only for AHV hypervisor.         </div>

Memory Usage	Entity Type(s)	Description
Metric		
Hypervisor IOPS	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Virtual Machine</li> </ul>	<p>Input/Output operations per second from Hypervisor. ID: <code>STATS_HYP_NUM_IOPS</code></p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• Cluster entity is applicable for AHV hypervisor.</li> <li>• Virtual Machine entity is applicable for ESXi.</li> </ul>
Hypervisor IOPS - Read	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Virtual Machine</li> </ul>	<p>Input/Output read operations per second from Hypervisor. ID: <code>STATS_HYP_NUM_READ_IOPS</code></p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• Cluster entity is applicable for AHV hypervisor.</li> <li>• Virtual Machine entity is applicable for ESXi.</li> </ul>
Hypervisor IOPS - Write	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Virtual Machine</li> </ul>	<p>Input/Output write operations per second from Hypervisor. ID: <code>STATS_HYP_NUM_WRITE_IOPS</code></p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• Cluster entity is applicable for AHV hypervisor.</li> <li>• Virtual Machine entity is applicable for ESXi.</li> </ul>
Hypervisor Memory Usage (%)	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Virtual Machine</li> </ul>	<p>Percent of memory used by the hypervisor. ID: <code>STATS_HYP_MEMORY_USAGE</code></p>
Logical Usage	Storage Container	<p>Logical usage of storage (physical usage divided by replication factor). ID: <code>STATS_UNTRANSFORMED_USAGE</code></p>
Memory Usage (%)	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Virtual Machine</li> </ul>	<p>Percentage of memory usage used by (any) hypervisor without HA. ID: <code>AGGREGATE_MEMORY_USAGE_PPM</code></p>
Overall Memory Usage (%)	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> </ul>	<p>Percentage of memory usage used by AHV with HA. ID: <code>OVERALL_MEMORY_USAGE_PPM</code></p>

Memory Usage	Entity Type(s)	Description
Metric		
Network Rx Bytes	Virtual Machine	<p>Number of bytes received from the network that is reported by the hypervisor.</p> <p>ID: <code>HYPERVERSOR_NUM_RECEIVED_BYTES</code></p> <p><b>Note:</b> Virtual Machine entity is applicable for AHV hypervisor.</p>
Network Tx Bytes	Virtual Machine	<p>Number of bytes transmitted from the network that is reported by the hypervisor.</p> <p>ID: <code>HYPERVERSOR_NUM_TRANSMITTED_BYTES</code></p> <p><b>Note:</b> Virtual Machine entity is applicable for AHV hypervisor.</p>
Physical Usage	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Disk</li> <li>• Storage Pool</li> <li>• Storage Container</li> </ul>	<p>Actual usage of storage.</p> <p>ID: <code>STATS_TRANSFORMED_USAGE</code></p>
Read IOPS (%)	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Disk</li> <li>• Storage Pool</li> </ul>	<p>Percent of IOPS that are reads.</p> <p>ID: <code>STATS_READ_IO_PPM</code></p>
Replication Bandwidth - Received	<ul style="list-style-type: none"> <li>• Cluster</li> <li>• Remote Site</li> <li>• Protection Domain</li> <li>• Replication Link</li> </ul>	<p>Replication data received per second in KB/second</p> <p>ID: <code>STATS REP BW RECEIVED</code></p>
Replication Bandwidth - Transmitted	<ul style="list-style-type: none"> <li>• Cluster</li> <li>• Remote Site</li> <li>• Protection Domain</li> <li>• Replication Link</li> </ul>	<p>Replication data transferred per second in KB/second</p> <p>ID: <code>STATS REP BW TRANSFERRED</code></p>

Memory Usage	Entity Type(s)	Description
Metric		
Replication Bytes - Received	<ul style="list-style-type: none"> <li>Cluster</li> <li>Remote Site</li> <li>Protection Domain</li> <li>Replication Link</li> </ul>	<p>Number of bytes received.</p> <p>ID: STATS REP NUM RECEIVED BYTES</p> <p><b>Note:</b> Cluster entity is applicable for AHV hypervisor.</p>
Replication Bytes - Total Received	Replication Link	<p>Total number of bytes received.</p> <p>ID: STATS REP TOT RECEIVED BYTES</p>
Replication Bytes - Total Transmitted	Replication Link	<p>Total number of bytes transmitted.</p> <p>ID: STATS REP TOT TRANSMITTED BYTES</p>
Replication Bytes - Transmitted	<ul style="list-style-type: none"> <li>Cluster</li> <li>Remote Site</li> <li>Protection Domain</li> <li>Replication Link</li> </ul>	<p>Number of bytes transmitted.</p> <p>ID: STATS REP NUM TRANSMITTED BYTES</p> <p><b>Note:</b> Cluster entity is applicable for AHV hypervisor.</p>
Storage Controller Bandwidth	<ul style="list-style-type: none"> <li>Cluster</li> <li>Storage Container</li> <li>Virtual Machine</li> <li>Volume Group</li> <li>Virtual Disk</li> </ul>	<p>Data transferred in KB/second from the Storage Controller.</p> <p>ID: STATS CONTROLLER BANDWIDTH</p>
Storage Controller Bandwidth - Read	<ul style="list-style-type: none"> <li>Cluster</li> <li>Storage Container</li> <li>Virtual Machine</li> <li>Volume Group</li> <li>Virtual Disk</li> </ul>	<p>Read data transferred in KB/second from the Storage Controller.</p> <p>ID: STATS CONTROLLER READ BANDWIDTH</p>
Storage Controller Bandwidth - Write	<ul style="list-style-type: none"> <li>Cluster</li> <li>Storage Container</li> <li>Virtual Machine</li> <li>Volume Group</li> <li>Virtual Disk</li> </ul>	<p>Write data transferred in KB/second from the Storage Controller.</p> <p>ID: STATS CONTROLLER WRITE BANDWIDTH</p>

Memory Usage	Entity Type(s)	Description
Metric		
Storage Controller IOPS	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Storage Container</li> <li>• Virtual Machine</li> <li>• Volume Group</li> <li>• Virtual Disk</li> </ul>	Input/Output operations per second from the Storage Controller ID: <code>STATS_CONTROLLER_NUM_IOPS</code> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <b>Note:</b> The Host entity is applicable for AHV hypervisor only. </div>
Storage Controller IOPS - Read	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Storage Container</li> <li>• Virtual Machine</li> <li>• Volume Group</li> <li>• Virtual Disk</li> </ul>	Input/Output read operations per second from the Storage Controller ID: <code>STATS_CONTROLLER_NUM_READ_IOPS</code> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <b>Note:</b> The Host entity is applicable for AHV hypervisor. </div>
Storage Controller IOPS - Read (%)	<ul style="list-style-type: none"> <li>• Cluster</li> <li>• Storage Container</li> <li>• Virtual Machine</li> <li>• Volume Group</li> <li>• Virtual Disk</li> </ul>	Percent of Storage Controller IOPS that are reads. ID: <code>STATS_CONTROLLER_READ_IO_PPM</code> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <b>Note:</b> The Host entity is applicable for AHV hypervisor. </div>
Storage Controller IOPS - Write	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Storage Container</li> <li>• Virtual Machine</li> <li>• Volume Group</li> <li>• Virtual Disk</li> </ul>	Input/Output write operations per second from the Storage Controller ID: <code>STATS_CONTROLLER_NUM_WRITE_IOPS</code>
Storage Controller IOPS - Write (%)	<ul style="list-style-type: none"> <li>• Cluster</li> <li>• Storage Container</li> <li>• Virtual Machine</li> <li>• Volume Group</li> <li>• Virtual Disk</li> </ul>	Percent of Storage Controller IOPS that are writes. ID: <code>STATS_CONTROLLER_WRITE_IO_PPM</code>

Memory Usage	Entity Type(s)	Description
Metric		
Storage Controller Latency	<ul style="list-style-type: none"> <li>Cluster</li> <li>Storage Container</li> <li>Virtual Machine</li> <li>Volume Group</li> <li>Virtual Disk</li> </ul>	<p>I/O latency in milliseconds from the Storage Controller.</p> <p>ID: STATS_CONTROLLER_AVG_IO_LATENCY</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>Cluster entity is applicable only for AHV hypervisor.</li> <li>Virtual Machine entity is applicable for AHV and Hyper-V hypervisors.</li> </ul>
Storage Controller Latency - Read	<ul style="list-style-type: none"> <li>Cluster</li> <li>Storage Container</li> <li>Virtual Machine</li> <li>Volume Group</li> <li>Virtual Disk</li> </ul>	<p>Storage Controller read latency in milliseconds.</p> <p>ID: STATS_CONTROLLER_AVG_READ_IO_LATENCY</p> <p><b>Note:</b> Cluster entity is applicable for AHV hypervisor.</p>
Storage Controller Latency - Write	<ul style="list-style-type: none"> <li>Cluster</li> <li>Storage Container</li> <li>Virtual Machine</li> <li>Volume Group</li> <li>Virtual Disk</li> </ul>	<p>Storage Controller write latency in milliseconds.</p> <p>ID: STATS_CONTROLLER_AVG_WRITE_IO_LATENCY</p> <p><b>Note:</b> Cluster entity is applicable for AHV hypervisor.</p>
Storage container own usage	Storage Container	<p>Storage container's own usage + Reserved (not used).</p> <p>ID: NEW_CONTAINER_OWN_USAGE_LOGICAL</p>
Swap In Rate	Virtual Machine	<p>Rate of data being swapped in.</p> <p>ID: STATS_HYP_SWAP_IN_RATE</p> <p><b>Note:</b> Virtual Machine entity is applicable for ESXi and Hyper-V hypervisors.</p>
Swap Out Rate	Virtual Machine	<p>Rate of data being swapped out.</p> <p>ID: STATS_HYP_SWAP_OUT_RATE</p> <p><b>Note:</b> Virtual Machine entity is applicable for ESXi and Hyper-V hypervisors.</p>

Memory Usage	Entity Type(s)	Description
Metric		
Virtual NIC bytes received packets with error.	Virtual Machine	<p>Virtual NIC bytes received packets with error.</p> <p><a href="#">STATS_NETWORK_ERROR_RECEIVED_PACKETS</a></p> <p><b>Note:</b> Virtual Machine entity is applicable for ESXi hypervisor.</p>
Virtual NIC bytes received rate.	Virtual Machine	<p>Virtual NIC bytes received rate in kbps.</p> <p><a href="#">STATS_NETWORK_RECEIVED_RATE</a></p> <p><b>Note:</b> Virtual Machine entity is applicable only for ESXi hypervisor.</p>
Virtual NIC bytes transmitted rate.	Virtual Machine	<p>Virtual NIC bytes transmitted rate in kbps.</p> <p><a href="#">STATS_NETWORK_TRANSMITTED_RATE</a></p> <p><b>Note:</b> Virtual Machine entity is applicable for ESXi hypervisor.</p>
Virtual NIC dropped transmitted packets.	Virtual Machine	<p>Number of dropped transmitted packets by the Virtual NIC.</p> <p><a href="#">STATS_NETWORK_DROPPED_TRANSMITTED_PACKETS</a></p> <p><b>Note:</b> Virtual Machine entity is applicable for ESXi hypervisor.</p>
Virtual NIC receive packets dropped.	Virtual Machine	<p>Number of receive packets dropped by the Virtual NIC.</p> <p><a href="#">STATS_NETWORK_DROPPED_RECEIVED_PACKETS</a></p> <p><b>Note:</b> Virtual Machine entity is applicable for ESXi hypervisor.</p>
Write IOPS (%)	<ul style="list-style-type: none"> <li>• Host</li> <li>• Cluster</li> <li>• Disk</li> <li>• Storage Pool</li> </ul>	<p>Percent of IOPS that are writes.</p> <p>ID: <a href="#">STATS_WRITE_IO_PPM</a></p>

## Exporting Performance Data

This topic describes how to view and export the performance chart.

### About this task

Performance data is available for three months. You can export the performance data results in CSV or JSON format.

### Procedure

1. Log into the Prism Element web console.

2. In the [Analysis Dashboard](#) on page 330, click **Home > Analysis**.  
The **Analysis** page displays.
3. Click the **Range** drop-down list and set the range to **1 Month**.  
The **1 Month** range shows the data in monthly segments.
4. Export the performance data into a CSV or JSON file. Click the drop-down arrow next to the cluster chart you want to export.



**Figure 52: Export Performance Data**

# ALERTS AND EVENTS

---

For information about Alerts and Events in Prism Element web console, see [Prism Element Alerts and Events Reference Guide](#).

# VIEW TASK STATUS

---

The web console displays detailed information about all tasks that have been performed on the cluster.

## Task Page Navigation

- To view the Task dashboard, log in to Prism Element web console, and select **Home > Tasks**.
- An icon also appears in the main menu when one or more tasks are active (running or completed within the last 48 hours). The icon appears blue when a task runs normally, yellow when it generates a warning, or red when it fails. Clicking the icon displays a drop-down list of active tasks; clicking the **View All Tasks** button at the bottom of that list displays a details screen with information about all tasks for this cluster.

**Note:** The drop-down list of active tasks may include a **Clean Up** button (top right). Clicking this button removes from the list any tasks that are no longer running. However, this applies to the current session only. The full active list (including the non-running tasks) appears when you open a new Prism Element web console session.

- When multiple tasks are active, you can filter the list by entering a name in the filter by field.
- You can also filter the list by clicking the **Filters** button and selecting the desired filter options

Each task appears in the list for a minimum of one hour after completion, but how long that task remains in the list depends on several factors. In general, the maximum duration is two weeks. However, tasks are rotated off the list as new tasks arrive, so a task might disappear from the list much sooner when activity is high. In some cases a task appears for longer than two weeks because the last task for each component is retained in the listing.

