



## Prism Web Console Guide

Acropolis 5.1

14-Sep-2017

# Contents

<b>Help Organization.....</b>	<b>8</b>
<b>1: 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.....	13
Medusa.....	13
Cassandra.....	13
Stargate.....	13
Curator.....	13
Prism.....	14
Failure Scenarios.....	14
Node Failure.....	14
Drive Failures.....	15
Network Link Failure.....	17
Block Fault Tolerance.....	17
Block Fault Tolerant Data Placement.....	20
Redundancy Factor 3.....	22
Nonconfigurable Components.....	24
System Maximums.....	26
Three Node Cluster Considerations.....	27
<b>2: Cluster Management.....</b>	<b>28</b>
Web Console Overview.....	28
Logging Into the Web Console.....	29
Logging Out of the Web Console.....	32
Main Menu Options.....	32
Home Dashboard.....	38
Understanding Displayed Statistics.....	41
Modifying Cluster Details.....	42
Modifying UI Settings.....	44
Checking Version.....	45
License Management.....	46
Before You License Your Cluster.....	46
AOS Licenses.....	47
Prism Pro License.....	48
Add-On Licenses.....	48
Configuring Portal Connection for License Management.....	49
Managing Licenses with Portal Connection.....	55
Managing Licenses without Portal Connection (Default).....	61
Displaying License Features and Details.....	72
License Warnings in the Web Console.....	74
Software and Firmware Upgrades.....	74

Options for Downloading Updates.....	76
AOS Upgrade Prerequisites.....	78
Upgrading AOS.....	79
Upgrading Disk Firmware: On Demand Download.....	81
Upgrading NCC Software.....	82
Installing NCC from an Installer File.....	84
Hypervisor Upgrade Overview and Requirements.....	86
Upgrading AHV Hosts.....	88
Upgrading ESXi Hosts by Uploading Binary and Metadata Files.....	90
Upgrading Hyper-V Hosts.....	94
Upgrading XenServer Hosts.....	94
Applying XenServer Patches.....	95
Upgrading BMC or BIOS Firmware.....	98
Upgrading Foundation.....	101
Upgrading HBA Firmware.....	101
Viewing the Progress of the Download or Upgrade Process.....	103
Multi-Cluster Management.....	105
Register (Unregister) with Prism Central.....	105
Increasing the Cluster Fault Tolerance Level.....	107
Increasing Controller VM Memory Size.....	111

## **3: Storage Management..... 113**

Storage Components.....	113
Compression.....	115
Deduplication.....	116
Erasure Coding.....	117
Capacity Reservation Best Practices.....	119
Storage Dashboard.....	119
Storage Overview View.....	120
Storage Diagram View.....	122
Storage Table View.....	129
Creating a Storage Pool.....	138
Modifying a Storage Pool.....	138
Creating a Storage Container.....	139
Modifying a Storage Container.....	143
Volume Group Configuration.....	143
Volume Management.....	144
Concurrent Access from Multiple Clients.....	147
Creating a Volume Group.....	147
Modifying a Volume Group.....	148
Flash Mode for Virtual Machines and Volume Groups.....	149
Removing Flash Mode for Virtual Disks of a Volume Group.....	150

## **4: Network Management..... 151**

Configuring Network Connections.....	151
Modifying Network Connections.....	154
Configuring Network Switch Information.....	155
Creating SNMP Profiles.....	158
Modifying Switch Information.....	159
Network Visualization.....	160
Prerequisites.....	161
Supported Switches.....	161
Network Visualizer.....	161
Viewing the Network Visualizer.....	162

Customizing the Topology View.....	162
Viewing VM Information.....	163
Viewing Host Information.....	163
Viewing Switch Information.....	164
<b>5: Hardware Management.....</b>	<b>166</b>
Hardware Dashboard.....	166
Hardware Overview View.....	167
Hardware Diagram View.....	168
Hardware Table View.....	176
Expanding a Cluster.....	186
Modifying a Cluster.....	196
Life Cycle Manager.....	199
Taking Inventory With the Life Cycle Manager.....	200
Performing Updates With the Life Cycle Manager.....	202
Using the Life Cycle Manager Without Web Access.....	207
<b>6: Acropolis Block Services.....</b>	<b>210</b>
Example Use Cases Supported by ABS.....	211
If You are Already Using Volume Groups.....	211
ABS Requirements and Supported Clients.....	211
Enabling Acropolis Block Services.....	213
Creating a Volume Group for Use with ABS.....	213
Configuring Windows Clients.....	217
Configuring Linux Clients.....	222
Configuring AIX Clients.....	225
Booting Over iSCSI.....	227
Converting Volume Groups and Updating Clients to Use ABS.....	230
Modifying Windows Client Settings to Use ABS.....	231
Modifying Linux Client Settings to Use ABS.....	231
Modifying a Volume Group for Use with ABS.....	232
<b>7: Data Protection.....</b>	<b>233</b>
Protection Strategies.....	233
Data Protection Concepts.....	236
Data Protection Dashboard.....	237
Data Protection Overview View.....	238
Data Protection Table View.....	239
Async DR Protection Domain Configuration.....	250
Data Protection Guidelines (Async DR).....	250
Configuring a Protection Domain (Async DR).....	256
Modifying a Protection Domain (Async DR).....	262
Restoration of Protected Entities.....	264
Protection Domain Failover and Failback (Async DR).....	266
Metro Availability Protection Domain Configuration.....	270
Data Protection Guidelines (Metro Availability).....	271
Configuring a Protection Domain (Metro Availability).....	274
Metro Availability Witness Option.....	283
Protection Domain Failover and Failback (Metro Availability).....	301
Reconfiguring Data Protection in a Metro Availability and Async DR Configuration.....	303
Upgrade Best Practices and Requirements with Metro Availability Enabled.....	303
Cloud Connect (AWS and Azure).....	304
Cloud Connect Guidelines (AWS and Azure).....	304

Remote Site Configuration.....	317
Configuring a Remote Site (Physical Cluster).....	317
Modifying a Remote Site (Physical Cluster or Cloud).....	322
Network Mapping.....	323
Recovering from the Remote Snapshots on a Backup or DR Site.....	325
Synchronous Replication.....	326
Failover Scenarios for Synchronous Replication in Hyper-V.....	327
Fallback Scenarios for Synchronous Replication in Hyper-V.....	328
Failing Over a Protection Domain Manually in Synchronous Replication (Planned Failover).....	330
Registering a VM on a Hyper-V Cluster.....	330
Unregistering a VM on a Hyper-V Cluster.....	331
Nutanix Cross Hypervisor Disaster Recovery.....	331
Recovering Virtual Machines in the Remote Cluster.....	332
Bringing Multiple SCSI Disks Online.....	333
Blacklisting Devices for Multipathing.....	334
Self-Service Restore.....	334
Requirements and Limitations of Self-Service Restore.....	335
Enabling Self-Service Restore.....	335
Restoring a File as a Guest VM Administrator (Using Web Interface).....	336
Restoring a File as a Guest VM Administrator.....	337
Restoring a File as a Nutanix Administrator.....	339
Single-Node Replication Target Clusters.....	340
Single-Node Replication Target Requirements and Limitations.....	341
Imaging Single-Node Replication Target Nodes.....	342
Setting Up Single-Node Replication Target Clusters.....	343
Recovery Procedures by using Single-Node Replication Target Clusters.....	343

## **8: Health Monitoring..... 344**

Health Dashboard.....	344
Configuring Health Checks.....	348
Running Checks by Using Web Console.....	349
Collecting Logs by Using Web Console.....	350

## **9: Virtual Machine Management..... 352**

VM Dashboard.....	352
VM Overview View.....	353
VM Table View.....	354
VM Management.....	366
Creating a VM (AHV).....	366
Managing a VM (AHV).....	372
Creating a VM (ESXi).....	377
Managing a VM (ESXi).....	379
Configuring Images.....	382
Virtual Machine Customization.....	385
Customizing Linux Virtual Machines with Cloud-Init.....	386
Customization of Windows Virtual Machines with System Preparation.....	386
VM High Availability in Acropolis.....	388
Enabling High Availability for the Cluster.....	389
Nutanix Guest Tools.....	390
Nutanix Guest Tools Requirements and Limitations.....	390
Enabling and Mounting Nutanix Guest Tools.....	393
Enabling and Mounting NGT Simultaneously on Multiple VMs.....	396
NGA and Controller VM Communication.....	396

CD-ROM Eject Functionality of NGT.....	397
Nutanix Guest Tools Usage in Disaster Recovery.....	397
Upgrading NGT.....	397
Disabling and Removing Nutanix Guest Tools.....	398
Affinity Policies for AHV.....	398
Configuring VM-VM Anti-Affinity Policy.....	399
<b>10: Performance Monitoring.....</b>	<b>401</b>
Analysis Dashboard.....	401
Creating an Entity Chart.....	403
Creating a Metric Chart.....	404
Chart Metrics.....	405
Exporting Performance Data.....	409
<b>11: Alert and Event Monitoring.....</b>	<b>410</b>
Alerts Dashboard.....	410
Alert Messages View.....	411
Event Messages View.....	413
Configuring Alert Emails.....	414
Configuring Alert Policies.....	416
Alerts/Health checks.....	417
Cluster.....	417
Controller VM.....	480
DR.....	488
Guest VM.....	510
Hardware.....	516
Network.....	534
Node.....	538
Other.....	549
Storage.....	552
<b>12: Task Status.....</b>	<b>567</b>
View Task Status.....	567
<b>13: System Management.....</b>	<b>569</b>
Configuring a Filesystem Whitelist.....	569
Configuring Name Servers.....	570
Cluster Time Synchronization.....	571
Recommendations for Time Synchronization.....	571
Configuring NTP Servers.....	572
Configuring an SMTP Server.....	573
Configuring SNMP.....	574
Nutanix MIB.....	578
Configuring a Banner Page.....	583
VM Management through Prism Element (ESXi).....	584
Registering a vCenter Server.....	585
In-Place Hypervisor Conversion.....	586
Requirements and Limitations for In-Place Hypervisor Conversion.....	586
In-Place Hypervisor Conversion Process.....	588
Converting Cluster (ESXi to AHV).....	589
Converting Cluster (AHV to ESXi).....	591
Aborting Cluster Conversion.....	592

Internationalization (i18n).....	593
Localization (L10n).....	594
Changing the Language Settings.....	594
Hyper-V Setup.....	595
Joining the Cluster and Hosts to a Domain.....	595
Creating a Failover Cluster for Hyper-V.....	597
Enabling Kerberos for Hyper-V.....	598
<b>14: Security Management.....</b>	<b>604</b>
Configuring Authentication.....	604
Assigning Role Permissions.....	610
Installing an SSL Certificate.....	612
Controlling Cluster Access.....	615
Data-at-Rest Encryption.....	616
Preparing for Data-at-Rest Encryption.....	618
Configuring Data-at-Rest Encryption.....	619
Enabling/Disabling Encryption.....	624
Changing Key Encryption Keys.....	624
Destroying Data on a SED.....	625
<b>15: User Management.....</b>	<b>626</b>
Creating a User Account.....	626
Updating a User Account.....	628
Updating My Account.....	630
Deleting a User Account.....	632
<b>16: Support Services.....</b>	<b>634</b>
Configuring Pulse.....	634
Pulse Access Requirements.....	636
Controlling Remote Connections.....	636
Configuring HTTP Proxy.....	637
Accessing the Nutanix Support Portal.....	639
Nutanix REST API.....	641
Accessing the REST API Explorer.....	642
<b>17: Help Resources.....</b>	<b>645</b>
Accessing Online Help.....	645
Accessing the Nutanix Next Community.....	647
Glossary.....	648
<b>Copyright.....</b>	<b>655</b>
License.....	655
Conventions.....	655
Default Cluster Credentials.....	655
Version.....	656

# Help Organization

This documentation is organized as follows:

- [\*Nutanix Platform Overview\*](#) on page 9 describes the Nutanix architecture.
- [\*Cluster Management\*](#) on page 28 describes how to access and use the 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.
- [\*Multi-Cluster Management\*](#) on page 105 describes how to install a VM that runs an application called *Prism Central* and how to use *Prism Central* to monitor and manage multiple clusters.
- [\*Storage Management\*](#) on page 113 describes how to monitor storage use in a Nutanix cluster and how to create storage pools and containers.
- [\*Hardware Management\*](#) on page 166 describes how to monitor hardware configurations in a Nutanix cluster and how to expand the cluster.
- [\*Data Protection\*](#) on page 233 describes disaster protection strategies for a Nutanix cluster and how to configure and use the Nutanix disaster recovery (DR) solution.
- [\*Health Monitoring\*](#) on page 344 describes how to monitor the health of VMs, hosts, and disks across a Nutanix cluster.
- [\*Virtual Machine Management\*](#) on page 352 describes how to monitor status of the VMs across a Nutanix cluster.
- [\*Performance Monitoring\*](#) on page 401 describes how to monitor and analyze performance in a Nutanix cluster.
- [\*Alert and Event Monitoring\*](#) on page 410 describes how to monitor activity in a Nutanix cluster and how to configure alert policies and notification.
- [\*System Management\*](#) on page 569 describes how to configure various system settings such as for SNMP, NTP, and SMTP.
- [\*Security Management\*](#) on page 604 describes how to configure various security settings including authentication method, SSL certificates, and SSH keys.
- [\*User Management\*](#) on page 626 describes how to add, edit, and delete user accounts.
- [\*Support Services\*](#) on page 634 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.

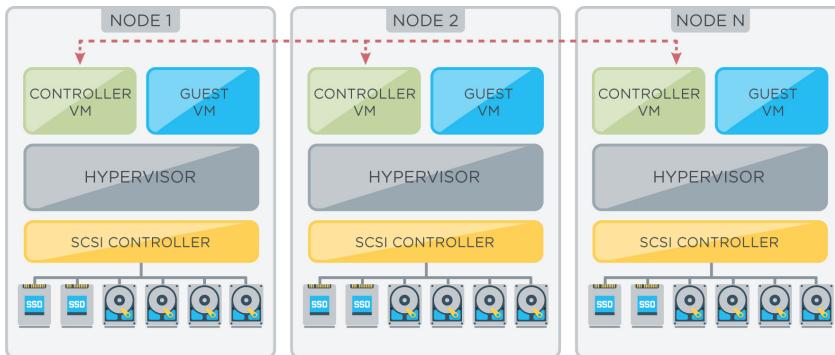
## Nutanix Platform Overview

The Nutanix Enterprise Cloud Platform is a converged, scale-out compute and storage system that is purpose-built to host and store virtual machines.

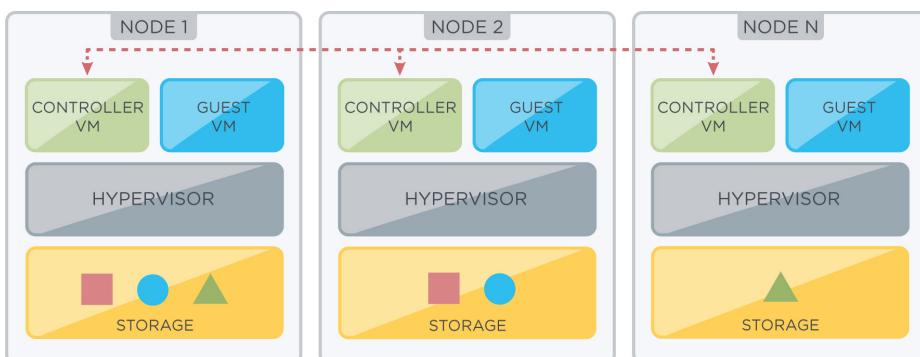
All nodes in a Nutanix cluster converge to deliver a unified pool of tiered storage and present resources to VMs for seamless access. A global data system architecture integrates each new node into the cluster, allowing you to scale the solution to meet the needs of your infrastructure.

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



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.

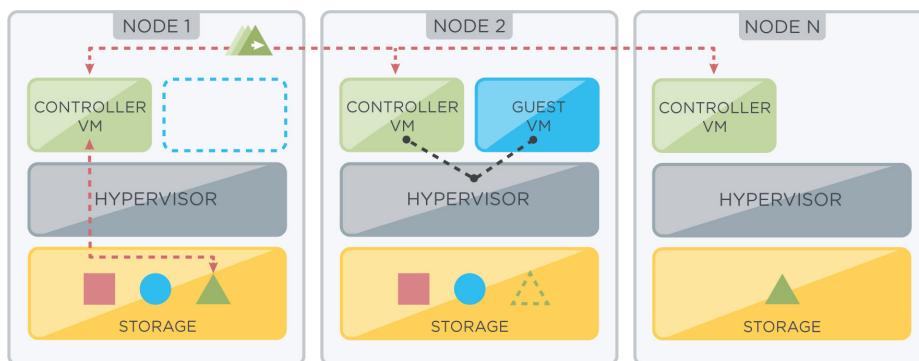
When the guest VM sends a read request through the hypervisor, the Controller VM reads from the local copy first, if present. If the host does not contain a local copy, then the Controller VM reads across the network from a host that does contain a copy. As remote data is accessed, the remote data is 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.

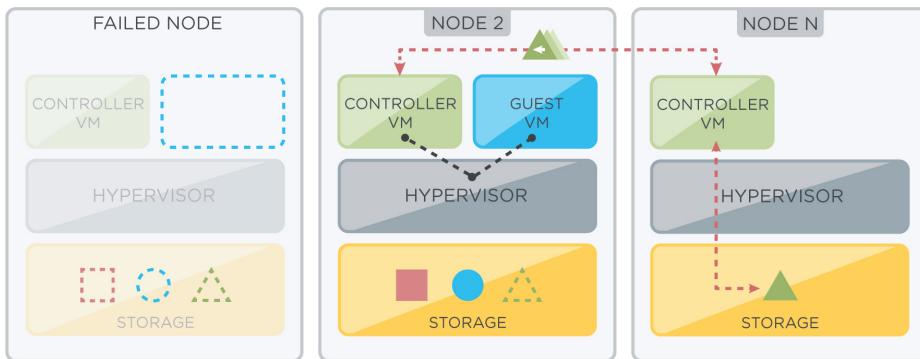
## Live Migration



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



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.

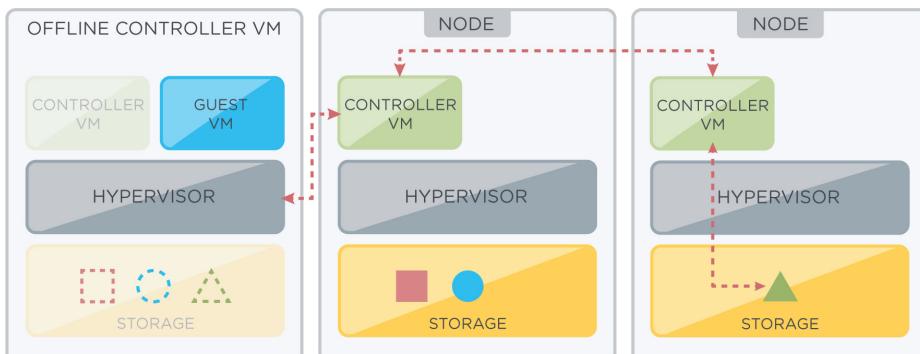
### Virtualization Management VM High Availability

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

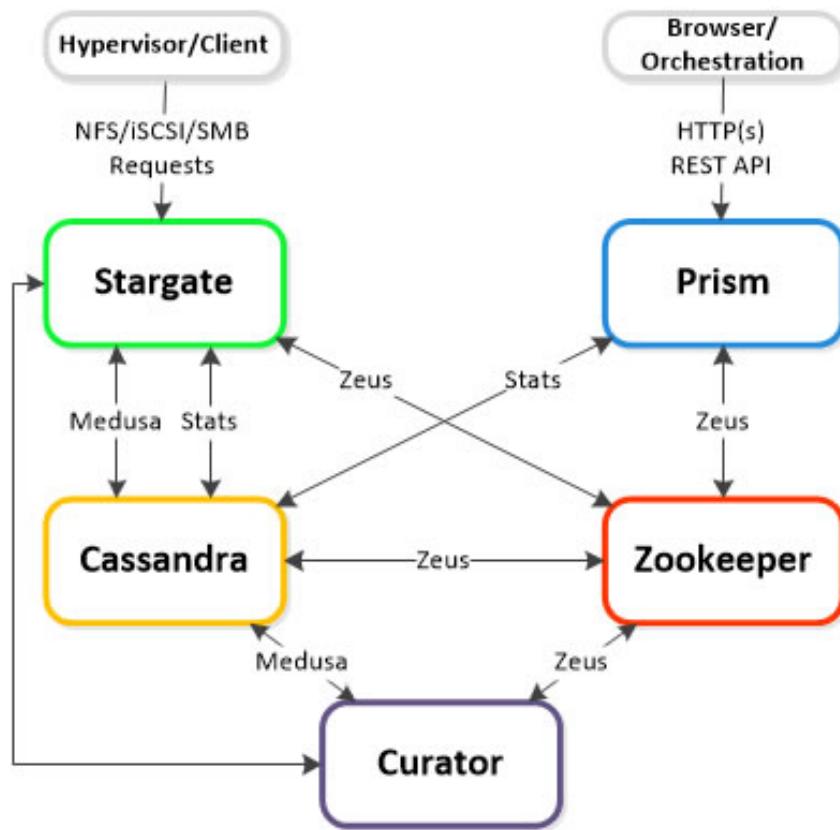


The Nutanix cluster automatically selects the optimal path between a hypervisor host and its guest VM data. The Controller VM has multiple redundant paths available, which makes the cluster more resilient to failures.

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



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 redundancy factor 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 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.

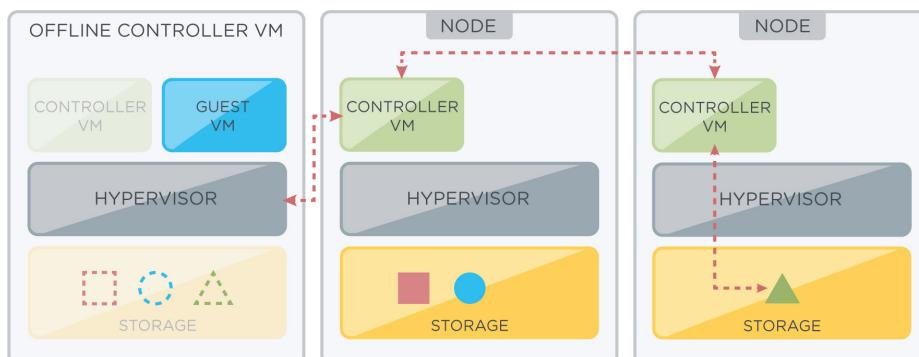
## Failure Scenarios

Hardware failures are a part of any datacenter lifecycle. The Nutanix architecture was designed with this inevitability in mind. A cluster can tolerate a single failure 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 in order to give the administrator a chance to respond to the situation.

### 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



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 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.

#### 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.

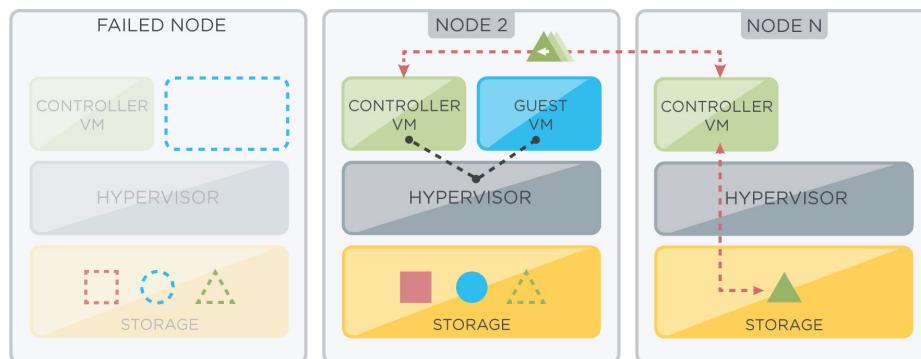
As soon as the redirection takes place, VMs can resume reads and writes. Performance may decrease slightly, because the IO is traveling across the network, rather than across the internal network. Because all

traffic goes across the 10 GbE network, most workloads does 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



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.

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 will notice that their VM is unavailable while it is restarted on the new host. Without HA, the VM will need to be manually restarted.

### 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.

## 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. Systems with two SATA-SSDs use the second drive for additional hot-tier DSF data storage. 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 the 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 14.



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

## Metadata Drive Failure

The metadata drive 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. All of these storage uses were designed for potential failure, and therefore are replicated to other metadata disks in the cluster.

If a metadata drive fails, the first component to notice the problem is Cassandra. It will no longer be able to access its share of the database, and will begin a persistent cycle of restarts in an attempt to fix the problem.

Stargate depends on Cassandra through Medusa, so eventually Stargate will fail, which will be detected by the cluster, and the path will be automatically redirected based on Data Path Redundancy. Soon, the host with the failed metadata drive will be redirected across the network to another Stargate.

If the Cassandra process is down on a node for more than five 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 five minutes, the procedure to detach the node 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=cvm_id
```

## What Will Users Notice?

During the switching process, the host with the failed SSD may report that the shared storage is unavailable. Guest VMs on this host will appear to "hang" until the storage path is restored.

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 will not diminish in a way that is perceivable to users.

## What Happens If Another One Fails?

A second metadata drive failure will have the same impact on the VMs on the other host, which means there will be two hosts sending IO requests across the network. The healing feature of the Cassandra ring reduces the risk involved with losing a second node provided that the second failure does not occur before the healing process has completed.



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

## 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.

The cluster software receives a hardware alert from the host that a data drive (HDD or SSD) has failed, and immediately begin 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 will need to read 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 2, losing two drives on different nodes and in the same storage tier 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 . Failure of a network link is tolerated with no impact to users if both 10 GbE ports are connected to the customer's network. If the cluster must fail over to a 1 GbE link, then write performance decreases.

### What Will Users Notice?

Each Nutanix node is configured at the factory to use one 10 GbE port as the primary pathway for vSwitch0. The other 10 GbE port is configured in standby mode. In this configuration, guest VM performance does not decrease. If a 10 GbE port is not configured as the failover path, then traffic will fail over to a 1 GbE port. This failover reduces the throughput of storage traffic, and decreases the write performance for guest VMs on the host with the failed link. Other hosts may experience a slight decrease as well, but only on writes to extents that are stored on the host with the link failure.

### What Happens if Another One Fails?

If both 10 GbE links are down, then the host will fail over to a 1 GbE port, if it is configured as a standby path. This failover reduces the throughput of storage traffic, and decreases the write performance for guest VMs on the host with the failed link. Other hosts may experience a slight decrease as well, but only on writes to extents that are stored on the host with the link failure.

## Block Fault Tolerance

Block fault tolerance is the Nutanix cluster's ability to make redundant copies of any data and place the data on nodes that are not in the same block. Metadata also must be block fault tolerant.



**Note:**

- Block Fault Tolerance is a "best effort" feature. In case of insufficient space across blocks, data copies are kept on the same block.
- Do not enable erasure coding on clusters with the block fault tolerance.

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

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

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.
- There is enough free space in all the tiers, in at least replication factor number of blocks in the cluster. For example, if the replication factor of storage containers in the cluster is two, then at least two blocks require free space.
- Erasure coding is not enabled on any storage container.



**Note:** This is not applicable for single-node replication target clusters. For more information on how single-node replication target clusters handle failures, see [Single-Node Replication Target Clusters](#) on page 340.

## Data Resiliency Levels

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.

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
3	6	3 (minimum 2 nodes each)	1 block or 2 nodes or 2 disks
Metro Cluster (see See "Metro Availability" in the "Data Protection" chapter of the <i>Prism Web Console Guide</i> .)	3 nodes at each site	2	1 cluster failure

The state of block fault tolerance is available for viewing through the Prism 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.

Web Console

*Data Resiliency Status* view on the **Home** screen

nCLI

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

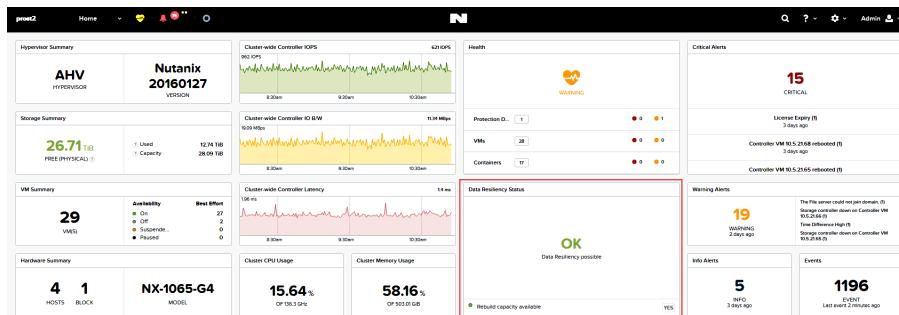


Figure: Data Resiliency Status from Prism.

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

- A replication factor two or replication factor three cluster with three or more blocks can tolerate a maximum failure of one block.
- A replication factor three cluster with 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/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 replication factor 2 and replication factor 3. To enable metadata block fault tolerance, your metadata must meet the following requirements.

#### 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>

#### Additional Requirements when Adding Nodes to an Existing Block Aware Cluster

Replication Factor	Requirement	Example
	<b>Note:</b> Be sure your cluster has met the previous minimum cluster requirements.	

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 RF=2, you need twice the number of nodes as there are in the block with the most or maximum number of nodes.	If a block contains 4 nodes, you need 8 nodes distributed across the remaining (non-failing) blocks to maintain block fault tolerance for that cluster. X = number of nodes in the block with the most nodes. In this case, 4 nodes in a block. $2X = 8$ nodes in the remaining blocks.
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 3 you need four times the number of nodes as there are in the block with the most or maximum number of nodes.	If a block contains 4 nodes, you need 16 nodes distributed across the remaining (non-failing) blocks to maintain block fault tolerance for that cluster. X = number of nodes in the block with the most nodes. In this case, 4 nodes in a block. $4X = 16$ nodes in the remaining blocks

## 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.

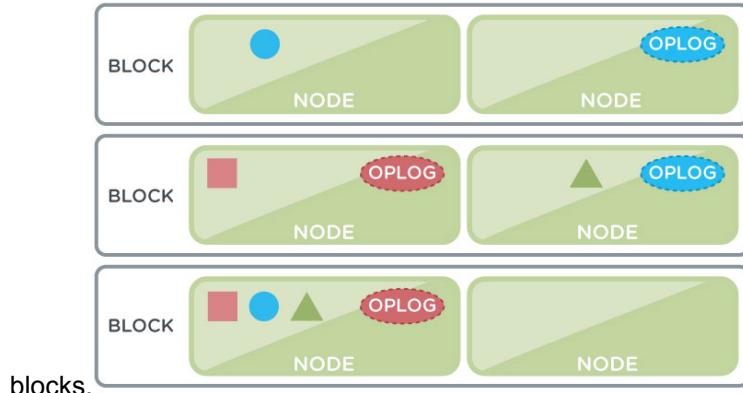
Depending on the volume of data that needs to be relocated, it might take Curator several scans over a period of hours to distribute data across the blocks.

Block fault tolerant data placement is on a best effort basis but is not guaranteed. Conditions such as high disk usage between blocks may 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 nodes in blocks other than the block that contains the node where the VM is running. The cluster keeps two copies of each write stored in the oplog.

Redundant copies of the guest VM data (designated by ■ ● ▲) are placed on different



blocks.

Figure: Block-aware placement of guest VM data

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

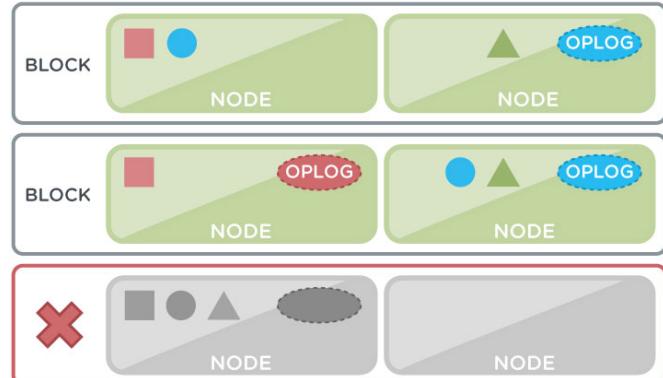
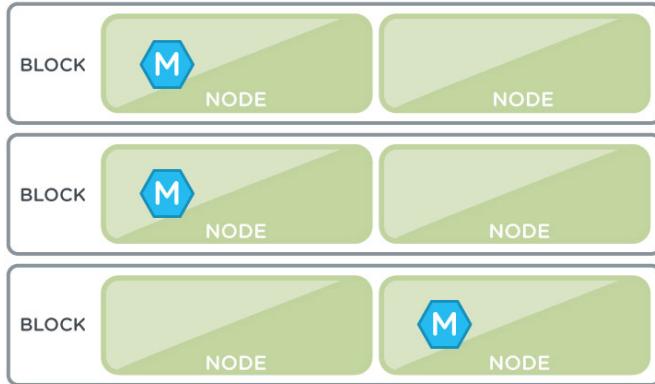


Figure: Block-aware placement of guest VM data with block failure

## 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.

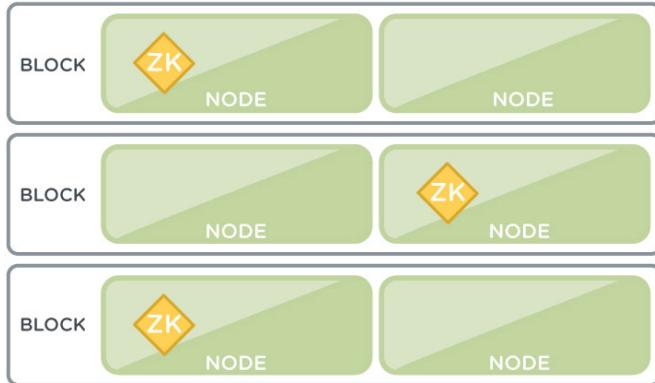
With block fault tolerance, the Cassandra peers are distributed among the blocks to ensure that no two peers are on the same block. In the event of a block failure, at least two copies of the metadata is present in the cluster .



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

## Redundancy Factor 3

Redundancy factor 3 is a configurable option that allows a Nutanix cluster to withstand the failure of two nodes or drives in different blocks.

By default, Nutanix clusters have redundancy factor 2, which means they can tolerate the failure of a single node or drive. The larger the cluster, the more likely it is to experience multiple failures. Without redundancy factor 3, multiple failures cause cluster unavailability until the failures are repaired.

Redundancy factor 3 has the following requirements:

- A cluster must have at least five nodes for redundancy factor 3 to be enabled.
- For guest VMs to tolerate the simultaneous failure of two nodes or drives in different blocks, the data must be stored on storage containers with replication factor 3.
- Controller VMs must be configured with 24 GB of memory.

The state of fault tolerance is available to view through the management interfaces.

Web Console

*Data Resiliency Status* view on the **Home** screen

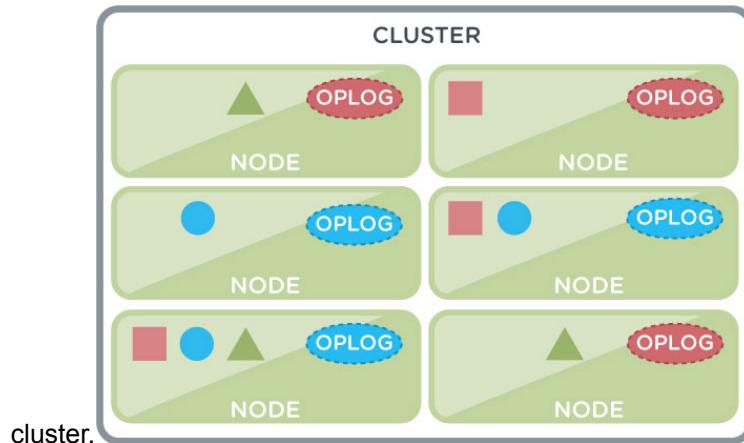
nCLI