## View Task Status Dashboard

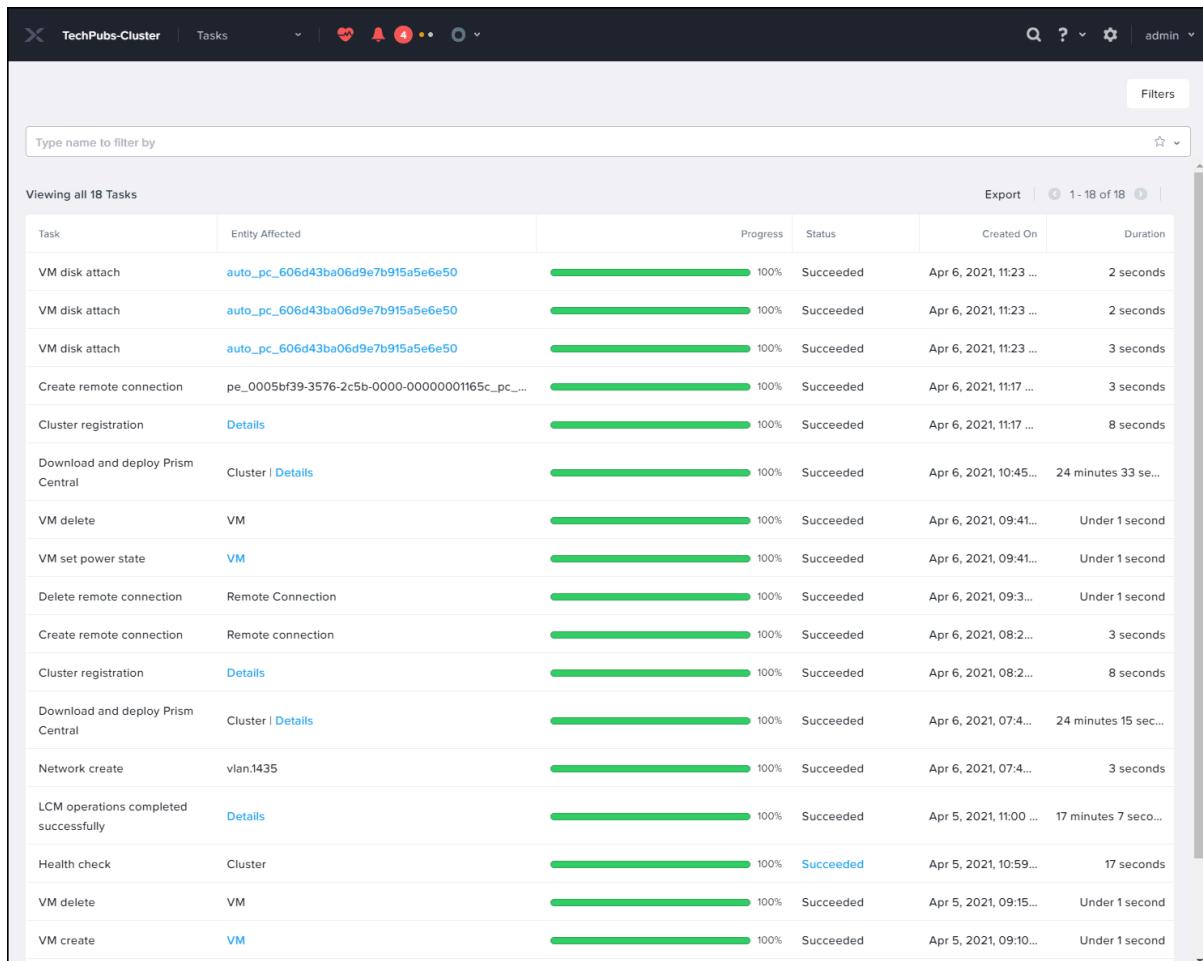


Figure 53: Task Dashboard

Table 64: Tasks List Fields

Parameter	Description	Values
Task	Specifies which type of operation the task is performing.	Any cluster operation you can perform in the Prism Element web console
Entity Affected	Display the entity on which task has been performed. If the link appears on the entity, click it to display the details.	Entity description
Percent	Indicates the current percentage complete for the task.	0%-100%
Status	Indicates the task status, which can be pending, running, completed, or failed.	pending, running, completed, failed
Created On	Displays when the task began.	seconds, minutes, hours

Parameter	Description	Values
Duration	Displays how long the task took to complete.	seconds, minutes, hours

# SYSTEM MANAGEMENT

---

The web console allow you to configure various system settings.

- You can specify one or more name servers. For more information, see [Configuring Name Servers](#) on page 349.
- If Acropolis is enabled, you can configure one or more network connections. For more information, see [Network Configuration for VM Interfaces](#) on page 162.
- You can create a whitelist of IP addresses that are allowed access. For more information, see [Configuring a Filesystem Whitelist](#) on page 348.
- You can specify one or more NTP servers for setting the system clock. For more information, see [Configuring NTP Servers](#) on page 350.
- You can configure one or more network switches for statistics collection. For more information, see [Configuring a Network Switch](#) on page 167.
- You can specify an SMTP mail server. For more information, see [Configuring an SMTP Server](#) on page 351.
- You can configure SNMP. For more information, see [Configuring SNMP](#) on page 351.
- You can configure a login banner page. For more information, see [Configuring a Banner Page](#) on page 361.

## Configuring a Filesystem Whitelist

### About this task

An allowlist is a set of addresses that are allowed access to the cluster. Allowlists are used to allow appropriate traffic when unauthorized access from other sources is denied. If you set an allowlist at storage container level, the system overrides any global whitelist for this storage container.

Setting an allowlist helps you provide access to the container via NFS. Some manual data migration workflows might require the allowlist to be configured temporally, while some third-party backup vendors might require the allowlist to be configured permanently to access the container via NFS.

#### Caution:

- There is no user authentication for NFS access, and the IP address in the allowlist has full read or write access to the data on the container.
- It is recommended to allow single IP addresses (with net mask such as 255.255.255.255) instead of allowing subnets (with netmask such as 255.255.255.0).
- Using a Nutanix storage container as a general-purpose NFS or SMB share is not supported. Because the Nutanix solution is VM-centric, the preferred mechanism is to deploy a VM that provides file share services.

To add (or delete) an address to (from) the filesystem allowlist, do the following:

### Procedure

1. Click the gear icon in the main menu and then select **Filesystem Whitelists** in the **Settings** page. The **Filesystem Whitelists** dialog box appears.

- To add an address to the allowlist, do the following in the indicated fields:

- IP address:** Enter the IP address.
- Netmask:** Enter the netmask value.
- Click the **+Add** button.

The entry is added to the **Whitelist Entry** list. An NFS allowlist is created when the hypervisor is ESXi or AHV; a CIFS allowlist is created when the hypervisor is Hyper-V.

- To delete an entry from the allowlist, click the X icon for that entry in the **Whitelist Entry** list.

A window prompt appears to verify the action; click the **OK** button. The entry is removed from the list.

## Configuring Name Servers

### About this task

Name servers are computers that host a network service for providing responses to queries against a directory service, such as a DNS server. To add (or delete) a name server, do the following:

### Procedure

- Log in to the Prism Element web console.
- Click the gear icon in the main menu and then select **Name Servers** in the **Settings** page.  
The **Name Servers** dialog box appears.
- To add a name server, enter the server IP address in the **Server IP** field and then click the **Add** button to the right of that field.  
The server is added to the **IP Address** list (below the **Server** field).

**Note:** Changes in name server configuration may take up to 5 minutes to take effect. Functions that rely on DNS may not work properly during this time. You can configure a maximum of three name servers.

- To delete a name server entry, click the X icon for that server in the **IP Address** list.  
A window prompt appears to verify the action; click the **OK** button. The server is removed from the list.

## Cluster Time Synchronization

Network Time Protocol (NTP) is a protocol for clock synchronization between computers. The hosts and CVMs in a Nutanix cluster must be configured to synchronize their system clocks with a list of stable NTP servers. Accurate timestamps are important for troubleshooting interactions with third-party software products such as Veeam or CommVault, which might require time synchronization between the hypervisor and the Controller VM to determine which files to back up. Accurate time synchronization between Nutanix clusters paired in Disaster Recovery (DR) configurations also ensures that snapshots do not expire too quickly or too late.

Graphs in the Prism interface rely on CVM time, and incorrect time skews graphs, especially in relation to other monitoring platforms such as vCenter, which rely on other clock sources.

## Recommendations for Time Synchronization

Adhere to the following guidelines when configuring time synchronization on a Nutanix cluster:

- Where possible, synchronize Nutanix clusters with internal NTP sources to ensure stability from both a network and a security vulnerability perspective. When you cannot avoid using an external NTP source, Nutanix recommends that you use a time source maintained by your national government.

- Make sure to specify at least five stable time sources that have a high degree of accuracy and that can be reached over a reliable network connection. Generally, the lower the stratum of an NTP source, the higher its accuracy.

Note that three is the minimum to identify one time source as a false ticker but provides no redundancy, four is the minimum for redundancy, and five is the recommended minimum for a good configuration.

If you want to use off-site NTP servers, see [Selecting Offsite NTP Servers](#) from the Network Time Protocol site for various recommendations. Review all the information in this section before choosing pool.ntp.org servers for your NTP use.

**Note:** Using a pool.ntp.org server is not appropriate for all circumstances. For more context, see the [Additional Notes](#) section.

- Do not use rate-limited NTP servers.
- Synchronizing a Nutanix cluster with a Windows time source is known to cause issues over a period of time, so Nutanix recommends that you not synchronize a cluster's time with Windows NTP sources. Use reliable non-Windows time sources instead. In an Active Directory domain, the best practice (a design that both works around and improves upon having to include domain controllers in the list of NTP sources) is to bypass the domain controllers and to synchronize the Nutanix hosts and CVMs directly with the NTP sources with which the domain controllers synchronize their time. Specify a common list of at least five reliable non-Windows NTP sources for both the domain controllers and the Nutanix cluster.

Bypassing the domain controller as a time source is not an option for Hyper-V clusters owing to Kerberos requirements. When being joined to a domain, Nutanix clusters running Hyper-V detect local domain controllers and add them to all CVMs as NTP sources. For Hyper-V clusters, supplement the list of detected domain controllers with as many reliable non-Windows NTP sources as are required to meet the recommendation of a minimum of five NTP time sources. For example, if the Nutanix cluster adds two domain controllers as time sources, specify at least three reliable non-Windows NTP sources in the NTP server list. Specifying additional non-Windows NTP sources is necessary even if the domain controllers synchronize their time with a time source that is considered to be reliable.

- Specify public NTP servers by using their FQDN to help mitigate issues caused by IP address changes.

## Configuring NTP Servers

### About this task

To add (or delete) an NTP server entry, do the following:

### Procedure

1. Log in to the Prism Element web console.
2. Click the gear icon in the main menu and then select **NTP Servers** in the **Settings** page.  
The **NTP Servers** dialog box appears.
3. To add an NTP server entry, enter the server IP address or fully qualified host name in the **NTP Server** field and then click the **Add** button to the right of that field.  
The name or address is added to the **HOST NAME OR IP ADDRESS** list (below the **NTP Server** field).
4. To delete an NTP server entry, click the cross icon for that server in the **Servers** list.  
A window prompt appears to verify the action; click the **OK** button. The server is removed from the list.

# Configuring an SMTP Server

## About this task

Simple Mail Transport Protocol (SMTP) is an Internet standard protocol for electronic mail transmission across Internet Protocol (IP) networks, and Nutanix systems use SMTP to send alert emails.

If you have an external firewall deployed in your organization, see [Ports and Protocols](#) to allow traffic from the cluster to Nutanix Support servers.

**Note:** Since Nutanix CVM has FIPS authentication enabled, the SMTP client in the Nutanix CVM is incompatible with an SMTP server with CRAM-MD5 Authentication enabled.

To configure an SMTP server entry, do the following:

## Procedure

1. Log in to the Prism Element web console.
2. Click the gear icon in the main menu and then select **SMTP Server** in the **Settings** page.  
The **SMTP Server Settings** dialog box appears.
3. Do the following in the indicated fields:
  - a. **Host Name or IP Address:** Enter the IP address or fully qualified domain name for the SMTP server.
  - b. **Port:** Enter the port number to use.  
The standard SMTP ports are 25 (unencrypted), 587 (TLS), and 465 (SSL). For the complete list of required ports, see [Port Reference](#).
  - c. **Security Mode:** Enter the desired security mode from the pull-down list.  
The options are NONE (unencrypted), STARTTLS (use TLS encryption), and SSL (use SSL encryption).
  - d. **User:** Enter a user name.  
The **User** and **Password** fields apply only when a secure option (STARTTLS or SSL) is selected. The user name might need to include the domain depending on the authentication process.
  - e. **Password:** Enter the user password.
  - f. **From Email Address** (optional): Enter an e-mail address that appears as the sender address.  
By default, alert and cluster status information e-mails display *cluster@nutanix.com* as the sender address. You have the option to replace that address with a custom address by entering a sender address in this field.
4. When all the fields are correct, click the **Save** button.

# Configuring SNMP

## About this task

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. Nutanix systems include an SNMP agent that provides interoperability with industry standard SNMP manager systems. Nutanix also provides a custom Management Information Base (MIB) for Nutanix-specific information.

**Note:**

- The Net-SNMP package version 5.7.2 does not support 256-bit AES encryption.

- Nutanix recommends that you configure your SNMP manager to use the virtual IP address of the cluster to communicate with the Nutanix SNMP agent instead of the Controller VM IP address.

To configure SNMP, do the following:

### Procedure

1. Log in to the Prism Element web console.
2. Click the gear icon in the main menu and then select **SNMP** in the **Settings** page. The **SNMP Configuration** dialog box appears.
3. To enable SNMP for this cluster, select the **Enable SNMP** checkbox. To disable SNMP, clear the checkbox.

**Note:**

SNMP traps are sent by the Controller VM that functions as the Alert Manager leader. If you need to open your firewall to receive the traps, keep in mind that the Alert Manager leader can rotate during tasks like AOS or host upgrades. Therefore, it might be necessary to open all the Controller VM IP addresses to ensure that the traps are received.

4. To view the Nutanix MIB (NUTANIX-MIB.txt), click the **View MIB** link. To download NUTANIX-MIB.txt, right-click and select the appropriate download action for your browser and then copy NUTANIX-MIB.txt to your SNMP manager systems.

See your SNMP manager documentation for instructions on how to install the Nutanix MIB.

5. To add an SNMP transport, click the **Transports** tab and the **New Transport** button, and then do the following in the indicated fields. An SNMP transport is a combination of the transport protocol and port number on which you want the Nutanix SNMP agent to receive queries. SNMP transports enable you to combine transport protocols and port numbers other than the default port number. The port numbers that are specified in SNMP transports are unblocked on the Controller VM, making them available to receive queries:

- a. **Protocol:** Select the protocol to use from the drop-down list.

The options are **TCP**, **TCP6**, **UDP**, and **UDP6**.

- b. **Port:** Enter the port number to use.

The standard SNMP port number is 161. For the complete list of required ports, see [Ports and Protocols](#).

- c. When the fields are correct, click the **Save** button (lower right).

This saves the configuration and redisplays the dialog box with the new transport appearing in the list.

**Note:** To return to the **SNMP Configuration** window without saving, click the **Cancel** button.

6. To add an SNMP user entry, click the **Users** tab and the **New User** button and then do the following in the indicated fields:
  - a. **Username:** Enter a user name.
  - b. **Priv Type:** Select the privacy encryption type from the pull-down list.  
The only option is **AES** (Advanced Encryption Standard). In the nCLI, this setting is optional.
  - c. **Priv Key:** Enter a privacy key phrase (password) into this field.
    - The key phrase is AES encrypted when the user is created.
    - The password you choose must meet the following complexity requirements:
      - Contain a minimum 8 characters and a maximum 64 characters.
      - Contain one upper case letter (A-Z).
      - Contain one lower case letter (a-z).
      - Contain one digit (0-9).
      - Contain only the following special characters: ~ @ # \$ % \* - = \_ + { } | [ ] ? , . : &.
  - d. **Auth Type:** Select the authentication hash function type from the drop-down list.  
The only option is **SHA** (Secure Hash Algorithm).
  - e. **Auth Key:** Enter an authentication key phrase (password) into this field.
    - The key phrase is SHA-1 encrypted when the user is created.
    - The password you choose must meet the following complexity requirements:
      - Contain a minimum 8 characters and a maximum 64 characters.
      - Contain one upper case letter (A-Z).
      - Contain one lower case letter (a-z).
      - Contain one digit (0-9).
      - Contain only the following special characters: ~ @ # \$ % \* - = \_ + { } | [ ] ? , . : &.
  - f. When all the fields are correct, click the **Save** button (lower right).  
This saves the configuration and redisplays the dialog box with the new user entry appearing in the list.

7. To add an SNMP trap receiver, click the **Traps** tab and the **New Trap Receiver** button, and then do the following in the indicated fields:

  - a. **Receiver Name:** Enter the receiver name.
  - b. **SNMP Version:** Select (click the radio button for) the SNMP version, either v3 or v2c. For SNMP v2c, Nutanix supports only SNMP TRAP and not SNMP GET.
  - c. This field is displayed based on your selection in the **SNMP Version**:
    - **Trap Username:** This field is displayed if you select v3 in the **SNMP Version**. Select a user from the drop-down list.
    - **Community:** This field is displayed if you select v2c in the **SNMP Version**. The default value for v2c trap community is public, or you can enter any other name of your choice.All users added previously (see Step 5) appear in the drop-down list. You cannot add a trap receiver entry until at least one user has been added.
  - d. **Address:** Enter the target address.

An SNMP target address specifies the destination and user that receives outgoing notifications, such as trap messages. SNMP target address names must be unique within the managed device.
  - e. **Port:** Enter the port number to use.

The standard SNMP port number is 161. For the complete list of required ports, see [Ports and Protocols](#).
  - f. **Engine ID:** Optionally, enter an engine identifier value, which must be a hexadecimal string between 5 and 32 characters long.

If you do not specify an engine ID, an engine ID is generated for you for use with the receiver. Every SNMP v3 agent has an engine ID that serves as a unique identifier for the agent. The engine ID is used with a hashing function to generate keys for authentication and encryption of SNMP v3 messages.
  - g. **Inform:** Select **True** from the drop-down list to use inform requests as the SNMP notification method; select **False** to use traps as the SNMP notification method.

SNMP notifications can be sent as traps or inform requests. Traps are one-way transmissions; they do not require an acknowledgment from the receiver. Informs expect a response. If the sender never receives a response, the inform request can be sent again. Therefore, informs are more reliable than traps. However, informs consume more resources. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and add overhead on the network. Thus, traps and inform requests provide a trade-off between reliability and resources.

**Note:** The SNMP server is blocked if it doesn't get a response to the inform traps in five consecutive attempts.
  - h. **Transport Protocol:** Select the protocol to use from the drop-down list.

The options are **TCP**, **TCP6**, **UDP**, and **UDP6**.
  - i. When all the fields are correct, click the **Save** button (lower right).

This saves the configuration and redisplays the dialog box with the new trap entry appearing in the list.
  - j. To test all configured SNMP traps, click the **Traps** tab, and then click **Test All**.

The Nutanix cluster sends test alerts to all the SNMP trap receivers configured on the cluster.
8. To edit a user or trap receiver entry, click the appropriate tab (**Users** or **Traps**) and then click the pencil icon for that entry in the list.

An edit window appears for that user or trap receiver entry with the same fields as the add window. (Transport entries cannot be edited.) Enter the new information in the appropriate fields and then click the **Save** button.

- To delete an SNMP entry, click the appropriate tab (**Transports**, **Users**, or **Traps**) and then click the X icon for that entry in the list.  
A window prompt appears to verify the delete action; click the **OK** button. The entry is removed from the list.

## Nutanix MIB

### Overview

The Simple Network Management Protocol (SNMP) enables administrators to monitor network-attached devices for conditions that warrant administrative attention. In the Nutanix SNMP implementation, information about entities in the cluster is collected and made available through the Nutanix MIB (NUTANIX-MIB.txt). The Nutanix enterprise tree is located at 1.3.6.1.4.1.41263.

The Nutanix MIB is divided into the following sections:

- Cluster information.* Status information about the cluster as a whole.
- Software version information.* Version information about the software packages that comprise the Controller VM.
- Service status information.* Information about the status of essential services on each Controller VM.
- Hypervisor information.* Information about each hypervisor instance.
- Virtual machine information.* Information about hosted virtual machines.
- Disk information.* Status information about the disks in the cluster.
- Controller VM resource information.* Indicate how much CPU and memory capacity is available to a Controller VM.
- Storage pool information.* Status information about the storage pools in the cluster.
- Storage Container information.* Status information about the disks in the cluster.
- Alerts information.* Information about generated alerts that can be captured through the SNMP trap (or inform) mechanism.

**Important:** A statistic (counter) value resets to zero and starts increasing again after it reaches the maximum limit defined for its corresponding data type. The counter reinitialization is compliant with the *RFC 2578* standard.

For example, the *vmRxBytes* statistic monotonically increases until it reinitializes on reaching a maximum value of its data type (Counter64).

**Table 65: Cluster Information Fields**

Name	Description	Data Type
clusterName	Cluster name.	Display string
clusterVersion	Cluster version number. This is the Nutanix core package version expected on all the Controller VMs.	Display string
clusterStatus	Current status of the cluster. Possible values are <i>started</i> and <i>stopped</i> .	Display string
clusterTotalStorageCapacity	Total storage capacity of the cluster in bytes.	Unsigned 64-bit integer
clusterUsedStorageCapacity	Storage used on the cluster, in bytes.	Unsigned 64-bit integer

Name	Description	Data Type
clusterIOPS	Average I/O operations per second (IOPS) in the cluster.	Unsigned 64-bit integer
clusterLatency	Average I/O latency in the cluster, in milliseconds.	Unsigned 64-bit integer
clusterIOBandwidth	Cluster-wide I/O bandwidth in kilobytes per second (KBps).	Unsigned 64-bit integer

**Table 66: Software Version Information Fields**

Name	Description	Data Type
svtIndex	Unique index that is used to identify an entry in the software version information table.	Signed 32-bit integer
svtControllerVMIId	Nutanix Controller VM identification number.	Display string
svtNutanixBootstrap	Nutanix bootstrap software package version.	Display string
svtNutanixInfrastructure	Nutanix infrastructure software package version.	Display string
svtNutanixCore	Nutanix core software package version.	Display string
svtNutanixToolchain	Nutanix toolchain software package version.	Display string
svtNutanixServiceability	Nutanix serviceability software package version.	Display string
svtLinuxKernel	Linux kernel version currently installed.	Display string

**Table 67: Service Status Information Fields**

Name	Description	Data Type
cstIndex	Unique index that is used to identify an entry in the service status information table.	Signed 32-bit integer
cstControllerVMIId	Nutanix Controller VM identification number.	Display string
cstControllerVMStatus	Status of the Nutanix node.	Display string
cstDataServiceStatus	Status of the core data services on the Controller VM.	Display string
cstMetadataServiceStatus	Status of the metadata services on the Controller VM.	Display string

**Table 68: Hypervisor Information Fields**

Name	Description	Data Type
hypervisorIndex	Number that is used to uniquely identify an entry in the hypervisor information table.	Signed 32-bit integer

Name	Description	Data Type
hypervisorID	System-generated string that Nutanix uses to uniquely identify a hypervisor instance.	Display string
hypervisorName	Name of the hypervisor instance.	Display string
hypervisorVmCount	Number of VMs configured on the hypervisor instance.	Unsigned 32-bit integer
hypervisorCpuCount	Number of CPU cores available to the hypervisor instance.	Unsigned 32-bit integer
hypervisorCpuUsagePercentage	Percentage of CPU resources in use by the hypervisor instance.	Unsigned 32-bit integer
hypervisorMemory	Total memory available to the hypervisor instance, in bytes.	Counter64
hypervisorMemoryUsagePercentage	Memory in use by the hypervisor instance, as a percentage of the total available memory.	Unsigned 64-bit integer
hypervisorReadIOPerSecond	Total number of read I/O operations per second (IOPS) being performed by the hypervisor.	Unsigned 32-bit integer
hypervisorWriteIOPerSecond	Total number of write I/O operations per second (IOPS) being performed by the hypervisor.	Unsigned 32-bit integer
hypervisorAverageLatency	Average I/O latency of the hypervisor in microseconds ( $\mu$ s).	Counter64
hypervisorIOBandwidth	I/O bandwidth of the hypervisor in kilobytes per second (Kbps).	Counter64
hypervisorRxBytes	Total number of bytes received by the hypervisor.	Counter64
hypervisorTxBytes	Total number of bytes transmitted by the hypervisor.	Counter64
hypervisorRxDropCount	Total number of packets dropped by the hypervisor when receiving data.	Counter64
hypervisorTxDropCount	Total number of packets dropped by the hypervisor when transmitting data.	Counter64

**Table 69: Virtual Machine Information Fields**

Name	Description	Data Type
vmIndex	Number that is used to uniquely identify an entry in the VM information table.	Signed 32-bit integer
vmlId	System-generated string that Nutanix uses to uniquely identify a virtual machine.	Display string
vmName	Name of the VM.	Display string
vmHypervisorId	System-generated ID of the hypervisor on which the VM is provisioned.	Display string
vmPowerState	Power state of the VM.	Display string

Name	Description	Data Type
vmCpuCount	Number of CPU cores available to the VM.	Unsigned 32-bit integer
vmCpuUsagePercent	Percentage of CPU resources in use by the VM.	Unsigned 32-bit integer
vmMemory	Total memory allocated to the VM, in bytes.	Counter64
vmMemoryUsagePercent	Memory in use by the VM, as a percentage of the total allocated memory.	Unsigned 64-bit integer
vmReadIOPerSecond	Total number of read I/O operations per second (IOPS) being performed by the VM.	Unsigned 32-bit integer
vmWriteIOPerSecond	Total number of write I/O operations per second (IOPS) being performed by the VM.	Unsigned 32-bit integer
vmAverageLatency	Average I/O latency of the VM, in microseconds ( $\mu$ s).	Counter64
vmIOBandwidth	I/O bandwidth of the VM in kilobytes per second (KBps).	Counter64
vmRxBytes	Total number of bytes received by the VM.	Counter64
vmTxBytes	Total number of bytes transmitted by the VM.	Counter64
vmRxDropCount	Total number of packets dropped by the VM when receiving data.	Counter64
vmTxDropCount	Total number of packets dropped by the VM when transmitting data.	Counter64

**Table 70: Disk Information Fields**

Name	Description	Data Type
dstIndex	Number that is used to uniquely identify an entry in the disk information table.	Signed 32-bit integer
dstDiskId	Disk identification number. The number is unique for each disk.	Display string
dstControllerVMIId	Nutanix Controller VM identification number.	Display string
dstSerial	Disk serial number.	Display string
dstNumRawBytes	Physical storage capacity on the device, in terms of number of raw bytes.	Unsigned 64-bit integer
dstNumTotalBytes	Usable storage on the device through its file system, in terms of number of usable bytes.	Unsigned 64-bit integer
dstNumFreeBytes	Available storage on the device through its file system for non-root users, in terms of number of free bytes.	Unsigned 64-bit integer
dstNumTotalInodes	Total number of usable inodes on the device through its file system.	Unsigned 64-bit integer

Name	Description	Data Type
dstNumFreelnodes	Total number of available (free) inodes on the device through its file system for non-root users.	Unsigned 64-bit integer
dstAverageLatency	Average I/O latency of the disk in microseconds ( $\mu\text{s}$ ).	Unsigned 64-bit integer
dstIOPBandwidth	I/O bandwidth of the disk in kilobytes per second (KBps).	Unsigned 64-bit integer
dstNumberlops	Current number of I/O operations per second (IOPS) for the disk.	Unsigned 64-bit integer
dstState	State of the disk.	Signed 32-bit integer

**Table 71: Controller VM Resource Information Fields**

Name	Description	Data Type
crtIndex	Number that is used to uniquely identify an entry in the Controller VM resource information table.	Signed 32-bit integer
crtControllerVMId	Nutanix Controller VM identification number.	Display string
crtMemory	Total memory available to the Controller VM in bytes.	Unsigned 64-bit integer
crtNumCpus	Total number of CPUs allocated to the Controller VM.	Signed 32-bit integer
crtName	Name of the Controller VM.	Display string

**Table 72: Storage Pool Information Fields**

Name	Description	Data Type
spitIndex	Number that is used to uniquely identify an entry in the storage pool information table.	Signed 32-bit integer
spitStoragePoolId	Storage pool identification number.	Display string
spitStoragePoolName	Storage pool name.	Display string
spitTotalCapacity	Total storage pool capacity in bytes.	Unsigned 64-bit integer
spitUsedCapacity	Used storage pool capacity in bytes.	Unsigned 64-bit integer
spitIOPerSecond	Current number of I/O operations per second (IOPS) for this storage pool.	Signed 32-bit integer
spitAvgLatencyUseconds	Average I/O latency for the storage pool in microseconds.	Unsigned 64-bit integer
spitIOPBandwidth	I/O bandwidth of the storage pool in kilobytes per second (KBps).	Unsigned 64-bit integer

**Table 73: Storage Container Information Fields**

Name	Description	Data Type
citIndex	Number that is used to uniquely identify an entry in the storage container information table.	Signed 32-bit integer
citContainerId	Storage Container identification number.	Display string
citContainerName	Storage Container name.	Display string
citTotalCapacity	Total storage container capacity in bytes.	Unsigned 64-bit integer
citUsedCapacity	Used storage container storage in bytes.	Unsigned 64-bit integer
citIOPerSecond	Current number of I/O operations per second (IOPS) for this storage container.	Signed 32-bit integer
citAvgLatencyUsecs	Average I/O latency for the storage container in microseconds.	Unsigned 64-bit integer
citIOBandwidth	I/O bandwidth of the storage container in kilobytes per second (Kbps).	Unsigned 64-bit integer

### Trap Resolution

In addition to generating an SNMP trap when an alert condition is detected, Nutanix clusters generate a trap when an alert condition is resolved. The resolved trap, named ntxTrapResolved, is generated regardless of whether the alert condition is resolved manually or automatically. If a Prism Central alert is resolved in Prism Central, Prism Central sends a resolved trap. If a Nutanix cluster alert is resolved in either the Prism Element web console or Prism Central, both Prism Central and the cluster send a resolved trap.