```
ncli> cluster get-redundancy-state
```

## Guest VM Data

For storage containers with replication factor 3, the cluster stores three redundant copies of guest VM data and the oplog.

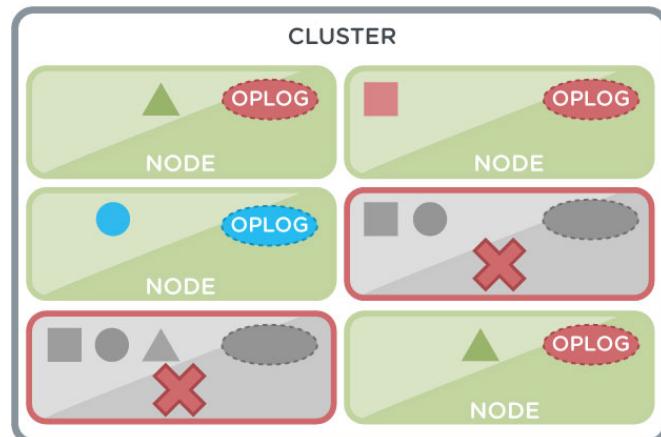
Redundant copies of the guest VM data (designated by □ ● ▲) are stored on different nodes in the



cluster.

*Figure: Replication factor 3 placement of guest VM data*

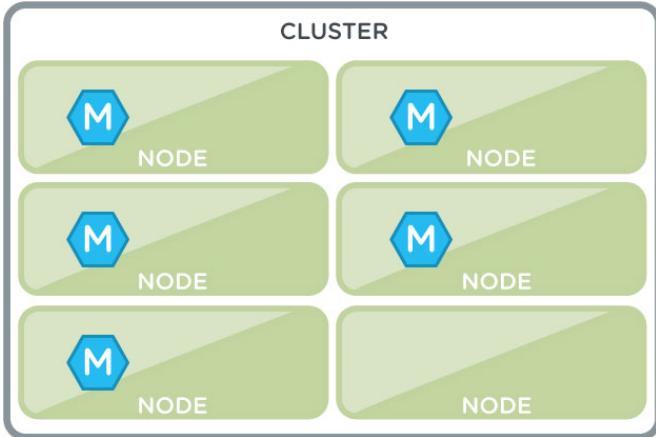
In the case of two nodes failing, at least one copy of all guest VM data, including the oplog, is available. Under-replicated VM data is copied to other nodes.



*Figure: Replication factor 3 placement of guest VM data with failure of 2 nodes*

## Metadata

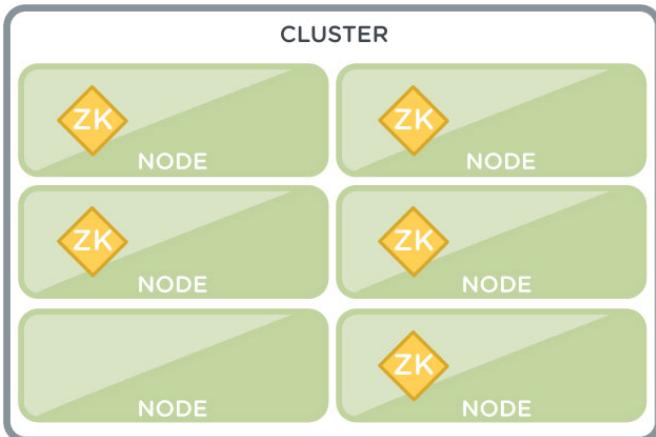
At least half of the redundant copies of metadata must be available to ensure consistency. Without redundancy factor 3, the cluster keeps three copies of metadata. With redundancy factor 3, the cluster keeps five copies of metadata so that if two nodes fail, at least three copies are available.



*Figure: Redundancy factor 3 metadata*

### Configuration Data

The Nutanix Zeus component uses Zookeeper to store essential configuration data for the cluster. Without redundancy factor 3, the cluster keeps three copies of configuration data. With redundancy factor 3, the cluster keeps five copies of configuration data so that if two nodes fail, at least three copies are available.



*Figure: Redundancy factor 3 configuration data*

### Nonconfigurable Components

The components listed here are configured by the Nutanix manufacturing and installation processes. Do not modify any of these components except under the direction of Nutanix Support.



**Warning:** Modifying any of the settings listed here may render your cluster inoperable.

In particular, do not, under any circumstances, use the **Reset System Configuration** option of ESXi, delete the Nutanix Controller VM, or take a snapshot of the Controller VM for backup.



**Warning:** You must not run any commands on a Controller VM that are not covered in the Nutanix documentation.

## Nutanix Software

- Local datastore name
- Settings and contents of any Controller VM, including the name and the virtual hardware configuration (except memory when required to enable certain features)

## ESXi Settings



**Important:** If you create vSphere resource pools, Nutanix Controller VMs must have the top share.

- NFS settings
- VM swapfile location
- VM startup/shutdown order
- iSCSI software adapter settings
- vSwitchNutanix standard virtual switch
- vmk0 interface in port group "Management Network"
- SSH enabled
- Host firewall ports that are open
- Taking snapshots of the Controller VM

## Hyper-V Settings

- English language pack  
Installation of other language packs is not supported.
- Cluster name (using the web console)
- Host name (you can configure the host name only at the time of creating and expanding the cluster.)
- Internal switch settings and external network adapter name

Two virtual switches are created on the Nutanix host, ExternalSwitch and InternalSwitch. Two virtual network adapters are created on the host corresponding to these virtual switches, vEthernet (ExternalSwitch) and vEthernet (InternalSwitch).



**Note:** Do not delete these switches and adapters and do not change the names of these virtual switches and the virtual network adapters.

- Windows roles and features

No new Windows roles or features must be installed on the Nutanix hosts. This especially includes the Multipath IO feature, which can cause the Nutanix storage to become unavailable.

- Controller VM pre-configured VM setting of Automatic Start Action
- Controller VM high-availability setting
- Controller VM operations: migrating, saving state, or taking checkpoints of the Controller VM

## AHV Settings

- Hypervisor configuration, including installed packages
- iSCSI settings
- Open vSwitch settings
- Taking snapshots of the Controller VM

## System Maximums

The figures listed here are the maximum tested and supported values for entities in a Nutanix cluster.

Entity	Supported Maximum
VMs or volume groups	Up to available hardware resources and hypervisor limitations (no known logical limit) <ul style="list-style-type: none"> <li>• Async DR: 200 VMs or volume groups for each protection domain, or consistency group</li> <li>• Metro Availability: See the <i>Maximum Limits for Metro Availability</i> table in <a href="#">Data Protection Guidelines (Metro Availability)</a> on page 271 topic.</li> <li>• 1200 files for all the entities per vStore</li> </ul>
vDisks (including snapshots)	AOS 4.7.x = 200,000 AOS 5.0.x = 200,000
vDisk size (limited by hypervisor or guest OS)	ESXi 5.5 and above = 62 TB ESXi 5.1 and below = 2 TB minus 512 B Hyper-V vhdx format = 64TB HyperV vhd format = 2TB AHV = No known limit
vCPUs per VM	Constrained by the number of logical processors available to the VM.
Memory per VM	Constrained by physical RAM capacity.
RDM vDisks	256 per vZone or ESXi host
NFS datastores	Nutanix = 256 per host ESXi 5.x and later = 256 per host
NFS datastore size	Available disk capacity in the Nutanix cluster (no known logical limit)
Small files (<512 KB) on NFS datastores	2.5 GB per Nutanix node
Storage pools	2 per Nutanix cluster
Storage pool size	Available disk capacity in the Nutanix cluster (no known logical limit)
Physical disks per storage pool	Number of disks in the Nutanix cluster (no known logical limit)
Storage Containers (created on Nutanix cluster)	256 per Nutanix cluster
Storage Container size	Available disk capacity in a storage pool (no known logical limit)
Replication factor	3

Entity	Supported Maximum
Nutanix management interface (Prism) simultaneous connections	20 clients per Controller VM
iSCSI	128 LUNs per node
	256 LUNS per Volume Group
	No limit for the number of volume groups if you do not exceed maximum number of LUNs per node

Nutanix clusters are also subject to the vSphere maximum values documented by VMware. For a list of the vSphere maximums, see *Configuration Maximums* for the version of vSphere you are running.

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 increases to more than 50, backup jobs start to get into NFS timeouts.

## Three Node Cluster Considerations

A Nutanix cluster must have at least three nodes. Minimum configuration (three node) clusters provide the same protections as larger clusters, and a three node cluster can continue normally after a node failure. However, one condition applies to three node clusters only.

When a node failure occurs in a cluster containing four or more nodes, you can dynamically remove that node to bring the cluster back into full health. The newly configured cluster still has at least three nodes, so the cluster is fully protected. You can then replace the failed hardware for that node as needed and add the node back into the cluster as a new node. However, when the cluster has just three nodes, the failed node cannot be dynamically removed from the cluster. The cluster continues running without interruption on two healthy nodes and one failed node, but the failed node cannot be removed when there are only two healthy nodes. Therefore, the cluster is not fully protected until you fix the problem (such as replacing a bad boot disk) for the existing 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 a web-based management console or a command line interface (nCLI).

- The web console is a graphical user interface (GUI) that allows you to monitor cluster operations and perform a variety of configuration tasks (see [Web Console Overview](#) on page 28).
- Nutanix employs a license-based system to enable your entitled Nutanix features, and you can install or regenerate a license through the web console (see [License Management](#) on page 46).
- You can upgrade a cluster when a new AOS release is available through the web console. You can also update other components such as disk firmware and hypervisor software (see [Software and Firmware Upgrades](#) on page 74).
- If you have multiple clusters, you can manage them all through a single web interface (see [Multi-Cluster Management](#) on page 105).



**Note:** You can perform most administrative actions using either the 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 web console or the task is part of an advanced feature that most administrators do not need to use. See the Nutanix *Command Reference* for information about using the nCLI. See the *AHV Administration Guide* and hypervisor-specific guides for information about platform configuration and hypervisor-specific tasks that are not performed through the web console.

### Web Console Overview

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

#### Display Features

The 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 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 pull-down list (Home, Health, VM, Storage, Hardware, DR, Analysis, or Alerts) to display information about that entity. You can also search for specific topics or select various tasks from the pull-down lists on the right side of the main menu bar (see [Main Menu Options](#) on page 32). In addition, the main menu bar includes status icons for quick access to health, alert, and event information.
- Entity views. There is a dashboard view for each entity. Some entities (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 (see [Alerts Dashboard](#) on page 410).

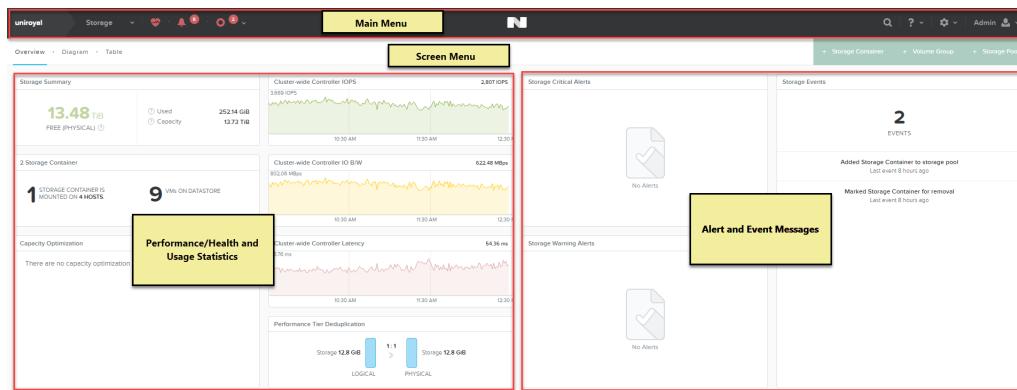


Figure: Overview Screen Sections

## Logging Into the Web Console

To log into the web console, do the following. Knowledge base article [KB 1661](#) lists default cluster credentials.

1. Open a web browser.

**Note:** The supported browsers are the current version and two major versions back of Firefox, Chrome, and Safari, plus Internet Explorer versions 10 and 11 and Microsoft Edge.

2. Enter `http://management_ip_addr` in the address field and press **Enter**. Replace `management_ip_addr` with 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 may 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 may appear (see [Configuring Authentication](#) on page 604).

3. If a welcome screen appears (see [Configuring a Banner Page](#) on page 583), read the message and then click the "Accept terms and conditions" bar at the bottom.
4. In the login screen, enter your Nutanix login credentials and press **Enter** or click the right arrow icon.

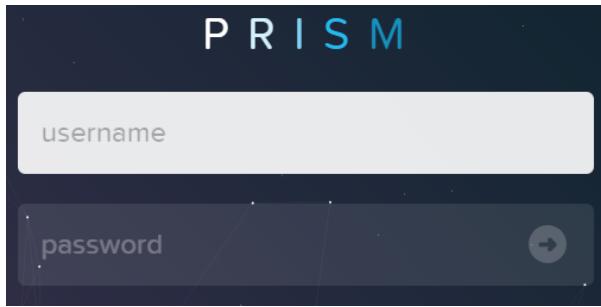


Figure: Login Screen

-  **Note:** If LDAP authentication is used, enter the user name in the *user@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](#) on page 604.)
-  **Note:** 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). To permanently disable (or enable) the animation, see [Modifying UI Settings](#) on page 44.

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.

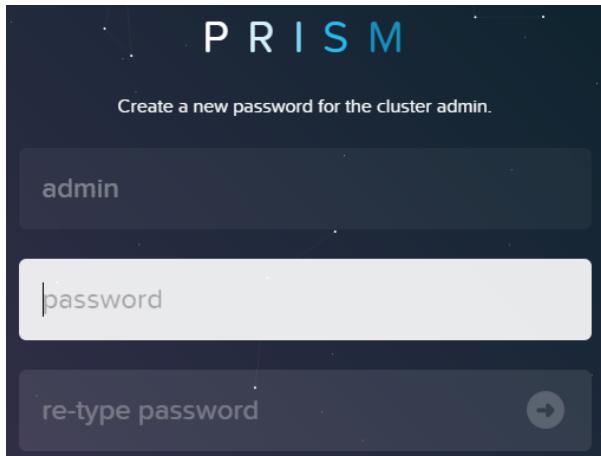


Figure: Login Screen (first admin login)

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
- At least 4 characters difference from the old password
- Should not be among the last 10 passwords

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

**Note:**

- After you upgrade to AOS 5.1 from an AOS earlier version and then attempt to log in to the Prism web console as the admin user, you are prompted to create a new admin user password.
- When you make an attempt to log in to the Prism web console for the first time after the upgrade, you can use your existing **admin** user password to log in and then change the existing password (you are prompted) to adhere to the password complexity requirements. However, if you are logging in to the Controller VM with SSH for the first time after the upgrade as the **admin** user, you must use the default admin user password (Nutanix/4u) and then change the default password (you are prompted) to adhere to the password complexity requirements.
- 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. The *Prism Web Console Guide* describes authentication and roles.

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. Check the "I have read and agree to the terms ..." box.
  - d. Click the **Accept** button.

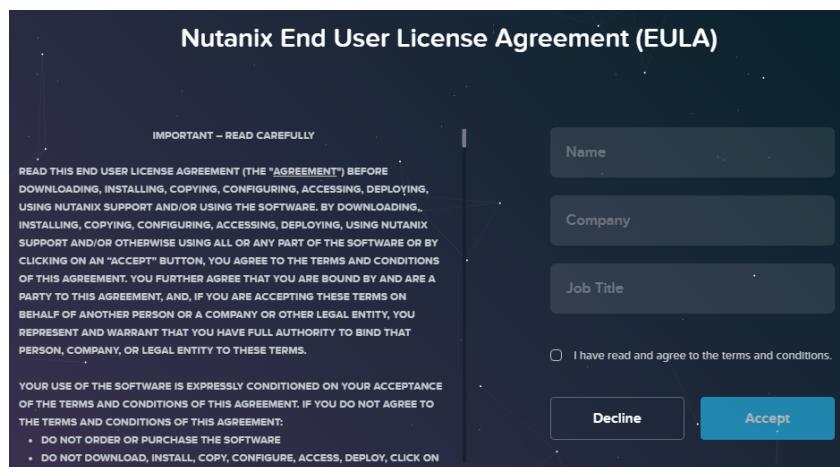


Figure: EULA Screen

7. If a "Pulse is Not Enabled" screen appears (typically on the first login or after an upgrade), which refers to the Pulse feature that alerts Nutanix customer support regarding the health of the cluster (see *Pulse Access Requirements* on page 636), read the statement and then do one of the following:
  - Click the **Enable & Continue** button to enable the Pulse feature (recommended).
  - Click the **No Thanks** button to keep the Pulse feature disabled.



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

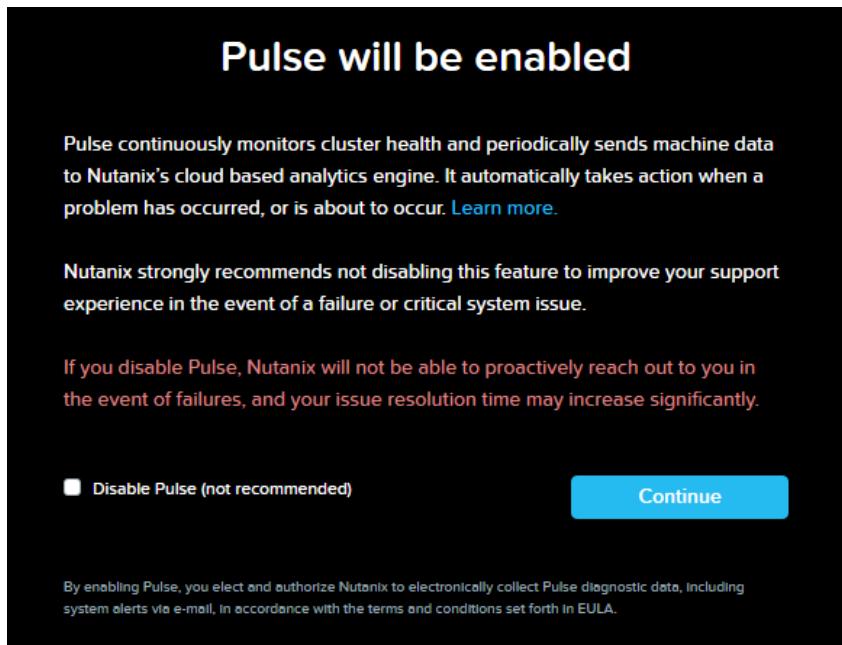


Figure: Pulse Screen

## Logging Out of the Web Console

To log out from the web console, click the user icon  in the main menu and then select the **Sign Out** option from the pull-down list. You are logged out immediately after selecting the option (no prompt or message).

## Main Menu Options

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

### Cluster Information

The cluster name appears on the far left of the main menu bar. Clicking the cluster name opens the *Cluster Details* window. This window displays the cluster ID number, cluster name, and cluster virtual IP address (if set). You can modify the name or virtual IP address at any time (see *Modifying Cluster Details* on page 42).

### View Options

Selecting a view (entity name) from the pull-down list 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 344).
- **VM.** Displays a virtual machine information dashboard (see *VM Dashboard*).
- **Storage.** Displays a storage information dashboard (see *Storage Dashboard* on page 119).
- **Network.** (AHV only) Displays the network visualiser.
- **Hardware.** Displays a hardware information dashboard (see *Hardware Dashboard* on page 166).

- **File Server.** Displays a file server dashboard see *Acropolis File Services 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 401).
- **Alerts.** Displays a screen of alert and events messages (see *Alerts Dashboard*).
- **Tasks.** Displays a screen of task messages (see *Task Status* on page 567).
- **Self Service.** (AHV only) Displays the initial configuration screen of the Acropolis self-service portal (SSP).



Figure: Main Menu with Expanded View List

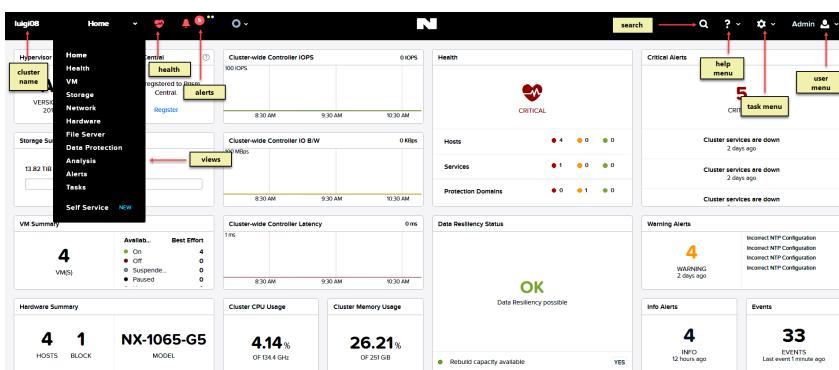


Figure: Main Menu with Expanded View List (AHV)

## Informational and Search Features

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

- **Health status.** A health icon appears on the left 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 (see *Health Dashboard* on page 344).
- **Alerts summary.** An alerts icon appears on the left of the main menu when critical (red), warning (yellow), or informational (gray) alert messages have been generated and have not been marked as resolved. An additional icon appears when events are running. The number of critical warnings (or running events) is displayed in the icon. Click the icon to display a drop-down list of the most recent unresolved alerts (or running events). Click a message or the right arrow link to open the alerts view (see *Alerts Dashboard*).
- **Online help.** You can access online help by clicking the **Help** option from the User Options list (see *Accessing Online Help* on page 645).
- **Search box.** A 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.

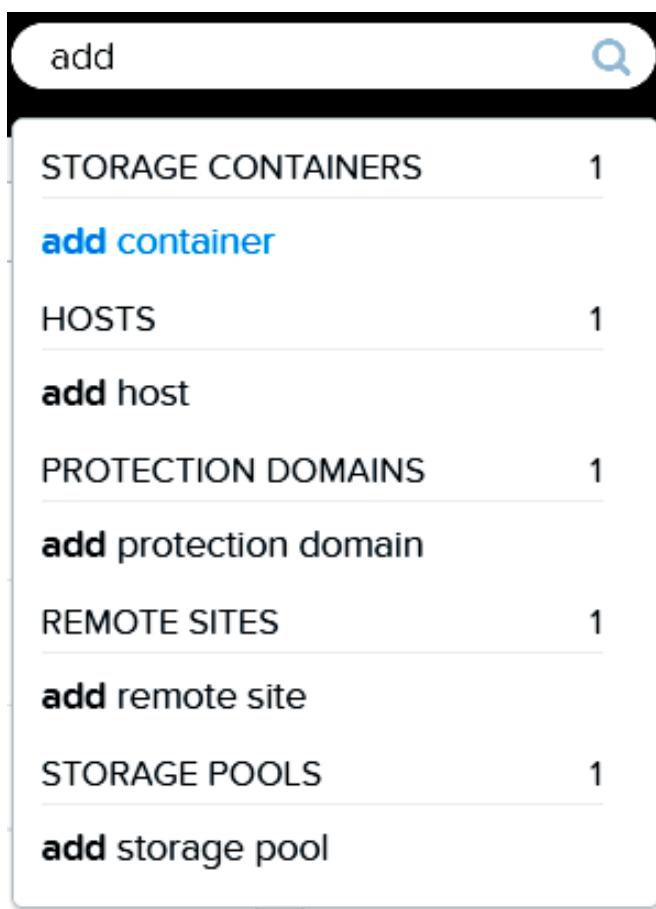


Figure: Search Box Example

## 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 pull-down list.

## User Menu List

Name	Description
Help with this page	Opens the online help at the page that describes this screen (see <a href="#">Accessing Online Help</a> on page 645).
Health Tutorial	Opens the Health dashboard tutorial that takes you through a guided tour of the health analysis features (see <a href="#">Health Dashboard</a> on page 344).
General Help	Opens the online help at the introduction page.
Support Portal	Opens a new browser tab (or window) at the Nutanix support portal login page (see <a href="#">Accessing the Nutanix Support Portal</a> on page 639).

Name	Description
Nutanix Next Community	Opens a new browser tab (or window) at the Nutanix Next Community entry page (see <a href="#">Accessing the Nutanix Next Community</a> on page 647). This is an online community site for customers and partners to exchange ideas, tips, and information about Nutanix technologies and related datacenter topics.

## Task Menu

A gear icon  appears on the right side of the main menu. Clicking the gear icon displays a list of tasks you can perform. The following table describes each option in the pull-down list.

### Task Menu List

Name	Description
Cluster Details	Opens the <b>Cluster Details</b> window to view or modify certain cluster parameters (see <a href="#">Modifying Cluster Details</a> on page 42).
Create Storage Container	Opens the <b>Create Storage Container</b> window to create a new storage container (see <a href="#">Creating a Storage Container</a> on page 139).
Expand Cluster	Opens the <b>Expand Cluster</b> window to add new nodes to the cluster (see <a href="#">Expanding a Cluster</a> on page 186).
Convert Cluster	Opens the <b>Convert Cluster</b> windows to convert the cluster from ESXi to AHV and then from AHV to ESXi.
Life Cycle Management	Opens the <b>Life Cycle Management</b> window to use the life cycle manager (LCM) to track software and firmware versions of all entities in the cluster.
Upgrade Software	Opens the <b>Upgrade Software</b> window to upgrade the cluster to a newer AOS version, update disk firmware, and other upgradeable components (see <a href="#">Software and Firmware Upgrades</a> on page 74).
Authentication	Opens the <b>Authentication Configuration</b> window to configure authentication for the cluster (see <a href="#">Configuring Authentication</a> on page 604).
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 (see <a href="#">Configuring Data-at-Rest Encryption</a> on page 619). This menu option appears only when the data drives in the cluster are SEDs.
SSL Certificate	Opens the <b>SSL Certificates</b> window to create a self-signed certificate (see <a href="#">Installing an SSL Certificate</a> on page 612).
Role Mapping	Opens the <b>Role Mapping</b> window to configure role mappings that apply in the user authentication process (see <a href="#">Assigning Role Permissions</a> on page 610).
User Management	Opens the <b>User Management</b> window. This window lists current users and allows you to add, (see <a href="#">Creating a User Account</a> on page 626), update (see <a href="#">Updating a User Account</a> on page 628), and delete (see <a href="#">Deleting a User Account</a> on page 632) user accounts.

Name	Description
Alert Email Configuration	Opens the <b>Alert Email Configuration</b> window, which enables (or disables) the e-mailing of alerts (see <a href="#">Configuring Alert Emails</a> on page 414).
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 (see <a href="#">Configuring Alert Policies</a> on page 416).
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 (see <a href="#">Controlling Cluster Access</a> on page 615). Removing all public keys locks down the cluster from external access.
HTTP Proxy	Opens the <b>HTTP Proxy</b> window to configure an HTTP proxy to which the Nutanix software can connect (see <a href="#">Configuring HTTP Proxy</a> on page 637).
Language Settings	Opens the <b>Languages</b> window, which allows you to select the language of the web console.
Licensing	Opens the <b>Licensing</b> window to install or update the cluster license that enables entitled Nutanix features (see <a href="#">License Management</a> on page 46).
Filesystem Whitelists	Opens the <b>Filesystem Whitelist</b> window to specify whitelist addresses (see <a href="#">Configuring a Filesystem Whitelist</a> on page 569).
Image Configuration [AHV only]	Opens the <b>Image Configuration</b> window to import and manage image files that can be used to create VMs (see <a href="#">Configuring Images</a> on page 382). This menu option appears in Acropolis managed clusters only.
MA Witness Registration [ESXi only]	Opens the <b>Metro Availability Witness Registration</b> window to add the Metro Availability Witness connection details (see <a href="#">Metro Availability Witness Option</a> on page 283). This menu option appears in ESXi clusters only.
Prism Central Registration	Opens the <b>Prism Central Registration</b> window to add the cluster into a central registration for multicluster connection and support (see <a href="#">Register (Unregister) with Prism Central</a> on page 105).
Pulse	Opens the <b>Pulse</b> window to enable the sending of cluster information to Nutanix customer support for analysis (see <a href="#">Configuring Pulse</a> on page 634).
Redundancy State	Opens the <b>Redundancy Factor Readiness</b> window to configure the redundancy factor readiness of the cluster.
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 (see <a href="#">Enabling High Availability for the Cluster</a> on page 389). This menu option appears in Acropolis managed clusters only.
Name Servers	Opens the <b>Name Servers</b> window to configure name servers for the cluster (see <a href="#">Configuring Name Servers</a> on page 570).
Network Configuration [AHV only]	Opens the <b>Network Configuration</b> window to configure network connections for the cluster (see <a href="#">Configuring Network Connections</a> on page 151). This menu option appears in Acropolis managed clusters only.

Name	Description
NTP Servers	Opens the <b>NTP Servers</b> window to specify which NTP servers to access (see <a href="#">Configuring NTP Servers</a> on page 572).
Network Switch	Opens the <b>Network Switch Configuration</b> window to configure network switch information needed for collecting network traffic statistics (see <a href="#">Configuring Network Switch Information</a> on page 155). This option does not appear when running a hypervisor that does not support this feature.
Remote Support	Opens the <b>Remote Support Services</b> window, which enables (or disables) Nutanix remote support access (see <a href="#">Controlling Remote Connections</a> on page 636).
SMTP Server	Opens the <b>SMTP Server Settings</b> window to configure an SMTP server (see <a href="#">Configuring an SMTP Server</a> on page 573).
SNMP	Opens the <b>SNMP Configuration</b> window to enable and configure SNMP for the cluster (see <a href="#">Configuring SNMP</a> on page 574).
vCenter Registration [ESXi only]	Opens the <b>vCenter Registration</b> window to register (or unregister) the cluster with the vCenter instance. This menu option appears in ESXi clusters only.
Welcome Banner	Opens the <b>Edit Welcome Banner</b> window to create a welcome banner message that appears before users login to the web console (see <a href="#">Configuring a Banner Page</a> on page 583).
UI Settings	Opens the <b>UI Settings</b> window to disable (or re-enable) the login screen (see <a href="#">Modifying UI Settings</a> on page 44).

## User Menu

A user icon  appears on the far right side of the main menu with the current user login name (for example `admin `). Clicking the user icon displays a list of options to update your user account, log out from the web console, and other miscellaneous tasks. The following table describes each option in the pull-down list.

## User Menu List

Name	Description
Update Profile	Opens the <b>Update Profile</b> window to update your user name and email address (see <a href="#">Updating My Account</a> on page 630).
Change Password	Opens the <b>Change Password</b> window to update your password (see <a href="#">Updating My Account</a> on page 630).
REST API Explorer	Opens a new browser tab (or window) at the Nutanix REST API Explorer web page (see <a href="#">Accessing the REST API Explorer</a> on page 642).
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 (no additional prompts). See the Nutanix <i>Command Reference</i> for information about installing the nCLI locally and for nCLI command descriptions.

Name	Description
Download Cmdlets Installer	Downloads the PowerShell installer for the Nutanix cmdlets. See the <i>Nutanix Command Reference</i> for information about installing the cmdlets locally and for cmdlet descriptions.
Download Prism Central	Opens a new browser tab (or window) at the <i>Support Tools</i> 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. See the <i>Prism Central Guide</i> for more information.
About Nutanix	Opens a window that displays Nutanix operating system (AOS) and other version information (see <a href="#">Checking Version</a> on page 45).
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 web console (see <a href="#">Logging Out of the Web Console</a> on page 32).

## Home Dashboard

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

### Menu Options

The Home dashboard does not include menu options other than those available from the main menu (see [Main Menu Options](#) on page 32).

### Home Screen Details

The Home dashboard displays 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 figure is a sample dashboard, and 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.

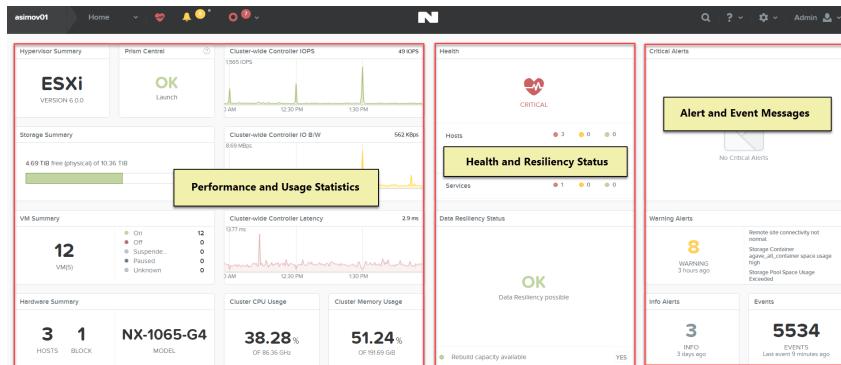


Figure: Home Dashboard



**Note:** See [Understanding Displayed Statistics](#) on page 41 for information about how the statistics are derived.

### Home Screen Fields

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 <b>OK</b> to launch the Prism Central instance in a new tab of your browser.
Storage Summary	Displays the total, used, and unused storage space in the cluster.
VM Summary	Displays the total number of VMs in the cluster broken down by on, off, and suspended states.
Hardware Summary	Displays the number of hosts and blocks in the cluster, plus one or more Nutanix block model numbers.
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. (These display features also apply to the I/O bandwidth and I/O latency monitors.) 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 link in the upper right of the chart (see <a href="#">Analysis Dashboard</a> on page 401).
Cluster-wide Controller IO Bandwidth	Displays I/O bandwidth used per second in the cluster. The value is displayed in an appropriate metric (Mbps, Kbps, and so on) depending on traffic volume.
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 GHz).
Cluster Memory Usage	Displays the current memory utilization percentage along with the total available capacity (in GB).
Health	Displays health status for the cluster as a whole (good, warning, critical) and summary health status for the VMs, hosts, and disks in the cluster. Clicking on the VMs, hosts, or disks line displays detailed information about that object in the Health page (see <a href="#">Health Dashboard</a> on page 344).

Name	Description
Data Resiliency Status	<p>Displays information indicating whether the cluster is protected currently from potential data loss due to a component failure. Click anywhere in this field to display a dialog box. <i>Data Resiliency Status</i> window with more information (see the following "Data Resiliency Status" section).</p> <ul style="list-style-type: none"> <li>• <b>Resiliency Status.</b> Indicates whether the cluster can safely handle a node failure, that is whether a copy exists somewhere in the cluster of all data in any node. If the status is not OK, the <i>Data Resiliency Status</i> window includes a message about the problem.</li> </ul> <p> <b>Note:</b> The resiliency status for single-node backup cluster is at the disk level and not at the node level. For more information, see <a href="#">Single-Node Replication Target Clusters</a> on page 340.</p> <ul style="list-style-type: none"> <li>• <b>Rebuild Capacity Available.</b> Indicates whether there is sufficient unused storage in the cluster to rebuild a data copy after a node is lost. If the status is not Yes, the <i>Data Resiliency Status</i> window includes a message about the problem.</li> </ul> <p> <b>Note:</b> This option does not appear for single-node replication target clusters.</p>
Critical Alerts	Displays the most recent unresolved critical alert messages. Click a message to open the Alert screen at that message (see <a href="#">Alerts Dashboard</a> ).
Warning Alerts	Displays the most recent unresolved warning alert messages. Click a message to open the Alert screen at that message.
Info Alerts	Displays a summary of informational alerts.
Events	Displays a summary of events.

## Data Resiliency Status

The *Data Resiliency Status* window displays more detailed cluster resiliency status information. (Click the **OK** button at the bottom or **X** icon at the top to close the window.) This window provides information about the number and type of failures the cluster can withstand safely. The following figure is an example. 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, as in this example where there are not enough blocks in the cluster to support a block failure.

 **Note:** When a node goes down, extent group (egroup) fault tolerance status remains unchanged as the node is assumed (initially) to be unavailable just temporarily. However, Stargate (see [Cluster Components](#) on page 12) 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.

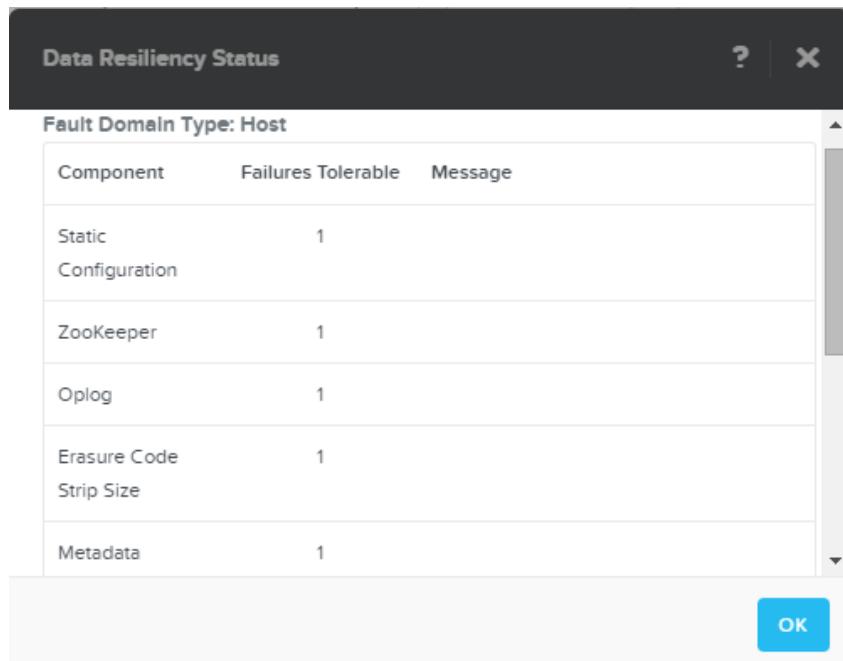


Figure: Data Resiliency Status Window

#### Fault Domain Type: Block

Component	Failures Tolerable	Message
Static Configuration	0	Not enough rackable units (blocks) in the cluster

## Understanding Displayed Statistics

A variety of statistics are displayed in the web console and *Prism Central* screens. There are three possible sources for a statistic:



**Note:** Most displayed statistics are shown 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*.)

1. Hypervisor. When the hypervisor can provide usage statistics, those figures are displayed where appropriate. ESXi provides such statistics, but Hyper-V and AHV do not. Getting the statistics from ESXi means numbers displayed in the web console should match the corresponding ones in vCenter.
2. Controller (Stargate). When hypervisor statistics are unavailable or inappropriate, the Controller VM provides statistics from Stargate. 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/Os before issuing them to the NFS server, thus increasing the number of operations reported by the controller.
  - The hypervisor might read I/Os from the cache in the hypervisor, which are not counted by the controller.

- Disk (Stargate). Stargate can provide statistics from both the controller and disk perspective. The difference is that the controller perspective includes read I/Os from memory as well as disk I/Os, while the disk perspective includes just the disk I/Os.



**Note:** The distinction between hypervisor, controller, and disk statistics applies only to storage-related statistics such as IOPS, latency, and bandwidth.

Field labels in the web console screens help identify the information source:

- A field name that does not include either "Controller" or "Disk" indicates that statistic is derived from the hypervisor (for example "IOPS").
- A field name that includes the word "Controller" indicates that statistic is derived from the controller (for example "Controller IOPS").
- A field name that includes the word "Disk" indicates that statistic is derived from the disk (for example "Disk IOPS").

The following table identifies the information source for various statistics. Overview, VM, and storage statistics come from either the hypervisor or controller. In the case of VM statistics in a mixed ESXi/AHV cluster, the source depends on the hypervisor hosting that VM (hypervisor for ESXi-based VMs and controller for AHV-based VMs). Hardware statistics come from the disk. Metrics in the analysis page can come from any of the sources (hypervisor, controller, or disk) depending on the type of metric.

#### Source for Displayed Statistics

Hypervisor Type	Overview, VM, and Storage	Hardware	Analysis
ESXi	hypervisor (controller for some storage stats)	disk	metric dependent
Hyper-V	controller	disk	metric dependent
AHV	controller	disk	metric dependent
XenServer	controller	disk	metric dependent
Mixed (ESXi + AHV)	hypervisor	disk	metric dependent
Prism Central	cluster dependent (hypervisor or controller)	disk	metric dependent

#### Modifying Cluster Details

You can add a cluster name or virtual facing IP address at any time. To create or modify either value, do the following:

- In the main menu, either click the cluster name at the far left or select **Cluster Details** from the gear



pull-down list on the right (see [Main Menu Options](#) on page 32).

The *Cluster Details* window appears. It displays the cluster UUID (universally unique identifier), ID, and incarnation ID values, and the cluster name and virtual IP address if configured. 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.

**Cluster Details**

CLUSTER UUID  
00054943-2419-e38e-0000-000000009102

CLUSTER ID  
00054943-2419-e38e-0000-000000009102::37122

CLUSTER INCARNATION ID  
1487927600866190

CLUSTER NAME

CLUSTER VIRTUAL IP ADDRESS

ISCSI DATA SERVICES IP

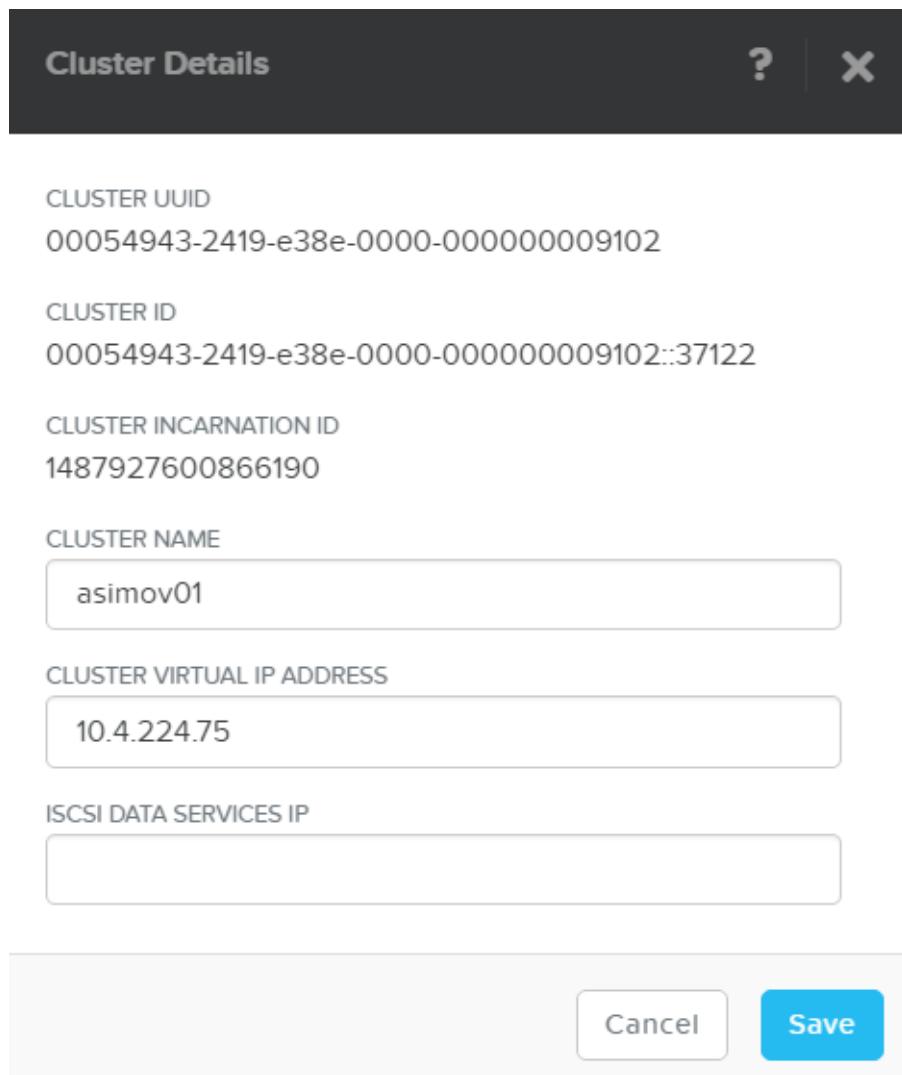


Figure: Cluster Details Window

2. Enter (or update) a name for the cluster in the **Cluster Name** field.

The default name is simply Unnamed. Providing a custom name is optional but recommended.

3. Enter (or update) an IP address for the cluster in the **Cluster Virtual IP Address** field.

A Controller VM runs on each node and has its own IP address, but this field sets a logical IP address that always connects to one of the active Controller VM in the cluster (assuming at least one is active), which removes the need to enter the address of a specific Controller VM. The virtual IP address is normally set during the initial cluster configuration (see the *Field Installation Guide*), but you can update the address at any time through this field. Providing an virtual IP address is optional but recommended.

 **Note:** All the features that use virtual IP address of the cluster will be impacted if you change the virtual IP address of the cluster. See [Impact of Changing Virtual IP Address of the Cluster](#) on page 44 for more information.

4. Enter (or update) an IP address for use with Acropolis Block Services in the **ISCSI Data Services IP Address** field.

 **Note:** For more information, see [About The ISCSI Data Services IP Address](#) on page 44.

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

#### Impact of Changing Virtual IP Address of the Cluster

All the Nutanix features that use virtual IP address will be affected if you change the virtual IP address of the cluster.

- Hyper-V, you cannot manage the Nutanix cluster by using SCVMM.
- Data Protection, Nutanix data protection service will be affected if you have configured the remote site by using virtual IP address of the remote cluster.
- Nutanix guest tools, all the VMs that are running the NGT instance will be affected.
- External machines mounting shares from Nutanix might fail as it recommended to use virtual IP address for HA functionality.

#### About The iSCSI Data Services IP Address



**Note:** Nutanix recommends setting the iSCSI data services IP address once for each cluster, but you can change it if needed through *Cluster Details* in the Prism web console. If you change the iSCSI data services IP address, you will need to reconfigure any clients to use the new IP address.

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

To provide access to the block storage, ABS utilizes an *iSCSI data services IP address* to clients for target discovery which simplifies external iSCSI configuration on clients. This iSCSI data services IP address acts as an iSCSI target discovery portal and initial connection point.

This IP address is also used as a cluster-wide address for use by clients configured as part of Acropolis File Services.

This IP address:

- Should 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)

#### Modifying UI Settings

By default, the login page includes background animation, and users are logged out automatically after being idle for 15 minutes. You can disable the background animation, change the session timeout for users, and configure to override the session timeout.

- In the main menu, select **UI Settings** from the gear icon pull-down list on the right (see [Main Menu Options](#) on page 32).  
The *UI Settings* window appears.

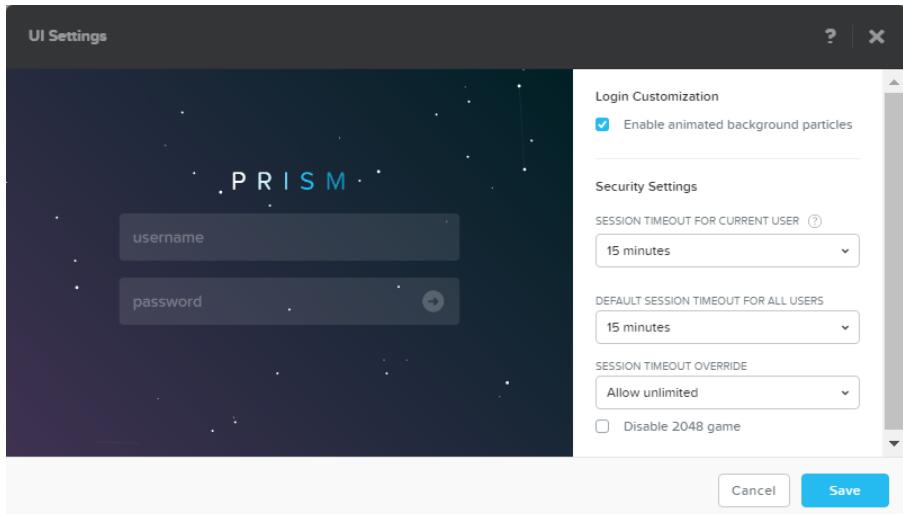


Figure: UI Settings Window

2. To disable the login page background animation, under **Login Customization**, clear the **Enable animated background particles** option (or select it to enable).
3. 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 the users from the **DEFAULT SESSION TIMEOUT FOR ALL USERS** drop-down list.
  - Select the appropriate option from the **SESSION TIMEOUT OVERRIDE** drop-down list to override the session timeout.



**Note:** The timeout interval for an administrator cannot be set for longer than 30 minutes.

4. Clear the **Disable 2048 game** option to disable the 2048 game.
5. Click **Save** to save your changes and close the window.

## Checking Version

1. To view the Nutanix version running in the cluster, click the user icon in the main menu and then select the **About Nutanix** option from the pull-down list.  
An *About Nutanix* window appears that includes the AOS and Nutanix cluster check (NCC) version numbers. It also includes a link to Nutanix patent information.



Figure: About Nutanix Window

2. Click the **OK** button to close the window.

## License Management

See also [Before You License Your Cluster](#) on page 46.

The Portal Connection feature simplifies license management by integrating the licensing workflow into a single interface in the Prism web console. Once you enable this feature, you can perform most licensing tasks from Prism without needing to explicitly log on to the Nutanix Support Portal. It is disabled by default. To use it, see [Configuring Portal Connection for License Management](#) on page 49 and [Managing Licenses with Portal Connection](#) on page 55.

If you do not want to enable this feature, you can manage licenses as described in [Managing Licenses without Portal Connection \(Default\)](#) on page 61.

### Before You License Your Cluster

Requirements and considerations for licensing.



**Note:** Generating a cluster summary file through the Prism web console, nCLI commands (`license generate-cluster-info`), or PowerShell commands (`Get-NTNXClusterLicenseInfo` and `Get-NTNXClusterLicenseInfoFile`) initiates the cluster licensing process. You might observe a Licensing Status: In Process alert message in the web console or log files in this case. [ENG-60722]

Consider the following before you attempt to manage your licenses.

- Before attempting to install a license, ensure that you have created a cluster and logged into the web console at least once. You must install a license after creating a cluster for which you purchased Pro or Ultimate licenses.
- Before destroying a cluster, you must reclaim your licenses. You do not need to reclaim Starter licenses in this case. These licenses are automatically applied whenever you create a cluster. See [Reclaiming Licenses \(Portal Connection\)](#) on page 59 or [Reclaiming Licenses](#) on page 70.
- If a cluster includes nodes with different license types, the cluster and each node in the cluster defaults to the minimum feature set enabled by the lowest license type. For example, if two nodes in the cluster have Ultimate licenses and two nodes in the same cluster have Pro licenses, all nodes effectively have Pro licenses and access to that feature set only. Attempts to access Ultimate features in this case result in a warning in the web console.

## AOS Licenses

AOS includes a variety of features to enable you to administer your environment based on your current and future needs. You can use the default feature set of AOS, upgrade to a richer feature set, update your license for a longer term, or reassign existing licenses to nodes or clusters as needed.

### **Starter License**

Each Nutanix node and block is delivered with a default Starter license, which does not expire. You are not required to register this license on the Nutanix Customer Portal account assigned to you when you purchased your nodes. These licenses are automatically applied whenever you create a cluster, including after you have destroyed a cluster. You do not need to reclaim Starter licenses in this case.

### **Pro and Ultimate Licenses**

The Pro and Ultimate license types require you to download a license file from the Customer Support Portal and install it on your cluster. When you upgrade to a Pro or Ultimate license or add nodes or clusters to your environment with these licensed features, you must generate the license file, download it, and install it.

### **Prism Central/Prism Pro**

AOS 4.6 introduced the Pro license for Prism Central. The Prism Pro license adds additional capabilities to Prism Central, including most of the features available through the Prism web console of an individual cluster (also known as Prism Element).

### **Add-Ons**

Individual features known as add-ons can be added to your existing license feature set. When Nutanix makes add-ons available, you can add them to your existing Starter or Pro license. For example, Acropolis File Services is an add-on.

See [Add-On Licenses](#) on page 48.

### **Viewing License Status**

The most current information about your licenses is available from the Prism web console. It is also available at the Nutanix Support Portal from the **My Products** link. You can view information about license types, expiration dates, and any free license inventory (that is, unassigned available licenses). See [Displaying License Features and Details](#) on page 72.

## Prism Pro License

The Prism Pro license for Prism Central adds additional capabilities to Prism Central, including custom dashboards, capacity planning, and advanced search capabilities. Each new installation of Prism Central includes a 60-day trial, which you can disable if desired (as described in the *Prism Central Guide*).

Each node registered to and managed by Prism Pro requires the application of a Prism Pro license through the Prism Central web console. For example, if you have registered and are managing 10 Nutanix nodes (regardless of the individual node or cluster license level), you need to apply 10 Prism Pro licenses through the Prism Central web console.

The workflow for applying a Prism Pro license in Prism Central is identical to the workflow for applying a license in a cluster's. For example, the workflow for applying a license to an unlicensed Prism Central instance is the same as the workflow for licensing a node (without using Portal Connection):

1. Purchase a Prism Pro license for each node managed by Prism Central.
2. Generate a cluster summary file from the Prism Central web console.
3. Upload the cluster summary file to the Nutanix Support Portal, then generate and download a license file.
4. Apply the license file to Prism Central through its web console.

Licensing dialog boxes and wizards subsequently show the license class is `prism_central` and the license type is *Prism Pro*.

## Add-On Licenses

See [Installing a New Add-On License](#) on page 65.

Individual features known as add-ons can be added to your existing license feature set. When Nutanix makes add-ons available, you can add them to your existing Starter or Pro license.

For example, you can purchase the Acropolis File Services add-on for your existing Pro licenses. You will need to purchase and apply one add-on license for each node in the cluster with a Pro license.

For example, if your current Pro-licensed cluster consists of four nodes, you need to purchase four add-on licenses, then apply them to your cluster. All nodes in your cluster need to be at the same license level (four Pro licenses and four add-on licenses). You cannot buy one add-on license, apply it to one node, and have three nodes without add-on licenses.

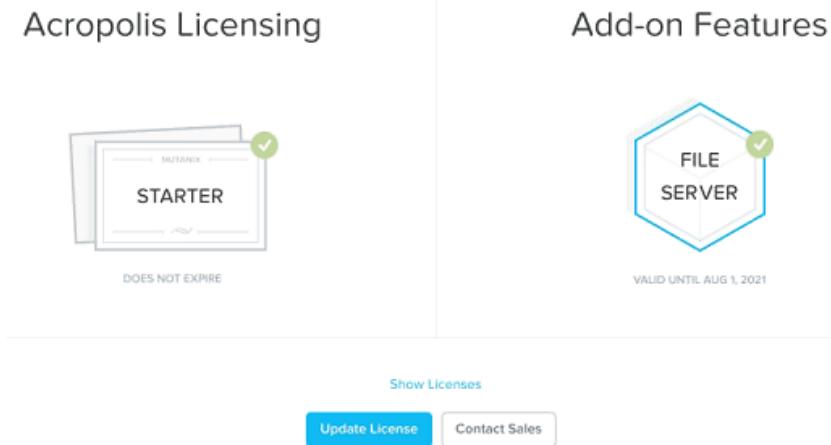


Figure: License Add-on Status

## Configuring Portal Connection for License Management

Simplifies licensing by integrating the licensing workflow into a single interface in the Prism web console. This feature is disabled by default.



**Note:** Your network must allow outbound traffic to portal.nutanix.com:443 to use this feature.

The Portal Connection feature simplifies licensing by integrating the licensing workflow into a single interface in the Prism web console. Once you configure this feature, you can perform most licensing tasks from Prism without needing to explicitly log on to the Nutanix Support Portal.

Portal Connection communicates with the Nutanix Support Portal to detect any changes or updates to your cluster license status. When you open **Licensing** from the Prism web console, the screen displays 1-click action buttons to enable you to manage your licenses without leaving the web console.

Portal Connection requires you to first create and then register an API key to secure communications between the Support Portal and the Prism web console.

- A Portal Connection API key is initially bound to the user that creates the key on the Support Portal. All subsequent licensing operations are done on behalf of the user who created the key and any operations written to an audit log will include information identifying this user. That is, licensing task X was performed by user Y (assuming user Y created the key).
- The Portal Connection API key is also bound to the Prism user that logs in to the web console and then registers the key. For example, if user `admin` registers the key, any licensing task performed by `admin` is performed on behalf of user Y (who created the key on the Support Portal). A Prism user (such as `admin`) must have access to the API key to use this feature. You can use Role Mapping and/or LDAP to manage key access or provide an audit trail if more than one `admin` user is going to manage licensing.
- You can create and register one or more keys per cluster. For example, create and register one key per user that will be administering licensing.

### Creating and Registering the Portal Connection API Key

Create the Portal Connection API key on the Nutanix Support Portal, then register it through the Prism web console. You might need to turn off any pop-up blockers in your browser to display dialog boxes.

1. Log on to the Nutanix Support Portal, select **API Keys** from your profile, then click **New API Key**.

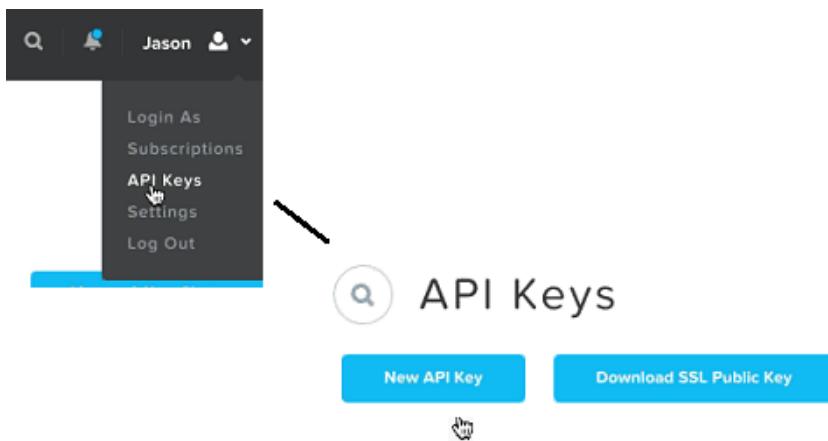


Figure: Generating API Keys in the Support Portal

2. Generate the key in the **Create New API Key** dialog box.

- a. Enter an alias (name) for the key to help you identify or keep track of the key on the portal, then click **Generate**.

- b. Copy the new key, then click **X** to close the dialog box.

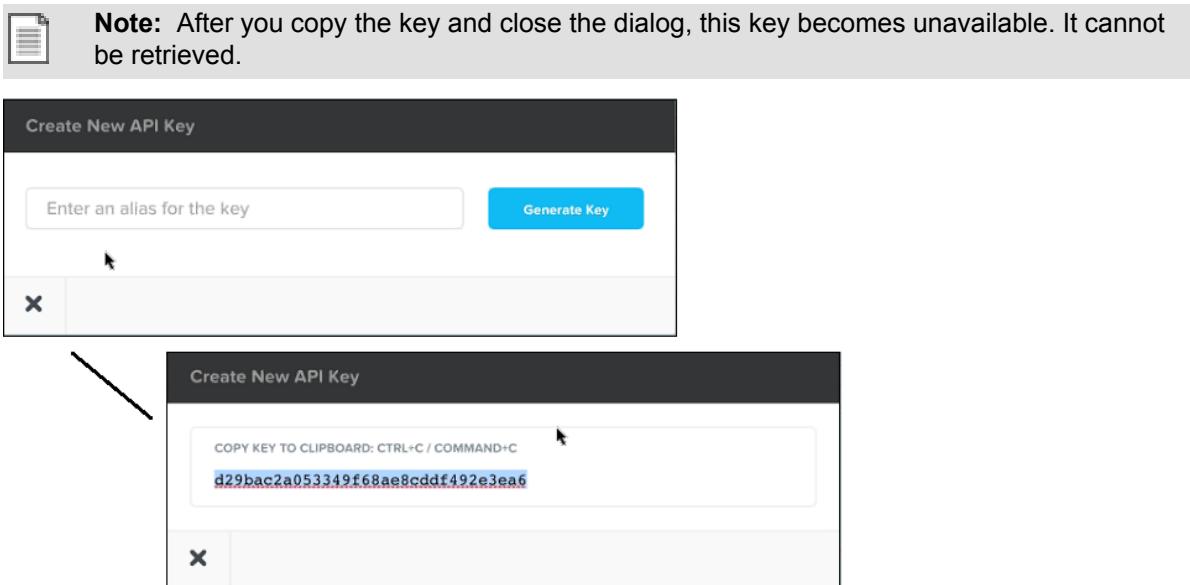


Figure: Entering an API Key Alias Name

- c. Optionally, click **Download SSL Public Key** for use when you register the API key in the web console.
3. Register the API key through the Prism web console.
- Log on to the Prism web console and open **Licensing** from the gear icon.
  - Click **Enable It** at the top banner in the licensing screen.
  - Paste the API key in the **API KEY** field in the **Portal Connection** dialog box. Optionally, paste the downloaded public key in the **PUBLIC KEY** field.
  - Click **Save**.



Figure: Registering the API Key in the Prism Web Console

The Portal connection has been created and Fetching licensing data messages are displayed. You can also register the API key by updating your user profile by selecting your user profile icon, then clicking **Update Profile**.

**Update Profile**

Profile settings for admin.

**General**

FIRST NAME      LAST NAME

EMAIL ADDRESS

LANGUAGE

No Applicable Option

---

**Portal Connection**

API KEY

PUBLIC KEY      Optional

**Cancel**      **Save**

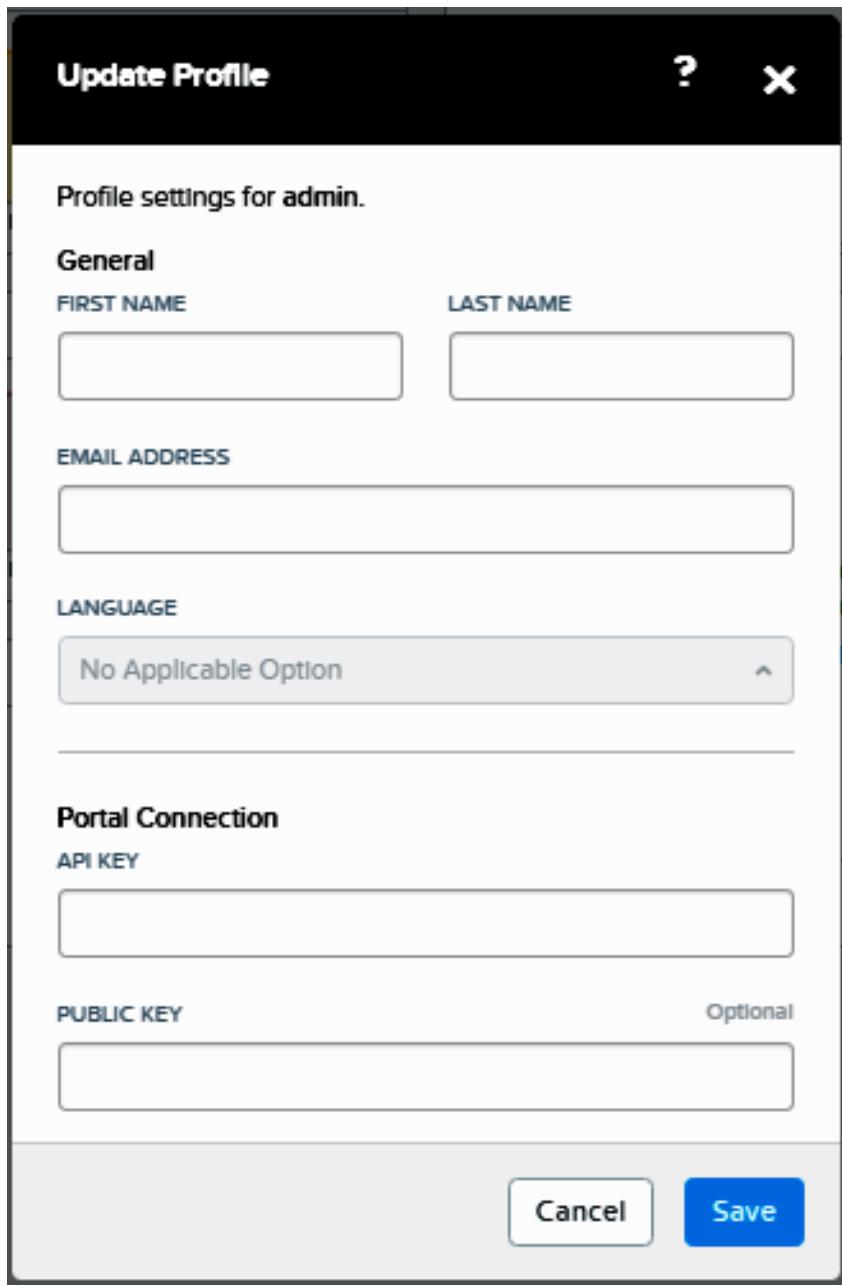


Figure: Register the API Key (Update Profile)

#### Disabling or Enabling the Portal Connection

Temporarily disable the Portal Connection through the Prism web console.

You might need to disable the Portal Connection or revoke the API key associated with it. If you disable the connection as described here, you can enable it again.

1. Log on to the Prism web console.
2. Click the user icon in the main menu, then select **Update Profile**.
3. Click **Disable** in the Portal Connection section. The status becomes disconnected.
4. Click **Save**.

5. To enable it again, open **Update Profile**, click **Enable**, then click **Save**.

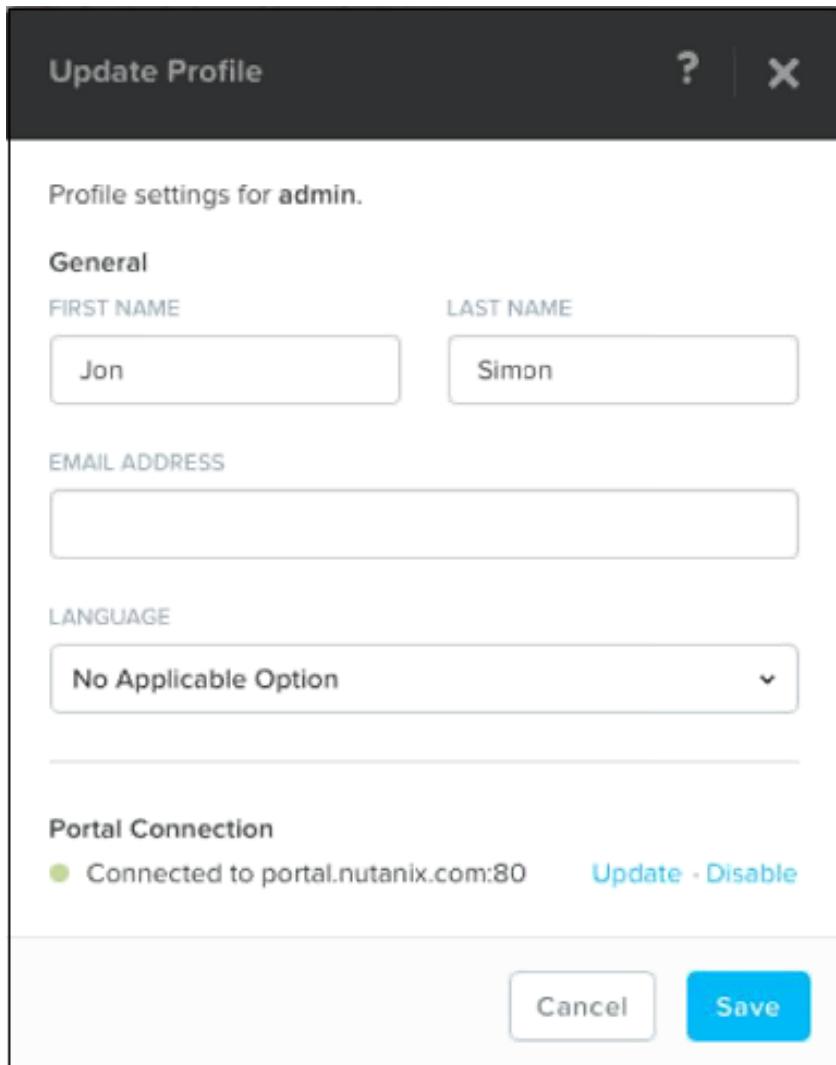


Figure: Enabled or Disable the Portal Connection

#### Revoking the Portal Connection

Revoke the API key on the Nutanix Support Portal, which disables the Portal Connection feature in the Prism web console.

You might need to revoke the API key associated with the Portal Connection. After revoking the key:

- You will need to create and register a new key to continue using the Portal Connection licensing feature.
- The connection between the Support Portal and the Prism web console is broken (disconnected).
- You might see a red connection state with a message of Error: Invalid API Key in the *Update Profile* dialog box.

1. Log in to the Nutanix Support Portal and select **API Keys** from your profile.  
The *API Keys* page is displayed.

API Keys					
				<a href="#">New API Key</a>	<a href="#">Download SSL Public Key</a>
				<input type="checkbox"/> Show Revoked	
ALIAS	CLUSTER	CREATED TIME	STATUS	ACTIONS	
js-pc	deddf2bc-44c9-41ee-b612-e47973e4ae31	9/21/2016 12:57 PM	active	<a href="#">Revoke</a>	
prost4	00053b54-d230-bc4d-0000-00000000807a	9/8/2016 9:04 PM	active	<a href="#">Revoke</a>	
annie2	00053be8-ac4f-5c5f-0000-000000008210	9/8/2016 8:59 PM	active	<a href="#">Revoke</a>	
johny5	00053aee-a9b1-0fb0-0000-0000000097fc	9/6/2016 10:59 AM	active	<a href="#">Revoke</a>	

Figure: API Keys Portal Page

2. Locate your key alias name, click **Revoke**, and then click the confirmation.

#### Updating the Portal Connection API Key

This procedure assumes you have already configured Portal Connection and have a working connection. You might need to update the Portal Connection API key associated with your profile. First get a new key and apply, then optionally revoke the existing key.

1. Log on to the Nutanix Support Portal, select **API Keys** from your profile, then click **New API Key**.

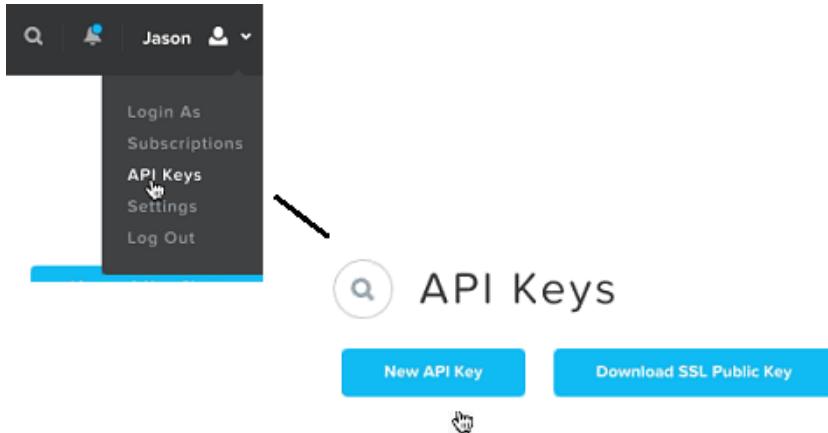


Figure: Generating API Keys in the Support Portal

2. Generate the key in the **Create New API Key** dialog box.

- a. Enter an alias (name) for the key to help you identify or keep track of the key on the portal, then click **Generate**.
- b. Copy the new key, then click **X** to close the dialog box.



**Note:** After you copy the key and close the dialog, this key becomes unavailable. It cannot be retrieved.

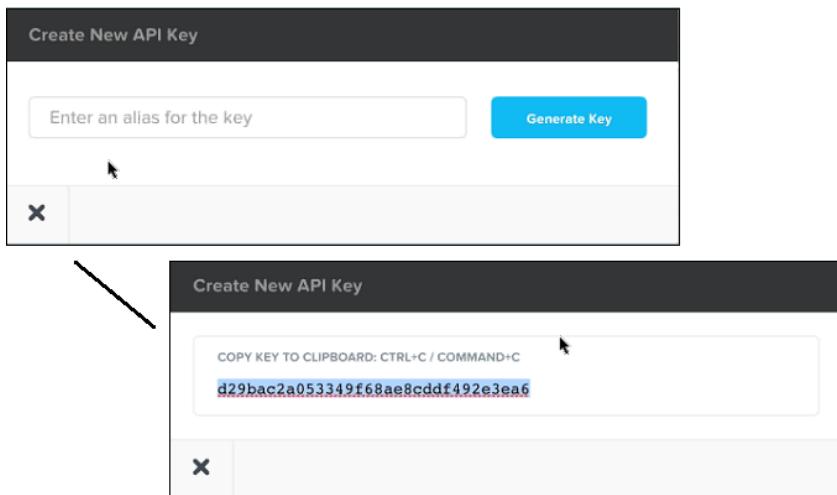


Figure: Entering an API Key Alias Name

- c. Optionally, click **Download SSL Public Key** for use when you register the API key in the web console.
3. Update the API key through the Prism web console.
  - a. Click the user icon in the main menu, then select **Update Profile**.
  - b. Click **Update** in the Portal Connection section.
  - c. Paste the API key in the **API KEY** field in the dialog box. Optionally, paste the downloaded public key in the **PUBLIC KEY** field.
  - d. Click **Save**.

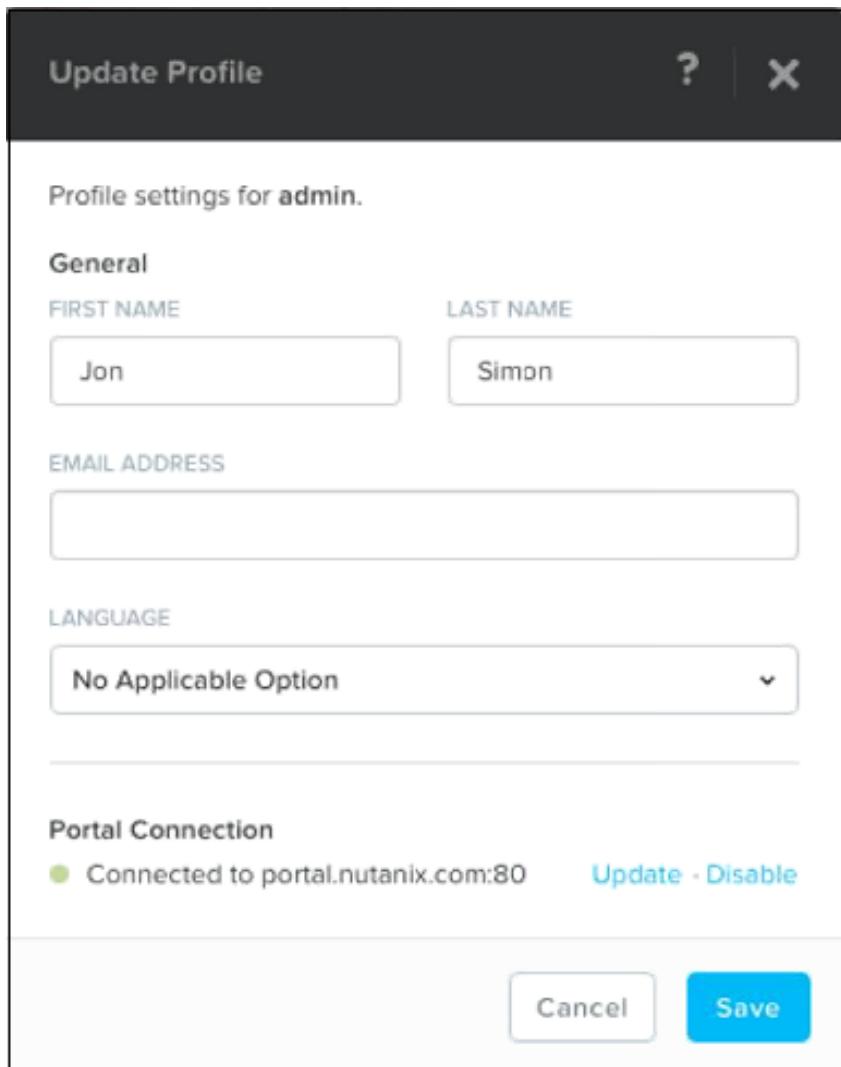


Figure: Update the API Key

4. Optionally, you can revoke other keys associated with the Portal Connection. See [Revoking the Portal Connection](#) on page 52.

## Managing Licenses with Portal Connection

Simplifies licensing by integrating the licensing workflow into a single interface in the Prism web console. This feature is disabled by default.



### Note:

- See [Configuring Portal Connection for License Management](#) on page 49.
- Your network must allow outbound traffic to portal.nutanix.com:443 to use this feature.

The Portal Connection feature simplifies licensing by integrating the licensing workflow into a single interface in the Prism web console. Once you configure this feature, you can perform most licensing tasks from Prism without needing to explicitly log on to the Nutanix Support Portal.

Portal Connection communicates with the Nutanix Support Portal to detect any changes or updates to your cluster license status. When you open **Licensing** from the Prism web console, the screen displays 1-click action buttons to enable you to manage your licenses without leaving the web console.

## 1-Click Licensing Action Buttons

When you open **Licensing** from the Prism web console, the screen displays 1-click action buttons to enable you to manage your licenses without leaving the web console.

Depending on your current licensing status and cluster configuration, you might see one or more of these 1-click action buttons.

## 1-Click Licensing Action Buttons

This Button Appears...	If You Are Eligible or Want To...
<b>Add</b>	Add an add-on license. This button appears if add-on features are available for licensing.
<b>Downgrade</b>	Downgrade your cluster to Pro from Ultimate or to Starter from Pro or Ultimate. Use this button when reclaiming licenses before destroying a cluster.
<b>Rebalance</b>	Ensure your available licenses are applied to each node in your cluster. For example: <ul style="list-style-type: none"><li>• If you have added a node and have an available license in your account, click <b>Rebalance</b>.</li><li>• If you have removed a node, click <b>Rebalance</b> to reclaim the now-unused license.</li></ul>
<b>Remove</b>	Remove an add-on license, disabling the add-on feature.
<b>Renew</b>	Applies newly-purchased licenses.
<b>Update</b>	Extends the expiration date of current valid licenses.
<b>Upgrade</b>	Upgrade your cluster from Starter to Pro or Ultimate, or Pro to Ultimate license types.

### Example: Upgrading Your Starter Cluster to Pro

In this example, Portal Connection is configured in this Starter-licensed cluster and the customer has purchased Pro licenses for a Starter-licensed cluster.

1. Open **Licensing** from the gear icon in the Prism web console for the connected cluster.

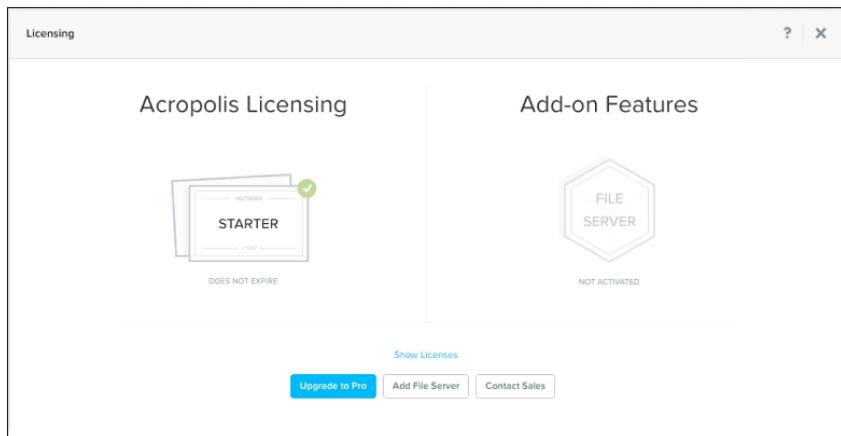


Figure: Portal Connection Upgrade Example

The Licensing window shows that you have Pro licenses available (that you have purchased and detected by Portal Connection) because the **Upgrade to Pro** button is highlighted. The Acropolis File Server add-on is not available as you have not purchased that add-on. You can click **Contact Sales** to buy that add-on feature.

2. Click **Upgrade to Pro**.

## Licensing action in progress...

- Step 1       Generate cluster summary file
- Step 2      Upload cluster summary file to Support Portal
- Step 3      Apply license

Figure: Upgrading to Pro

AOS is automatically performing each step, including contacting the Support Portal to download a license file, and then applying the license. After applying the license, the window displays a **Successfully applied licenses** message.

3. Click **X** to close the Licensing window.

### Example: Renewing a License with Portal Connection

In this example, Portal Connection is configured and the customer has purchased new Pro licenses for a cluster with expired Pro licenses.

Downgrade your cluster to renew your licenses and then apply the renewed licenses.

1. Open **Licensing** from the gear icon in the Prism web console for the connected cluster.  
Because the license has expired, you can also **Downgrade to Starter** if you did not purchase new licenses.

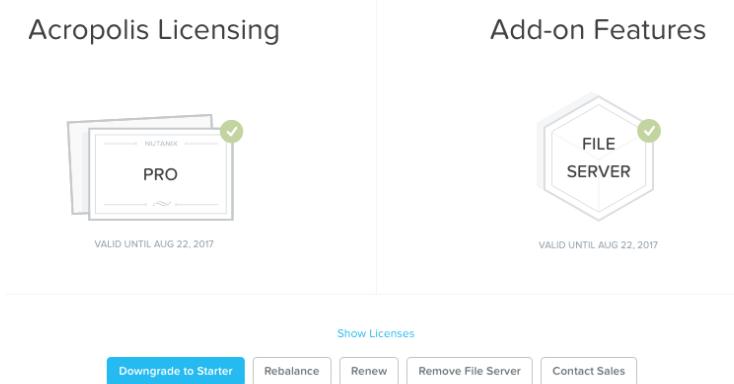


Figure: Portal Connection License Renewal Example

2. Click **Renew** to apply the new Pro licenses.  
AOS is automatically performing each step, including contacting the Support Portal to download a license file, and then applying the license. After applying the license, the window displays a **Successfully applied licenses** message.
3. Click **X** to close the Licensing window.

### Example: Removing An Add-on Feature

In this example, Portal Connection is configured in this Pro-licensed cluster and the customer had previously purchased an add-on feature license. Here, the customer removes this feature.

1. Open **Licensing** from the gear icon in the Prism web console for the connected cluster.

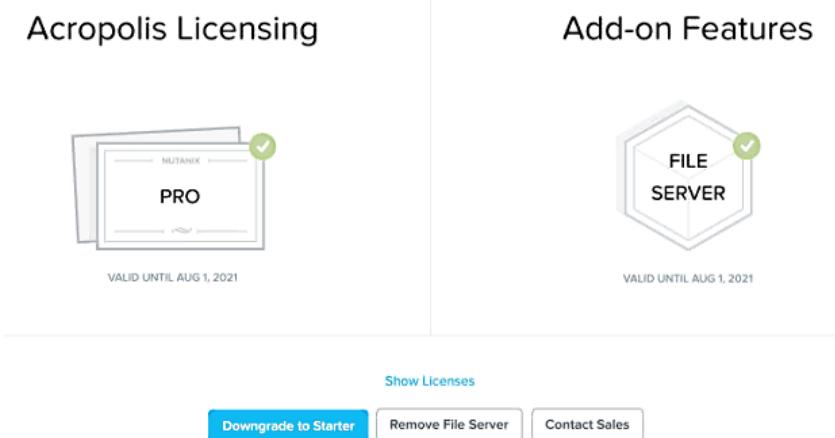


Figure: Pro License with Add-on

The Licensing window shows that you have installed the Acropolis File Server add-on. You can click **Contact Sales** to buy add-on features or licenses.

- Click **Remove File Server** to remove this add-on feature. Click **Yes** in the confirmation window. Portal Connection places the cluster into standby mode to remove the feature and update the cluster license status. After this operation is complete, license status is updated.

### Acropolis Licensing

### Add-on Features

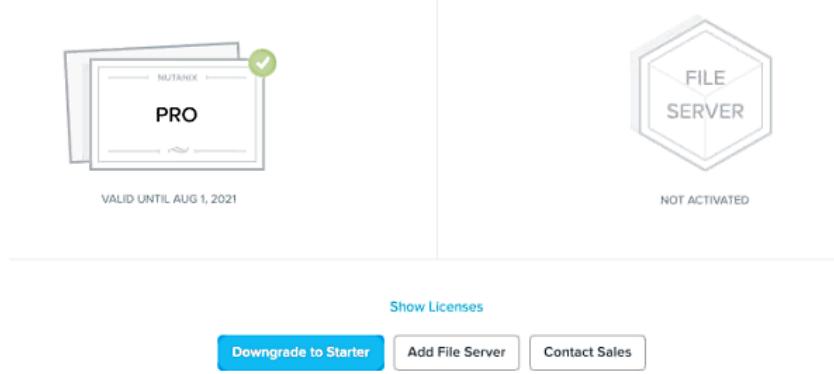


Figure: Add-On Removed

- Click **X** to close the Licensing window.

### Reclaiming Licenses (Portal Connection)

#### Before you begin:



**Note:** If you have destroyed the cluster and did not reclaim the existing licenses (except for Starter licenses), contact Nutanix Support to help reclaim the licenses. The *Acropolis Advanced Administration Guide* describes how to destroy a cluster.

See [Reclaiming Licenses](#) on page 70 to reclaim licenses where the cluster is not configured with Portal Connection or the cluster is not connected to the internet (also known as dark-site clusters).

You can reclaim and optionally re-apply licenses for nodes in your clusters when using Portal Connection.

- You must reclaim licenses (other than Starter) when you plan to destroy a cluster. First downgrade to Starter, then destroy the cluster. You do not need to reclaim Starter licenses. These licenses are automatically applied whenever you create a cluster.
- Return licenses to your inventory when you remove one or more nodes from a cluster. Also, if you move nodes from one cluster to another, first reclaim the licenses, move the nodes, then re-apply the licenses. Otherwise, if you are removing a node and not moving it to another cluster, use the **Rebalance** button.
- You can reclaim licenses for nodes in your clusters in cases where you want to make modifications or downgrade licenses. For example, applying an Ultimate license to all nodes in a cluster where some nodes are currently licensed as Pro and some nodes are licensed as Ultimate. You might also want to transition nodes from Ultimate to Pro licensing.

- Open **Licensing** from the gear icon in the Prism web console for the connected cluster.
- Remove any add-ons as described in [Example: Removing An Add-on Feature](#) on page 58.
- Click **Downgrade to Starter** after any add-ons are removed.

## Acropolis Licensing



## Add-on Features



Show Licenses

[Downgrade to Starter](#)

[Add File Server](#)

[Contact Sales](#)

*Figure: Add-On Removed*

4. Click **X** to close the Licensing window.

You can now perform any additional tasks, such as destroying the cluster or re-applying licenses.

### Example: Updating a License with Portal Connection

In this example, Portal Connection is configured and the customer has extended existing Pro licenses for a cluster. That is, the expiration date for existing licences has been extended before the licenses have expired.

Update your cluster to apply the new license expiration date.

1. Open **Licensing** from the gear icon in the Prism web console for the connected cluster.

## Acropolis Licensing



## Add-on Features



Show Licenses

[Update](#)

[Downgrade to Starter](#)

[Remove File Server](#)

[Contact Sales](#)

*Figure: Portal Connection License Update Example*

2. Click **Update** to extend the expiration date of the existing Pro licenses.

AOS is automatically performing each step, including contacting the Support Portal to download a license file, and then applying the license. After applying the license updates, the window displays a Successfully applied licenses message.

3. Click **Show Licenses** to ensure the new expiration date has been applied.
4. Click **X** to close the Licensing window.

## Managing Licenses without Portal Connection (Default)

AOS is installed or upgraded (from AOS 4.x versions) with the Portal Connection disabled by default. If you do not want to enable this feature, you can manage licenses as described in these topics.



**Note:** Generating a cluster summary file through the Prism web console, nCLI commands (`license generate-cluster-info`), or PowerShell commands (`Get-NTNXClusterLicenseInfo` and `Get-NTNXClusterLicenseInfoFile`) initiates the cluster licensing process. You might observe a Licensing Status: In Process alert message in the web console or log files in this case. [ENG-60722]

You can perform the licensing procedures described in these topics from a cluster's Prism web console or from the Prism Central web console (if you have purchased and want to apply or manage a Prism Pro license for Prism Central). See the [Prism Pro License](#) on page 48 topic.

With Portal Connection disabled by default (disabled as described in [Disabling or Enabling the Portal Connection](#) on page 51), you can manage licenses as described in these licensing topics:

- Install a license on Internet-connected clusters that can contact the Nutanix Support Portal.  
[Installing a New License](#) on page 61
- Manually install a license on a cluster that is not connected to the Internet and cannot contact the Nutanix Support Portal.  
[Installing a New License \(Dark Site\)](#) on page 63
- Install a license for a node added to a cluster.  
[Re-Installing the License File After Adding a Node to a Cluster](#) on page 67
- Install a newly-purchased license to upgrade features or extend the licensing term on your cluster or nodes. Alternately, you can downgrade licenses.  
[Upgrading or Downgrading Licenses](#) on page 69
- Reclaim a license by returning it to your inventory before destroying a cluster, when modifying license assignment, or after removing a node from a cluster. (After you remove a node, you can move the node to another cluster. Doing so requires using an available license in your inventory.)  
[Reclaiming Licenses](#) on page 70

### Installing a New License

This procedure assumes you have purchased licenses and describes how to:

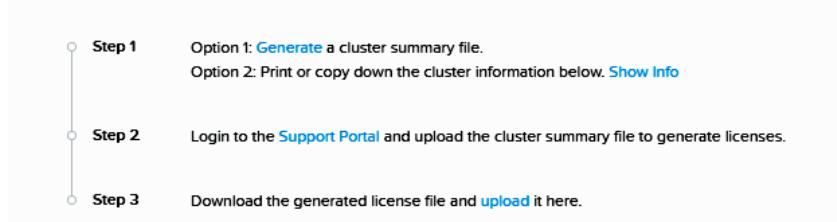
- Generate a cluster summary file and upload it to the Nutanix support portal
- Generate and download a license from the support portal
- Install the license on a cluster connected to the Internet

You can also perform this procedure from the Prism Central web console to apply a Prism Pro license.

1. Generate a cluster summary file in the Prism web console.

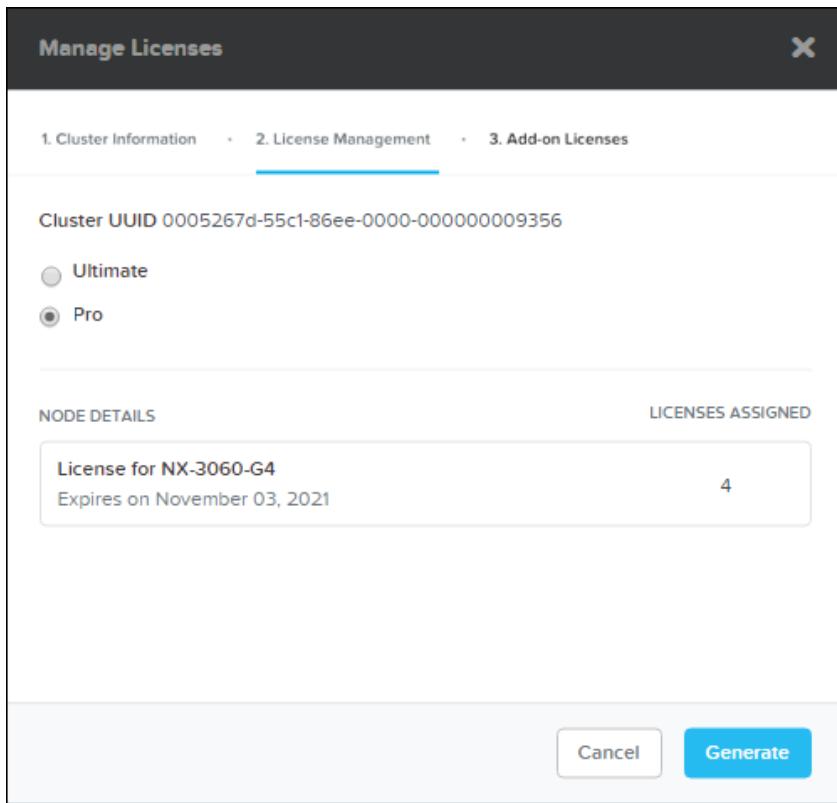
- a. Open **Licensing** from the gear icon  in the Prism web console for the connected cluster.
- b. Click **Update License**.
- c. Click **Generate** to create and save a cluster summary file to your local machine.

The cluster summary file is saved to your browser download directory or directory you specify.



*Figure: Manage Licensing*

2. Upload the cluster summary file to the Nutanix support portal.
  - a. Click **Support Portal**, log on to the Nutanix Support Portal, and click **My Products > Licenses**.
  - b. Click **License a New Cluster**. The **Manage Licenses** dialog box is displayed.
  - c. Click **Choose File**. Browse to the cluster summary file you just downloaded, select it, and click **Next**.  
The portal automatically assigns a license required based on the information contained in the cluster summary file.
3. Generate and apply the downloaded license file to the cluster.
  - a. Click **Generate** to download the license file created for the cluster to your browser download folder or directory you specify.



*Figure: Generating a License*

- b. In the Prism web console, click the **upload** link in the **Manage Licenses** dialog box.
- c. Browse to the license file you downloaded, select it, and click **Save**.

**Results:** The Licensing dialog box shows the license key as successfully uploaded and also displays all license details for the cluster. **What to do next:** See *Displaying License Features and Details* on page 72

#### Installing a New License (Dark Site)

This procedure assumes you have purchased licenses and describes how to:

- Generate and upload a cluster summary file to the Nutanix support portal
- Generate and download a license from the support portal
- Install the license on the cluster that is not connected to the Internet (that is, a *dark site*).



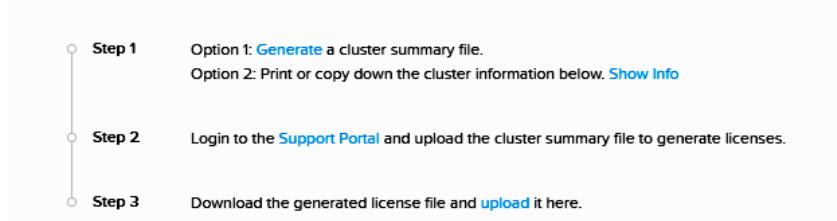
**Note:** You can also use Option 1 shown in *Manage Licensing* to generate a cluster summary file and copy that file to a machine connected to the Internet to upload to the Nutanix Support Portal. However, as dark-site systems are not connected to the Internet to adhere to regulatory, security, or compliance policies at the customer site, this procedure describes the manual entry of cluster information.



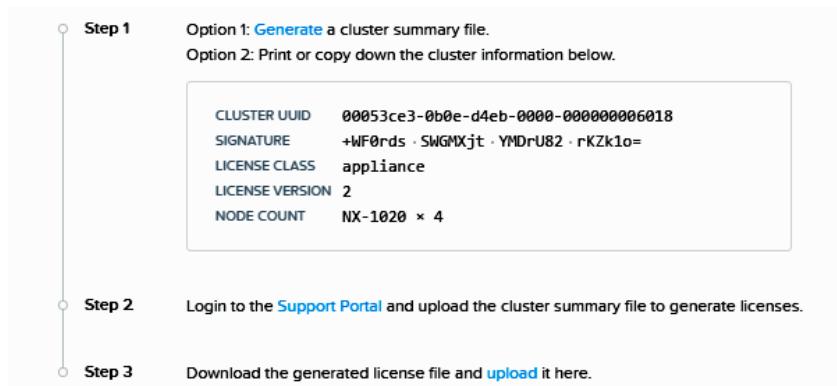
**Note:** Generating a cluster summary file through the Prism web console, nCLI commands (`license generate-cluster-info`), or PowerShell commands (`Get-NTNXClusterLicenseInfo` and `Get-NTNXClusterLicenseInfoFile`) initiates the cluster licensing process. You might observe a **Licensing Status: In Process** alert message in the web console or log files in this case. [ENG-60722]

1. Get your cluster information from the Prism web console.

- a. Open **Licensing** from the gear icon  in the Prism web console for the connected cluster.
- b. Click **Update License**.
- c. Click **Show Info** and copy the cluster information needed to generate a license file.



*Figure: Manage Licensing*



*Figure: Cluster Information Needed for Licensing*

The page displays information that you need to upload to the support portal on an internet-connected system. Copy this information needed to complete this procedure.

<b>Cluster UUID</b>	String indicating the unique cluster ID
<b>Signature</b>	Cluster security key
<b>License Class</b>	Indicates a software-only, appliance-based, or Prism Central license class
<b>License Version</b>	Indicates the version of the any installed license file
<b>Node Count</b>	Number of available licenses for this model

2. On a machine connected to the Internet, enter the cluster summary file info, then generate and download the license file at the Nutanix support portal.
    - a. Log on to the Nutanix Support Portal and click **My Products > Licenses**.
    - b. Click **License a New Cluster**, then click **enter one manually** in **Manage Licenses**.
    - c. Type and select the cluster information you copied, then click **Next**.
- The **License Type** to select is one of: Appliance, Software Only, or Prism Central.

**Manage Licenses**

1. Cluster Information · 2. License Management

**Cluster Summary File**  
Input your cluster information from the Prism GUI or go back to [File Upload](#).

**LICENSE CLASS**

Appliance  
 Software Only  
 Prism Central  
 n/a

**CLUSTER UUID**  
00000000-0000-0000-0000-000000000000

**SIGNATURE**  
00000000-00000000-00000000-00000000

**Node Information**

MODEL	COUNT
Model	Number of nodes <input type="text"/>

**Cancel** **Next**

- d. Click **Generate** to download the license file created for the cluster to your browser download folder or directory you specify.
3. Apply the downloaded license file to the cluster.
    - a. Open **Licensing** from the gear icon in the Prism web console of the unconnected cluster.
    - b. Click **Manage Licenses**, then click the **upload** link.
    - c. Browse to the license file you downloaded, select it, and click **Save**.

**Results:** The Licensing dialog box shows the license key as successfully uploaded and also all license details for the cluster. **What to do next:** See [Displaying License Features and Details](#) on page 72

#### Installing a New Add-On License

This procedure assumes you have purchased one or more add-in licenses and describes how to:

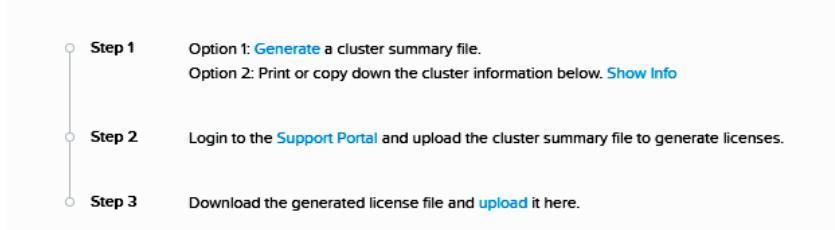
- Generate a cluster summary file and upload it to the Nutanix support portal
- Generate and download an add-on license from the support portal
- Install the license on a cluster connected to the Internet



**Note:** Generating a cluster summary file through the Prism web console, nCLI commands (`license generate-cluster-info`), or PowerShell commands (`Get-NTNXClusterLicenseInfo` and `Get-NTNXClusterLicenseInfoFile`) initiates the cluster licensing process. You might observe a Licensing Status: In Process alert message in the web console or log files in this case. [ENG-60722]

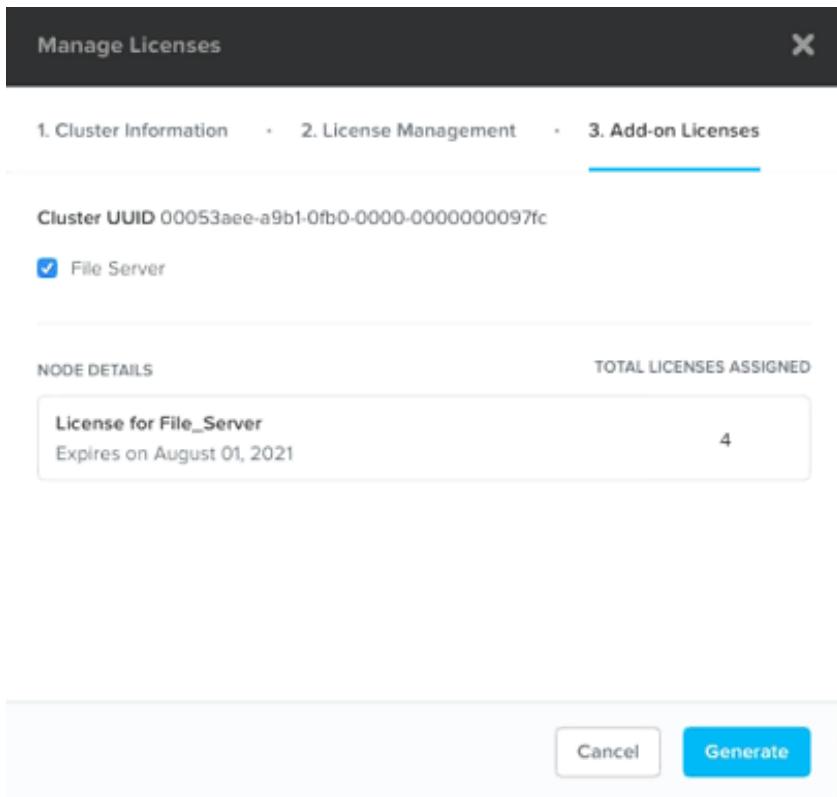
1. Generate a cluster summary file in the Prism web console.
  - a. Open **Licensing** from the gear icon in the Prism web console for the connected cluster.
  - b. Click **Update License**.
  - c. Click **Generate** to create and save a cluster summary file to your local machine.

The cluster summary file is saved to your browser download directory or directory you specify.



*Figure: Manage Licensing*

2. Upload the cluster summary file to the Nutanix support portal.
  - a. Click **Support Portal**, log on to the Nutanix Support Portal, and click **My Products > Licenses**.
  - b. Click **License a New Cluster** and the **Manage Licenses** dialog box is displayed.
  - c. Click **Choose File**, then browse to the cluster summary file you just downloaded, select it, and click **Next**.
3. To claim your add-on license, generate and apply the downloaded license file to the cluster.
  - a. Click **Add-on Licenses**, then **Generate** to download the license file created for the cluster to your browser download folder or directory you specify.



- b. In the Prism web console, click the **upload** link in the **Manage Licenses** dialog box.
- c. Browse to the license file you downloaded, select it, and click **Save**.

**Results:** The Licensing dialog box shows the license key as successfully uploaded and also all license details for the cluster. **What to do next:** See *Displaying License Features and Details* on page 72

#### Re-Installing the License File After Adding a Node to a Cluster

If you added a node to your cluster, you must install a new updated license file. To obtain the new license:

- Generate a cluster summary file and upload it to the Nutanix support portal
- Generate and download a license from the support portal
- Install the license on the cluster

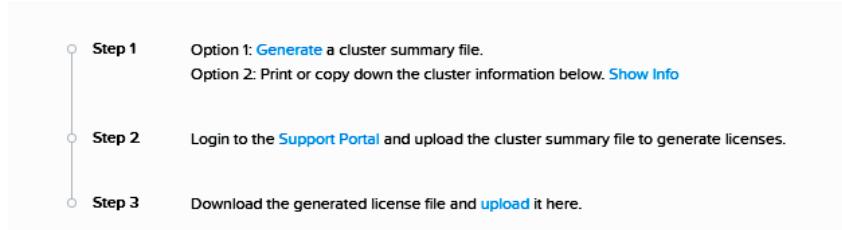


**Note:** Generating a cluster summary file through the Prism web console, nCLI commands (`license generate-cluster-info`), or PowerShell commands (`Get-NTNXClusterLicenseInfo` and `Get-NTNXClusterLicenseInfoFile`) initiates the cluster licensing process. You might observe a **Licensing Status: In Process** alert message in the web console or log files in this case. **[ENG-60722]**

#### Installing a License After Adding a Node

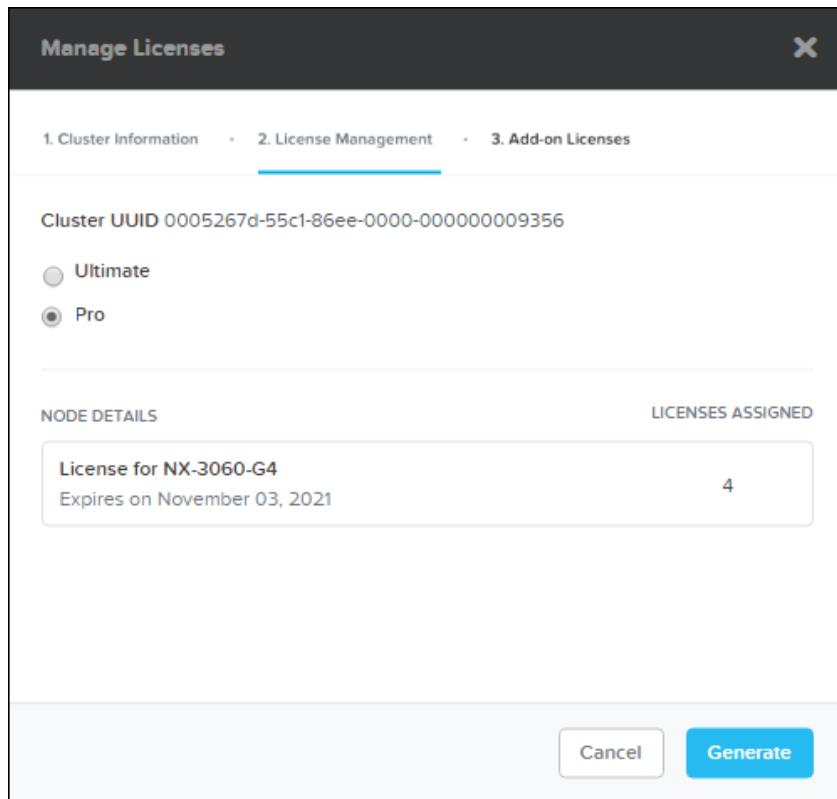
1. Generate a cluster summary file in the Prism web console.
  - a. Open **Licensing** from the gear icon  in the Prism web console for the connected cluster.
  - b. Click **Update License**.

- c. Click **Generate** to create and save a cluster summary file to your local machine.  
The cluster summary file is saved to your browser download directory or directory you specify.



*Figure: Manage Licensing*

2. Upload the cluster summary file to the Nutanix support portal.
  - a. Click **Support Portal**, log on to the Nutanix Support Portal, and click **My Products > Licenses**.
  - b. Click **Licensed Clusters**, find the **Cluster UUID** of your cluster, and click **Add Node**.
  - c. In the **Manage Licenses** dialog box, click **Choose File**, then browse to the cluster summary file you just downloaded, select it, and click **Next**.
3. Generate and apply the downloaded license file to the cluster.
  - a. Click **Generate** to download the license file created for the cluster to your browser download folder or directory you specify.



*Figure: Generating a License*

- b. In the Prism web console, click the **upload** link in the **Manage Licenses** dialog box.

- c. Browse to the license file you downloaded, select it, and click **Open**.

**Results:** The Licensing dialog box shows the license key as successfully uploaded and also displays all license details of the cluster. **What to do next:** See *Displaying License Features and Details* on page 72

### Upgrading or Downgrading Licenses

#### Upgrading Licenses

Perform this procedure after purchasing license upgrades. The Nutanix support portal displays the **Upgrade** link when your inventory contains newly-available licenses.

- Generate and upload a cluster summary file to the Nutanix support portal
- Generate and download a license from the support portal
- Install the license on the cluster that is not connected to the Internet.



**Note:** Generating a cluster summary file through the Prism web console, nCLI commands (`license generate-cluster-info`), or PowerShell commands (`Get-NTNXClusterLicenseInfo` and `Get-NTNXClusterLicenseInfoFile`) initiates the cluster licensing process. You might observe a Licensing Status: In Process alert message in the web console or log files in this case. [ENG-60722]

1. Generate a cluster summary file in the Prism web console.

- a. Open **Licensing** from the gear icon in the Prism web console for the connected cluster.
- b. Click **Update License**.
- c. Click **Generate** to create and save a cluster summary file to your local machine.

The cluster summary file is saved to your browser download directory or directory you specify.

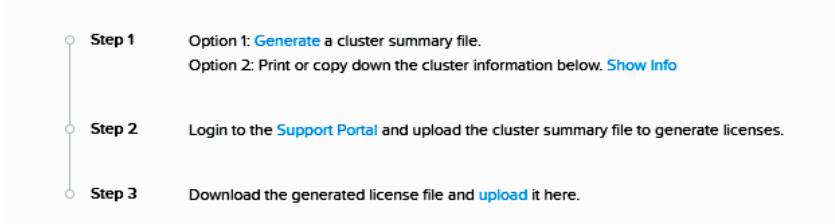


Figure: Manage Licensing

2. Upload the cluster summary file to the Nutanix support portal.
  - a. Click **Support Portal**, log on to the Nutanix Support Portal, and click **My Products > Licenses**.
  - b. Click **Licensed Clusters** to display a summary of your licensed clusters.
  - c. Find the **Cluster UUID** for the cluster you want to upgrade, then click **Upgrade**.
  - d. In the **Manage Licenses** dialog box, click **Choose File**, then browse to the cluster summary file you just downloaded, select it, and click **Next**.
3. Generate and apply the license file to the cluster.

- a. Click **Generate** to download the license file created for the cluster to your browser download folder or directory you specify.
- b. In the Prism web console, click the **upload** link in the **Manage Licenses** dialog box.
- c. Browse to the license file you downloaded, select it, and click **Save**.

**Results:** The Licensing dialog box shows the license key as successfully uploaded and also all license details for the cluster.

### Downgrading Licenses

You can downgrade a license as follows:

1. Reclaim licenses as described in [Reclaiming Licenses](#) on page 70.
2. Install the new licenses as described in [Installing a New License](#) on page 61 or [Installing a New License \(Dark Site\)](#) on page 63.

### Reclaiming Licenses

#### Before you begin:



**Note:** If you have destroyed the cluster and did not reclaim the existing licenses (except for Starter licenses), contact Nutanix Support to help reclaim the licenses. The *Acropolis Advanced Administration Guide* describes how to destroy a cluster.

You can reclaim and optionally re-apply licenses for nodes in your clusters. This procedure describes how to reclaim licenses where the cluster is not configured with Portal Connection or the cluster is not connected to the internet (also known as dark-site clusters).

- You must reclaim licenses (other than Starter) when you plan to destroy a cluster. First reclaim the licenses, then destroy the cluster.
  - You do not need to reclaim Starter licenses. These licenses are automatically applied whenever you create a cluster.
  - You do not need to downgrade to Starter licenses where the cluster is not configured with Portal Connection or where clusters are not connected to the internet (also known as dark-site clusters).
- Return licenses to your inventory when you remove one or more nodes from a cluster. Also, if you move nodes from one cluster to another, first reclaim the licenses, move the nodes, then re-apply the licenses.
- You can reclaim licenses for nodes in your clusters in cases where you want to make modifications or downgrade licenses. For example, applying an Ultimate license to all nodes in a cluster where some nodes are currently licensed as Pro and some nodes are licensed as Ultimate. You might also want to transition nodes from Ultimate to Pro licensing.



**Note:** Generating a cluster summary file through the Prism web console, nCLI commands (`license generate-cluster-info`), or PowerShell commands (`Get-NTNXClusterLicenseInfo` and `Get-NTNXClusterLicenseInfoFile`) initiates the cluster licensing process. You might observe a Licensing Status: In Process alert message in the web console or log files in this case. [ENG-60722]

### Reclaiming Licenses When Destroying a Cluster

#### Before you begin:



**Note:** If you have destroyed the cluster and did not reclaim the existing licenses (except for Starter licenses. These licenses are automatically applied whenever you create a cluster), contact Nutanix Support to help reclaim the licenses. The *Acropolis Advanced Administration Guide* describes how to destroy a cluster.

1. Generate a cluster summary file in the Prism web console.

- a. Open **Licensing** from the gear icon in the Prism web console for the connected cluster.
- b. Click **Update License**.
- c. Click **Generate** to create and save a cluster summary file to your local machine.

The cluster summary file is saved to your browser download directory or directory you specify.

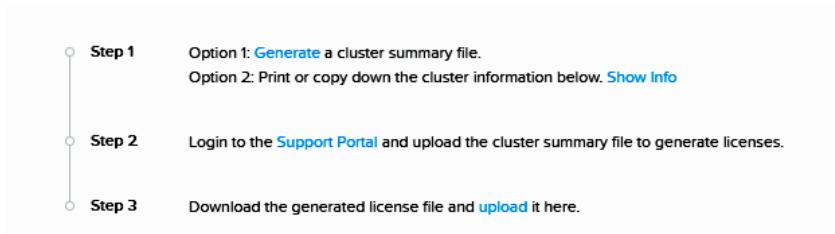


Figure: Manage Licensing

2. Upload the cluster summary file to the Nutanix support portal.

- a. Click **Support Portal**, log on to the Nutanix Support Portal, and click **My Products > Licenses**.
- b. Click **Licensed Clusters** to display a summary of your licensed clusters.
- c. Find your Cluster UUID and click **Reclaim All**.
- d. In the **Manage Licenses** dialog box, click **Choose File**, then browse to the cluster summary file you downloaded, select it, and click **Next**.
- e. Click **Done**.

3. Destroy the cluster as described in the *Acropolis Advanced Administration Guide*.

#### Reclaiming Licenses When Removing Nodes from a Cluster

**Before you begin:** The *Acropolis Advanced Administration Guide* describes how to remove a node from a cluster.

1. Remove a node from a cluster.

2. Generate a cluster summary file in the Prism web console.

- a. Open **Licensing** from the gear icon in the Prism web console for the connected cluster.
- b. Click **Update License**.
- c. Click **Generate** to create and save a cluster summary file to your local machine.

The cluster summary file is saved to your browser download directory or directory you specify.

3. Upload the cluster summary file to the Nutanix support portal.
  - a. Click **Support Portal**, log on to the Nutanix support portal and click **My Products > Licenses**.
  - b. Click **Licensed Clusters**, find your Cluster UUID, and click **Reclaim**.
  - c. In the **Manage Licenses** dialog box, click **Choose File**, then browse to the cluster summary file you downloaded, select it, and click **Next**.
  - d. Click **Done**.

#### Reclaiming Licenses When Modifying License Assignments

1. Generate a cluster summary file in the Prism web console.
  - a. Open **Licensing** from the gear icon  in the Prism web console for the connected cluster.
  - b. Click **Update License**.
  - c. Click **Generate** to create and save a cluster summary file to your local machine.  
The cluster summary file is saved to your browser download directory or directory you specify.
2. Upload the cluster summary file to the Nutanix support portal.
  - a. Click **Support Portal**, log on to the Nutanix support portal and click **My Products > Licenses**.
  - b. Click **Licensed Clusters**, find your Cluster UUID, and click **Reclaim All**.
  - c. In the **Manage Licenses** dialog box, click **Choose File**, then browse to the cluster summary file you downloaded, select it, and click **Next**.
  - d. Click **Done**.
3. To apply the same license to all nodes in a cluster, perform the steps described in [Installing a New License](#) on page 61 or [Installing a New License \(Dark Site\)](#) on page 63.

#### Displaying License Features and Details

1. Open **Licensing** from the gear icon in the Prism web console.
2. Click the license certificate (**Starter**, **Pro**, **Ultimate**) to show the feature list for your license. For example:

## Acropolis Licensing

The screenshot shows the 'Licensing' interface. On the left, there's a 'STARTER' license card icon with a green checkmark. Below it, a link says 'DOES NOT EXPIRE Show Licenses'. Buttons for 'Update License' and 'Contact Sales' are at the bottom. A callout arrow points from the 'Show Licenses' link to the right panel.

**Licensing**

**Starter License Features**

You are viewing the complete list of all features and their enablement status.

FEATURE	PERMITTED
Application Consistent Snapshot	Yes
Automatic Download	Yes
Cluster Lockdown	Yes
Heterogeneous Clusters	Yes
Inline Compression	Yes
Inline Performance Deduplication	Yes
Maximum Node Limit (within cluster)	12
Maximum Redundancy Factor	2
Prism Central	Yes
Pulse	Yes
Remote Site Compression	Yes
SNMP	Yes
Cloud Connect	No
Common Access Card (CAC)	No

**< Back**

Figure: License Features

Scroll down to see other features, then click **Back** to return to the licensing page.

- Click Show Licenses to show a list of all licenses and their details.

## Acropolis Licensing

The screenshot shows the 'Licensing' interface. On the left, there's a 'STARTER' license card icon with a green checkmark. Below it, a link says 'DOES NOT EXPIRE Show Licenses'. Buttons for 'Update License' and 'Contact Sales' are at the bottom. A callout arrow points from the 'Show Licenses' link to the right panel.

**Licensing**

**License Details**

You are viewing the complete list of all licenses and their details.

LICENSE ID	MODEL	LICENSE TYPE	IN USE	EXPIRATION
—	NX-1020	Starter	Yes	Never
—	NX-1020	Starter	Yes	Never
—	NX-1020	Starter	Yes	Never
—	NX-1020	Starter	Yes	Never

Add-on Licenses:

LICENSE ID	MODEL	LICENSE TYPE	IN USE	EXPIRATION
There are no licenses of this type.				

**< Back**

Figure: License Details

Scroll down to see all licenses, then click **Back** to return to the licensing page.

## License Warnings in the Web Console

Most license warnings in the web console are related to license violations or licenses that are about to expire or expired. In most cases, the resolution is to extend or purchase licenses.

- Starter licenses never expire.
- Pro and Ultimate licenses do have an expiration date and the web console alerts you 60 days before expiration.
- If you attempt to use features not available in your cluster's license type, a Warning is issued. Please upgrade your license type if you require continued access to Pro or Ultimate features.
- If a cluster includes nodes with different license types, the cluster and each node in the cluster defaults to the minimum feature set enabled by the lowest license type. For example, if two nodes in the cluster have Pro licenses and two nodes in the same have Ultimate licenses, all nodes will effectively have Pro licenses and access to that feature set only. Attempts to access Ultimate features in this case result in a Warning in the web console.
- If you are using a Prism Pro trial license, the warning shows the expiration date and number of days left in the trial period. Typically, the trial period is 60 days. The license name will also display as a Pro\_Trial license type.
- During upgrade of AOS, the Prism web console might incorrectly display a license violation alert. After you complete the upgrade, the alert is not displayed.
- *ENG-60722 ENG-60827* Generating a cluster summary file through the Prism web console, nCLI commands (generate-cluster-info), or PowerShell commands (Get-NTNXClusterLicenseInfo and Get-NTNXClusterLicenseInfoFile) initiates the cluster licensing process. You might observe a Licensing Status: In Process alert message in the web console or log files in this case.

## Software and Firmware Upgrades



### Note:

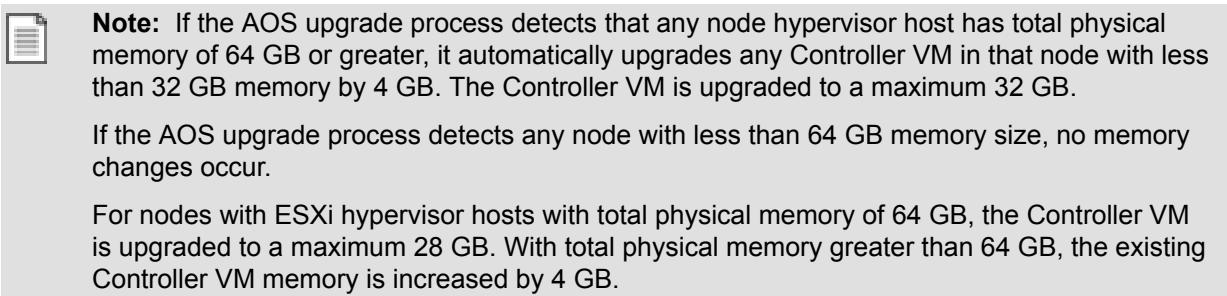
- If you are adding a new node to a cluster, see [Expanding a Cluster](#) on page 186 for information about upgrading a new node.
- Always wait for an upgrade operation to complete before attempting to perform any additional procedures or operations, including another upgrade procedure.
- Before performing any upgrade procedure, run the Nutanix Cluster Check health checks from a Controller VM by typing ncc health\_checks run\_all or from the Prism web console Health page: select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Do not perform any cluster upgrades (AOS, Controller VM memory, hypervisor, and so on) if you have just registered your cluster in vCenter. Wait at least one hour before performing upgrades to allow cluster settings to become updated. Also do not register the cluster in vCenter and perform any upgrades at the same time.
- During upgrades that require host restarts in AHV clusters (such as AHV or firmware upgrades), a task named HostRestoreVmLocality appears on the **All VM Tasks** tab. The task is scheduled during the upgrade process as part of a group of tasks that check the state of the cluster. No migration is required or expected for AOS upgrades.

AOS supports upgrades that you can apply through the Prism web console **Upgrade Software** feature (also known as 1-click upgrade).

- AOS

### [Upgrading AOS](#) on page 79

Each node in a cluster runs AOS. When upgrades are available and you want to upgrade the cluster to a new AOS version, every node must be upgraded to that version. Nutanix provides a live upgrade mechanism that allows the cluster to run continuously while a rolling upgrade of the nodes is started in the background.



- Hypervisor software

[Hypervisor Upgrade Overview and Requirements](#) on page 86

[Upgrading AHV Hosts](#) on page 88

[Upgrading ESXi Hosts by Uploading Binary and Metadata Files](#) on page 90

[Upgrading Hyper-V Hosts](#) on page 94

[Upgrading XenServer Hosts](#) on page 94

Available hypervisor upgrades provided by vendors such as VMware and qualified by Nutanix might become available on occasion. The upgrade process updates one node in a cluster at a time. Once the upgrade is complete on the first node in the cluster you have selected, the process begins on the next node, until all nodes in the cluster have been updated.

- Nutanix Cluster Check (NCC)

[Upgrading NCC Software](#) on page 82

[Installing NCC from an Installer File](#) on page 84

Nutanix occasionally updates the NCC software and makes those updates available for download. The process updates one node at a time. Once the update is complete on the first node in the cluster, the process begins on the next node, until all nodes in the cluster have been updated.

- Foundation

[Upgrading Foundation](#) on page 101

Nutanix occasionally updates the Foundation software and makes those updates available for download. The process updates one node at a time. Once the update is complete on the first node in the cluster, the process begins on the next node, until all nodes in the cluster have been updated.

- BIOS and BMC firmware

[Upgrading BMC or BIOS Firmware](#) on page 98

Nutanix occasionally provides updated BIOS and base management controller (BMC) firmware. Nutanix rarely includes this firmware on the Nutanix Support Portal. Nutanix recommends that you open a case on the Support Portal to request if any firmware updates are available for your platform.

The process updates one node at a time. Once the upgrade is complete on the first node in the cluster, the process begins on the next node, and so on, until all nodes in the cluster have been updated.

- Disk firmware

[Upgrading Disk Firmware: On Demand Download](#) on page 81

Firmware upgrades provided by the manufacturers of the hard or solid-state disk drives in your cluster and qualified by Nutanix might become available on occasion. Nutanix rarely includes this firmware on the Nutanix Support Portal. Nutanix recommends that you open a case on the Support Portal to request if any disk firmware updates are available for your platform.

Nutanix provides a live upgrade mechanism similar to the AOS upgrade for the disk firmware. The upgrade process updates one disk at a time on each node for the disk group you have selected to upgrade. Once the upgrade is complete on the first node in the cluster, the process begins on the next node, updating one disk at a time, and so on, until all drives in the cluster have been updated.

- HBA Disk Controller Firmware

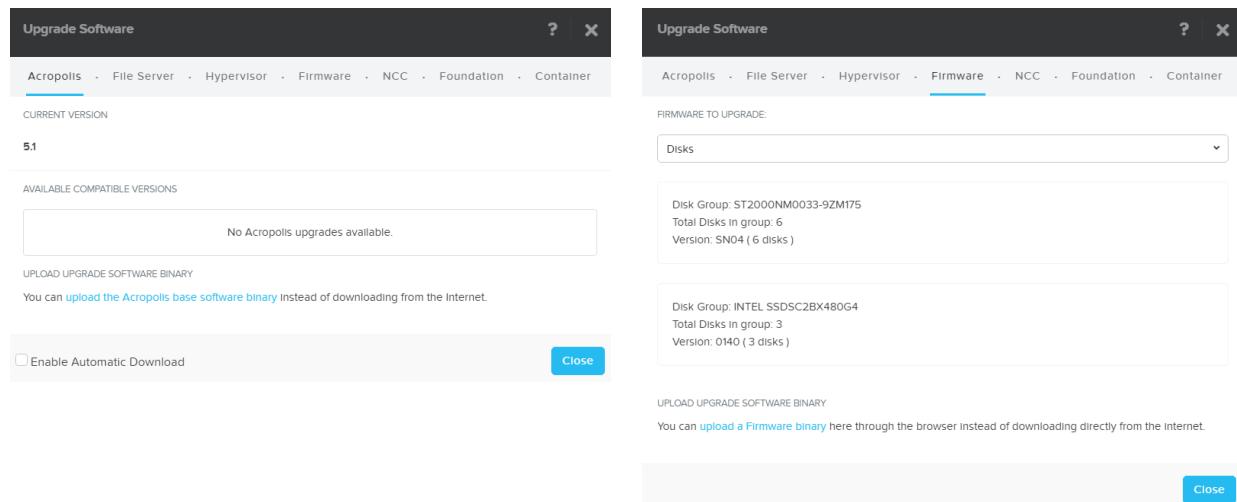
#### *Upgrading HBA Firmware* on page 101

Nutanix occasionally provides updated HBA disk controller firmware. Nutanix rarely includes this firmware on the Nutanix Support Portal. Nutanix recommends that you open a case on the Support Portal to request if any firmware updates are available for your platform. Nutanix Support will provide you with metadata (.json) and firmware binary files.

You can view the available upgrade options, start an upgrade, and monitor upgrade progress through the web console. **Upgrade Software**, available from the main menu, shows the current status of your software and firmware versions.

For example:

#### Upgrade Software Dialog



- **CURRENT VERSION** displays the AOS version running currently in the cluster.
- **AVAILABLE COMPATIBLE VERSIONS** displays any versions to which the cluster can be updated.
- The **upload the Acropolis base software binary** link enables you to install AOS from binary and metadata files, which might be helpful for updating isolated clusters not connected to the Internet.
- **FIRMWARE TO UPGRADE** enables you to select upgradeable firmware categories.
- **AVAILABLE COMPATIBLE VERSIONS** displays any versions to which the drive can be updated.
- The **upload a Firmware binary** link enables you to install the firmware from binary and metadata files, which might be helpful for updating isolated clusters not connected to the Internet.

#### Options for Downloading Updates



**Note:**

- Ensure that you allow access to the following through your firewall to ensure that automatic download of updates can function:
  - \*.compute-\*.amazonaws.com:80
  - release-api.nutanix.com:80

You can choose how to obtain the latest versions of the AOS, firmware, or other software that Nutanix or hypervisor vendors make available on support and release portals.

### Software and Firmware Download Options

Downloadable Component	Automatic/On-Demand 1-Click Upgrade	File Upload 1-Click Upgrade
<ul style="list-style-type: none"> <li>• AOS</li> </ul>	<ul style="list-style-type: none"> <li>• Automatic: When <b>Enable Automatic Download</b> is selected in <b>Upgrade Software</b>, the web console regularly checks for new versions and downloads the software package for you. You can then choose to install it.</li> <li>• On demand: When <b>Enable Automatic Download</b> is cleared in <b>Upgrade Software</b>, you must click <b>Download</b> to retrieve the software package.</li> </ul>	<ul style="list-style-type: none"> <li>• Nutanix Support Portal. Binaries, metadata, and checksums are listed when available. For example, you can download a version, copy it to a USB stick or other media, and upgrade clusters not connected to the Internet.</li> </ul>
<ul style="list-style-type: none"> <li>• Firmware</li> <li>• Foundation</li> <li>• Nutanix Cluster Check (NCC)</li> </ul>	<ul style="list-style-type: none"> <li>• On demand: The web console regularly checks for new versions and notifies you through the <b>Upgrade Software</b> dialog box that a new version is available. You can then choose to download and install it.</li> </ul>	<ul style="list-style-type: none"> <li>• Nutanix Support Portal. Binaries, metadata, and checksums are listed <i>when available</i>. For example, you can download a version, copy it to a USB stick or other media, and upgrade clusters not connected to the Internet.</li> </ul>

Downloadable Component	Automatic/On-Demand 1-Click Upgrade	File Upload 1-Click Upgrade
<ul style="list-style-type: none"> <li>Hypervisor</li> </ul>	<ul style="list-style-type: none"> <li>On demand: The web console regularly checks for new AHV and Nutanix-qualified ESXi versions and notifies you through the <b>Upgrade Software</b> dialog box that a new version is available. You can then choose to download and install it.</li> <li>Not available for Hyper-V.</li> </ul>	<ul style="list-style-type: none"> <li>Nutanix Support Portal.</li> <li>AHV host installation and upgrade software bundles, metadata, and checksums required to install hypervisor software are listed when available for download.</li> <li>Other hypervisor metadata and checksums required to install hypervisor software are listed when available.</li> <li>Hypervisor vendor web site. Hypervisor vendors such as VMWare provide upgrade packages. For example, you can download the metadata file from Nutanix and hypervisor binary package from VMWare, copy it to a USB stick or other media, and then upgrade cluster hosts. See <a href="#">Hypervisor Upgrade Overview and Requirements</a> on page 86 for more information.</li> </ul>



**Note:** For 4.7 to 5.0 upgrade, AHV is automatically installed. Install from 4.6 or 4.7 to 5.0 and from 4.5 to 4.6 or 4.7 before updating to 5.0.

## AOS Upgrade Prerequisites

- Ensure that you allow access to the following through your firewall to ensure that automatic download of updates can function:
  - \*.compute-\*.amazonaws.com:80
  - release-api.nutanix.com:80
- If you had previously set the cluster's timezone by using the nCLI command `ncli cluster set-timezone timezone=cluster_timezone`, the timezone settings will persist after your cluster is upgraded. If you need to set or reset the cluster time zone, always use the nCLI command as shown above. If you set the timezone manually on a Controller VM through an SSH connection and copy command (`cp`) to each node in the cluster, the timezone will not persist and will be reset to the default PST timezone after the upgrade is completed. (For example, the timezone will not persist if you set the timezone by using `for i in `svmips` ; do echo $i; ssh $i "sudo cp /usr/share/zoneinfo/Asia/Seoul /etc/localtime; date"; done`.)
- If you use Prism Central to manage your Nutanix clusters, upgrade Prism Central first, then upgrade AOS on the clusters managed by Prism Central. See [Upgrading Prism Central](#).
- If you are adding a new node to a cluster, see [Expanding a Cluster](#) for information about upgrading a new node.
- As part of the AOS upgrade, the Controller VM where you have logged on and initiated the upgrade restarts. The Prism 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 web console again.

- (Async DR) If you previously upgraded from version 3.5.x to 4.0.x or 4.1.x, are currently running those versions, and did not delete existing protection domain schedules before upgrading to version 4.0.x or 4.1.x, delete them now, as described in the Nutanix *Upgrade Guide* for 4.x.
- You can upgrade a node or cluster through Prism Central in some cases. See [Upgrading Managed Clusters](#) in the *Prism Central Guide*.
- Pre-upgrade checks fail if the existing SNMP user, traps, or account are configured with MD5 authentication or DES encryption. Before upgrading, change the authentication type to SHA and remove the traps. For details, see Knowledge Base article [KB 2140](#).

## Upgrading AOS

**Before you begin:** See [AOS Upgrade Prerequisites](#) on page 78.

- Do the following steps to download and upgrade AOS through **Upgrade Software** in the Prism web console.
- If you are adding a new node to a cluster, see [Expanding a Cluster](#) on page 186 for information about upgrading a new node.
- If the AOS upgrade process detects that any node hypervisor host has total physical memory of 64 GB or greater, it automatically upgrades any Controller VM in that node with less than 32 GB memory by 4 GB. The Controller VM is upgraded to a maximum 32 GB.

If the AOS upgrade process detects any node with less than 64 GB memory size, no memory changes occur.

For nodes with ESXi hypervisor hosts with total physical memory of 64 GB, the Controller VM is upgraded to a maximum 28 GB. With total physical memory greater than 64 GB, the existing Controller VM memory is increased by 4 GB.

### 1. Run the Nutanix Cluster Checks (NCC).

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

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

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

### 2. Log on to the web console for any node in the cluster.

3. Open **Upgrade Software** from the gear icon  in the Prism web console and click **Acropolis**.
4. [Optional] To run the pre-upgrade installation checks only on the Controller VM where you are logged on without upgrading, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.

### 5. Do one of the following:

- If you previously selected **Enable Automatic Download** and the software package has been downloaded, click **Upgrade > Upgrade Now**, then click **Yes** to confirm.
- If **Enable Automatic Download** is cleared, click **Download**. When the download task is completed, click **Upgrade > Upgrade Now**, then click **Yes** to confirm.

The **Upgrade Software** dialog box shows the progress of your selection, including pre-installation and cluster health checks. After the upgrade process is completed on a Controller VM, the Controller VM restarts. This restart is not disruptive to node operations.

### What to do next:



**Important:** If you use SNMP to manage or collect information from the Nutanix cluster, as soon as the upgrade process is complete, update the Nutanix SNMP MIB file that is used by your network management system. Until the MIB file is updated, SNMP queries might return erroneous data or data of the wrong type. To download the latest SNMP MIB file, do the following:

1. In the web console, click the gear icon and then click **SNMP**.
2. In the **SNMP Configuration** dialog box, click **Download MIB**, and then save the MIB file to your local hard drive.

### Upgrading AOS by Uploading Binary and Metadata Files

**Before you begin:** See [AOS Upgrade Prerequisites](#) on page 78.

- Do the following steps to download AOS binary and metadata .JSON files from the Nutanix Support Portal, then upgrade AOS through **Upgrade Software** in the Prism web console.
- Typically you would need to perform this procedure if your cluster is not directly connected to the Internet and you cannot download the binary and metadata .JSON files through the Prism web console.

#### 1. Run the Nutanix Cluster Checks (NCC).

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

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

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

#### 2. Log on to the Nutanix support portal and select the AOS release from **Downloads**.

3. Click the download link to save the AOS binary and metadata .JSON files on your local media. You can also copy these files to a USB stick, CD, or other media.

#### 4. Log on to the Prism web console for any node in the cluster.

#### 5. Open **Upgrade Software** from the gear icon in the Prism web console and click **Acropolis**.

#### 6. Click the **upload an AOS binary** link.

#### 7. Click **Choose File** for the AOS metadata and binary files, respectively, browse to the file locations, and click **Upload Now**.

#### 8. [Optional] When the file upload is completed, to run the pre-upgrade installation checks only on the Controller VM where you are logged on without upgrading, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.

#### 9. When the upload process is completed, click **Upgrade > Upgrade Now**, then click **Yes** to confirm. The **Upgrade Software** dialog box shows the progress of your selection, including pre-installation and cluster health checks. After the upgrade process is completed on a controller VM, the controller VM restarts. This restart is not disruptive to node operations.

## What to do next:



**Important:** If you use SNMP to manage or collect information from the Nutanix cluster, as soon as the upgrade process is complete, update the Nutanix SNMP MIB file that is used by your network management system. Until the MIB file is updated, SNMP queries might return erroneous data or data of the wrong type. To download the latest SNMP MIB file, do the following:

1. In the web console, click the gear icon and then click **SNMP**.
2. In the **SNMP Configuration** dialog box, click **Download MIB**, and then save the MIB file to your local hard drive.

## Upgrading Disk Firmware: On Demand Download

**Before you begin:** Nutanix rarely includes this firmware on the Nutanix Support Portal. Nutanix recommends that you open a case on the Support Portal to request if any firmware updates are available for your platform. Nutanix Support will provide you with metadata (.json) file and firmware binary files. In this case, use the procedure described in *Upgrading Disk Firmware By Using a Shell File*.

Use this procedure if the web console detects that a new version is detected automatically.

1. Run the Nutanix Cluster Checks (NCC).

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

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

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

2. Log on to the web console for any node in the cluster.
3. Open **Upgrade Software** from the gear icon in the web console.
4. Click **Firmware > Disks** in the dialog box.
5. If an update is available, click **Upgrade Available** and then click **Download**.

6. When the download is complete, click **Upgrade > Upgrade Now**, then click **Yes** to confirm.

To run the pre-upgrade installation checks only on the controller VM where you are logged on, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.

The **Upgrade Software** dialog box shows the progress of your selection, including pre-installation checks.

The disk firmware upgrade process takes approximately five minutes per disk. Controller VM boot disk upgrade might take a few minutes longer. The upgrade process updates one disk at a time on each node for the disk group you have selected to upgrade. Once the upgrade is completed on the first node in the cluster, the process begins on the next node, updating one disk at a time, and so on, until all drives in the cluster have been updated.



**Note:** You might see the Alert message There have been 10 or more cluster services restarts within 15 minutes in the Controller VM as each drive is upgraded and the cluster services are restarted. This message is expected in this case.

## Upgrading Disk Firmware By Using a Nutanix-Provided Shell File

**Before you begin:** Nutanix rarely includes this firmware on the Nutanix Support Portal. Nutanix recommends that you open a case on the Support Portal to request if any firmware updates are available for your platform. Nutanix Support will provide you with metadata (.json) and firmware binary files.

When it is available on the Support Portal from the **Downloads** page, the related metadata and firmware binary files might be contained in an executable shell file. In this case, download the file from the Nutanix Support Portal, then copy the file to and run the file from any controller VM in the cluster. The file extracts the related metadata and firmware binary files, which you use to upgrade the firmware. For example, the file names might be similar to *nfw-intel-ssd-sata-model-version.bin* and *nfw-intel-ssd-sata-model-version.json*.

### 1. Run the Nutanix Cluster Checks (NCC).

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

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

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

### 2. Log on to the web console and open **Upgrade Software** from the gear icon in the web console.

#### 3. Click **Firmware > Disks**.

#### 4. Click the **upload a Firmware binary** link.

#### 5. Click **Choose File** for the extracted metadata and binary files, respectively, browse to the file locations, select the file, and click **Upload Now**.

#### 6. Do one of the following.

- To run only the pre-upgrade installation checks on the Controller VM where you are logged on, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.
- Click **Upgrade > Upgrade Now**, then click **Yes** to confirm.



**Note:** If you have uploaded software or firmware which is already installed or upgraded, the **Upgrade** option is not displayed, as the software or firmware is already installed.

The **Upgrade Software** dialog box shows the progress of your selection, including pre-installation checks.

The disk firmware upgrade process takes approximately five minutes per disk. Controller VM boot disk upgrade might take a few minutes longer. The upgrade process updates one disk at a time on each node for the disk group you have selected to upgrade. Once the upgrade is completed on the first node in the cluster, the process begins on the next node, updating one disk at a time, and so on, until all drives in the cluster have been updated.



**Note:** You might see the Alert message There have been 10 or more cluster services restarts within 15 minutes in the Controller VM as each drive is upgraded and the cluster services are restarted. This message is expected in this case.

## Upgrading NCC Software

### Before you begin:

 **Note:**

- NCC 3.0 is not supported on AOS 4.5.x and previous versions.
- If you are adding one or more nodes to expand your cluster, the latest version of NCC might not be installed on each newly-added node. In this case, re-install NCC in the cluster after you have finished adding the one or more nodes.
- This topic describes how to install NCC software from the Prism web console. To install NCC from the command line, see [Installing NCC from an Installer File](#) on page 84.

 **Note:** To help ensure that Prism Central and each managed cluster are taking advantage of NCC features, ensure that:

- Each node in your cluster is running the same NCC version.
- Prism Central and each cluster managed by Prism Central are all running the same NCC version.

To check the NCC version and optionally upgrade the NCC software version on Prism Central, see the [Prism Central Guide](#), [Upgrading Nutanix Cluster Check \(NCC\) on Prism Central](#) topic.

**1. Run the Nutanix Cluster Checks (NCC).**

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

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

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

**2. Do this step to download and install the NCC upgrade files.**

- Log on to the Prism web console for any node in the cluster.
- Click **Upgrade Software** from the gear icon in the Prism web console, then click **NCC** in the dialog box.
- If an update is available, click **Upgrade Available** and then click **Download**.
- When the download is complete, do one of the following:

- To run only the pre-upgrade installation checks on the controller VM where you are logged on, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.
- Click **Upgrade > Upgrade Now**, then click **Yes** to confirm.

The **Upgrade Software** dialog box shows the progress of your selection, including pre-installation checks.

As part of installation or upgrade, NCC automatically restarts the cluster health service on each node in the cluster, so you might observe notifications or other slight anomalies as the service is being restarted.

#### **Upgrading NCC by Uploading Binary and Metadata Files**

- Do the following steps to download NCC binary and metadata .JSON files from the Nutanix Support Portal, then upgrade NCC through **Upgrade Software** in the Prism web console.

- Typically you would need to perform this procedure if your cluster is not directly connected to the Internet and you cannot download the binary and metadata .JSON files through the Prism web console.

1. Log on to the Nutanix support portal and select **Downloads > Tools & Firmware**.
2. Click the download link to save the binary gzipped TAR (.tar.gz) and metadata (.json) files on your local media.
3. Log on to the Prism web console for any node in the cluster.
4. Click **Upgrade Software** from the gear icon in the Prism web console, then click **NCC** in the dialog box.
5. Click the **upload the NCC binary** link.
6. Click **Choose File** for the NCC metadata and binary files, respectively, browse to the file locations, and click **Upload Now**.
7. When the upload process is completed, click **Upgrade > Upgrade Now**, then click **Yes** to confirm. The **Upgrade Software** dialog box shows the progress of your selection, including pre-installation checks.

As part of installation or upgrade, NCC automatically restarts the cluster health service on each node in the cluster, so you might observe notifications or other slight anomalies as the service is being restarted.

## Installing NCC from an Installer File

### Before you begin:



#### Note:

- NCC 3.0 is not supported on AOS 4.5.x and previous versions.
- If you are adding one or more nodes to expand your cluster, the latest version of NCC might not be installed on each newly-added node. In this case, re-install NCC in the cluster after you have finished adding the one or more nodes.
- This topic describes how to install NCC from the command line. To install NCC software from the web console, see [Upgrading NCC Software](#) on page 82.



**Note:** To help ensure that Prism Central and each managed cluster are taking advantage of NCC features, ensure that:

- Each node in your cluster is running the same NCC version.
- Prism Central and each cluster managed by Prism Central are all running the same NCC version.

To check the NCC version and optionally upgrade the NCC software version on Prism Central, see the **Prism Central Guide**, [Upgrading Nutanix Cluster Check \(NCC\) on Prism Central](#) topic.

You can download the NCC installation file from the Nutanix support portal under **Downloads > Tools & Firmware**. The file type to download depends on the NCC version:



**Tip:** Note the MD5 value of the file as published on the support portal.

- Some NCC versions include a single installer file (*ncc\_installer\_filename.sh*) that you can download and run from any Controller VM.
- Some NCC versions include an installer file inside a compressed tar file (*ncc\_installer\_filename.tar.gz*) that you must first extract, then run from any Controller VM.

- The directory to which you copy the installation package should exist on all nodes in the cluster (/home/nutanix is suggested). Additionally, the folder should be owned by any accounts that uses NCC.

- Download the installation file to any controller VM in the cluster and copy the installation file to the /home/nutanix directory.
- Check the MD5 value of the file. It must match the MD5 value published on the support portal. If the value does not match, delete the file and download it again from the support portal.