In this section, the terms *original alert* and *original trap* are used to refer, respectively, to the alert and trap that are generated when the alert condition is detected, and the terms *resolved alert* and *resolved trap* are used to refer, respectively, to the alert and trap that are generated when the alert condition is resolved.

To enable you to associate a resolved trap with the original alert and original trap, the UUID of the original alert is included in the original trap, as part of the alert message (ntxAlertDisplayMsg), and in the resolved trap, as a MIB object (ntxAlertUuid).

A resolved trap has the following MIB objects:

- ntxTrapName (name of the original trap)
- ntxAlertUuid (UUID of the original alert)
- ntxAlertResolvedTime
- ntxAlertDisplayMsg (message of the original alert)
- ntxAlertTitle (title of the original alert)
- ntxAlertSeverity (severity of the original alert)

The fields are described in the rows that follow.

**Table 74: Alerts Information Fields**

Name	Description	Data Type
ntxAlertCreationTime	Time of alert creation. The value is the number of seconds since the UNIX epoch (01/01/1970).	Unsigned 64-bit integer
ntxAlertDisplayMsg	Alert message text.	Display string
ntxAlertTitle	Alert title.	Display string
ntxAlertSeverity	Alert severity, which has one of the following values:  1. Informational 2. Warning 3. Critical 4. Audit	Integer
ntxTrapName	Name of the trap that was generated when the alert condition was detected. This MIB object is included in resolved traps.	Display string
ntxAlertUuid	UUID of the alert that was generated when the alert condition was detected. This MIB object is included in resolved traps.	Display string
ntxAlertResolvedTime	Time at which the alert was resolved. The value is the number of seconds since the UNIX epoch (01/01/1970). This MIB object is included in resolved traps.	Unsigned 64-bit integer

## Configuring a Banner Page

You have the option to create a welcome banner, which will be the first screen that appears when a user attempts to log into the web console. The content of the banner page is configurable, and it can include a custom message and graphics.

### About this task

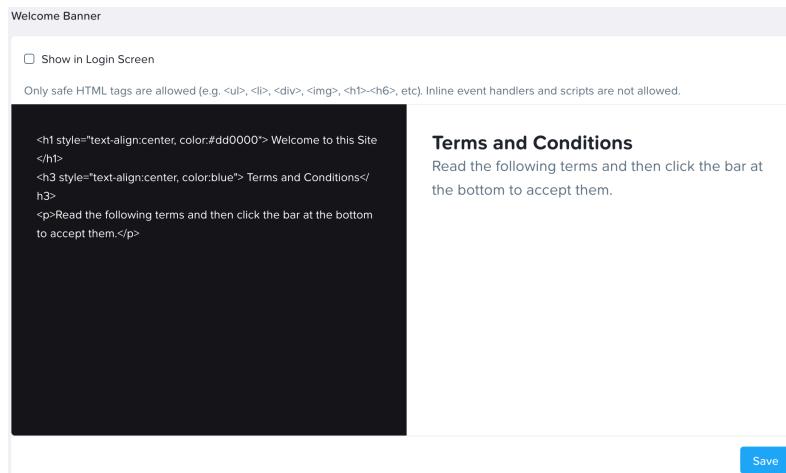
To configure a banner page, do the following:

### Procedure

1. Log in to the Prism Element web console.
2. Click the gear icon in the main menu and then select **Welcome Banner** in the **Settings** page.  
The **Edit Welcome Banner** dialog box appears.
3. Enter (paste) the desired content in HTML format in the pane on the left.  
Only *safe* HTML tags are supported. Inline event handlers, scripts, and externally-sourced graphics are not allowed.
4. Click the **Preview** button to display the banner in the pane on the right.
5. If the banner is not correct, update the HTML code as needed until the preview pane displays the desired message.

- When the preview is correct, check the **Enable Banner** box (lower left) and then the **Save** button.  
You can disable (or enable) the banner at any time by clearing (selecting) the **Enable Banner** checkbox.

**Note:** A live banner page includes an *Accept terms and conditions* bar at the bottom. Clicking on this bar sends the user to the login page.



**Figure 54: Welcome Banner Window**

## Registering a Cluster to vCenter Server using Prism Element

Register your cluster with an external vCenter Server using the Prism Element web console.

### Before you begin

If you choose to register a cluster with a vCenter Server using extension-based authentication, ensure that you have the required extension privileges. These privileges provide permission to register the cluster with vCenter using extension-based authentication.

### About this task

To perform core VM management operations directly from the Prism Element web console without switching to vCenter Server, you must register your cluster with vCenter Server.

- Nutanix stores external vCenter Server credentials only when you register the cluster with vCenter Server using SSO-based authentication. Nutanix does not store credentials when you use extension-based authentication for registration.
- Whenever a new node is added to Nutanix cluster, vCenter Server registration for the new node is automatically performed.
- Nutanix supports vCenter Enhanced Linked Mode.

When registering a Nutanix cluster to a vCenter Enhanced Linked Mode (EHM) enabled ESXi environment, ensure that Prism is registered to the vCenter containing the vSphere Cluster and Nutanix nodes (often the local vCenter). For information on vCenter Enhanced Linked Mode, see *vCenter Enhanced Linked Mode* in the *vCenter Server Installation and Setup* documentation.

To register a cluster with a vCenter Server, follow these steps:

### Procedure

- Log into the Prism Element web console.

2. Click **Settings** from the dropdown menu.  
The system displays the **Global Settings** page.
3. From the **Setup** section in the left navigation menu, click **vCenter Integration**.  
The system displays the **vCenter Integration** page, where the system automatically discovers the vCenter Server that manages the hosts in the cluster.
4. Click the **Connect** option associated with the vCenter Server to register.  
The system displays the IP address of the vCenter Server in the **IP ADDRESS** field and the port number in the **PORT** field.

**Note:** Do not change the port number. For the complete list of required ports, see [Ports and Protocols](#).

5. From the **Choose an Authentication Method** section, select one of the following:
  - » **EXTENSION**: Choose this option to register using the extension-based authentication method.
  - » **SSO**: Choose this option to register using the SSO-based authentication method.
6. In the **ADMIN USERNAME** and **ADMIN PASSWORD** fields, enter the administrator user name and password of the external vCenter Server.
7. Click **Connect**.  
The system starts registering the cluster with the vCenter Server and a certificate is generated to communicate with the vCenter Server.

After registration is complete, the **Status** column for the vCenter Server shows **Active**, and the **Integration Type** column displays the method you used to register the cluster. Also, a relevant message is displayed in the **Tasks** dashboard. The **Host Connection** column displays **Connected**, which implies that all the hosts are being managed by the vCenter Server to which the cluster is registered.

## Unregistering a Cluster from the vCenter Server using Prism Element

Unregister a cluster from the vCenter Server.

### About this task

To unregister a cluster from a vCenter Server, follow these steps:

### Procedure

1. Log into the Prism Element web console.
2. Click **Settings** from the dropdown menu.  
The system displays the **Global Settings** page.
3. From the **Setup** section in the left navigation menu, click **vCenter Integration**.  
The system displays the **vCenter Integration** page, where the system lists the vCenter Server registered to the cluster.
4. Click **Disconnect**.

5. Perform one of the following: The system starts unregistering the vCenter Server from the cluster.
  - » If the cluster was registered to the vCenter Server using SSO-based authentication, click **Disconnect**.
  - » If the cluster was registered to the vCenter Server using extension-based authentication, enter the administrator user name and password of the vCenter Server in the **ADMIN USERNAME** and **ADMIN PASSWORD** fields, and click **Disconnect**.

The system starts unregistering the vCenter Server from the cluster.

After unregistration is complete, the **Status** column for the vCenter Server on the **vCenter Integration** page displays **Not Configured**. Also, a relevant message is displayed in the Tasks dashboard.

## Migrating a Nutanix Cluster between Two vCenter Servers using Prism Element

Migrate a cluster from an existing external vCenter Server instance to a new vCenter Server instance using the Prism Element web console.

### About this task

The vCenter Server Registration page displays the registered vCenter Server. If for some reason (for example, after you change the password or the IP address of the vCenter Server or if current vCenter Server is not managing the hosts) the **Host Connection** field changes to **Not Connected**, it implies that the hosts are being managed by a different vCenter Server. In this case, there will be new vCenter entry with host connection status as Connected and you need to migrate to this vCenter Server.

### Procedure

1. Log into the Prism Element web console.
2. Click **Settings** from the dropdown menu.  
The system displays the **Global Settings** page.
3. From the **Setup** section in the left navigation menu, click **vCenter Integration**.  
The system displays the **vCenter Integration** page that lists the vCenter Server managing the hosts in the cluster and the vCenter Server from which you must unregister the cluster.
4. Unregister the existing vCenter Server instance by clicking **Disconnect**.  
For more information on how to unregister a cluster from a vCenter Server, see [Unregistering a Cluster from the vCenter Server using Prism Element](#) on page 363.
5. Register the cluster to a new vCenter Server instance by clicking **Connect**.  
For more information on how to register a cluster to a vCenter Server, see [Registering a Cluster to vCenter Server using Prism Element](#) on page 362.

## Updating the vCenter Service Account Credentials in Prism Element

Update the vCenter Server service account credentials used to register a cluster with vCenter Server in the Prism Element web console.

### Before you begin

Ensure that you register the cluster with vCenter Server using SSO-based authentication.

## About this task

Each time you update your user credentials in vCenter Server, you must also update them in the Prism Element web console. If you do not, Prism Element cannot perform VM operations, and the **Status** column for a vCenter Server in the **vCenter Integration** page displays **Inactive**.

To update the vCenter Server service account credentials, follow these steps:

## Procedure

1. Log into the Prism Element web console.
2. Click **Settings** from the dropdown menu.  
The system displays the **Global Settings** page.
3. From the **Setup** section in the left navigation menu, click **vCenter Integration**.  
The system displays the **vCenter Integration** page that lists the vCenter Server to which the cluster is registered.
4. Click the Update icon associated with the vCenter Server to which the cluster is registered.
5. In the **ADMIN USERNAME** and **ADMIN PASSWORD** fields, enter the new administrator user name and password of the vCenter Server.
6. Click **Update**.

## In-Place Hypervisor Conversion

The In-place hypervisor conversion feature provides you with an option to convert your existing ESXi cluster to an AHV cluster. All the VMs that are running in the ESXi cluster are converted so that they can run on the AHV cluster. The VM conversion is independent of the host that the VM is running on. The conversion process occurs in such a way that the VM down time is minimised. You can also convert the cluster back to ESXi. This conversion from AHV to ESXi is a file system restore of the host. Hence the cluster will be similar to what it was before the conversion.

### Note:

- This feature converts your existing ESXi cluster to an AHV cluster. You cannot start the conversion process on the AHV cluster.
- Do not remove the hosts from the vCenter Server if you want to perform the reverse conversion process (AHV to ESXi).
- This feature is supported on the clusters with multiple hypervisors (combination of ESXi nodes with one AHV node or multiple AHV nodes).
- When you are converting the cluster from ESXi to AHV, remove the unused adapters displayed under **Teaming and Failover** in vCenter Server and keep only those adapters that are active and of the same speeds as the standby and active adapters.

Following are enhancements to In-Place Hypervisor Conversion feature.

- **Decreased VM downtime:** With the implementation of the new workflow of converting the nodes in the cluster in a rolling manner, the VM downtime is reduced to only shutdown time and conversion time required for that particular VM. Approximately, the VM downtime has been reduced from 3 to 4 hours to less than 5 minutes.
- **Prism state:** The Prism console is responsive during the conversion process. However, Prism goes into read-only state.

- **State of the VM:** The current state of the VM is preserved and the VM is brought back into the same state post conversion. For example, the VM is automatically powered on post conversion if that VM was powered on before you started the conversion.
- **Preservation of the MAC addresses of the VM NICs:** After cluster conversion to AHV or ESXi, the MAC addresses of the VM NICs are preserved. The preservation of the IP address depends on the operating system. Typically, some Linux operating systems preserve the IP address when the MAC address is preserved, but Windows operating systems do not.
- VMs that were created after conversion to AHV are retained post conversion back to ESXi.

## Requirements and Limitations for In-Place Hypervisor Conversion

Following are the prerequisites with the requirements and limitations for an in-place hypervisor conversion.

### Prerequisites

- Before performing In-place hypervisor conversion, ensure that you resolve all the NCC health check alerts (warnings, failures and errors) and upgrade the firmware to the latest version using LCM firmware upgrade.
- HA and DRS must be enabled.
- All the hosts must be managed by the same vCenter Server.
- The vCenter Server VM that is managing the cluster must not be running on the cluster which is being converted.
- For ESXi to AHV cluster conversion, ensure to download the AHV ISO that is compatible with the AOS version from [Nutanix Portal](#).
- Install NGT on all the VMs. For more information, see [Enabling NGT and Mounting the NGT Installer in a VM](#) on page 303. If NGT is not installed, the VM does not boot after conversion.

**Note:** You can convert an ESXi cluster, which hosts a Prism Central VM, to an AHV cluster without installing NGT in the Prism Central VM. After the conversion, the Prism Central VM starts successfully.

- All hardware platforms are supported.
- Ensure that you have all the ESXi ISOs (if you have more than one version of ESXi running in your cluster) at the foundation/isos/hypervisor/esx/ location. This ISO image or images are used to bring the cluster back to its pre-conversion state if you abort the cluster conversion operation from ESXi to AHV.
- 

### General Limitations

In-place hypervisor conversion has the following limitations:

- Clusters with container-level encryption are not supported for conversion.
- Metro availability protection domains cannot be enabled in your environment.
- You cannot have Nutanix Files deployed in your cluster.
- Affinity policies (if configured) are not honored after conversion to AHV.
- In-place hypervisor conversion is not supported for single-node clusters and two-node clusters.
- Nutanix Objects cluster does not support In-place hypervisor conversion. If you convert the hosting Prism Element cluster, the Objects cluster becomes unmanageable.
- In-place hypervisor conversion can lead to a loss or failure of Prism Central features such as Calm, Objects, Files, and so on.

- VMware snapshots (snapshots created through vCenter or ESXi) must not be created during in-place hypervisor conversion because it can lead to cluster conversion failure. Therefore, pause any backup schedules (created manually or by backup applications) before starting an in-place hypervisor conversion.

## ESXi Supported Versions

**Table 75: Supported ESXi Versions**

Version	Support
5.5	All the versions that are included in the ISO Whitelist (see <code>~/foundation/config/iso_whitelist.json</code> file) that is bundled with AOS are supported. If you have upgraded foundation by using standalone foundation, the ISO Whitelist is invalidated. In this case, you need to see the original Whitelist that was present before you performed the upgrade. To verify the json file that was bundled with AOS, see the <code>nutanix-packages.json</code> file.
6.0	
6.5	
6.7	
7.0	
8.0	

## ESXi Network Requirements and Limitations

**Table 76: ESXi Network Requirements and Limitations**

Component	Description
NIC	Minimum of two or more homogenous NICs of 1 GB, 10 GB, or 40 GB are supported.
vSwitch	<ul style="list-style-type: none"> <li>Each host must have only one external vSwitch. If you have more than one external vSwitch validation fails.</li> <li>Ensure you have one active and multiple passive failover configuration of NICs on vSwitch.</li> <li>Active/active load balancing policies are not supported and is converted to active/passive on AHV.</li> <li>For a standard switch configuration it is recommended that all the port groups are present on all the hosts because there might be a possibility that the conversion process might move the VMs to a different host.</li> </ul>
Distributed vSwitch	Each host must have only one external distributed vSwitch. If you have more than one external distributed vSwitch validation fails.
Internal vSwitch	Internal vSwitch apart from Nutanix vSwitch is not supported.
LACP	Not supported.

- The vSwitch is converted to an open vSwitch on the AHV side. If you perform any configuration changes on AHV, these changes may not be maintained after converting the cluster back to ESXi.

- Networks not in use by a VM prior to the cluster conversion may not be converted.
- All the VMs may end up on a single host during conversion back to ESXi. The network configuration that you might have defined for the VMs may not be maintained.
- After migration to AHV, NIC may not have same type of virtualized hardware device (for example VMXNET3 may be E1000 after conversion).
- Serial ports and virtual graphics processing unit (vGPU) configurations may be lost after conversion.

## **Virtual Machine Requirements and Limitations**

- Only VMs with flat disks are supported. The delta disks are not supported.
- Only IDE and SCSI storage controllers are supported for automatic conversion. SATA and PCI disks are not supported.
- On Windows VMs, set the SAN policy to **OnlineAll** for non-boot SCSI disks so that they can be automatically brought online. For more information about setting SAN policy, see [Bringing Multiple SCSI Disks Online](#).
- VMs that have NFS datastore folders with vSphere tagging can not be converted.
- Virtual machines with attached volume groups or shared virtual disks are not supported.
- All VMs supported by AOS remain supported after converting the cluster to AHV.
- VMs with VirtIO drivers installed boot successfully after the conversion. If VirtIO is not installed, users can install NGT, which includes VirtIO as part of the installation.
- Prism Element does not support Virtual Trusted Platform Module (vTPM) VMs. Features that can be configured only at the Prism Central level for these VMs are not retained, and memory overcommit is not enabled for them.
- After reverting to ESXi from AHV, the VMs are converted to the maximum hardware version that is supported by that specific ESXi version.
- Guest OS network interfaces on Linux VMs may change to generic type during ESXi to AHV conversion (for example, in RHEL 7 network interface enoXXXX changes to eth0). You may have to reconfigure the network settings according to changes post conversion.
- Guest OS type for the Linux VMs may change to a more generic type (for example RHEL 7 may change to Other Linux 64-bit) during the conversion back from AHV to ESXi.

## **In-Place Hypervisor Conversion Process**

### **ESXi to AHV**

After you start the conversion process, all the nodes in the cluster are converted in a rolling manner to AHV one node at a time. During conversion, the first node is placed in the maintenance mode and all the VMs that are running on the node are migrated to other ESXi nodes in the cluster using the HA and DRS feature. After the VMs are migrated, the node is converted to AHV. After node is successfully converted, all VMs that were migrated to ESXi are migrated one at a time to AHV. Similar steps are performed for the rest of the nodes in the ESXi cluster until the last ESXi node. The VMs that are running on the last ESXi node in the cluster are converted and migrated to the AHV hosts and then the ESXi host is converted to AHV. If any error occurs during VM conversion, appropriate alerts or error messages are displayed. When converting a VM the source vdisk is not modified. Therefore, if there are any fatal errors during imaging, storing, or restoring of the configuration, the conversion is stopped and you are prompted to abort the conversion.

**Note:** After conversion, do not remove the host from the vCenter Server until you are sure that the conversion is successful, because it may impact the reverse conversion process.

## Port Groups and VLAN Transformation

Before the conversion all of the ESXi port groups, VLAN IDs, and virtual machines that belong to a particular group are captured. On AHV, a corresponding Acropolis virtual network is created for every unique ESXi port group on the cluster including any corresponding VLAN ID, and then associated with the VMs. If the ESXi host has a VLAN set on the management port group, after conversion the Acropolis management interface and the Controller VM public interface are placed in that same VLAN.

### AHV to ESXi

During the reverse conversion (AHV to ESXi), the process of conversion is similar. Additionally, if the cluster does not have the ESXi ISO stored on the cluster, you need to provide the ESXi ISO image during the conversion process.

#### Note:

- The image that you provide should be of the same major ESXi version that you have used during ESXi to AHV conversion.
- If new nodes were added to the cluster after conversion to AHV, then these nodes need to be removed before starting the reverse conversion process.

After conversion to ESXi, all the hosts are automatically registered to the vCenter Server.

## Converting Cluster (ESXi to AHV)

Perform the following procedure to convert the cluster from ESXi to AHV.

### Before you begin

Verify that you have met all the networking and virtual machine requirements as described in [Requirements and Limitations for In-Place Hypervisor Conversion](#) on page 366.

### About this task

#### Procedure

1. Log into the Prism Element web console.
  2. Click the gear icon in the main menu and then select **Convert Cluster** in the **Settings** page.
  3. From the **Available Hypervisor** drop-down menu, select **AHV**.
  4. Select the state of the VMs that you want post conversion from the **VM Boot Options** drop-down menu.
    - » **Preserve power state of the user VMs:** Select this option if you want to keep the original power state of the VMs. For example, if you want the VMs to be in a running state post conversion automatically, select this option.
    - » **Power Off User VMs:** Select this option if you want power off all the VMs running on ESXi cluster before you start the conversion process. After conversion, these VMs will be in the powered off state.
  5. Click **Validate** to enter vCenter Server credentials and to verify whether you have met all the requirements.
  6. Enter the IP address of the vCenter Server in the **vCenter Sever IP Address** along with the administrator user name and password of the vCenter Server in the **Username** and **Password** fields.
  7. Click **Yes**.
- A validation that you have met all the requirements is performed. Once the validation is successful the conversion process proceeds. If validation fails (for any reason), a relevant message to take appropriate action is displayed.

8. In the **Software Upload** dialog box, upload the AHV ISO that you had downloaded earlier.

9. Click **Convert Cluster**.

A confirmation message is displayed.

**Note:** The cluster changes to Read Only mode. A message Oops - server Error may be displayed when the Prism node is undergoing conversion. Wait for the conversion process to complete. You can access other Controller VM for Read-Only Prism operations.

The entire conversion process may take 3 to 4 hours depending on the nodes that are present in your cluster. However, the VM downtime will be less than 5 minutes because all the nodes in the cluster are converted in a rolling manner. You can also track the progress of the conversion by logging again into the web console.

## Converting Cluster (AHV to ESXi)

Perform the following procedure to convert the cluster back to ESXi from AHV.

### About this task

Perform this procedure only if you have converted your cluster from ESXi to AHV. You cannot start the conversion process on the AHV cluster.

### Before you begin

Ensure that you have met all the networking and virtual machine requirements as described in [Requirements and Limitations for In-Place Hypervisor Conversion](#) on page 366 topic.

### Procedure

1. Log into the Prism Element web console.

2. Click the gear icon in the main menu and then select **Convert Cluster** in the **Settings** page.

3. From the **Available Hypervisor** drop-down menu, select **ESXi**.

4. Select the state of the VMs that you want post conversion from the **VM Boot Options** drop-down menu.

» **Preserve power state of the user VMs:** Select this option if you want to keep the original power state of the VMs. For example, if you want the VMs to be in a running state post conversion automatically, select this option.

» **Power Off User VMs:** Select this option if you want power off all the VMs running on ESXi cluster before you start the conversion process. After conversion, these VMs will be in the powered off state.

5. Click **Validate** to enter vCenter Server credentials and to verify whether you have met all the requirements.

6. Enter the IP address of the vCenter Server in the **vCenter Sever IP Address** along with the administrator user name and password of the vCenter Server in the **Username** and **Password** fields.

7. Click **Yes**.

A validation that you have met all the requirements is performed. Once the validation is successful the conversion process proceeds. If validation fails (for any reason), a relevant message to take appropriate action is displayed.

8. Click **Convert Cluster** button to start the conversion process.

9. (Optional) If you have not saved the ESXi ISOs at the foundation/isos/hypervisor/esx/ location, click **Choose File** and select the ESXi ISO.

**Note:** If you have different versions of ESXi running in your cluster, you have to perform this step for every version of ESXi ISO.

10. Click **Convert**.

All cluster operations stops and you will not be able to perform any operations on the cluster while the conversion is in progress. A message to this effect is displayed.

11. Click **Yes** to proceed with the conversion.

The conversion begins. The time taken to finish the conversion is dependent on your environment. For example, it might take between 2 to 3 hours for the conversion to finish for a 3 or 4 nodes cluster. However, the VM downtime will be less than 5 minutes.

## Stopping Cluster Conversion

If any issues occur with the cluster conversion process, a message to stop the cluster conversion or to continue with the conversion process is displayed. Depending on the type of message, you can appropriate action.

### Before you begin

Ensure that you have saved the ESXi ISO at the foundation/isos/hypervisor/esx/ location. This ISO image is used to bring the cluster back to its pre-conversion state if you stop the cluster conversion operation from ESXi to AHV.

### About this task

Issues in the cluster conversion process might occur because of the following reasons.

- Imaging Issue: If this issue occurs, you can only stop the cluster conversion process and a relevant message is displayed. Aborting the conversion reverts the cluster back to its original state.
- VM Conversion Issue: If this issue occurs, you can either stop the conversion or can continue with the process. If you decide to continue with the process, cluster conversion is completed keeping the current state of the VM. After conversion is completed, you must perform appropriate actions on the VMs to bring back the VMs.

### Procedure

Click **Abort** when a message to stop the cluster conversion is displayed.

The cluster goes back to its original state. You may need to manually power on the VMs depending on its state after you perform this operation.

## Internationalization (i18n)

The following table lists all the supported and unsupported entities in UTF-8 encoding.

**Table 77: Internationalization Support**

Supported Entities	Unsupported Entities
Cluster name	Acropolis file server
Storage Container name	Share path
Storage pool	Internationalized domain names

Supported Entities	Unsupported Entities
VM name	E-mail IDs
Snapshot name	Hostnames
Volume group name	Integers
Protection domain name	Password fields
Remote site name	Any Hardware related names ( for example, vSwitch, iSCSI initiator, vLAN name)
User management	
Chart name	

**Caution:** The creation of none of the above entities are supported on Hyper-V because of the DR limitations.

### Entities Support (ASCII or non-ASCII) for the Active Directory Server

- In the New Directory Configuration, **Name** field is supported in non-ASCII.
- In the New Directory Configuration, **Domain** field is not supported in non-ASCII.
- In Role mapping, **Values** field is supported in non-ASCII.
- User names and group names are supported in non-ASCII.

## Localization (L10n)

Nutanix localizes the user interface in Simplified Chinese and Japanese language. All the static screens are translated to the selected locale language. All the dashboards (including tool tips) and menus of the Prism Element are localized.

You have an option to change the language settings of the cluster from English (default) to Simplified Chinese or Japanese. For more information, see [Changing the Language Settings](#) on page 372.

If the Prism Central instance is launched from the Prism Element, language settings of the Prism Central takes precedence over Prism Element.

You can also create new users with the specified language setting. For more information, see [User Management](#).

### Conditions and Limitations

- Logical entities that do not have a contextual translation available in the localized language are not localized.
- The AOS generated alerts and events are not localized to the selected locale language.
- Following strings are not localized: VM, CPU, vCPU, Language Settings, licensing details page, hardware names, storage denominations (GB, TB), About Nutanix page, EULA, service names (SNMP, SMTP), hypervisor types.

## Changing the Language Settings

Perform the following procedure to set the Prism language settings to a chosen language (English, simplified Chinese, or Japanese). You also have an option to set the calendar, date, and time format to a selected region.

### Procedure

1. Log in to the Prism Element web console.

2. Click the gear icon in the main menu and then select **Language Settings** in the **Settings** page. The **Language Settings** dialog box appears.
3. To change the language, select the desired language from the **Languages** field pull-down menu. The **English** language is selected by default, but you can change that to either **Simplified Chinese** or **Japanese**.
4. To change the locale settings (date, time, calendar), select the appropriate region from the **Region** field drop-down menu.

A default locale is set based on the language setting. However, you can change the region to display the date, time, and calendar in some other format. This format for date, time, and calendar is applied to the entire cluster.
5. When the settings are correct, click the **Save** button.

The language and locale settings are changed according to the selection. For example, the language setting for a cluster can be changed to Chinese and the locale setting to Russian.

For more information on the entities that are supported, see [Internationalization \(i18n\)](#) on page 371. For more information about localization, see [Localization \(L10n\)](#) on page 372.

## Hyper-V Setup

### Adding the Cluster and Hosts to a Domain

After completing foundation of the cluster, you need to add the cluster and its constituent hosts to the Active Directory (AD) domain. The adding of cluster and hosts to the domain facilitates centralized administration and security through the use of other Microsoft services such as Group Policy and enables administrators to manage the distribution of updates and hotfixes.

#### Before you begin

- If you have a VLAN segmented network, verify that you have assigned the VLAN tags to the Hyper-V hosts and Controller VMs. For information about how to configure VLANs for the Controller VM, see the [Acropolis Advanced Administration Guide](#).
- Ensure that you have valid credentials of the domain account that has the privileges to create a new computer account or modify an existing computer account in the Active Directory domain. An Active Directory domain created by using non-ASCII text may not be supported. For more information about usage of ASCII or non-ASCII text in Active Directory configuration, see [Internationalization \(i18n\)](#) in *Prism Element Web Console Guide*.

#### Procedure

1. Log on to the Web Console by using one of the Controller VM IP address or by using cluster virtual IP address.
2. Click the gear icon in the main menu and select **Join Cluster and Hosts to the Domain** on the **Settings** page.
3. Enter the fully qualified name of the domain that you want to join the cluster and its constituent hosts to in the **Full Domain Name** field.
4. Enter the IP address of the name server in the **Name Server IP Address** field that can resolve the domain name that you have entered in the **Full Domain Name** field.

- In the **Base OU Path** field, type the OU (organizational unit) path where the computer accounts must be stored after the host joins a domain. For example, if the organization is nutanix.com and the OU is Documentation, the Base OU Path can be specified as *OU=Documentation,DC=nutanix,DC=com*

Specifying the Base OU Path is optional. When you specify the Base OU Path, the computer accounts are stored in the Base OU Path within the Active Directory after the hosts join a domain. If the Base OU Path is not specified, the computer accounts are stored in the default Computers OU.

- Enter a name for the cluster in the **Nutanix Cluster Name** field.