```
nutanix@cvm$ md5sum ./ncc_installer_filename.sh
```

- Perform these steps for NCC versions that include a single installer file (*ncc\_installer\_filename.sh*)

- Make the installation file executable.

```
nutanix@cvm$ chmod u+x ./ncc_installer_filename.sh
```

- Install NCC.

```
nutanix@cvm$ ./ncc_installer_filename.sh
```

The installation script installs NCC on each node in the cluster.

NCC installation file logic tests the NCC tar file checksum and prevents installation if it detects file corruption.

- If it verifies the file, the installation script installs NCC on each node in the cluster.
- If it detects file corruption, it prevents installation and deletes any extracted files. In this case, download the file again from the Nutanix support portal.

- Perform these steps for NCC versions that include an installer file inside a compressed tar file (*ncc\_installer\_filename.tar.gz*).

- Extract the installation package.

```
nutanix@cvm$ tar xvmf ncc_installer_filename.tar.gz --recursive-unlink
```

Replace *ncc\_installer\_filename.tar.gz* with the name of the compressed installation tar file.

The `--recursive-unlink` option is needed to ensure old installs are completely removed.

- Run the install script. Provide the installation tar file name if it has been moved or renamed.

```
nutanix@cvm$ ./ncc/bin/install.sh [-f install_file.tar]
```

The installation script copies the *install\_file.tar* tar file to each node and install NCC on each node in the cluster.

- Check the output of the installation command for any error messages.

- If installation is successful, a Finished Installation message is displayed. You can check any NCC-related messages in /home/nutanix/data/logs/ncc-output-latest.log.
- In some cases, output similar to the following is displayed. Depending on the NCC version installed, the installation file might log the output to /home/nutanix/data/logs/ or /home/nutanix/data/serviceability/ncc.

```
Copying file to all nodes [ DONE ]
-----
+-----+
| State | Count |
+-----+
| Total | 1     |
+-----+
Plugin output written to /home/nutanix/data/logs/ncc-output-latest.log
```

```
[ info ] Installing ncc globally.  
[ info ] Installing ncc on 10.130.45.72, 10.130.45.73  
[ info ] Installation of ncc succeeded on nodes 10.130.45.72, 10.130.45.73.
```

### What to do next:

- As part of installation or upgrade, NCC automatically restarts the cluster health service on each node in the cluster, so you might observe notifications or other slight anomalies as the service is being restarted.

## Hypervisor Upgrade Overview and Requirements



#### Note:

- If you have just upgraded your cluster's AOS version, Nutanix recommends that you wait until the **Data Resiliency Status** is green or **OK** (as shown on the Prism web console Home dashboard) before upgrading your hypervisor.
- You cannot perform a manual upgrade of nodes or clusters through Prism Central (if installed and configured). To perform a manual upgrade, log on to the Prism web console for any node in the cluster you are upgrading.

#### *General Workflow to Upgrade the Existing Hypervisor*

- Run the Nutanix Cluster Check (NCC) health checks from any Controller VM in the cluster.
- Download the available hypervisor software from the vendor and the metadata file (JSON) from the Nutanix support portal. If you are upgrading AHV, you can download the binary bundle from the Nutanix support portal.
- Upload the software and metadata through **Upgrade Software**.
- Upgrading the hypervisor restarts each Controller VM as part of the upgrade process.
- The upgrade process upgrades one node at a time, then begins the upgrade process on the next node in the cluster.

#### *Hypervisor Versions in a Cluster*

Ensure that all the hypervisors hosted in your cluster are running the same version (All ESXi hosts running the same version, all AHV hosts running the same version, and so on). Nutanix does not recommend running a major version like ESXi 6.5 on some hosts and running ESXi 6.0 on the remaining hosts in the same cluster for production use. The NCC check `same_hypervisor_version_check` returns a FAIL status in this case. Using the **Upgrade Software** (1-click upgrade) feature would not complete successfully in this case.

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

#### *Guest VMs Running in an Affinity/Anti-Affinity Rules Environment*

- Hypervisor upgrades might not complete successfully in environments where third-party or other applications apply affinity or anti-affinity rules. For example, some anti-virus appliances or architectures might install an anti-virus scanning guest VM on each node in your cluster. This guest VM might not be allowed to power off or migrate from the host being upgraded, causing maintenance mode to time out. In this case, disable such rules or power off such VMs before upgrading.



**Note:** When performing one-click hypervisor upgrades that have AFS, disable the anti-affinity rules on all FSVMs. After the hypervisor successfully upgrades, enable the anti-affinity rules on the FSVMs.

## Auto-provisioning Guest VMs

- Hypervisor upgrades might not complete successfully in environments where applications or scripts are configured to automatically provision guest VMs. For example, if VMware View Composer is configured to automatically provision guest VMs and attempts to place the VMs on a host being upgraded (and placed in maintenance mode), maintenance mode operations might time out, and prevent the upgrade operation. In this case, disable such applications or scripts before upgrading.

## AHV

### AHV Support and Requirements

Hypervisor	Requirements
AHV	<ul style="list-style-type: none"><li>• Use the AHV version available from Nutanix support portal and upgrade through the Prism web console <b>Upgrade Software</b> feature only</li></ul> <p> <b>Note:</b> See <i>Upgrading the KVM Hypervisor to Use Acropolis Features</i> in the <i>AHV Administration Guide</i> if you are currently using a legacy, non-Acropolis version of KVM and want to use AHV and its Acropolis App Mobility Fabric features.</p>

### Checking Your AHV Version

#### How to Check Your AHV Version

Use this procedure	Result
Log in to the hypervisor host and type cat /etc/nutanix-release	For example, the following result indicates that you are running an Acropolis-compatible hypervisor: e16.nutanix.2015412. The minimum result for AHV is e16.nutanix.20150120
Log in to the hypervisor host and type cat /etc/centos-release	For example, the following result indicates that you are running an Acropolis-compatible hypervisor: CentOS release 6.6 (Final). Any result that returns CentOS 6.4 or previous is non-Acropolis (that is, KVM).
Log in to the Prism web console	View the <b>Hypervisor Summary</b> on the home page. If it shows a version of 20150120 or later, you are running AHV.

## VMWare ESXi

### ESXi Support and Requirements

Hypervisor	Requirements
VMware ESXi	<ul style="list-style-type: none"><li>Always consult the VMWare web site for any vCenter and hypervisor installation dependencies. For example, <a href="#">ESXi 5.5 Update 3b</a> requires that you upgrade vCenter first.</li><li>For ESXi hosts, mixing different hypervisor versions in the same cluster is temporarily allowed for deferring a hypervisor upgrade as part of an add-node/expand cluster operation, re-imaging a node as part of a break-fix procedure, planned migrations, and similar temporary operations.</li><li>If you have not enabled DRS in your environment and want to upgrade the ESXi host, you need to upgrade the ESXi host manually. For more information about upgrading ESXi hosts manually, see <a href="#">vSphere Administration Guide</a>.</li><li>If you are mixing nodes with different processor (CPU) types in the same cluster, you must enable 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.</li></ul>

## Microsoft Hyper-V

### Hyper-V Support and Requirements

Hypervisor	Requirements
Microsoft Hyper-V	<ul style="list-style-type: none"><li>The Hyper-V version released with Microsoft Windows Server 2012 R2 is supported</li><li>Upgrade using ISOs</li></ul>

## Upgrading AHV Hosts

**Before you begin:** See [Hypervisor Upgrade Overview and Requirements](#) on page 86.

Do the following steps to download AHV and upgrade the AHV hosts through **Upgrade Software** in the Prism web console.

### 1. Run the Nutanix Cluster Checks (NCC).

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

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

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

2. Log on to the Prism web console and open **Upgrade Software** from the gear icon and click **Hypervisor**.
3. If **Available Compatible Versions** shows a new version of AHV, 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 on without upgrading, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.

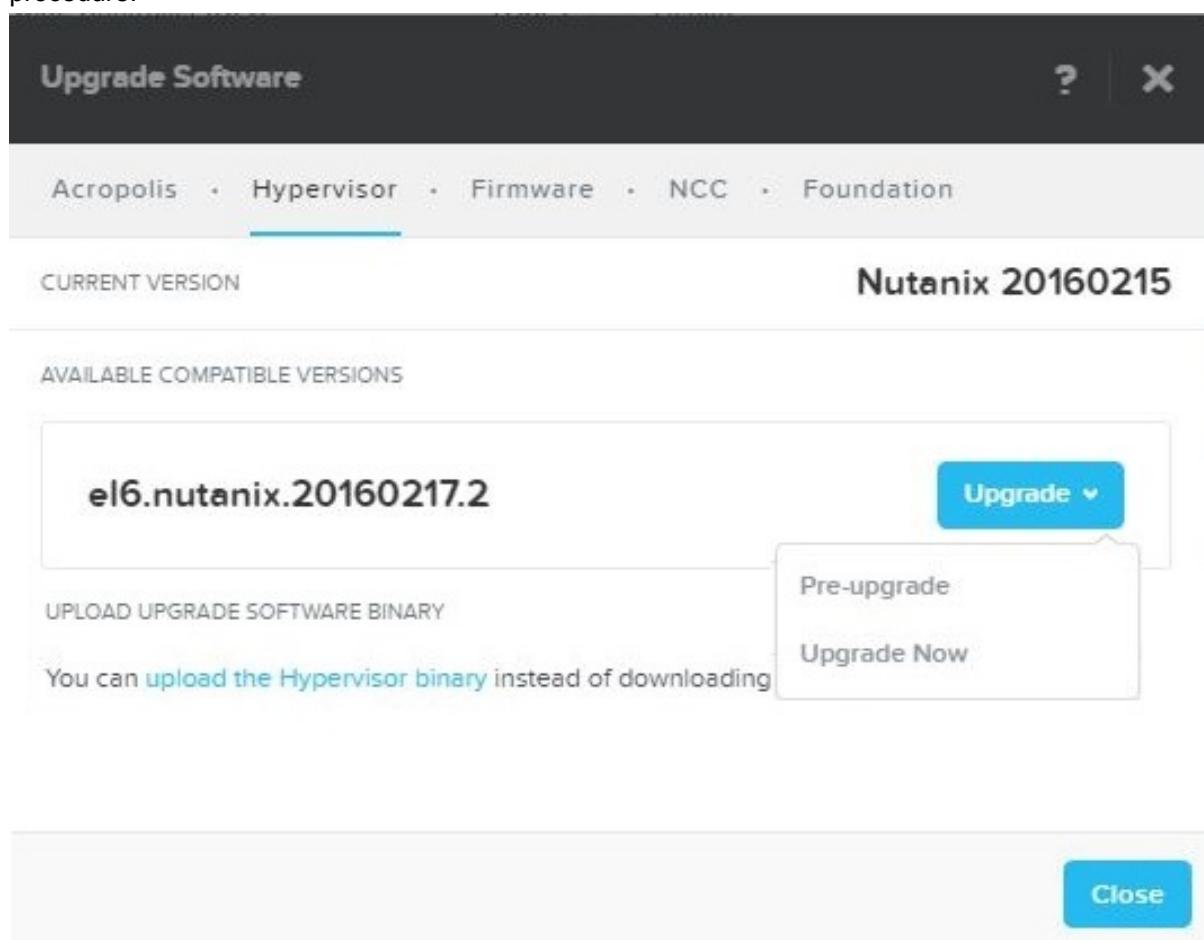


Figure: AHV 1-Click Upgrade

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

#### Upgrading AHV by Uploading Binary and Metadata Files

**Before you begin:** See [Hypervisor Upgrade Overview and Requirements](#) on page 86.

- Do the following steps to download AHV binary and metadata .JSON files from the Nutanix Support Portal, then upgrade AHV through **Upgrade Software** in the Prism web console.
  - Typically you would need to perform this procedure if your cluster is not directly connected to the Internet and you cannot download the binary and metadata .JSON files through the Prism web console.
1. Run the Nutanix Cluster Checks (NCC).

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

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

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

2. Log on to the Nutanix support portal and navigate to the hypervisor details from the **Downloads** menu.
3. Select and download the AHV ISO binary and metadata .JSON files to your local machine or media. You can also copy these files to a USB stick, CD, or other media.
4. In the Prism web console, open **Upgrade Software** from the gear icon and click **Hypervisor**.
5. Click the **upload the Hypervisor binary** link.
6. Click **Choose File** for the metadata and binary files, respectively, browse to the file locations, select the file, and click **Upload Now**.
7. When the file upload is completed, click **Upgrade > Upgrade Now**, then click **Yes** to confirm.

[Optional] When the file upload is completed, to run the pre-upgrade installation checks only on the Controller VM where you are logged on without upgrading, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.



**Note:** AOS can detect if you have uploaded software or firmware which is already installed or upgraded. In this case, the **Upgrade** option is not displayed, as the software or firmware is already installed.

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

## Upgrading ESXi Hosts by Uploading Binary and Metadata Files

**Before you begin:** See [Hypervisor Upgrade Overview and Requirements](#) on page 86.



### Note:

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 web console **Software Upgrade** feature.

Nutanix does not provide ESXi binary files, only related JSON metadata upgrade files. Please obtain ESXi offline bundles (not ISOs) from the VMware web site.

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. Please see the Nutanix hypervisor support statement in our [Support FAQ](#). For updates that are made available by VMware that do not have a Nutanix-provided JSON metadata upgrade file, obtain the offline bundle and md5sum checksum available from VMware, then use the Prism web console **Software Upgrade** feature to upgrade ESXi.

Do the following steps to download Nutanix-qualified ESXi metadata .JSON files and upgrade the ESXi hosts through **Upgrade Software** in the Prism web console. Nutanix does not provide ESXi binary files, only related JSON metadata upgrade files.

- Disable Admission Control to upgrade ESXi on AOS; if enabled, the upgrade process will fail. You can enable it for normal cluster operation otherwise.

- Do not perform any cluster upgrades (AOS, Controller VM memory, hypervisor, and so on) if you have just registered your cluster in vCenter. Wait at least one hour before performing upgrades to allow cluster settings to become updated. Also do not register the cluster in vCenter and perform any upgrades at the same time.

1. Run the Nutanix Cluster Checks (NCC).

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

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

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

2. Log on to the Nutanix support portal and navigate to the hypervisor details from the **Downloads** menu.
3. Select and download the Nutanix-qualified ESXi metadata .JSON files to your local machine or media. You can also copy these files to a USB stick, CD, or other media.
4. Log on to the Prism web console and open **Upgrade Software** from the gear icon and click **Hypervisor**.
5. Click the **upload the Hypervisor binary** link.
6. Click **Choose File** for the metadata and binary files (obtained from VMware), respectively, browse to the file locations, select the file, and click **Upload Now**.
7. When the file upload is completed, 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 on without upgrading, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.
8. Type your vCenter IP address and credentials, then click **Upgrade**.

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



**Note:** AOS can detect if you have uploaded software or firmware which is already installed or upgraded. In this case, the **Upgrade** option is not displayed, as the software or firmware is already installed.

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

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

**Before you begin:** See [Hypervisor Upgrade Overview and Requirements](#) on page 86.

- Do the following steps to download a non-Nutanix-qualified (patch) ESXi upgrade offline bundle from VMWare from the Nutanix Support Portal, then upgrade ESXi through **Upgrade Software** in the Prism web console.
- Typically you would need to perform this procedure if you need to patch your version of ESXi and Nutanix has yet to officially qualify 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.

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 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. In the Prism web console, open **Upgrade Software** from the gear icon and click **Hypervisor**.
4. Click the **upload the Hypervisor binary** link.
5. Click **enter md5 checksum** and copy the MD5 checksum into the **Hypervisor MD5 Checksum** field.
6. Scroll down and click **Choose File** for the binary file, browse to the offline bundle file location, select the file, and click **Upload Now**.

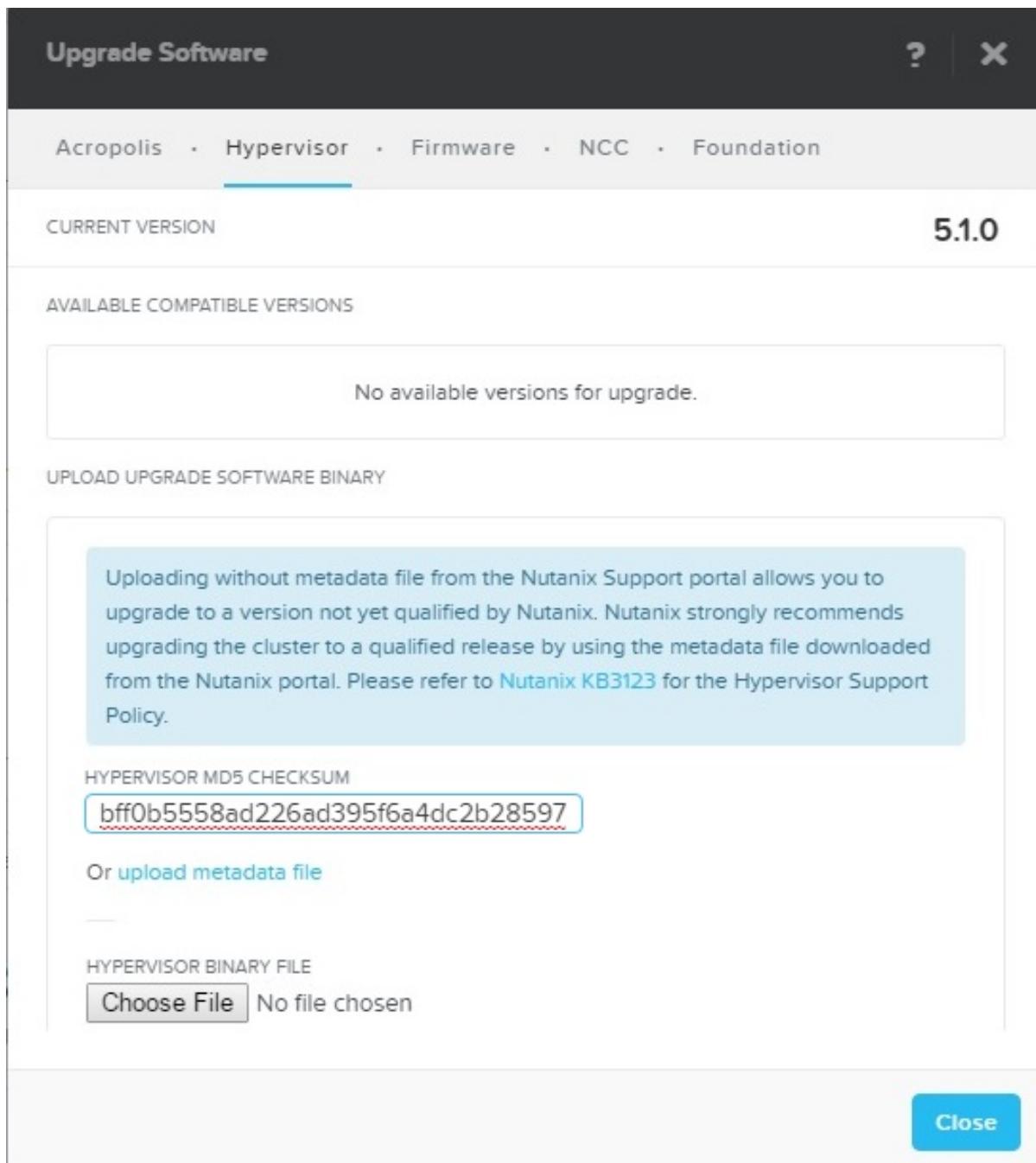


Figure: ESXi 1-Click Upgrade, Unqualified Bundle

7. When the file upload is completed, 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 on without upgrading, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.
8. Type your vCenter IP address and credentials, then click **Upgrade**.  
Ensure that you are using your Active Directory or LDAP credentials in the form of domain\username or username@domain.



**Note:** AOS can detect if you have uploaded software or firmware which is already installed or upgraded. In this case, the **Upgrade** option is not displayed, as the software or firmware is already installed.

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

## Upgrading Hyper-V Hosts

**Before you begin:** See [Hypervisor Upgrade Overview and Requirements](#) on page 86.

This procedure enables you to update Hyper-V through the Prism web console **Upgrade Software** dialog box.

1. Run the Nutanix Cluster Checks (NCC).

→ From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.

→ Log in to a Controller VM and use the ncc CLI.

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

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

2. Download the Microsoft Hyper-V Windows Server .ISO file from the Microsoft web site.

3. Log on to the Nutanix support portal and select the hypervisor metadata .JSON file from the **Downloads** menu.

4. Save the files to your local machine or media, such as a USB drive or other portable media.

5. In the Prism web console, open **Upgrade Software** from the gear icon and click **Hypervisor**.

6. Click the **upload a Hypervisor binary** link.

7. Click **Choose File** for the metadata and binary files, respectively, browse to the file locations, select the file, and click **Upload Now**.

8. [Optional] When the file upload is completed, to run the pre-upgrade installation checks only on the Controller VM where you are logged on without upgrading, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.

9. When the file upload is completed, click **Upgrade > Upgrade Now**, then click **Yes** to confirm.



**Note:** AOS can detect if you have uploaded software or firmware which is already installed or upgraded. In this case, the **Upgrade** option is not displayed, as the software or firmware is already installed.

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



**Note:** Manual update ESXi for incremental patches are now available through one-click. It is not a need for manual upgrade of AOS or Hyper-V.

## Upgrading XenServer Hosts

This procedure enables you to update XenServer through the Prism web console **Upgrade Software** dialog box.

**Before you begin:** See [Hypervisor Upgrade Overview and Requirements](#) on page 86.

**1. Run the Nutanix Cluster Checks (NCC).**

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

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

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

**2. Download the XenServer .ISO file from the Citrix web site.**

**3. Log on to the Nutanix support portal and select the hypervisor metadata .JSON file from the **Downloads** menu.**

**4. Save the files to your local machine or media, such as a USB drive or other portable media.**

**5. In the Prism web console, open **Upgrade Software** from the gear icon and click **Hypervisor**.**

**6. Click the **upload a Hypervisor binary** link.**

**7. Click **Choose File** for the metadata and binary files, respectively, browse to the file locations, select the file, and click **Upload Now**.**

**8. [Optional] When the file upload is completed, to run the pre-upgrade installation checks only on the Controller VM where you are logged on without upgrading, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.**

**9. When the file upload is completed, click **Upgrade > Upgrade Now**, then click **Yes** to confirm.**



**Note:** AOS can detect if you have uploaded software or firmware which is already installed or upgraded. In this case, the Upgrade option is not displayed, as the software or firmware is already installed.

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

## Applying XenServer Patches

To apply the XenServer patches to your XenServer nodes in the Nutanix cluster, first upload the XenServer patch to one of the XenServer nodes in the cluster, apply the patches to all the XenServer nodes, and then restart the XenServer nodes by using the Prism web console. The Request Reboot operation in the Prism web console restarts each XenServer node one after the other.

You can upload and apply a XenServer patch by either using the XenServer command line or XenCenter.

Perform the following procedure to apply a XenServer patch by using the XenServer command line.

- 1. Download the XenServer .ISO patch file from the Citrix website.**
- 2. Log on to one of the XenServer nodes in the cluster with SSH.**
- 3. Upload the XenServer .ISO patch file to the XenServer node.**

```
root@host# xe update-upload file-name=xenserver-patch-iso-file-name
```

Replace *xenserver-patch-iso-file-name* with the name of the XenServer .ISO patch file.

**4.** Determine the UUID of the patch.

```
root@host# xe update-list
```

An output similar to the following is displayed.

```
uuid ( RO)          : 9e365284-c927-445e-adbc-fa9d7a2fb8af
name-label ( RO)     : test-hotfix-basic-3
name-description ( RO) : Simple basic hotfix with a single package, host reboot
installation-size ( RO) : 32
hosts (SRO)         : after-apply-guidance (SRO): restartHost
```

**5.** Determine the UUID of the XenServer hosts.

```
root@host# xe host-list
```

**6.** Apply the patch to all the XenServer nodes in the cluster.

```
root@host# xe update-apply host=host-uuid uuid=uuid-of-the-patch
```

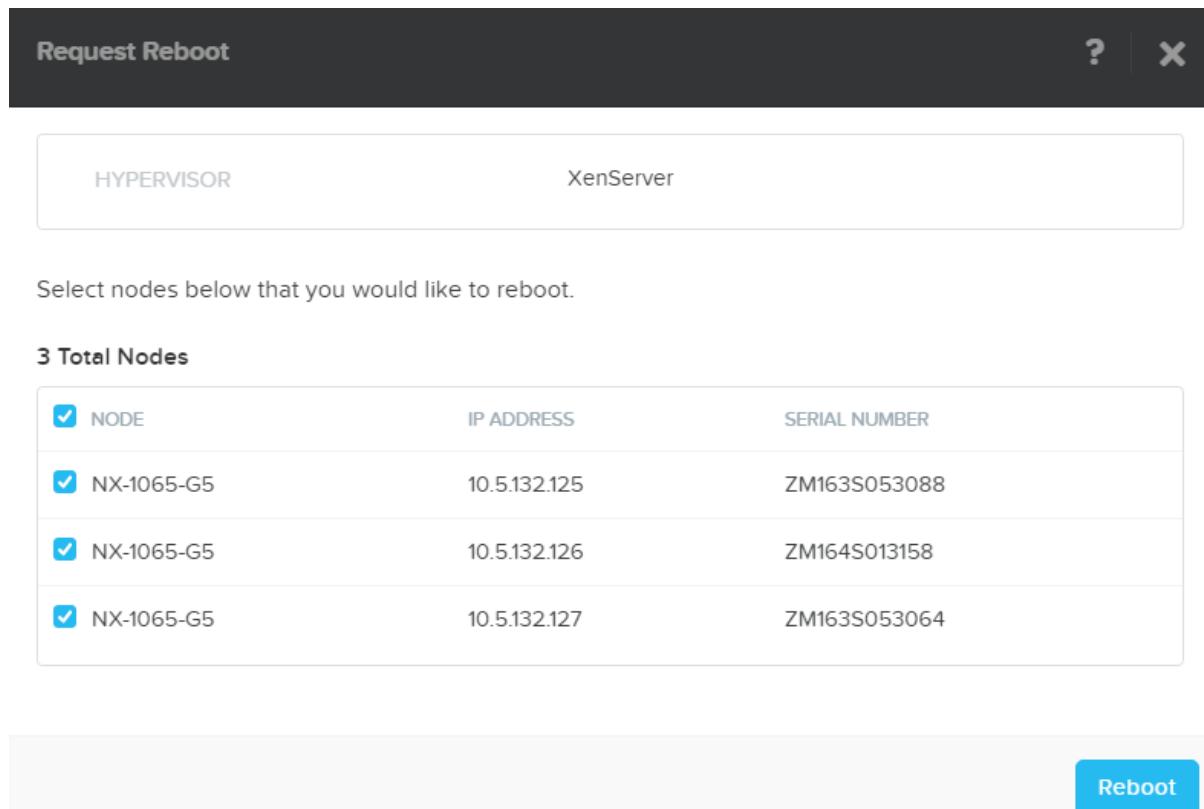
Replace *host-uuid* with the UUID of the host and *uuid-of-the-patch* with the UUID of the XenServer patch.

Repeat this step for all the XenServer hosts to which you want to apply the patch.

**7.** Log on to the Prism web console.

**8.** In the gear icon drop-down list, click **Request Reboot**.

**9.** In the **Request Reboot** window, select all the nodes to which you want to apply the patch, and click **Reboot**.



*Figure:*

A progress bar is displayed that indicates the progress of the restart of each node.

#### Applying XenServer Patches by Using XenCenter

Perform the following procedure to apply a XenServer patch by using XenCenter.

1. Download the XenServer .ISO patch file from the Citrix website.
2. Start a XenCenter session on your workstation.
3. On the XenCenter homepage, select the cluster on which you want to apply the XenServer patch and go to **Tools > Install Update**.
4. Follow the prompts in XenCenter to upload the XenServer patch, select the nodes to which you want to apply the patch, and apply the patch to the XenServer nodes.
5. Log on to the Prism web console.
6. In the gear icon drop-down list, click **Request Reboot**.
7. In the **Request Reboot** window, select all the nodes to which you want to apply the patch, and click **Reboot**.

The screenshot shows the 'Request Reboot' dialog box. At the top, there are buttons for help (?) and close (X). Below the title, there are two tabs: 'HYPERVISOR' and 'XenServer'. The 'XenServer' tab is selected. A message says 'Select nodes below that you would like to reboot.' Below this, a table lists '3 Total Nodes':

NODE	IP ADDRESS	SERIAL NUMBER
NX-1065-G5	10.5.132.125	ZM163S053088
NX-1065-G5	10.5.132.126	ZM164S013158
NX-1065-G5	10.5.132.127	ZM163S053064

In the bottom right corner of the dialog box is a blue 'Reboot' button.

Figure: Reboot XenServer nodes to apply XenServer patches

A progress bar is displayed that indicates the progress of the restart of each node.

## Upgrading BMC or BIOS Firmware

**Before you begin:** See these topics for information about AOS and hypervisor upgrades that might also apply before you perform a firmware upgrade:

- [AOS Upgrade Prerequisites](#) on page 78
- [Hypervisor Upgrade Overview and Requirements](#) on page 86
- The Prism web console supports upgrading the base management controller (BMC) firmware on clusters running Foundation 3.6 or later. Check the current Foundation version by clicking the gear icon, then click **Upgrade Software > Foundation**. Otherwise, the BMC update must be performed manually. The procedure is described in the [Nutanix BMC Manual Upgrade Guide](#).
- The firmware updates (BMC or BIOS) are not supported on the single-node replication target clusters.
- Nutanix occasionally provides updated BIOS and BMC firmware. Nutanix rarely includes this firmware on the Nutanix Support Portal. Use this procedure to easily check if updates are available there, then install them if available.
- Update the BMC firmware first. After successfully updating the BMC firmware, you can update the BIOS firmware.
- The 1-Click upgrade for BIOS firmware feature is available for AHV, Hyper-V, and ESXi hypervisor host environments running on NX-xxxx-G4 (Haswell) or NX-xxxx-G5 (Broadwell) platforms only.
- For Hyper-V clusters where you are using System Center Virtual Machine Manager (SCVMM), ensure that the SCVMM instance (VM or physical host) includes a minimum 4 vCPUs and 2 GB RAM.
- Nutanix recommends that you open a case on the Support Portal to request if any firmware updates are available for your platform. If you receive updated firmware from Nutanix Support, use the procedure described in [Upgrading BMC or BIOS Firmware by Uploading Binary and Metadata Files](#).
- Ensure that the cluster is back to full health before performing these procedures on the next cluster.

**1.** Run the Nutanix Cluster Checks (NCC).

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

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

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

**2.** Log on to the web console for any node in the cluster.

- 3.** Open **Upgrade Software** from the gear icon in the web console.
- 4.** Click **Firmware > BMC or Firmware > BIOS** in the dialog box for the firmware type you are upgrading.
- 5.** If an update is available, click **Upgrade Available** and then click **Download**.

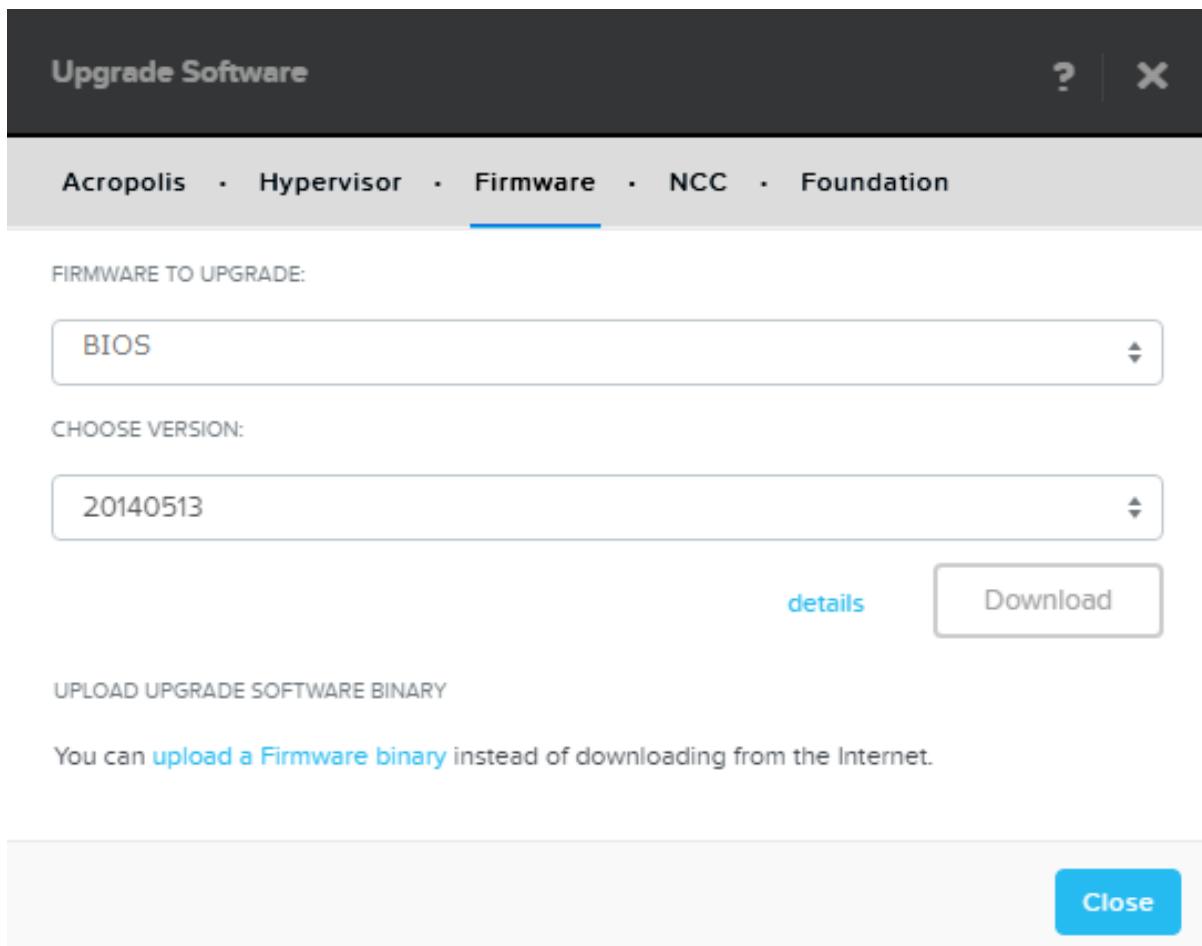


Figure: Upgrade Software dialog box

6. When the download is complete, do one of the following.

- To run the pre-upgrade installation checks only on the Controller VM where you are logged on, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.
- Click **Upgrade > Upgrade Now**, then click **Yes** to confirm.



**Note:** AOS can detect if you have uploaded software or firmware which is already installed or upgraded. In this case, the **Upgrade** option is not displayed, as the software or firmware is already installed.

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

The upgrade process updates one node at a time. Once the upgrade is completed on the first node in the cluster, the process begins on the next node, and so on, until all nodes in the cluster have been updated. The total amount of time for the upgrade operation to complete is dependent on your environment (cluster size, number of VMs, and so on).

7. If you have upgraded the BMC firmware, repeat these steps to upgrade the BIOS firmware (select **Firmware > BIOS** in the dialog box).

#### Upgrading BMC or BIOS Firmware by Uploading Binary and Metadata Files

**Before you begin:** See these topics for information about AOS and hypervisor upgrades that might also apply before you perform a firmware upgrade:

- [AOS Upgrade Prerequisites](#) on page 78
- [Hypervisor Upgrade Overview and Requirements](#) on page 86
- Nutanix recommends that you open a case on the Support Portal to request if any firmware updates are available for your platform. If you receive updated firmware from Nutanix Support, use this procedure to upgrade the BIOS through **Upgrade Software** in the Prism web console.
- The Prism web console supports upgrading the base management controller (BMC) firmware on clusters running Foundation 3.6 or later. Check the current Foundation version by clicking the gear icon, then click **Upgrade Software > Foundation**. Otherwise, the BMC update must be performed manually. The procedure is described in the [Nutanix BMC Manual Upgrade Guide](#).
- Update the BMC firmware first. After successfully updating the BMC firmware, you can update the BIOS firmware.
- The firmware updates (BMC or BIOS) are not supported on the single-node replication target clusters.

1. Run the Nutanix Cluster Checks (NCC).

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

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

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

2. Obtain the firmware and metadata files from Nutanix Support by opening a case from the Support Portal.
3. Log on to the web console and open **Upgrade Software** from the gear icon in the web console.
4. Click **Firmware > BMC or Firmware > BIOS** in the dialog box for the firmware type you are upgrading.
5. Click the **upload a Firmware binary** link.
6. Click **Choose File** for the metadata and binary files, respectively, browse to the file locations, select the file, and click **Upload Now**.
7. When the file upload is completed, do one of the following.
  - To run the pre-upgrade installation checks only on the Controller VM where you are logged on, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.
  - Click **Upgrade > Upgrade Now**, then click **Yes** to confirm.



**Note:** If you have uploaded software or firmware which is already installed or upgraded, the **Upgrade** option is not displayed, as the software or firmware is already installed.

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

The upgrade process updates one node at a time. Once the upgrade is completed on the first node in the cluster, the process begins on the next node, and so on, until all nodes in the cluster have been updated. The total amount of time for the upgrade operation to complete is dependent on your environment (cluster size, number of VMs, and so on).

8. If you have upgraded the BMC firmware, repeat these steps to upgrade the BIOS firmware (select **Firmware > BIOS** in the dialog box).

## Upgrading Foundation

### 1. Run the Nutanix Cluster Checks (NCC).

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

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

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

### 2. Log on to the Prism web console, open **Upgrade Software** from the gear icon, then click **Foundation**.

#### 3. If an update is available, click **Upgrade Available** and then click **Download**.

#### 4. When the download is complete, click **Upgrade > Upgrade Now**, then click **Yes** to confirm.

To run the pre-upgrade installation checks only on the controller VM where you are logged on, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.

The **Upgrade Software** dialog box shows the progress of your selection, including pre-installation checks.

### Upgrading Foundation by Uploading Binary and Metadata Files

- Do the following steps to download the Foundation binary gzipped TAR (.tar.gz) file from the Nutanix Support Portal, then upgrade AOS through **Upgrade Software** in the Prism web console.
- Typically you would need to perform this procedure if your cluster is not directly connected to the Internet and you cannot download the binary file through the Prism web console.

### 1. Log on to the Nutanix support portal and select **Downloads > Foundation**

### 2. Click the download link to save the binary gzipped TAR (.tar.gz) file on your local media. You can also copy these files to a USB stick, CD, or other media.

### 3. Log on to the Prism web console, open **Upgrade Software** from the gear icon, then click **Foundation**.

### 4. Click the **upload the Foundation binary** link.

### 5. Click **Choose File** for the binary file, browse to the file location, and click **Upload Now**.

### 6. When the upload process is completed, click **Upgrade > Upgrade Now**, then click **Yes** to confirm. To run the pre-upgrade installation checks only on the controller VM where you are logged on, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.

The **Upgrade Software** dialog box shows the progress of your selection, including pre-installation checks.

## Upgrading HBA Firmware

**Before you begin:** Nutanix rarely includes this firmware on the Nutanix Support Portal. Nutanix recommends that you open a case on the Support Portal to request if any firmware updates are available for your platform. Nutanix Support will provide you with metadata (.json) and firmware binary files.

- The HBA firmware upgrade feature is available for AHV and ESXi hypervisor host environments running on NX-xxxx G4 (Haswell) or NX-xxxx-G5 (Broadwell) platforms only.
- Ensure that the cluster is back to full health before performing this procedures on the next cluster.

- Ensure that the **Data Resiliency Status** is **OK** in the Prism Web Console for the cluster before performing this procedure.

1. Run the Nutanix Cluster Checks (NCC).

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

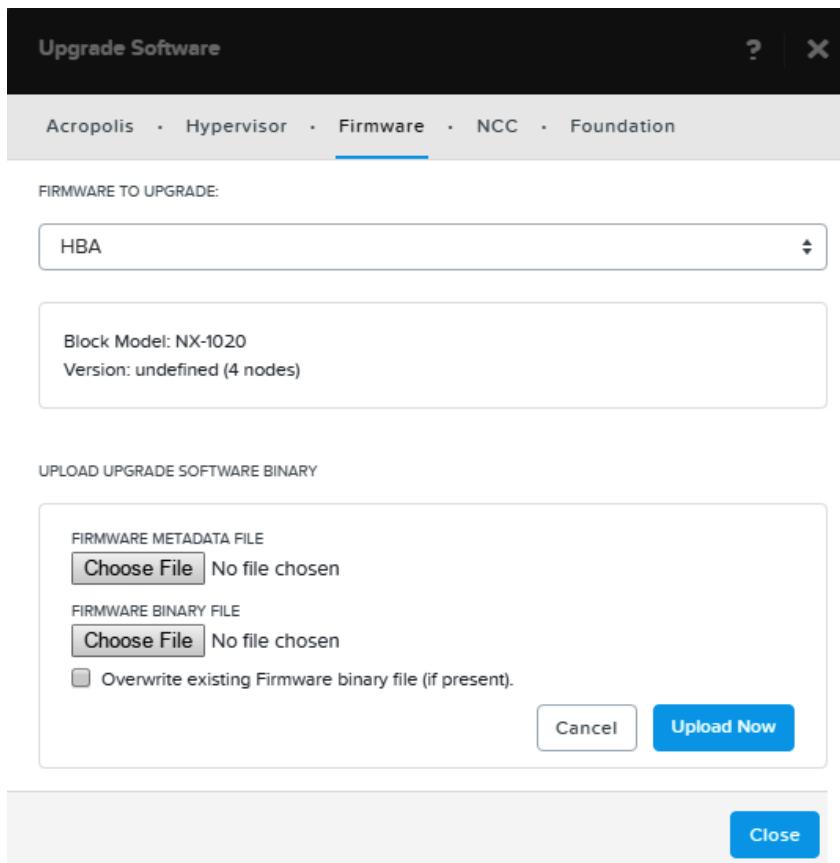
```
nutanix@cvm$ ncc health_checks run_all
```

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

2. Log on to the web console and open **Upgrade Software** from the gear icon in the web console.

3. Click **Firmware > HBA**.

4. Click the **upload a Firmware binary** link.



*Figure: Upgrade Software dialog box*

5. Click **Choose File** for the metadata and binary files, respectively, browse to the file locations, select the file, and click **Upload Now**.
6. Do one of the following.
  - To run only the pre-upgrade installation checks on the Controller VM where you are logged on, click **Upgrade > Pre-upgrade**. These checks also run as part of the upgrade procedure.
  - Click **Upgrade > Upgrade Now**, then click **Yes** to confirm.

The **Upgrade Software** dialog box shows the progress of your selection, including pre-installation checks.

## Viewing the Progress of the Download or Upgrade Process

**Note:** As part of the AOS upgrade, the node where you have logged on and initiated the upgrade restarts. The Prism 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 web console again.

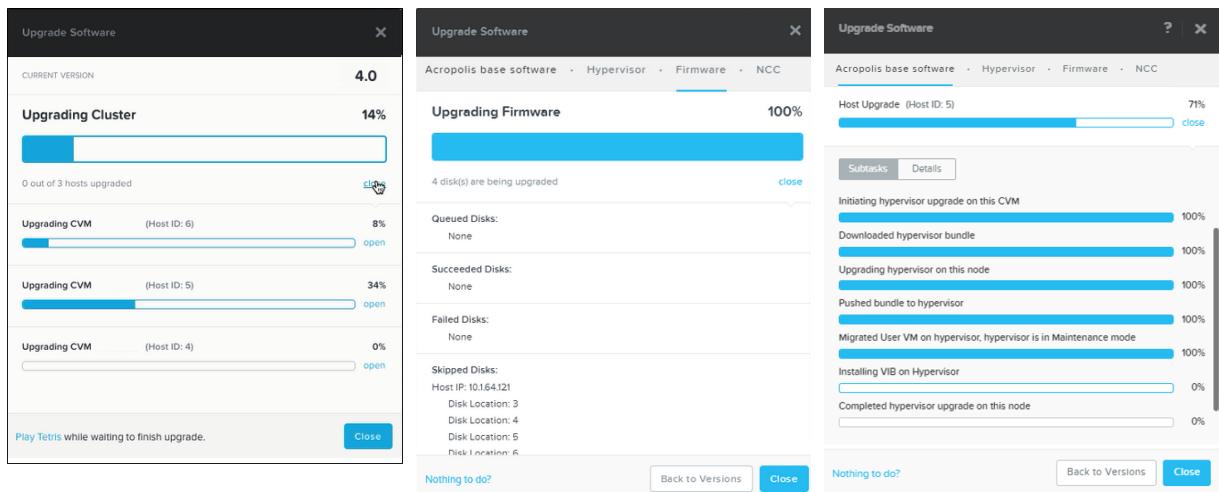
You can see the progress of the download or upgrade process through one of the following:

- **Upgrade Software** dialog box
- **Alerts** summary on the main menu

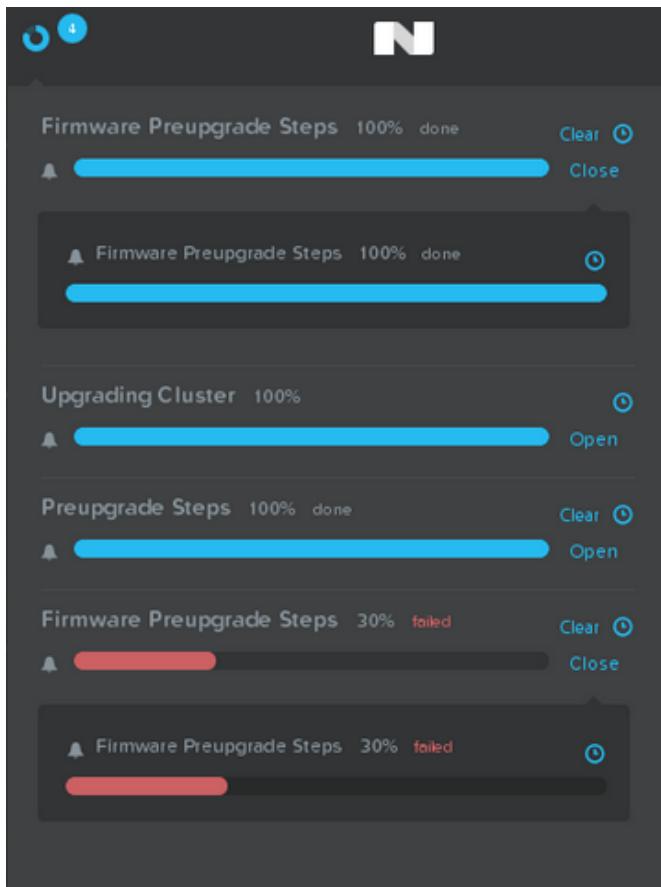
### 1. Under the **Upgrade Software** dialog box progress bar, click **Open**.

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

#### Upgrade Progress



2. Click **open** to see progress including download, installation, and upgrade completion progress bars.
3. 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.
4. Click the **Alerts** summary on the main menu.
5. Click **Open** to see progress details, including download, installation, and upgrade completion progress bars.



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

#### Pausing an In-Progress Download

1. If a software download is in progress, do one of the following:
  - Open **Upgrade Software** from the gear icon in the Prism 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

In some cases, you might need to delete a downloaded software or firmware 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.

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, firmware, 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. The multi-cluster view, known as *Prism Central*, is a centralized management tool that runs as a separate VM. *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 drill-down options to view detailed information about individual entities
- Multi-cluster analytics capabilities
- Multi-cluster alerts summary with drill-down options to view information about possible causes and corrective actions for each alert
- Ability to configure individual clusters through direct *Prism Central* actions (for selected administrative tasks) or through one-click access to the web console for a cluster



**Note:** See the *Prism Central Guide* for more information about *Prism Central*.

### Register (Unregister) with Prism Central

#### Before you begin:

- Log in to the web console as the user `admin`.
- If you enable client authentication on a registered cluster, it interferes when communicating with *Prism Central*. Therefore, do not enable authentication on any registered clusters.
- Port 9440 needs to be open in both directions between the *Prism Central* VM and any registered clusters.

A cluster must be registered with *Prism Central* to be included in that multi-cluster group. To register a cluster, do the following:

1. Run the Nutanix Cluster Checks (NCC).
  - From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
  - Log in to a Controller VM and use the `ncc` CLI.

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

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

2. Log into the web console as the user `admin` for a cluster.
3. Do one of the following:
  - a. Select **Prism Central Registration** from the gear icon pull-down list of the main menu.

- b. On the **Home** dashboard, click **Register** from the **Prism Central** widget, then click **Connect to an existing Prism Central**.

The *Prism Central Registration* dialog box appears.

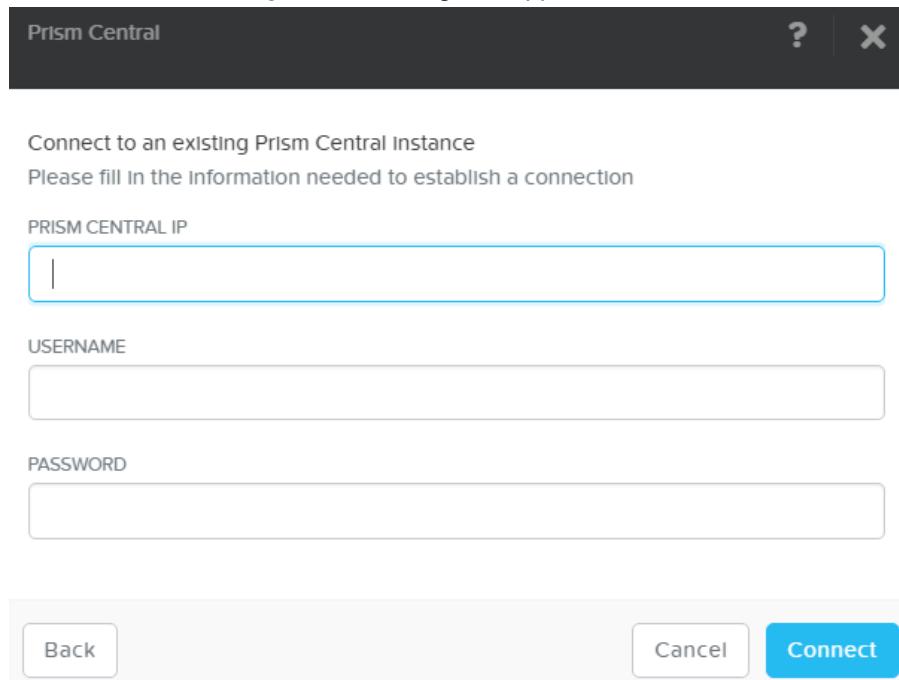


Figure: Prism Central Registration Window

4. To register a cluster, do the following in the indicated fields:
  - a. **Prism Central IP:** Enter the IP address of the *Prism Central* VM.
  - b. **Username:** Enter the *Prism Central* VM user logon name.
  - c. **Password:** Enter the *Prism Central* VM user password.
5. When all the fields are correct, click the **Connect** button to save the values and close the window. This registers the cluster on the specified *Prism Central* VM and allows the passing of information between the cluster and *Prism Central*.

#### Unregistering from Prism Central

To unregister a cluster from an existing instance of *Prism Central*, do the following.

1. Log into the web console as the user **admin** for a cluster.
2. In the gear icon pull-down list of the main menu, select **Prism Central Registration**. The *Prism Central Registration* dialog box appears.

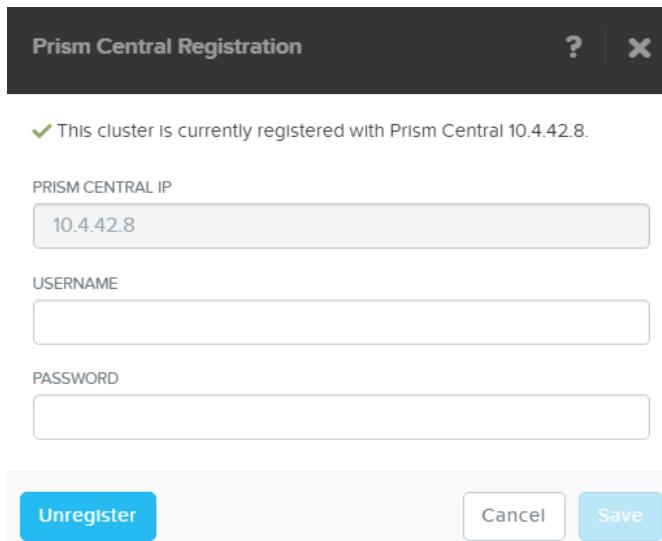


Figure: Prism Central Registration Window (unregister)

3. Type the user name and password for *Prism Central* in the **Username** and **Password** fields.

4. Click the **Unregister** button.



**Note:** If the *Prism Central* IP address changes after registering, you must unregister and then re-register the cluster with the new IP address.

#### Unregistering from a Deleted or Destroyed Prism Central VM

To unregister a cluster from a instance of *Prism Central* that you have deleted or destroyed, do the following.

1. Log on to any Controller VM of the registered cluster through an SSH session.

2. Obtain Prism Central's cluster ID (*cluster\_id*), then delete the cluster state.

```
nutanix@cvm$ ncli multicluster get-cluster-state
```

```
nutanix@cvm$ ncli multicluster delete-cluster-state cluster-id=cluster_id
```

After performing these steps, the cluster is not registered with a *Prism Central* server. The `ncli multicluster get-cluster-state` command should not return a cluster ID. You can now re-register with a new or re-created *Prism Central* VM.



**Note:** If the *Prism Central* IP address changes after registering, you must unregister and then re-register the cluster with the new IP address.

#### Increasing the Cluster Fault Tolerance Level

If you have a cluster set to Fault Tolerance one (FT1), you have the option to increase the cluster to FT2. Redundancy factor 3 is only supported in clusters that have FT2. This topic describes how to increase the cluster FT level.



**Note:**

- If you enabling block awareness in addition to increasing the FT level, you need a minimum of 5 blocks.

- Increasing the cluster FT level might require at least 30% of your disk space.
- Clusters must have a minimum of five nodes.
- Changes to Fault Tolerance cannot be reverted.

1. To view the number of host failures that Zookeeper can tolerate, open a web browser and log on to the Prism web console. Click **Data Resiliency** on the main dashboard to display the *Data Resiliency Status* window.

The screenshot shows the 'Data Resiliency Status' window with two sections: 'Fault Domain Type: Host' and 'Fault Domain Type: Block'. The 'Host' section contains a table with columns: COMPONENT, FAILURES TOLERABLE, and MESSAGE. The 'Block' section also has a similar table. The 'ZooKeeper' row in the 'Host' section is highlighted with a red box.

COMPONENT	FAILURES TOLERABLE	MESSAGE
Static Configuration	1	
Extent Groups	1	
Erasure Code Strip Size	1	
Metadata	1	
ZooKeeper	1	
Stargate Health	1	
Oplog	1	
Free Space	1	

COMPONENT	FAILURES TOLERABLE	MESSAGE
-----------	--------------------	---------

Figure: Data Resiliency Status window (RF 2)

2. To increase the cluster from redundancy factor 2 to redundancy factor 3, log on to any Controller VM in the cluster through SSH and start the nCLI.
3. To view the cluster redundancy factor state:

```
ncli> cluster get-redundancy-state
```

Output similar to the following shows redundancy factor 2.

```
Current Redundancy Factor : 2
Desired Redundancy Factor : 2
Redundancy Factor Status   : kCassandraPrepareDone=true;kZookeeperPrepareDone=true
```

4. Set the cluster to redundancy factor 3.



**Note:** Increasing the cluster FT level take up significant disk space. Be sure there is enough disk space.

```
ncli> cluster set-redundancy-state desired-redundancy-factor=3
```

Output similar to the following is displayed.

```
Current Redundancy Factor : 2  
Desired Redundancy Factor : 3  
Redundancy Factor Status : -
```

The nCLI output might take several minutes to update the redundancy factor.

5. Verify that the redundancy factor is now 3.

```
ncli> cluster get-redundancy-state
```

Output similar to the following shows redundancy factor 3.

```
Current Redundancy Factor : 3  
Desired Redundancy Factor : 3  
Redundancy Factor Status : kCassandraPrepareDone=true;kZookeeperPrepareDone=true
```

The process of increasing the cluster redundancy factor can take hours to complete because it must replicate metadata across the ring. You can check the status by again going to the *Data Resiliency Status* window in Prism. When the Zookeeper failures tolerable value increases to 2 as in the following example, it confirms that the redundancy factor is now 3.

Data Resiliency Status		
Fault Domain Type: Host		
COMPONENT	FAILURES TOLERABLE	MESSAGE
Static Configuration	2	
ZooKeeper	2	
Stargate Health	2	
Oplog	2	
Erasure Code Strip Size	2	
Extent Groups	1	Based on placement of extent group replicas the cluster can tolerate a maximum of 1 node failure(s)
Metadata	2	
Free Space	2	

Fault Domain Type: Block		
		OK

Figure: Data Resiliency Status window (RF 3)

6. Update the replication factor to 3 for the target (desired) storage containers.

Increasing the redundancy factor for the cluster does not automatically increase the container replication factor, because you might have some containers where two copies is sufficient, and you do not want to incur the overhead of a third copy for those containers. Therefore, you need to increase the replication factor to 3 for any containers you want to keep a third copy of the data.

a. Locate the storage container(s) to update.

```
ncli> ctr list
```

Output similar to the following is displayed.

Id	:	00052e5a-bc71-2112-0000-0000000261a::11
Uuid	:	c49eb9af-2eba-41b1-bae5-08227f7cff13
Name	:	storage_container_name
Storage Pool Id	:	00052e5a-bc71-2112-0000-0000000261a::10
Storage Pool Uuid	:	b785ff57-9d53-4f05-bad7-3ac3587f2960
Free Space (Logical)	:	10.29 TiB (11,316,325,361,581 bytes)
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	:	
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-SATA
Compression	:	off
Fingerprint On Write	:	off
On-Disk Dedup	:	none
Erasure Code	:	off

- b. For each target storage container, set the replication factor to 3.

```
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
Uuid	:	a567b66d-b356-4883-90c5-c37b2f3e0fad
Name	:	<i>storage_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
Random I/O Pri Order	:	SSD-PCIe, SSD-SATA, DAS-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

As with increasing the redundancy factor, increasing the replication factor can take some time to complete. You can verify the status by again going to the *Data Resiliency Status* window in Prism. When the Extent Groups failures tolerable value (which reflects the container replication level) increases to 2, it confirms that the replication factor is now 3.

## Increasing Controller VM Memory Size

**Before you begin:** If your cluster is running the ESXi hypervisor and you are managing your cluster by using VMware vCenter, download and run the `get_vcenter_info` script as described in Knowledge Base article [KB 4332](#). You will need the IP address and administrator credentials of your vCenter instance.

You can increase memory reserved for each Controller VM in your cluster by using the 1-click Controller VM Memory Upgrade available from the Prism web console. Increase memory size depending on the workload type or to enable certain AOS features. See the *Controller VM Memory Configurations* topic in the *Acropolis Advanced Administration Guide*.

For nodes with ESXi hypervisor hosts with total physical memory of 64 GB, the Controller VM can be upgraded to a maximum 28 GB.

**1.** Run the Nutanix Cluster Checks (NCC).

- From the Prism web console Health page, select **Actions > Run Checks**. Select **All checks** and click **Run**.
- Log in to a Controller VM and use the ncc CLI.

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

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

**2.** Log on to the web console for any node in the cluster.

**3.** Open **Configure CVM** from the gear icon in the web console.

The *Configure CVM* dialog box is displayed.

**4.** Select the **Target CVM Memory Allocation** memory size and click **Apply**.

The values available from the drop-down menu can range from 16 GB to the maximum available memory in GB.

AOS applies memory to each Controller VM that is below the amount you choose.

If a Controller VM was already allocated more memory than your choice, it remains at the memory amount. For example, selecting **28 GB** upgrades any Controller VM currently at 20 GB. A Controller VM with a 48 GB memory allocation remains unmodified.

## Storage Management

Storage in a Nutanix cluster is organized hierarchically into several components that allow you to manage data storage and performance characteristics.

- Nutanix clusters contain storage pool, storage container, and virtual disk components to organize storage across hardware (disk type) tiers. (see [Storage Components](#) on page 113).
- The web console allows you to monitor storage usage across the cluster (see [Storage Dashboard](#) on page 119).
- You can create storage pools (see [Creating a Storage Pool](#) on page 138), storage containers (see [Creating a Storage Container](#) on page 139), and volume groups (see [Creating a Volume Group](#) on page 147) through the web console.

### Storage Components

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

#### **Storage Tiers**

Storage tiers define the type of physical storage that is available. You can determine the tier breakdown for disks in a storage pool through the web console (see [Storage Table View](#) on page 129). The tiers depend on the Nutanix model type and can include the following:

#### **Storage Pools**

Storage pools are groups of physical disks from one or more tiers (see [Creating a Storage Pool](#) on page 138). Storage pools provide physical separation between virtual machines because a storage device can only be assigned to a single storage pool at a time. Nutanix recommends creating a single storage pool to hold all disks within the cluster. This configuration, which supports the majority of use cases, allows the cluster to dynamically optimize the distribution of resources like capacity and IOPS. Isolating disks into separate storage pools provides physical separation between VMs, but can also create an imbalance of these resources if the disks are not actively used. When you expand your cluster by adding new nodes, the new disks can also be added to the existing storage pool. This scale-out architecture allows you to build a cluster that grows with your needs.

#### **Storage Containers**

A storage container is a subset of available storage within a storage pool (see [Creating a Storage Container](#) on page 139). Storage containers hold the virtual disks (vDisks) used by virtual machines. Selecting a storage pool for a new storage container defines the physical disks where the vDisks are stored. Nodes in the Nutanix cluster can mount a storage container as an NFS datastore (vSphere), an SMB share (Hyper-V), or iSCSI target (vSphere or AHV) to provide shared storage for VM files. This storage is thinly provisioned, which means that storage is allocated to the storage container only as needed when data is written, rather than allocating the total maximum capacity when the storage container is created. One of the options at the storage container level is to enable compression either inline (as it is written) or after it is written (see [Compression](#) on page 115).