The maximum length of the cluster name should not be more than 15 characters and it should be a valid NetBIOS name.

- Enter the virtual IP address of the cluster in the **Nutanix Cluster Virtual IP Address** field.

If you have not already configured the virtual IP address of the cluster, you can configure it by using this field.

- Enter the prefix that should be used to name the hosts (according to your convention) in the **Prefix** field.

- The prefix name should not end with a period.
- The maximum length of the prefix name should not be more than 11 characters.
- Should be a valid NetBIOS name.

For example, if you enter prefix name as Tulip, the hosts are named as Tulip-1, Tulip-2, and so on, in the increasing order of the external IP address of the hosts.

If you do not provide any prefix, the default name of *NTNX-block-number* is used. Click **Advanced View** to see the expanded view of all the hosts in all the blocks of the cluster and to rename them individually.

- In the **Credentials** field, enter the logon name and password of the domain account that has the privileges to create a new or modify an existing computer accounts in the Active Directory domain.

Ensure that the logon name is in the *DOMAIN\USERNAME* format. The cluster and its constituent hosts require these credentials to join the AD domain. Nutanix does not store the credentials.

- When all the information is correct, click **Join**.

The cluster is added to the domain. Also, all the hosts are renamed, added to the domain, and restarted. Allow the hosts and Controller VMs a few minutes to start. After the cluster is ready, the logon page is displayed.

## What to do next

Create a Microsoft failover cluster. For more information, see [Creating a Failover Cluster for Hyper-V](#) on page 374.

## Creating a Failover Cluster for Hyper-V

### Before you begin

Perform the following tasks before you create a failover cluster:

- Join the hosts to the domain as described in [Adding the Cluster and Hosts to a Domain](#).
- Ensure that the Windows failover cluster IP address and hypervisor or host IP address are in the same subnet.

Perform the following procedure to create a failover cluster that includes all the hosts in the cluster.

### Procedure

- Log on to the Prism Element web console by using one of the Controller VM IP addresses or by using the cluster virtual IP address.

2. Click the gear icon in the main menu and select **Configure Failover Cluster** from the **Settings** page.
3. Type the failover cluster name in the **Failover Cluster Name** field.  
The maximum length of the failover cluster name must not be more than 15 characters and must be a valid NetBIOS name.
4. Type an IP address for the Hyper-V failover cluster in the **Failover Cluster IP Address** field.  
This address is for the cluster of Hyper-V hosts that are currently being configured. It must be unique, different from the cluster virtual IP address and from all other IP addresses assigned to the hosts and Controller VMs. It must be in the same network range as the Hyper-V hosts.
5. In the **Credentials** field, type the logon name and password of the domain account that has the privileges to create a new account or modify existing accounts in the Active Directory domain.  
The logon name must be in the format *DOMAIN\USERNAME*. The credentials are required to create a failover cluster. Nutanix does not store the credentials.
6. Click **Create Cluster**.  
A failover cluster is created by the name that has been provided and it includes all the hosts in the cluster.  
For information on manually creating a failover cluster, see [Manually Creating a Failover Cluster \(SCVMM User Interface\)](#) on page 375.

## Manually Creating a Failover Cluster (SCVMM User Interface)

### About this task

Perform the following procedure to manually create a failover cluster for Hyper-V by using System Center VM Manager (SCVMM).

If you are not using SCVMM or are using Hyper-V Manager, see [Creating a Failover Cluster for Hyper-V](#) on page 374.

### Before you begin

Join the hosts to the domain as described in [Adding the Cluster and Hosts to a Domain](#) in the *Hyper-V Administration for Acropolis* guide.

### Procedure

1. Start the Failover Cluster Manager utility.
2. Right-click and select **Create Cluster**, and click **Next**.
3. Enter all the hosts that you want to add to the Failover cluster, and click **Next**.
4. Select the **No. I do not require support from Microsoft for this cluster, and therefore do not want to run the validation tests. When I click Next continue creating the cluster** option, and click **Next**.

#### Note:

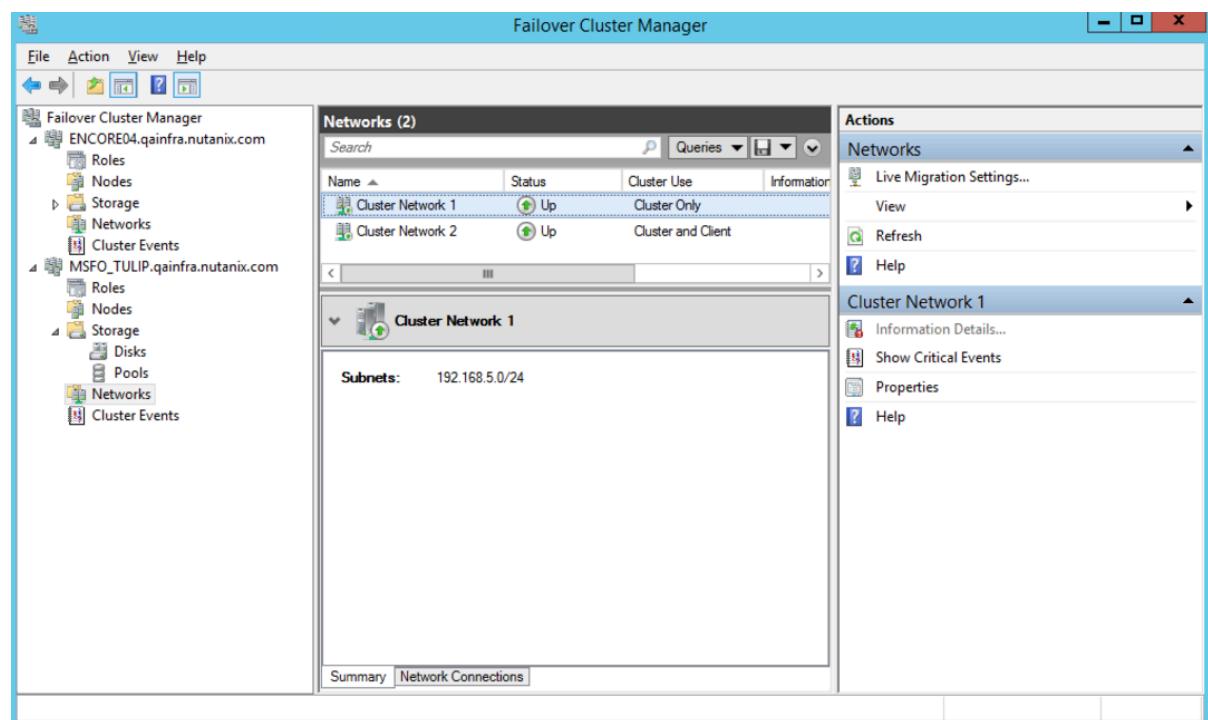
If you select **Yes**, two tests fail when you run the cluster validation tests. The tests fail because the internal network adapter on each host is configured with the same IP address (192.168.5.1). The network validation tests fail with the following error message:

Duplicate IP address

The failures occur despite the internal network being reachable only within a host, so the internal adapter can have the same IP address on different hosts. The second test, Validate Network

Communication, fails due to the presence of the internal network adapter. Both failures are benign and can be ignored.

5. Enter a name for the cluster, specify a static IP address, and click **Next**.
6. Clear the **All eligible storage to the cluster** check box, and click **Next**.
7. Wait until the cluster is created. After you receive the message that the cluster is successfully created, click **Finish** to exit the **Cluster Creation** wizard.
8. Go to **Networks** in the cluster tree and select **Cluster Network 1** and ensure it is in the internal network by verifying the IP address in the summary pane. The IP address must be 192.168.5.0/24 as shown in the following screen shot.



**Figure 55: Failover Cluster Manager**

9. Click the **Action** tab on the toolbar and select **Live Migration Settings**.
10. Remove **Cluster Network 1** from **Networks** for Live Migration and click **OK**.

**Note:** If you do not perform this step, live migrations fail because the internal network is added to the live migration network lists. Log on to SCVMM, add the cluster to SCVMM, check the host migration setting, and ensure that the internal network is not listed.

## Enabling Kerberos for Hyper-V

If you are running Windows Server 2012 R2, perform the following procedure to configure Kerberos to secure the storage. You do not have to perform this procedure for Windows Server 2016 because Kerberos is enabled automatically during failover cluster creation.

### Before you begin

- Join the hosts to the domain as described in [Adding the Cluster and Hosts to a Domain](#) on page 373.

- Verify that you have configured a service account for delegation. For more information on enabling delegation, see the *Microsoft documentation*.

## Procedure

- Log on to the web console by using one of the Controller VM IP addresses or by using the cluster virtual IP address.
- Click the gear icon in the main menu and select **Kerberos Management** from the **Settings** page.
- Set the **Kerberos Required** option to enabled.
- In the **Credentials** field, type the logon name and password of the domain account that has the privileges to create and modify the virtual computer object representing the cluster in Active Directory. The credentials are required for enabling Kerberos.

The logon name must be in the format *DOMAIN\USERNAME*. Nutanix does not store the credentials.

- Click **Save**.

## Configuring the Hyper-V Computer Object by Using Kerberos

### About this task

Perform the following procedure to complete the configuration of the Hyper-V Computer Object by using Kerberos and SMB signing (for enhanced security).

**Note:** Nutanix recommends you to configure Kerberos during a maintenance window to ensure cluster stability and prevent loss of storage access for user VMs.

## Procedure

1. Log on to Domain Controller and perform the following for each Hyper-V host computer object.
  - a. Right-click the host object, and go to **Properties**. In the **Delegation** tab, select the **Trust this computer for delegation to specified services only** option, and select **Use any authentication protocol**.
  - b. Click **Add** to add the **cifs** of the Nutanix storage cluster object.

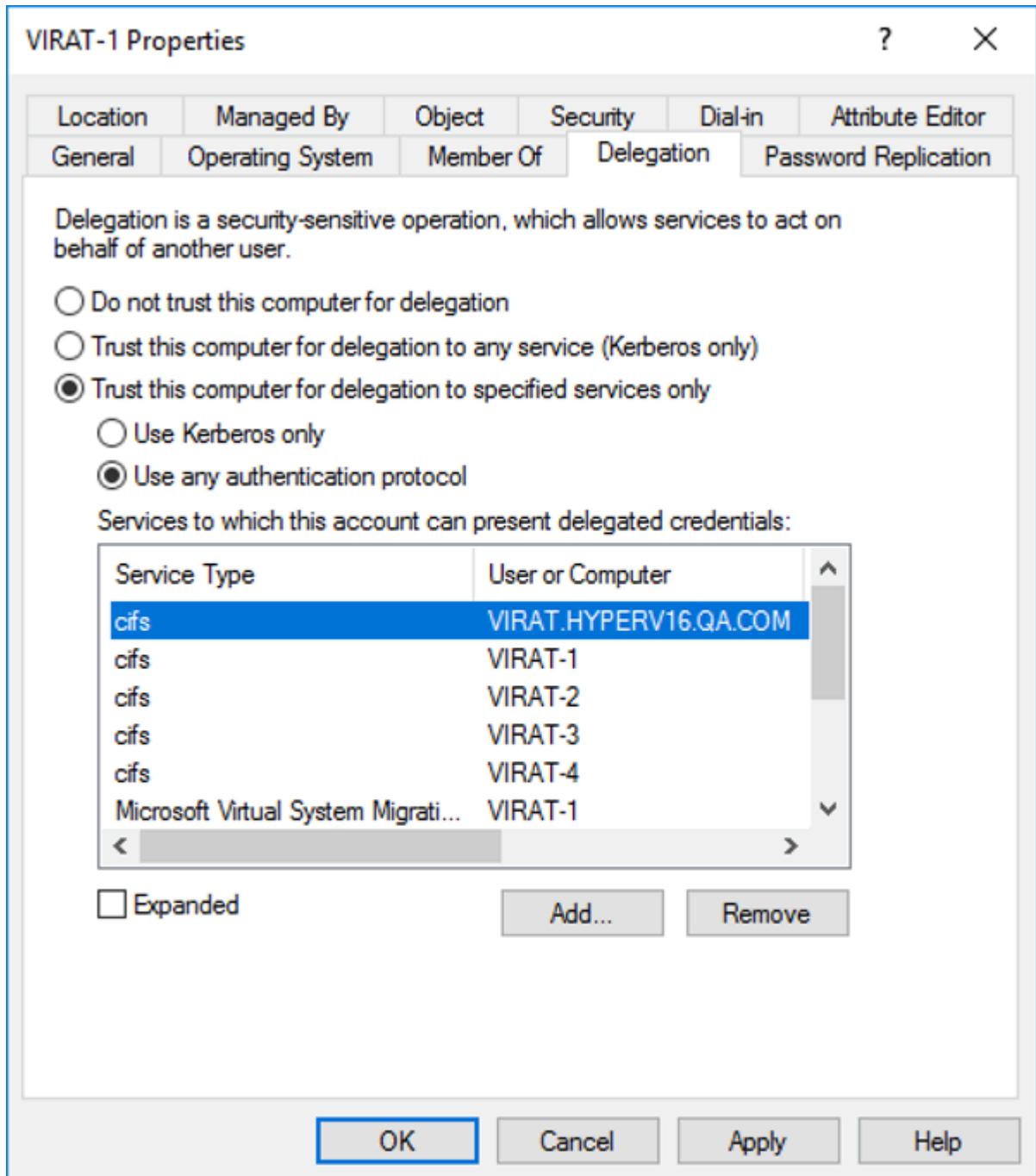


Figure 56: Adding the cifs of the Nutanix storage cluster object

- Check the Service Principal Name (SPN) of the Nutanix storage cluster object.

```
> Setspn -l name_of_cluster_object
```

Replace *name\_of\_cluster\_object* with the name of the Nutanix storage cluster object.

Output similar to the following is displayed.

```
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> setspn -l virat
Registered ServicePrincipalNames for CN=VIRAT,CN=Computers,DC=hyperv16, DC=qa,DC=com:
    cifs/VIRAT.HYPERV16.QA.COM
    cifs/VIRAT
PS C:\Users\Administrator>
```

If the SPN is not registered for the Nutanix storage cluster object, create the SPN by running the following commands.

```
> Setspn -S cifs/name_of_cluster_object name_of_cluster_object
> Setspn -S cifs/FQDN_of_the_cluster_object name_of_cluster_object
```

Replace *name\_of\_cluster\_object* with the name of the Nutanix storage cluster object and *FQDN\_of\_the\_cluster\_object* with the domain name of the Nutanix storage cluster object.

### Example

```
> Setspn -S cifs/virat virat
> Setspn -S cifs/virat.sre.local virat
```

- [Optional] To enable SMB signing feature, log on to each Hyper-V host by using RDP and run the following PowerShell command to change the **Require Security Signature** setting to **True**.

```
> Set-SMBClientConfiguration -RequireSecuritySignature $True -Force
```

**Caution:** The SMB server will only communicate with an SMB client that can perform SMB packet signing, therefore if you decide to enable the SMB signing feature, it must be enabled for all the Hyper-V hosts in the cluster.

# SECURITY AND USER MANAGEMENT

---

Prism provides several mechanisms to maintain security in a cluster and control user access.

- Set the user authentication method. For more information, see [Configuring Authentication](#) in the *Nutanix Security Guide*.
- Add, edit, or delete local user accounts. For more information, see [User Management](#) in the *Nutanix Security Guide*.
- Install or replace an SSL certificate. For more information, see [Certificate Management](#) in the *Nutanix Security Guide*.
- Control SSH access to the cluster. For more information, see [Controlling Cluster Access](#) in the *Nutanix Security Guide*.
- Enable data-at-rest encryption. For more information, see [Data-at-Rest Encryption](#) in the *Nutanix Security Guide*.
- Enable network segmentation. For more information, see [Securing Traffic Through Network Segmentation](#) in the *Nutanix Security Guide*.
- Review authentication best practices. For more information, see [Authentication Best Practices](#) in the *Nutanix Security Guide* and for firewall requirements see [Firewall Requirements](#) in the *Nutanix Security Guide*.

# SUPPORT SERVICES

---

Nutanix provides support services in several ways.

- Nutanix technical support can monitor your clusters and provide assistance when problems occur. For more information, see [Controlling Remote Connections](#) on page 390, [Configuring HTTP Proxy](#) on page 391, and [Pulse Health Monitoring](#) on page 381.
- Nutanix technical support maintains a portal that you can access to request assistance, download AOS updates, or view documentation. For more information, see [Accessing the Nutanix Support Portal](#) on page 392.
- Nutanix supports a REST API that allows you to request information or run administration scripts for a Nutanix cluster. For more information, see [Accessing the REST API Explorer](#) on page 394.

## Pulse Health Monitoring

The Pulse feature provides diagnostic system data about a Prism Element cluster to Nutanix Support to help deliver proactive, context-aware support for Nutanix solutions. Pulse collects this information without affecting system performance and shares only basic system-level information necessary for monitoring the health and status of a Prism Element cluster.

This information includes the following items.

- System alerts
- Current Nutanix software version
- Nutanix processes and Controller VM information
- Hypervisor details such as type and version

Pulse frequently collects important data, like system-level statistics and configuration information, to automatically detect issues and help simplify troubleshooting. With this information, Nutanix Support can apply advanced analytics to optimize your implementation and address potential problems.

Pulse sends messages through HTTPS (port 443) using TLS 1.2. The HTTPS request uses certificate authentication to validate that Pulse has established communication with the Nutanix Remote Diagnostics service. The TLS 1.2 protocol uses public key cryptography and server authentication to provide confidentiality, message integrity, and authentication for traffic passed over the Internet. For the complete list of required ports, see [Ports and Protocols](#).

### Pulse Transport Methods

Nutanix recommends that you configure one of the following Pulse transport methods (in the order of preference):

1. Enable Pulse and use Prism Central as a proxy for the Pulse data transmitted by each node (for clusters registered with Prism Central).

Advantages: The configuration is automatic (as described in [Prism Central Proxy for Pulse Data](#) of the *Prism Central Admin Center Guide*), and no new firewall configurations are required when you add a node to the cluster or remove a node from the cluster.

2. Enable Pulse and configure an HTTP proxy server. For information on how to configure an HTTP proxy server see [Configuring HTTP Proxy](#) on page 391.

Advantage: No new firewall configurations are required when you add a node to the cluster or remove a node from the cluster.

3. Enable Pulse and configure your firewall. Enable Pulse by using each Controller VM IP address in each managed cluster. For more information, see [Pulse Configuration](#) on page 383 and [Pulse Access Requirements](#).

Disadvantage: New firewall configurations are required when you add a node to the cluster or remove a node from the cluster.

## Pulse Access Requirements

To successfully send Pulse-collected data from a Prism Element cluster to the Nutanix Insights endpoints, Pulse requires the following access:

- Ensure your firewall allows the IP addresses of all Controller VMs because Pulse data is sent from each controller VM of the cluster to insights.nutanix.com over port 443 using the HTTPS REST endpoint.
- Ensure your firewall allows traffic from each Controller VM to the Nutanix Insights endpoints. For more information, see [Ports and Protocols](#).

**Note:** Firewall port requirements for the Controller VMs might not be necessary if you have a Prism Central deployment. For more information, see [Prism Central Proxy for Pulse Data](#) in the *Prism Central Admin Center Guide*.

## Remote Diagnostics

Remote Diagnostics enables Nutanix Support to request granular diagnostic information from Pulse-enabled clusters. Pulse streams a collection of configuration data, metrics, alerts, events, and select logs to Nutanix Insights, providing a high-level representation of the cluster state. If the Pulse data stream is not detailed enough to diagnose a specific issue, Nutanix Support might need to collect more diagnostic data from the cluster. Remote Diagnostics allows Nutanix to remotely collect the following data only.

- Logs
  - Nutanix services logs
  - Custom gflags set for any Nutanix service
  - Activity traces for Nutanix services
  - Hypervisor logs
  - Hypervisor configuration
  - Cluster configuration
  - System statistics like memory usage
- Nutanix NCC health check reports
- Nutanix log summary report (Panacea)
- A curated set of read-only commands

Each time Remote Diagnostics triggers a collection, it adds an entry to the audit trail of the cluster. There are always two entries, the start (initiation) and finish (termination) of the diagnostics collection.

By default, every Pulse-enabled cluster has Remote Diagnostics enabled. If your security policy or other consideration does not allow cluster access to Nutanix Support for remote diagnostics collection, you can disable Remote Diagnostics without disabling Pulse. Nutanix Support continues to provide seamless and proactive support based on the Pulse data.

- To check the Remote Diagnostics status, log on to a Controller VM through SSH and run the following command.

```
nutanix@cvm$ zkcat /appliance/logical/nusights/collectors/kCommand/override_config
```

**Note:** This command prints the Remote Diagnostics status only if the Remote Diagnostics status is set explicitly. The command does not print anything if the status is the default status.

- To disable Remote Diagnostics, log on to a Controller VM through SSH and run the following command.

```
nutanix@cvm$ /home/nutanix/ncc/bin/nusights/set_remote_diagnostics_status --enable=false --reason="text"
```

Replace *text* with a string describing the reason for disabling Remote Diagnostics. The --reason parameter is optional.

- To enable Remote Diagnostics, log on to a Controller VM through SSH and run the following command.

```
nutanix@cvm$ /home/nutanix/ncc/bin/nusights/set_remote_diagnostics_status --enable=true --reason="text"
```

Replace *text* with a string describing the reason for enabling Remote Diagnostics. The --reason parameter is optional.

## Pulse Configuration

When you log in to the Prism Element web console for the first time after an installation or an upgrade, the system checks whether Pulse is enabled. If it is not enabled, a pop-up window appears recommending that you enable Pulse.

- To enable Pulse, click **Continue** and follow the prompts.
- To continue without enabling Pulse, select the **Disable Pulse (not recommended)** checkbox and click **Continue**.

For Pulse configuration recommendations, see [Pulse Transport Methods](#).

### Enabling Pulse

#### About this task

Perform the following steps to enable Pulse in a cluster.

##### Note:

- For information on how to enable Pulse simultaneously in all the clusters registered to a Prism Central, see [Enabling Pulse](#) in the *Prism Central Admin Center Guide*.
- Nutanix recommends that you enable Pulse to allow Nutanix Support to receive cluster data and deliver proactive and context-aware support.
- Nutanix does not collect any personally identifiable information (PII) through Pulse.

### Procedure

- Log in to the Prism Element web console.
- Go to **Settings > Setup > Pulse**.  
The **Enable Insights powered by Pulse** window appears.
- Click **Enable Pulse**.

Pulse is enabled in the cluster and the following message is displayed.

```
Pulse has been enabled for this cluster.
```

### Disabling Pulse

#### About this task

Perform the following steps to disable Pulse from a cluster.

**Caution:** Nutanix recommends that you enable Pulse to allow Nutanix Support to receive cluster data and deliver proactive and context-aware support. If Pulse is disabled, the clusters do not send alerts to Nutanix Support when problems occur.

## Procedure

1. Log in to the Prism Element web console.
2. Go to **Settings > Setup > Pulse**.  
The **Enable Insights powered by Pulse** window appears.
3. Click **Disable Pulse**.

Pulse is disabled from the cluster and the following message is displayed.

Pulse has been disabled for this cluster.

## Mask Entity Names and IP Addresses

When you enable Pulse, Pulse periodically sends data to the Nutanix Insights tool and the Nutanix Support team for troubleshooting. Pulse is the underlying technology that securely transmits system-level diagnostic data to the Insights platform, enabling predictive health and context-aware support automation workflows. Nutanix Insights is an integrated service that utilizes this data to augment product support, reducing customer case volume and expediting issue resolution time.

Nutanix does not share any data that Pulse sends with any third parties unless permitted by your agreement with Nutanix or the Nutanix Privacy Statement. Certain Nutanix products require Pulse enablement for functionality and features. For more information, see [Nutanix Privacy Statement](#) and the applicable product documentation.

You can mask the entity names and IP addresses not masked by default. The entity names and IP addresses link to Nutanix entities, such as cluster names, and not to individuals.

To check masking settings on a specific Prism Element cluster, run these commands.

- Check if partial scrubbing is enabled.

```
nutanix@cvm$ curl -H "Content-Type: application/json" -X GET -H "X-Nutanix-Prauth-User:admin" http://localhost:9080/PrismGateway/services/rest/v1/pulse
```

If the output contains the string "identificationInfoScrubbingLevel":"PARTIAL" or "identificationInfoScrubbingLevel":"AUTO", partial scrubbing is enabled. By default, the scrubbing level is set to AUTO. If the output contains the string "identificationInfoScrubbingLevel":"ALL", identificationInfoScrubbingLevel is still set to ALL, and the **Open In Prism** button on the Insights Portal remains deactivated.

- Mask entity names and IP addresses, and update the PII scrub level.

```
nutanix@cvm$ curl -H "Content-Type: application/json" -X PUT -H "X-Nutanix-Prauth-User:admin" --data '{"identificationInfoScrubbingLevel": "ALL"}' http://localhost:9080/PrismGateway/services/rest/v1/pulse
```

## Pulse Health Monitoring Data Collection

The following categories serve as a general overview of the types of information that Pulse gathers from the clusters. Note that some of this information may be anonymized depending on your settings. This list is not exhaustive; for more details about the Pulse information your clusters send to Nutanix, contact Nutanix Support.

**Table 78: Pulse Data Collection**

Entity	Data Collected
Cluster	<ul style="list-style-type: none"><li>• Cluster name (may be anonymized)</li><li>• Uptime</li><li>• AOS version</li><li>• Cluster ID</li><li>• Block serial number</li><li>• HW model</li><li>• Cluster IOPS</li><li>• Cluster latency</li><li>• Cluster memory</li></ul>

Entity	Data Collected
Hardware	<p><b>Note:</b> In this context, hardware can include nodes, blocks, boards, disks, BMCs, fans, DIMMs, BIOS, CPUs, NICs, storage controllers, and power supplies.</p> <ul style="list-style-type: none"> <li>• Model number</li> <li>• Serial number</li> <li>• Part number</li> <li>• Block number</li> <li>• Node UUID</li> <li>• Type</li> <li>• Size</li> <li>• Version</li> <li>• Name (may be anonymized)</li> <li>• Manufacturer</li> <li>• Status</li> <li>• Memory (size)</li> <li>• Hypervisor type</li> <li>• Hypervisor version</li> <li>• Firmware version</li> <li>• Disk type</li> <li>• Disk model</li> <li>• Disk capacity</li> <li>• Node temperature</li> <li>• Network interface model</li> <li>• SATADOM firmware</li> <li>• PSU status</li> <li>• Node location</li> <li>• IPMI version</li> <li>• Fan RPM</li> <li>• Component location</li> <li>• DIMM bank connection</li> <li>• Clock speed</li> <li>• DIMM temperature</li> <li>• BIOS release date</li> <li>• BIOS ROM size</li> <li>• CPU signature</li> <li>• CPU core count</li> <li>• CPU cores enabled</li> <li>• CPU thread count</li> <li>• CPU temperature</li> </ul>

<b>Entity</b>	<b>Data Collected</b>
Storage Pool	<ul style="list-style-type: none"> <li>• Name (may be anonymized)</li> <li>• Capacity (logical used capacity and total capacity)</li> <li>• IOPS and latency</li> </ul>
Container	<ul style="list-style-type: none"> <li>• Container name (may be anonymized)</li> <li>• Capacity (logical used and total)</li> <li>• IOPS and latency</li> <li>• Replication factor</li> <li>• Compression ratio</li> <li>• Deduplication ratio</li> <li>• Inline or post-process compression</li> <li>• Inline deduplication</li> <li>• Post-process deduplication</li> <li>• Space available</li> <li>• Space used</li> <li>• Erasure coding and savings</li> </ul>
Controller VM (CVM)	<ul style="list-style-type: none"> <li>• Details of logs, attributes, and configurations of services on each CVM</li> <li>• CVM memory</li> <li>• vCPU usage</li> <li>• Uptime</li> <li>• Network statistics</li> <li>• IP addresses (may be anonymized)</li> </ul>

Entity	Data Collected
VM	<ul style="list-style-type: none"> <li>• Name (may be anonymized)</li> <li>• VM state</li> <li>• vCPU</li> <li>• Memory</li> <li>• Disk space available</li> <li>• Disk space used</li> <li>• Number of vDisks</li> <li>• Name of the container that contains the VM (may be anonymized)</li> <li>• VM operating system</li> <li>• IOPS</li> <li>• Latency</li> <li>• VM protection status</li> <li>• Management VM (yes or no)</li> <li>• I/O pattern (read, read/write, random, sequential)</li> <li>• IP address (may be anonymized)</li> </ul>
Disk Status	<ul style="list-style-type: none"> <li>• Performance stats</li> <li>• Usage</li> </ul>
Hypervisor	<ul style="list-style-type: none"> <li>• Hypervisor software and version</li> <li>• Uptime</li> <li>• Installed VMs</li> <li>• Memory usage</li> <li>• Attached datastore</li> </ul>
Datastore	<ul style="list-style-type: none"> <li>• Usage</li> <li>• Capacity</li> <li>• Name</li> </ul>
Protection Domains	<ul style="list-style-type: none"> <li>• Name (may be anonymized)</li> <li>• Count and names of VMs in each protection domain</li> </ul>

<b>Entity</b>	<b>Data Collected</b>
Gflags	<ul style="list-style-type: none"> <li>• Key and value</li> <li>• State (set)</li> <li>• Node ID</li> <li>• Service name</li> <li>• Time of modification</li> </ul>
Feature	<ul style="list-style-type: none"> <li>• Feature ID</li> <li>• Name</li> <li>• State (enabled or disabled)</li> <li>• Mode</li> </ul>
License	License type (Starter, Ultimate, or Pro)
Alerts	<ul style="list-style-type: none"> <li>• Alert ID</li> <li>• Type</li> <li>• Severity</li> <li>• Resolution status</li> <li>• Acknowledgement status</li> <li>• Impact type</li> <li>• Message</li> <li>• Creation time</li> <li>• Modification time</li> </ul>
Tasks	<ul style="list-style-type: none"> <li>• Task ID</li> <li>• Operation type</li> <li>• Status</li> <li>• Entities</li> <li>• Message Completion percentage</li> <li>• Creation time</li> <li>• Modification time</li> </ul>
Logs	<ul style="list-style-type: none"> <li>• Component</li> <li>• Timestamp</li> <li>• Source file name</li> <li>• Line number</li> <li>• Message</li> </ul>

Entity	Data Collected
Nutanix Services	Service-specific metrics

## Remote Support Connections

Nutanix technical support can remotely assist with problems by logging into the faulty cluster through an SSH connection.