## Volume Groups

A volume group is a collection of logically related virtual disks (or volumes). A volume group is attached to one or more execution contexts (VMs or other iSCSI initiators) that share the disks in the volume group. You can manage volume groups as first-class entities: you can add disks to a volume group, attach them to one or more execution contexts, include them in disaster recovery policies, and perform other management tasks. You can also detach a volume group from its current execution context and attach it to another execution context that is running an instance of the same application, possibly at a remote location to which the volume is replicated.

You can manage volume groups as a single unit. You attach a volume group as a whole, as an iSCSI target, and you detach the volume group as a whole. However, you can resize the disks in a volume group.

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 a LUN number that specifies ordering within the volume group. A volume group can be configured for either exclusive or shared access.

You can backup, protect, restore (in-place restore and out-of-place restore), and migrate volume groups. You can include volume groups in 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 snapshotting is enabled.

## vDisks

A vDisk is a subset of available storage within a storage container that provides storage to virtual machines. If the storage container is mounted as an NFS volume, then the creation and management of vDisks within that storage container is handled automatically by the cluster.

## Datastores/SMB Shares

A datastore is a logical container for files necessary for VM operations. Nutanix provides the choice by supporting 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 it is the recommended datastore type.

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



**Note:** Using a Nutanix storage container as a general-purpose NFS or SMB share is not recommended. Because the Nutanix solution is VM-centric, the preferred mechanism is to deploy a VM that provides file share services.

*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 ESX 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.

The screenshot shows the vSphere Configuration interface for an NFS datastore named 'NTNX-NFS'. At the top, there's a navigation bar with tabs like 'Getting Started', 'Summary', 'Virtual Machines', 'Hosts', 'Performance', 'Configuration', 'Tasks & Events', 'Alarms', 'Permissions', and 'Storage Views'. Below the navigation bar, a message says 'The following hosts are connected to this datastore (select a host from the list to view the details):'. A table lists four hosts: 172.16.8.186, 172.16.8.185, 172.16.8.187, and 172.16.8.184, all mounted and connected. To the right of the table is a 'Datastore Details' panel for 'NTNX-NFS'. It shows the server (192.168.5.2), folder (/nfs-ctr), capacity (17.39 TB), used space (0.00 B), and free space (17.39 TB). There's also a circular progress bar indicating usage.

Figure: vSphere Configuration of NFS Datastore

**SMB Library Share.** The Nutanix SMB share implementation is the Hyper-V equivalent of an NFS Datastore with 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.

The screenshot shows the Hyper-V Configuration interface. On the left, there's a navigation pane with 'VMs and Services', 'Clouds', 'VM Networks', 'Storage', 'All Hosts', and 'Fabric'. Under 'Storage', it shows 'All Storage' with three entries: 'NTNX-14SM15030023-A-CVM', 'NTNX-14SM15030023-B-CVM', and 'NTNX-14SM15030023-C-CVM'. In the center, there's a 'Disk Information for Virtual Machines (4)' table. The table has columns for 'Name', 'Classification', 'Array', 'Type', 'Total Capacity', and 'Available Capacity'. The data shows three dynamic disks with 4.098.66 GB total capacity and 0 GB available capacity, and one test disk with 40.00 GB total capacity and 40.00 GB available capacity. Below the table, there's a section for 'Virtual machine information' showing status (Running), owner (ExternalSwitch), and recent job (Refresh virtual machine, 100% completed). There are also sections for 'Logical networks' and 'Recent job'.

Figure: Hyper-V Configuration of an SMB Share

## Compression

Storage containers can have compression enabled. Compression optimizes the use of storage in a cluster. Enabling compression has other benefits—such as optimized I/O bandwidth utilization from reduced I/O and better memory efficiency—which may have a positive impact on overall system performance.



**Note:** If the metadata usage is high, compression is automatically disabled. If compression is automatically disabled, an alert is generated.

The following types of compression are available.

### 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.



**Tip:** Post-process compression is recommended for all use cases.

If your cluster has a Pro or Ultimate license, post-process compression is enabled by default on newly created containers.

#### *Inline compression*

Data is compressed as it is written. This type of compression is recommended for workloads that perform batch processing.

### **Compression Ratios**

You can view compression ratios and usage savings in the Prism Web Console.

- 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**.

## Deduplication

Deduplication allows the sharing of guest VM data on Nutanix storage tiers. You can either enable cache deduplication or capacity deduplication or both on a storage container.

### **Cache Deduplication**

You can enable cache deduplication of read caches to optimize performance. Cache deduplication is not enabled by default and is available if you have purchased a Starter or higher license.

### **Capacity Deduplication**

You can enable capacity deduplication of persistent data. Capacity deduplication is not enabled by default and is available if you have purchased a Pro or higher license. Note that you can enable capacity deduplication only if cache deduplication is enabled.

### **Enabling Deduplication**

To enable deduplication, the **Cache** property for cache deduplication and **Capacity** property for capacity deduplication must be turned on at the storage container level. These storage container properties can be set in the web console or nCLI.

In addition, Controller VMs in clusters with deduplication enabled need to be configured with additional RAM:

- Cache deduplication: 24 GB RAM
- Capacity deduplication: 32 GB RAM

For more information about enabling deduplication, see [Creating a Storage Container](#) on page 139.

### **Deduplication Best Practices**

This table shows when deduplication is recommended and when it is not.

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>• Linked clones or Nutanix VAAI clones: Duplicate data is managed efficiently by DSF so deduplication has no additional benefit</li> <li>• Server workloads: Redundant data is minimal so may not see significant benefit from deduplication</li> </ul>

## Erasure Coding

Erasure coding increases the effective or usable capacity on a cluster. The savings that arises after enabling erasure coding is in addition to deduplication and compression savings.

Nutanix maintains data copies for data resiliency. If you have configured redundancy factor 2, two data copies are maintained. For example, consider a 6-node cluster with 4 data blocks (a b c d) as displayed in the following image. If you have configured redundancy factor 2, two copies of data are maintained. In the following image green text represents data copies.

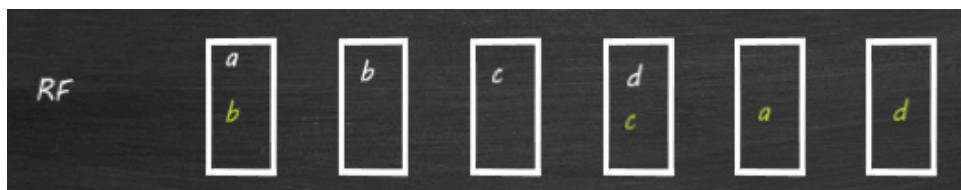


Figure: Data copies before Erasure Coding

Once the data becomes cold, the erasure code engine computes parity “P” for the data copies by taking all the data copies and performing an exclusive OR operation.

$$a \ b \ c \ d = P \text{ (parity)}$$

Figure: Computing Parity

Achieving 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:** Parity “P” and data blocks a b c d are placed on distinct nodes to achieve single node failure protection in a redundancy factor 2 configuration.

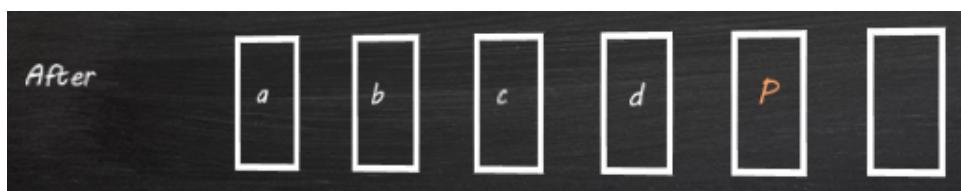


Figure: After Computation of Parity

If node containing data block c fails, block c is recovered by using the rest of the erasure coded strip (a b d and P) as displayed in the following image.

Data block c is rebuilt by using other members of the strip (a, b, d and P). Block c is then placed on a node that does not have any other members of this erasure coded strip.

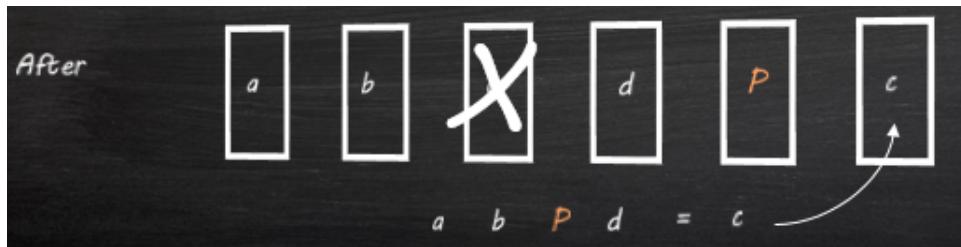


Figure: Post Node Failure



**Note:** In the redundancy factor 3 configuration, two parity blocks are maintained where two nodes can simultaneously fail without losing data. With two parity blocks, the system can rebuild lost data when two nodes simultaneously fail.

### Example of Savings from Erasure Coding

The savings from the erasure coding feature depends on the cluster size and coldness of the data.

Consider a 6-node cluster configured with redundancy factor 2. A strip size of 5 is possible: 4 nodes for data and 1 node for parity. Data and parity comprising the erasure coded strip leaves one node in the cluster to ensure that if a node failure occurs, a node is available for rebuild. If you use a strip of (4, 1), the overhead is 25% (1 for parity and 4 for data). Without erasure coding, the overhead is 100%.

Consider a cluster that has 20 TB of raw space available for each node. The following image displays the various configurations of cluster size, possible strips, and approximate savings that might occur after erasure coding is enabled.

	Cluster Size	Raw	Usable	After Erasure
	4 nodes	80 TB	40 TB	$\rightarrow \sim 53 \text{ TB}$ 80/1.5 = ~53
	5 nodes	100 TB	50 TB	$\rightarrow 75 \text{ TB}$ 100/1.33 = 75
	6 nodes	120 TB	60 TB	$\rightarrow 96 \text{ TB}$ 120/1.25 = 96
	7 nodes	140 TB	70 TB	$\rightarrow 112 \text{ TB}$ 140/1.25 = 112
Node avoided by Data or Parity		Node used for Parity		Node used for Data

Figure: Example of Space Saving from Erasure Coding

### Erasure Coding Best Practices and Requirements

- A cluster must have at least 4 nodes for erasure coding to be enabled.
- Avoid strips greater than (4, 1) because capacity savings provides diminishing returns and the larger strip size increases the cost of rebuild.
- Erasure coding effectiveness may be reduced on workloads that have many overwrites outside of the erasure coding window, which by default is seven days.
- Read performance may be degraded during failure scenarios.
- As erasure coding is a backend job, realization of savings might take some time.

- Multiple node removal operations can break the erasure coded strip. If it is necessary to remove multiple nodes from a cluster that uses erasure coding turn off erasure coding before removing the nodes.
- Do not enable erasure coding on clusters with the block fault tolerance.
- Erasure coding mandates that data and parity comprising a strip must be distinctly placed on the failure domain (node). For example, a strip size of (4, 1) requires you to have at least 6 nodes.

## Capacity Reservation Best Practices

Although the amount of physical storage in a storage pool is limited, each storage container on a storage pool appears to have access to all unused storage in the pool. If a storage pool has multiple storage containers, one storage container may take all the remaining storage space and leave others with no available space.

Capacity reservation allows you to guarantee that a storage container or a vDisk has a minimum amount of space. Space reserved in this fashion is unavailable to other storage containers, even if is not used by the storage container that reserves it.

Following are best practices for capacity reservation.

- Reserve capacity for a storage container only if the storage pool has multiple storage containers. Unless there is a specific reason to have multiple storage containers, Nutanix recommends having a single storage pool with a single storage container.
- If you need capacity reservation, reserve space for storage containers rather than for vDisks. Although it is possible to reserve space for vDisks, it takes more effort to manage.
- In total, reserve no more than 90% of the space in the storage pool.
- If you make clones from a vDisk that has reserved capacity, every clone has the same reserved capacity value. Ensure that the storage container has adequate capacity for all the clones.
- Do not enable compression on storage containers that have vDisks with reserved capacity. Some capacity will be unused because the capacity will be reserved but the vDisk data will be compressed.
- Ensure that the space needed for swap vDisks is available. If sufficient space for swap is not available, the VM will fail to start. This consideration applies if you are reserving space for storage containers as recommended or for vDisks.

## Storage Dashboard

The Storage dashboard displays dynamically updated information about the storage configuration in a cluster. To view the Storage dashboard, select **Storage** from the pull-down list on the far left of the main menu.

### Menu Options

In addition to the main menu (see [Main Menu Options](#) on page 32), the Storage screen includes a menu bar with the following options:

- **View selector.** The Storage dashboard provides three viewing modes.
  - Click the **Overview** button on the left to display storage information in a summary view (see [Storage Overview View](#) on page 120).
  - Click the **Diagram** button to display a diagram of the storage pools and storage containers in the cluster nodes from which you get detailed information by clicking on a storage pool or storage container of interest (see [Storage Diagram View](#) on page 122).
  - Click the **Table** button to display hardware information in a tabular form. The Table screen is further divided into Volume Group, Storage Pool, and Storage Container views; click the **Volume Group** tab to view volume group information, the **Storage Pool** tab to view storage pool information, and

the **Storage Container** tab to view storage container information (see *Storage Table View* on page 129).

- **Action buttons.** Click the **Volume Group** button on the right to add a volume group to the cluster (see *Creating a Volume Group* on page 147) in a storage container. Click the **Storage Container** button to add a storage container to a storage pool (see *Creating a Storage Container* on page 139). Click the **Storage Pool** button to add a storage pool to the cluster (see *Creating a Storage Pool* on page 138).
- **Page selector.** In the Table view, hosts and disks are listed 10 per page. When there are more than 10 items in the list, left and right paging arrows appear on the right, along with the total count and the count for the current page.
- **Export table content.** In the Table view, you can export the table 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 pull-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.

## Storage Overview View

The Storage Overview view displays storage-specific performance and usage statistics on the left plus the most recent storage-specific alert and event messages on the right. 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. The following figure is a sample view, and the table describes each field in this view.

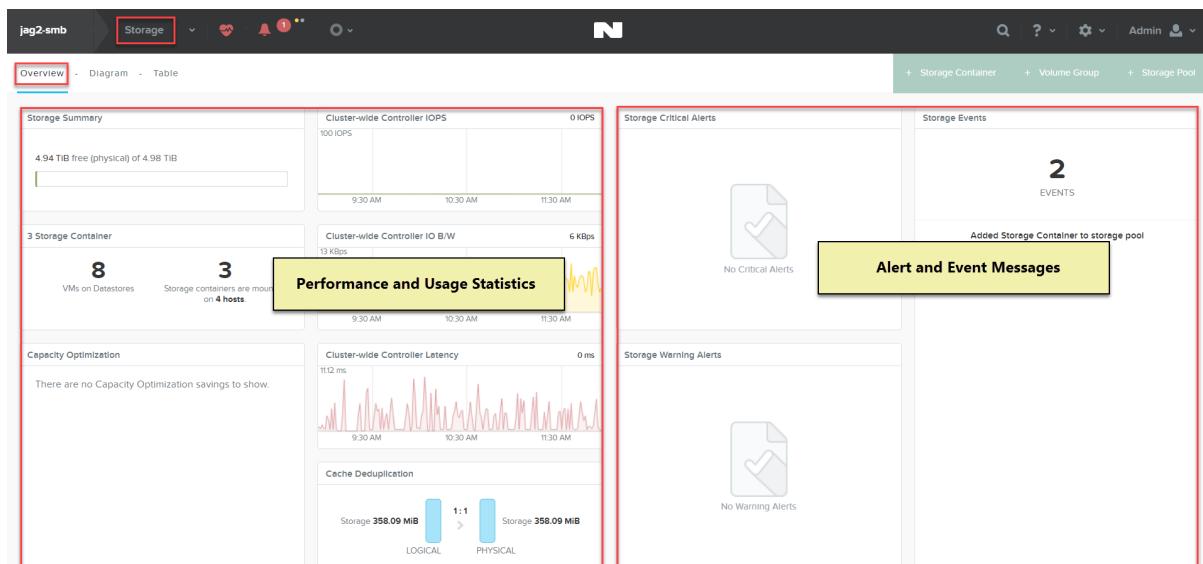


Figure: Storage Overview View



**Note:** See *Understanding Displayed Statistics* on page 41 for information about how the statistics are derived.

## Storage Overview Screen Fields

Name	Description
Storage Summary	Displays the amount of used, free, and total storage space (in GB or TB) in the cluster.

Name	Description				
Storage Containers	Displays the number of storage containers, number of VMs, and number of hosts on which the storage containers are mounted in the cluster.				
Capacity Optimization	Displays the data reduction ratio (compression, deduplication, or erasure coding), data reduction savings (compression, deduplication, or erasure coding), and the overall efficiency that you can achieve by enabling compression, deduplication, and erasure coding features.				
<span style="font-size: small;">Capacity Optimization</span> <b>1.61 : 1</b> <span style="font-size: small;">Data Reduction</span>					
	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Data Reduction Savings</td> <td style="width: 70%;">1.84 TiB</td> </tr> <tr> <td>Overall Efficiency</td> <td>1.85 : 1</td> </tr> </table>	Data Reduction Savings	1.84 TiB	Overall Efficiency	1.85 : 1
Data Reduction Savings	1.84 TiB				
Overall Efficiency	1.85 : 1				
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. (These display features also apply to the I/O bandwidth and I/O latency monitors.)				
Cluster-wide Controller IO BW	Displays I/O bandwidth used per second in the cluster. 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 link in the upper right of the chart (see <a href="#">Analysis Dashboard</a> on page 401).				
Cluster-wide Controller Latency	Displays the average I/O latency (in milliseconds) in the cluster.				
Cache Deduplication	Displays summary statistics (example below) for memory and flash (SSD) storage used and saved through deduplication (fingerprint-on-write enabled).				
<span style="font-size: small;">Deduplication</span>  <p>The chart illustrates deduplication ratios for Memory and SSD. On the left, 'LOGICAL' storage is shown as a stack of blue (Memory) and purple (SSD). An arrow points to the right, labeled '2.93 : 1', indicating the deduplication ratio. On the right, 'PHYSICAL' storage is shown as a stack of blue (Memory) and purple (SSD), with the total size being smaller than the logical size due to deduplication. The chart shows a total logical size of 64.72 GB + 82.99 GB = 147.71 GB, and a physical size of 22.07 GB + 26.78 GB = 48.85 GB, resulting in a savings of 98.86 GB.</p>					
Storage Critical Alerts	Displays the five most recent unresolved storage-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 <b>view all alerts</b> button at the bottom of the list (see <a href="#">Alerts Dashboard</a> ).				
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.				

Name	Description
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.

## Storage Diagram View

The Storage Diagram view displays information about 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) and colored blocks in the bar for each storage pool. Clicking on a storage pool block displays storage information about the storage pool and a bar with blocks for each storage container in that storage pool. Clicking on a storage container block displays storage information about the storage container and a bar for that storage container. The storage container bar includes **Physical** and **Logical** buttons on the right that you can click to display information about the physical capacity, which is the total addressable space, or logical capacity, which is the usable space after accounting for the data replication factor. Because the default replication factor is set to two, the logical space is typically half the physical space. 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:** See *Understanding Displayed Statistics* on page 41 for information about how the statistics are derived.

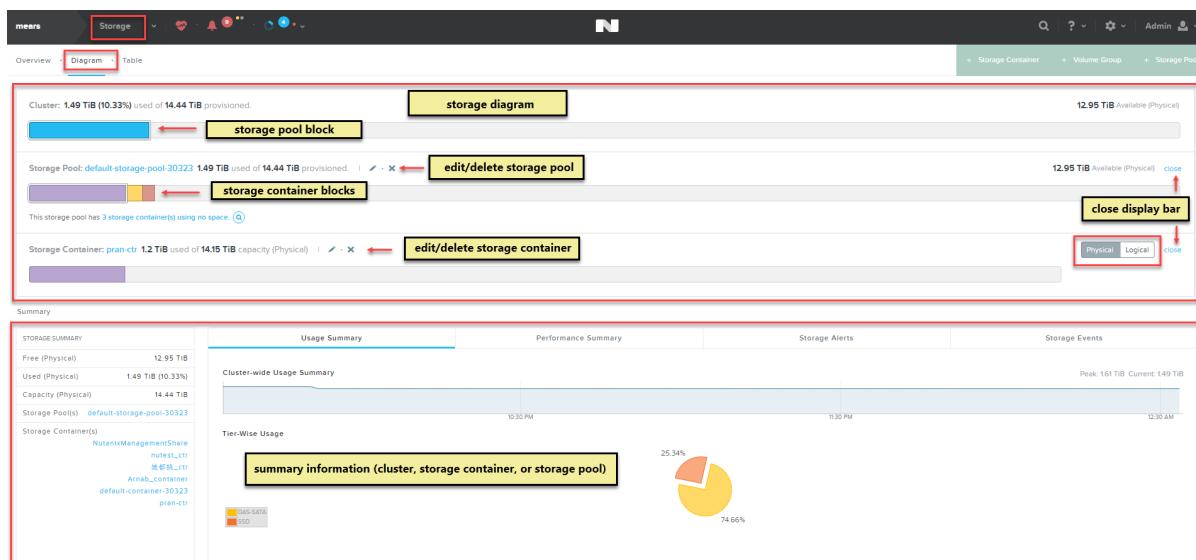


Figure: Storage Diagram View

## Storage Container Details

Selecting a storage container in the diagram displays information about that storage container in the lower section of the screen (see [Creating a Storage Container](#) on page 139).

- When a storage container is selected, **Summary: storage\_container\_name** appears below the diagram, and action links appear on the right of this line (see [Modifying a Storage Container](#) on page 143 for more information about these actions):
  - Click the **Update** link to update the settings for this storage container.
  - Click the **Delete** link to delete this storage container configuration.
- 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**.

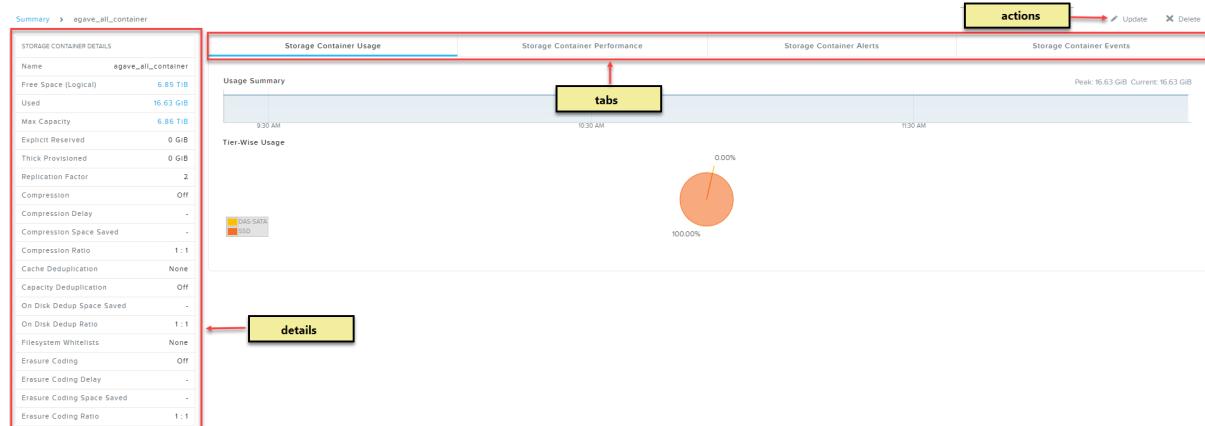


Figure: Storage Diagram View: Storage Container

## Storage Container Details Fields

Parameter	Description	Values
Name	Displays the name of the storage container.	(name)
Free Space	Displays the amount of free storage space available to the storage container that is unreserved.	xxx [GB TB]
Used	Displays the amount of used storage space for the storage container.	xxx [GB TB]
Max Capacity	Displays the total amount of storage capacity available to the storage container (see the Reserved Capacity description).	xxx [TB]

Parameter	Description	Values
Explicit Reserved	Displays the total reserved storage capacity in the storage container. Nutanix employs a "thin" 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 the field values for both storage containers show the full amount. However, capacity can be reserved for a specific storage container, and this field displays how much storage (if any) has been reserved for this storage container.	xxx [GB TB]
Thick Provisioned	Displays the amount of storage space that is thick provisioned.	xxx [GB TB]
Replication Factor	Displays the replication factor, which is the number of maintained data copies. The replication factor is specified (2 or 3) when the storage container is created.	[2-3]
Compression	Displays whether compression is enabled.	[Off On]
Compression Delay	Displays the delay (number of minutes) required to perform the data compression.	xxx [min.]
Compression Space Saved	Displays the amount of storage space saved by enabling data compression.	xxx [MB GB TB]
Compression Ratio	Displays how much the data size is reduced (percentage) by enabling compression.	[0 - 100%]
Performance Tier Deduplication	Displays whether "fingerprint on write" is enabled, which allows data duplication compression when data is read. Data duplication (commonly referred to as dedup) is a specialized data compression technique for eliminating duplicate copies of repeating data. Setting this parameter to <b>On</b> causes dedup compression to be applied to data both in memory and in solid state storage (SSD).	[None, On, Off]
On Disk Deduplication	Displays whether on disk deduplication is enabled, that is dedup compression applied to data on hard disks (HDD). Performance tier deduplication is a prerequisite for on disk deduplication.	[On, Off]
On Disk Dedup Space Saved	Displays the disk space saved through deduplication. A dash appears when deduplication is off.	xxx [MB GB TB]
On Disk Dedup Ratio	Displays the pre- and post-deduplication ratio. For example, the ratio would be 2:1 if deduplication reduced the space used by 50%. The ratio is 1:1 when deduplication is off (or there is no deduplication savings).	x.xx : 1

Parameter	Description	Values
Filesystem Whitelists	Displays whether you have configured filesystem whitelist for this storage container.	[None, On, Off]
Erasure Coding	Displays whether erasure coding is enabled or not.	[On, Off]
Erasure Coding Delay	Displays the delay after which erasure coding is going to start.	xxx [min.]
Erasure Coding Space Saved	Displays the amount of storage space saved by enabling erasure coding.	xxx [MB GB TB]
Erasure Coding Ratio	Displays the pre- and post-erasure coding ratio. For example, the ratio would be 2:1 if erasure coding has reduced the space used by 50%. The ratio is 1:1 when erasure coding is off (or there is no erasure coding savings).	x.xx : 1

## Storage Pool Details

Selecting a storage pool in the diagram displays information about that storage pool in the lower section of the screen (see [Creating a Storage Pool](#) on page 138).

- When a storage pool is selected, **Summary: storage\_pool\_name** appears below the diagram, and action links appear on the right of this line (see [Modifying a Storage Pool](#) on page 138 for more information about these actions):
  - Click the **Update** link to update the settings for this storage pool.
  - Click the **Delete** link to delete this storage pool configuration.
- 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**.

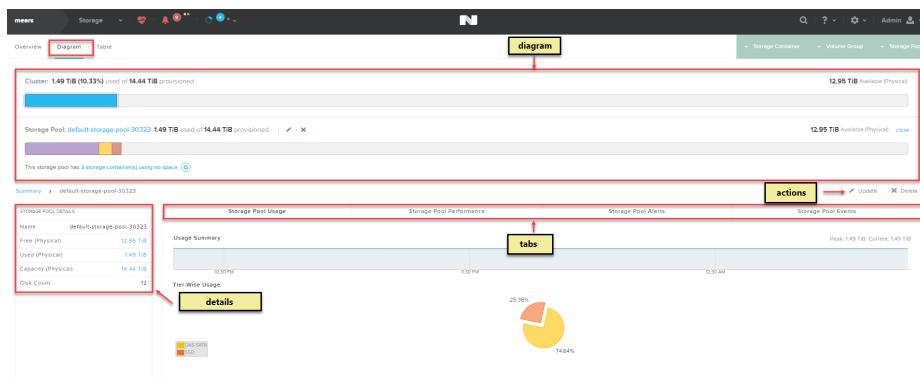


Figure: Storage Diagram View: Storage Pool

## 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]

Parameter	Description	Values
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:
  - 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(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:

- 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 (see [Analysis Dashboard](#) on page 401).
- 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.

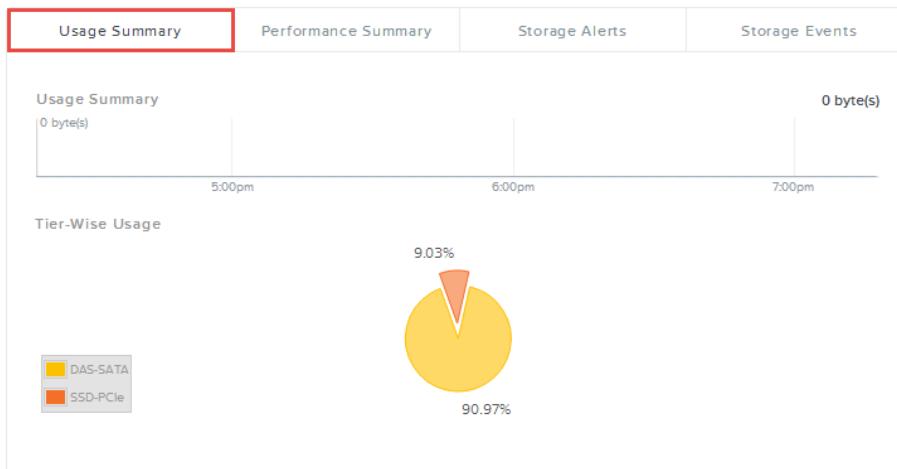


Figure: Storage Table View: Usage Tab

## 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 (see [Analysis Dashboard](#) on page 401). 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.

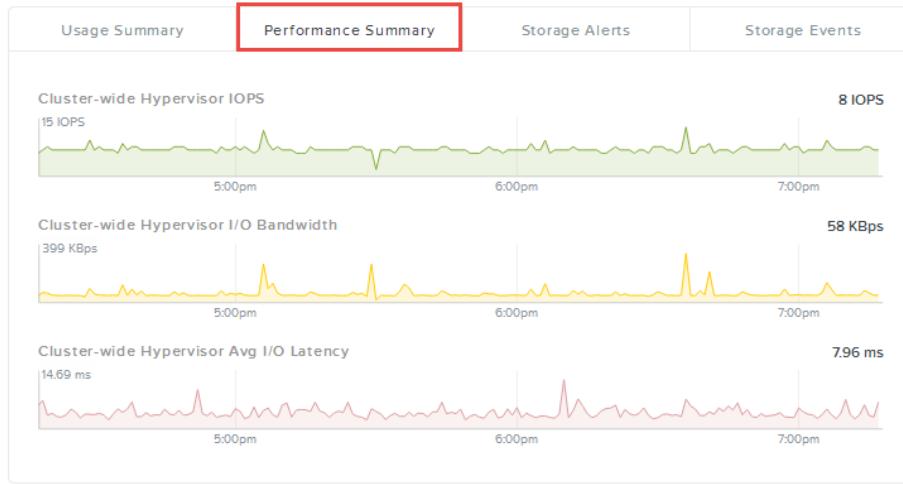


Figure: Storage Table View: Performance Tab

## Alerts Tab

The Alerts tab displays the unresolved alert messages about storage pools or storage containers in the same form as the Alerts page (see [Alert Messages View](#) on page 411). Click the **Unresolved X** button in the filter field to also display resolved alerts.

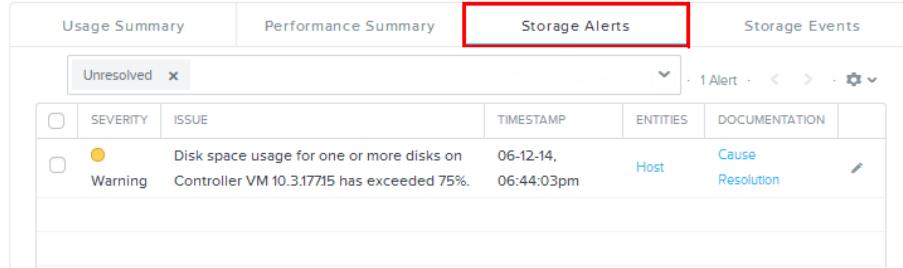


Figure: Storage Table View: Alerts Tab

## Events Tab

The Events tab displays the unacknowledged event messages about storage pools or storage containers in the same form as the Events page (see [Event Messages View](#) on page 413). Click the **Include Acknowledged** button to also display acknowledged events.

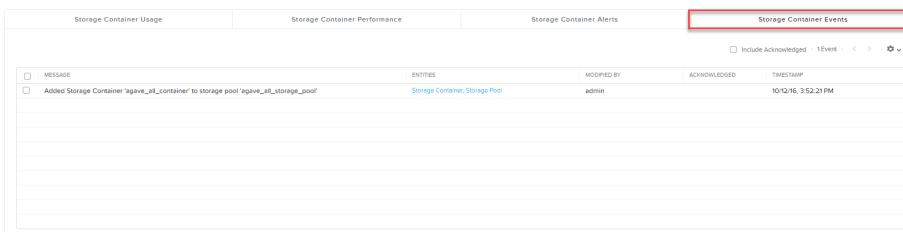


Figure: Storage Table View: Events Tab

## 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:** See [Understanding Displayed Statistics](#) on page 41 for information about how the statistics are derived.

The screenshot shows the Storage Table View interface. At the top, there's a navigation bar with tabs for Overview, Diagram, and Table, with Table being the active tab. Below the navigation bar is a search bar and some administrative links. The main area is divided into two main sections: a table section and a summary section. The table section contains a single row for a storage pool named 'agave\_all\_storage\_pool'. The summary section on the right contains tabs for Usage Summary, Performance Summary, Storage Alerts, and Storage Events. A yellow box highlights the table information (storage container, volume group, or storage pool) in the table section, and another yellow box highlights the summary information (cluster, storage container, volume group, or storage pool) in the summary section.

Figure: Storage Table View

## Volume Group tab

Clicking the Volume Group tab displays information about volume groups in the cluster (see [Creating a Volume Group](#) on page 147).

- 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 (see [Modifying a Volume Group](#) on page 148 for more information about these actions):
  - Click the **Update** link to update the settings for this volume group.
  - Click the **Delete** link to delete this volume group.

Four tabs appear that display information about the selected volume group (see following sections for details about each tab): Virtual Disks, Volume Group Tasks, Volume Group Alerts, and Volume Group Events.

Figure: Storage Table View: Volume Group

### Volume Group Table and Detail Fields

Parameter	Description	Values
<b>Volume Group Table Fields (upper screen)</b>		
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]
<b>Volume Group Details Fields (lower screen)</b>		
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]
Shared	Indicates whether the volume group is shared across iSCSI initiators.	[Yes No]
iSCSI Initiators	Displays the iSCSI initiators to which the volume group is attached.	(None List of names)

## Storage Container Tab

Clicking the **Storage Container** tab displays information about storage containers in the cluster (see *Creating a Storage Container* on page 139).

- 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 (see *Modifying a Storage Container* on page 143 for more information about these actions):
  - Click the **Update** link to update the settings for this storage container.
  - Click the **Delete** link to delete this storage container configuration.
- 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**.

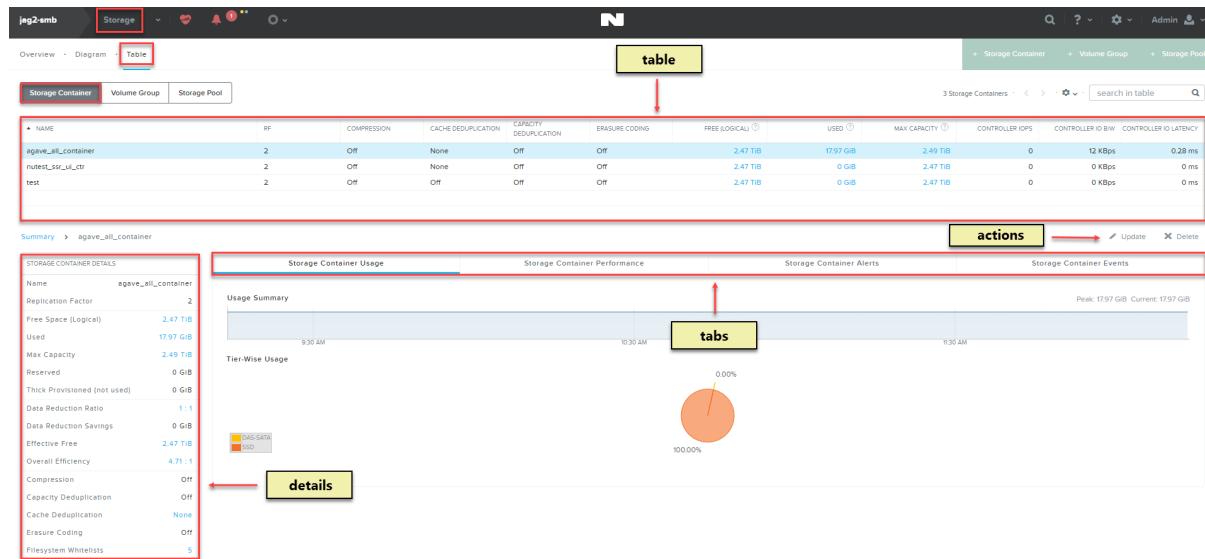


Figure: Storage Table View: Storage Container

## 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)
RF	Displays the replication factor, which is the number of maintained data copies. The replication factor is specified (2 or 3) when the storage container is created.	[2-3]
Compression	Displays whether compression is enabled.	[Off On]

Parameter	Description	Values
Cache Deduplication	Displays whether "fingerprint on write" is enabled, which allows data duplication compression when data is read. Data duplication (commonly referred to as dedup) is a specialized data compression technique for eliminating duplicate copies of repeating data. Setting this parameter to <b>On</b> causes dedup compression to be applied to data both in memory and in solid state storage (SSD).	[None, On, Off]
Capacity Deduplication	Displays whether on disk deduplication is enabled, that is dedup compression applied to data on hard disks (HDD). Cache deduplication is a prerequisite for Capacity deduplication.	[On, Off]
Erasure Coding	Displays whether erasure coding is enabled for the storage container or not	[On, Off]
Free (logical)	Displays the amount of free storage space in the storage container.	xxx [GB TB]
Used	Displays the amount of used storage space in the storage container.	xxx [GB TB]
Max Capacity	Displays the total amount of storage capacity available to the storage container (see the Reserved Capacity description).	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 (lower screen)</i>		
Name	Displays the name of the storage container.	(name)
Free Space (Logical)	Displays the amount of free storage space available to the storage container that is unreserved.	xxx [GB TB]
Used	Displays the amount of used storage space for the storage container.	xxx [GB TB]
Max Capacity	Displays the total amount of storage capacity available to the storage container (see the Reserved Capacity description).	xxx [TB]

Parameter	Description	Values
Reserved	Displays the total reserved storage capacity in the storage container. Nutanix employs a "thin" 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 the field values for both storage containers show the full amount. However, capacity can be reserved for a specific storage container, and this field displays how much storage (if any) has been reserved for this storage container.	xxx [GB TB]
Thick Provisioned	Displays the amount of storage space that is thick provisioned.	xxx [GB TB]
Replication Factor	Displays the replication factor, which is the number of maintained data copies. The replication factor is specified (2 or 3) when the storage container is created.	[2-3]
Compression	Displays whether compression is enabled.	[Off On]
Data Reduction Ratio	Displays the ratio of how much the data size is reduced by enabling compression, deduplication, or erasure coding.	x.xx : 1
Data Reduction Savings	Displays the data reduction savings by enabling compression, deduplication, or erasure coding.	xxx [GB TB]
Effective Free	Displays the amount of usable free space after data reduction.	xxx [GB TB]
Overall Efficiency	Displays the overall efficiency that you can achieve by enabling compression, deduplication, and erasure coding features.	xxx [GB TB]
Cache Deduplication	Displays whether "fingerprint on write" is enabled, which allows data duplication compression when data is read. Data duplication (commonly referred to as dedup) is a specialized data compression technique for eliminating duplicate copies of repeating data. Setting this parameter to <b>On</b> causes dedup compression to be applied to data both in memory and in solid state storage (SSD).	[None, On, Off]
Capacity Deduplication	Displays whether on disk deduplication is enabled, that is dedup compression applied to data on hard disks (HDD). Cache deduplication is a prerequisite for Capacity deduplication.	[On, Off]
Filesystem Whitelists	Displays whether you have configured filesystem whitelist 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 (see [Creating a Storage Pool](#) on page 138).

- The table at the top of the screen displays information about all the configured storage pools, 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 (see [Modifying a Storage Pool](#) on page 138 for more information about these actions):
  - Click the **Update** link to update the settings for this storage pool.
  - Click the **Delete** link to delete this storage pool configuration.
- 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**.

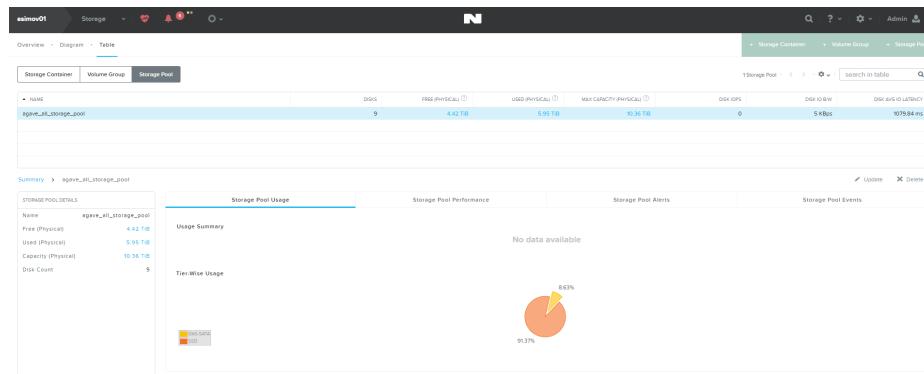


Figure: Storage Table View: Storage Pool

## 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]
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]

Parameter	Description	Values
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]
<b>Storage Pool Details Fields (lower screen)</b>		
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(s)**. Displays the names of the storage pools in the cluster. Clicking a name displays detailed information about that 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**.

## 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 (see [Analysis Dashboard](#) on page 401).

- **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.

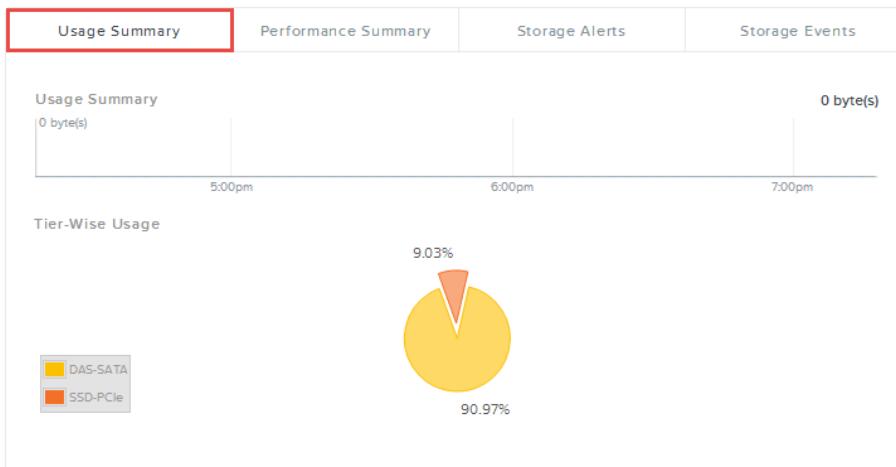


Figure: Storage Table View: Usage Tab

## 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 (see [Analysis Dashboard](#) on page 401). 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.

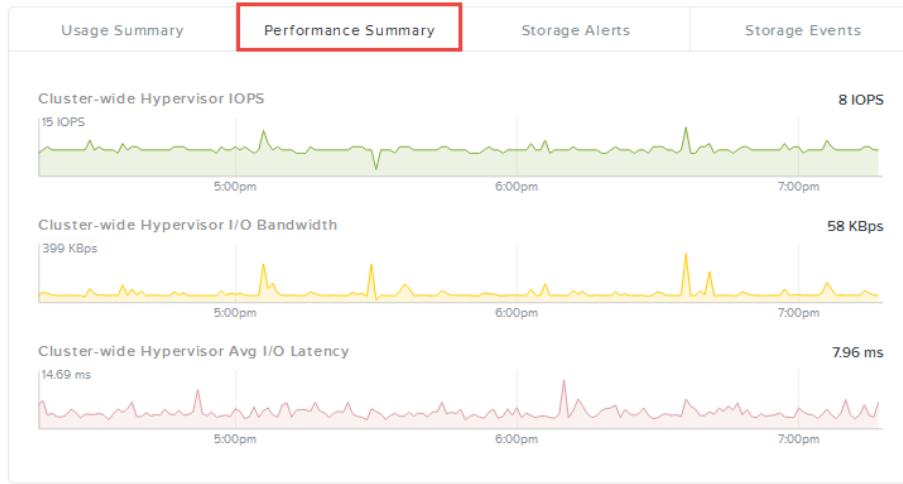


Figure: Storage Table View: Performance Tab

## 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 (see [Alert Messages View](#) on page 411). Click the **Unresolved X** button in the filter field to also display resolved alerts.

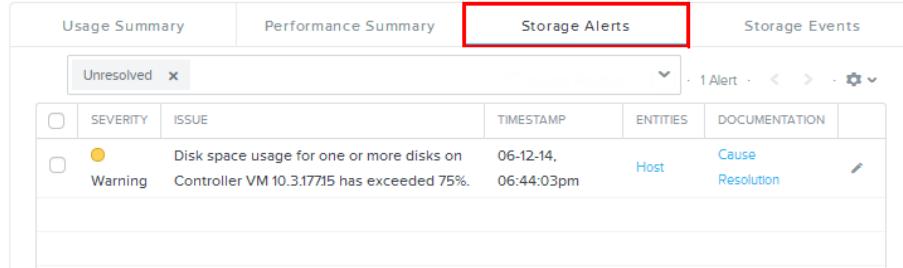


Figure: Storage Table View: Alerts Tab

## 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 (see [Event Messages View](#) on page 413). Click the **Include Acknowledged** button to also display acknowledged events.

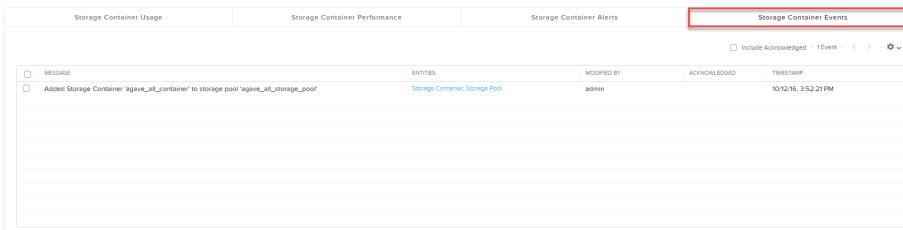


Figure: Storage Table View: Events Tab

## Creating a Storage Pool

A storage pool is a set of physical disks that are configured as a single storage group.

**Note:** A storage pool is created automatically when the cluster is created. It is not necessary to have more than one storage pool, and Nutanix recommends using a single storage pool to hold all storage within the cluster. This configuration, which supports the majority of use cases, allows the cluster to dynamically optimize the distribution of resources like capacity and IOPS. Isolating disks into separate storage pools provides physical separation between VMs, but it can also create an imbalance of these resources if the disks are not actively used.

To create a storage pool, do the following:

1. In the Storage dashboard (see [Storage Dashboard](#) on page 119), click the **Storage Pool** button. The *Create Storage Pool* dialog box appears.

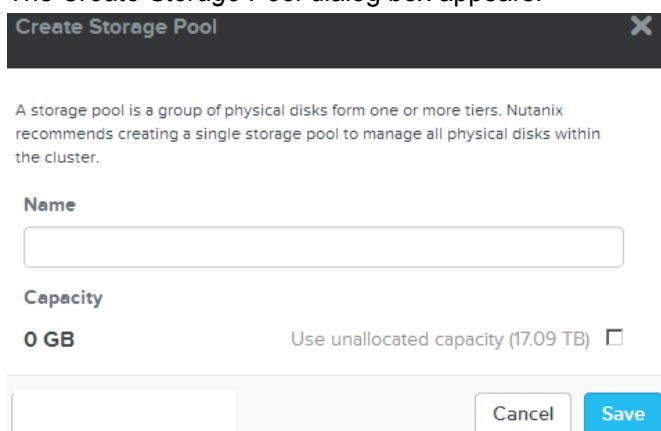


Figure: Create Storage Pool Window

2. In the **Name** field, enter a name for the storage pool.

**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), Simplified Chinese, decimal digits (0-9), dots (.), hyphens (-), and underscores (\_).

3. In the **Capacity** field, check the **Use unallocated capacity** box (if present) to add the available unallocated capacity to this storage pool.

The **Capacity** field indicates the amount of space in the cluster that is available to this storage pool. The listed storage size (0 GB initially) is the assigned capacity for this storage pool. When there is unallocated capacity in the cluster, that means there are storage resources that have not yet been assigned to a storage pool, and the **Use unallocated capacity** box appears. Checking this box adds that space to this storage pool. The check box does not appear if there is no unallocated storage capacity.

4. When the field entries are correct, click the **Save** button.

## Modifying a Storage Pool

A storage pool is a defined group of physical disks that can be modified as the cluster changes.

The main reason to modify a storage pool is to add the storage capacity from newly installed nodes into the storage pool. To modify (or delete) a storage pool, do the following:

1. In the web console select **Storage** from the pull-down main menu (upper left of screen) and then select the **Table** and **Storage Pool** tabs.
2. To update the storage pool, select the target storage pool and then click the **Update** link.  
The *Update Storage Pool* window appears, which includes the same fields as the *Create Storage Pool* window (see [Creating a Storage Pool](#) on page 138). Through this window you can change the storage pool name, add unallocated storage capacity, or change the information life cycle management (ILM) threshold.
3. To delete the storage pool, select the target storage pool and then click the **Delete** link.

## Creating a Storage Container

A storage container is a defined subset of available storage within a storage pool. Storage Containers allow you to apply rules or transformations such as compression to a data set.

**Before you begin:** Confirm the cluster is configured to synchronize time with NTP servers (see [Configuring NTP Servers](#) on page 572) and that the time on the Controller VMs is synchronized and current. If the time on the Controller VMs is ahead of the current time cluster services may fail to start. Files within the storage containers may also have timestamps ahead the current time when viewed from the hypervisor.

Clusters handle storage containers differently depending on the hypervisor.

- Hyper-V: Each hypervisor host accesses the storage container as an SMB share.
- vSphere: Each hypervisor host mounts the storage container as an NFS datastore. This requires access to the vSphere APIs. Ensure that you have appropriate license of vSphere to access the APIs.
- AHV: Nutanix VM management scripts create and manage each virtual disk as an iSCSI target stored on the storage container.



**Note:** A storage pool and one storage container are created automatically when the cluster is created.



**Note:** Acropolis File Services does not support Hyper-V.

To create a storage container, do the following:

1. In the Storage dashboard (see [Storage Dashboard](#) on page 119), click the **Storage Container** button. The *Create Storage Container* dialog box appears.

Create Storage Container

Enter a name for your storage container and select a storage pool for it. You can provision the storage container for all hosts or select individual hosts.

NAME

STORAGE POOL

default-storage-pool-30323

MAX CAPACITY  
12.95 TiB (Physical) Based on storage pool free unreserved capacity

NFS DATASTORE

Mount on all ESXi hosts  
 Mount on the following ESXi hosts

Advanced Settings      Cancel      Save

Figure: Create Storage Container (vSphere)

Create Storage Container

Enter a name for your storage container and select a storage pool for it. You can provision the storage container for all hosts or select individual hosts.

NAME

STORAGE POOL

agave\_all\_storage\_pool

MAX CAPACITY  
13.77 TiB (Physical) Based on storage pool free unreserved capacity

Advanced Settings      Cancel      Save

Figure: Create Storage Container (AHV)

Create Storage Container

Enter a name for your storage container and select a storage pool for it. You can provision the storage container for all hosts or select individual hosts.

NAME

STORAGE POOL

agave\_all\_storage\_pool

MAX CAPACITY  
10.27 TiB (Physical) Based on storage pool free unreserved capacity

MAKE THIS STORAGE CONTAINER THE DEFAULT STORE FOR VMS ON HYPER V HOSTS

None  
 Make default on all Hyper V hosts  
 Make default on particular Hyper V hosts

Advanced Settings      Cancel      Save

Figure: Create Storage Container (Hyper-V)

## 2. Do the following in the indicated fields:

- a. **Name:** Enter a name for the storage container.



**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), Simplified Chinese, decimal digits (0-9), dots (.), hyphens (-), and underscores (\_).

- b. **Storage Pool:** Select a storage pool from the drop-down list.

The following field, **Max Capacity**, displays the amount of free space available in the selected storage pool.

- c. (vSphere only) **NFS Datastore:** Select the **Mount on all hosts** button to mount the storage container on all hosts. Select the **Mount on the following hosts** button to mount the storage container on a subset of hosts, which displays a list of host IP addresses below this field. Check the boxes of the hosts to be included.

- 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.

**Make default on all Hyper-V hosts**

Makes this storage container a default location for storing virtual machine configuration and virtual hard disk files on all the Hyper-V hosts.

**Make default on particular Hyper-V hosts**

Provides you with an option to select the hosts on which you want 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** button.

The screenshot shows a configuration interface for a storage container. At the top, a button labeled "ADVANCED SETTINGS" is highlighted with a red box. Below this are three input fields: "REPLICATION FACTOR" (set to 2), "RESERVED CAPACITY (GiB)" (set to 0), and "ADVERTISED CAPACITY (GiB)" (set to "Total GiB").

Figure: Create Storage Container Advanced Settings (1)

Do the following in the indicated fields:

- Replication Factor:** Select the number of data copies to maintain from the pull-down list.

The options are 2 or 3. Setting the replication factor to 3 (meaning maintaining three copies of the data instead of two) adds an extra layer of data protection at the cost of storing an additional copy of the data.



**Note:** To change the storage container level setting to replication factor 3, the cluster level setting must be FT=2. See [Modifying a Storage Container](#) on page 143.

- Reserved Capacity:** To reserve storage space for this storage container, enter the amount (in GiB) to reserve in this field.

A storage container can use any available space in the storage pool, but you can reserve space for a storage container to ensure the storage container has at least that much storage capacity. However, reserving space for a specific storage container means that space is no longer available to other storage containers even if the reserved space is unused. See [Capacity Reservation Best Practices](#) on page 119 for more information.

- Advertised Capacity:** To reserve an advertised storage space for this storage container, enter the amount (in GiB) to reserve in this field.

This sets an "advertised" capacity given to the hypervisor, which is the maximum storage size that the storage container can use. This can be set to any arbitrary value, but it must be greater than or equal to the reservation on the storage container (if set). The hypervisor ensures that the storage

container storage does not go beyond the advertised capacity. (When a storage container reaches a threshold percentage of the actual storage pool size, an alert is issued.)



Figure: Create Storage Container Advanced Settings (2)

- d. **Compression:** Select the check box to enable compression. A **Delay (In Minutes)** field appears after checking the box. Enter a zero to enable inline compression or a value (number of minutes) to enable post-write compression, which can begin (up to) that number of minutes after the initial write. All data in the storage container is compressed when this box is checked. See [Compression](#) on page 115 for guidelines about using compression.
- e. **Deduplication:** Select the **CACHE** check box to perform inline deduplication of read caches to optimize performance. If you enable this option, the Controller VMs must be configured to have at least 24 GB of RAM. This feature is primarily recommended for full-clone, persistent desktops, and physical to virtual migration use cases. Turning deduplication on for VAAI clone or linked clone environments is not recommended.  
Select the **CAPACITY** check box to perform post-process deduplication of persistent data. This option is recommended primarily for full clone, persistent desktops, and physical to virtual migration use cases that need storage capacity savings (not just performance savings from deduplication). It is further recommended that the Controller VMs have at least 32GB of RAM and 300GB SSDs for the metadata disk to use this option.

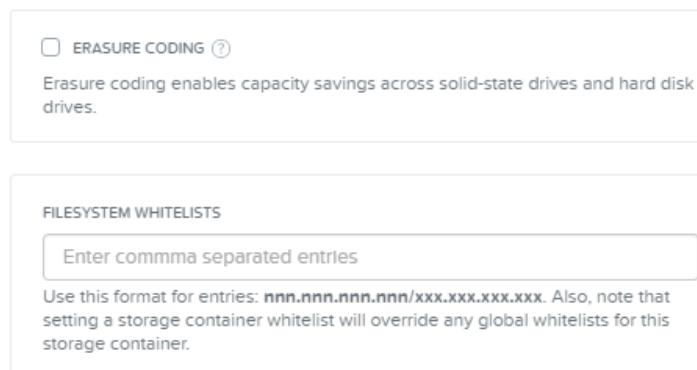


Figure: Create Storage Container Advanced Settings (3)

- f. **Erasure Coding:** Select the check box 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 117.
- g. **Filesystem Whitelists:** Enter the comma-separated IP address and netmask value (in the form *ip\_address/netmask*).  
A whitelist is a set of addresses that are allowed access to this storage container. Whitelists are used to allow appropriate traffic when unauthorized access from other sources is denied.



**Note:** Setting a storage container level whitelist overrides any global whitelist for this storage container.

- When all the field entries are correct, click the **Save** button.

## Modifying a Storage Container

A storage container is a defined subset of available storage within a storage pool that can be modified as conditions change.

Storage Containers can be modified to change how the data in that storage container is handled, for example to apply compression. To modify (or delete) a storage container, do the following:

- In the web console select **Storage** from the pull-down main menu (upper left of screen) and then select the **Table** and **Storage Container** tabs.
- To update the storage container, select the target storage container and then click the **Update** link. The *Update Storage Container* window appears, which includes the same fields as the *Create Storage Container* window (see [Creating a Storage Container](#) on page 139). Through this window you can specify NFS datastore mounts, reserve storage capacity, enable (or disable) compression, enable or disable erasure coding, select or deselect fingerprinting on writes which enables deduplication on reads, and configure filesystem whitelist.



**Note:**

- 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 web console does not provide an option to change the container replication factor. That can be done only through the nCLI (see [Increasing the Cluster Fault Tolerance Level](#) on page 107).

- To delete the storage container, select the target storage container and then click the **Delete** link.

## Volume Group Configuration

You create a volume group on a storage container and enable VMs and other iSCSI initiators to access the volume group in one of the following ways:

### *In-Guest iSCSI Connections*

You use in-guest iSCSI to attach a volume group to VMs and other iSCSI initiators. You whitelist the initiator IQN in the volume group configuration, and then configure in-guest iSCSI attachments (from the VM or iSCSI initiator, you discover the volume groups as iSCSI targets and log in to them). You can whitelist IQNs either when creating a volume group or when modifying a volume group. You can configure in-guest iSCSI connections on any hypervisor.

### *Attach Volume Groups Directly to VMs*

You create a volume group and attach it to one or more VMs as a SCSI disk by using the web console, REST API, nCLI, or aCLI. You do not have to whitelist initiator IQNs and configure in-guest attachments. You can attach a volume group to a VM only when updating a volume group or VM. This option is available only to VMs, and the hypervisor must be AHV.

## Volume Management

A volume group is a collection of logically related vDisks called volumes. Each volume group is identified by a UUID. Each disk of the volume group also has a UUID, and a name, and is supported by a file on DSF. Disks in a volume group are also provided with integer IDs to specify the ordering of disks. For external attachment through iSCSI, the iSCSI target name identifies the volume group, and the LUN number identifies the disk in the group.

Volume groups are managed independently of the VMs to which volumes must be explicitly attached or detached. A volume group may be configured for either exclusive or shared access.



**Caution:** You can attach a volume group to multiple VMs at same time. If a VM writes to a vDisk that belong to a shared volume group it may lead to data corruption. Do not use VM disks for write operations simultaneously from multiple VMs.

The volumes API exposes back-end DSF storage to guest operating system, physical hosts, and storage containers through iSCSI. iSCSI support allows any operating system to use the storage capabilities of DSF. In this deployment scenario, the operating system works directly with Nutanix storage bypassing any hypervisor.



**Note:** Currently, you can configure iSCSI multipathing by utilizing the Windows MPIO feature.

Volumes API consists of the following entities:

### *Volume group*

iSCSI target and group of disk devices.

### *Disks*

Storage devices in the volume group (displayed as LUNs for the iSCSI target).

### *Attachment*

Allowing a specified initiator IQN access to the volume group.

The following image shows an example of a VM running on Nutanix with its operating system hosted on the Nutanix storage, mounting the volumes directly.

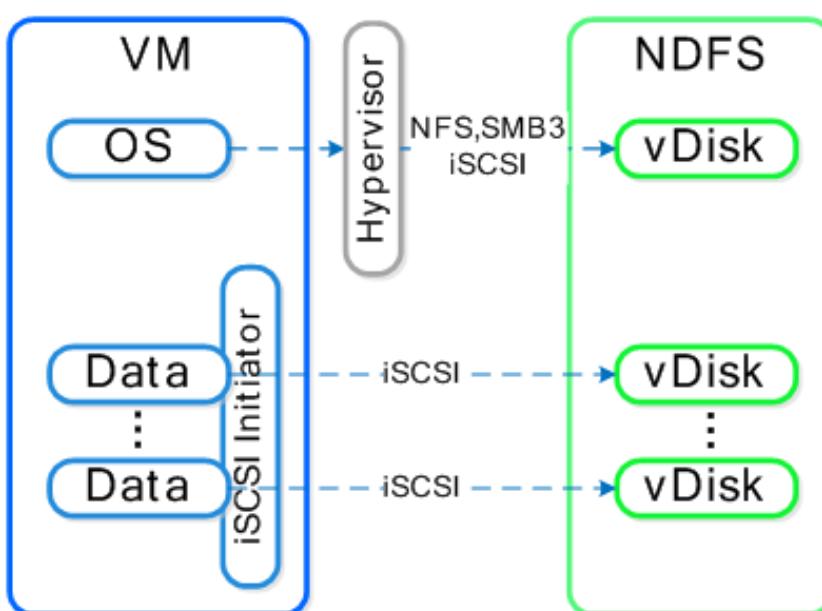


Figure: Regular Deployment Scenario

## Configuring iSCSI multipathing

In Windows deployments, you can configure iSCSI multipathing with the Windows MPIO feature. It is recommended to use the failover only policy (default) to ensure vDisk ownership does not change.

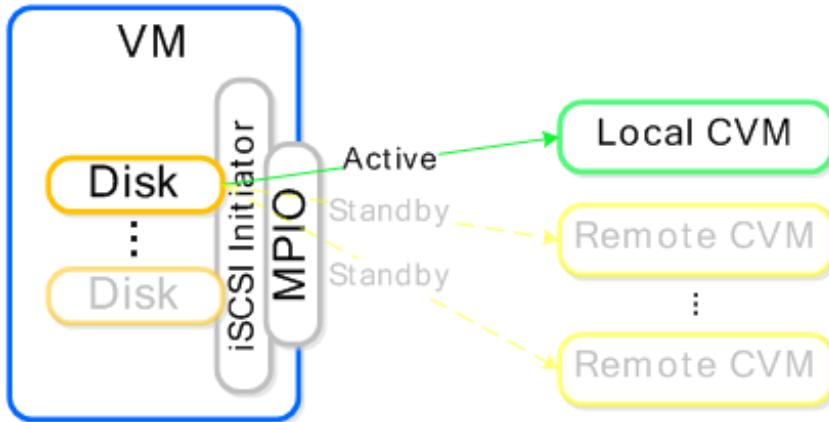


Figure: Configure iSCSI multipathing

If multiple disk devices are present, each disk can have an active path to the local Controller VM as displayed in the following image.

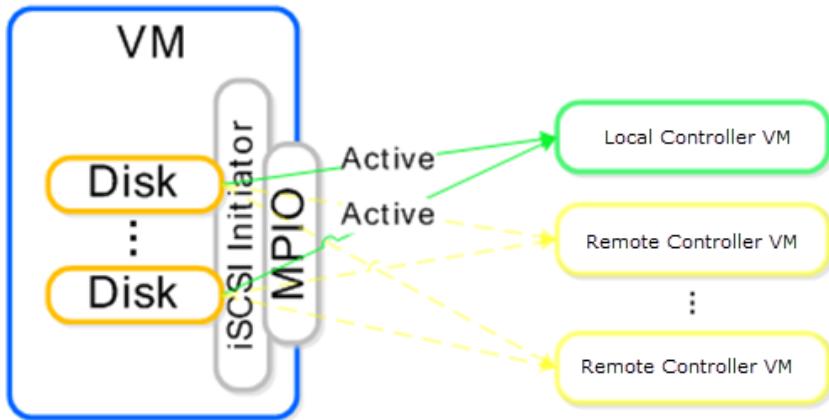


Figure: Active Path for Multiple Disk Devices

If the active Controller VM fails as displayed in the following image, another path becomes active and I/O resumes.

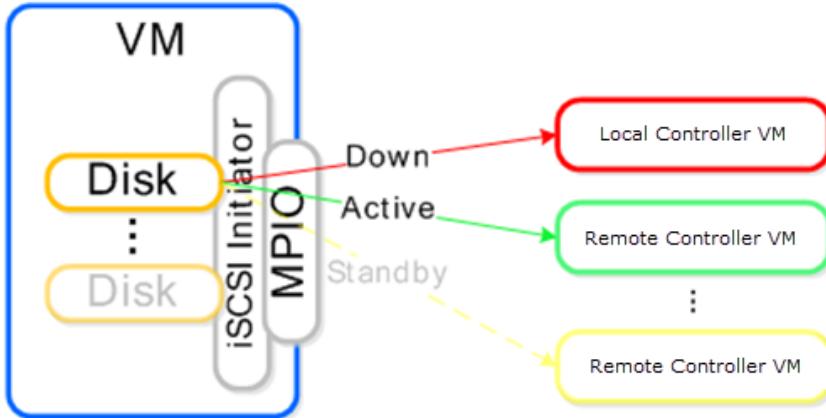


Figure: Failure Scenario

MPIO takes approximately 15 to 16 seconds to complete, which is within the Windows disk I/O timeout (default is 60 seconds). If RAID or Logical Volume Management (LVM) is desired the attached disk devices can be configured as a dynamic or a logical disk.

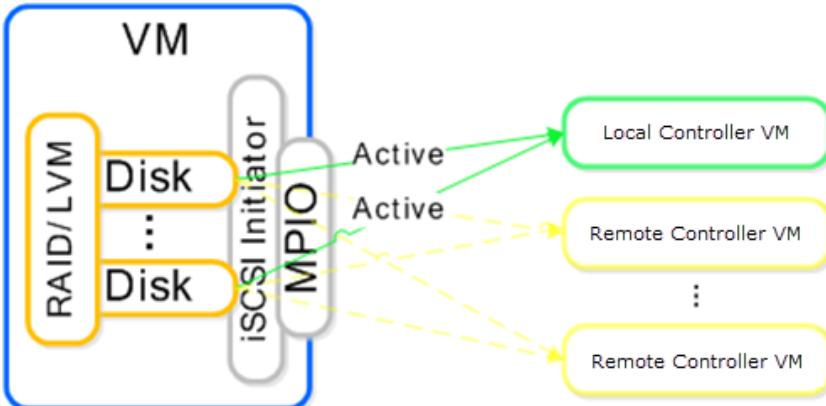


Figure: New Active Path

If the local Controller VM is heavily used, it is possible to have active paths to other Controller VMs. Having multiple active paths balances the I/O load across multiple Controller VMs; however, primary I/O has to traverse the network.

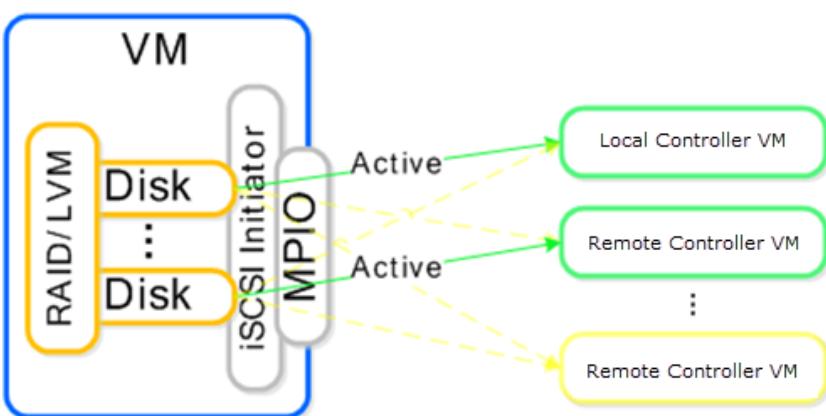


Figure: Multiple Active Paths

For information about configuring volume groups, see "Volume Group Configuration" in the "Storage Management" chapter of the *Prism Web Console Guide*.

## Concurrent Access from Multiple Clients

The following lists provide support information for products, features, or solutions that might require volume groups to be accessed concurrently, either by multiple iSCSI initiators or multiple VM attachments.

### Multiple iSCSI Initiators

The following products, features, or solutions are supported for concurrent access to volume groups:

- Oracle RAC (bare-metal and virtualized environments)
- Linux VMs
- Windows Failover Clustering

### Multiple VM Attachments

The following products, features, or solutions are supported for concurrent access to volume groups:

- Oracle RAC (MPIO is not required)
- Linux VMs (MPIO is not required)

The following products, features, or solutions are not supported for concurrent access to volume groups:

- Windows Failover Clustering
- Linux guest VM clustering is not supported for solutions other than Oracle RAC with Oracle Clusterware and Microsoft Windows Failover Clusters.

## Creating a Volume Group

To create a volume group, do the following:

1. In the Storage dashboard (see *Storage Dashboard* on page 119), click the **Volume Group** button. The *Create Volume Group* dialog box is displayed.
2. 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 (-).

3. 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**.
4. In **Description**, enter a description for the volume group.
5. To add a disk to the volume group, do the following:
  - a. In the **Storage** section, click **Add New Disk**.
  - b. In the **Add Disk** dialog box, in **Storage Container**, select the storage container to use from the pull-down list.
  - c. In **Size**, enter the disk size in GiBs.

- d. Click **Add**.
  - e. Repeat these steps to add another disk for this volume group, if desired.
6. Do the following in the **Access Settings** section:
- a. Select **Enable external client access** if you are whitelisting clients that are external to or not residing in this cluster. Otherwise, leave this clear. If you select this check box, it remains selected the next time you create a volume group.
  - b. If you are using one-way CHAP security, select **CHAP Authentication** 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.
  - c. Click **Add New Client** to configure the iSCSI initiators, and then enter the client IP address in the **Client IQN/IP Address** field to create the initial IP whitelist (optionally, you can use iSCSI initiator names (Initiator iSCSI Qualified Name [IQN]) from the Windows or Linux clients). If you have configured Mutual CHAP authentication on the client, select **CHAP Authentication** and enter the iSCSI client password (secret). Click **Add**.  
**Access Control** 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 about which products, features, or solutions are supported for concurrent access to a volume group, see [Concurrent Access from Multiple Clients](#) on page 147.

7. To enable the flash mode feature, select **Enable Flash Mode**.



**Note:** Individual virtual disks of a volume group cannot be excluded from flash mode by using Prism. However, you can exclude individual virtual disks from flash mode by using aCLI. For more information, see [Removing Flash Mode for Virtual Disks of a Volume Group](#) on page 150.

8. Click **Save**.

**What to do next:** If you whitelisted initiators, log in to the VMs, and then configure in-guest iSCSI attachments.

## Modifying a Volume Group

To modify a volume group, do the following:

1. In the web console, select **Storage** from the pull-down main menu (upper left of screen), and then select the **Table** and **Volume Group** tabs.
2. To update a volume group, select the volume group, and then click the **Update** link.  
The *Update Volume Group* window appears, which includes the same fields as the *Create Volume Group* window (see [Creating a Volume Group](#) on page 147). In this window you can change the volume group name, add and remove disks, configure the volume group for sharing, and add or remove entries from the initiator whitelist. On AHV clusters, you can attach the volume group to a VM as a SCSI disk. If you attach a volume group to a VM that is part of a protection domain, the volume group is not protected automatically. Add the volume group to the same consistency group manually.  
You can also increase the size of the volume group. Reducing the size of a volume group is not supported.
3. To delete a volume group, select the volume group, and then click the **Delete** link.

## Flash Mode for Virtual Machines and Volume Groups

The flash mode for VM and VG feature provides an ability to the administrator to set the storage tier preference (SSD tier) for a virtual machine or volume group that may be running some latency-sensitive mission critical applications. For example, a cluster running mission critical applications (such as SQL database) workload with a large working set alongside other workloads may be too large to fit into the SSD tier (hot tier) and could potentially migrate to the HDD tier (cold tier). For extremely latency-sensitive workloads, this migration to HDD tier could seriously affect the read and write performance of a workload.

By default, you can use 25% of the SSD tier of the entire cluster as flash mode for VMs or VGs. After you enable this feature, the data residing on the SSD tier is flashed and placed in the SSD tier and is never down migrated regardless of the amount of usage or degree of hotness of data of VMs with flash mode disabled. If the data that is flashed exceeds the 25% of SSD usage, the system may down migrate the data of even the flash mode VMs. Before performing this down-migration, the flash mode feature tries to preserve the excess data on the SSD tier for some reasonable amount of time so that you can take corrective actions on the cluster and bring back to stable state. Hence, ensure that the flashed usage is brought to less than 25% by reducing the number of flash mode VMs or VGs or by adding additional SSDs to get the full benefits of the flash mode feature.

If you enable this feature on a VM, all the virtual disks that are attached to the VM are automatically flashed on the SSD tier. Also, any subsequently added virtual disks to this VM are automatically flashed. However, you can update the VM configuration to remove the flash mode from any virtual disks.



**Caution:** The VM with flash mode enabled increases the performance of the virtual disks that are attached to the VM, but if you enable this feature it can lower the performance of the VMs on which this feature is not enabled. Hence, ensure that you perform a thorough analysis of the potential performance issues that may arise after enabling this feature. To overcome this issue, you can update the VM configuration and remove the flash mode on individual virtual disks. For example, you can flash only the data disks and leave out the log disks.

If a node failure occurs, this may cause a reduction in SSD tier capacity and can drive the flash mode usage above the 25% of the tier capacity. As a result alerts may be raised related to the flash usage exceeding 25%.



**Note:**

- This feature is supported on ESXi and AHV for VMs and on all the hypervisors for VGs.
- For the cluster created using ESXi hosts, you must register your cluster with the vCenter Server. For more information, see [Registering a vCenter Server](#) on page 585.

You can enable the feature on the VM only during the VM update workflow from the Prism Element. However, for VGs, you can enable the feature during the creation of VGs. For more information on enabling the feature on VMs, see [VM Management](#) on page 366 and for enabling the feature on VGs, see [Creating a Volume Group](#) on page 147.



**Note:** You cannot enable this feature by using Prism Central.

Alerts are raised in the following scenarios.

- When the flash usage exceeds 25% of the SSD tier.
- When the VM has the flash mode feature enabled, but is in the powered off state.

### Guidelines for the Flash Mode feature

- If a VM or a VG with flash mode feature enabled is cloned, then the flash mode policies are not automatically applied to the cloned VM or VG.

- The flash mode policies are not automatically applied if a VM or VG is restored from the DR snapshot on the local or the remote site.
- The flash mode policies can be used for controlling down migration from the hot tier to the cold tier. The policies do not restrict the usage for the VM or VG on the hot tier. If space is available on the hot tier, more data from the VM or VG can reside on the hot tier.
- If you enable erasure coding on the cluster, the parity always reside on the HDD.
- If you replicate a VM or VG to a remote site (by using Metro Availability or Async DR), the remote site does not have flash mode feature enabled automatically. You need to manually enable the flash mode feature again.
- Enabling flash mode feature does not affect performance tier deduplication. Do not use flash mode feature with capacity 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.
- If you try to upgrade the AOS with VM pinning feature enabled from the previous release, the upgrade process fails. Hence, ensure that you have disabled the VM pinning feature before performing an upgrade. Also, do not enable the VM pinning feature during the upgrade process.
- If you delete and then create the storage pool in your cluster, you cannot configure flash mode feature for a small duration of time because for some time there will be two storage pools in your cluster and flash mode feature is not supported if you have two storage pools in your cluster.

## Removing Flash Mode for Virtual Disks of a Volume Group

Individual virtual disks of a volume group cannot be excluded from flash mode by using Prism. However, you can exclude individual virtual disks from flash mode by using aCLI.

1. Log in to the Controller VM in your cluster through an SSH session and access the Acropolis command line.
2. (Optional) If you have not enabled the flash mode feature for the VG by using Prism, you can enable it by running the following command.

```
acli> vg.update vg_name flash_mode=true
```

Replace *vg\_name* with the name of the VG on which you want to enable the flash mode.

3. Remove the flash mode feature on a particular disk.

```
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
```

## Network Management

Nutanix provides several features to manage and monitor network settings for the cluster.

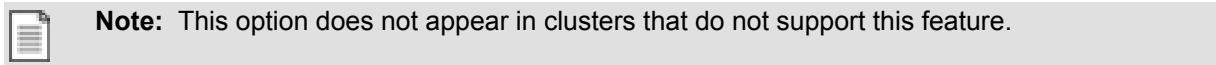
- In clusters with Nutanix virtualization management (such as those running AHV as the hypervisor), you can configure network connections through the web console (see [Configuring Network Connections](#) on page 151).
- To track and record networking statistics for a cluster, the cluster requires information about the first-hop network switches and the switch ports being used. You can configure one or more network switches for statistics collection (see [Configuring Network Switch Information](#) on page 155).
- A network visualizer is provided that presents 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 (see [Network Visualization](#) on page 160).

### Configuring Network Connections

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. To create one or more network configurations, do the following:

1. In the gear icon pull-down list of the main menu , select **Network Configuration**.



The *Network Configuration* window appears.

NAME	VLAN ID
network1	vlan.10
network2	vlan.12

**Close**

*Figure: Network Configuration Window*

2. Click the **Create Network** button.

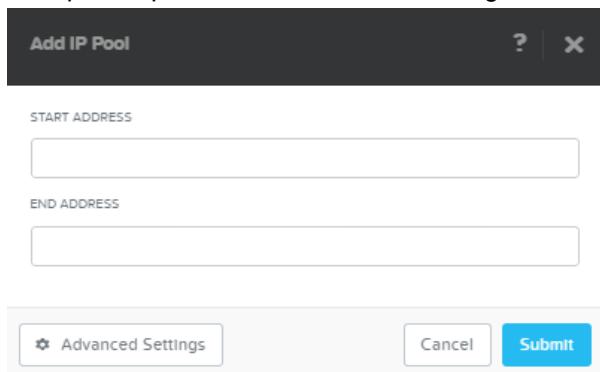
The **Create Network** dialog box appears. Do the following in the indicated fields:

The figure consists of two vertically stacked screenshots of a 'Create Network' dialog box. The top screenshot shows basic network configuration fields: NAME, VLAN ID, ENABLE IP ADDRESS MANAGEMENT (checked), NETWORK IP ADDRESS / PREFIX LENGTH, and GATEWAY IP ADDRESS. The bottom screenshot shows advanced domain settings: CONFIGURE DOMAIN SETTINGS (checked), DOMAIN NAME SERVERS, DOMAIN SEARCH, DOMAIN NAME, TFTP SERVER NAME, and BOOT FILE NAME. Both screenshots include a 'Cancel' button and a 'Save' button at the bottom.

*Figure: Create Network Dialog Box*

- a. **Name:** Enter a name for the network.
- b. **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 value appears as `vlan.1` or `vlan.27` in displays.
- c. **Enable IP Address Management:** Check the box to have the cluster control IP addressing in the network.  
Checking this box displays additional fields. If this box is not checked, no network management is attempted. In this case it is assumed management for this virtual LAN is handled outside the cluster.
- d. **Network IP Address/Prefix Length:** Enter the IP address of the gateway for the network and prefix with the network prefix (CIDR notation, for example, 10.1.1.0/24).
- e. **Gateway IP Address:** Enter the VLAN default gateway IP address.

- f. **Configure Domain Settings:** Check this box to display fields for defining a domain. Checking this box displays fields to specify DNS servers and domains. Unchecking this box hides those fields.
  - g. **Domain Name Servers (comma separated):** Enter a comma-delimited list of DNS servers.
  - h. **Domain Search (comma separated):** Enter a comma-delimited list of domains.
  - i. **Domain Name:** Enter the VLAN domain name.
  - j. **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).
  - k. **Boot File Name:** Name of the boot file to download from the TFTP server.
3. To define a range of addresses for automatic assignment to virtual NICs, click the **Create Pool** button (under **IP Address Pools**) and enter the following in the *Add IP Pool* dialog box:  
If no pool is provided, the user must assign IP addresses to VMs manually.



*Figure: Add IP Pool Dialog Box*

- 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 the **Submit** button to close the window and return to the Create Network dialog box.
4. To configure a DHCP server, click the **Override DHCP server** box 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 this box is not checked, the **DHCP Server IP Address** field is not displayed and the DHCP server IP address is generated automatically. The automatically generated address is `network_IP_address_subnet.254`, or if the default gateway is using that address, `network_IP_address_subnet.253`.



Figure: DHCP Server IP Field

5. When all the information is correct, click the **Save** button to configure the network connection, close the *Create Network* dialog box, and return to the *Network Configuration* window.
6. Click the **Close** button to close *Network Configuration* window.

 **Note:** You can also specify network mapping to control network configuration for the VMs when they are started on the remote site. For more information on configuring networking mapping on remote site, see [Configuring a Remote Site \(Physical Cluster\)](#) on page 317.

## Modifying Network Connections

To modify or delete a network configuration defined through Nutanix virtualization management, do the following:

1. In the gear icon pull-down list of the main menu , select **Network Configuration**.

 **Note:** This option does not appear when running a hypervisor that does not support this feature.

The Network Configuration window appears. It lists the following information for each defined network configuration:

- **NAME:** Displays the name of the network.
- **VLAN ID:** Displays the VLAN identification number for the network in the form `vlan.#`, for example `vlan.27` for virtual LAN number 27.

A screenshot of the 'Network Configuration' window. At the top, there's a header bar with the title 'Network Configuration' and a help/cross icon. Below the header is a message: 'Configure one or more networks to be used for NIC configuration.' A 'Create Network' button is located in the top-left corner of the main content area. The main content area contains a table with two rows:

NAME	VLAN ID	edit icon	delete icon
network1	vlan.10	edit icon	delete icon
network2	vlan.12	edit icon	delete icon

At the bottom right of the window is a 'Close' button.

Figure: Network Configuration Window

2. To modify a network configuration, select the target line and click the pencil icon (on the right).

The Update Network Configuration dialog box appears, which contains the same fields as the Create Network Configuration dialog box (see [Configuring Network Connections](#) on page 151). Do the following:

- a. Update the field values as desired.
  - b. When the configuration is correct, click the **Save** button to close the dialog box, update the network configuration, and return to the Network Configuration window.
3. To delete a network configuration, select the target line and click the X icon (on the right). A window prompt appears to verify the action; click the **OK** button. The network configuration is removed from the list.
4. Click the **Close** button to close the *Network Configuration* window.

## Configuring Network Switch Information

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. Switch port discovery is supported with switches that are RFC 2674 compliant. Switch port discovery involves obtaining statistics from the 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.

To configure one or more network switches for statistics collection, do the following:

1. In the gear icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Network Switch**.



**Note:** This option does not appear when running a hypervisor that does not support this feature.

The *Network Switch Configuration* dialog box appears.

2. Click the **Switch Configuration** tab and then click the **Add Switch Configuration** button.
3. 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 fully qualified host name of each host in the cluster that uses this switch to route traffic.  
When there are multiple hosts, enter the addresses in a comma separated list. Failing to add the host list might result in issues with switch port discovery.



**Note:** Selecting a profile populates the remaining fields automatically with the profile values. If you have not created a profile (or select **None** from the list), you must enter the values in the remaining fields manually.

4. **SNMP Version:** Select the SNMP version to use from the pull-down list.  
The options are **SNMPv2c** and **SNMPv3**.
5. **SNMP Security Level (SNMPv3 only):** Select the security level to enforce from the pull-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:** 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 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.

- i. **SNMP Authentication Pass Phrase:** Enter the appropriate authentication pass phrase.
- j. **SNMP Privacy Type:** Select the privacy protocol to use from the pull-down list.  
The options are **None**, **AES**, and **DES**.
- k. **SNMP Privacy Pass Phrase:** Enter the appropriate privacy pass phrase.

- I. When all the fields are correct, click the **Save** button.

This 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).

**Network Switch Configuration**

Configure one or more network switches for stats collection.

Switch Configuration - SNMP Profile

SWITCH MANAGEMENT IP ADDRESS

HOST IP ADDRESSES OR HOST NAMES (SEPARATED BY COMMAS)

SNMP PROFILE

SNMP VERSION

SNMP SECURITY LEVEL

SNMP COMMUNITY NAME

SNMP USERNAME

**Cancel** **Save**

SNMP COMMUNITY NAME

SNMP USERNAME

SNMP AUTHENTICATION TYPE

SNMP AUTHENTICATION PASS PHRASE

SNMP PRIVACY TYPE

SNMP PRIVACY PASS PHRASE

**Cancel** **Save**

The screenshot displays a software interface titled "Network Switch Configuration". At the top, there are standard window controls for help (?) and close (X). Below the title, a descriptive text says "Configure one or more network switches for stats collection." followed by a breadcrumb navigation "Switch Configuration - SNMP Profile". The main area contains two distinct configuration sections, each with several input fields and dropdown menus. The first section includes fields for "SWITCH MANAGEMENT IP ADDRESS" (a text input), "HOST IP ADDRESSES OR HOST NAMES (SEPARATED BY COMMAS)" (a text input), "SNMP PROFILE" (a dropdown menu set to "None"), "SNMP VERSION" (a dropdown menu set to "SNMP v3"), and "SNMP SECURITY LEVEL" (a dropdown menu set to "No Authorization No Privacy"). It also has fields for "SNMP COMMUNITY NAME" and "SNMP USERNAME", both represented by text inputs. The second section, which is partially visible, includes fields for "SNMP AUTHENTICATION TYPE" (dropdown menu set to "None") and "SNMP AUTHENTICATION PASS PHRASE" (text input), as well as "SNMP PRIVACY TYPE" (dropdown menu set to "None") and "SNMP PRIVACY PASS PHRASE" (text input). At the bottom of each section are "Cancel" and "Save" buttons. A vertical scroll bar is located on the right side of the window.

Figure: Network Switch Configuration Window (add configuration)

## Creating SNMP Profiles

If you need to configure multiple network switches, it may be useful to create one or more SNMP profiles that can be applied when configuring the switches (see [Configuring Network Switch Information](#) on page 155). To create an SNMP profile, do the following:

1. In the gear icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Network Switch**.  
The *Network Switch Configuration* dialog box appears.
2. Click the **SNMP Profile** tab and then click the **Add SNMP Profile** button.
3. Do the following in the indicated fields:
  - a. **Profile Name:** Enter a name for the profile.  
The name can be anything as it is for display purposes only.
  - b. **SNMP Version:** Select the SNMP version to use from the pull-down list.  
The options are **SNMPv2c** and **SNMPv3**.
  - c. **SNMP Security Level (SNMPv3 only):** Select the security level to enforce from the pull-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.
  - d. **SNMP Community Name:** 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. When all the fields are correct, click the **Save** button.

This saves the profile and displays the new entry in the SNMP Profile tab.

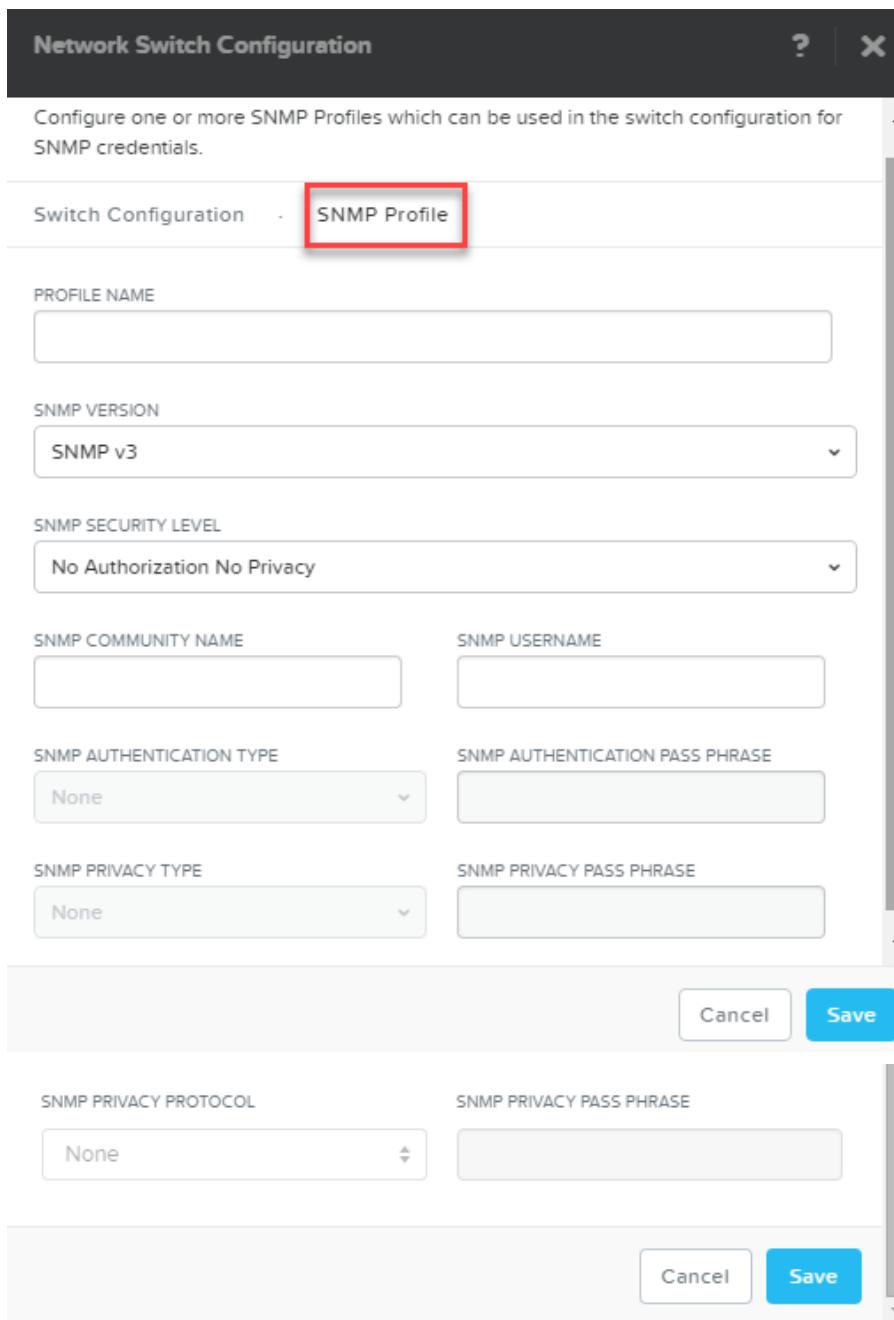


Figure: Network Switch Configuration Window (add SNMP profile)

## Modifying Switch Information

To modify the information about a network switch (or the SNMP profile used in the switch information), do the following:

1. In the gear icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Network Switch**.  
The *Network Switch Configuration* dialog box appears.

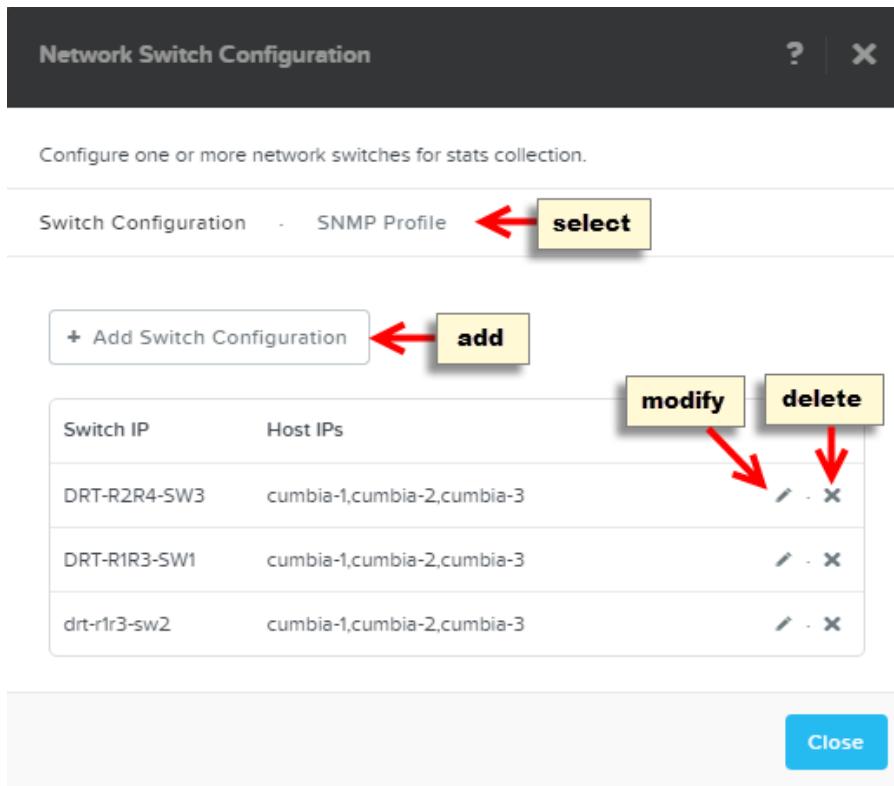


Figure: Network Switch Configuration Window

2. To modify a switch configuration (or SNMP profile), select the **Switch Configuration** (or **SNMP Profile**) tab, go to the target switch (or profile) entry in the table, and click the pencil icon.  
This displays the configuration fields (see [Configuring Network Switch Information](#) on page 155 or [Creating SNMP Profiles](#) on page 158). Edit the entries as desired and then click the **Save** button.
3. To delete a switch configuration (or SNMP profile), select the **Switch Configuration** (or **SNMP Profile**) tab, go to the target switch (or profile) entry in the table, and click the X icon.  
This deletes the entry and removes it from the table.

## 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.

You cannot use the visualizer to configure the 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. See [Configuring Network Switch Information](#) on page 155.
- Configure SNMP v3 or SNMP v2c on the first-hop switches. 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.
- 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 best-effort basis. For information about configuring LLDP or CDP, see the switch manufacturer's documentation.

## Supported Switches

The network visualizer supports the following switches:

- Cisco Nexus Series switches
- Cisco Catalyst Series switches
- Dell switches
- Arista switches

## 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.

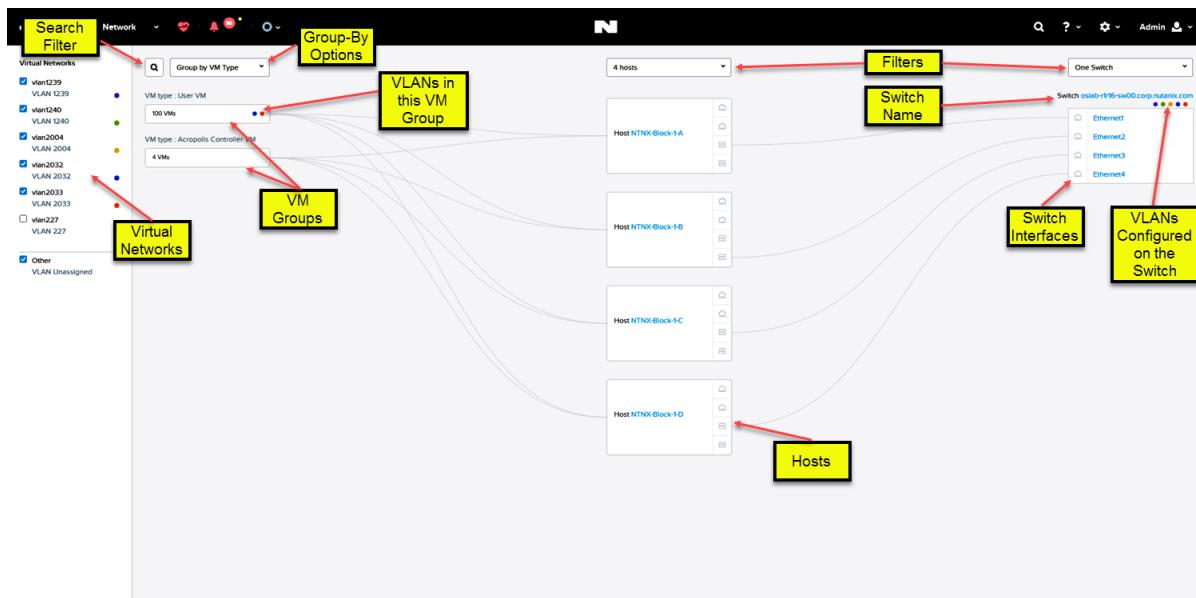


Figure: Network Visualizer

The network visualizer includes the virtual networks pane and the topology view.

## Virtual Networks Pane

Lists the virtual networks (VLANs) configured on the Nutanix cluster. Selecting a VLAN includes the VMs on that VLAN in the topology view. Conversely, clearing a check box excludes the VMs on that VLAN from the topology view. You can show up to five VLANs at a time.

The check box titled Other corresponds to VMs that are not on any VLAN. At a minimum, this check box is associated with the Controller VMs in the cluster.

## Topology View

Displays the network topology. The topology view shows the following entities:

### VLANs

VLANs configured on the cluster. The visualizer displays a different color for each VLAN. It shows the VLANs to which a VM or the VMs in a VM group belong. It also shows which VLANs are configured on a first-hop switch.

### VMs

VMs on the VLANs that are selected in the virtual networks pane. Filter and group-by options enable you to customize the topology view.

### Hosts

Hosts in the Nutanix cluster. The filter above the hosts enables you to specify which hosts you want to show in the topology view.

### Switches

First-hop switches and the VLANs configured on each of them. The filter above the switches enables you to specify which switches you want to show in the topology view.

## Viewing the Network Visualizer

To view the network visualizer, do the following:

1. Log on to the web console.
2. Click **Network** in the main menu.

## Customizing the Topology View

You can group VMs by a VM property or use a search filter to specify which network devices you want to show or exclude.

To customize the topology view, do the following:

1. Specify which VLANs you want to show in the topology view:
  - In the virtual networks pane, select the VLANs that you want to show in the topology view and clear those that you do not want to show.
  - Select or clear **Other** if you want to include or exclude, respectively, the VMs that are not on any VLAN.

You can show a maximum of five VLANs at a time.

2. Specify which VMs you want to show in the topology view:
  - Select a 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.

**3.** Specify which Nutanix hosts you want to show in the topology view:

- Click the menu above the Nutanix hosts.
- Select the hosts that you want to show and clear those that you want to exclude.

**4.** Specify which switches you want to show in the topology view:

- Click the menu above the switches.
- Select the switches that you want to show and clear those that you want to exclude.

## Viewing VM Information

In the visualizer, you can view the settings and real-time statistics of a virtual NIC.

To view VM information, do the following:

1. Use the group-by and filtering capabilities of the visualizer (see [Customizing the Topology View](#) on page 162) to show the VM you want, and then click the name of the VM.  
The VM network information window appears.
2. From the virtual NIC list at the top of the dialog box, select the NIC for which you want to show settings and statistics.  
For information about the statistics that are displayed for the virtual NICs, see [VM NICs Tab](#) on page 361.
3. Optionally, point to a location on a graph to view the value at that point in time.
4. If you want additional information about the VM, click **Go to VM Details**.  
The **VM** table view on the **VM** page is displayed.



**Tip:** You can return to the visualizer by pressing the back button in your browser.

## Viewing Host Information

In the visualizer, you can view the internal network diagram of a Nutanix host. You can click a network component, such as a bridge or bond, to view the settings and statistics of that component.

To view host information, do the following:

1. In the topology view, click the name of a host.  
The host network information window appears. The window shows a diagram of the host's internal network. The right pane displays host network information.
2. Click any network component in the diagram and view its network settings and statistics 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 361.
  - Click a bridge to view the settings 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.
  - Click a host interface to view the settings of the interface. For a host interface, statistics are shown in addition to interface settings. 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 host NICs, see [Host NICs Tab](#) on page 185.
  - A solid line leading from a bond to a host interface indicates an active connection. A dotted line indicates a backup connection.
3. If you want additional information about the host, click **Go to VM Details**.  
The **Host** table view on the **Hardware** page is displayed.



**Tip:** You can return to the visualizer by pressing the back button in your browser.

## Viewing Switch Information

In the visualizer, you can view both switch-level information and interface-level information.

### Viewing Switch-Level Information

Switch-level information includes details such as switch name, vendor, and management IP address.

To view switch-level information, do the following:

1. In the topology view, click the name of a switch.  
The switch information window is displayed.
2. To view additional switch information, click **Go to Switch Details**.  
The **Switch** view on the **Hardware** page is displayed.



**Tip:** You can return to the visualizer by pressing the back button in your browser.

### Viewing Interface-Level Information

Interface-level information includes details such as interface name, physical address, and interface type. The visualizer also displays statistics for each interface.

To view interface-level information, do the following:

1. Click a switch interface.

The switch port information window is displayed. The window shows both network settings and interface statistics.

For information about the statistics that are displayed for switch interfaces, see [Switch Tab](#) on page 180.

2. Optionally, to show the value at any given point in time in a graph, point to the location on the graph.

## Hardware Management

A Nutanix block is a 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 also includes dual power supplies. A Nutanix cluster can contain an unlimited number of nodes (and blocks), and you can expand the cluster size at any time.

- You can monitor hardware configurations and status across the cluster through the web console (see [Hardware Dashboard](#) on page 166).
- You can expand the cluster through the web console (see [Expanding a Cluster](#) on page 186).



Figure: Nutanix Block

## Hardware Dashboard

The Hardware dashboard displays dynamically updated information about the hardware configuration in a cluster. To view the Hardware dashboard, select **Hardware** from the pull-down list on the far left of the main menu.

### Menu Options

In addition to the main menu (see [Main Menu Options](#) on page 32), the Hardware screen includes a menu bar with the following options:

- **View selector.** The Hardware dashboard provides three viewing modes.
  - Click the **Overview** button on the left to display hardware information in a summary view (see [Hardware Overview View](#) on page 167).

- Click the **Diagram** button to display a diagram of the cluster nodes from which you get detailed hardware information by clicking on a component of interest (see [Hardware Diagram View](#) on page 168).
- Click the **Table** button 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 (see [Hardware Table View](#) on page 176).
- Expand cluster button.** Click the **Expand cluster** button on the right to add nodes to the cluster (see [Expanding a Cluster](#) on page 186).
- Page selector.** In the Table view, hosts and disks are listed 10 per page. When there are more than 10 items in the list, left and right paging arrows appear on the right, along with the total count and the count for the current page.
- Export table content.** In the Table view, you can export the table 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 pull-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.



Figure: Hardware Dashboard Menu

## Hardware Overview View

The Hardware Overview view displays hardware-specific performance and usage statistics on the left plus the most recent hardware-specific alert and event messages on the right. 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.

The following figure is a sample view, and the table describes each field in this view.

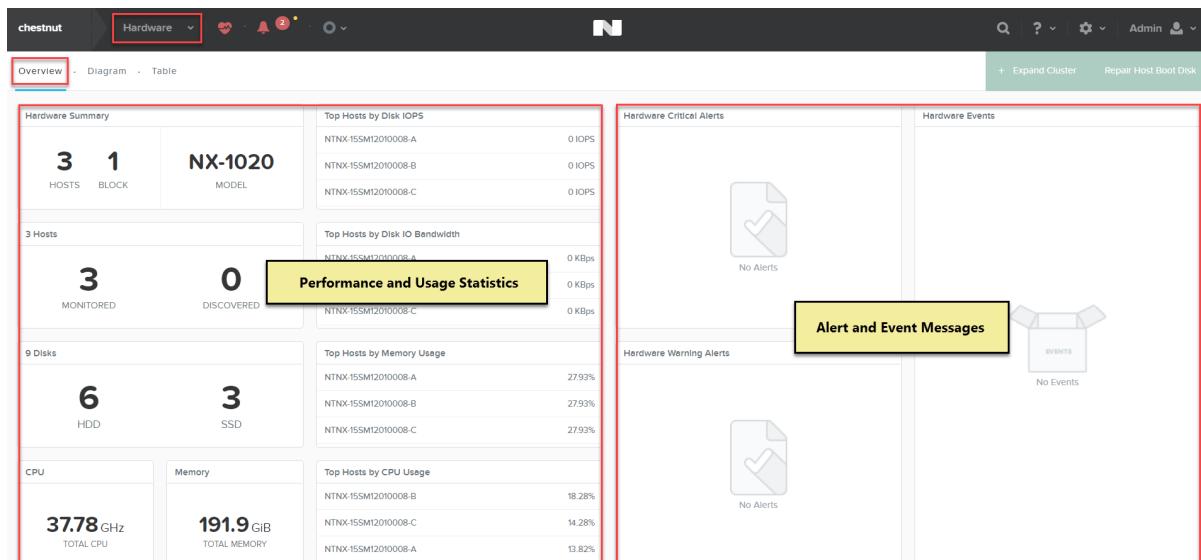


Figure: Hardware Overview View



**Note:** See [Understanding Displayed Statistics](#) on page 41 for information about how the statistics are derived.

### Hardware Overview View Fields

Name	Description
Hardware Summary	Displays the number of hosts and blocks in the cluster. It also displays the Nutanix model number.
Hosts	Displays the number of hosts in the cluster broken down by on, off, and suspended states. It also displays the number of discovered nodes that have not yet been added to the cluster.
Disks	Displays the total number of disks in the cluster broken down by tier type (SSD-PCIe, SSD-SATA, DAS-SATA).
CPU	Displays the total amount of CPU capacity (in GHz) in the cluster.
Memory	Displays the total amount of memory (in GBs) in 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 I/O bandwidth used per host for the 10 most active hosts. The value is displayed in an appropriate metric (MBps, KBps, and so on) depending on 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 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 (see <a href="#">Alerts Dashboard</a> ).
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 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.

### Hardware Diagram View

The Hardware Diagram view displays information about hosts and disks. The displayed information is dynamically updated to remain current.

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:** See [Understanding Displayed Statistics](#) on page 41 for information about how the statistics are derived.

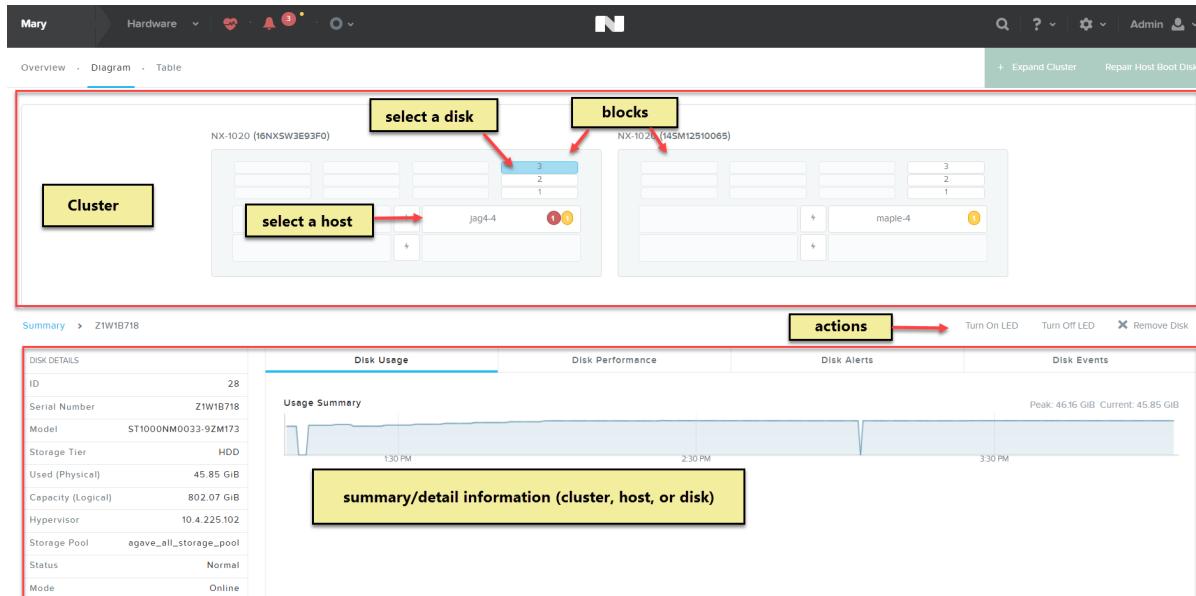


Figure: Hardware Diagram View

## 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 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 **Remove Host** link to remove this host from the cluster.
- Five tabs appear that display information about the selected host (see following sections for details about each tab): **Host Performance**, **Host Usage**, **Host Alerts**, **Host Events**, **Host NICs**.



Figure: Hardware Diagram View: Hosts

## Host Detail Fields

Parameter	Description	Values
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 this host.	xxx [GB TB]
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 this host.	xxx [MB GB]
CPU Capacity	Displays the total CPU capacity for this host.	xxx [GHz]
No. of VMs	Displays the number of VMs running on this host.	(number)
Opslog Disk %	Displays the percentage of the operations log (opslog) capacity currently being used. The opslog resides on the metadata disk.	[0 - 100%]
Opslog Disk Size	Displays the current size of the operations log. (The opslog maintains a record of write requests in the cluster.) A portion of the metadata disk is reserved for the opslog, and you can change the size through the nCLI.	xxx [GB]
Monitored	Displays whether the host is high availability (HA) protected. A <b>true</b> value means HA is active for this host. A <b>false</b> value means VMs on this host are not protected (will not be restarted on another host) if the host fails. Normally, this value should always be <b>true</b> . A <b>false</b> value is likely a sign of a problem situation that should be investigated.	[true false]
Hypervisor	Displays the name and version number of the hypervisor running on this host.	(name and version #)

Parameter	Description	Values
Datastores	Displays the names of any datastores. This field does not appear in <i>Prism Central</i> .	(name)

## 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 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**.

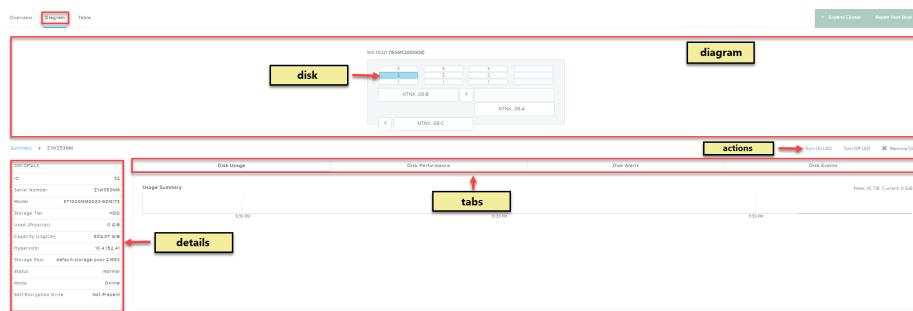


Figure: Storage Diagram View: Disks

## Disk Detail Fields

Parameter	Description	Values
ID	Displays the disk identification number.	(ID number)
Serial Number	Displays the disk serial number.	(serial 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 (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)
Storage Pool	Displays the name of the storage pool in which the disk resides.	(name)

Parameter	Description	Values
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 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 (see <a href="#">Configuring Data-at-Rest Encryption</a> on page 619), 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]

### 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) 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**.

### Performance Tab

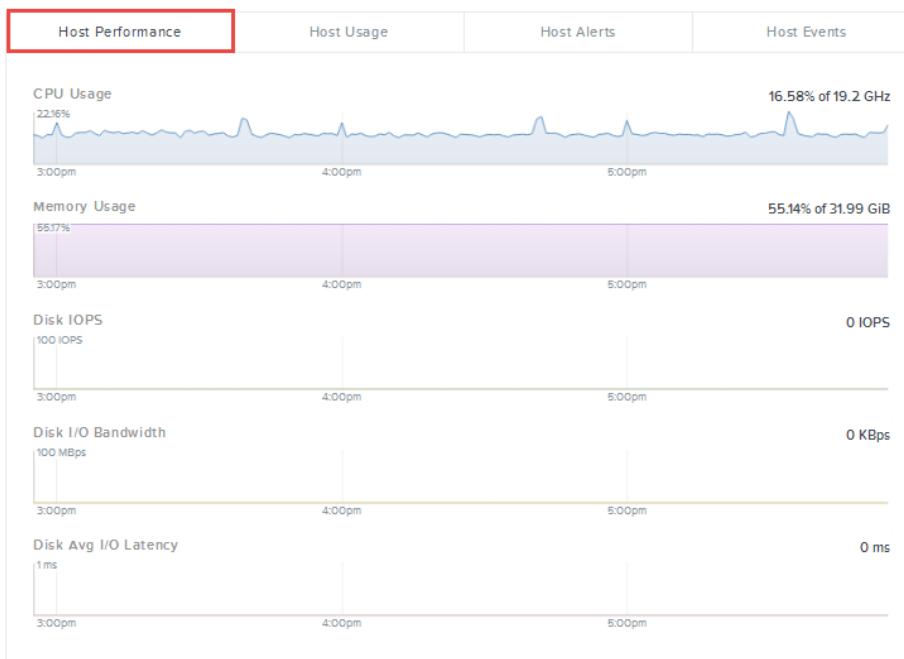
The Performance tab displays graphs of performance metrics. The tab label and number of graphs varies depending on what is selected in the diagram:

- **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 blue link in the upper right of the graph (see [Analysis Dashboard](#) on page 401). 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: Performance Tab*

## Usage Tab

The 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 diagram:

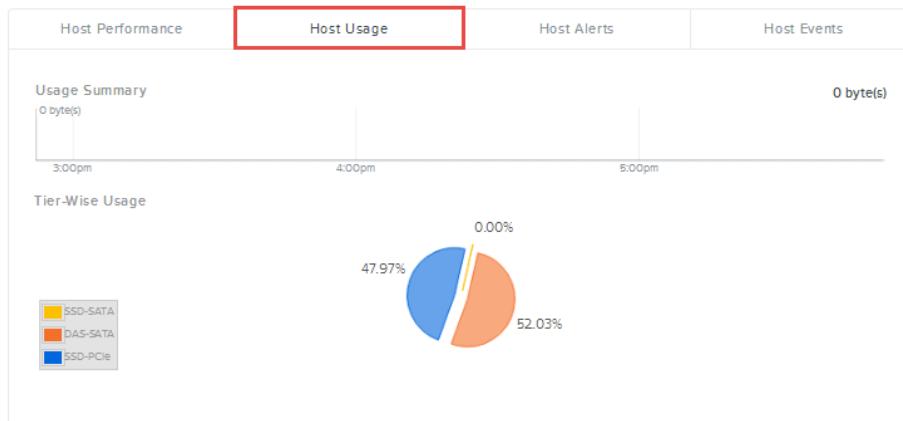
- **Host Usage** (host selected). Displays usage statistics for the selected host.
- **Disk Usage** (disk selected). Displays usage statistics for the selected disk.

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 (see [Analysis Dashboard](#) on page 401).

- **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: 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 (see [Alert Messages View](#) on page 411). Click the **Unresolved X** button in the filter field to also display resolved alerts.

The figure shows the Host Alerts tab of the Prism Web Console. At the top, there is a horizontal navigation bar with four tabs: Host Performance, Host Usage, Host Alerts (which is highlighted with a red border), and Host Events. Below the tabs, there is a search/filter field with the text "Unresolved" and a close button "X". To the right of the search field, it says "6 Alerts". There is also a set of navigation icons. The main area displays a table of alerts. The columns are labeled: SEVERITY, ISSUE, TIMESTAMP, ENTITIES, and DOCUMENTATION. The table contains the following data:

SEVERITY	ISSUE	TIMESTAMP	ENTITIES	DOCUMENTATION
<input type="checkbox"/>	Info NIC eth0 in host 10.4.60.203 has encountered more than 200 rx_errors in one hour.	01-16-15, 11:00:07pm	Host	Cause Resolution ✓
<input type="checkbox"/>	Critical There have been 10 or more cluster services restarts within 15 minutes in the Controller VM 10.4.60.207.	01-16-15, 04:29:07pm	Host	Cause Resolution ✓
<input type="checkbox"/>	Critical Controller VM 10.4.60.207 has been rebooted on Fri Jan 16 16:27:00 2015.	01-16-15, 04:29:04pm	Host	Cause Resolution ✓
<input type="checkbox"/>	Critical Stargate on Controller VM 10.4.60.207 is down for 331 seconds.	01-16-15, 04:22:45pm	Host	Cause Resolution ✓
<input type="checkbox"/>	Critical Hypervisor 10.4.60.203 is not reachable from Controller VM 10.4.60.208 in the last six attempts.	01-16-15, 04:22:07pm	Host	Cause Resolution ✓
<input type="checkbox"/>	Critical Hypervisor 10.4.60.203 is not reachable from Controller VM 10.4.60.208 in the last three attempts.	01-16-15, 04:19:06pm	Host	Cause Resolution ✓

*Figure: 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 (see [Event Messages View](#) on page 413). Click the **Include Acknowledged** button to also display acknowledged events.

Performance Summary		Hardware Alerts		Hardware Events	
<input type="checkbox"/> Include Acknowledged · No entities found · < > ⚙️					
	MESSAGE	ENTITIES	MODIFIED BY	TIMESTAMP	

Figure: 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.
- **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 Rate.** Displays the host NIC received packets rate.
- **Tx Rate.** Displays the host NIC transmitted packets rate.
- **Network Usage Rate.** Displays the host NIC total network usage rate.

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 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.)
- **Total Packets Transmitted.** Displays a monitor of the total packets that were transmitted.
- **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 of error packets that were received.



Figure: Host NICs Tab

## Hardware Table View

The Hardware Table view displays information about hosts and disks 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 displayed information is dynamically updated to remain current.

The Hardware table view is divided into two sections:

- The top section is a table. Each row represents a single host or disk and includes basic information about that host or disk. 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.

The screenshot shows the Prism Web Console interface with the 'Hardware' tab selected. At the top, there's a navigation bar with 'Overview', 'Diagram', and 'Table' buttons. Below that is a sub-navigation bar with 'Host', 'Disk', and 'Switch' buttons, where 'Host' is highlighted. The main content area is divided into two sections: a table at the top and a summary/detial information section below it. The table has columns for ID, Name, IP Address, Model, Status, and various performance metrics like CPU Usage, Memory Usage, and Disk IOPS. A yellow box highlights the table area with the text 'table information (host, disk, or switch)'. The summary section on the right contains tabs for 'Disk Details', 'Usage Summary', 'Disk Performance', 'Disk Alerts', and 'Disk Events'. A yellow box highlights this area with the text 'summary/detail information (cluster, host, disk, or switch)'. On the far right, there are buttons for 'actions' (Turn On LED, Turn Off LED, Remove Disk), 'export', and 'search'. A yellow box highlights the search button with the text 'search'. Arrows point from the text labels to their respective components in the interface.

Figure: Hardware Table Screen

## Host Tab

Clicking the **Host** tab displays information about 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 **Remove Host** link to remove this host from the cluster.
- Five tabs appear that display information about the selected host (see following sections for details about each tab): **Host Performance**, **Host Usage**, **Host Alerts**, **Host Events**, **Host NICs**.



Figure: Hardware Table View: Host Tab

### Host Table and Detail Fields

Parameter	Description	Values
<i>Host Table Fields (upper screen)</i>		
Host Name	Displays the name of the host.	(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 this host.	xxx [GHz]
Memory Usage	Displays the percentage of memory capacity currently being used by this host.	0 - 100%
Memory Capacity	Displays the memory capacity of this host.	xxx [MB GB]
Total Disk Usage	Displays the percentage of storage space used and total disk capacity of this host.	[0 - 100%] of xxx [TB]
Disk IOPS	Displays I/O operations per second (IOPS) for this host.	[0 - unlimited]
Disk IO B/W	Displays I/O bandwidth used per second for this host.	xxx [Mbps Kbps]
Disk IO Latency	Displays the average I/O latency (in milliseconds) for this host.	xxx [ms]
<i>Host Detail Fields (lower screen)</i>		
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)

Parameter	Description	Values
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 this host.	xxx [GB TB]
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 this host.	xxx [MB GB]
CPU Capacity	Displays the total CPU capacity for this host.	xxx [GHz]
No. of VMs	Displays the number of VMs running on this 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>true</b> value means HA is active for this host. A <b>false</b> value means VMs on this host are not protected (will not be restarted on another host) if the host fails. Normally, this value should always be <b>true</b> . A <b>false</b> value is likely a sign of a problem situation that should be investigated.	[true false]
Hypervisor	Displays the name and version number of the hypervisor running on this host.	(name and version #)
Datastores	Displays the names of any datastores.	(name)

## 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**.



Figure: Hardware Table View: Disk Tab

### Disk Table and Detail Fields

Parameter	Description	Values
<b>Disk Table Fields (upper screen)</b>		
Disk ID	Displays the disk identification number.	(ID number)
Serial Number	Displays the disk serial number.	(serial number)
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]
Mode	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]
<b>Disk Detail Fields (lower screen)</b>		
ID	Displays the disk identification number.	(ID number)
Serial Number	Displays the disk serial number.	(serial number)

Parameter	Description	Values
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 (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)
Storage Pool	Displays the name of the storage pool in which the disk resides.	(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 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 (see <a href="#">Configuring Data-at-Rest Encryption</a> on page 619), 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 (see [Configuring Network Switch Information](#) on page 155), but only the switches that are actually being used for virtual NIC traffic appear in this table. 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).

The screenshot shows the 'Hardware Table View: Switch Tab' in the Prism Web Console. At the top, there are tabs for 'Host', 'Disk', and 'Switch', with 'Switch' being the active tab. Below the tabs is a search bar and a 'table' button. The main area is divided into three sections:

- Summary**: A table showing two switches: 'drt-rl3-sw1' (Arista Networks) and 'drt-rl3-sw2.nutanix.com' (Cisco). The Cisco entry includes a detailed description of the Cisco IOS Software.
- switch details**: A table showing switch details for 'drt-rl3-sw1'. It includes columns for Name, Vendor Name, Management Addresses, and Services.
- Physical Switch Interfaces**: A table showing physical switch interfaces for 'drt-rl3-sw1'. It includes columns for Physical Switch Interface, Switch ID, Index, MTU (in bytes), MAC Address, Unicast Rx Pkts, Unicast Tx Pkts, Error Rx Pkts, Error Tx Pkts, Discard Rx Pkts, and Discard Tx Pkts. The table lists four interfaces: Ethernet2/1, Ethernet2/1, Ethernet2/2, and Ethernet2/3.

Figure: Hardware Table View: Switch Tab

### 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)
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)

Parameter	Description	Values
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)

When you click a physical switch interface entry, usage graphs about that interface appear below the table:

- **Unicast Packets Received.** Displays a monitor of the received unicast packets 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.)
- **Unicast Packets Transmitted.** Displays a monitor of the transmitted unicast packets.
- **Error Packets Received.** Displays a monitor of error packets received.
- **Dropped Packets Received.** Displays a monitor of received packets that were dropped.
- **Dropped Packets Transmitted.** Displays a monitor of transmitted packets that were dropped.

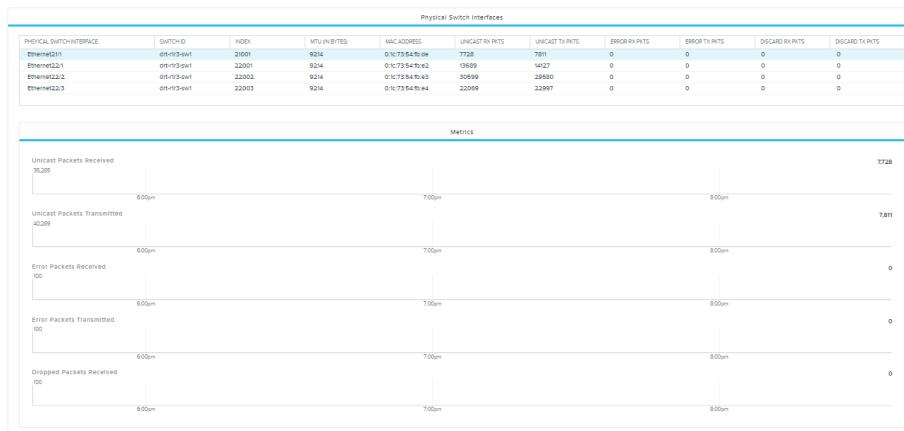


Figure: Physical Switch Interface Monitors

## Cluster Summary Information

When a host or disk 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 **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**.

## Performance Tab

The 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 (see [Analysis Dashboard](#) on page 401). 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.

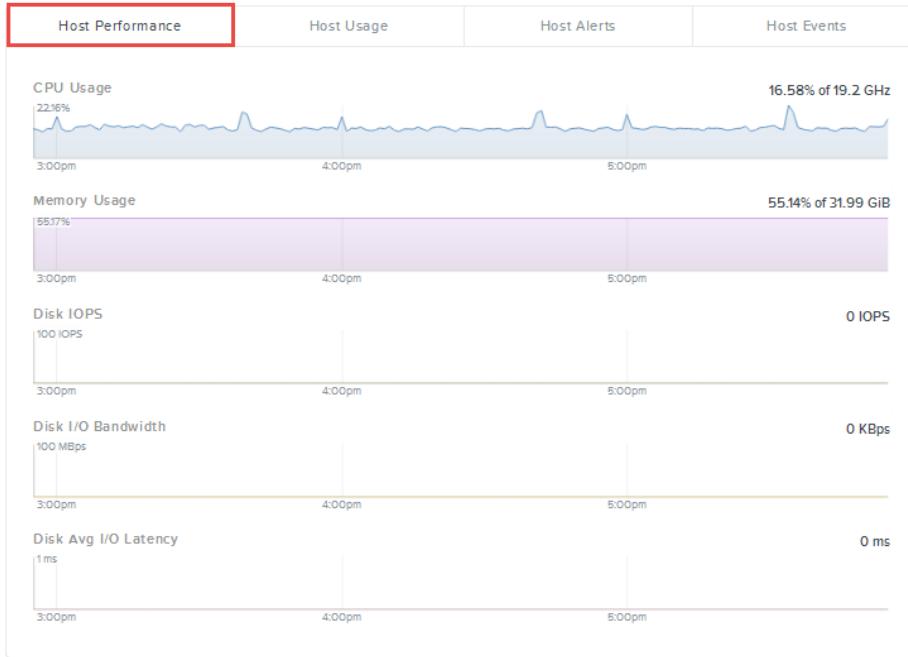


Figure: Hardware Table View: Performance Tab

## Usage Tab

The 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 (see [Analysis Dashboard](#) on page 401).
- **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.

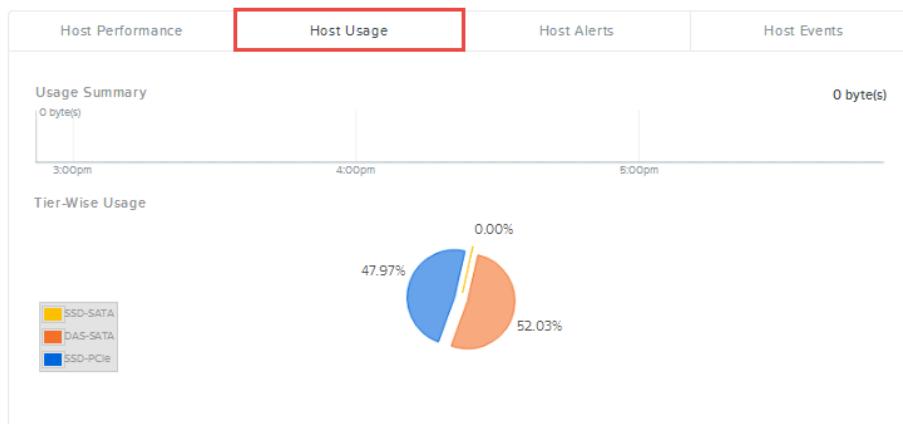


Figure: Hardware Table View: Usage Tab

## Alerts Tab

The Alerts tab displays the unresolved alert messages about hosts, disks, and other hardware in the same form as the Alerts page (see [Alert Messages View](#) on page 411). Click the **Unresolved X** button in the filter field to also display resolved alerts.

A screenshot of a software interface titled "Host Alerts". The table has columns: SEVERITY, ISSUE, TIMESTAMP, ENTITIES, and DOCUMENTATION. The data rows are:

SEVERITY	ISSUE	TIMESTAMP	ENTITIES	DOCUMENTATION
<input type="checkbox"/>	Info NIC eth0 in host 10.4.60.203 has encountered more than 200 rx_errors in one hour.	01-16-15, 11:00:07pm	Host	<a href="#">Cause</a> <a href="#">Resolution</a>
<input type="checkbox"/>	Critical There have been 10 or more cluster services restarts within 15 minutes in the Controller VM 10.4.60.207.	01-16-15, 04:29:07pm	Host	<a href="#">Cause</a> <a href="#">Resolution</a>
<input type="checkbox"/>	Critical Controller VM 10.4.60.207 has been rebooted on Fri Jan 16 16:27:00 2015.	01-16-15, 04:29:04pm	Host	<a href="#">Cause</a> <a href="#">Resolution</a>
<input type="checkbox"/>	Critical Sargeate on Controller VM 10.4.60.207 is down for 331 seconds.	01-16-15, 04:22:45pm	Host	<a href="#">Cause</a> <a href="#">Resolution</a>
<input type="checkbox"/>	Critical Hypervisor 10.4.60.203 is not reachable from Controller VM 10.4.60.208 in the last six attempts.	01-16-15, 04:22:07pm	Host	<a href="#">Cause</a> <a href="#">Resolution</a>
<input type="checkbox"/>	Critical Hypervisor 10.4.60.203 is not reachable from Controller VM 10.4.60.208 in the last three attempts.	01-16-15, 04:19:06pm	Host	<a href="#">Cause</a> <a href="#">Resolution</a>

Figure: Hardware Table View: 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 (see [Event Messages View](#) on page 413). Click the **Include Acknowledged** button to also display acknowledged events.

A screenshot of a software interface titled "Hardware Events". The table has columns: MESSAGE, ENTITIES, MODIFIED BY, and TIMESTAMP. The message column contains several empty lines. The status bar at the top says "No entities found".

MESSAGE	ENTITIES	MODIFIED BY	TIMESTAMP

Figure: Hardware Table View: 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.) 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.

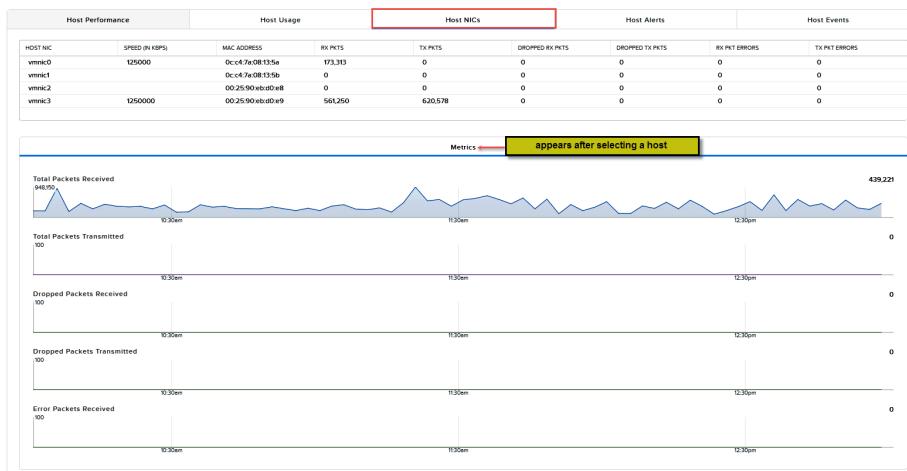


Figure: Host NICs Tab

## Expanding a Cluster

A cluster is a collection of nodes. New nodes can be added to a cluster at any time after they have been physically installed and connected to the network on the same subnet as the cluster.

### Before you begin:

- Check the *Health Dashboard* (see [Health Dashboard](#) on page 344). If any health checks are failing, resolve them to ensure that the cluster is healthy before adding any nodes.
- Allow any current add node operations to complete.
- If the Controller VMs in the cluster reside in a VLAN configured network, note the following before attempting to add any nodes:
  - If the cluster is running AHV (version 4.5 or later), the discovery process should find and allow you to add any factory-prepared nodes regardless of their current VLAN status (configured or not configured).
  - If the cluster is running ESXi or Hyper-V (or an earlier version of AHV), you must first configure the nodes in the VLAN before attempting to add them. Otherwise, the discovery process will not find these nodes. See the "Configuring the Cluster in a VLAN-Segmented Network" section in the *Acropolis Advanced Setup Guide* for VLAN configuration instructions.
- Ensure that all nodes are in the correct metadata state by checking the **Hardware** dashboard **Diagram** or **Table** view. 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**.
- If you try to add a node to the cluster with a different processor class, ensure that there are no running VMs on the node and the host has the following configuration:
  - ESXi: Verify that EVC is already 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 navigating to **Settings > Processor > Compatibility** in the **Action** pane of the Hyper-V Manager.
- AHV: The CPU features are automatically set in AHV clusters running AOS 4.5 or later releases. If you are upgrading from pre-4.5 release, you need to restart all the VMs for successful migration between nodes.



**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 G4 processor changes.

Power cycle guest VMs from the Prism web console VM dashboard. Do not perform a Guest Reboot; a VM power cycle is required in this case. See [VM Management](#) in the *Prism Web Console Guide*.

- If a node was physically added to a block (for example, if a single node was shipped from Nutanix and placed into an empty slot in an existing chassis), edit the `/etc/nutanix/factory_config.json` on the Controller VM to be added and update the following parameters:

*rackable\_unit\_serial*

Same as another Controller VM in the same block

*node\_position*

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.

- For expanding a XenServer cluster, ensure the following in addition to the preceding points:
  - The nodes that you want to add are not part of any other XenServer pool.
  - The nodes do not have any shared repositories.
  - The nodes do not have any VMs running on them.
- The cluster expansion process checks the memory allocation of the existing Controller VMs in the cluster and increases the base Controller VM memory allocation on the new node if necessary. The new Controller VM is upgraded to a maximum 32 GB.

The Controller VM is upgraded to a maximum 28 GB for nodes with ESXi hypervisor hosts with total physical memory of 64 GB. With total physical memory greater than 64 GB, the existing Controller VM memory is increased by 4 GB.

The process for adding a node varies depending on the cluster hypervisor type, AOS version, and Data-At-Rest Encryption status:



**Note:** You can re-image a node (both hypervisor and AOS) when adding it if AOS 4.5 or later is installed on the node. However, if it has a pre-4.5 version, you cannot re-image the node when adding it. Contact Nutanix customer support for help in re-imaging a pre-4.5 node.

## Node Addition Configurations

Configuration	Description
Same hypervisor and AOS version	The node is added to the cluster without re-imaging it.
AOS version is different	<p>The node is re-imaged before it is added.</p> <p> <b>Note:</b> If the AOS version on the node is different (lower) but the hypervisor version is the same, you have the option to upgrade just AOS from the command line. To do this, log into a Controller VM in the cluster and run the following command:</p> <pre>nutanix@cvm\$ /home/nutanix/cluster/bin/cluster -u new_node_cvm_ip_address upgrade_node</pre> <p>After the upgrade is complete, you can add the node to the cluster without re-imaging it. Alternately, if the AOS version on the node is higher than the cluster, you must either upgrade the cluster to that version (see <a href="#">Upgrading AOS</a> on page 79) or re-image the node.</p>
AOS version is same but hypervisor version is different	You are provided with the option to re-image the node before adding it. (Re-imaging is appropriate in many such cases, but in some cases it may not be necessary such as for a minor version difference.)
Data-At-Rest Encryption	<p>If Data-At-Rest Encryption is enabled for the cluster (see <a href="#">Data-at-Rest Encryption</a> on page 616), you must configure Data-At-Rest Encryption for the new nodes. (The new nodes must have self-encrypting disks.)</p> <p> <b>Note:</b> Re-imaging is not an option when adding nodes to a cluster where Data-At-Rest Encryption is enabled. Therefore, such nodes must already have the correct hypervisor and AOS version.</p>



**Note:** You can add multiple nodes to an existing cluster at the same time.



**Note:** 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](#).

To add one or more nodes to an existing cluster, do the following:

1. Either select **Expand Cluster** from the gear icon pull-down list of the main menu or go to the Hardware dashboard (see [Hardware Dashboard](#) on page 166) and click the **Expand Cluster** button. The network is searched for Nutanix nodes and then the *Expand Cluster* dialog box appears (on the "Host Selection" screen) with a graphical list of the discovered blocks and nodes.



**Note:** "Discovered" blocks are those with one or more unassigned factory-prepared nodes (meaning nodes with the hypervisor and Controller VM installed that are not in a cluster currently) residing on the same subnet as the cluster. Discovery of new Controller VMs relies on IPv6 multicast packets to be allowed through the physical switch. A lack of IPv6 multicast support might prevent node discovery and successful cluster expansion.

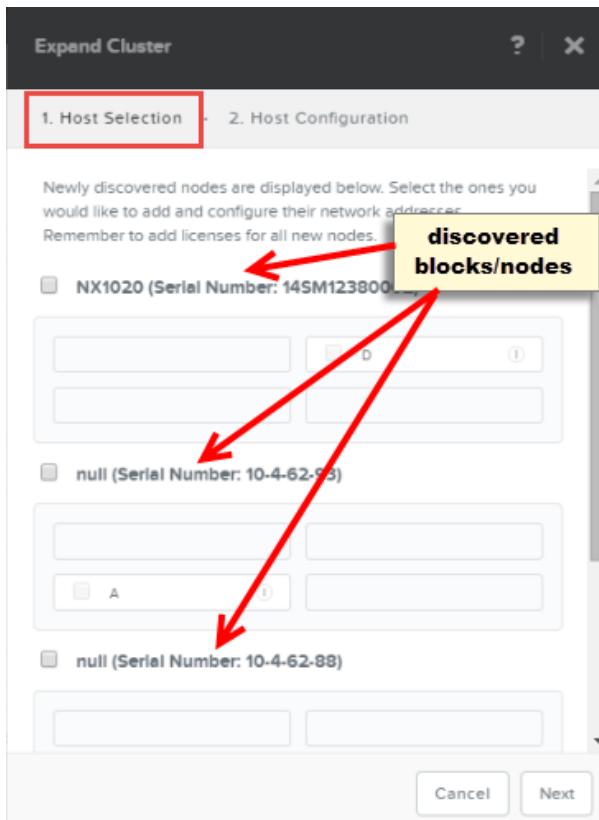


Figure: Expand Cluster Window: Host Selection (unselected blocks)

2. Select the check box for each block to be added to the cluster. All nodes within a checked block are also checked automatically; uncheck any nodes you do not want added to the cluster.  
When a block is checked, additional fields appear below the block diagram. A separate line for each node (host) in the block appears under each field name. In the following example, there is just one node in the block (Host D), so there is only a single line for each field.

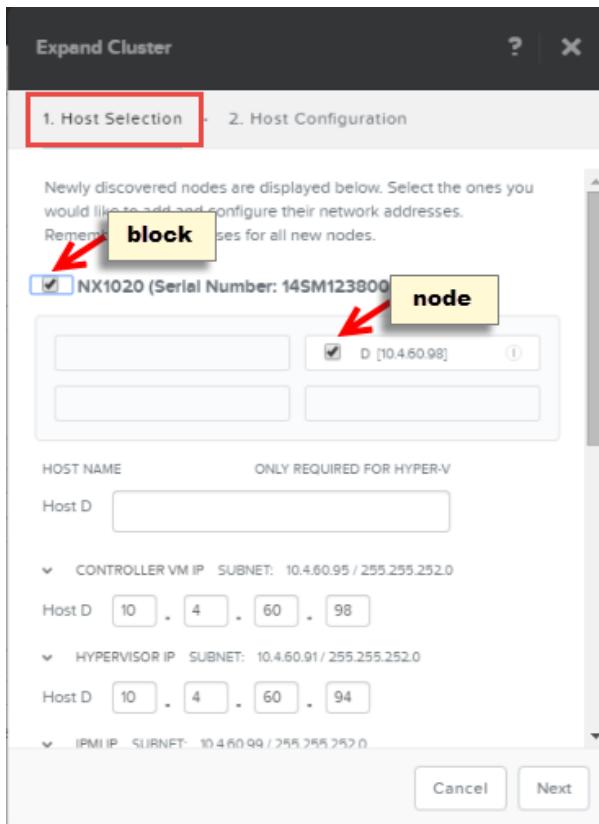


Figure: Expand Cluster Window: Host Selection (selected block)

3. Do the following in the indicated fields for each checked block:

a. **Host Name:** Enter the name of the host.

This is a required entry for Hyper-V clusters. Do not enter the fully-qualified domain name in the host name field. This field is ignored for ESXi and AHV clusters.

b. **Controller VM IP:** Review the Controller VM IP address assigned to each host and do one of the following:

- If the address is correct, do nothing in this field.
- If the address is not correct, either change the incorrect address or (if there are multiple hosts) enter a starting IP address for the Controller VMs on the top line (above the first host). The entered address 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 IP:** Repeat the previous step for this field.

This sets the hypervisor IP addresses for all the hosts to be added.

d. **IPMI IP:** Repeat the previous step for this field.

This 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 all the node values are correct, click the **Next** button (lower right).

The network addresses are validated before continuing. If an issue is discovered, the problem addresses are highlighted in red. If there are no issues, the process moves to the *Host Configuration* screen with a message at the top when the hypervisor, AOS, or other relevant feature is incompatible with the cluster versions.



**Note:** If Data-At-Rest Encryption is enabled, node imaging is bypassed. You can skip to Data-At-Rest Encryption configuration step.

4. If the node needs to be imaged, do the following in the **Hypervisor: <type>** field:

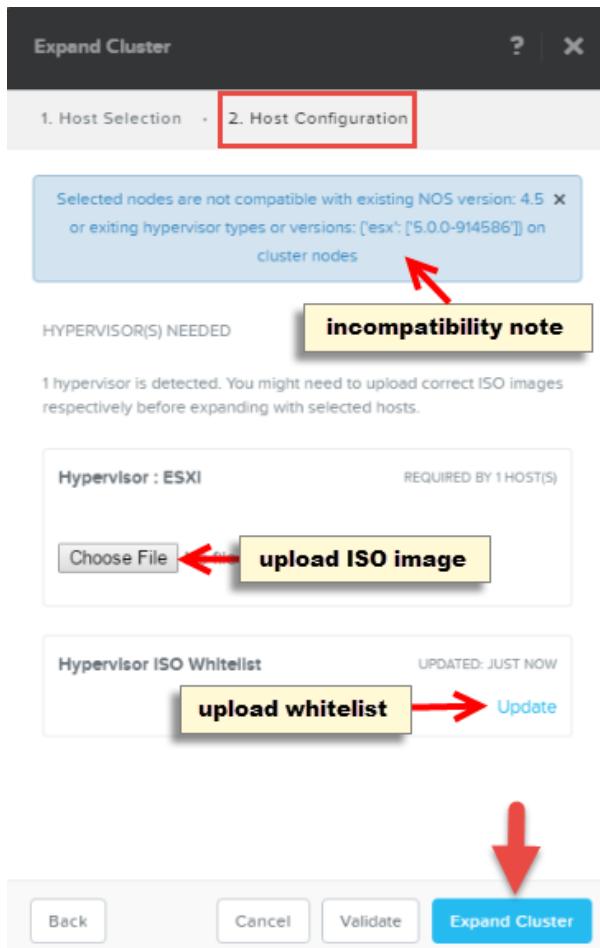


Figure: Expand Cluster Window: Host Configuration

- If a hypervisor image is listed in the **Hypervisor: <type>** field and it is the desired one, skip to the next step.  
If you uploaded a hypervisor image when adding nodes previously (and it is still compatible for imaging the new nodes), that image will be listed here. You can use that image or upload a different one.
- If no hypervisor image is listed or the listed one is not the desired one, click the **Choose File** button (which opens a search window), find and select the image file on your workstation, and then click the **Open** button (in the search window) to upload that image file.



**Note:** You must provide an ISO file for imaging ESXi or Hyper-V. You can get a compatible AHV image from the **Downloads > Hypervisor Details** page of the Nutanix support portal (see [Accessing the Nutanix Support Portal](#) on page 639). The AHV image to upload is an installation bundle (not an ISO file) such as `kvm_host_bundle_version#.tar.gz`. AOS includes a default AHV installation bundle named `kvm_host_bundle_version#.tar.gz`. If this

version is appropriate, use it instead of uploading an installation bundle from the support portal.

- c. 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 whitelist.

The cluster includes a hypervisor ISO whitelist, which lists the approved hypervisor images. You can only use an image that is in the approved list. See the *Hypervisor ISO Images* section in the *Field Installation Guide* for more information about the whitelist. If your hypervisor image was added to the official whitelist after the cluster was created (meaning the current whitelist is an older version that does not include your hypervisor image), you can update the whitelist as follows:

1. Download the latest hypervisor ISO whitelist from the **Downloads > Foundation** page of the Nutanix support portal.
  2. Click the **Update** link in the **Hypervisor ISO Whitelist** field.
  3. Click the **Choose File** button (which opens a search window), find and select the whitelist file on your workstation, and then click the **Open** button.
  4. Click the **Upload** button. The incompatible message will disappear and you can continue if the hypervisor image is on the uploaded whitelist.
5. [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.

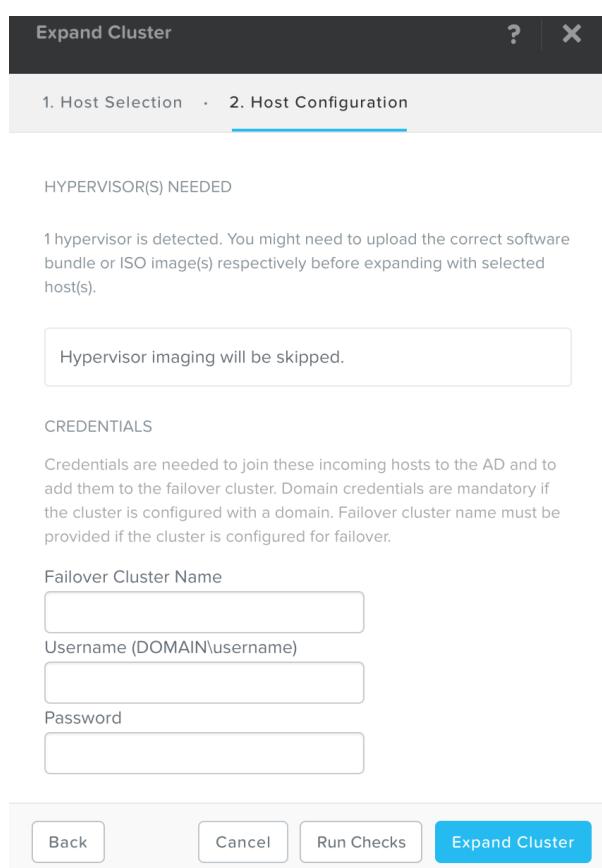
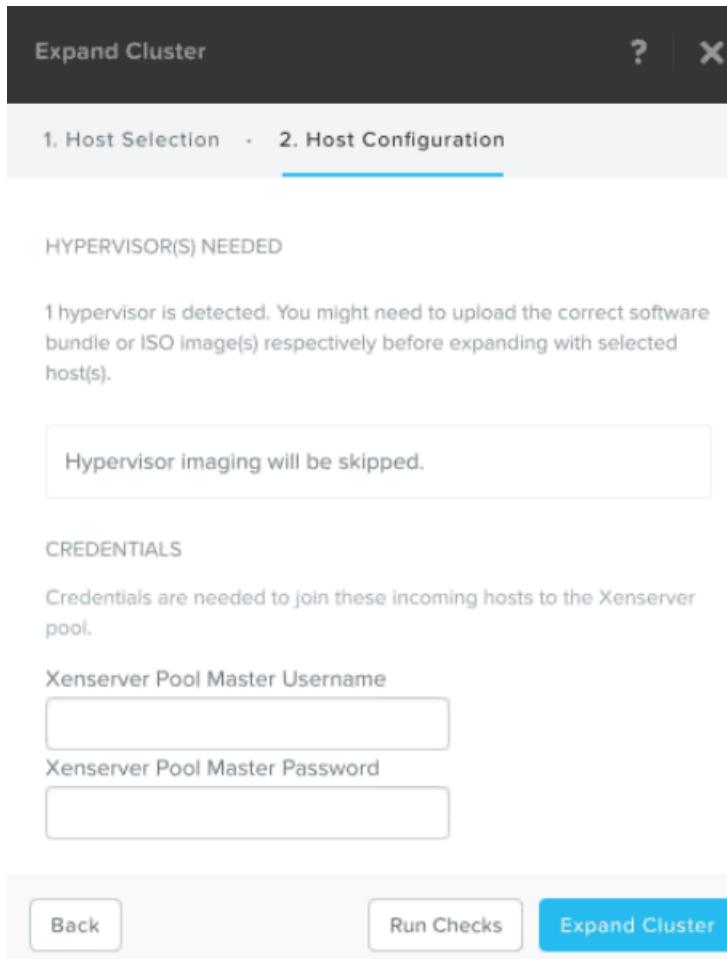


Figure: Expand Cluster Hyper-V Credentials

6. [XenServer only] Specify the credentials of the master node of the XenServer pool.



7. When all the fields are correct, click the **Expand Cluster** button.

The *Expand Cluster* dialog box closes and the add node process begins. Dynamic messages appear on the dashboard as the nodes are added to the cluster. A blue bar indicates the task is progressing normally. Nodes are processed (upgraded or re-imaged 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.

 **Note:** A red bar indicates there is a problem; hovering the cursor over the red bar text displays more information about the problem.

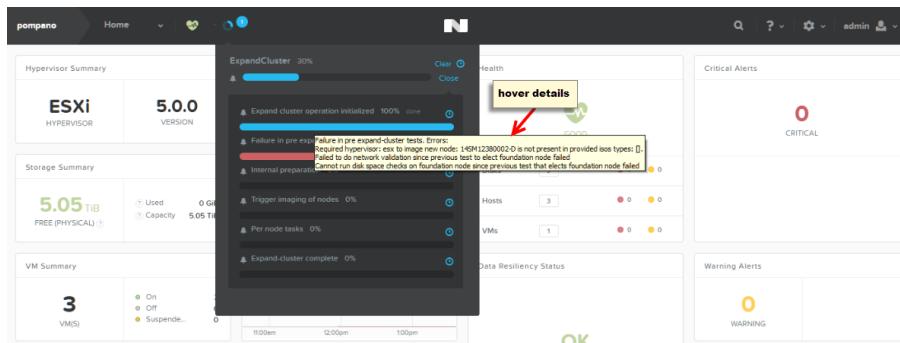


Figure: Progress Messages

8. [Data-At-Rest Encryption only] On the encryption page, do the following (see [Configuring Data-at-Rest Encryption](#) on page 619 for more information):

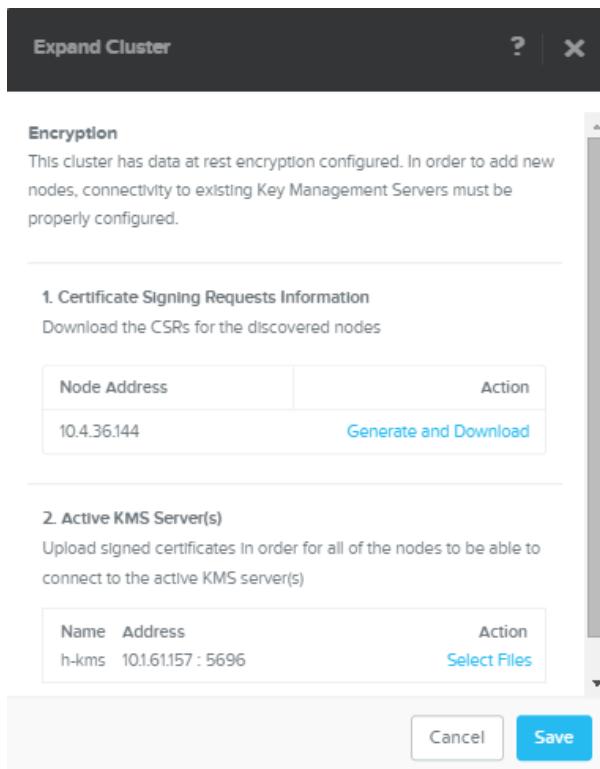


Figure: Expand Cluster Window: Encryption Page

- a. In the Certificate Signing Request Information field, click the **generate and download** link for each node to be added.  
This generates a certificate signing request (CSR) named `csr_for_discovered_node` for the node, which you download to your workstation.
  - b. Get the CSRs signed by a certificate authority (CA).
  - c. In the **Active KMS Servers** field, click the **select files** link for each key management server and upload the signed certificates for the nodes to be added.
  - d. Click the **Save** button.  
The *Expand Cluster* dialog box closes and the add node process begins as described above.
9. 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, this step is not needed because the new storage is added to that storage pool automatically.

- a. Select **Storage** from the pull-down main menu (upper left of screen) and then select the **Table** and **Storage Pool** tabs.
- b. Select the target storage pool (upper display) and then click the **update** link.  
A storage pool must already exist to do this step (see [Creating a Storage Pool](#) on page 138).

NAME	DISKS	FREE UNRESERVED	USED	MAX CAPACITY	DISK IOPS	DISK IO B/W	DISK AVG IO LATENCY
agave_all_storage_pool	30	22.36 TB	925.02 GB	23.49 TB	177	60.9 MBps	65.39 ms

Figure: Storage Pool Screen

- c. In the *Update Storage Pool* window, check the **Use unallocated capacity** box in the **Capacity** line (see [Creating a Storage Pool](#) on page 138) and then click the **Save** button.  
This step adds all the unallocated capacity to the selected storage pool.

### What to do next:

One or more of the following items might apply to the added nodes:

- Non-default timezones are not updated on added nodes and must be reconfigured manually.
- If the Controller VM password for the cluster was changed from the default, the password on any new nodes must be changed manually (after the nodes are added to the cluster) to match the cluster password. See the *Changing the Controller VM Password* section in the *Acropolis Advanced Administration Guide* for more information.
- After cluster expansion, you can verify the Controller VM memory on the new node(s) is the same as the other Controller VMs in the cluster and sufficient for the intended workload, run the `cvm_same_mem_level_check` and `cvm_memory_check` NCC checks (see [Running Checks by Using Web Console](#) on page 349).
  - If the `cvm_same_mem_level_check` result is FAIL, the memory size 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.

See also [Increasing Controller VM Memory Size](#) on page 111.

Additional procedures to change (increase) Controller VM memory are included in the appropriate administration guide for your hypervisor (*AHV Administration Guide*, *vSphere Administration Guide for Acropolis*, *Hyper-V Administration for Acropolis*, or *Citrix XenServer on Nutanix Administration Guide*). For Controller VM memory size recommendations, see the "Controller VM Memory Configurations" section of the *Acropolis Advanced Administration Guide*.

- When running ESXi, the target storage containers must be set to mount on the new hosts. You can check this by going to the **Storage Container** tab, selecting a storage container, clicking the **Update** button, and verifying that **Mount on all ESXi Hosts** is selected (or the new hosts are checked in **Mount/Unmount on the following ESXi Hosts**) in the **NFS DATASTORE** field (see [Modifying a Storage Container](#) on page 143).
- (vSphere only)
  - If an added node has an older processor class than the existing nodes in the cluster, cluster downtime is required to enable EVC with the lower feature set as the baseline. For an indication of the processor class of a node, see the **Block Serial** field on the **Diagram** (see [Hardware Diagram](#)

[View](#) on page 168) or **Table** (see [Hardware Table View](#) on page 176) view of the *Hardware Dashboard*. For instructions on enabling EVC, see the vSphere documentation.



**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 the vCenter Server before enabling EVC and later need to enable EVC, cluster downtime is required because all VMs (including the Controller VM) have to 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 Enhanced vMotion Compatibility (EVC) with the lower feature set as the baseline before adding the node to vCenter.
- (Hyper-V only) After you add a node to the Hyper-V cluster by using the Prism web console, perform the following additional 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.

## Modifying a Cluster

Hardware components (nodes and disks) can be removed from a cluster or reconfigured in other ways when conditions warrant it.

**Before you begin:** If the Data-at-Rest Encryption is enabled then before removing a drive or node from a cluster, test the certificates again by clicking **Test all nodes** and ensure that testing is successful and the status is **Verified**. For a detailed procedure, refer to the [Configuring Data-at-Rest Encryption](#) on page 619. In case of an SED drive or node, if the drive or node is not removed as recommended then the drive or node will be locked.

To reconfigure one or more hardware components in a cluster, do the following:

1. In the Hardware dashboard (see [Hardware Dashboard](#) on page 166), click the **Diagram** or **Table** tab. The following actions can be performed from either the **Diagram** or **Table** view.
  2. To remove a disk from the cluster (which is necessary when replacing a failed disk), either select the target disk in the diagram (Diagram view) or click the **Disk** tab and select that disk in the table (Table view), and click the **Remove Disk** link on the right of the **Summary** line. A dialog box appears to verify the action; click the **OK** button.

Removing a disk can take some time because data on that disk must be migrated to other disks before it can be removed from a node. You can monitor progress through the dashboard messages.



**Caution:** Do not physically remove a disk until that disk appears red in the diagram. The status message might indicate the data migration is complete, but the disk is not ready for removal until that disk turns red in the diagram.

**Cluster**

**select a disk**

**select a host**

**summary/detail information**

DISK DETAILS	
ID	28
Serial Number	Z1W1B718
Model	ST1000NM0033-9ZM173
Storage Tier	HDD
Used (Physical)	45.85 GiB
Capacity (Logical)	802.07 GiB
Hypervisor	10.4.225.102
Storage Pool	agave_all_storage_pool
Status	Normal
Mode	Online

Figure: Cluster Hardware (Diagram View)

- To remove a host (node) from the cluster, either select the target host in the diagram (Diagram view) or click the **Host** tab and select that host in the table (Table view), and click the **Remove Host** link on the right of the **Summary** line. A dialog box appears to verify the action; click the **OK** button.

The Prism web console displays a warning message that you need to reclaim the license after you have removed the node. See [Reclaiming Licenses](#) on page 70 or [Reclaiming Licenses \(Portal Connection\)](#) on page 59.

Removing a host takes some time because data on that host must be migrated to other hosts before it can be removed from the cluster. You can monitor progress through the dashboard messages. Removing a host automatically removes all the disks in that host. Only one host can be removed at a time. If you want to remove multiple hosts, you must wait until the first host is removed completely before attempting to remove the next host.

(Hyper-V only) Initiating a 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 is displayed.

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 is displayed in either nCLI or in Web interface, cluster administrators must use the management tools provided by Microsoft such as Failover Cluster Manager to drain all the highly-available roles off the host and then remove the host from the failover cluster and then remove the host from the AOS cluster.

The screenshot shows the Prism Web Console interface for managing cluster hardware. At the top, there's a navigation bar with 'Chestnut' and a dropdown menu set to 'Hardware'. Below the navigation is a toolbar with icons for heart rate, alert, and more. The main area has tabs for 'Overview', 'Diagram', and 'Table', with 'Table' selected. Under the 'Table' tab, there are three filter buttons: 'Host', 'Disk' (which is highlighted with a red border), and 'Switch'. The main content is a table of disk details:

DISK ID	SERIAL NUMBER	HYPERSERVER IP	TIER	MODE
26	Z1W36737	10.4.152.43	HDD	Online
27	Z1W353PP	10.4.152.43	HDD	Online
28	BTTV432204LC200GGN	10.4.152.43	SSD	Online
31	Z1W34H6Z	10.4.152.41	HDD	Online
32	Z1W353NM	10.4.152.41	HDD	Online
33	BTTV432204KW200GGN	10.4.152.41	SSD	Online
37	Z1W34WSK	10.4.152.42	HDD	Online
38	Z1W34H7W	10.4.152.42	HDD	Online
39	BTTV432204K5200GGN	10.4.152.42	SSD	Online

Below the table, a link 'Summary > Z1W36737' leads to a detailed view of a specific disk. This view includes a 'Disk Details' table and a 'Disk Usage' chart. The 'Disk Details' table contains the following information:

DISK DETAILS	
ID	26
Serial Number	Z1W36737
Model	ST1000NM0033-9ZM173
Storage Tier	HDD
Used (Physical)	1.45 GB
Capacity (Logical)	802.07 GB
Hypervisor	10.4.152.43
Storage Pool	default-storage-pool-21653
Status	Normal
Mode	Online
Self Encryption Drive	Not Present

The 'Disk Usage' chart shows a single data series for the disk 'Z1W36737' over time, with a value of 10.30 PM. A yellow box highlights the word 'summary' in the URL.