If you encounter an issue in your Nutanix cluster and the Nutanix Support team needs access to your cluster to troubleshoot the issue, you can open a support tunnel for the Nutanix Support team to give remote access to your cluster. The Nutanix Support team ensures that the connection to your cluster through the support tunnel is secure and compliant by consolidating connectivity, authentication, authorization, audit, and recorded sessions.

You have complete control over enabling or disabling the support tunnel for a specific cluster. You can enable the support tunnel for a certain amount of time, close it at any time, or extend the duration to keep the support tunnel open. The support tunnel is automatically closed after a defined period.

### Configuring Remote Connection Using CLI

You can enable a remote support connection tunnel for a maximum of 72 hours using CLI.

#### About this task

Use the following procedure to enable the remote support connection tunnel.

#### Procedure

1. SSH into CVM or PCVM .

2. Start ncli.

```
nutanix@cvm$ ncli
<ncli>
```

3. Run the cluster start-remote-support with the duration parameter set as required.

The duration parameter must be set in minutes even if you need a duration of hours.

```
ncli> cluster start-remote-support duration=<minutes>
```

Add duration that you want to enable the remote support connection tunnel for, in minutes. For example, if you want to keep the connection open for 24 hours, enter `duration=1440`.

**Note:** You can keep the remote support connection tunnel between 0-72 hours.

## Controlling Remote Connections

#### About this task

To enable (or disable) Nutanix technical support remote access to your cluster through this connection, do the following:

#### Procedure

1. Click the gear icon in the main menu and then select **Remote Support** in the **Settings** page.  
The **Remote Support** dialog box appears.

2. Select (click the radio button for) the desired access state.
  - To allow remote access (temporarily) for Nutanix support, select **Enable for**, enter the desired number in the field provided, and select the duration (hours or minutes) from the drop-down menu.

**Note:**

- Remote Support can be enabled for any time period between 1 minute and 24 hours.
- When you enable Remote Support, a new SSH key pair is automatically generated and pushed to the Nutanix servers. This key is used to connect to the cluster in a secure way without sharing CVM password with Nutanix Support.

- To prevent remote access by Nutanix support, select **Disable**.
- Click the **Save** button to save the new setting. A **Remote Support has been updated** message is displayed along with the updated connection status.

**Note:** It might take a few minutes for the connection status to update. The settings might not reflect the change on the screen immediately. You might need to refresh the Remote Support settings screen periodically to see the updated status. If the updated status message is not displayed, the changes might still be pending.

## Configuring HTTP Proxy

### About this task

If the customer site cannot send traffic to a Nutanix service center directly, an HTTP proxy is required. To configure an HTTP proxy, do the following:

### Procedure

- Log in to the Prism Element web console.
- Click the gear icon in the main menu and then select **HTTP Proxy** in the **Settings** page.  
The **HTTP Proxy** dialog box appears.
- To add an HTTP proxy, click the **New Proxy** button and do the following in the displayed fields:

**Note:** Only one HTTP proxy can be configured at a time. If one exists currently, you must first delete it before creating a new one.

- Name:** Enter a proxy server name.
- Address:** Enter an IP address or host name for the proxy server.
- Port:** Enter the port number to use.
- Username:** Enter a user name.
- Password:** Enter a password.
- Protocols:** Select the checkbox(es) for the protocol to proxy (HTTP, HTTPS, or both).
- When all the fields are correct, click the **Save** button (lower right).  
This saves the configuration and redisplays the dialog box with the new HTTP proxy entry appearing in the list.

**Note:** To return to the **HTTP Proxy** window without saving, click the **Cancel** button.

- To edit an HTTP proxy entry, click the pencil icon on the line for that entry, update one or more of displayed field entries as desired, and then click the **Save** button.

The **Update HTTP Proxy** dialog box appears with the same fields as the **Create HTTP Proxy** dialog box plus the option (below the protocol checkboxes) to add whitelist entries. To configure HTTP proxy whitelist entries, do the following:

- To add an allowlist target, click the **+ Create** link. This opens a line to enter a target address or a network. An allowlist entry is a single host identified by an IP address or a network identified by the network address and subnet mask. Adding an allowlist entry instructs the system to ignore proxy settings for a particular address or network.
    - To allow a single IP address, enter the target IP address and then click the **Save** link in that field.
    - To allow an entire subnet, enter the network address and the subnet mask in the following format: *network\_address/subnet\_mask*, and then click the **Save** link in that field. Replace *network\_address* with the network address and *subnet\_mask* with the subnet mask of the network that you want to allow.
  - To edit an allowlist target, click the pencil icon for that target and update as needed.
  - To delete an allowlist target, click the X icon for that target.
- To delete an HTTP proxy entry, click the X icon for that entry. A window prompt appears to verify the action; click the **OK** button. The entry is removed from the HTTP proxy list.

## Accessing the Nutanix Support Portal

### About this task

Nutanix provides a variety of support services and materials through its support portal.

### Procedure

- Log in to the Prism Element web console.
- To access the Nutanix support portal, select **Support Portal** from the question mark icon  dropdown menu. The login screen for the Nutanix support portal appears in a new tab or window.
- Enter your support account user name and password. The Nutanix support portal home page appears.
- Select the desired service from the screen options.

You can select an option from one of the main menu dropdown menus or search for a topic at the top of the screen, click one of the icons (Documentation, Open Case, View Cases, Downloads) in the middle, or view one of the selections at the bottom such as an announcement or KB article. The following table lists the menu options.

**Note:** Some options have restricted access and are not available to all users.

**Table 79: Main Menu Options**

Category	Option	Description
Documentation	Product Documentation	Displays a page from which you can view the Nutanix product manuals.

<b>Category</b>	<b>Option</b>	<b>Description</b>
	Knowledge Base	Displays a page from which you can view the knowledge base (KB) articles.
	Solutions Documentation	Displays a page from which you can view documents that describe how to implement the Nutanix platform to solve a variety of business applications.
	EOL Information	Displays a page from which you can view the end of life policy and bulletins.
	Field Advisories	Displays a page from which you can view field advisories.
	Training	Provides a link to the separate Nutanix training portal.
	Security Advisories	Displays a page from which you can view security advisories.
	Acropolis Upgrade Paths	Displays a table of the supported AOS release upgrade paths.
	Compatibility Matrix	Displays a page from which you can view a compatibility matrix broken down (filtered) by hardware model, AOS version, hypervisor type and version, and feature version (NCC, Foundation, BMC/BIOS).
	Webinar Recordings	Displays a page with links to a selection of Nutanix training webinars.
Support & Forums	Open Case	Displays a form to create a support case.
	View Cases	Displays a page from which you can view your current support cases.
	.NEXT Forums	Provides a link to the (separate) Nutanix Next Community forum.
	Terms & Conditions	Displays a page from which you can view various warranty and terms and conditions documents.
Downloads	AOS (NOS)	Displays a page from which you can download AOS releases.
	Hypervisor Details	Displays a page from which you can download Acropolis hypervisor versions. You can also download supporting files used when manually upgrading a hypervisor version (AHV, ESXi, or Hyper-V).
	Prism Central	Displays a page from which you can download the Prism Central installation bundle. There are separate bundles for installing on AHV, ESXi, or Hyper-V.
	Tools & Firmware	Displays a table of tools that can be downloaded, including the Nutanix Cluster Check (NCC) and Prism Central VM.
My Products	Phoenix	Displays a page from which you can download Phoenix ISO files.
	Foundation	Displays a page from which you can download Foundation releases.
	Installed Base	Displays a table of your installed Nutanix appliances, including the model type and serial number, location, and support coverage.
	Licenses	Displays a table of your product licenses along with buttons to add or upgrade licenses for your clusters.

# Nutanix REST API

The Nutanix REST APIs allow you to create scripts that run system administration commands against the Nutanix cluster. The API enables the use of HTTP requests to get information about the cluster as well as make changes to the configuration. Output from the commands are returned in JSON format.

There are two versions of the Nutanix REST API.

- **v1:** The original Nutanix REST API.
- **v2:** An update of the v1 API. Users of the v1 API are encouraged to migrate to v2.

A complete list of REST API functions and parameters is available in the REST API Explorer section of the Prism Element web console. In addition, the complete reference for the v2 Nutanix API, including code samples in multiple languages, and tutorials are available at <http://developer.nutanix.com/>.

## Accessing the REST API Explorer

### About this task

Nutanix provides a utility with the Prism Element web console to help you get started with the REST API. The Explorer displays the parameters and format for the API calls that can be included in scripts. Sample API calls can be made to show the type of output you should expect to receive.

You can access the REST API Explorer as an admin user or a non-admin user. The v1 and v2 APIs can both be viewed in the REST API Explorer.

### Procedure

1. Open the explorer for the desired version of the API.

- » v1: Connect to the Prism Element web console, click the user icon in the upper-right corner of the Prism Element web console, and select **REST API Explorer**. In the explorer, select **Version 1** from the menu.
- » v2: Connect to the Prism Element web console, click the user icon in the upper-right corner of the web console, and select **REST API Explorer**. In the explorer, select **Version 2** from the menu.

The REST API Explorer displays a list of the cluster objects that can be managed by the API. Each line has four options:

- **Show/Hide:** Expand or reduce the detail shown for the object
- **List Operations:** Show all operations that can be run on this object
- **Expand Operations:** Show the detailed view of the operations that can be run on this object

**Tip:** The objects are listed by a relative path that is appended to the base URL  
`https://management_ip_addr:9440/PrismGateway/services/rest/v[1,2,3]/api`, where `management_ip_addr` is the IP address of any Nutanix Controller VM in the cluster.

2. Find the line for the object you want to explore and click **Expand Operations**. For this example, you will operate on a storage pool.
3. Click **GET** on the first line to show the details for this API call.

The explorer displays the parameters that can be passed when this action is used.

4. Click **Try it out!** to test the API call when used with your cluster.

The test displays the request URL required for scripting, as well as sample responses expected from the API call.

# Determining Compatibility Between Hardware and Supported Products

The Compatibility and Interoperability Matrix provides information about supported product compatibility with hardware platforms,

## Supported Products Information

Nutanix provides a [Compatibility and Interoperability Matrix](#) that helps you with information about hardware and software compatibility and interoperability. This section provides information about finding compatibility of hardware platforms for software (features, components or products) such as Microsoft System Center Operations Manager (SCOM), Nutanix Mine, or Single-Node Replication Target.

To find out if the hardware you deploy supports a feature, do the following:

1. Click the [Compatibility and Interoperability Matrix](#).
2. On the **Platform** tab, in the **Hardware Manufacturer** field, select the name of the hardware manufacturer. Select **Select All** in the **Hardware Manufacturer** field to check compatibility with hardware manufactured by all the listed manufacturers.
3. Turn on the **Supported Products** toggle switch.
4. In the filter field below **Hardware Model** column name, type the name of the software to filter the list of compatible platforms.

This field supports only certain variations in the name of a feature. For example, SNRT is not a supported filter for Single Node Replication Target feature. Instead, type single or single-node.

# HELP RESOURCES

---

There are several information sources that you can access at any time when you need help:

- Context-sensitive help documentation. For more information, see [Accessing Online Help](#) on page 396.
- Health dashboard tutorial. For more information, see [Health Dashboard](#).
- Customer support portal. For more information, see [Accessing the Nutanix Support Portal](#) on page 392.
- Nutanix community forum. For more information, see [Accessing the Nutanix Next Community](#) on page 397.
- REST API explorer. For more information, see [Accessing the REST API Explorer](#) on page 394.
- Glossary of terms. For more information, see [Nutanix Glossary](#).

## Accessing Online Help

### About this task

The Prism Element web console includes online help documentation that you can access at any time.

### Procedure

1. Log in to the Prism Element web console.
2. To open the online help, choose one of the following from the question mark icon drop-down list of the [Main Menu](#):
  - » Select **Help with this page** to display help documentation that describes the current screen.

**Note:** In a task window click the question mark icon in the upper right to display the help documentation for that window.

- » Select **General Help** to display the **Help Organization** page.

A context-sensitive help page or the **Help Organization** page appears in a new tab or window. (These pages are located on the Nutanix support portal.) The **Help Organization** page provides descriptions of the major help topics with links to the entry page for each major topic. The display includes a breadcrumb at the top to navigate through the help pages.

3. To select a topic from the table of contents, click the click the collapse menu icon (also know as a *hamburger* button) in the upper left.  
A table of contents pane appears on the left. Click a topic in the table of contents to display that topic.
4. To display all the help contents as a single document (*Prism Element Web Console Guide*), click the **ePub** or **PDF** button in the upper right corner.  
You can view the *Prism Element Web Console Guide* in either ePUB or PDF format by selecting the appropriate button. If your browser does not support the selected format, you can download the PDF or ePUB file.
5. To search for a topic, click the **Other** icon in the main menu bar and enter a search string in the field.  
This searches not only the help contents, but also all the documentation, knowledge base articles, and solution briefs. Matching results appear below the search field. Click a topic from the search results to display that topic.

## Accessing the Nutanix Next Community

Nutanix maintains a community forum for customers and partners to facilitate a peer-to-peer exchange of ideas, tips, and information about Nutanix technologies and the rapidly changing landscape of data center IT.

### Procedure

1. Log in to the Prism Element web console.
2. To access the Nutanix next community forum, select **Nutanix Next Community** from the question mark icon  dropdown menu of the [Main Menu](#).

The Nutanix Next Community main page appears in a new tab or window. From this page you can search existing posts, ask questions, and provide comments.

## Glossary

For terms used in this guide, see [Nutanix Glossary](#).

# COPYRIGHT

---

Copyright 2025 Nutanix, Inc.

Nutanix, Inc.  
1740 Technology Drive, Suite 150  
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.