Figure: Cluster Hardware (Table View)

4. To add a host into the metadata store, either select the target host in the diagram (Diagram view) or click the **Host** tab and select that host in the table (Table view), and click the **Enable Metadata Store** link on the right of the **Summary** line.

Each node includes a disk used for metadata storage, and AOS maintains a metadata store across these disks to ensure uninterrupted resiliency should a metadata disk fail. After such a failure, that node is taken out of the metadata store group and the cluster continues to operate seamlessly without it. Normally, the node is brought back into the metadata store automatically after the failed metadata disk is replaced. However, under certain (rare) circumstances this might not happen. If the node is ready but was not added back automatically, the alert message `Node ready to be added to metadata store` is displayed and the **Enable Metadata Store** link appears indicating you can add the node back into the metadata store manually.

## Life Cycle Manager

The life cycle manager (LCM) tracks software and firmware versions of all entities in the cluster.

### Limitations

LCM is not supported on single-node clusters, because firmware updates usually require services to be stopped (in a single-node cluster there is no other node to take over the workload from the node being updated.)

### LCM Structure

LCM consists of a framework and a set of modules for inventory and update. LCM is supported for all Nutanix NX and SX platforms.

The LCM framework is accessible through the Prism interface. It acts as a download manager for LCM modules, validating and downloading a module's content. All communication between the cluster and LCM modules goes through the LCM framework.

LCM modules are independent of AOS. They contain libraries and images, as well as metadata and checksums for security. Currently all modules are supplied by Nutanix.

The LCM framework targets a configurable URL to download content from the LCM modules.

You can use the LCM Scheduler to schedule update checks automatically, or perform checks only when you do it manually.

### LCM Operation

LCM performs two functions: taking inventory of the cluster and performing updates on the cluster. Note that an LCM update is not reversible.

Before performing an update, LCM runs a pre-check to verify the state of the cluster. If the check fails, the update operation is aborted.

All LCM operation logs are written to `genesis.out` and `lcm_ops.out`. The log files record all operations, including success and failures. If an operation fails, LCM suspends it to wait for mitigation. Contact Nutanix Support for assistance if there is an LCM failure.

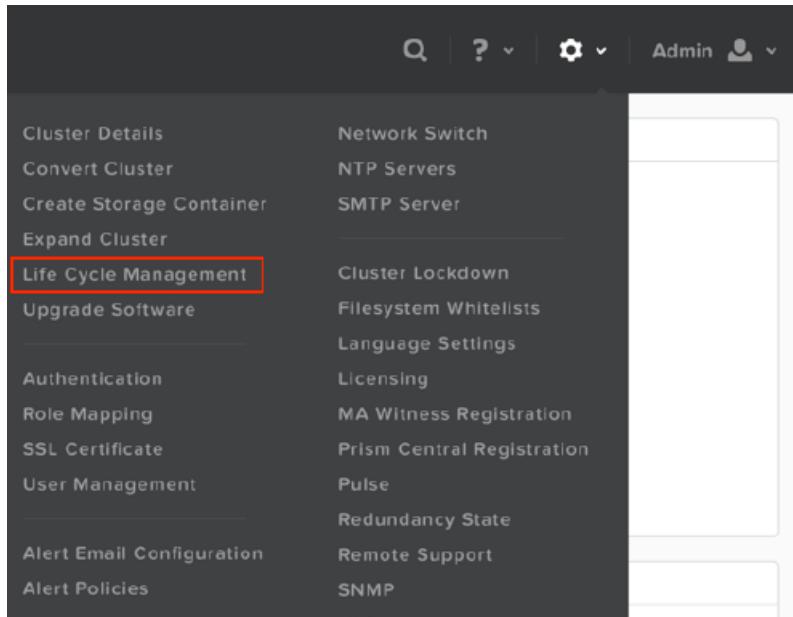
The LCM framework can also update itself when necessary. Although connected to AOS, the framework is not tied to the AOS release cycle.

## Taking Inventory With the Life Cycle Manager

Use LCM to display software and firmware versions of entities in the cluster.

Inventory information for a given node is persistent as long as the node remains in the chassis. When you remove a node from a chassis, all inventory information for that node is reset. When you return the node to the chassis, you must perform the inventory operation again to restore the inventory information.

1. In Prism, click the gearbox button and select **Life Cycle Management** from the drop-down menu.



Prism opens the Life Cycle Manager page.

2. Click the **Inventory** tab.
3. Click **Options > Perform Inventory**.  
The LCM displays all discovered entities.

Available Updates      Inventory

**Cluster software component**

**1 Entities**

Last Updated: Unknown

[See All](#)

**BIOS**

**3 Entities**

Last Updated: Unknown

[See All](#)

**DISK**

**18 Entities**

Last updated 2 days ago

[See All](#)

**HBA**

**3 Entities**

Last Updated: Unknown

[See All](#)

4. For details about any entity, click **See All**.

The entity shows the current version, as well as the date and time of the most recent update.

Available Updates      Inventory

All Entities > BIOS

HOST: NTNX-BLOCK-1-A

dummy.smc.gen10.bios - BI11S546  
Current Version: 1.0

Last Updated: Unknown

HOST: NTNX-BLOCK-1-B

dummy.smc.gen10.bios - BI11S546  
Current Version: 1.0

Last Updated: Unknown

HOST: NTNX-BLOCK-1-C

dummy.smc.gen10.bios - BI11S546  
Current Version: 1.0

Last Updated: Unknown

5. Click **All Entities** to return to LCM.
6. To close LCM and return to the web console, click the **X** in the upper right corner.

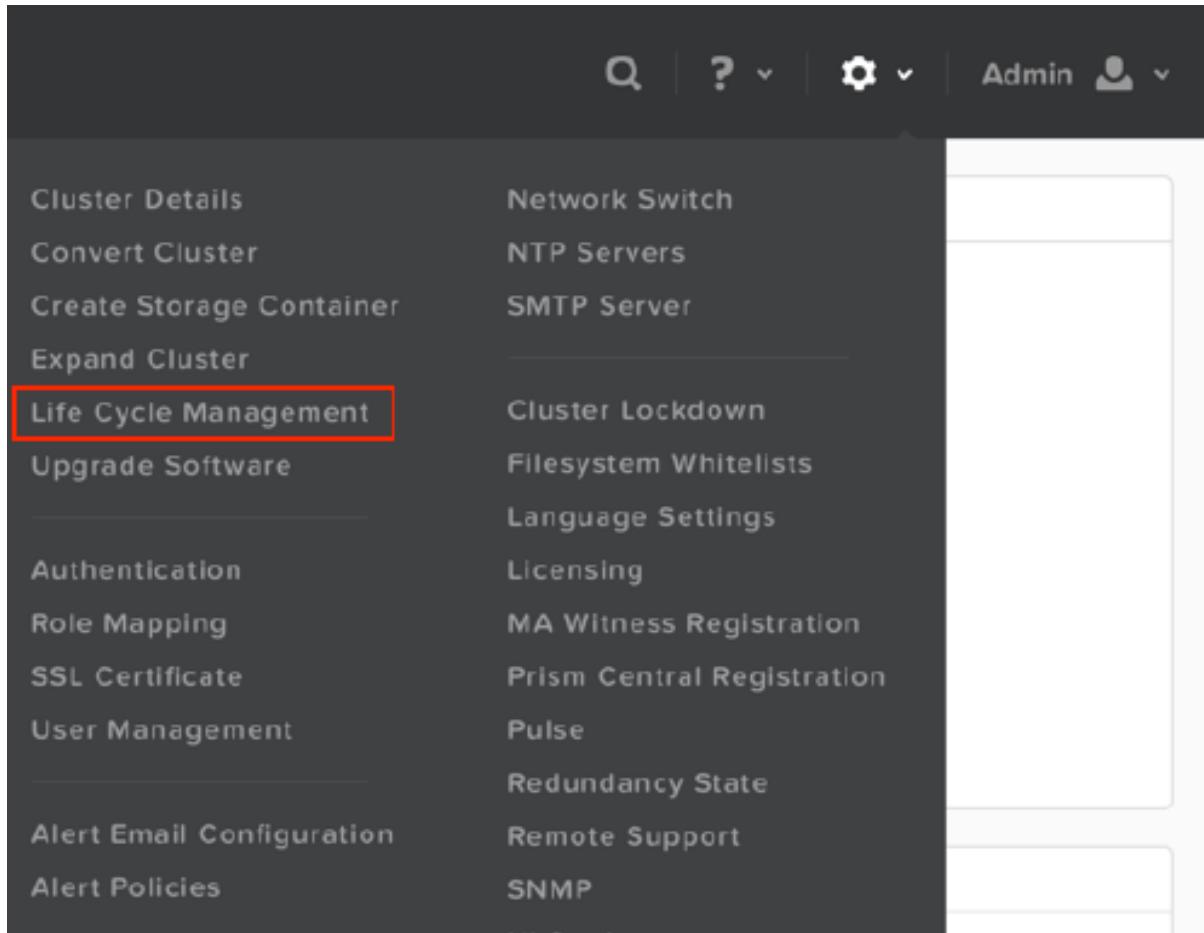
## Performing Updates With the Life Cycle Manager

Use LCM to perform firmware updates for components in a cluster.

**Before you begin:** Make sure that firewall ports 80, 8443, and 443 are open. The cluster uses ports 80 and 8443 to connect to the Nutanix support servers. Nutanix recommends that you open both ports. If one port is disabled, the cluster automatically attempts to connect on the other. On some advanced firewalls, port 80 may only allow HTTP traffic to pass; since Pulse or Alert messages are not HTTP

formatted, the traffic is not processed. In this case, enable port 8443. The cluster uses the SSH protocol for communication through the firewall.

1. In Prism, click the gearbox button and select **Life Cycle Management** from the drop-down menu.



Prism opens the Life Cycle Manager page.

A screenshot of the Life Cycle Manager page. At the top, there is a header bar with tabs for 'Available Updates' (which is selected and highlighted in blue) and 'Inventory'. Below the header, there is a section titled 'REQUIRED UPDATES' with a dropdown menu set to 'Host Boot Devices'. Underneath the dropdown, there is a link 'Update 2 Entities' and a 'Define' button. At the bottom right of the page, there are 'Options' and 'Update All' buttons.

2. Click **Available Updates**.
3. Specify the location where LCM should look for updates.
  - a. Click **Options > Advanced Settings**.

## Life Cycle Management Advanced Settings

? | X

Fetch updates from:

Check for updates every  days

Starting from  at

- b. The **Fetch updates from** field auto-populates with the URL where LCM will look for updates. To change the location, enter a different address in the **Fetch updates from** and click **Save**. You are returned to the Life Cycle Manager.

4. For each displayed component, you can click **Define** to see available updates for that component.

Available Updates      Inventory

---

[All Updates](#) > **Host Boot Devices**

HOST: NTNX-BLOCK-1-B

**SATADOM-SL 3ME - 20150311AA19384...** 

Installed Version: S161

Update to S170

[Change](#)

---

No dependencies found

HOST: NTNX-BLOCK-1-C

**SATADOM-SL 3ME - 20150730AA10960..** 

Installed Version: S161

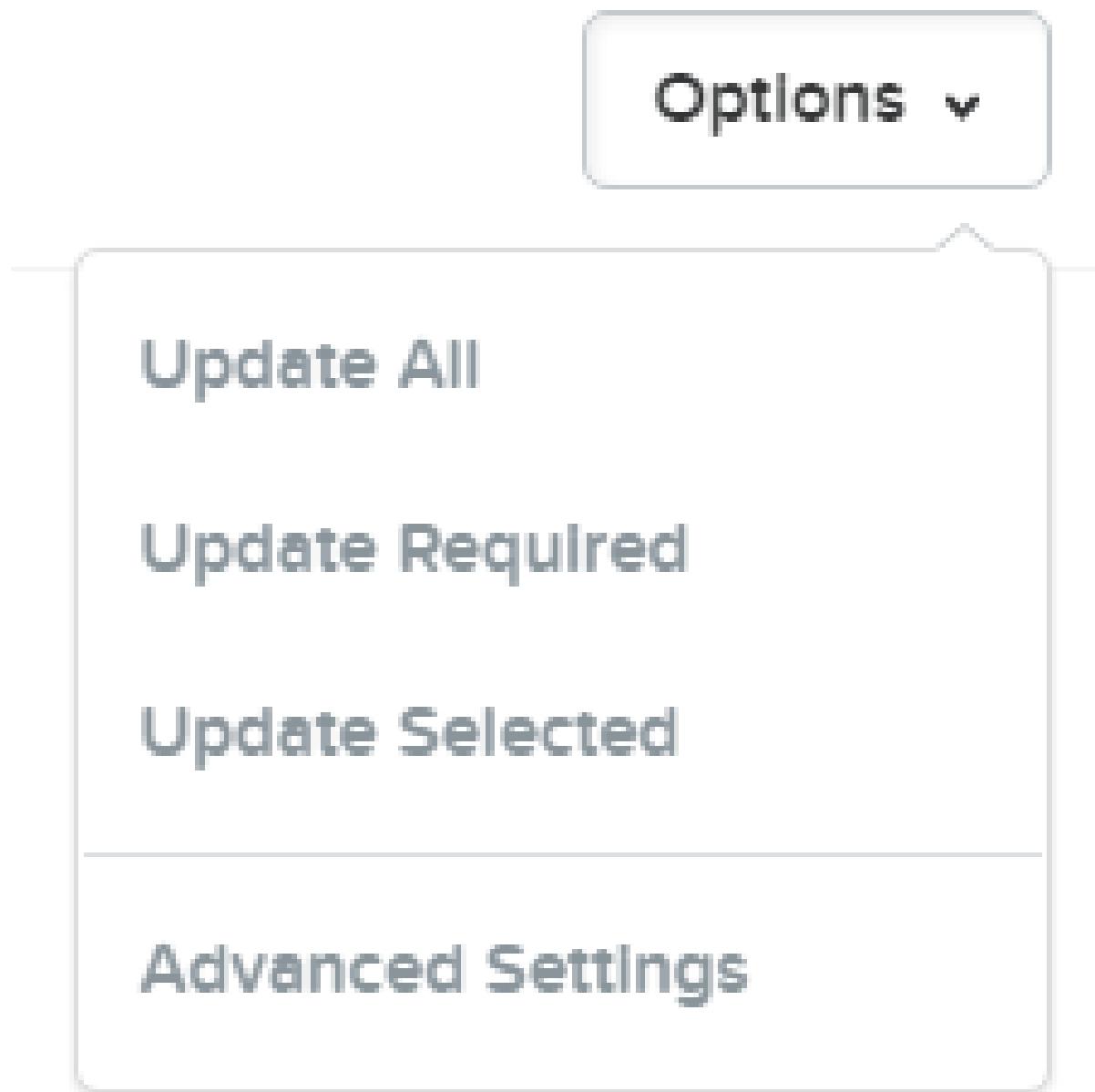
Update to S170

[Change](#)

---

No dependencies found

- a. If you want to perform only some updates and not others, select the button in the upper left of each update to let Prism know which updates it should execute. If you do not select any updates, Prism assumes you want to perform them all.
  - b. To return to the Life Cycle Manager, click **All Updates**.
5. From the **Options** drop-down menu, perform your updates.



- a. To perform all available updates, select **Update All**.

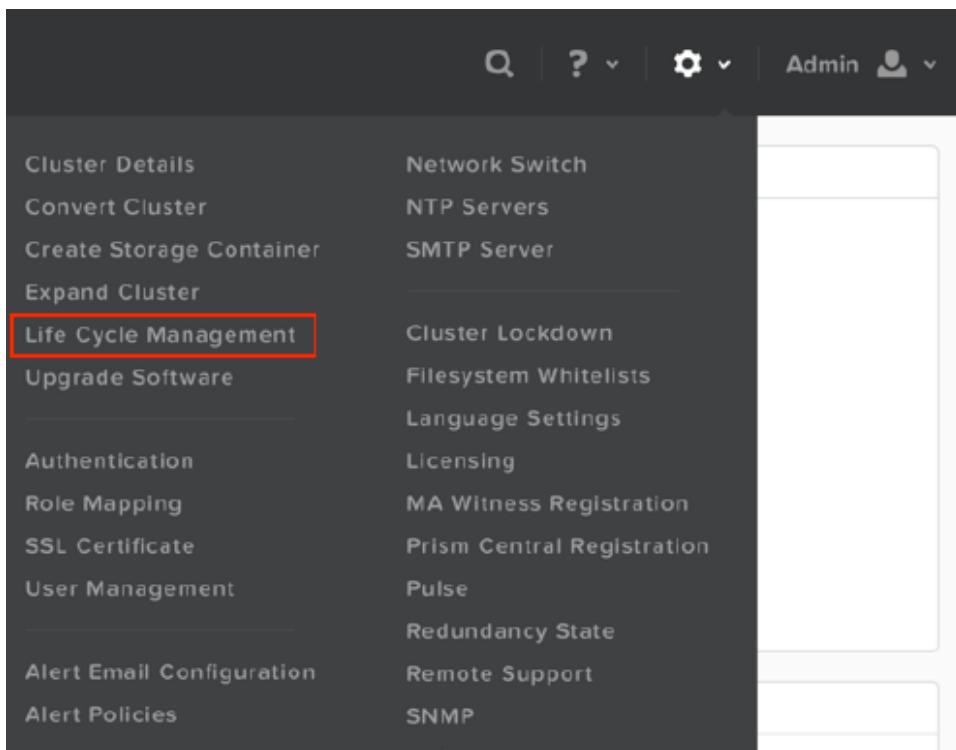
- b. To perform only required updates, select **Update Required**.
  - c. To perform only updates you have selected, select **Update Selected**. (If you have not selected any updates, this has the same effect as **Update All**).
- 6. To close LCM and return to the web console, click the **X** in the upper right corner.

## Using the Life Cycle Manager Without Web Access

Use LCM at a site without Internet access.

By default, LCM automatically fetches updates from a pre-configured URL. If you are managing a Nutanix cluster at a site that cannot access the provided URL, you must configure LCM to fetch updates locally, using the following procedure.

1. Set up a local web server that is reachable by all your Nutanix clusters. (You will use this server to host the LCM repository.)
2. From a device that has public Internet access, go to the Nutanix portal and select **Downloads > Tools & Firmware**. Download the tar file `LCM_1.1.tgz`.
3. Transfer `LCM_1.1.tgz` to your local web server.
4. On your local web server, extract `LCM_1.1.tgz` into your local directory.
  - For a Linux web server, untar the file with the command `tar zxvf LCM_1.1.tgz`.
  - For a Windows web server, extract the file into a directory called `release` and perform the following configuration steps:
    - a. Set `.sign` (type: plain/text) as a new mime type. (See [here](#) for details.)
    - b. In IIS, set permissions on the `release` directory to **Full Control**.
5. Perform the following steps on each Nutanix cluster.
  - a. Log in to Prism.
  - b. In Prism, click the gearbox button and select **Life Cycle Management** from the drop-down menu.



Prism opens the Life Cycle Manager page.

- c. On the LCM page, click **Options > Advanced Settings**.

A screenshot of the "Life Cycle Management Advanced Settings" dialog box. The title bar has a question mark icon and a close (X) icon. The main area contains the following fields:

- "Fetch updates from:" input field containing "http://198.51.100.0/release"
- "Check for updates every" dropdown menu set to "7" days
- "Starting from" date input field set to "05/15/2017" and a time input field set to "5:21:48 PM" with a clock icon

At the bottom right are "Cancel" and "Save" buttons, with "Save" being highlighted in blue.

- d. In the **Fetch updates from** field, enter the path to the directory where you extracted the tar file on your local server. Use the format `http://webserver_IP_address/release`.
- e. Click **Save**.  
You are returned to the Life Cycle Manager.
- f. Click **Options > Perform Inventory**.
- g. Update the LCM framework before trying to update any other component.

The LCM Inventory page now shows the LCM Framework with the same version as the file you downloaded.

## Acropolis Block Services

AOS supports two methods for client iSCSI connectivity to volume groups.

### Available Methods for iSCSI Connectivity to Volume Groups

Method	Description
iSCSI initiators with MPIO	This method enables you to use software iSCSI initiators combined with the initiating operating system's native Multipath I/O (MPIO) capability. In this case, MPIO helps control path management for vDisk load balancing and path resiliency.
iSCSI initiators with Acropolis Block Services (ABS)	Nutanix recommends that you use Acropolis Block Services instead of MPIO. ABS provides highly available and high performance block storage as iSCSI LUNs to clients with simple client configuration. Clients can be non-Nutanix servers external to the cluster or guest VMs internal or external to the cluster, with the cluster block storage configured as one or more volume groups.

Block storage 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 from within the client operating systems. Eligible block storage is storage from any new or existing Nutanix cluster.

To provide access to the block storage and simplify client configuration management, ABS exposes a single *iSCSI data services IP address* to clients for target discovery, which also simplifies external iSCSI configuration on clients. This iSCSI data services IP acts as an iSCSI target discovery portal and initial connection point. The client is configured with this single IP address, which helps load balance storage requests and enables path optimization in the cluster, preventing bottlenecks.

ABS does not require multipath I/O (MPIO) configuration on the client but it is compatible with clients that are currently using or configured with MPIO.

A significant advantage of ABS is that the cluster-wide iSCSI data services IP address enables you to expand your cluster without requiring you to reconfigure clients using ABS. It also makes it easy to scale storage capacity and performance without the need for downtime.

ABS provides high availability by design. Because all nodes in a Nutanix cluster support ABS, storage access and requests are redirected to surviving nodes if any node fails or becomes unavailable. Failover in this case is non-disruptive, with an initial minimal delay of 10 seconds or less possibly experienced by applications.

### Securing Initiators and The Nutanix Cluster Target with CHAP

For additional security, ABS also enables you to use Challenge-Handshake Authentication Protocol (CHAP) authentication for iSCSI as part of [Creating a Volume Group for Use with ABS](#) on page 213.

- Use one-way CHAP for basic security between the initiator and Nutanix cluster target. Nutanix recommends using one-way CHAP authentication.
- Use Mutual CHAP for additional security, where the client and target authenticate each other. When you configure a volume group, you can set a shared initiator CHAP secret, common and known only to the authenticator and peer. AOS manages the secrets, with the AOS `iscsi_adapter` implementing CHAP.

## Example Use Cases Supported by ABS

ABS can support use cases including but not limited to:

- iSCSI for Microsoft Exchange Server. ABS enables Microsoft Exchange Server environments to use iSCSI as the primary storage protocol.
- Shared storage for Windows Server Failover Clustering (WSFC). ABS supports SCSI-3 persistent reservations for shared storage-based Windows clusters, commonly used with Microsoft SQL Server and clustered file servers.
- Bare-metal environments. ABS enables existing server hardware separate from a Nutanix cluster to consume the Acropolis Distributed Storage Fabric (DSF) resources. Workloads not targeted for virtualization can also use the DSF.
- Boot over iSCSI. ABS enables and supports the ability to boot an operating system over iSCSI for physical servers. In this configuration, a host can start a supported operating system from a LUN instead of a local disk instance.



**Note:** Linux guest VM clustering is not supported for solutions other than Oracle RAC with Oracle Clusterware and Microsoft Windows Failover Clusters.

## If You are Already Using Volume Groups

ABS does not require multipath I/O (MPIO) configuration on the client but it is compatible with clients that are currently using or configured with MPIO.

If you are already using volume groups with MPIO and individual Controller VM IP addresses as targets, upgrading to AOS 5.0 will not disable or affect your existing configuration or functionality.

Nutanix recommends that you convert to Acropolis Block Services where applicable to take advantage of load balancing and other capabilities provided by the iSCSI data services IP address. See [Converting Volume Groups and Updating Clients to Use ABS](#) on page 230.

## ABS Requirements and Supported Clients

Supported clients and associated requirements for using Acropolis Block Services.

### ABS Requirements

- Synchronous Replication or Metro Availability are not currently supported for volume groups.
- You must configure an iSCSI data services IP address in **Cluster Details** available from the Prism web console. See [Modifying Cluster Details](#) on page 42.
- Ensure that ports 3260 and 3205 are open on any clients accessing the cluster where Acropolis Block Services is enabled.
- Linux guest VM clustering is not supported for solutions other than Oracle RAC with Oracle Clusterware and Microsoft Windows Failover Clusters.

## Supported Client Operating Systems

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 R2
- Red Hat Enterprise Linux 6.7
- Red Hat Enterprise Linux 6.8
- Red Hat Enterprise Linux 7.2
- Oracle Linux 6.x
- Oracle Linux 7.x
- CentOS 7.x
- Oracle Solaris 11.3 on SPARC
- SuSE Linux Enterprise Server 11 / 12 (x86 servers)
- IBM AIX 7.1 / 7.2 on POWER<sup>1</sup>

1. PowerHA cluster configurations are not supported as AIX requires a shared drive for cluster configuration information and that drive cannot be connected over iSCSI.

## Supported Network Cards and Client Operating Systems, Booting An Operating System Over iSCSI Feature

ABS supports the ability to boot an operating system over iSCSI for physical servers. In this configuration, a host can start a supported operating system from a LUN instead of a local disk instance.

### Client OS Support, Boot Over iSCSI

Network Device	Intel 10 GbE Network Adapter X520 / I350	QLogic QLE 8442 Converged Network Adapter
Client OS	-	-
Microsoft Windows Server 2008 R2	● <sup>1</sup>	●
Microsoft Windows Server 2012 R2	●	
Red Hat Enterprise Linux 6.7 / 6.8	●	●
Red Hat Enterprise Linux 7.2	●	●
Oracle Linux 6.x		
Oracle Linux 7.x		
Oracle Solaris 11.3 on SPARC	●	
SuSE Linux Enterprise Server 11 / 12 (x86 servers)		
IBM AIX 7.1 / 7.2 on POWER	● <sup>2</sup>	

1. ● = Supported

2. To boot AIX over iSCSI, set the `use_redirection` property to `false` for the new or existing volume group where the boot LUN resides. See [Modifying a Volume Group \(AIX Boot Over iSCSI\)](#) on page 230.

## Enabling Acropolis Block Services

This topic describes the first-use workflow for enabling and implementing Acropolis Block Services (ABS). To convert existing AOS volume groups and clients, see [Converting Volume Groups and Updating Clients to Use ABS](#) on page 230.



**Note:** A valid client is a server running an operating system listed in [ABS Requirements and Supported Clients](#) on page 211, or guest VMs using in-guest iSCSI.

1. Get the client IP address that you will add to a volume group client whitelist.

You can also use unique iSCSI initiator names (Initiator iSCSI Qualified Name [IQN]) from each client. See [Obtaining the Windows Client iSCSI Initiator Name](#) on page 221 or [Obtaining the Linux Client iSCSI Initiator Name](#) on page 225.

2. Create an iSCSI data services IP address for the Nutanix cluster.

This address cannot be the same as the cluster virtual IP address. See [Modifying Cluster Details](#) on page 42 and [About The iSCSI Data Services IP Address](#) on page 44.

3. Provision storage on the Nutanix cluster by creating a volume group. Create a client whitelist to enable access to the volume group by using the IP addresses or client initiator IQNs in a whitelist (as part of the volume group configuration). Create a secret for the volume group if you are using CHAP authentication.

See [Creating a Volume Group for Use with ABS](#) on page 213.

4. Perform an iSCSI target discovery of the Nutanix cluster from the clients.

5. [Optional] Configure CHAP or Mutual CHAP authentication on the initiators and target Nutanix clusters.

### Creating a Volume Group for Use with ABS

Create a volume group to serve storage to one or more client initiators. Use the *Create Volume Group* window scrollbar to see all fields and buttons.

1. In the **Storage** dashboard (see [Storage Dashboard](#) on page 119), click the **Volume Group** button. The *Create Volume Group* dialog box is displayed.

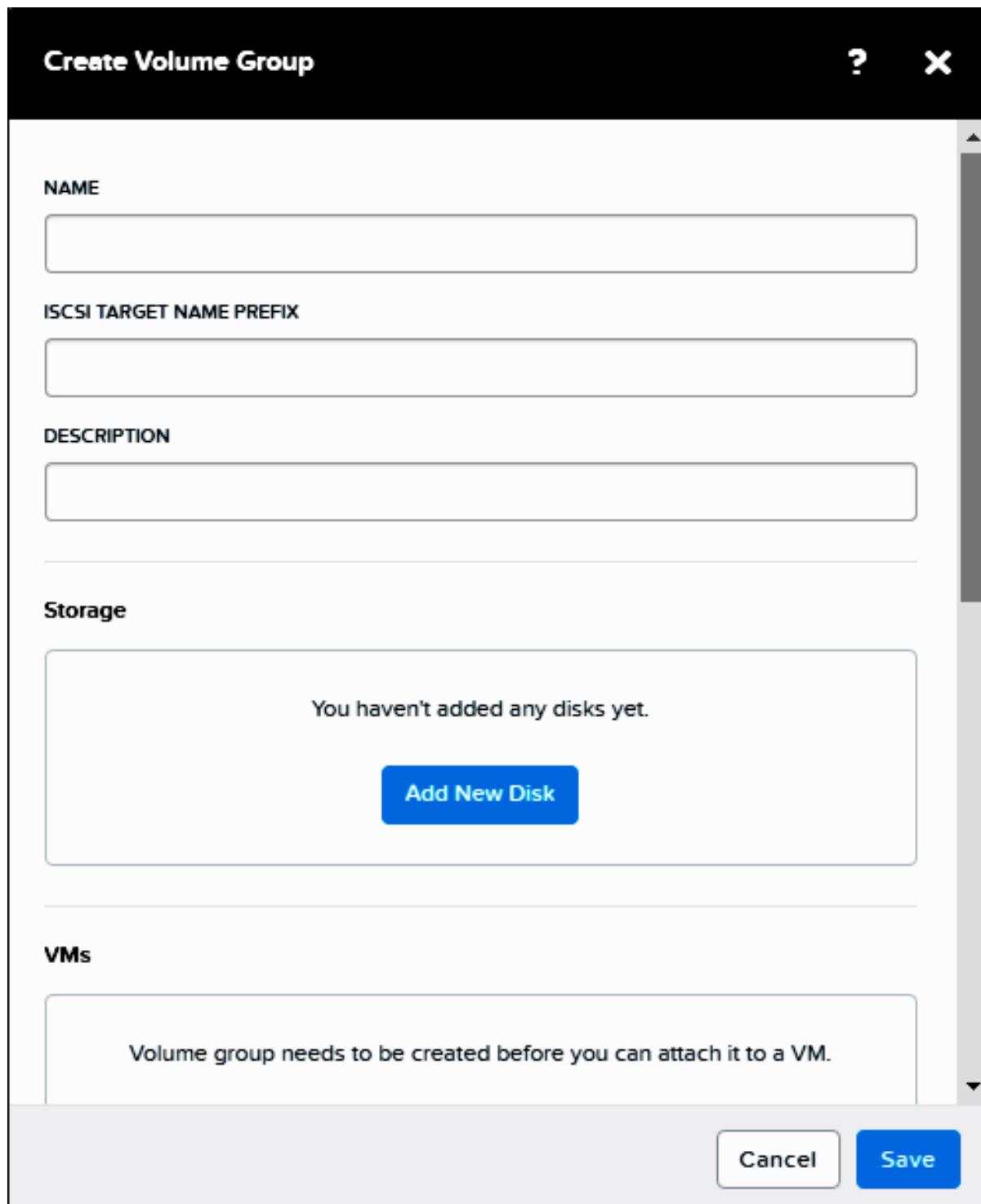


Figure: Create Volume Group Dialog Box

2. Name and describe the volume group.

- a. 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 (-).

- b. 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**.

You also use **iSCSI Target Name Prefix** as the user name (*username\_in*) if you configure Mutual CHAP authentication for Linux clients.

- c. In **Description**, provide a description for the volume group.
- 3. To add one or more disks to the volume group, do the following:
  - a. In the **Storage** section, click **Add New Disk**.
  - b. In the **Add Disk** dialog box, select the storage container to use from the **Storage Container** pull-down list. The list includes all storage containers created on this cluster.
  - c. In **Size**, enter the disk size in GiBs.
  - d. Click **Add**.
  - e. Repeat these steps to add another disk for this volume group, if desired.

**What to do next:** Add the iSCSI initiators to the volume group and enable client access to the cluster storage.

#### Add the Client iSCSI Initiators to the Volume Group

1. Scroll down to the **Access Settings** section.

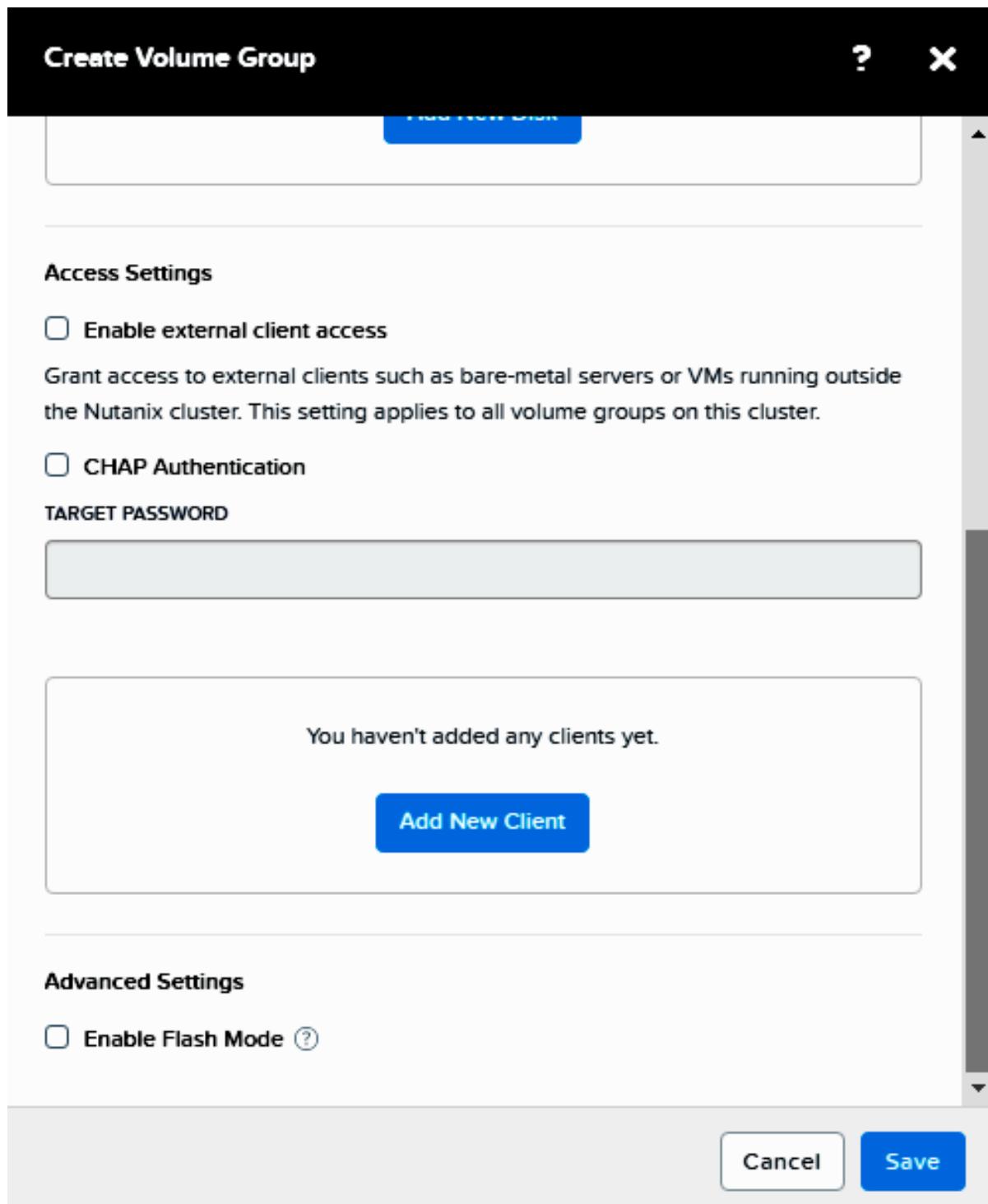


Figure: Enable External Client Access

2. Select **Enable external client access** if you are whitelisting clients that are external to or not residing in this cluster. Otherwise, leave this clear. If you select this checkbox, it remains automatically selected if you create more volume groups.
3. If you are using one-way CHAP security, select **CHAP Authentication** and type a 12 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.

4. Click **Add New Client** to configure the initiators.
  - a. Enter the client IP address in the **Client IQN/IP Address** field to create the initial IP whitelist. Optionally, you can use iSCSI initiator names (Initiator iSCSI Qualified Name [IQN]) from the Windows or Linux clients. See [Obtaining the Windows Client iSCSI Initiator Name](#) on page 221 or [Obtaining the Linux Client iSCSI Initiator Name](#) on page 225.
  - b. [Option] Select **CHAP Authentication** and enter the iSCSI client password (secret) used when you configure Mutual CHAP authentication on the client. See [Discovering the ABS Target from the Windows Client](#) on page 217, [Configuring Mutual CHAP Authentication \(Linux\)](#) on page 223, or [Adding iSCSI Targets on the AIX Host](#) on page 226.
  - c. Click **Add**.

**Access Control** displays any configured clients. This list includes any clients attached to volume groups in the cluster.

5. Click **Add New Client** in the **Create Volume Group** window to add more initiators allowed to access this storage.
6. Repeat these steps until you have added all the initiators that you want to whitelist.
7. Click **Save**.

**What to do next:** For the whitelisted initiators, perform an iSCSI discovery and target connection of the data services IP address for the Nutanix cluster on the client (Windows or Linux). See:

- [Discovering the ABS Target from the Windows Client](#) on page 217
- [Discovering the ABS Target from the Linux Client](#) on page 222
- [Changing the AIX Initiator Name](#) on page 225

## Configuring Windows Clients

### Discovering the ABS Target from the Windows Client

#### Before you begin:

1. You will need the Nutanix cluster data services IP address you created when you modified cluster details. See [Modifying Cluster Details](#) on page 42 and [About The iSCSI Data Services IP Address](#) on page 44.
2. Make sure you have already created a volume group with the client IP address or initiator IQNs specified in the **Access Control** whitelist. Any LUNs associated with the volume group will be automatically discovered. See [Creating a Volume Group for Use with ABS](#) on page 213.
3. From the Windows client, make sure that you have:
  - Started the *Microsoft iSCSI Initiator Service* and that the **Startup Type** is set to **Automatic**.
  - Set your firewall rules to allow iSCSI service traffic.

This procedure describes how to perform a Windows client iSCSI discovery and connection of the data services IP address for the Nutanix cluster (the ABS target). This allows the cluster and its volume groups to be discoverable by the initiators. Do the following from Windows to discover and connect the ABS target. You can also configure CHAP authentication here.

1. Open the *iSCSI Initiator Properties* window.  
If *iSCSI Initiator* is not available from **Administrative Tools**, you can open it by clicking **Start**, typing *iscsi* in the search box, and clicking **iSCSI Initiator** from **Programs**.

2. In the *iSCSI Initiator Properties* window, click the **Discovery** tab.
3. Click **Discover Portal**, add the iSCSI data services IP address for the Nutanix cluster.

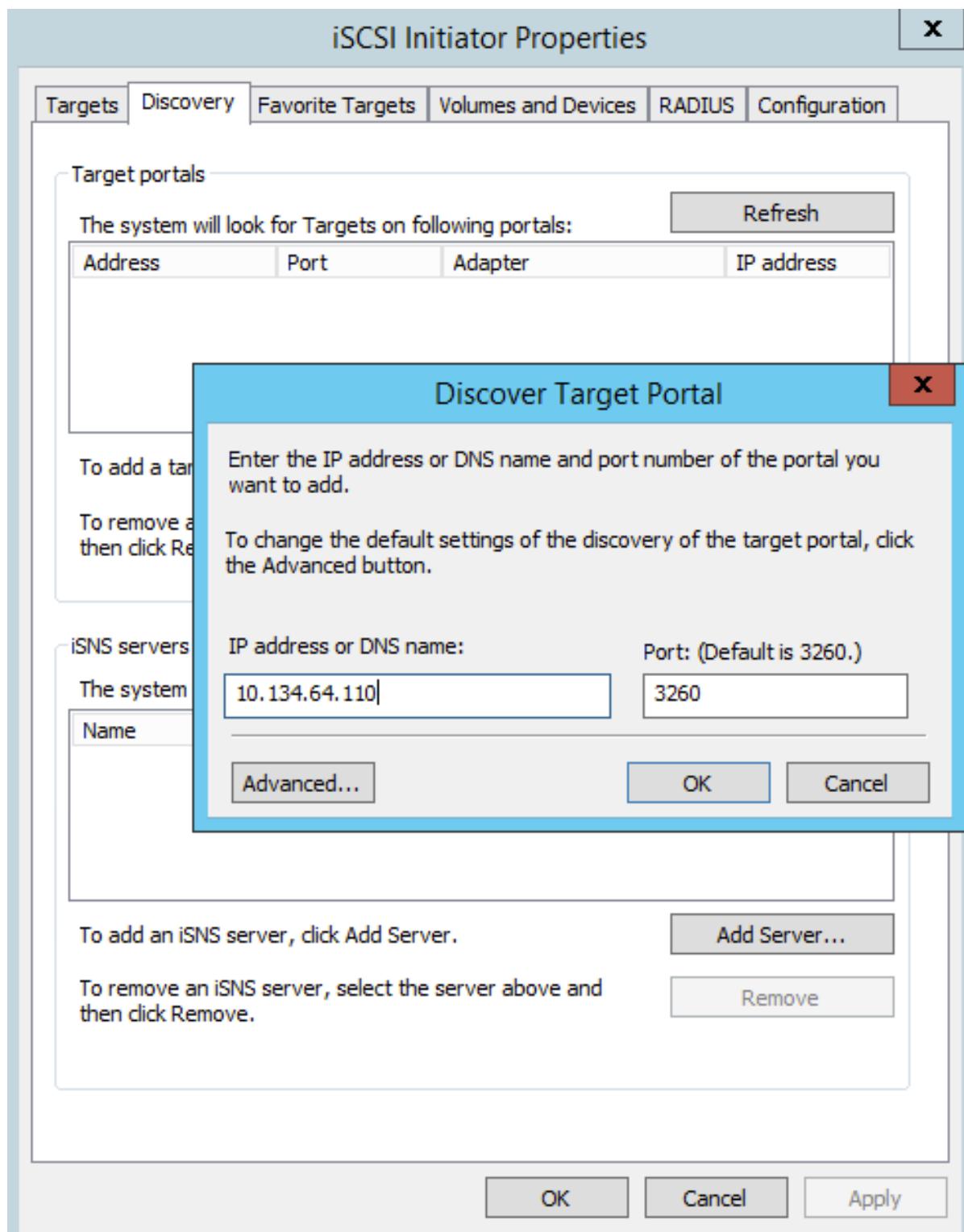


Figure: *iSCSI Initiator Properties*

4. Click **OK**.
5. To connect to the ABS target, go to the **Targets** tab.

- a. Click **Refresh**. The ABS target is shown as *Inactive*.
- b. Select the target and click **Connect**.
- c. Select *Add this connection to the list of Favorite Targets* to ensure this connection is persistent. Ensure that **Enable multi-path** is disabled (not selected).
- d. Click **OK**.

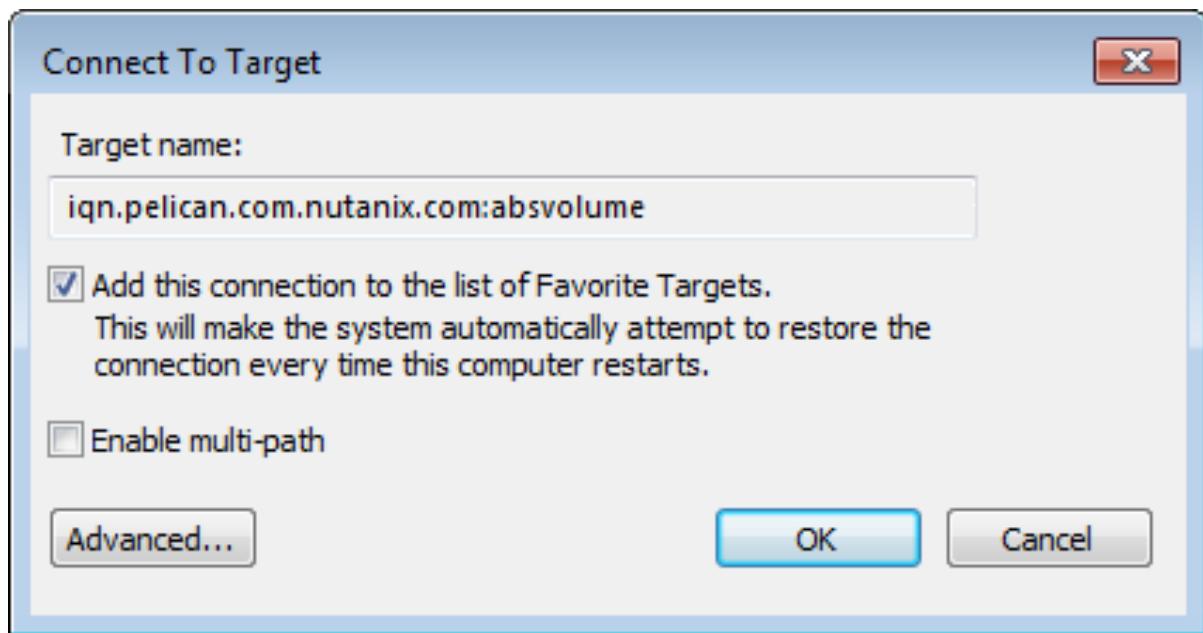


Figure: iSCSI ABS Target

The ABS target is now shown as **Connected**.

**What to do next:** See [Configuring CHAP Authentication \(Windows\)](#) on page 219.

#### Configuring CHAP Authentication (Windows)

**Before you begin:** Nutanix recommends setting one-way or Mutual CHAP authentication. Set the CHAP secret in the Nutanix cluster from the Prism web console *Updating Volume Group* dialog box first. Then configure CHAP authentication from the client side on the Windows server hosting your initiators.

This procedure describes how to configure CHAP authentication.

1. Open the *iSCSI Initiator Properties* window.
2. In the *iSCSI Initiator Properties* window, click the **Targets** tab and select the ABS target.
3. Click **Properties** to configure CHAP Authentication.
  - a. Ensure that **Enable Chap log on** is cleared (not selected).
  - b. Use the default **Name** as the initiator name
  - c. Type the same password in the **Target Secret** field as the one you used in the **Target Password** field in the Prism web console **Create Volume Group** dialog box.
  - d. For mutual CHAP authentication, select **Perform mutual authentication**. Otherwise, leave this setting cleared for one-way CHAP authentication.

e. Click **OK**.

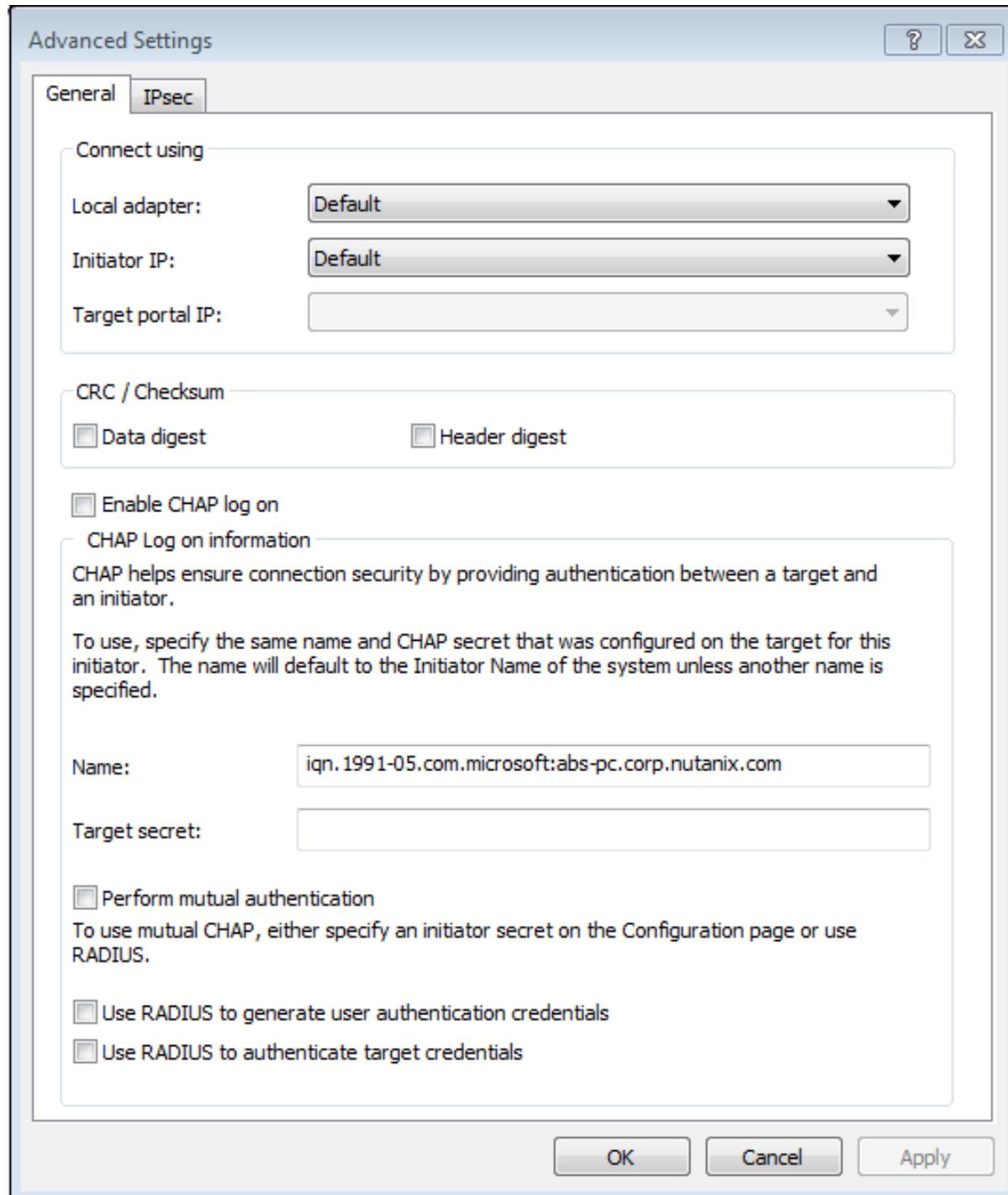


Figure: Configuring CHAP Authentication

- a. [Mutual CHAP configuration only; otherwise skip this step.] In the *iSCSI Initiator Properties* window, click the **Configuration** tab.
- b. Click **CHAP...**, type a password (or secret) in the **Initiator CHAP Secret** field, and click **OK**.



Figure: Windows Initiator Name

#### Obtaining the Windows Client iSCSI Initiator Name

This task is optional.

If you are configuring a volume group for use with Acropolis Block Services (ABS), you can optionally use the iSCSI initiator name (Initiator iSCSI Qualified Name [IQN]) instead of the IP address from the Windows clients. For supported clients, see [ABS Requirements and Supported Clients](#) on page 211.



**Note:** Each initiator IQN must be unique. Connections from two clients having same initiator IQN name might result in undesirable behavior or results.

1. Open the *iSCSI Initiator Properties* window.

If *iSCSI Initiator* is not available from Administrative Tools, you can open it by clicking **Start**, typing *iSCSI* in the search box, and clicking **iSCSI Initiator** under *Programs*.

2. In the *iSCSI Initiator Properties* window, click the **Configuration** tab.

The **Initiator Name** field contains the initiator IQN name. Copy this name for use with the procedures in this section.

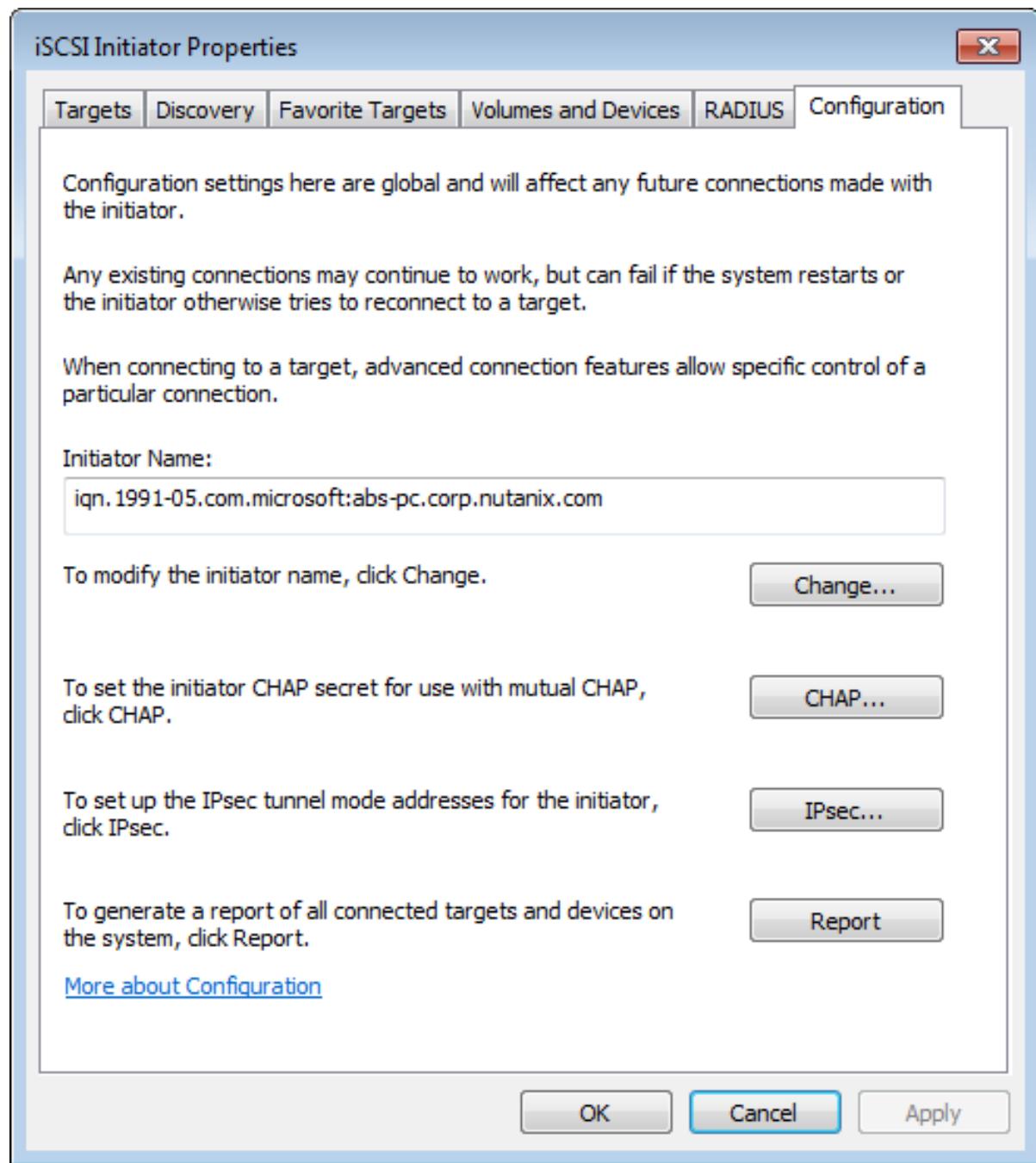


Figure: Windows Initiator Name

**What to do next:** Create a volume group. See [Creating a Volume Group for Use with ABS](#) on page 213.

## Configuring Linux Clients

### Discovering the ABS Target from the Linux Client

#### Before you begin:

1. You will need the Nutanix cluster data services IP address you created when you modified cluster details. See [Modifying Cluster Details](#) on page 42 and [About The iSCSI Data Services IP Address](#) on page 44.

2. Make sure you have already created a volume group with the initiators specified in the whitelist. Any LUNs associated with the volume group will be automatically discovered. See [Creating a Volume Group for Use with ABS](#) on page 213.
3. For additional security, see [Configuring Mutual CHAP Authentication \(Linux\)](#) on page 223.

This procedure describes how to perform a Linux client iSCSI discovery and connection of the data services IP address for the Nutanix cluster (the ABS target). This allows the cluster and its volume groups to be discoverable by the initiators. Do the following from a Linux client terminal window to discover and connect the ABS target.

1. Ensure that the iSCSI service is started.

- a. For Red Hat Enterprise Linux 6.0:

```
$ sudo /etc/init.d/iscsi status
```

- b. For Red Hat Enterprise Linux 6.7:

```
$ sudo service iscsid status
```

2. If the `iscsi status` command returns any status other than `running`, start the service.

- a. For Red Hat Enterprise Linux:

```
$ sudo /etc/init.d/iscsi start
```

- b. For SuSE Linux Enterprise Server Enterprise Linux:

```
$ sudo rcopen-iscsi restart
```

If the `iscsi status` command returns any status other than `running`, start the service by typing `sudo /etc/init.d/iscsi start` or

3. Discover the ABS target by specifying the iSCSI data services IP address on the default port 3260.

```
$ sudo /sbin/iscsiadm --mode discovery --type sendtargets \
--portal data_services_IP_address:3260
```

The command output will appear similar to `external_data_services_IP_address:3260, 1 iqn_name`, where `iqn_name` is the ABS target IQN.

4. Connect the ABS target by specifying `iqn_name` from the previous command.

```
$ sudo /sbin/iscsiadm --mode node --targetname iqn_name \
--portal data_services_IP_address:3260,1 --login
```

**What to do next:** Nutanix recommends that you configure CHAP authentication. See [Configuring Mutual CHAP Authentication \(Linux\)](#) on page 223.

#### Configuring Mutual CHAP Authentication (Linux)

For additional security, ABS also enables you to use Challenge-Handshake Authentication Protocol (CHAP) authentication with Linux clients.

Set this Mutual CHAP user names and passwords (secrets) from the client side on the Linux server hosting your initiators.

1. Log in to the linux server and get the name of the initiator(s).

```
$ sudo cat /etc/iscsi/initiatorname.iscsi
```

For example, the command displays:

```
InitiatorName=iqn.1991-05.com.redhat:8ef967b5b8f
```

Copy this name for use with the procedures in this section.

**2.** Open the /etc/iscsi/iscsid.conf file with a text editor.

Search for the CHAP SETTINGS section in the file. You might see text similar to the following.

```
*****
#CHAP Settings
*****

#To enable CHAP authentication set node.session.auth.authmethod
#to CHAP. The default is None.
#node.session.auth.authmethod = CHAP

#To set a CHAP username and password for initiator
#authentication by the target(s), uncomment the following lines:
#node.session.auth.username = username
#node.session.auth.password = password
node.session.auth.username = iqn.somename.somedomain.com
node.session.auth.password = xxxxxxxxxxxxxxxx

#To set a CHAP username and password for target(s)
#authentication by the initiator, uncomment the following lines:
#node.session.auth.username_in = username_in
#node.session.auth.password_in = password_in
node.session.auth.password_in = yyyyyyyyyyyyyy

#To enable CHAP authentication for a discovery session to the target
#set discovery.sendtargets.auth.authmethod to CHAP. The default is None.
#discovery.sendtargets.auth.authmethod = CHAP
#discovery.sendtargets.auth.authmethod = CHAP

#To set a discovery session CHAP username and password for the initiator
#authentication by the target(s), uncomment the following lines:
#discovery.sendtargets.auth.username = username
#discovery.sendtargets.auth.password = password

#To set a discovery session CHAP username and password for target(s)
#authentication by the initiator, uncomment the following lines:
#discovery.sendtargets.auth.username_in = username_in
#discovery.sendtargets.auth.password_in = password_in
```

**3.** Configure Mutual CHAP authentication. Be sure to uncomment any commented lines by removing the hash character [#, as shown here.

**a.** Enable CHAP authentication.

```
#To enable CHAP authentication set node.session.auth.authmethod
#to CHAP. The default is None.
#node.session.auth.authmethod = CHAP
```

**b.** Configure the initiator user name (initiator IQN) and **Target Password** password from [Add the Client iSCSI Initiators to the Volume Group](#) on page 215 procedure.

```
node.session.auth.username = initiator_IQN
node.session.auth.password = password
```

**c.** Configure the ABS target IQN user name and password.

The user name and password are derived from the [Add the Client iSCSI Initiators to the Volume Group](#) on page 215 procedure:

- Use the **iSCSI Target Name Prefix** as the *username\_in*.
- Use the **Target Password** as the *password*.

```
node.session.auth.username_in = username_in  
node.session.auth.password_in = password
```

4. Save and exit the file. Log out of any connected sessions and perform a discovery. See [Discovering the ABS Target from the Linux Client](#) on page 222.
5. Repeat for any additional initiators used with ABS.

#### Obtaining the Linux Client iSCSI Initiator Name

This task is optional.

If you are configuring a volume group for use with Acropolis Block Services (ABS), you can optionally use the iSCSI initiator name (Initiator iSCSI Qualified Name [IQN]) instead of the IP address from the Linux clients. For supported clients, see [ABS Requirements and Supported Clients](#) on page 211.



**Note:** Each initiator IQN must be unique. Connections from two clients having same initiator IQN name might result in undesirable behavior or results.

On the Linux client, open a terminal window and type:

```
$ sudo cat /etc/iscsi/initiatorname.iscsi
```

For example, the command displays:

```
InitiatorName=iqn.1991-05.com.redhat:8ef967b5b8f
```

Copy this name for use with the procedures in this section.



**Note:** If you change the initiator names, you must restart the `iscsi` service by typing `sudo /etc/init.d/iscsi restart`.

**What to do next:** Create a volume group. See [Creating a Volume Group for Use with ABS](#) on page 213.

#### Configuring AIX Clients

##### Changing the AIX Initiator Name

The default iSCSI initiator name (IQN) of an AIX host does not strictly conform to the iSCSI RFC standard. Change the IQN of each AIX host before connecting to the Nutanix cluster.

Change the IQN of each AIX host to include the date (year and month) before adding the initiators to the cluster volume group or connecting to the Nutanix cluster.

1. Log on to the AIX host through SSH.
2. Display the iSCSI initiator name (IQN) of the AIX host. For example, note the absence of the year and month in the name.

```
# lsattr -E -l iscsi0  
nodename.iqn.aixhost1.hostid.0a4cac48
```

- In this example, change the IQN to include the date (format yyyy-mm).

```
# chdev -l iscsi0 -a initiator_name=iqn.2016-04.aixhost1.hostid.0a4cac48
```

A successful message of iscsi0 changed is displayed.

- Verify the change.

```
# lsattr -E -l iscsi0  
nodename.iqn.2016-04.aixhost1.hostid.0a4cac48
```

- Repeat these steps for each AIX host.

**What to do next:** See [Creating a Volume Group for Use with ABS](#) on page 213 and [Adding iSCSI Targets on the AIX Host](#) on page 226.

#### Adding iSCSI Targets on the AIX Host

**Before you begin:** The AIX software initiator supports static discovery only. As a result, add the cluster iSCSI targets to the AIX host by editing the /etc/iscsi/targets file on the AIX host so the host can discover the cluster targets. You can obtain the volume group base target name from the Prism web console.

- Log in to the Prism web console and get the volume group virtual target IQN prefix names
  - Click **Storage**, then select the **Table** view.
  - Click **Volume Group** and select the volume group.
  - Obtain the **Target IQN Prefix** in the *Summary* for the volume group. All disks in the volume group will have the same target IQN prefix.  
For example:

```
iqn.2010-06.com.nutanix:vg1-5ff34411-080e-4b95-97c8-c2e34d9e1a82
```

- Log on to the AIX host through SSH.
- Using a text editor, open the /etc/iscsi/targets file and add the cluster target information.  
Include the Controller VM IP address or iSCSI data services IP address and port 3260, then append -tgt x to the target IQN entry, where x starts at 0. The number of entries depends of the number of disks in the volume group. The maximum number of targets is 32 (that is, -tgt0 through -tgt31). If there are more than 32 disks in the volume group, you do not have to enter additional targets beyond the 32nd disk.

Example: For a volume group consisting of a single disk:

```
10.1.216.192 3260 iqn.2010-06.com.nutanix:vg1-5ff34411-080e-4b95-97c8-c2e34d9e1a82-tgt0
```

Example: For a volume group consisting of 5 disks:

```
10.1.216.192 3260 iqn.2010-06.com.nutanix:vg1-5ff34411-080e-4b95-97c8-c2e34d9e1a82-tgt0  
10.1.216.192 3260 iqn.2010-06.com.nutanix:vg1-5ff34411-080e-4b95-97c8-c2e34d9e1a82-tgt1  
10.1.216.192 3260 iqn.2010-06.com.nutanix:vg1-5ff34411-080e-4b95-97c8-c2e34d9e1a82-tgt2  
10.1.216.192 3260 iqn.2010-06.com.nutanix:vg1-5ff34411-080e-4b95-97c8-c2e34d9e1a82-tgt3  
10.1.216.192 3260 iqn.2010-06.com.nutanix:vg1-5ff34411-080e-4b95-97c8-c2e34d9e1a82-tgt4
```

- If you are using CHAP authentication, append the CHAP secret to the end of each entry, enclosed in double-quote characters.

For example:

```
10.1.216.192 3260 iqn.2010-06.com.nutanix:vg1-5ff34411-080e-4b95-97c8-c2e34d9e1a82-tgt0  
"AIXforyou@123"
```

5. Save and close the file.

**What to do next:** See [Discovering the ABS Target from the AIX Client](#) on page 227.

#### Discovering the ABS Target from the AIX Client

##### Before you begin:

1. Modify the AIX IQN name to make it compliant and useable by ABS. See [Changing the AIX Initiator Name](#) on page 225.
2. Make sure you have already created a volume group with the initiators specified in the whitelist. Any LUNs associated with the volume group will be automatically discovered. See [Creating a Volume Group for Use with ABS](#) on page 213.
3. Add iSCSI targets to the AIX host. See [Adding iSCSI Targets on the AIX Host](#) on page 226.

This procedure describes how to perform an AIX client iSCSI discovery and connection of the data services IP address for the Nutanix cluster (the ABS target). This allows the cluster and its volume groups to be discoverable by the initiators. Do the following from an AIX client terminal window to discover and connect the ABS target.

1. Log on to the AIX host through SSH (if you are not already logged on).
2. Verify that the AIX host can contact the cluster targets.

```
# cfgmgr -v -l iscsi0
```

3. If the command is successful, AIX defines a new hard disk for each discovered LUN. Display them as follows.

```
# lsdev -c disk
```

The command result shows iSCSI disk drives.

## Booting Over iSCSI

#### Configuring the Intel NIC

**Before you begin:** ABS supports the ability to boot an operating system over iSCSI for physical servers. In this configuration, a host can start a supported operating system from a LUN instead of a local disk instance. This procedure describes how to configure the Intel NIC BIOS settings to enable this feature.

- See the Intel Ethernet Adapter vendor documentation for more details about *Intel iSCSI Boot* configuration.
  - According to Intel, you might be able to configure these settings through the adapter's **Properties > Data Options** tab in Microsoft Windows Device Manager.
  - See [ABS Requirements and Supported Clients](#) on page 211 for a list of the supported network hardware and clients.
1. See [Enabling Acropolis Block Services](#) on page 213 and read about the procedures to perform on the Nutanix cluster. Before performing an iSCSI target discovery of the Nutanix cluster, configure BIOS boot settings for the network adapter as described in these steps.
  2. Open the **iSCSI Port Selection** page to configure the network adapter.

Start or restart the host machine where the network adapter is installed and press the **Ctrl+D** keys when you see the Press **Ctrl-D** to run setup... message during the boot sequence.

3. Select the adapter you are configuring and press **P** to select the adapter as the primary boot device, then press **Enter**.

4. Select **iSCSI Boot Configuration**, press **Enter**, then complete these fields .

Initiator network information

- **Use DHCP**. Clear (not selected).
- **Initiator Name**. iSCSI RFC 3720 compliant name.
- **Initiator IP**. Client IP address.
- **Subnet Mask**. IP subnet mask address
- **Gateway**. Network gateway IP address.

Nutanix iSCSI target information

- **Use DHCP for iSCSI Target Information**. Clear (not selected).
- **Target Name**. Use **iSCSI Target Name Prefix** Nutanix cluster target name from the volume group you created in [Creating a Volume Group for Use with ABS](#) on page 213 appended with the disk index number `-tgtx` as shown in the volume group dialog box. You can select any disk in the volume group.

For example, for a volume group consisting of a single disk:

```
iqn.2010-06.com.nutanix:vg1-5ff34411-080e-4b95-97c8-c2e34d9e1a82-tgt0
```

- **Target IP**. Use the iSCSI data services IP address of the Nutanix cluster. See [Modifying Cluster Details](#) on page 42.
- **Target Port**. 3260
- **Boot LUN**. 0

5. Select **OK**.

6. [Optional] Select **iSCSI CHAP Configuration** to configure CHAP/Mutual CHAP authentication.

- Select **Use CHAP** and enter a user name and target secret (from the procedures described in [Creating a Volume Group for Use with ABS](#) on page 213).
- Select **Use Mutual CHAP** and enter an initiator secret.

7. Select **OK**.

8. Select **Save changes and Exit**.

9. Press **Esc** to exit the **iSCSI Port Selection** page.

10. Install the supported operating systems listed in [ABS Requirements and Supported Clients](#) on page 211 on the iSCSI LUN.

11. Perform an iSCSI target discovery of the Nutanix cluster from the clients.

12. [Optional] Configure CHAP or Mutual CHAP authentication on the initiators and target Nutanix clusters. See [Configuring CHAP Authentication \(Windows\)](#) on page 219 or [Configuring Mutual CHAP Authentication \(Linux\)](#) on page 223.

## Configuring the QLogic HBA

**Before you begin:** ABS supports the ability to boot an operating system over iSCSI for physical servers. In this configuration, a host can start a supported operating system from a LUN instead of a local disk instance. This procedure describes how to configure the QLogic HBA BIOS settings to enable this feature.

- See the QLogic 10GbE Converged Network Adapter vendor documentation for more details.
  - See [ABS Requirements and Supported Clients](#) on page 211 for a list of the supported network hardware and clients.
1. See [Enabling Acropolis Block Services](#) on page 213 and read about the procedures to perform on the Nutanix cluster. Before performing an iSCSI target discovery of the Nutanix cluster, configure BIOS boot settings for the network adapter as described in these steps.
  2. Open the **Comprehensive Configuration Management** page to configure the network adapter. Start or restart the host machine where the network adapter is installed and press the **Ctrl+S** keys when you see the Ethernet Boot Agent banner during the boot sequence.
  3. Select the adapter you are configuring and press **Enter**, then select **MBA Configuration**.
  4. Go to **Boot Protocol** and select **iSCSI**.
  5. Press **Esc** to go back to the *Main Menu*, select **iSCSI Boot Configuration** and press **Enter**.
  6. Select **1st Target Parameters**, enable **Connect**, then complete these fields:
    - **IP Address**. Use the iSCSI data services IP address of the Nutanix cluster. See [Modifying Cluster Details](#) on page 42.
    - **TCP Port**. 3260
    - **Boot LUN**. 0
    - **iSCSI Name**. Use **iSCSI Target Name Prefix** Nutanix cluster target name from the volume group you created in [Creating a Volume Group for Use with ABS](#) on page 213 appended with the disk index number `-tgtx` as shown in the volume group dialog box. You can select any disk in the volume group.

For example, for a volume group consisting of a single disk:

```
iqn.2010-06.com.nutanix:vg1-5ff34411-080e-4b95-97c8-c2e34d9e1a82-tgt0
```

    - **CHAP ID**. Use for CHAP / Mutual CHAP authentication .
    - **CHAP Secret**. Use for Mutual CHAP authentication. (from the procedures described in [Creating a Volume Group for Use with ABS](#) on page 213).
  7. Press **Esc** twice to exit the menu and save the configuration.
  8. Press **CTRL+ALT+DEL** to apply adapter changes and exit the **Comprehensive Configuration Management** page.
  9. See the QLogic 10GbE Converged Network Adapter vendor documentation to install the supported operating systems listed in [ABS Requirements and Supported Clients](#) on page 211 on the iSCSI LUN.
-  **Note:** As described in the vendor documentation, Windows installations require you to create a slipstream Windows Server image that includes the network adapter drivers. During Windows installation, the iSCSI LUN will then be displayed in the list of disks where Windows Server will be installed.
10. Perform an iSCSI target discovery of the Nutanix cluster from the clients.
  11. [Optional] Configure CHAP or Mutual CHAP authentication on the client initiators and target Nutanix clusters.  
See [Configuring CHAP Authentication \(Windows\)](#) on page 219 or [Configuring Mutual CHAP Authentication \(Linux\)](#) on page 223.

## Modifying a Volume Group (AIX Boot Over iSCSI)

**Before you begin:** Modify the default iSCSI initiator name (IQN) for AIX hosts to make it compliant and useable by ABS. See [Changing the AIX Initiator Name](#) on page 225.

To boot AIX over iSCSI, use the Acropolis command line `acli` to set the `use_redirection` property to `false` for the new or existing volume group where the boot LUN resides.

1. To access the Acropolis command line, log on to a Controller VM in the cluster with SSH and type `acli` at the shell prompt.
2. Set the volume group `use_redirection` property to `false`. Here, the example volume group name is `vg1` and example initiator name is `iqn.2016-04.aixhost1.hostid.0a4cac48`.

→ Do this step for a new volume group.

```
vg.attach_external vg1 initiator_name=iqn.2016-04.aixhost1.hostid.0a4cac48:aeou \
use_redirection=false
```

→ Do this step for an existing volume group where the initiator is already attached by adding `use_redirection=false`.

```
vg.update_external vg1 initiator_name=iqn.2016-04.aixhost1.hostid.0a4cac48:aeou \
use_redirection=false
```

3. Exit the command line by typing `exit`, then log out of the SSH session.

## Converting Volume Groups and Updating Clients to Use ABS

This topic describes the workflow to use Acropolis Block Services if you have upgraded to AOS 5.1 or later and want to convert an existing volume group that includes attached external initiators with previously-discovered Controller VM IP address as target portal addresses. Use these procedures also if you are using clients currently configured to use multipath I/O (MPIO) and want to use Acropolis Block Services instead.

1. From the Windows or Linux client: Disconnect and remove any existing targets configured on the client.
  - [Modifying Linux Client Settings to Use ABS](#) on page 231
  - [Modifying Windows Client Settings to Use ABS](#) on page 231
2. From the Prism web console:
  - a. Modify the existing AOS volume group to delete (detach) existing whitelisted initiator IQNs.
  - b. Add (re-attach) the initiators to the volume group.

See [Modifying a Volume Group for Use with ABS](#) on page 232.
3. Create an iSCSI data services IP address for the Nutanix cluster. This address cannot be the same as the cluster virtual IP address. See [Modifying Cluster Details](#) on page 42.
4. From the Windows or Linux client: Discover and connect to the new targets. Do not use MPIO. (For Windows, ensure that **Enable multi-path** is disabled (not selected).

## Modifying Windows Client Settings to Use ABS

For all Controller VM IP addresses previously discovered as targets, disconnect each session and delete the target portal IP addresses. Then discover and connect to the new target.

1. From Windows Server, open the *iSCSI Initiator Properties* window to disconnect and remove any existing targets.

If *iSCSI Initiator* is not available from **Administrative Tools**, you can open it by clicking **Start**, typing **iSCSI** in the search box, and clicking **iSCSI Initiator** from *Programs*.

- a. In the *iSCSI Initiator Properties* window, click the **Targets** tab.
- b. Select a discovered target, then click **Disconnect**.
- c. In the *iSCSI Initiator Properties* window, click the **Discovery** tab.
- d. In **Target portals**, select each Controller VM IP address, then click **Remove**.
- e. Click the **Favorite Targets** tab, select the discovered target, then click **Remove**.

This step is needed because Windows clients will connect to **Favorites Targets** even if you remove them from the **Discovery** tab.

2. From the Prism web console, delete (detach), then add (re-attach) initiator IQNs in the AOS volume group as described in [Modifying a Volume Group for Use with ABS](#) on page 232.
3. Create an iSCSI data services IP address for the Nutanix cluster. This address cannot be the same as the cluster virtual IP address. See [Modifying Cluster Details](#) on page 42.
4. Discover and connect to the new target as described in [Discovering the ABS Target from the Windows Client](#) on page 217.

## Modifying Linux Client Settings to Use ABS

For all Controller VM IP addresses previously discovered as targets, disconnect by logging out of each session and delete the target portal IP addresses. Then discover and connect to the new target.

1. Open a Linux terminal window and log out of the iSCSI targets to disconnect the iSCSI session by doing one of the following.

- a. Log out of all targets.

```
$ sudo /sbin/iscsiadm -m node -u
```

- b. Log out of a specific target.

```
$ sudo /sbin/iscsiadm --mode node --targetname iqn_name \
--portal target_IP_address:3260,1 --logout
```

2. Remove the now-disconnected target records from *discoverydb*.

```
$ sudo /sbin/iscsiadm -m node -o delete
```

3. From the Prism web console, delete (detach), then add (re-attach) initiator IQNs in the AOS volume group as described in [Modifying a Volume Group for Use with ABS](#) on page 232.

4. Create an iSCSI data services IP address for the Nutanix cluster. This address cannot be the same as the cluster virtual IP address. See [Modifying Cluster Details](#) on page 42.

- Discover and connect to the new target as described in [Discovering the ABS Target from the Linux Client](#) on page 222.

## Modifying a Volume Group for Use with ABS

**Before you begin:** If you choose to use iSCSI initiator names instead of whitelisting IP addresses, get the iSCSI initiator name(s) from your client server (Windows Server or Linux). See [Obtaining the Windows Client iSCSI Initiator Name](#) on page 221 or [Obtaining the Linux Client iSCSI Initiator Name](#) on page 225.

To boot AIX over iSCSI, set the `use_redirection` property to `false` for the new or existing volume group where the boot LUN resides. See [Modifying a Volume Group \(AIX Boot Over iSCSI\)](#) on page 230.

Modify an existing AOS volume group to delete (detach) existing whitelisted initiator IQNs from it, then add (re-attach) the initiators to the volume group. Use the scrollbar to see all fields and buttons.

- In the Prism web console, select **Storage** from the pull-down main menu, and then select the **Table** and **Volume Group** tabs.
- To update a volume group, select the volume group, and then click the **Update** link. The *Update Volume Group* dialog box is displayed.
- Scroll down to the **Access Settings** section and remove any IQN initiators listed.
- Click **Save**.
- Select the volume group again and click **Update**.
- To whitelist the initiators that must access the volume group, in the **Initiators** section, see [Add the Client iSCSI Initiators to the Volume Group](#) on page 215.



**Note:** If the initiator is a VM on AHV and you want to attach the volume group as a SCSI disk, skip this step and save the volume group. After it is saved, modify the volume group to attach VMs.

- Click **Save**.

**What to do next:** For the whitelisted initiators, perform an iSCSI discovery and connection of the data services IP address for the Nutanix cluster on the client (Windows or Linux). See [Discovering the ABS Target from the Windows Client](#) on page 217 or [Discovering the ABS Target from the Linux Client](#) on page 222.

## Data Protection

Nutanix offers data protection solutions for virtual datacenters. Nutanix provides data protection functions at the VM, file, and volume group level, so VMs and data remain safe in a crash-consistent environment.



**Warning:** Nutanix native snapshots and replication is not supported for VMs configured with Hyper-V host snapshots. If such VMs are configured with Nutanix native snapshot or replication, unexpected snapshot behavior could result.

- Nutanix supports several types of protection strategies including one-to-one or one-to-many replication (see [Protection Strategies](#) on page 233).
- You can implement a data protection strategy by configuring protection domains and remote sites through the web console.
  - A protection domain is a defined set of virtual machines, volume groups (see [Configuring a Protection Domain \(Async DR\)](#) on page 256), or storage containers (see [Configuring a Protection Domain \(Metro Availability\)](#) on page 274) to be protected.
  - A remote site (see [Configuring a Remote Site \(Physical Cluster\)](#) on page 317 or [Cloud Connect \(AWS and Azure\)](#) on page 304) is the target location to store data replications (Async DR) or standby storage containers (metro availability).
- The web console allows you to monitor data protection implementations and status across the cluster (see [Data Protection Dashboard](#) on page 237).
- You can restore a protected VM or volume group at any time through the web console (see [Restoration of Protected Entities](#) on page 264).

### Protection Strategies

Replication is a fundamental component of any enterprise data protection solution, ensuring that critical data and applications can be reliably and efficiently replicated to a different site or a separate infrastructure. While enterprise IT architects have many technology options, there are replication capabilities that are requisite for any successful enterprise data protection initiative.

- *Per-VM Backup.* The ability to designate certain VMs for backup to a different site is particularly useful in branch office environments. Typically, only a subset of VMs running in a branch location require regular back up to a central site. Such per-VM level of granularity, however, is not possible when replication is built on traditional storage arrays. In these legacy environments replication is performed at a coarse grain level, entire LUNs or volumes, making it difficult to manage replication across multiple sites.
- *Selective Bi-directional Replication.* In addition to replicating selected VMs, a flexible replication solution must also accommodate a variety of enterprise topologies. It is no longer sufficient to simply replicate VMs from one active site to a designated passive site, which can be "lit up" in event of a disaster. Supporting different topologies demands that data and VMs can be replicated bi-directionally.
- *Synchronous Datastore Replication (metro availability).* Datastores can be spanned across two sites to provide seamless protection in the event of a site disaster (see [Data Protection Guidelines \(Metro Availability\)](#) on page 271).

The Nutanix native replication infrastructure and management supports a wide variety of enterprise topologies to meet real-world requirements. The following are four replication options to consider.

1. **Two-Way Mirroring.** The ability to mirror VM replication between multiple sites is necessary in environments where all sites must support active traffic. Consider a two-site example. Site 2 is used as the target for selected workloads running on Site 1. At the same time, Site 1 serves as the data protection target for designated workloads running at Site 2. In this scenario there are active workloads running on both sites simultaneously, such that there are no idle resources in either location. Utilizing storage, compute and networking resources at both locations has a significant advantage over traditional data protection strategies where servers sit idle in anticipation of a future data disaster event.



Figure: Two-Way Mirroring Topology

2. **One-to-Many.** In a different scenario, there may be one central site with multiple remote locations. Consider an example where tier-one workloads run at site 1, and sites 2 and 3 serve as remote backup locations. Site 1 workloads can then be replicated to both 2 and 3 locations. In the event of a data disaster event, the protected workloads can be started on either the desired replication sites for greater overall VM availability.

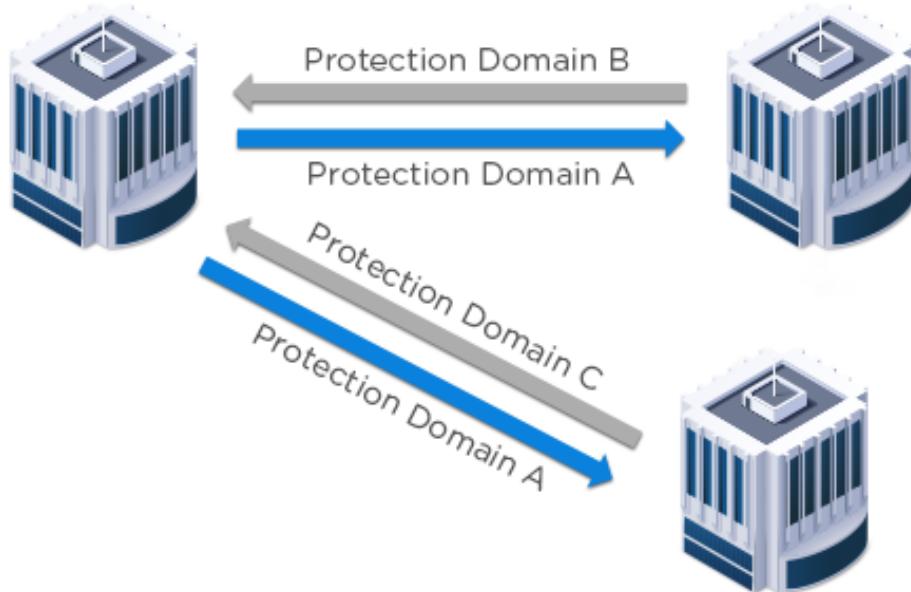


Figure: One-to-Many Topology

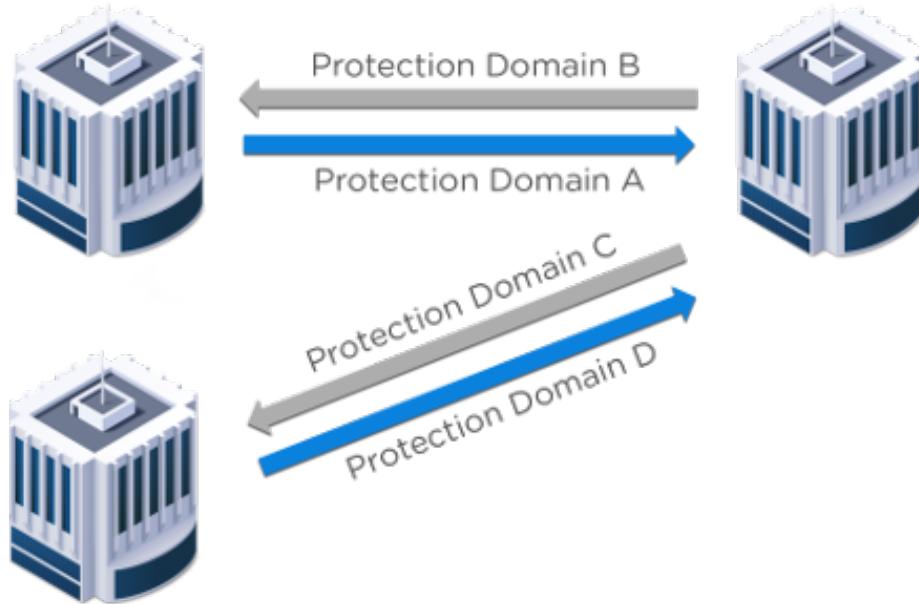
A one-to-many topology can also be designed to optimize bandwidth between sites. For example, assume the available wide area network (WAN) bandwidth between sites 1 and 3 is greater than that between sites 1 and 2. (Sites 1 and 2 could be in the same city, whereas site 3 may be across the country). In this case, the replication schedule can be set such that larger size VMs running at site 1 are

replicated to site 2 in order to conserve bandwidth and improve performance. Similarly, smaller VMs are backed up to site 3, to make better use of lower bandwidth resources.

3. **Many-to-One.** In a hub and spoke architecture workloads running on site 1 and 2, for example, can be replicated to a central site 3. Centralizing replication to a single site may improve operational efficiency for geographically disperse environments. Remote and branch offices (ROBO) are a classical use case of a many-to-one topology.

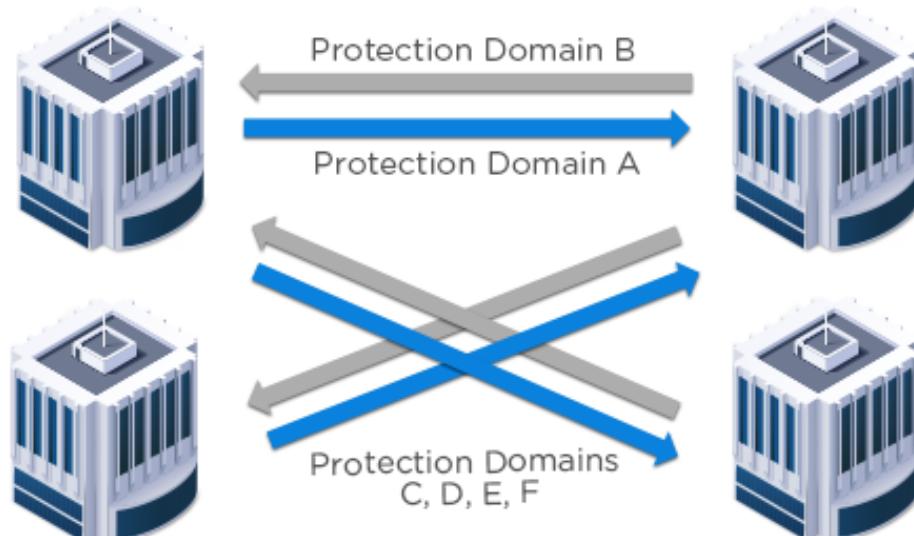


**Note:** Many-to-one replication with the same protection domain name is not supported.



*Figure: Many-to-One Topology*

4. **Many-to-Many.** This topology allows for the most flexible setup. Here, IT departments have a maximum amount of control and flexibility to ensure application and service level continuity.



*Figure: Many-to-Many Topology*

## Data Protection Concepts

The data protection features for a Nutanix cluster employ the following components and capabilities.

### Protection Domain

There are two types of protection domains.

- *Protection domain (Async DR)*. A standard (Async DR) protection domain is a defined group of entities (VMs and volume groups) that are backed up locally on a cluster and optionally replicated to one or more remote sites (see [Configuring a Protection Domain \(Async DR\)](#) on page 256). This type of protection domain uses asynchronous data replication to create snapshots. Protection domain names must be unique across sites. An entity can be in at most one protection domain.

A protection domain on a cluster is in one of two modes:

#### *Active*

Manages volume groups and live VMs; makes, replicates, and expires snapshots.

#### *Inactive*

Receives snapshots from a remote cluster.

- *Protection domain (Metro Availability)*. A metro availability protection domain consists of a specified (active) storage container in the local cluster linked to a (standby) container with the same name on a remote site in which synchronous data replication occurs when metro availability is enabled (see [Configuring a Protection Domain \(Metro Availability\)](#) on page 274).

### Consistency Group

A consistency group is a subset of the entities in a protection domain. (Consistency groups are configured when creating a protection domain.) All entities within a consistency group for that protection domain are snapshotted in a crash-consistent manner. For all VMs in a consistency group, a snapshot creates one snapshot for all VMs in the group.

### Snapshot

A snapshot is read-only copy of the state and data of a VM or volume group at a point in time.

### Time Stream

A time stream is a set of snapshots that are stored on the same cluster as the source VM or volume group.

### Remote Site

A remote site is a separate cluster used as a target location to replicate backed up data. You can configure one or more remote sites for a cluster (see [Configuring a Remote Site \(Physical Cluster\)](#) on page 317 or [Cloud Connect \(AWS and Azure\)](#) on page 304 ).

### Replication

Replication is the process of asynchronously copying snapshots from one cluster to one or more remote sites. Several replication scenarios are supported (see [Protection Strategies](#) on page 233).

### Schedule

A schedule is a property of a protection domain that specifies the intervals to take snapshots and how long the snapshots should be retained. (Schedules are set up when configuring a protection domain.) A schedule optionally specifies which remote site or sites to replicate to.

## Related Entities

Related entities are the VMs and volume groups that are associated with the entities that you want to protect. The association can be direct (in the form of direct hypervisor attachment or in-guest iSCSI) or transitive (if a volume group is attached to two VMs, then the VMs are considered to be related to each other).

For example, if a volume group named VG1 is directly attached to a VM named VM1 as a SCSI disk, VG1 and VM1 are related entities. If VG1 is also connected to a VM named VM2, VG1 and VM2 are related entities. In this configuration, VM1 and VM2 are considered to be related entities too because they are associated with the same volume group.

For the requirements to include related entities and limitations, see [Data Protection Guidelines \(Async DR\)](#) on page 250.

## Data Protection Dashboard

The Data Protection dashboard displays dynamically updated information about the data protection configuration in a cluster. To view the Data Protection dashboard, select **Data Protection** from the pull-down list on the far left of the main menu.

### Menu Options

In addition to the main menu (see [Main Menu Options](#) on page 32), the Data Protection screen includes a menu bar with the following options:

- **View selector.** The Data Protection dashboard provides three viewing modes.
  - Click the **Overview** button on the left to display data protection and recovery information in a summary view (see [Data Protection Overview View](#) on page 238).
  - Click the **Table** button to display data protection information in a tabular form. The table screen is further divided into protection domain and remote site views; click the **Async DR** or **Metro Availability** tabs to view protection domain information or the **Remote Site** tab to view remote site information (see [Data Protection Table View](#) on page 239).
- **Action buttons.** Click the **Remote Site** button on the right to configure a remote site (see [Configuring a Remote Site \(Physical Cluster\)](#) on page 317). Click the **Protection Domain** button on the right and then select **Async DR** from the pull-down list to configure a protection domain for asynchronous data replications used to create backup snapshots (see [Configuring a Protection Domain \(Async DR\)](#) on page 256) or **Metro Availability** to configure a protection domain for a metro availability configuration (see [Configuring a Protection Domain \(Metro Availability\)](#) on page 274).
- **Page selector.** In the Table view, remote sites and protection domains are listed 10 per page. When there are more than 10 items in the list, left and right paging arrows appear on the right, along with the total count and the count for the current page.
- **Export table content.** In the Table view, you can export the table 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 pull-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 table content.** In the Table view, you can search for specific content in the table by entering a string in the search field.



Figure: Data Protection Dashboard Menu

## Data Protection Overview View

The Data Protection Overview view displays data protection-specific performance and usage statistics on the left plus the most recent data protection-specific alert and event messages on the right. 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.

The following figure is a sample view, and the table describes each field in this view.

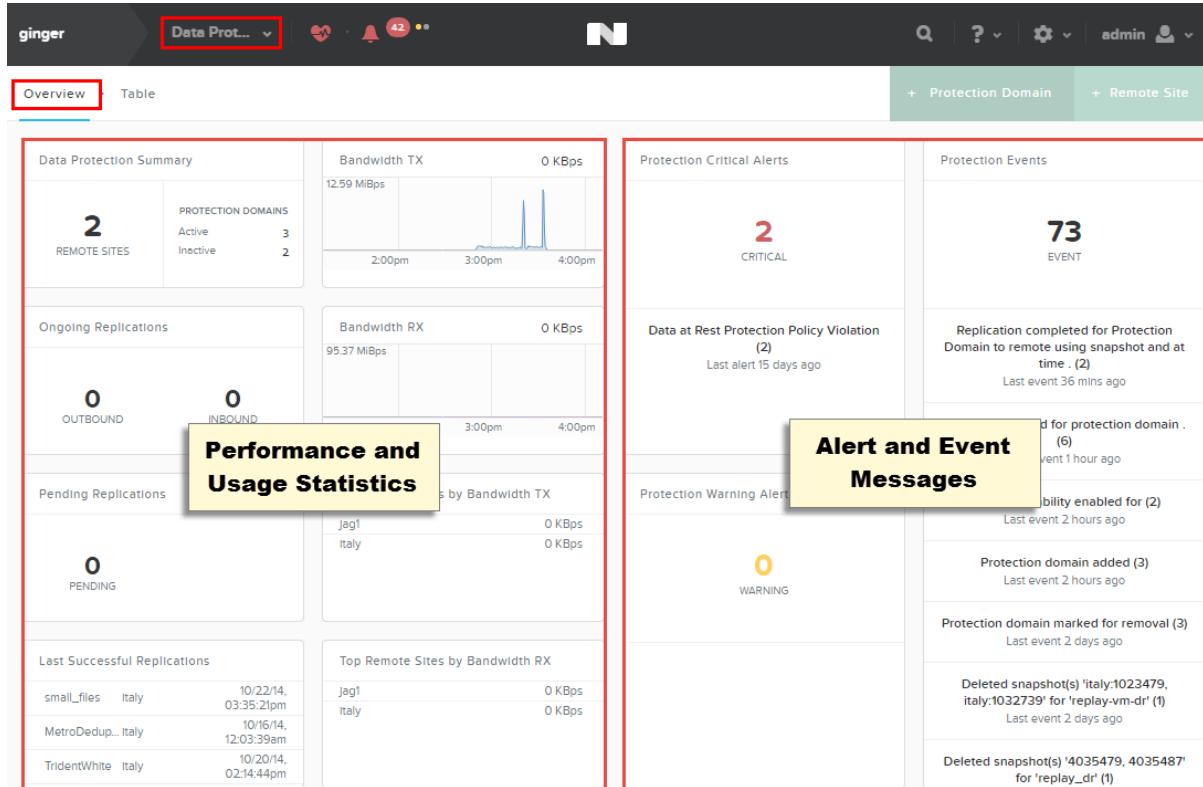


Figure: Data Protection Overview View

## Data Protection Overview View Fields

Name	Description
Data Protection Summary	Displays the current number of remote sites, active protection domains, and inactive protection domains.
Ongoing Remote Replication	Displays the number of ongoing outbound and inbound replications.

Name	Description
Pending Replication	Displays the number of pending replications.
Last Successful Replication	Displays the date and time of the last successful replication (and the remote site name) for each protection domain.
Bandwidth TX	Displays the amount of replication data (in GB or TB) transmitted from protection domains to remote sites in the cluster. 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 link in the upper right of the chart (see <a href="#">Analysis Dashboard</a> on page 401).
Bandwidth RX	Displays the amount of recovery data (in GB or TB) received by protection domains from remote sites in the cluster.
Top Remote Sites by Bandwidth TX	Displays the names of the protection domains using the most replicated data storage. Clicking on a protection domain name displays the Table detail page for that protection domain (see <a href="#">Data Protection Table View</a> on page 239).
Top Remote Sites by Bandwidth RX	Displays the names and amount of storage (in GB or TB) at the remote sites storing the largest amounts of replicated data.
Protection Critical Alerts	Displays the five most recent unresolved data protection-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 <b>view all alerts</b> button at the bottom of the list (see <a href="#">Alerts Dashboard</a> ).
Protection Warning Alerts	Displays the five most recent unresolved data protection-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.
Protection Events	Displays the 10 most recent data protection-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.

## Data Protection Table View

The *Data Protection* table view displays information about remote sites and protection domains in a tabular form. Click the **Async DR** or **Metro Availability** tab in the screen menu bar to display protection domain information; click the **Remote Site** tab to display remote site information. The displayed information is dynamically updated to remain current.

The *Data Protection* table view is divided into two sections:

- The top section is a table. Each row represents a single protection domain (configured for asynchronous data replication or metro availability) or remote site and includes basic information about that protection domain or remote site. 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 content and set of tabs varies depending on what has been selected.

This screenshot shows the Data Protection Table View in the Prism Web Console. The Async DR tab is selected. At the top, there's a navigation bar with tabs for Overview, Table (highlighted), Metro Availability, and Remote Site. On the right, there are buttons for pagination, export, and search. Below the navigation, a table lists protection domains: CH-DR-TEST, TEST-DR, WINDOWS-FLR, and WINTEST-PU. The table includes columns for Name, Remote Sites, Entity Count, Next Snapshot Time, Snapshot Exclusive Usage, B/W Used (Tx), B/W Used (Rx), Ongoing, and Pending. A yellow box highlights the 'entity information (protection domain or remote site)' section. At the bottom, there's a summary for CH-DR-TEST with tabs for Replications, Entities, Schedules, Local Snapshots, Remote Snapshots, Metrics, Alerts, and Events. A yellow box highlights the 'summary information (cluster, protection domain, or remote site)' section.

Figure: Data Protection Table View

## Async DR Tab

Clicking the **Async DR** tab displays information about protection domains configured for asynchronous data replication in the cluster (see [Configuring a Protection Domain \(Async DR\)](#) on page 256). This type of protection domain consists of a defined group of virtual machines to be backed up (snapshots) locally on a cluster and optionally replicated to one or more remote sites.

- The table at the top of the screen displays information about all the configured protection domains, and the details column (lower left) displays additional information when a protection domain is selected in the table. The following table describes the fields in the protection domain table and detail column.
- When a protection domain is selected, **Summary: protection\_domain\_name** appears below the table, and action links relevant to that protection domain appear on the right of this line. The actions vary depending on the state of the protection domain and can include one or more of the following (see [Modifying a Protection Domain \(Async DR\)](#) on page 262 for more information about these actions):
  - Click the **Take Snapshot** link to create a snapshot (point-in-time backup) of this protection domain.
  - Click the **Migrate** link to migrate this protection domain.
  - Click the **Update** link to update the settings for this protection domain.
  - Click the **Delete** link to delete this protection domain configuration.
- Eight tabs appear that display information about the selected protection domain (see following sections for details about each tab): **Replications**, **Entities**, **Schedules**, **Local Snapshots**, **Remote Snapshots**, **Metrics**, **Alerts**, **Events**.

This screenshot shows the Data Protection Table View for the Async DR tab. The Async DR tab is selected. At the top, there's a navigation bar with tabs for Overview, Table (highlighted), Metro Availability, and Remote Site. On the right, there are buttons for actions, search in table, and a dropdown for protection domains. Below the navigation, a table lists protection domains: CH-DR-TEST, TEST-DR, WINDOWS-FLR, and WINTEST-PU. The table includes columns for Name, Remote Sites, Entity Count, Next Snapshot Time, Snapshot Exclusive Usage, B/W Used (Tx), B/W Used (Rx), Ongoing, and Pending. A yellow box highlights the 'entity information (protection domain or remote site)' section. At the bottom, there's a summary for CH-DR-TEST with tabs for Replications, Entities, Schedules, Local Snapshots, Remote Snapshots, Metrics, Alerts, and Events. A yellow box highlights the 'tabs' section. A red arrow points from the 'details' button in the Local Snapshots tab to the 'details' button in the Local Snapshots tab.

Figure: Data Protection Table View: Async DR

## Async DR Protection Domain Table and Detail Fields

Parameter	Description	Values
<i>Protection Domain Table Fields (upper screen)</i>		
(color coded circle)	Displays a color coded circle that indicates whether protection is active or inactive for the protection domain. There are separate colors for regular protection domains (green=active, gray=inactive) and protection domains created by vStore protect (blue=active vStore, light blue=inactive vStore). The protection domains created by vStore protect are special ones with limited administrative operations (update only).	(green, gray, blue, or light blue circle)
Name	Displays the name of the protection domain.	(name)
Remote Sites	Displays the number of remote sites configured for this protection domain.	[0-unlimited]
Entity Count	Displays the number of entities in the protection domain.	[0-unlimited]
Next Snapshot Time	Displays the date and time of the next scheduled snapshot.	[date and time No Schedule]
Snapshot Exclusive Usage	The amount of space that is reclaimed after the snapshot is deleted.	xxx [GB TB]
B/W Used (Tx)	Displays the amount of replication data transmitted from the protection domain to a remote site.	xxx [GB TB]
B/W Used (Rx)	Displays the amount of recovery data received by the protection domain from a remote site.	xxx [GB TB]
Ongoing	Displays the number of ongoing replications to this remote site.	[0-unlimited]
Pending	Displays the number of pending replications scheduled for this remote site.	[0-unlimited]
<i>Protection Domain Detail Fields (lower screen)</i>		
Name	Displays the name of the protection domain.	(name)
Mode	Displays whether protection is active or inactive for the protection domain.	[Active Inactive with color coded circle]
Next Snapshot Time	Displays the date and time of the next scheduled snapshot.	[date and time No Schedule]
VM Count	Displays the number of protected VMs in this domain.	(quantity or ID number)
Volume Group Count	Displays the number of protected volume groups in this domain.	(quantity or ID number)

Parameter	Description	Values
File Count	Displays the number of protected files (outside of a VM) in this domain. One reason to save individual files outside of a VM is to store templates or other common files that might be used when configuring VMs.	(quantity or name)
Remote Site(s)	Displays the name of the remote sites configured for the domain.	(remote site names)

## Metro Availability Tab

Clicking the **Metro Availability** tab displays information about protection domains configured for metro availability in the cluster (see [Configuring a Protection Domain \(Metro Availability\)](#) on page 274). This type of protection domain consists of a primary (active) storage container in the local cluster linked to a standby storage container of the same name on a remote site in which synchronous data replication to the remote site occurs when metro availability is enabled.

- The table at the top of the screen displays information about all the configured protection domains, and the details column (lower left) displays additional information when a protection domain is selected in the table. The following table describes the fields in the protection domain table and detail column.
- When a protection domain is selected, **Summary: protection\_domain\_name** appears below the table, and action links relevant to that protection domain appear on the right of this line. The actions vary depending on the state of the protection domain and can include one of the following:
  - Click the **Take Snapshot** link to take a snapshot of the protection domain locally and to one or more remote sites.
  - Click the **Update** link to modify the protection domain.
  - Click the **Activate** link to set a disabled protection domain to active status.
  - Click the **Disable** link to disable an active protection domain.
  - Click the **Promote** link to promote this protection domain from standby to active status. This option is available only when metro functionality is disabled on the active site. See the "Performing Site Maintenance" section in [Data Protection Guidelines \(Metro Availability\)](#) on page 271 for instructions on how to safely migrate VMs and promote a site from standby to active.
- Four tabs appear that display information about the selected protection domain (see following sections for details about each tab): **Local Snapshots**, **Metrics**, **Alerts**, **Events**.

Figure: Data Protection Table View: Metro Availability

## Metro Availability Protection Domain Table and Detail Fields

Parameter	Description	Values
<i>Protection Domain Table Fields (upper screen)</i>		
(color coded circle)	Displays a color coded circle that indicates whether the protection domain is active (dark green), standby (light green), or inactive (gray) in the metro availability configuration.	(dark green, light green, or gray circle)
Name	Displays the name of the protection domain.	(name)
Role	Displays the role of this protection domain in the metro availability configuration: <ul style="list-style-type: none"> <li>• Active means this is the active (primary) protection domain.</li> <li>• Standby means this is the standby protection domain.</li> </ul>	[Active Standby]
Metro Remote Site	Displays the name of the remote site containing the paired metro availability protection domain.	(remote site name)
Storage Container	Displays the name of the storage container configured for this protection domain.	(storage container name)
Status	Displays the status of this protection domain in the metro availability configuration: <ul style="list-style-type: none"> <li>• Enabled means metro availability is enabled currently for this protection domain.</li> <li>• Disabled means metro availability is not enabled currently for this protection domain.</li> </ul>	[Enabled Disabled]
Failure Handling	Failure handling timeout range in seconds.	10 to 30 seconds
B/W Used (Tx)	Displays the amount of replication data transmitted from the protection domain to the remote site.	xxx [GB TB]
B/W Used (Rx)	Displays the amount of replication data received by the protection domain from the remote site.	xxx [GB TB]
<i>Protection Domain Detail Fields (lower screen)</i>		
Name	Displays the name of the protection domain.	(name)
Role	Displays the role of this protection domain in the metro availability configuration: <ul style="list-style-type: none"> <li>• Active means this is the active (primary) protection domain.</li> <li>• Standby means this is the standby protection domain.</li> </ul>	[Active Standby with color coded circle]
Storage Container Name	Displays the name of the storage container configured for this protection domain.	(storage container name)
Remote Site	Displays the name of the remote site containing the paired metro availability storage container.	(remote site name)

Parameter	Description	Values
Status	Displays the status of this protection domain in the metro availability configuration: <ul style="list-style-type: none"> <li>Enabled means metro availability is enabled currently for this protection domain.</li> <li>Disabled means metro availability is not enabled currently for this protection domain.</li> </ul>	[Enabled Disabled]
Failure Handling	Failure handling timeout range in seconds.	10 to 30 seconds

## Remote Site Tab

Clicking the **Remote Site** tab displays information about remote sites available to the cluster (see [Configuring a Remote Site \(Physical Cluster\)](#) on page 317).

- The table at the top of the screen displays information about all the configured remote sites, and the details column (lower left) displays additional information when a remote site is selected in the table. The following table describes the fields in the remote site table and detail column.
- When a remote site is selected, **Summary: remote\_site\_name** appears below the table, and action links appear on the right of this line (see [Modifying a Remote Site \(Physical Cluster or Cloud\)](#) on page 322) for more information about these actions:
  - Click the **Test Connection** link to check whether the remote site is alive and accessible.
  - Click the **Update** link to update the settings for this remote site.
  - Click the **Delete** link to delete this remote site configuration.
- Five tabs appear that display information about the selected remote site (see following sections for details about each tab): **Replications**, **Remote Snapshots**, **Metrics**, **Alerts**, **Events**.

Figure: Data Protection Table View: Remote Site

## Remote Site Table and Detail Fields

Parameter	Description	Values
<i>Remote Site Table Fields (upper screen)</i>		
Name	Displays the name of the remote site.	(name)

Parameter	Description	Values
Remote Site Type	Displays the type of remote site.	[physical or cloud]
Remote Addresses	Displays the IP addresses of the remote site.	(IP addresses)
vStore Mappings	Displays the vStore map entries (local source storage container name and remote target storage container name) for the remote site.	( <i>local_name:remote_name</i> )
Capabilities	Displays how the remote site can be used. A value of <i>Backup</i> means the remote site is a backup (replication) target only. A value of <i>Disaster Recovery</i> means the remote site is both a backup target and a source for dynamic recovery (see <a href="#">Restoring an Entity from a Protection Domain</a> on page 265).	[Backup Disaster Recovery]
Compress on Wire	Displays whether compression is enabled for transmission to this site.	[On Off]
Use SSH Tunnel	Displays whether an SSH tunnel is enabled for secure transmission between the local cluster and the remote site.	[Yes No]
B/W Limit (Tx)	Displays the bandwidth limit set for transmissions to the remote site.	xxx [KBps]
B/W Used (Tx)	Displays the amount of replication data transmitted from protection domains to the remote site.	xxx [GB TB]
B/W Used (Rx)	Displays the amount of recovery data received by protection domains from the remote site.	xxx [GB TB]
<i>Remote Site Details Fields</i> (lower screen)		
Name	Displays the name of the remote site.	(name)
Capabilities	Displays how the remote site can be used. A value of <i>Backup</i> means the remote site is a backup (replication) target only. A value of <i>Disaster Recovery</i> means the remote site is both a backup target and a source for dynamic recovery (see <a href="#">Restoring an Entity from a Protection Domain</a> on page 265).	[Backup Disaster Recovery]
Cluster	Displays the cluster ID number.	(ID number)
Remote Address	Displays the IP addresses of the remote site.	(IP addresses)
vStore Map	Displays the configured association between the local source storage container and the remote target storage container. The entry syntax is <i>source_storage_container_name : target_storage_container_name</i> .	( <i>source_container : target_container</i> )
Max Bandwidth	Displays the bandwidth limit set for transmissions to the remote site.	xxx [KBps]
Compression on Wire	Displays whether compression is enabled for transmission to this site.	[On Off]

Parameter	Description	Values
Proxy Enabled	Displays whether a proxy is enabled, which allows specified addresses to be used as a proxy to communicate with other Nutanix components on the remote site.	[Yes No]
Use SSH Tunnel	Displays whether an SSH tunnel is enabled for secure transmission between the local cluster and the remote site.	[Yes No]

### Cluster Summary Information

When a protection domain or remote site 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 **Data Protection Summary** column (on the left) includes two fields:
  - Remote Site(s)**. Displays the number of remote sites configured in the cluster.
  - Protection Domain(s)**. Displays the number of protection domains configured in the cluster.
- Six tabs appear that display cluster-wide information (see following sections for details about each tab): **Replications**, **Local Snapshots**, **Remote Snapshots**, **Metrics**, **Alerts**, **Events**.

### Replications Tab

The Replications tab displays information in tabular form about ongoing and pending replications in the cluster. When a protection domain is selected, it also displays tabular information about successful replications for that protection domain. The following information is displayed:

- Direction** (ongoing and successful tables only). Displays the direction (incoming or outgoing) of the replication, this is whether the replication is coming in from a remote site to the cluster or going out from the cluster to a remote site.
- Protection Domain** (ongoing and pending tables only). Displays the name of the protection domain being replicated.
- Remote Site**. Displays the names of the target remote sites for this replication.
- Snapshot [ID]**. Displays the snapshot ID number assigned to this replication.
- Start Time** (ongoing and successful tables only). Displays the time when the replication started.
- Create Time** (pending table only). Displays the time when the pending replication is scheduled to start.
- Time Remaining**. Displays the approximate time remaining to complete the replication.
- End Time** (successful table only). Displays the time when the replication completed successfully.
- Data Completed** (ongoing table only). Displays the amount of data replicated successfully as replication progresses (xxx KB|MB|TB).

Replications	Local Snapshots	Remote Snapshots	Metrics	Alerts	Events																																			
<b>Total Ongoing (7)</b>																																								
<table border="1"> <thead> <tr> <th>DIRECTION</th><th>PROTECTION DOMAIN</th><th>REMOTE SITE</th><th>SNAPSHOT</th><th>START TIME</th><th>TIME REMAINING</th><th>DATA COMPLETED</th></tr> </thead> <tbody> <tr> <td>Outgoing</td><td>FIVE</td><td>tendulkar</td><td>11468903</td><td>02/08, 11:38:05am</td><td>2h 15m</td><td>181 MB</td></tr> <tr> <td>Outgoing</td><td>SIX</td><td>jordan</td><td>11468982</td><td>02/08, 11:38:13am</td><td>8h 8m</td><td>31.71 MB</td></tr> <tr> <td>Incoming</td><td>ONE_PD</td><td>jordan</td><td>jordan:1606095</td><td>02/08, 11:31:02am</td><td>8m 56s</td><td>1.69 GB</td></tr> <tr> <td>Incoming</td><td>FOUR</td><td>tendulkar</td><td>tendulkar:2337166</td><td>02/08, 11:30:05am</td><td>24m 45s</td><td>2.85 GB</td></tr> </tbody> </table>						DIRECTION	PROTECTION DOMAIN	REMOTE SITE	SNAPSHOT	START TIME	TIME REMAINING	DATA COMPLETED	Outgoing	FIVE	tendulkar	11468903	02/08, 11:38:05am	2h 15m	181 MB	Outgoing	SIX	jordan	11468982	02/08, 11:38:13am	8h 8m	31.71 MB	Incoming	ONE_PD	jordan	jordan:1606095	02/08, 11:31:02am	8m 56s	1.69 GB	Incoming	FOUR	tendulkar	tendulkar:2337166	02/08, 11:30:05am	24m 45s	2.85 GB
DIRECTION	PROTECTION DOMAIN	REMOTE SITE	SNAPSHOT	START TIME	TIME REMAINING	DATA COMPLETED																																		
Outgoing	FIVE	tendulkar	11468903	02/08, 11:38:05am	2h 15m	181 MB																																		
Outgoing	SIX	jordan	11468982	02/08, 11:38:13am	8h 8m	31.71 MB																																		
Incoming	ONE_PD	jordan	jordan:1606095	02/08, 11:31:02am	8m 56s	1.69 GB																																		
Incoming	FOUR	tendulkar	tendulkar:2337166	02/08, 11:30:05am	24m 45s	2.85 GB																																		
<b>Total Pending (1)</b>																																								
<table border="1"> <thead> <tr> <th>PROTECTION DOMAIN</th><th>REMOTE SITE</th><th>SNAPSHOT</th><th>CREATE TIME</th></tr> </thead> <tbody> <tr> <td>AWSCloudConnect</td><td>MarkNCloudProtect</td><td>11428766</td><td>02/08, 10:58:01am</td></tr> </tbody> </table>						PROTECTION DOMAIN	REMOTE SITE	SNAPSHOT	CREATE TIME	AWSCloudConnect	MarkNCloudProtect	11428766	02/08, 10:58:01am																											
PROTECTION DOMAIN	REMOTE SITE	SNAPSHOT	CREATE TIME																																					
AWSCloudConnect	MarkNCloudProtect	11428766	02/08, 10:58:01am																																					

Figure: Data Protection Table View: Replications Tab

## Entities Tab

The entities tab, which appears only when a protection domain is selected, displays the following information about entities (VMs and volume groups) in the selected protection domain:

- **Name.** Displays the name of the entity.
- **Type.** Displays the type of entity.
- **Consistency Group.** Displays the name of the consistency group in which the entity is assigned.
- **Powerstate on Recovery.** Displays the power setting that will be started after recovering the entity.

NAME	TYPE	CONSISTENCY GROUP	POWER STATE ON RECOVERY	
cerebro_clone_Windows_2012R2_ServerCore_Clone	Virtual Machine	cerebro_clone_Windows_2012R2_ServerCore_Clone	power state at time of snapshot	Unprotect
Windows_2012R2_ServerCore_Clone	Virtual Machine	Windows_2012R2_ServerCore_Clone	power state at time of snapshot	Unprotect
Windows_2012R2_ServerCore_Clone_NGT_installed	Virtual Machine	Windows_2012R2_ServerCore_Clone_NGT_installed	power state at time of snapshot	Unprotect

Figure: Data Protection Table View: VMs Tab

## Schedules Tab

The Schedules tab, which appears only when a protection domain is selected, displays backup schedule information in tabular form. The following information is displayed:

- **Type.** Displays the schedule type, which indicates the interval metric (minutes, hours, days) used to set the schedule.
- **Repeat On.** Displays when to start the next backup run, such as every 60 minutes (when the type is set to minutes).
- **Start Date.** Displays the time when the first run is to start (or did start).
- **End Date.** Displays when the schedule is disabled, that is the latest date a backup run should start because of this schedule. A dash (-) indicates the backup schedule should continue indefinitely (no end date).
- **Retention Policy.** Displays how many snapshots from this schedule to keep locally and on remote sites (if configured).
- Click the pencil icon (far right) to update a schedule; click the X icon to delete a schedule. See the [Modifying a Protection Domain \(Async DR\)](#) on page 262 for more information.

▲ TYPE	REPEAT ON	START DATE	END DATE	RETENTION POLICY	
Minutely	Every 300 minutes	05/23/14, 12:51:00pm	-	Local: 1	
Minutely	Every 200 minutes	05/23/14, 12:51:00pm	-	Local: 1, worm: 156	
Minutely	Every 200 minutes	05/23/14, 12:51:00pm	-	Local: 1	
Minutely	Every 60 minutes	05/23/14, 11:22:00am	-	Local: 1, worm: 60	

Figure: Data Protection Table View: Schedules Tab

## Local Snapshots Tab

The Local Snapshots tab displays information in tabular form about snapshots stored locally. (This tab does not appear when a remote site is selected.) The following information is displayed:

- **ID.** Displays the snapshot identification number.
- **Create Time.** Displays the time when the snapshot was created.
- **Reclaimable Space.** Displays the total space that can be recovered after the snapshot is deleted.
- **Expiry Time.** Displays the date and time when the snapshots are about to expire.
- **VM Recovery.** Displays whether the snapshot that is present on the local cluster is recoverable or not. Click **Recovery Details** link for more information.
- Use the links in the far right column to do the following:
  - Click the **Details** link to display information about the VMs backed up in the snapshot.
  - Click the **Restore** link to restore one or more VMs from this snapshot (see *Restoring an Entity from a Protection Domain* on page 265).
  - Click the X icon to delete the snapshot.



**Note:** You must delete the protection domain to delete all the snapshots in the protection domain. Deleting the schedules alone is not sufficient. If you do not delete the protection domain, but delete all the snapshots, a reference snapshot is kept to allow for delta replication in future.

Data Protection Table View: Local Snapshots Tab					
Replications		Entities	Schedules	Local Snapshots	
				Remote Snapshots Metrics Alerts Events	
ID	CREATE TIME	RECLAIMABLE SPACE	EXPIRY TIME	VM RECOVERY	
chuckd:461062	01/12/2016, 03:57:36 PM	0	01/13/2016, 03:57:37 PM	Recovery Details	Details - Restore - X
chuckd:350904	01/12/2016, 03:46:49 PM	0	01/13/2016, 03:46:50 PM	Recovery Details	Details - Restore - X

Figure: Data Protection Table View: Local Snapshots Tab

## Remote Snapshots Tab

The Remote Snapshots tab displays information in tabular form about snapshots stored on remote sites. The following information is displayed:

- **ID.** Displays the snapshot identification number.
- **Create Time.** Displays the time when the snapshot was created.
- **Location.** Displays the name of the remote site on which the snapshot is stored.
- **Usage.** Displays the size of the snapshot (xxx MB|GB|TB).
- **Expiry Time.** Displays the date and time when the snapshots are about to expire.
- **VM Recovery.** Displays whether the snapshot that is present on the remote cluster is recoverable on the local cluster or not. Click **Recovery Details** link for more information.
- Use the links in the far right column to do the following:
  - Click the **Details** link to display information about the VMs backed up in the snapshot.
  - Click the **Retrieve** link to copy (replicate) the snapshot from the remote site to the local cluster.
  - Click the X icon to delete the snapshot.



**Note:** You must delete the protection domain to delete all the snapshots in the protection domain. Deleting the schedules alone is not sufficient. If you do not delete the protection domain, but delete all the snapshots, a reference snapshot is kept to allow for delta replication in future.

Replications	Entities	Schedules	Local Snapshots	Remote Snapshots	Metrics	Alerts	Events
<input type="checkbox"/>	ID	CREATE TIME	LOCATION	EXPIRY TIME	VM RECOVERY		
<input type="checkbox"/>	chuckd:461062	01/12/2016, 03:57:36 PM	chuckd	01/13/2016, 03:57:36 PM	Recovery Details	Details - Retrieve -	
<input type="checkbox"/>	chuckd:350904	01/12/2016, 03:46:49 PM	chuckd	01/13/2016, 03:46:49 PM	Recovery Details	Details - Retrieve -	
<input type="checkbox"/>	22627:1450867413451914:2182987	01/12/2016, 03:31:05 PM	chuckd	01/13/2016, 03:31:07 PM	Recovery Details	Details - Retrieve -	
<input type="checkbox"/>	22627:1450867413451914:2173530	01/12/2016, 03:27:45 PM	chuckd	01/13/2016, 03:27:46 PM	Recovery Details	Details - Retrieve -	

Figure: Data Protection Table View: Remote Snapshots Tab

## Metrics Tab

The Metrics tab displays two graphs of replication data transmissions during a rolling time interval:

- **Bandwidth Tx.** Displays the amount of replication data transmitted from protection domains in the cluster to remote sites.
- **Bandwidth Rx.** Displays the amount of recovery data received by protection domains in the cluster from remote sites.
- For more in depth analysis, you can add either of these charts to the analysis page by clicking the blue link in the upper right of the chart (see [Analysis Dashboard](#) on page 401).

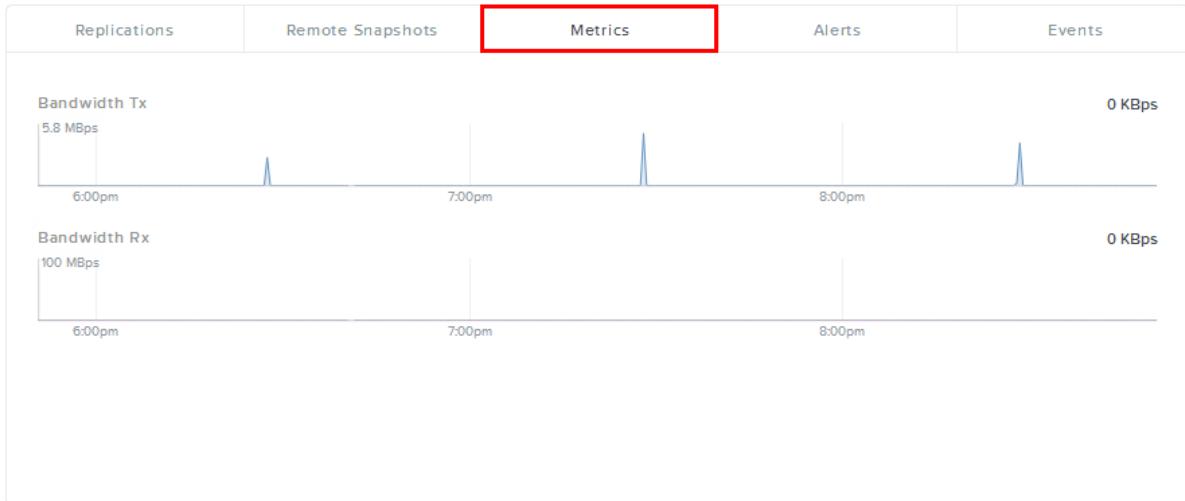


Figure: Data Protection Table View: Metrics Tab

## Alerts Tab

The Alerts tab displays the unresolved alert messages about protection domains or remote sites in the same form as the Alerts page (see [Alert Messages View](#) on page 411). You can click the drop-down button to retrieve the alerts according to severity, resolution, and duration.

Replications	Local Snapshots	Remote Snapshots	Metrics	Alerts	Events
<input type="checkbox"/>	SEVERITY	ISSUE	TIMESTAMP	ENTITIES	DOCUMENTATION
<input type="checkbox"/>	Info	The replication for protection domain pd1 to remote site toucan-dirst was a full replication.	01-13-16, 11:25:46am	Remote site, Protection domain	Cause: Resolution
<input type="checkbox"/>	Critical	No network mapping specified for remote site toucan-dirst.	01-13-16, 11:23:46am	Remote site	Cause: Resolution
<input type="checkbox"/>	Warning	Vss is enabled but Nutanix Guest Tools are not installed on the guest VM(s) restored_Windows_7_FLR protected by W7_FLR_P0.	01-09-16, 08:51:41pm	Protection domain	Cause: Resolution
<input type="checkbox"/>	Info	The replication for protection domain PD_NGT_L_DISK to remote site toucan was a full replication.	01-09-16, 02:33:56am	Remote site, Protection domain	Cause: Resolution
<input type="checkbox"/>	Critical	No network mapping specified for remote site toucan.	01-08-16, 09:53:27am	Remote site	Cause: Resolution
<input type="checkbox"/>	Info	The replication for protection domain FLR_PD_Base_VM to remote site toucan was a full replication.	01-08-16, 08:07:09am	Remote site, Protection domain	Cause: Resolution

Figure: Data Protection Table View: Alerts Tab

## Events Tab

The Events tab displays the unacknowledged event messages about protection domains or remote sites in the same form as the Events page (see [Event Messages View](#) on page 413). Click the **Include Acknowledged** button to also display acknowledged events.

	MESSAGE	ENTITIES	MODIFIED BY	TIMESTAMP
<input type="checkbox"/>	Replication started for Protection Domain 'ONE_1400869261847' to remote 'worm' using snapshot '(795, 1400630012940088, 16406402)' at time '1401240145261762'.	Protection domain, Remote site	05-27-14, 06:22:25pm	
<input type="checkbox"/>	Snapshot '(795, 1400630012940088, 16406402)' created for protection domain 'ONE_1400869261847'.	Protection domain	05-27-14, 06:22:25pm	
<input type="checkbox"/>	Replication started for Protection Domain 'ONE_1400869261847' to remote 'worm' using snapshot '(795, 1400630012940088, 16401746)' at time '1401236548464796'.	Protection domain, Remote site	05-27-14, 05:22:28pm	

Figure: Data Protection Table View: Events Tab

## Async DR Protection Domain Configuration

You configure a standard (Async DR) protection domain by defining a group of entities (VMs and volume groups) that are backed up locally on a cluster and optionally replicated to one or more remote sites (see [Configuring a Protection Domain \(Async DR\)](#) on page 256).

### Data Protection Guidelines (Async DR)

Follow these protection domain best practices, and be aware of these limitations.

#### General Guidelines

- For VM migration as part of data replication to succeed in an ESXi hypervisor environment, ensure that you configure forward (DNS A) and reverse (DNS PTR) DNS entries for each ESXi management host on the DNS servers used by the Nutanix cluster. The **Hardware** page on the web console shows the host name and hypervisor IP address for each management host. The nCLI command `ncli host ls` also lists each hypervisor's IP address
- If you need encryption of data replication, set up an encrypted site-to-site tunnel and specify the tunnel IP address when you create the remote site (by specifying the tunnel IP address in the **Addresses** parameter).
- If bandwidth between sites is limited, set a limit on the bandwidth that replication uses (by specifying the **Maximum Bandwidth** parameter).
- A consistency group is a subset of the entities in a protection domain. Consistency group typically should not exceed more than 5 to 10 entities.
- One-time snapshots have infinite expiry time and hence it is recommended to specify retention time when you are creating one-time snapshots.
- Do not include the source and the destination cluster under the same datacenter because VMs might get deleted from both the source and destination clusters post the migration process.

- If you are using the same vCenter Server to manage both the primary and remote sites, do not have the storage containers with the same name on both the sites.
- Do not have VMs with the same name on the primary and the secondary clusters. Otherwise, it may affect the recovery procedures.
- If you take snapshot of the VM from the vCenter Server and then at the same time, while the snapshot creation from vCenter Server is in progress, initiated a snapshot of the protection domain that has the same VM from the Prism, sometimes the VM restored from snapshot taken from Prism may fail to power on and `files not found` error message is displayed. Hence it is recommended to not to take both the snapshots at the same time.
- To protect VMs created by VMware View Composer or Citrix XenDesktop, Nutanix recommends adding files associated with the VM gold image to a protection domain. Use the nCLI command to create the protection domain. For example, to protect the `replica-ABC.vmdk` file in a protection domain named `vmware1-pd` and a consistency group named `vmware1-cg`:

```
ncli> protection-domain protect \
  files=/container1/view-gold-image/replica-ABC.vmdk name=vmware1-pd cg-name=vmware1-cg
```



**Note:** You must disable the VMware View pool from the View Composer. For more information about disabling View Pool from the View Composer, see *VMware View documentation*.

- If you are deploying an intrusion prevention system (IPS) appliance or software, consider whether any configured filters or other network monitoring aides could block packets transferred during replication operations. You can add the IP address of any appliances or systems running the software to the whitelist as described in *Configuring a Filesystem Whitelist* in the *Web Console Guide*.
- (Hyper-V) It is recommended to create a VM in their unique folders instead of using a default folder. If a default folder is used to create the VMs, you will not be able to protect these VMs.

## Best Practices for Application-Consistent Snapshots

- When you configure a protection domain and select **Use application consistent snapshots**, the Nutanix cluster transparently invokes the Volume Shadow Copy Service (VSS; also known as Shadow Copy or Volume Snapshot Service). This option creates an application-consistent snapshot for a VM and is limited to consistency groups consisting of a single VM.
- **Note:** This option is available for ESXi and AHV only; it is not supported for Hyper-V. However, a third-party product could be used to invoke VSS when the hypervisor is Hyper-V.
- Nutanix recommends to install NGT on the VM for which you are planning to take application-consistent snapshots. For installing and configuring NGT and its requirements and limitations, see *Nutanix Guest Tools* on page 390. As part of this mechanism, 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.



**Note:**

- Nutanix VSS snapshots of the VMs with delta, SATA, and IDE disks are not supported.
- Nutanix VSS snapshots fails if the VM has any iSCSI attachments.
- Nutanix VSS snapshots of UEFI VMs on AHV are not supported.

- Application-consistent snapshots are only supported for Microsoft SQL Server 2008 and 2012 versions.
- The following table provides a detailed information on whether a snapshot will be application consistent or not depending on the operating systems and hypervisors running in your environment.

## Application-Consistent Snapshots

	ESXi		AHV	
	NGT Status	Result	NGT Status	Result
Microsoft Windows Server Edition	Installed and Active. Also pre_freeze and post_thaw scripts are present	Nutanix script-based VSS snapshots	Installed and Active. Also pre_freeze and post_thaw scripts are present	Nutanix script-based VSS snapshots
	Installed and Active	Nutanix VSS-enabled snapshots.	Installed and Active	Nutanix VSS-enabled snapshots
	Not enabled	Hypervisor-based application-consistent or crash-consistent snapshots.	Not enabled	Crash-consistent snapshots
Microsoft Windows Client Edition	Installed and Active. Also pre_freeze and post_thaw scripts are present	Nutanix script-based VSS snapshots	Installed and Active. Also pre_freeze and post_thaw scripts are present	Nutanix script-based VSS snapshots
	Not enabled	Hypervisor-based snapshots or crash-consistent snapshots.	Not enabled	Crash-consistent snapshots
Linux VMs	Installed and Active. Also pre_freeze and post_thaw scripts are present	Nutanix script-based VSS snapshots	Installed and Active. Also pre_freeze and post_thaw scripts are present	Nutanix script-based VSS snapshots
	Not enabled	Hypervisor-based snapshots or crash-consistent snapshots.	Not enabled	Crash-consistent snapshots



### Note:

- Installed and Active means that the VM has NGT installed, has VSS capability is enabled, is powered on, and is actively communicating with the Controller VM.
- Hypervisor-based snapshots are taken only when you have VMware tools running on the VM and the VM does not have any independent disks attached to it. If these requirements are not met, crash-consistent snapshot is taken.
- The consistency group and schedule setting determines whether an application-consistent snapshots or crash-consistent snapshots are taken. See the Snapshot Consistency table to get more information on snapshot consistency.
- The pre\_freeze and post\_thaw scripts can be Python or shell scripts or any executable files for Linux and batch files for Windows. These scripts should contain commands specific to

the particular applications that are running on the Linux or Windows VMs. Backup vendors like CommVault can provide these scripts. You can also write your own scripts. See the [Pre\\_Freeze and Post\\_Thaw Script Guidelines](#) on page 255 for more information.

- In AHV: If you receive a non-zero return code from the pre\_freeze script, a non-application consistent snapshot will be taken and an alert is raised on the Prism web console. If you receive a non-zero return code from the post\_thaw script, application-consistent snapshot will be tried again once and if that fails, a non-application consistent snapshot will be taken and an alert is raised on the Prism web console.
- Nutanix recommends that you consider your VM workload type before selecting this option. For example, you may enable this option for VMs running database applications or similar workload types.
- Applications running in these environments must be able to quiesce I/O operations.
- Nutanix recommends to not take Nutanix-enabled application-consistent snapshots while using any third-party backup provider enabled VSS snapshots (for example, Veeam).
- You must configure one consistency group for each VM. That is, each consistency group must consist of one VM. If the consistency group includes more than one VM, the application-consistent snapshot feature is ignored.
- (vSphere) If you enable application-consistent snapshots, a Nutanix native snapshot as well as a single vSphere host-based snapshot is also created (which is then deleted).
- For protection of VAAI clones with application consistency, each VAAI clone should be in its own protection domain.
- The snapshot consistency (whether a snapshot will be application consistent or crash consistent) is dependent on whether or not you have selected **Create application consistent snapshot** check box while creation of the consistency group and creation of the schedules. The rules are as follows.

### Snapshot Consistency

Consistency Group Setting	Schedule Setting	Result
Checked	Unchecked	Crash-consistent snapshot is taken.
Checked	Checked	Application-consistent snapshot is taken.
Unchecked	Unchecked	Crash-consistent snapshot is taken.
Unchecked	Checked	Crash-consistent snapshot is taken.

### Limitations

General limitations for Async DR are as follows.

- Protection domains can have no more than 200 entities (VMs or volume groups). It is recommended that each application which constitutes set of entities is protected by a unique protection domain.
- Because restoring a VM does not allow for VMX editing, VM characteristics such as MAC addresses may be in conflict with other VMs in the cluster.
- To be in a protection domain, a VM must be entirely on Nutanix datastore (no external storage).
- Data replication between sites relies on the connection for encryption.
- It is not possible to make snapshots of entire filesystems or storage containers.
- The shortest possible snapshot frequency is once per hour.
- Consistency groups cannot define boot ordering.

- Inactivating a protection domain deletes the entities from the cluster. Deleting a protection domain removes all the snapshots associated with the protection domain from the cluster. Hence, do not deactivate and then delete a protection domain that contains VMs. Either delete the protection domain without deactivating it, or remove the VMs from the protection domain before deleting it.



**Caution:** If you deactivate and then delete a protection domain that contains VMs, the VMs in the protection domain gets deleted.

- Some VMs might not appear in the web console or in nCLI command results during rolling upgrades, planned Controller VM maintenance, or when hosts are down or unavailable. Some protection domain operations like snapshots or protection might also fail in this case.
- The following limitations apply to the inclusion of related entities in a protection domain:
  - If the number of entities in a consistency group exceeds ten, protection of related entities fails. However, if you want to include more than ten entities in a protection domain, protect the entities in separate consistency groups within the same protection domain. Even if two related entities are in separate consistency groups, as long as they are in the same protection domain, their attachment configuration is included in the snapshots and restored during recovery.
  - Snapshot creation and recovery of attachments are not supported if you have configured volume groups with the following:
    - Challenge-Handshake Authentication Protocol (CHAP). The iSCSI target secret is cleared after a volume group is restored from a snapshot.
    - IP addresses. If you attach volume groups to VMs by whitelisting the IP addresses of the VMs, entities are recovered, but their attachment configuration is not recovered. You must manually reattach the entities after recovery.
  - Supported Operating Systems*

Microsoft Windows Server 2008 R2 and Microsoft Windows Server 2012 R2

Red Hat Enterprise Linux 6.7 and 6.8

Oracle Linux 6.7 and 7.2

Limitations specific to vSphere environment are as follows.

- Nutanix native snapshots cannot be used to protect VMs on which VMware fault tolerance is enabled.

Limitations specific to Hyper-V environment are as follows.

- A disaster replication snapshot fails and raises an alert if:
  - Any VM files (for example, configuration, snapshots, virtual disks, and ISOs) are residing on non-Nutanix storage containers
  - All virtual disks associated with a VM are located in different directories or folders. That is, all virtual disks associated with a VM must be located in a single directory or folder.
  - A VM's folder and its snapshot folder are located in different directory/folder paths. That is, a snapshot folder is typically located in a snapshot folder under the VM's folder. The snapshot folder must be under the VM folder or the replication fails.
- Run-as account must be a domain account and must have local administrator privileges on the Nutanix hosts. This can be a domain administrator account. When the Nutanix hosts are joined to the domain, the domain administrator accounts automatically takes administrator privileges on the host. If the domain account used as the run-as account in SCVMM is not a domain administrator account, you need to manually add it to the list of local administrators on each host by running sconfig.
- Nutanix does not support Hyper-V replica VM in the Async DR protection domain.
- The name of the Hyper-V virtual switches between primary and remote site should be same, otherwise restore fails.
- If the base VM and the differencing disk is in the same protection domain, after migrating to the protection domain to the secondary site in-place restore fails.

Limitations specific to volume groups are as follows.

- You cannot include volume groups in a protection domain that is configured for metro availability.
- You cannot include volume groups in a protected vStore.
- You cannot include volume groups in a consistency group that is configured for application-consistent snapshotting.
- Volume group protection is disabled when a cluster is upgrading to 4.6. All nodes in the cluster must be on AOS 4.6 for volume groups to be protected.
- Volume group replication and protection fail if a remote site is running an AOS release that does not support volume groups or disaster recovery for volume groups.
- When configuring volume group protection in the nCLI, you must specify volume group UUIDs. You cannot specify volume group names.
- Volume groups must be manually reattached to VMs and other iSCSI initiators after failover, fallback, migration, or in-place restore events.

#### **Pre\_Freeze and Post\_Thaw Script Guidelines**

The pre\_freeze and post\_thaw scripts can be Python or shell scripts or any executable files. These scripts should contain commands specific to the particular applications that are running on the Linux or Windows VMs. Backup vendors like CommVault can provide these scripts. You can also write your own scripts. Following are some of guidelines and samples for pre\_freeze and post\_thaw scripts.

#### **Location**

- For Windows VMs, create pre\_freeze.bat and post\_thaw.bat scripts under *system\_drive:\Program Files\Nutanix\scripts\pre\_freeze.bat* and *system\_drive:\Program Files\Nutanix\scripts\post\_thaw.bat*. For example, if your system\_drive is C, create these scripts at *C:\Program Files\Nutanix\scripts\pre\_freeze.bat* and *C:\Program Files\Nutanix\scripts\post\_thaw.bat*.
- For the Linux VMs on AOS 5.1 or later releases running NGT 1.1 version, you must create the pre\_freeze /usr/local/sbin/pre\_freeze and post\_thaw /usr/local/sbin/post\_thaw scripts with owner root:root and 700 permissions.



**Note:** If you are using NGT 1.0 version, you must create the pre\_freeze sbin/pre\_freeze and post\_thaw sbin/post\_thaw scripts with owner root:root and 700 permissions.

The pre\_freeze script is executed before creating the snapshot and post\_thaw script is executed after the snapshot creation. If the pre\_freeze or post\_thaw scripts are not present or the permissions are incorrect then VSS gets disabled and crash-consistent snapshots are taken. The pre\_freeze and post\_thaw scripts can be Python or shell scripts or any executable files. These scripts should contain commands specific to the particular applications that are running on the Linux VMs. Backup vendors like CommVault can provide these scripts. You can also write your own scripts. The pre\_freeze script should finish within 50 seconds and post\_thaw script should finish within 25 seconds.

#### **Requirements**

- For Windows VMs, the administrator should have read and execute permissions on the scripts.
- For Windows Server operating systems if scripts are present, pre\_freeze script is executed first, then the VSS quiesce is performed, and then post\_thaw script is executed.
- For Linux VMs, the scripts should have 700 permissions and should be owned by root:root.
- Both pre\_freeze and post\_thaw scripts should be present for the operation to complete successfully.
- Timeout for both the scripts is 60 seconds.
- Return code of 0 from the script is considered as a success. Otherwise, it implies that the script execution has failed.
- If pre\_freeze script executes, irrespective of its success or failure post\_thaw script is executed.

## Sample Pre\_Freeze and Post\_Thaw Scripts

Sample pre\_freeze and post\_thaw scripts for MySQL on Linux are as follows.

```
#!/bin/sh
#pre_freeze-script
date >> '/scripts/pre_root.log'
echo -e "\n attempting to run pre_freeze script for MySQL as root user\n" >> /scripts/
pre_root.log
if [ "$(id -u)" -eq "0" ]; then
python '/scripts/quiesce.py' &
echo -e "\n executing query flush tables with read lock to quiesce the database\n" >> /
scripts/pre_freeze.log
echo -e "\n Database is in quiesce mode now\n" >> /scripts/pre_freeze.log
else
date >> '/scripts/pre_root.log'
echo -e "not root user\n" >> '/scripts/pre_root.log'
fi

#!/bin/sh
#post_thaw-script
date >> '/scripts/post_root.log'
echo -e "\n attempting to run post_thaw script for MySQL as root user\n" >> /scripts/
post_root.log
if [ "$(id -u)" -eq "0" ]; then
python '/scripts/unquiesce.py'
else
date >> '/scripts/post_root.log'
echo -e "not root user\n" >> '/scripts/post_root.log'
fi
```

Sample pre\_freeze and post\_thaw for Windows are as follows.

```
echo -e "\n attempting to run pre_freeze script for myapplication \n"
python '/scripts/quiesce.py' &
echo -e "\n the pre_freeze script executed successfully for myapplication \n"

echo -e "\n attempting to run post_thaw script for myapplication \n" >>
python '/scripts/unquiesce.py'
echo -e "the post_thaw script executed successfully \n"
```

## Configuring a Protection Domain (Async DR)

This procedure creates a protection domain that supports backup snapshots for entities (selected VMs and volume groups) through asynchronous data replication.

### Before you begin:

- Ensure that you have met the protection domain guidelines for configuring Async DR before proceeding, [Data Protection Guidelines \(Async DR\)](#) on page 250.
- See the *DR practices guide* for guidance to set up DR in your environment, [DR Best Practices](#).

To configure a standard (async DR) protection domain, do the following:



**Note:** To create a protection domain that supports a metro availability configuration through synchronous data replication, see [Configuring a Protection Domain \(Metro Availability\)](#) on page 274.

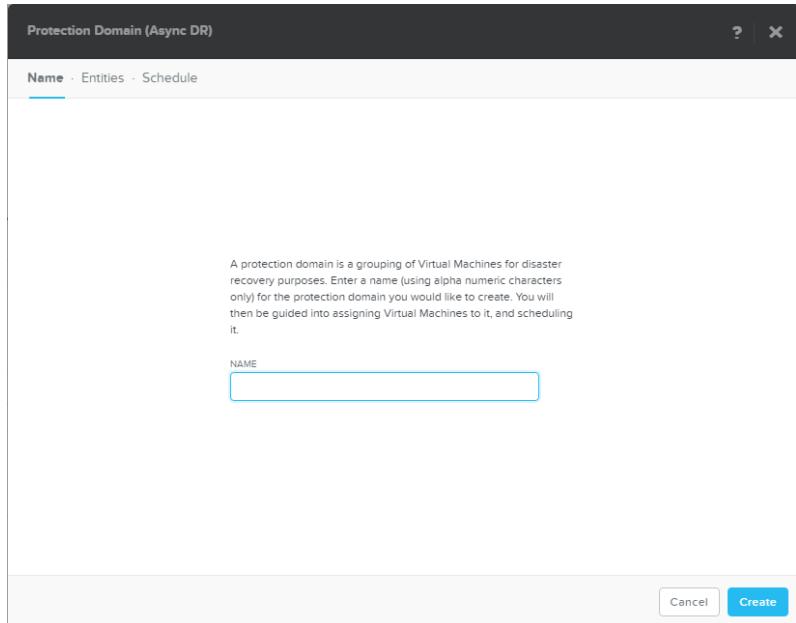


**Note:**

- For Acropolis File Services (AFS), protection domain operations are not available during file server operations.

- Asynchronous data replication (Async DR) is supported between Nutanix NX/SX Series and Dell XC Series clusters and between Nutanix NX/SX Series and Lenovo HX Series clusters.

- In the Data Protection dashboard (see [Data Protection Dashboard](#) on page 237), click the **Protection Domain** button and select **Async DR** from the drop-down list.  
The *Protection Domain* window appears.



*Figure: Protection Domain (Async DR): Create Screen*

- Enter a name for the protection domain on the first screen and then click **Create**.

Clicking the **Create** button immediately creates the protection domain (even if you do not continue to the next step).

**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), Simplified Chinese, decimal digits (0-9), dots (.), hyphens (-), and underscores (\_).

**Note:** In your environment if you have more than one primary and secondary clusters, ensure that the names of the protection domain are unique for each pair of clusters.

The Entities display appears. This display is divided into two sections for unprotected entities (left side) and protected entities (right side).

- Do the following in the indicated fields:

- Check the boxes next to the entities you want in a consistency group from the list of unprotected entities on the left. You can filter the list by entering an entity or host name in the **Filter By:** fields above the list.

A consistency group is a subset of the entities in a protection domain that are treated as a single group and backed up collectively in a snapshot. Protection domains can have multiple consistency groups. You can protect a maximum of 200 entities (VMs or volume groups) within any number of consistency groups (up to 200) in a single protection domain.

- If there are additional entities you want in this consistency group that are already protected, check the boxes next to those entities in the list of protected entities on the right, and then click the **Unprotect Selected Entities** button at the bottom of the column to move them into the unprotected entities list.

- c. Select a consistency group (in the left column) for the checked entities. Click the **Use Entity Name** button to create a new consistency group for each checked entity with the same name as that entity, click the **Use an existing CG** button and select a consistency group from the pull-down list to add the checked entities to that consistency group, or click the **Create a new CG** button and enter a name in the field to create a new consistency group with that name for all the checked entities.



**Note:** Only one entity is allowed in a consistency group if the hypervisor is Hyper-V, so always click **Use Entity Name** for Hyper-V. (Multiple entities are allowed in a consistency group for ESXi or AHV.)

- d. [ESXi and AHV only] Check the **Use application consistent snapshots** box to ensure that application consistency is maintained in the snapshots.

This option invokes VSS to create an application-consistent snapshot for a VM and is limited to consistency groups with just a single VM.



**Note:**

- This option is available for ESXi and AHV only; it does not appear when the hypervisor is Hyper-V.
- For AHV, you must install NGT on the VM for which you are planning to take Nutanix VSS-based application-consistent snapshots. See [Nutanix Guest Tools](#) on page 390 for more information.
- For ESXi, you can take application-consistent snapshots without installing NGT on the VMs, but these snapshots will be hypervisor based and leads to VM stuns (temporary unresponsive VMs).

See [Data Protection Guidelines \(Async DR\)](#) on page 250 for application-consistent snapshot rules, best practices, and snapshot consistency (whether a snapshot will be application consistent or crash consistent).

This box is ignored if there are multiple VMs in the consistency group. Therefore, check this box only if you have selected just one VM (and **Use VM Name** or **Create a new CG**) or selected multiple VMs and the **Use VM Name** button to create a separate consistency group for each of those VMs.

You cannot create application-consistent snapshots of volume groups.

- e. Click **Auto protect related entities** if you want to include all related entities in the consistency group.

By default, the check box is selected. If you choose to leave the check box selected when you add entities to the Protected Entities list, all related entities are also added. All protected entities are included in the same consistency group and snapshots of the related entities are created for subsequent recovery. Additionally, the attachment configuration of all related entities is included in the snapshot so that you do not have to reattach entities again after using the snapshot for recovery.

If you choose to clear the check box when adding entities for protection, only the entities that you select are included in the protection domain.

If you choose to protect only a subset of the related entities, the selected entities are protected, but their attachment configuration is not captured, and you must manually reattach the entities after recovery. If the entities you excluded need to be included at a later time, update the protection domain and add those entities.

For a description of what the term *related entities* means, see [Data Protection Concepts](#) on page 236. For requirements and limitations to the inclusion of related entities and supporting operating systems, see [Data Protection Guidelines \(Async DR\)](#) on page 250.

- f. Click the **Protect Selected Entities** button at the bottom of the column to move the selected entities into the Protected entities column.

- g. Repeat this step as desired to create additional consistency groups for the remaining unchecked entities (or as many of them as you want in the protection domain).
- h. When all desired consistency groups have been created, click the **Next** button (lower right).

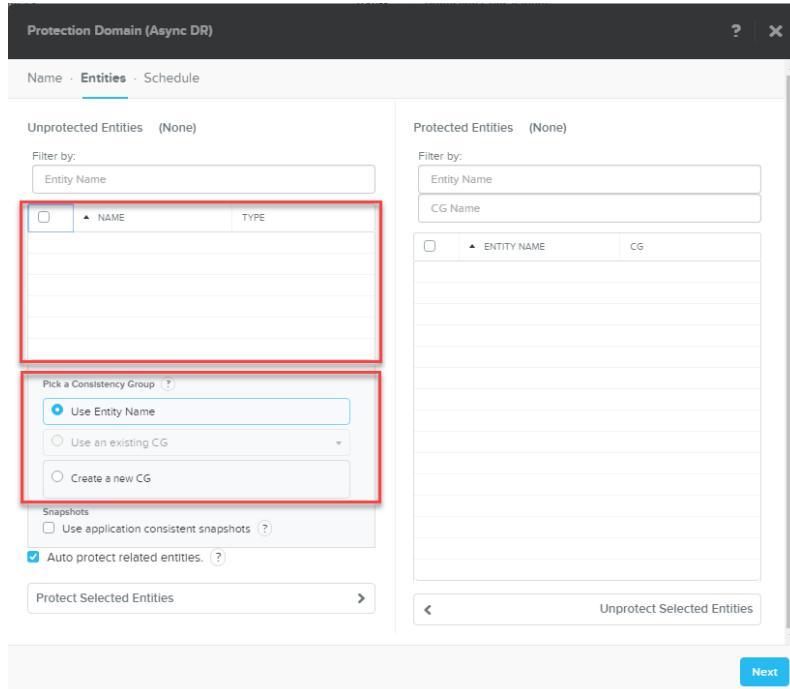


Figure: Protection Domain (Async DR): Virtual Machines Screen

The Schedule screen appears. There are no default backup schedules for a protection domain. All schedules must be defined by the user.

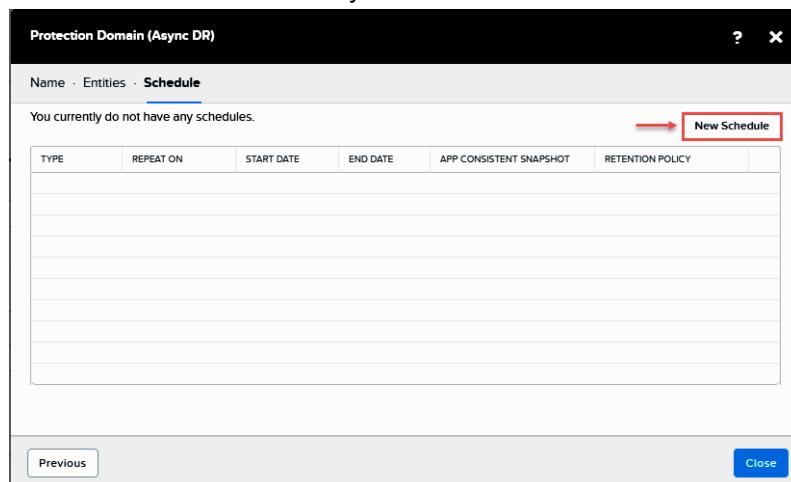


Figure: Protection Domain (Async DR): Schedule Screen (initial)

4. To create a schedule, click the **New Schedule** button to display the create schedule screen and then do the following in the indicated fields:
  - a. **Repeat every ## [minutes|hours|days]**: Click the appropriate circle for minutes, hours, or days and then enter the desired number in the box for the scheduled time interval.  
The interval cannot be less than an hour, so the minutes value must be at least 60.
  - b. **Occur [weekly|monthly]**: Select which days the schedule should run.

- If you select weekly, check the boxes for the days of the week the schedule should run.
- If you select monthly, enter one or more integers (in a comma separated list) to indicate which days in the month to run the schedule. For example, to run the schedule on the first, tenth, and twentieth days, enter "1,10,20".

c. **Start on:** Enter the start date and time in the indicated fields.

The default value is the current date and time. Enter a new date if you want to delay the schedule from starting immediately.



**Note:** A storage container-level protection domain requires a system metadata scan (Curator process) to populate the file list. In some cases, this scan might take a few hours. Any snapshots started before the scan completes do not contain any data.

d. **End on:** To specify an end date, check the box and then enter the end date and time in the indicated fields.

The schedule does not have an end date by default, and it runs indefinitely unless you enter an end date here.

e. **Retention Policy:** Enter how many intervals of snapshots that you want to retain.

For example, if you enter 1 in the retention policy check box and select one of the following:

- For **Repeat every minutes/hours/days** option: Total of only 1 snapshot is retained.
- For **Repeat weekly/monthly** option: Total of 1 for each period/occurrence is retained. Suppose if you select Occur weekly with Monday, Tuesday, Friday, a total of 3 snapshots are retained.
- Enter the number to save locally in the **Local** line "**keep the last xx snapshots**" field. The default is 1.
- A separate line appears for each configured remote site. To replicate to a remote site, check the remote site box and then enter the number of snapshots to save on that site in the appropriate field. Only previously configured remote sites appear in this list (see *Configuring a Remote Site (Physical Cluster)* on page 317).
- The snapshots that are saved are equal to the value that you have entered in the **keep the last ## snapshots** field + 1. For example, if you have entered the value **keep the last ## snapshots** field as 20, a total of 21 snapshots are saved. When the next (22nd) snapshot is taken, the oldest snapshot is deleted and replaced by the new snapshot.

f. Select the **Create application consistent snapshot** check box to make the snapshots that are created as part of the new schedule application consistent.

You can use this option to control the time when an application-consistent snapshot should be created. If you already have an application-consistent snapshots attached to a protection domain from a previous version, after upgrading to the new version the same schedules are marked as application consistent. For more information about application-consistent snapshot rules, best practices, and snapshot consistency (whether a snapshot will be application consistent or crash consistent), see *Data Protection Guidelines (Async DR)* on page 250.

g. When all the field entries are correct, click the **Create Schedule** button.

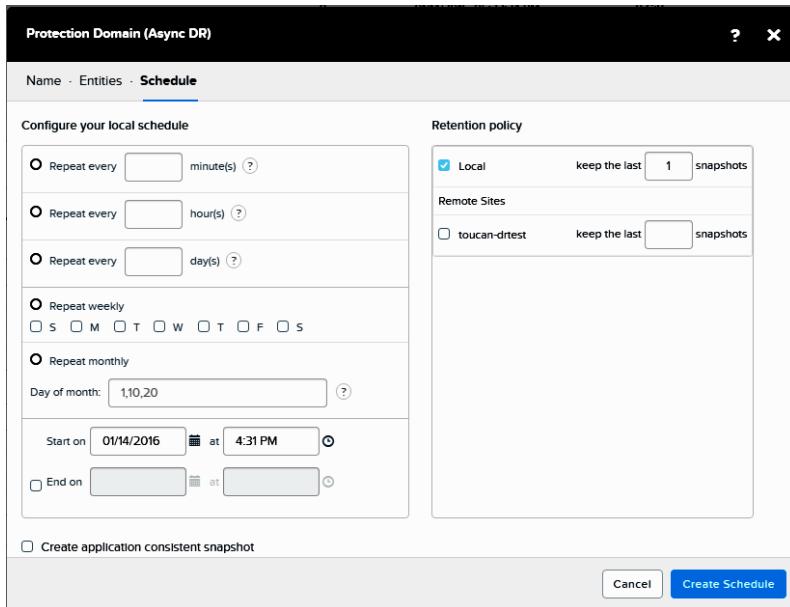


Figure: Protection Domain (Async DR): Schedule Screen (configure)

This returns you to the Schedules screen.

- Click the **New Schedule** button to create another schedule, update or delete the schedule you just created, or click the **Close** button to close the window.

**Note:**

- Replications can fall behind if too many schedules have the same start time. Therefore, it is recommended that start times be staggered across schedules.
- If you delete a schedule, the snapshots that were taken when the schedule was active does not get deleted.

The screenshot shows the 'Schedule' screen with two scheduled entries in a table:

TYPE	REPEAT ON	START DATE	END DATE	APP CONSISTENT SNAPSHOT	RETENTION POLICY
Hourly	Every 1 hour	09/08/15, 03:46:00pm	-	No	Local: 2, colossus08: 3
Hourly	Every 1 hour	09/09/15, 02:33:00pm	-	Yes	Local: 1, aster: 2

At the top right is a 'New Schedule' button. At the bottom right are 'Update' and 'Delete' buttons. Navigation buttons 'Previous' and 'Close' are at the bottom left and right respectively.

Figure: Protection Domain (Async DR): Schedule Screen (populated)

**Results:** Information about the new protection domain appears in the Data Protection dashboard (see [Data Protection Table View](#) on page 239).

## Modifying a Protection Domain (Async DR)

You can modify an existing protection domain (see [Configuring a Protection Domain \(Async DR\)](#) on page 256) by changing the domain mode (active/inactive), replicating the domain, migrating the domain, updating the domain settings, or deleting the domain. To modify a protection domain in one or more of these ways, do the following:

1. In the Data Protection dashboard (see [Data Protection Dashboard](#) on page 237), click the **Table** view.
2. Click the **Async DR** tab and select the target domain line in the table (top section of screen).

The Summary line (middle of screen) displays the domain name with a set of relevant action links on the right. The possible actions are **Activate** (not shown), **Take Snapshot**, **Migrate**, **Update**, and **Delete**. The following steps describe how to perform each action.

Name	Status	Entity Count	Next Snapshot Time	Snapshots Exclusive Usage	RW Used (%)	RW Used (MB)	Reads	Writes
None	Inactive	0	09/14/2016, 05:23:34 PM	0.6GB	0 %	0 Kilobytes	0	0
pdl	Source-standby	0	09/14/2016, 05:32:09 PM	-	-	0 Kilobytes	0	0

Figure: Protection Domain Action Links

3. To change the protection domain mode from inactive to active, click the **Activate** action link. This action is typically taken to recover from a site disaster (see [Failing Over a Protection Domain](#) on page 267). An active protection domain cannot be deactivated through the web console, but you can deactivate it through the nCLI. When a protection domain is inactive, backups (scheduled snapshots) in that protection domain are disabled.
4. To create a snapshot (point-in-time backup) of the protection domain locally and to one or more remote sites, click the **Take Snapshot** action link.

The *Replicate Protection Domain* dialog box appears. Do the following in the indicated fields:

- a. **Local:** Do nothing in this field.

The box is checked by default to indicate a local snapshot is always created. If no remote site is checked, the snapshot is saved locally only. If one or more remote sites are checked, the snapshot is saved locally and at the specified remote sites.

- b. **Remote sites:** Check the box(es) of the target remote sites.



**Note:** If no remote site is checked, the snapshot is saved locally only.

- c. **Replication start time:** Select the start time from the pull-down list.

Choices range from now to 48 hours from now.

- d. **Retention time:** Select the retention interval (how long the snapshot is saved on the remote sites) from the pull-down list.

Choices range from one day to indefinitely.

- e. Select the **Create application consistent snapshot** check box to make the snapshots application consistent.

For more information on application consistent snapshot, see [Data Protection Guidelines \(Async DR\)](#) on page 250.

- f. When all the field entries are correct, click the **Save** button.

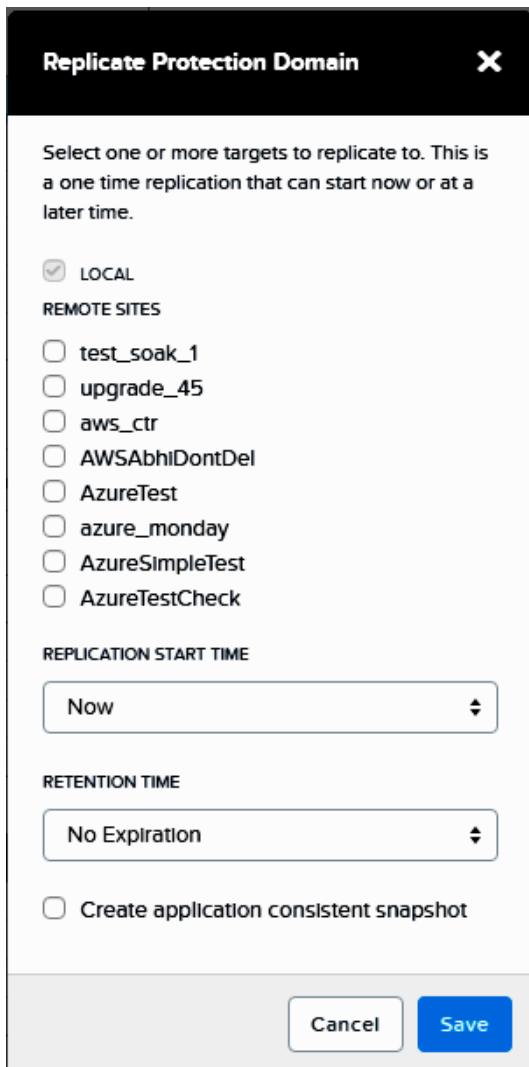


Figure: Replicate Protection Domain Dialog Box

5. To migrate the protection domain to a remote site, click the **Migrate** action link. See the "Migration (Planned) Failover" section of [Failing Over a Protection Domain](#) on page 267 for instructions on how to migrate a protection domain.
6. To update the protection domain settings, click the **Update** action link. Update the displayed screens as desired and then click the **Save** button.  
The *Update Protection Domain* dialog box appears, which redisplays the Entities and Schedule screens that appear when creating the protection domain (see [Configuring a Protection Domain \(Async DR\)](#) on page 256).

 **Note:** If you are adding entities to an existing consistency group, make sure to click the **Use an existing CG** option, and then select the consistency group from the list.
7. To delete the protection domain, click the **Delete** action link. A window prompt appears; click the **OK** button to delete the protection domain.  
The deleted protection domain disappears from the list of domains in the table.



**Caution:** Do not delete an inactivated protection domain that contains entities. If you do so, the entities in the protection domain are deleted. Either keep the protection domain activated before deleting it, or remove the entities from the protection domain.

## Restoration of Protected Entities

### In-Place and Out-of-Place Restore

You can perform either an in-place restore or an out-of-place restore of a protected entity. In-place restoration processes detach entities, and you must manually reconfigure the attachment after the restoration is complete. The steps that you need to perform after restoration depend on which hypervisor is installed on the host.

Consider that you rewrite an entity in a protection domain that contains VMs and volume groups, and the volume groups are attached to the VMs. The following table describes the possible scenarios, results, and steps to perform after restoration:

#### Steps to Perform After Restoring Protected Entities

Scenario	Result	Follow-Up Steps
VMware ESXi and Microsoft Hyper-V		
You overwrite one or more of the VMs in the protection domain.	Volume groups are not detached from the restored VMs, but follow-up steps are required. Other VMs attached to the volume groups are not affected.	Log on to the restored VMs and configure the in-guest iSCSI attachments.
You overwrite a volume group.	The volume group is detached from all VMs.	Log on to all the VMs to which the volume group was attached and configure in-guest iSCSI attachments.
AHV		
You overwrite one or more of the VMs in the protection domain.	Volume groups are detached from the restored VMs. Other VMs attached to the volume groups are not affected.	Log on to the web console and reattach the volume groups to the VMs. Alternatively, log on to the VMs and configure in-guest iSCSI attachments.
You overwrite a volume group.	The volume group is detached from all VMs.	Log on to the web console and reattach the volume groups to the VMs. Alternatively, log on to the VMs and configure in-guest iSCSI attachments.

Out-of-place restoration processes do not detach the existing entities, but the new entities are created without attachments, and any desired attachments must be manually reconfigured. For example, if a VM and a volume group in a protection domain are restored to a different location, the existing volume group remains attached to the VM, but the new VM and volume group are not attached to each other. You must manually attach the volume group to the VM.

For information about attaching volume groups to VMs, see [Volume Group Configuration](#) on page 143

## Restoring an Entity from a Protection Domain

### Before you begin:

If you are restoring only volume groups, log on to the attached VMs, stop the applications that are using the volume groups, and take the volume group disks offline.

If a VM in the cluster fails for any reason or there is a disaster that fails multiple VMs, you can restore one or more VMs to an earlier version if those VMs are protected (see [Configuring a Protection Domain \(Async DR\)](#) on page 256). You can also restore the protected volume groups.

To restore a protected entity, do the following:

1. In the Data Protection dashboard (see [Data Protection Dashboard](#) on page 237), click the **Table** tab and then the **Async DR** tab.  
See [Data Protection Table View](#) on page 239 for screen shots and additional information about the following three steps.
2. Select the target protection domain in the table (upper screen).
3. If the desired snapshot is stored locally, skip to the next step. If it is stored on a remote site, click the **Remote Snapshots** tab, select the target snapshot from the displayed list, and then click the **Retrieve** link (and verify the request in the dialog box) to copy the snapshot from the remote site to the local cluster.
4. Click the **Local Snapshots** tab, select the target snapshot from the displayed list, and then click the **Restore** link.

The *Restore Snapshot* window appears.



**Note:** This option does not appear if you are using single-node replication target clusters.

5. Do the following in the indicated fields:

- a. **What to Restore:** Check the boxes for the entities to restore.

Clicking the box at the top selects all the entities in the list. When you select a protected entity (VM or volume group) for restoration from a snapshot, the user interface selects all related entities so that they can be restored along with the selected entity. If you want their attachment configurations to be restored automatically after recovery, you must restore all related entities. If you choose to restore only a subset of the selected entities, only the selected entities are restored. Their attachment configurations are not restored, and you must manually reattach the restored entities after recovery.

The following changes occur after related entities are restored:

- The IQN of a VM changes if the snapshot includes in-guest iSCSI attachments. A string of the form `ntnx-timestamp`, where `timestamp` is the recovery time stamp, is appended to the previous IQN. For example, if the previous IQN was `iqn.1991-04.com.an-authority:1234`, the IQN after recovery is `iqn.1991-04.com.an-authority:1234:ntnx-timestamp`.
- A VM connects to volume groups by using the data services IP address as the iSCSI target IP address. All previous iSCSI target IP addresses are cleared.
- Volume groups are attached to the new IQNs assigned to the VMs.
- After a VM starts, the Nutanix Guest Agent (NGA) on the guest VM reads updated iSCSI configuration from the Nutanix Guest Tools (NGT) CD, and it updates the configuration on the guest VM so that no manual configuration is required on the VM.

- b. **How to Restore:** Do one of the following:

- Click the **Overwrite existing entities** option to overwrite the selected entities. This powers off each selected VM, deletes the entities from the inventory, copies the entity files from the chosen snapshot to the current location, and registers the entities. The VMs are not powered on

automatically; you must start them manually. You must also manually reattach any volume groups that were attached to the VMs (see [Volume Group Configuration](#) on page 143). This operation does not affect the UUIDs of restored entities.

- Click the **Create new entities** button and then enter the desired path in the **Path** field and optional name prefix in the **VM Name Prefix** and **Volume Group Name Prefix** fields. This creates a clone of each selected entity in the path location with the same name and the specified prefix. If a prefix is not specified, the prefix Nutanix-Clone- is used. For example, if the original VM name is myvm and a prefix is not specified, the cloned VM name is Nutanix-Clone-myvm (or Nutanix-Clone-myvm-yyymmdd-hhmmss if Nutanix-Clone-myvm already exists). The VM clone is not powered on automatically; you must start it manually. You must also manually attach volume groups to the new VM (see [Volume Group Configuration](#) on page 143). This operation creates entities with new UUIDs.

**Note:**

- Entered paths are relative to the current entity location. For example, to clone the VM in NewDirectoryX, provide the path as //NewDirectoryX. Entities cannot be cloned to a different datastore.
- (ESXi only) Before restoring an entity in ESXi, ensure that you have all the storage containers mounted in the ESXi hosts. This helps in registering the newly created entity.
- (ESXi only) Snapshot recovery fails on VMs that contain split VMDK files as these files are not supported by VMware.

- When the fields are correct, click the **Restore** button.

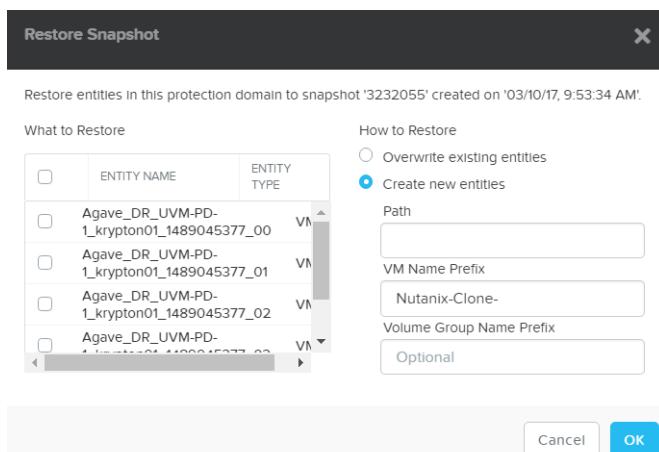


Figure: Restore Snapshot Window

#### What to do next:

If you restored only volume groups, log on to the attached VMs, bring the volume group disks back online, and start the application.



**Important:** If a VM does not connect automatically to a volume group after a clone, migrate, or activate operation, reboot the VM, discover the newly restored iSCSI target, and log in manually.

#### Protection Domain Failover and Failback (Async DR)

After a protection domain is replicated to at least one remote site, you can carry out a planned migration of the contained entities by failing over the protection domain. You can also trigger failover in the event of a site disaster.

Failover and fallback events re-create the VMs and volume groups at the other site, but the volume groups are detached from the iSCSI initiators to which they were attached before the event. After the failover or fallback event, you must manually reattach the volume groups to iSCSI initiators and rediscover the iSCSI targets from the VMs.

### Failing Over a Protection Domain

#### Migration (Planned) Failover

System maintenance or expansion might dictate moving a protection domain to another site as a planned event. To migrate a protection domain to a remote site, do the following:

1. Log into the web console for the primary site (see [Logging Into the Web Console](#) on page 29).
2. Go to the **Async DR** tab of the **Data Protection** table view (see [Data Protection Table View](#) on page 239).

NAME	REMOTE SITES	ENTITY COUNT	LAST SNAPSHOT TIME	SNAPSHOT EXCLUSIVE USE	BW USED (K)	BW USED (K)	ONLINE	PEND
pd1	toucan-drtest	0	02/06/2016, 05:23:34 PM	0 GB	0 Kbps	0 Kbps	0	0
PD_Win_01_FLR	toucan-drtest	2	02/06/2016, 05:31:00 PM	2.47 GB	0 Kbps	0 Kbps	0	0
test	toucan-drtest	0	02/06/2016, 05:21:00 PM	0 GB	0 Kbps	0 Kbps	0	0
ONE	toucan-drtest	0	-	195.42 GB	0 Kbps	0 Kbps	0	0
TWO	toucan-drtest	0	-	196.45 GB	0 Kbps	0 Kbps	0	0
WAK_FLR	toucan-drtest	0	-	65.22 GB	0 Kbps	0 Kbps	0	0

Figure: Migrating a Protection Domain

3. Select the target protection domain and click the **Migrate** action link.

The *Migrate Protection Domain* dialog box appears. Select the site where you want to migrate the protection domain. The VMs that are part of the protection domain, but cannot be recovered on the remote site are also displayed. Click **Learn more** for additional information.

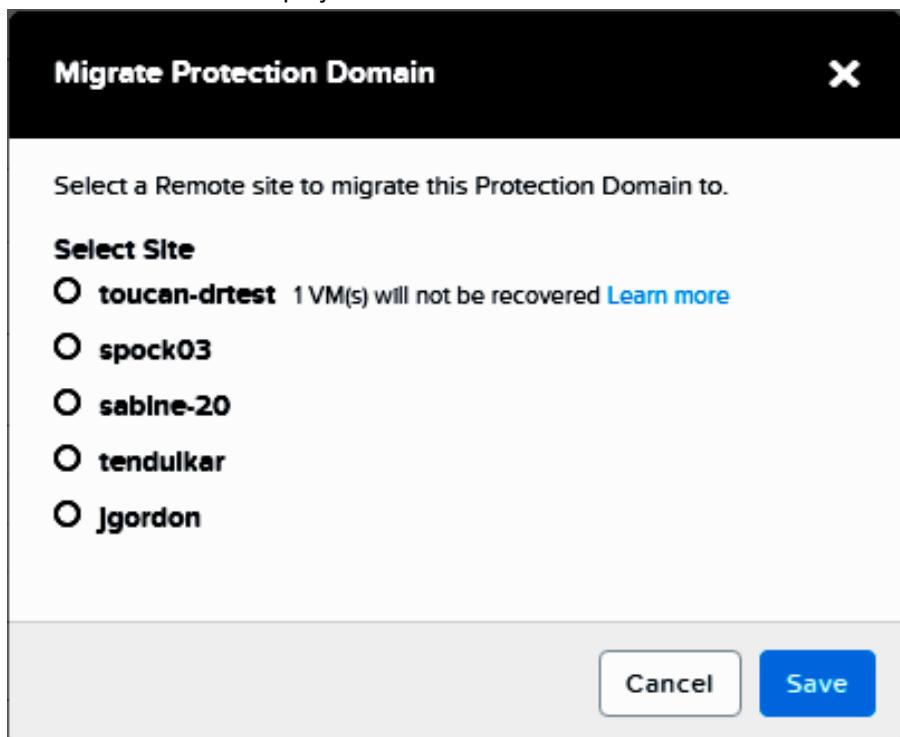


Figure: Migrate Protection Domain Dialog Box

4. When the field entries are correct, click the **Save** button.

Migrating a protection domain does the following:

- Creates and replicates a snapshot of the protection domain.
- Powers off the VMs on the local site.



**Note:** The data protection service waits for 5 minutes for the VM to shutdown. If the VM does not get shutdown within 5 minutes, it is automatically powered off.

- Creates and replicates another snapshot of the protection domain.
- Registers all VMs and volume groups and removes their associated files.
- Marks the local site protection domain as inactive.
- Restores all VM and volume group files from the last snapshot and registers them with new UUIDs at the remote site.
- Marks the remote site protection domain as active.



**Note:** (Hyper-V) If VMs are registered with Microsoft Failover Cluster, you need to manually re-register these VMs with the Microsoft Failover Cluster after the Async DR is completed.

The VMs on the remote site are not powered on automatically. This allows you to resolve any potential network configuration issues, such as IP address conflicts, before powering on the VMs. Additionally, you must manually reattach the volume groups that were affected by the migration or restore operation, perform in-guest iSCSI attachment. If you use the nCLI for attaching volume groups, note that the UUIDs of volume groups change when they are restored at the remote site, and so do their iSCSI target names, which contain the volume group UUID. See [Volume Group Configuration](#) on page 143.

### Disaster (Unplanned) Failover

When a site disaster occurs, do the following to fail over a protection domain to a remote site:

- Log into the web console for the target remote site (see [Logging Into the Web Console](#) on page 29).
- Go to the **Async DR** tab of the **Data Protection** table view (see [Data Protection Table View](#) on page 239).
- Select the target protection domain and click the **Activate** button. A window prompt appears; click the **Yes** button.

This operation does the following:

- Restores all VM and volume group files from the last fully-replicated snapshot.

The process first detaches the volume groups that are included in the protection domain or attached to the VMs in the protection domain.

- Registers the VMs and volume groups on the recovery site.
- Marks the failover site protection domain as active.



**Note:** (Hyper-V) If VMs are registered with Microsoft Failover Cluster, you need to manually re-register these VMs with the Microsoft Failover Cluster after the Async DR is completed.

The VMs are not powered on automatically. This allows you to resolve any potential network configuration issues, such as IP address conflicts, before powering on the VMs. Additionally, you must manually reattach the volume groups that were affected by the migration or restore operation, perform in-guest discovery of the volume groups as iSCSI targets, and log in to the targets. If you use the nCLI for attaching volume groups, note that the UUIDs of volume groups change when they are restored at the remote site, and so do their iSCSI target names, which contain the volume group UUID. See [Volume Group Configuration](#) on page 143.

The screenshot shows the NetApp Prism Web Console interface. At the top, there's a navigation bar with 'healey' and other options like 'Data Prot...', 'Heartbeat', and 'Alerts'. Below the navigation is a search bar and user info ('admin'). The main area has tabs for 'Overview' and 'Table'. Under 'Table', there are three tabs: 'Async DR' (which is selected), 'Metro Availability', and 'Remote Site'. The 'Async DR' tab displays a table of protection domains. One row for 'Bogota' is highlighted. At the bottom of the table, there's a summary section for 'Bogota' with tabs for 'PROTECTION DOMAIN DETAILS', 'Replications', 'VMs', 'Schedules', 'Local Snap...', 'Remote Sna...', 'Metrics', 'Alerts', and 'Events'. The 'Replications' tab is active. In the 'PROTECTION DOMAIN DETAILS' section, 'Name' is Bogota and 'Mode' is Inactive. The 'Replications' section shows 'Total Ongoing (0)' with columns for DIRECTION, PROTECTION DOMAIN, REMOTE SITE, SNAPSHOT, START TIME, and DATA COMPLETED.

Figure: Activating a Protection Domain

### Failing Back a Protection Domain

Perform the following steps to failback a protection domain from remote site to primary site.

1. Login to the Web console of the remote site. The site where the protection domain is currently active.
2. From the **Async DR** tab under Data Protection, select the protection domain that you want to failback.
3. Click **Migrate**.  
The *Migrate Protection Domain* dialog box appears. Select the site where you want to migrate the protection domain. The VMs that are part of the protection domain, but cannot be recovered on the remote site are also displayed. Click **Learn more** for additional information.
4. When the field entries are correct, click the **Save** button.

**What to do next:** Manually reattach the volume groups that were affected by the migration or restore operation. Note that the UUIDs of volume groups change when they are restored at the remote site, and so do their iSCSI target names, which contain the volume group UUID.

### Failing Back a Protection Domain (Unplanned)

If an unplanned failure occurs on the primary site, all the entities are failed over to the remote site. After the primary site gets restored, you can failback the entities to the primary site.

1. Log into the vCenter Server of the primary site.  
All the hosts are down.
2. Power on all the hosts of the primary site.
  - Controller VMs get automatically restarted and the cluster configuration is established again.
  - All the protection domains that were active before the disaster occurred gets recreated in an active state. However, you cannot replicate the protection domains to the remote site since the protection domains are still active at the remote site.
  - The user VMs get powered on.
3. Log on to one of the Controller VMs at the primary site and deactivate and destroy the VMs by using the following hidden nCLI command. Execute this command only when the protection domain is active on the secondary site as executing this command deletes the VMs from the primary site.

```
ncli> pd deactivate-and-destroy-vms name=protection_domain_name
```

Replace *protection\_domain\_name* with the name of the protection domain that you want to deactivate and destroy.



**Caution:** Do not use this command for any other workflow. Otherwise, it will delete the VMs and data loss will occur.

VMs get deleted from the primary site and the protection domain is no longer active on the primary site. Remove the orphaned VMs from the inventory of the primary site.

4. (Optional) If you want to schedule frequent replications, log into the remote site and schedule replication to the primary site.
5. Log into the remote site and click **Migrate** to migrate the protection domain to the primary site. The VMs get unregistered from the secondary site (not removed) and data gets replicated to the primary site, and then the VMs gets registered on the primary site. Protection domain starts replicating from the primary site to the remote site based on the schedule that was originally configured on the primary site.
6. Power on the VMs in the correct sequence and configure the IP address again (if required). Additionally, manually reattach any volume groups that were either included in the protection domain or attached to the VMs in the protection domain. You can start using the VMs from the primary site.
7. Remove the orphaned VMs from the inventory of the secondary site.

## Metro Availability Protection Domain Configuration

You configure a metro availability protection domain by specifying an active storage container in the local cluster and linking it to a standby storage container with the same name on a remote site in which synchronous data replication occurs when metro availability is enabled.

Nutanix native replication infrastructure provides flexible options to backup and restore VMs from snapshots (see [Protection Strategies](#) on page 233). In addition, Nutanix offers a metro availability option that is a policy applied on a datastore, which effectively spans the datastore across two sites. This is accomplished by pairing a storage container on the local cluster with one on a remote site and then synchronously replicating data between the local (active) and remote (standby) storage containers. When metro availability is enabled, everything in the active storage container is replicated synchronously to the remote storage container. Metro availability configurations can include VMs, but they cannot include volume groups.

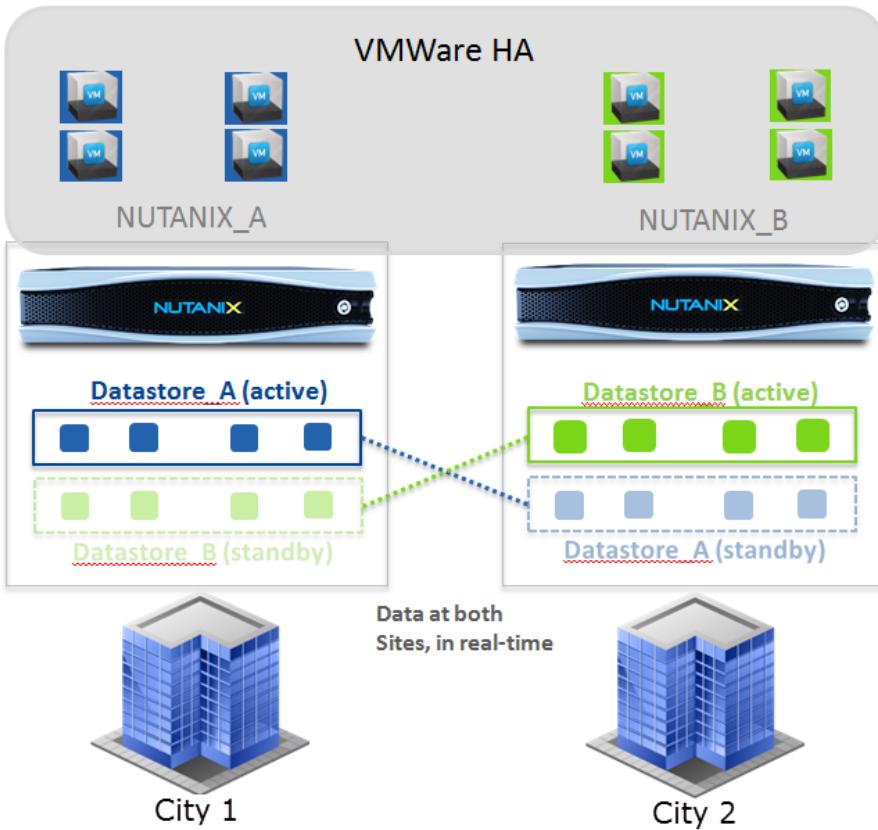


**Note:** After you enable metro availability, the cluster no longer automatically takes a backup snapshot of the storage container at the secondary site, as this snapshot can consume a large amount of storage. This snapshot was previously intended to protect pre-existing data on that storage container.

Metro availability minimizes application downtime due to unplanned failure events like site disasters and planned events such as site maintenance. A metro availability policy for a storage container interoperates seamlessly with the compression data management policy.



**Note:** Metro availability is only supported on the ESXi hypervisor.



*Figure: Metro Availability Example*

## Data Protection Guidelines (Metro Availability)

### General Guidelines for Applying a Metro Availability Policy

A protection domain is created by specifying a primary storage container on the local cluster and a standby storage container of the same name on a remote cluster. Following are settings and guidelines for applying metro availability.

- When a storage container is used with metro availability, the datastore name must be the same as the storage container name.
- Ensuring datastore availability across two sites requires data to be present at both sites in real-time. Therefore, it is required that the round trip latency between clusters be less than 5 ms. Maintain adequate bandwidth to accommodate peak writes. It is recommended that you have a redundant physical network between the sites.
- Ensure that all virtual disks associated with a given VM reside on a container enabled for metro availability.
- Protected VMs can run on either the Nutanix cluster associated with the active storage container or the cluster associated with the standby storage container. However, when VMs are running on the cluster associated with the standby storage container, reads and writes occur over the wire to the active storage container. Therefore, it is recommended the VMs should run locally to the active container on which the data of the VMs is residing to reduce network traffic and associated network latency.
- Metro availability policies apply per storage container (not cluster), so a cluster can be active for one datastore and standby for another. For example, consider a cluster configuration with an Oracle datastore (Datastore A) in storage container 1 and an Exchange datastore (Datastore B) in storage container 2. Cluster A can be active for Datastore A with Cluster B the standby, while Cluster B can be

- active for the Datastore B with Cluster A the standby. In addition, metro availability storage containers can co-exist with regular storage containers in the same cluster.
- Communication between the two Metro clusters happens over the following ports and, therefore, requires that these ports be open from all Controller VM IP addresses in Cluster A to all Controller VM IP addresses in Cluster B:
  - TCP 2009
  - TCP 2020

#### *Cluster Configuration Settings*

- Cluster models can be different between primary and secondary sites.
- vMotion may require Enhanced vMotion Compatibility (EVC) feature.
- Cluster resource sizes can be different.
- Redundancy factor can be different across clusters.

#### *Container Configuration Settings*

- Compression settings for a container can be different.
- Redundancy factor settings for a container can be different.

#### *Remote Site Configuration Guidelines*

- Do not enable a proxy on remote sites that you use with a metro availability protection domain.
- Set up the remote site clusters using the virtual IP address of the remote site.
- Ensure that you have redundant remote replication links between the clusters.
- Enable remote site compression in bandwidth-limited environments.
- When linked clones are in a metro availability storage container, the gold image must reside in the same storage container.
- Linked cloned VMs must have host affinities to either primary site or secondary site. The linked cloned VMs must always be registered on the same site as their root VM.
- If you upgrade to AOS 4.6 or later releases, it is recommended to re-establish metro availability between primary and secondary sites to get the seamless vMotion benefits across failovers. If your VMs are running on the secondary site and if you have to promote the secondary site for any unexpected event, there is no need to restart the VMs on the secondary site because the secondary site will handle IO requests directly. To achieve this, you can perform following steps.
  - Take a snapshot of the protection domain. This snapshot helps with efficient re-synchronization.
  - Disable the metro availability configuration.
  - Re-enable metro availability in the same direction.

#### **vSphere Configuration Guidelines**

- VMware network port group names should be identical between the VMware hosts in each Nutanix cluster.
- Configure the hosts in the two Nutanix clusters as a single VMware HA cluster in the vCenter Server. This provides high availability protection for VMs across the Nutanix clusters.
- For metro availability configuration, Nutanix recommends to use an empty container. However, if SIOC is enabled on a container (which is enabled by default), you must disable SIOC and also delete all the files from the container that are related to SIOC. For more information on disabling SIOC on a container, see *vSphere Administration Guide*.

#### *vCenter Server Configuration and Guideline*

- A single vCenter Server instance should manage the VMware cluster(s) between the sites. It is recommended to maintain the vCenter server in a third site to allow cluster management regardless of the site failure.
- Metro availability can also protect and replicate the vCenter Server if the third site is not available.

### *DRS Affinity Settings*

- Configure DRS affinity rules such that VMs are not migrated to hosts on a cluster that owns the standby container.
- Use **Should** affinity rules to allow automated VM restart on the nodes owning the standby datastore.
- Use **Must** affinity rules if you do not want automated VM restart against the standby datastore.
- Manually modify the **Must** rules to allow VMs to restart against blocked hosts. Modifying rules assumes the availability of the vCenter Server.

### *VMware HA Settings*

- Change the VM restart priority of all Controller VMs to **Disabled**.
- Change the host isolation response of all Controller VMs to **Leave Powered On**.



**Note:** For user VMs, it is recommended to change the VM restart priority and host isolation response settings to **Disabled**.

- Change the VM monitoring setting for all the Controller VMs to **Disabled**.
- Configure VMware HA admission control based on the cluster configuration. For example, assuming you have a balanced configuration, you can set **Percentage of cluster resources reserved as failover spare capacity** setting to 50 percent or lower. This setting ensures that enough resources exist in a single Nutanix cluster to support both sites.

### *Datastore Monitoring Settings*

- During the configuration of datastore, select **Select only from my preferred datastores** option and select the datastores that is used for metro availability.
- If the VMware cluster has only one datastore, add the advanced option `das.ignoreInsufficientHbDatastore=true`

## **System Maximums**

### **Maximum Limits for Metro Availability**

<b>Component</b>	<b>Limit</b>
Maximum number of files for all the entities in a protected container	3600
Maximum number of files for all the entities in a consistency group	1200
Maximum number of files for all the entities on a remote container	50000 (because of snapshots)
Maximum number of protection domains supported in a metro availability pair configured with a Metro Availability Witness	50

### **Guidelines to Stop a Cluster**

If you are planning to stop your cluster for any maintenance related activities, perform the following before you run `cluster stop` command.

- For the protection domains which are active on this cluster, perform a planned failover. For more information, see [Failing Over a Protection Domain Manually \(Planned Failover\)](#) on page 301.

- For the protection domains which are standby on the container of cluster, perform a disable operation on the remote site that is configured in the metro availability configuration.

## Limitations

- Before enabling metro availability on a container with VMs in an async DR protection domain, delete the async DR protection domain.
- Latency on vDisks might increase during the synchronization between two clusters.
- For protection domains in metro availability configuration, restoring snapshots of the protection domain with overwrite is not a supported workflow.
- Symbolic links and hard links are not supported.
- VMs cannot be hosted on the secondary cluster during the metro enable operation for the same container.
- VMs cannot be hosted on the primary cluster during promote of the secondary site for the same container.

See the *Acropolis Release Notes* for additional limitations and workarounds related to metro availability.

## Configuring a Protection Domain (Metro Availability)

This procedure describes how to create a protection domain that supports synchronous data protection for a metro availability configuration.

**Before you begin:** Ensure that you have met the protection domain guidelines for configuring metro availability before proceeding, [Data Protection Guidelines \(Metro Availability\)](#) on page 271.



**Note:** Metro Availability are now supported across different hardware vendors (NX/SX, Dell, or Lenovo). You can also establish a Metro Availability relationship between Nutanix NX/SX Series and other non-NX clusters (Dell or Lenovo). However, mixing of NX and non-NX nodes in the same cluster are not supported.

To configure a protection domain for metro availability, do the following:

- In the *Data Protection* dashboard (see [Data Protection Dashboard](#) on page 237), click the **Protection Domain** button and select **Metro Availability** from the drop-down list.  
The *Protection Domain (Metro Availability)* window appears.
- In the *Name* screen, enter a name for the protection domain and then click the **Next** button (lower right).
- In the *Storage Containers* screen, select (click the option for) the target storage container and then click the **Next** button.

The screen displays a list of existing storage containers in the cluster. The selected storage container will be the primary storage container in a metro availability pair.



### Note:

- You cannot select multiple storage containers. Create a separate protection domain for each storage container you want to protect. If the desired storage container does not appear in the list, click the **Cancel** button, create the storage container (see [Creating a Storage Container](#) on page 139), and then restart this procedure.
- The Nutanix native backup snapshots are supported for VMs in a metro availability storage container. These snapshots are crash consistent. Restoration of such snapshots results in restoring the files that constitutes the VMs. However, unless SRM is used, you need to manually register these VMs on the hosts.
- See the *Maximum Limits for Metro Availability* table in [Data Protection Guidelines \(Metro Availability\)](#) on page 271 topic to get more information on limits before proceeding.

The screenshot shows the 'Protection Domain (Metro Availability)' interface. The 'Storage Containers' tab is selected. The table lists the following storage containers:

NAME	CAPACITY	REMAINING SPACE
NutanixManagementShare	6.36 TiB	6.36 TiB
nuteset_ctrl	6.45 TiB	6.36 TiB
她都挂_ctrl	6.36 TiB	6.36 TiB
Arbab_container	6.4 TiB	6.36 TiB
default-container-30323	6.36 TiB	6.36 TiB
pran-ctr	7.08 TiB	6.36 TiB

At the bottom right of the screen are 'Cancel' and 'Next' buttons.

Figure: Protection Domain (Metro Availability): Storage Containers Screen

- In the *Remote Sites* screen, select the target storage container in the *Compatible Remote Sites* section and then click the **Next** button.

The screen is broken into the following two sections:

- Compatible Remote Sites* (upper screen). This section lists all storage containers on remote sites that could be used as the standby storage container in a metro availability pair. The storage container must have the same name as the primary storage container selected in the previous step. In this example, the `second_stretch_container` was selected as the primary storage container, and a storage container with the same name appears in the `italy` remote site.



**Note:** Make sure the target standby storage container does not contain any data. A storage container must be empty before you can select it as the standby in a metro availability pair.

- Incompatible Remote Sites* (lower screen). This section lists remote sites that are incompatible as a standby site. For a remote site to be compatible, it must first be set up to support metro availability, have a storage container with the same name, and have a transmission latency between the clusters of less than 5 ms. Remote sites that do not satisfy all three requirements cannot be used as the standby site.

*Figure: Protection Domain (Metro Availability): Remote Sites Screen*

5. In the *Failure Handling* screen, select the failure handling mode (manually or automatically) when a network or other problem interrupts the connection between clusters.
  - (Recommended) Selecting the **Witness** option means the Witness VM can automatically distinguish a site failure from a network interruption between the metro availability sites and decide whether to failover in case of a site failure or network interruption.
  - Note: You must configure a Witness VM to use this option (see [Metro Availability Witness Option](#) on page 283).
  - Selecting the **Automatic Resume** option means VM writes resume automatically after 30 seconds. This option supports VM availability at the cost of storage container consistency between the clusters.
  - Selecting the **Manual** option means VM writes does not resume until a user disables metro availability manually or the problem is resolved. This option supports storage container consistency between the clusters at the cost of VM availability.

*Figure: Protection Domain (Metro Availability): Failure Handling Screen*

6. Create a schedule:

Protection Domain (Metro Availability) ? | X

Name · Storage Containers · Remote Sites · Failure Handling · **Schedule** · Review

Configure your local schedule

<input type="radio"/> Repeat every <input type="text"/> minute(s)	<a href="#">?</a>
<input type="radio"/> Repeat every <input type="text"/> hour(s)	<a href="#">?</a>
<input type="radio"/> Repeat every <input type="text"/> day(s)	<a href="#">?</a>
<input type="radio"/> Repeat weekly	
<input type="checkbox"/> S <input type="checkbox"/> M <input type="checkbox"/> T <input type="checkbox"/> W <input type="checkbox"/> F <input type="checkbox"/> S	
<input type="radio"/> Repeat monthly	
Day of month: <input type="text" value="1,10,20"/>	<a href="#">?</a>
Start on <input type="text" value="10/18/2016"/> <a href="#">Calendar</a> at <input type="text" value="11:49 AM"/> <a href="#">Clock</a>	
<input type="checkbox"/> End on <input type="text"/> <a href="#">Calendar</a> at <input type="text"/> <a href="#">Clock</a>	

Retention policy

<input checked="" type="checkbox"/> Origin Site	keep the last <input type="text" value="1"/> snapshots
<input checked="" type="checkbox"/> Metro Remote Site (Kr_02_Metro)	keep the last <input type="text" value="1"/> snapshots
Remote Sites	
<input type="checkbox"/> krypton02	keep the last <input type="text"/> snapshots

[Previous](#) [Cancel](#) [Next](#)

Figure: Protection Domain (Metro Availability): Schedule Screen

- a. **Repeat every ## [minutes|hours|days]:** Click the appropriate circle for minutes, hours, or days and then enter the desired number in the box for the scheduled time interval.

The interval cannot be less than an hour, so the minutes value must be at least 60.

- b. **Repeat [weekly|monthly]:** Select which days the schedule should run.

- If you select weekly, select the boxes for the days of the week the schedule should run.
- If you select monthly, enter one or more integers (in a comma separated list) to indicate which days in the month to run the schedule. For example, to run the schedule on the first, tenth, and twentieth days, enter "1,10,20".

- c. **Start on:** Enter the start date and time in the indicated fields.

The default value is the current date and time. Enter a new date if you want to delay the schedule from starting immediately.



**Note:** A storage container-level protection domain requires a system metadata scan to populate the file list. In some cases, this scan might take a few hours. Any snapshots started before the scan completes does not contain any data.

- d. **End on:** To specify an end date, check the box and then enter the end date and time in the indicated fields.

The schedule does not have an end date by default, and the schedule runs indefinitely unless you enter an end date.

- e. **Retention Policy:** Enter the number of snapshots to save locally and at the remote sites.

- Enter a number in the **Origin Site** line "keep the last ## snapshots" field. The default is 1. The number that you enter in the **keep the last ## snapshots** field is automatically copied in the **Target Site** line.
- Enter a number of snapshots to save on the remote site in the "**keep the last ## snapshots**" field. This number can be different from the number that you have entered in the **Origin Site** line. This replication is an async replication and after the replication is completed, the protection domain is going to be available in the **Async DR** tab of the remote site.
- The snapshots that are saved is equal to the value that you have entered in the **keep the last ## snapshots** field + 1. For example, if you have entered the value **keep the last ## snapshots** field as 20, a total of 21 snapshots are saved. When the next (22nd) snapshot is taken, the oldest snapshot is deleted and replaced by the new snapshot.

**Note:**

- Replications can fall behind if too many schedules have the same start time. Therefore, it is recommended that start times be staggered across protection domains and across schedules.
- It is recommended to create a schedule during the creation of metro availability protection domain. In any case (if you create a schedule or do not create a schedule), snapshots are taken for every four hours. These snapshots will help minimize the data replication when the metro availability direction is reversed.

**7.** In the *Review* screen, verify that the configuration is correct and then click the **Create** button.

This configures the metro cluster but does not activate it.

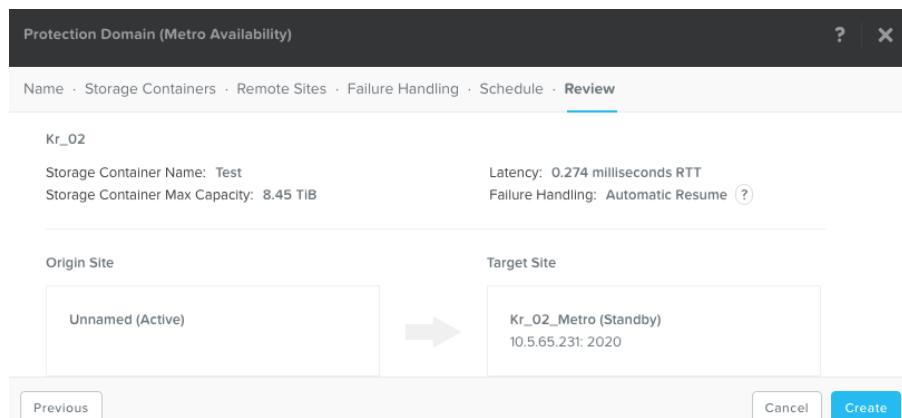


Figure: Protection Domain (Metro Availability): Review Screen

**8.** Click **Yes** in the confirmation dialog box.

Metro availability is enabled on the storage container across two sites. You can modify an existing protection domain to create the backup schedules and also replicate the domain to local site and remote site. For more information, see [Modifying Protection Domain \(Metro Availability\)](#) on page 278.

#### Modifying Protection Domain (Metro Availability)

You can modify an existing protection domain by replicating the domain, updating the domain settings, or disabling the domain.

- Taking snapshot of the protection domain:** You can take a snapshot of the protection domain locally and to one or more remote sites.
- Disabling the protection domain:** You can disable the metro availability configuration on the selected storage container.

- **Updating the protection domain:** You can create the backup schedules for the metro availability configuration. You can also replicate a protection domain to one or more remote sites (sites that are not part of the metro availability configuration). This replication to the remote sites is an async replication and after the replication is completed, the protection domain is going to be available in the **Async DR** tab of the third site.



**Note:** The backup schedule information is only available in **Schedules** tab of the primary site. If you perform a failover to the remote site, only then you can add a new schedule in the remote site.

1. In the Data Protection dashboard, click the **Table** view.
2. Click the **Metro Availability** tab.
3. Select the protection domain that you want to modify.
4. To replicate a protection domain, click **Take Snapshot**. Select one or more targets where you want to replicate the protection domain.

**a. Local:** Do nothing in this field.

The box is checked by default to indicate a local snapshot is always created. If no remote site is checked, the snapshot is saved locally only. If one or more remote sites are checked, the snapshot is saved locally and at the specified remote sites.

**b. Remote sites:** Check the boxes of the target remote sites.



**Note:** If no remote site is checked, the snapshot is saved locally only.

**c. Replication start time:** Select the start time from the pull-down list.

Choices range from now to 48 hours from now.

**d. Retention time:** Select the retention interval (how long the snapshot is saved on the remote sites) from the pull-down list.

Choices range from one day to 3 months.

**e. When all the field entries are correct, click the **Save** button.**

5. To disable a protection domain, click **Disable**.

See the guidances for disabling metro availability before you perform disable operation. For more information, see [Enabling or Disabling Metro Availability](#) on page 281.

6. To update a protection domain, click **Update**.

You can create the backup schedules for the metro availability configuration from the **Schedule** tab. You can also select the method to disable metro availability (manually or automatically) when a network or other problem interrupts the connection between clusters from the **Failure Handling** tab.

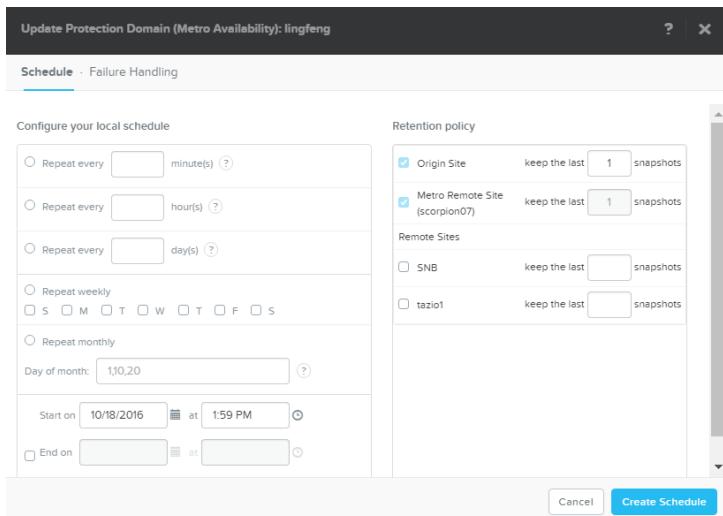


Figure: Updating the Protection Domain

7. To create a schedule, click the **New Schedule** to display the create schedule screen and then do the following in the indicated fields:
  - a. **Repeat every ## [minutes|hours|days]**: Click the appropriate circle for minutes, hours, or days and then enter the desired number in the box for the scheduled time interval.  
The interval cannot be less than an hour, so the minutes value must be at least 60.
  - b. **Occur [weekly|monthly]**: Select which days the schedule should run.
    - If you select weekly, select the boxes for the days of the week the schedule should run.
    - If you select monthly, enter one or more integers (in a comma separated list) to indicate which days in the month to run the schedule. For example, to run the schedule on the first, tenth, and twentieth days, enter "1,10,20".
  - c. **Start on**: Enter the start date and time in the indicated fields.  
The default value is the current date and time. Enter a new date if you want to delay the schedule from starting immediately.
 

**Note:** A storage container-level protection domain requires a system metadata scan to populate the file list. In some cases, this scan might take a few hours. Any snapshots started before the scan completes does not contain any data.
  - d. **End on**: To specify an end date, check the box and then enter the end date and time in the indicated fields.  
The schedule does not have an end date by default, and the schedule runs indefinitely unless you enter an end date.
  - e. **Retention Policy**: Enter the number of snapshots to save locally and at the remote sites.
    - Enter a number in the **Origin Site** line "keep the last ## snapshots" field. The default is 1. The number that you enter in the **keep the last ## snapshots** field is automatically copied in the **Target Site** line.
    - Enter a number of snapshots to save on the remote site in the "keep the last ## snapshots" field. This number can be different from the number that you have entered in the **Origin Site** line. This replication is an async replication and after the replication is completed, the protection domain is going to be available in the **Async DR** tab of the remote site.
    - The snapshots that are saved is equal to the value that you have entered in the **keep the last ## snapshots** field + 1. For example, if you have entered the value **keep the last ## snapshots**

field as 20, a total of 21 snapshots are saved. When the next (22nd) snapshot is taken, the oldest snapshot is deleted and replaced by the new snapshot.

- f. When all the field entries are correct, click the **Create Schedule**.

You can create multiple schedules, update or delete the schedule you have created.



**Note:** Replications can fall behind if too many schedules have the same start time. Therefore, it is recommended that start times be staggered across schedules.

8. To disable metro availability (manually or automatically) when a network or other problem interrupts the connection between clusters, click *Failure Handling* tab.

- Selecting the **Manual** option means VM writes does not resume until a user disables metro availability manually or the problem is resolved. This option supports storage container consistency between the clusters at the cost of VM availability.

See the guidances for disabling metro availability before you perform disable operation. For more information, see [Enabling or Disabling Metro Availability](#) on page 281.

- Selecting the **Automatic Resume** option means VM writes resume automatically after 30 seconds. This option supports VM availability at the cost of storage container consistency between the clusters.
- Selecting the **Witness** option means the Witness VM can automatically distinguish a site failure from a network interruption between the metro availability sites and decide whether to failover in case of a site failure or network interruption.

9. To delete the protection domain, click **Delete** button.

10. In the confirmation box, enter DELETE word in the text box and then click the **Delete** button.

The selected protection domain is deleted.

#### **Enabling or Disabling Metro Availability**

Following are the general guidances before you enable or disable metro availability on a storage container.

#### **Enabling Metro Availability**

1. All the VMs in a metro availability protection domain should be on the primary site.
2. Set the DRS rules to ensure that the VMs have affinity to the hosts of the primary site. The DRS rules should be **Fully Automated**.
3. Ensure that the default schedule on the metro availability protection domain is available and is not paused.

#### **Disabling Metro Availability**

1. All the VMs in a metro availability protection domain should be on the primary site.
2. Set the DRS rules to ensure that the VMs have affinity to the hosts of the primary site. The DRS rules should be **Fully Automated**.
3. Datastore on the secondary site will be active, but it is in the read-only state. Do not promote the secondary site at this point as this can lead to the datastore being readable and writeable on both the sites, which may lead to VM inconsistency or even corruption when a VM is live-migrated from the primary to the secondary site.

## Restoring a VM from a Metro Availability Snapshot

Since metro availability uses storage container-level protection, you can only restore the entire contents of the snapshot. The restoration happens by using a separate path to prevent overwriting the protected entities.



**Caution:** You can restore a VM from a snapshot by using only the following procedure. Do not perform any manual operations with the files located in .snapshot directory as it might lead to cluster stability issues.

**Before you begin:** The restore operation on the metro protection domain must be performed when the replication schedules are disabled. You can suspend the schedules for a protection domain as follows.

1. Log in to the Controller VM and run the following ncli command

```
ncli> pd suspend-schedules name=pd_name
```

Replace *pd\_name* with the name of the protection domain. This command returns a status of either true or false. True means all schedules for that protection domain have been suspended. If the status is false, repeat the command until the status is true. Run the command for all the protection domains in your cluster.

2. Verify the status of the protection domains by running the command `ncli> pd status` and ensure that the status that is returned is `false`.



### Note:

- You can only use nCLI to perform the restore operation as currently the option is not available in the Prism.
- If there are any linked clones or shared files between the VMs, then ensure that you do not delete the dependent files or directories.

Log into the Controller VM and run the following nCLI command.

```
ncli> pd restore-snapshot name=protection_domain_name snap-id=snapshot_id \\\npath-prefix=/path_restore_files
```

- Replace *protection\_domain\_name* with the name of the protection domain.
- Replace *snapshot\_id* with the ID of the snapshot.
- Replace *path\_restore\_files* with the path where you want to restore the files.

For example, for the protection domain *test\_pd* with metro availability enabled on the storage container *test\_storage\_container* and the snapshot ID of 16388, to restore the files to the path *test\_restore* on the *test\_storage\_container*, use the following command:

```
ncli pd restore-snapshot name=test_pd snap-id=16388 path-prefix=/test_restore
```



### Note:

- The / in the restored path creates a folder *test\_restore* in the *test\_storage\_container*. All the files that were in that snapshot are restored to the */test\_restore* location. You can then navigate to the folder to retrieve the necessary files.
- If you omit the path-prefix parameter, a folder with a starting name of */Nutanix-Clone* is created automatically.
- If you perform the snapshot-restore operation when metro availability is enabled, the restored file path is also replicated to the secondary site. The restored file paths are like user-created files and they are synchronously restored in both the active and the standby sites.
- You can only restore from the snapshots that were created after the most recent time you enabled the metro availability protection domain. You can restore older snapshots either when the metro availability is **Disabled** or **Promoted** on the secondary site (in both these cases, the status of metro availability is **Disabled**).

- Place the VMs that are frequently snapshotted and restored together in the same protection domain to avoid unnecessary storage space utilization. This also avoids the restoration and subsequent deletion of unnecessary VMs.
- Once the restore operation is complete and all the desired files are restored, you must delete the unnecessary files from the restore folder before you proceed with the next snapshot operation.

## Metro Availability Witness Option

You have the option of adding a Witness to a Metro Availability configuration (see [Data Protection Guidelines \(Metro Availability\)](#) on page 271). A "Witness" is a special VM that monitors the Metro Availability configuration health. The Witness resides in a separate failure domain to provide an outside view that can distinguish a site failure from a network interruption between the Metro Availability sites. The main functions of a Witness include:

- Making a failover decision in the event of a site or inter-site network failure.
- Avoiding a split brain condition where the same storage container is active on both sites due to (for example) a WAN failure.
- Handling situations where a single storage or network domain fails.

## Metro Availability Failure Process (no Witness)

In the event of either a primary site failure (the site where the Metro storage container is currently active) or the link between the sites going offline, the Nutanix administrator is required to manually disable Metro Availability and promote the target storage container on the remote (or current) site to Active.

In case of a communication failure with the secondary site (either due to the site going down or the network link between the sites going down), Metro Availability does one of the following depending on the setting (automatic or manual):

- Automatic: The system automatically disables Metro Availability on the storage container on the primary site after a short pause if the secondary site connection does not recover within the specified time.
- Manual: The system waits for the administrator to manually take action.

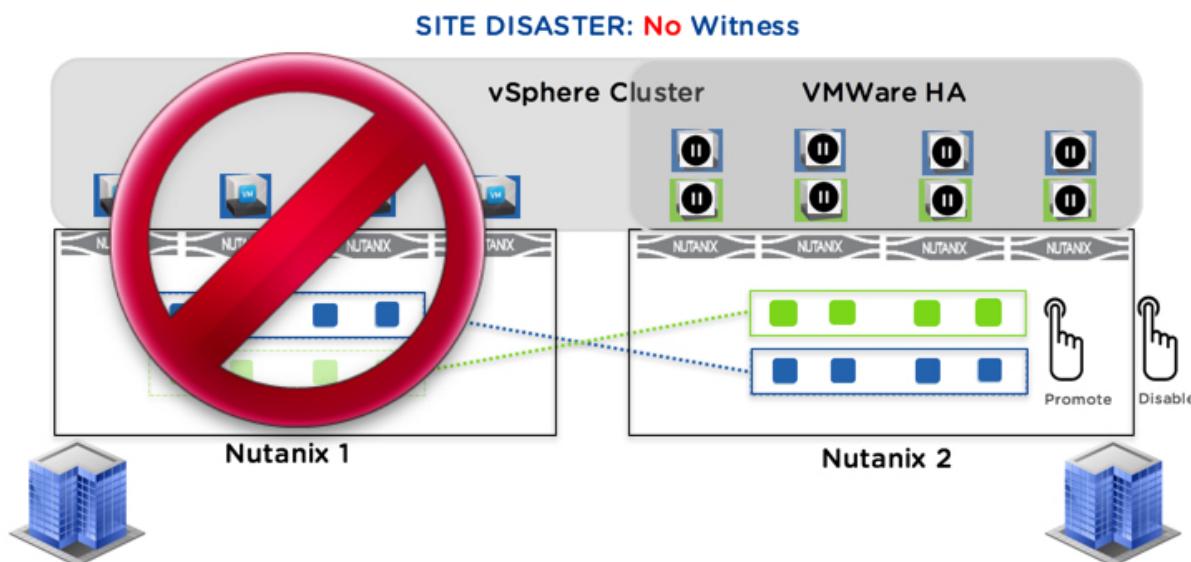


Figure: Site Disaster (no witness)

## Metro Availability Failure Process (with a Witness)

When a Witness is added, the process of disabling Metro Availability and promoting the storage container in case of a site outage or a network failure is fully automated. The Witness functionality is only used in case of a failure, meaning a Witness failure itself does not affect VMs running on either site.

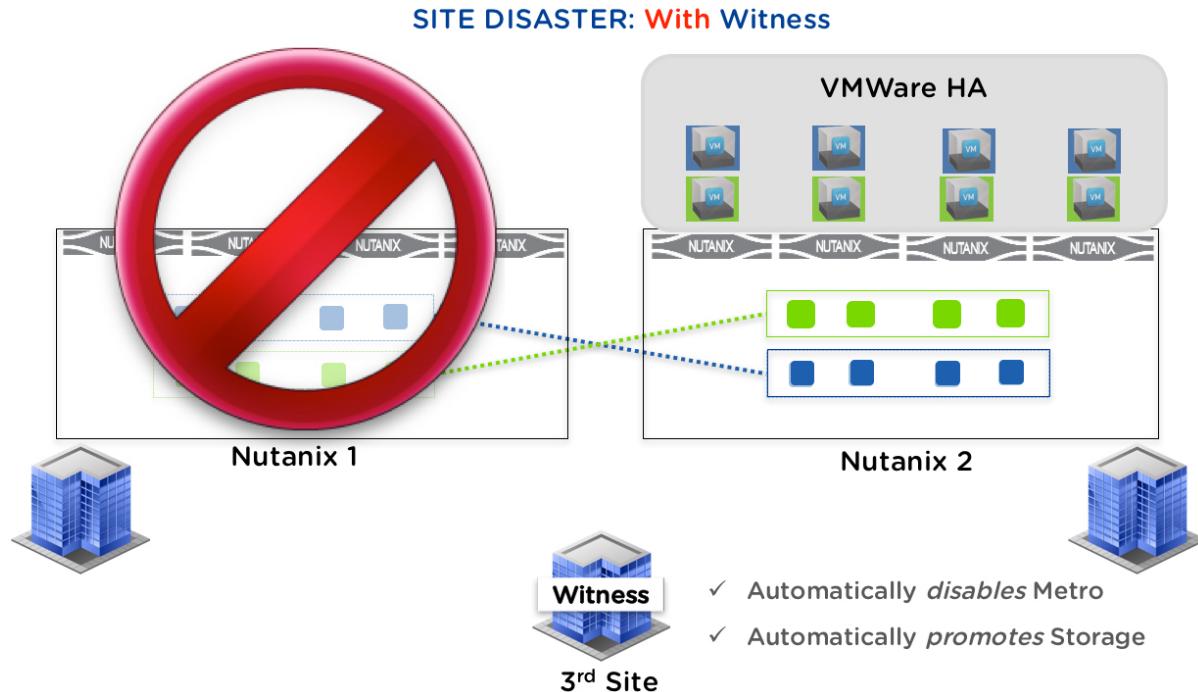


Figure: Site Disaster (with a witness)

## Metro Availability Operational Modes

After adding a Witness, you can select from three Metro Availability operational modes: Witness Mode (new), Automatic Resume Mode, or Manual Mode. The Metro Availability response to a failure scenario varies depending on which operational mode is selected. The following table details the failure scenarios and the response behavior based on the operational mode.

### Operational Mode Response Behaviors

Failure Scenario	Witness Mode	Automatic Resume Mode	Manual Mode
Site 1 outage or complete network failure in Site 1	Automatically fails over to Site 2	Metro Availability stops. Administrator must manually activate protection domain on Site 2 and restart VMs.	Metro Availability stops. Administrator must manually activate protection domain on Site 2 and restart VMs.
Site 2 outage or complete network failure in Site 2	VMs continue to run on Site 1	VMs continue to run on Site 1	All VMs are paused. Administrator intervention required.
Connection loss between Sites 1 and 2	VMs continue to run on Site 1	VMs continue to run after timeout	All VMs are paused. Administrator intervention required.

Failure Scenario	Witness Mode	Automatic Resume Mode	Manual Mode
Witness failure	No impact. However, ability to recover automatically in some scenarios is lost.	n/a	n/a
Connection loss between Witness and Site 1	VMs continue to run on Site 1	n/a	n/a
Connection loss between Witness and Site 2	VMs continue to run on Site 1	n/a	n/a
Connection loss between Witness and both Sites 1 and 2	VMs continue to run on Site 1	n/a	n/a
Failure at both Site 1 and Site 2	Metro Availability stops. Administrator intervention required.	Metro Availability stops. Administrator intervention required.	Metro Availability stops. Administrator intervention required.
Connection loss between Site 1 and Site 2 and between Witness and Site 1	VMs on Site 1 are paused. Site 2 will automatically be promoted and vSphere HA will automatically start the VMs. Administrator intervention required to hard-stop the VMs on site 1.	Metro Availability is disabled, but VMs on Site 1 continue to run. Administrator intervention required.	All VMs are powered down. Administrator intervention required.

## Witness Requirements

There are several requirements when setting up a Witness:

- The Witness VM requires (at a minimum) the following:
  - 2 vCPUs
  - 6 GB memory
  - 25 GB storage
- The Witness VM must reside in a separate failure domain, which means independent power and network connections from each of the Metro Availability sites. It is recommended that the Witness VM be located in a third physical site. This site should have dedicated network connections to Site 1 and Site 2 to avoid a single point of failure.
- Communication with the Metro Witness happens over port TCP 9440 and, therefore, requires that this port be open for the Controller VMs on any Metro cluster that uses the Witness.
- Network latency between each Metro Availability site and the Witness VM must be less than 200 ms.
- The Witness VM may reside on any supported hypervisor, and it can run on either Nutanix or non-Nutanix hardware.
- You can register multiple (different) Metro cluster pairs to a single Witness VM, but there is a limit of 50 Witnessed Metro protection domains per cluster pair.

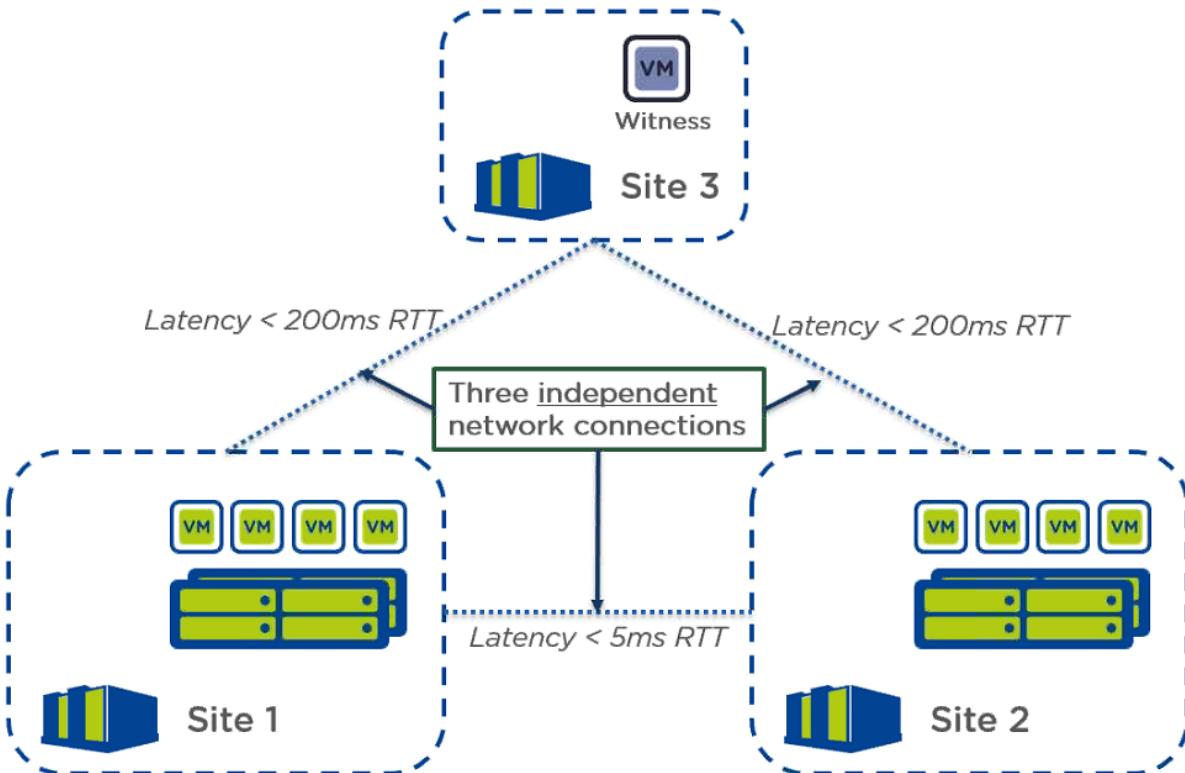


Figure: Witness Network Connections

### Installing a Witness VM

To install a Witness VM, do the following:

1. Download the Witness VM image file to your workstation as follows:
  - a. Log on to the Nutanix support portal (<http://portal.nutanix.com>).
  - b. Click **Downloads > Tools & Firmware** from the main menu (at the top).
  - c. Find the Metro Witness line(s) for your hypervisor and click on the file link(s) in the **Download** column to download the file(s).
    - ESXi: *version#-witness\_vm.ova*
    - AHV: *version#-witness\_vm-boot.qcow2*, *version#-witness\_vm-data.qcow2*, and *version#-witness\_vm-home.qcow2*
2. Upload the VM image to the desired location.
  - If it is being uploaded to a Nutanix cluster, use the Prism image service to upload the VM image. See the "Configuring Images" section in the *Prism Web Console Guide* for instructions on uploading an image file.
  - If it is being uploaded to non-Nutanix hardware, refer to the documentation from that vendor for instructions.
3. Create and power on the Witness VM.
  - If the hypervisor is AHV, see the "Creating a VM" section in the *Prism Web Console Guide* for instructions.

→ If the hypervisor is ESXi, see your ESXi documentation for instructions.



**Note:** The VM must have at least 2 vCPUs, 4 GBs of memory, and 25 GBs of storage.

**4.** Open a console window and log in to the Witness VM.

- The user name is `nutanix` and the password `nutanix/4u` by default when logging in through SSH.
- The user name is `admin` and the password `Nutanix/4u` by default when logging in through Prism.

**5.** Assign a static IP address to the Witness VM as follows:

**a.** Open the `ifcfg-eth0` file for editing.

The following command opens the file using the `vi` editor:

```
$ sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

**b.** Update the `NETMASK`, `IPADDR`, `BOOTPROTO`, and `GATEWAY` entries as needed.

```
NETMASK="xxx.xxx.xxx.xxx"
IPADDR="xxx.xxx.xxx.xxx"
BOOTPROTO="none"
GATEWAY="xxx.xxx.xxx.xxx"
```

- Enter the desired netmask value in the `NETMASK` field. (Replace `xxx.xxx.xxx.xxx` with the appropriate value.)
- Enter the appropriate static IP address (usually assigned by your IT department) for the Witness VM in the `IPADDR` field.
- Enter `none` as the value in the `BOOTPROTO` field. (You might need to change the value from `dhcp` to `none` if you employ DHCP. Only a static address is allowed; DHCP is not supported.)
- Enter the IP address for your gateway in the `GATEWAY` field.



**Warning:** Carefully check the file to ensure there are no syntax errors, whitespace at the end of lines, or blank lines in the file.

**c.** Save the changes.

**d.** Restart the Witness VM.

```
$ sudo reboot
```

**6.** Enter the following command to create a Witness VM cluster:

```
$ cluster -s vm_ip_address --cluster_function_list=witness_vm create
```

The `vm_ip_address` is the Witness VM IP address.

This completes the Witness VM installation. The next step is to register the VM with each of the Metro Availability sites.

**7.** To change the Witness VM default password, enter the `passwd` command while still logged in to the Witness VM (as the `nutanix` user) and follow the prompts.

```
$ passwd
Changing password for user admin.
Changing password for admin.
(current) UNIX password: admin_password
New password: new_admin_password
Retype new password: new_admin_password
passwd: all authentication tokens updated successfully.
```

 **Note:** The `passwd` command is supported on AOS 5.1.1 or later. If you are running an earlier AOS version, use the `nuclei` command instead to change the password:

```
$ nuclei  
Enter username: admin  
Enter password: new_admin_password  
<aplos> diag.change_password user_name=admin new_password=new_admin_password
```

This is sufficient if the password is changed just after creating the Witness VM. However, if the password is changed after the Witness VM is registered with the Metro Availability clusters, additional steps are required:

- a. Log in to a Controller VM on the primary Metro Availability cluster using SSH and then use the nCLI to display information about the Witness VM registered with that cluster:

```
nutanix@cvm$ ncli  
ncli> cluster list-witness  
  
Id : id_number  
Cluster Name : cluster_name  
External IP Address : ip_address  
Marked for Removal : value
```

- b. Update the password for the registered Witness VM by entering the following command:

```
ncli> cluster update-witness id=id_number password=pw_string
```

The `id_number` is the ID number obtained from the `cluster list-witness` command in the previous step, and the `pw_string` is the same as what you entered to create the new password in the `passwd` (or `nuclei`) command.

- c. Repeat these steps for the secondary Metro Availability cluster.

## Upgrading a Witness VM

To upgrade a Witness VM to a newer version, do the following:

 **Note:** A new Witness VM may not be generated for every new AOS release. A Witness VM upgrade will be blocked if the upgrade path is not supported.

 **Note:** The Witness VM upgrade may not be successful if there is a time synchronization issue. The clock on VMs can be unreliable, so to avoid such issues it is recommended that you have three (or more) NTP servers configured for the cluster (see [Cluster Time Synchronization](#) on page 571) before attempting an upgrade. If the Witness VM is not located in a Nutanix cluster, see the appropriate NTP configuration documentation for your environment.

1. Log in to the Witness VM using SSH and go to the `~/tmp` directory (`cd ~/tmp`).
2. Download the target AOS installation bundle from the Nutanix support portal using the `wget` command from the download directory (`~/tmp`):

```
user@host$ wget https://nutanix_installer_package-release_version.tar.gz
```

To determine the exact URL to use, log on to the Nutanix support portal (<http://portal.nutanix.com>), select **Downloads > Tools & Firmware** from the main menu, select the target AOS version (latest version is displayed; you can select other versions from the **Additional Releases** column), click the **URL COPY** link, and copy that link into the `wget` command. For example, enter the following to download the AOS 5.0.2 installation bundle:

```
user@host$ wget https://nutanix_installer_package-release-euphrates-5.0.2-stable.tar.gz
```

AOS 5.0.2

AOS (NOS) v5.0.2 is available for download from a link on the right and documentation on how to upgrade can be found here.

**Note**

- Please review to the following cautions prior to downloading 5.0.2. Refer to the [Acropolis 5.0.2 Release Notes](#) for list of New Features, Resolved Issues and other Notes and Cautions.

**EOL Notice :** The release of Nutanix AOS 5.x will start the clock for EOL on all 4.x releases. All releases up to 4.6.x will reach end of their support life on July 31, 2017. If you are on an earlier release, please plan on moving to 4.7.x or a more recent version by that date, to avoid disruption in support.

**Download 5.0.2**

URL COPY [Link to 5.0.2 Download](#) (arrow)

**SIZE** 3.16 GB  
**DATE** April 03, 2017  
**MD5** Obbe869bbe63d2de3070a46de7501dae  
**METADATA** Upgrade Metadata File

**Feedback**

**ADDITIONAL RELEASES**

[Download 4.7.5.2 · Documentation](#)  
3.4 GB · Mar 21, 2017  
md5: 775e20c08447ba76e2a56278e7ec103a

Figure: AOS Download Page



**Note:** If the wget command does not work, there might be a DNS issue. In this case you can download the installation bundle to your workstation and then copy it to the Witness VM's /home/nutanix/tmp folder using a program such as WinSCP, or you can configure a DNS server for the Witness VM by editing the /etc/resolv.conf file and adding a **nameserver** entry (nameserver x.x.x.x) as illustrated in the following example:

```
nutanix@cvm$ cat /etc/resolv.conf
# Auto generated by DnsConfig on Fri Apr 7 12:20:54 2017
nameserver 10.4.8.15
```

### 3. Extract the bundle by entering the following command:

```
user@host$ tar -xvzf nutanix_installer_package-release_version.tar.gz
```

The installation bundle (nutanix\_installer\_package-release\_version.tar.gz) is a large file, so delete it after the tar command completes successfully.

### 4. Upgrade the cluster (Witness VM) to the target AOS release by entering the following command:

```
user@host$ ./install/bin/cluster -i install/ upgrade
```

This command must be run from the same directory as the tar command in step 3 (~tmp).

### 5. If you upgraded a pre-AOS 5.1.1 Witness VM to 5.1.1 or later, the default admin user password is automatically reset to Nutanix/4u. When you log in through SSH as the admin user (with the Nutanix/4u password) the first time after the upgrade, you are prompted to set a custom password. Once the custom password has been set, you need to update the Witness VM password on any Nutanix clusters using (registered with) that Witness VM.

## Registering a Witness VM

To register a Witness for a Metro Availability site, do the following:

- Open a browser and log in to Prism for the primary site Metro Availability cluster.

- Select **MA Witness Registration** from the gear icon pull-down list of the main menu.

The *Metro Availability Witness Registration* window appears. Do the following in the indicated fields:

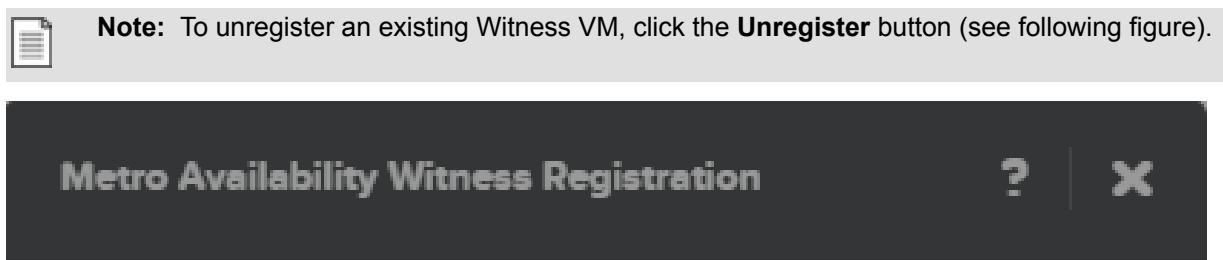
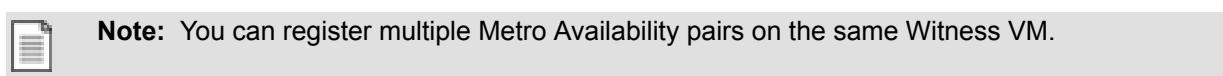


Figure: Metro Availability Witness Registration Window

- a. **MA Witness IP Address:** Enter the Witness VP IP address.
  - b. **Username:** Enter the administrator user name (admin by default).
  - c. **Password:** Enter the user password (Nutanix/4u by default).
  - d. Click the **Save** button.
3. Log in to the standby Metro Availability cluster and repeat these steps.



## Changing Witness VM for a Protection Domain

If it becomes necessary to change the Witness VM for a protection domain, for example if the Witness VM goes away permanently, do the following to associate a protection domain with a new Witness VM:

1. Create the new Witness VM if it is not created already (see [Installing a Witness VM](#) on page 286).
2. On the primary Metro Availability cluster, change the failure handling setting from **Witness** to **Automatic** (or Manual) for each Metro Availability protection domain that uses the Witness VM and then disable these protection domains (see [Modifying Protection Domain \(Metro Availability\)](#) on page 278).
3. First unregister the current Witness VM and then register the new Witness VM on both the primary and secondary clusters (see [Registering a Witness VM](#) on page 289).
4. Change the failure handling settings back to **Witness** on all the protection domains changed in step 2 and then re-enable those protection domains.

## Configuring Witness Mode

To configure a Witness for Metro Availability, do the following:

1. Log in to Prism for the primary site Metro Availability cluster.
2. Select **Data Protection** from the view option pull-down list of the main menu and then do one of the following :
  - If you are creating a new Metro Availability configuration (see [Configuring a Protection Domain \(Metro Availability\)](#) on page 274), click the **Protection Domain** button and select **Metro Availability**.
  - If you are adding a Witness to an existing Metro Availability configuration (see [Modifying Protection Domain \(Metro Availability\)](#) on page 278), click the **Table** tab, click the **Metro Availability** tab, select the primary site from the table list, and then click the **Update** button.



**Note:** You need to first disable Metro Availability on the protection domain before changing the failure handling mode. Re-enable Metro Availability on the protection domain after changing the failure handling mode.

3. Complete the protection domain creation or update steps as normal. In the Failure Handling screen, select **Witness**.

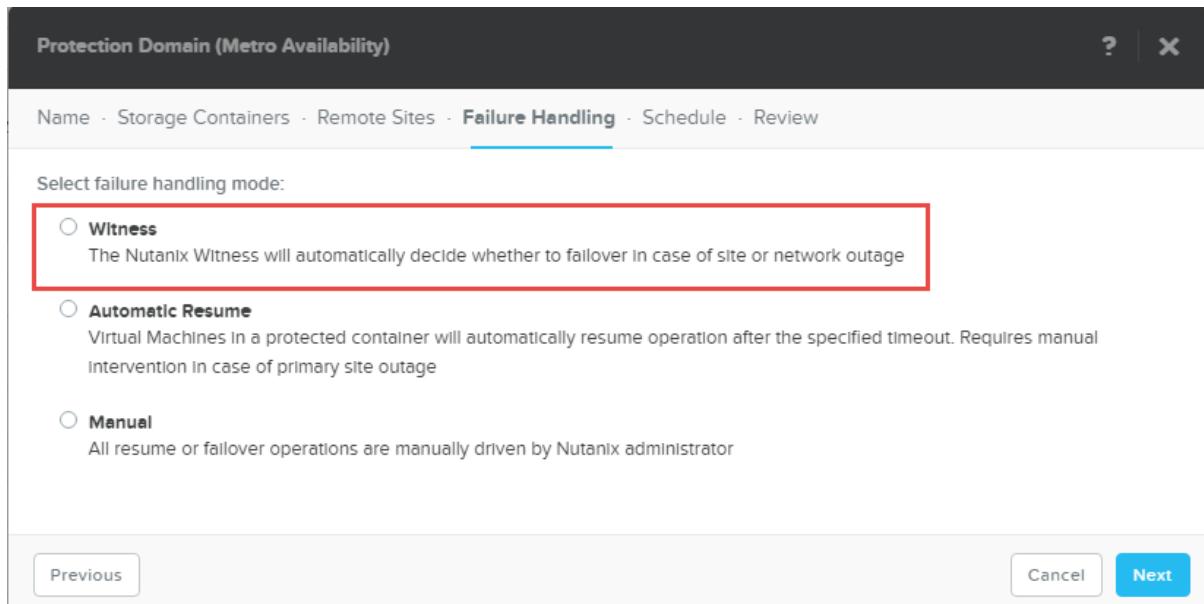


Figure: Failure Handling Screen (protection domain creation work flow)

### Witness VM Dashboard

The Witness provides a dashboard of status information about all the registered storage containers. To view the Witness dashboard, do the following:

1. Open a browser to [https://witness\\_vm\\_ip\\_address](https://witness_vm_ip_address).
2. Log in to the Witness VM. (The user name is admin and the password Nutanix/4u by default.)



Figure: Witness Login Screen

The Witness dashboard appears. A line appears for each storage container across all the registered protection domains. Each line includes the following fields:

- **Storage Container Name:** Lists the name of the storage container.
- **Active Cluster:** Lists the name of the active (primary) cluster for this storage container.
- **Status:** Lists the current Metro Availability status of the storage container:
  - **In Sync:** Both sites (clusters) are in a steady state.
  - **Promoted:** One site got promoted.
  - **Disabled:** Metro Availability is broken between the primary and secondary sites.
- **Standby Cluster:** Lists the name of the standby cluster for this storage container.

To log out from the witness VM, go to the user icon menu (upper right of the screen) and select **Logout** from the pull-down list.

CONTAINER NAME	ACTIVE CLUSTER	STATUS	STANDBY CLUSTER	PD NAME
ctr_207	cluster_00053aca-b38f-3a3b-0000-000000006094	Disabled	cluster_00053aca-b37a-3c98-0000-000000003fb5	pd_207
ctr_239	cluster_00053aca-b37a-3c98-0000-000000003fb5	Promoted	cluster_00053aca-b38f-3a3b-0000-000000006094	pd_239
ctr_38	cluster_00053aca-b38f-3a3b-0000-000000006094	Disabled	cluster_00053aca-b37a-3c98-0000-000000003fb5	pd_38
ctr_179	cluster_00053aca-b37a-3c98-0000-000000003fb5	Promoted	cluster_00053aca-b38f-3a3b-0000-000000006094	pd_179
ctr_4	cluster_00053adb-bc88-4f03-0000-000000006094	Disabled	cluster_00053adb-bcf6-7e56-0000-000000003fb5	pd_4
ctr_156	cluster_00053aca-b37a-3c98-0000-000000003fb5	Unknown	cluster_00053aca-b38f-3a3b-0000-000000006094	pd_156
ctr_94	cluster_00053aca-b37a-3c98-0000-000000003fb5	Promoted	cluster_00053aca-b38f-3a3b-0000-000000006094	pd_94
ctr_89	cluster_00053aca-b37a-3c98-0000-000000003fb5	Promoted	cluster_00053aca-b38f-3a3b-0000-000000006094	pd_89
ctr_167	cluster_00053aca-b38f-3a3b-0000-000000006094	Disabled	cluster_00053aca-b37a-3c98-0000-000000003fb5	pd_167
ctr_7	cluster_00053adb-bcf6-7e56-0000-000000003fb5	Unknown	cluster_00053adb-bc88-4f03-0000-000000006094	pd_7
ctr_252	cluster_00053aca-b37a-3c98-0000-000000003fb5	Unknown	cluster_00053aca-b38f-3a3b-0000-000000006094	pd_252

Figure: Witness Dashboard

## Recovery Procedures (Witness VM installed)

The steps for recovering from a Metro Availability failure when a Witness is enabled depend on the nature of the failure. This section describes the steps needed (or not needed) when a failure occurs.

### Recovering from a Primary Site Failure

When Site 1 (primary site) goes down, Site 2 (secondary site) detects the outage and acquires the lock from the Witness. The storage container automatically becomes active on Site 2. If the hypervisor has HA enabled, any protected VMs are failed over to Site 2. When Site 1 recovers, however, it cannot get the Witness lock and so cannot automatically make the local storage container active to re-enable Metro Availability. To re-establish replication (in this case from Site 2 to Site 1), do the following:

1. Log in to Prism on Site 1 and disable Metro Availability for the storage container (see [Modifying Protection Domain \(Metro Availability\)](#) on page 278).
2. Log in to Prism on Site 2 and re-enable Metro Availability for the storage container.

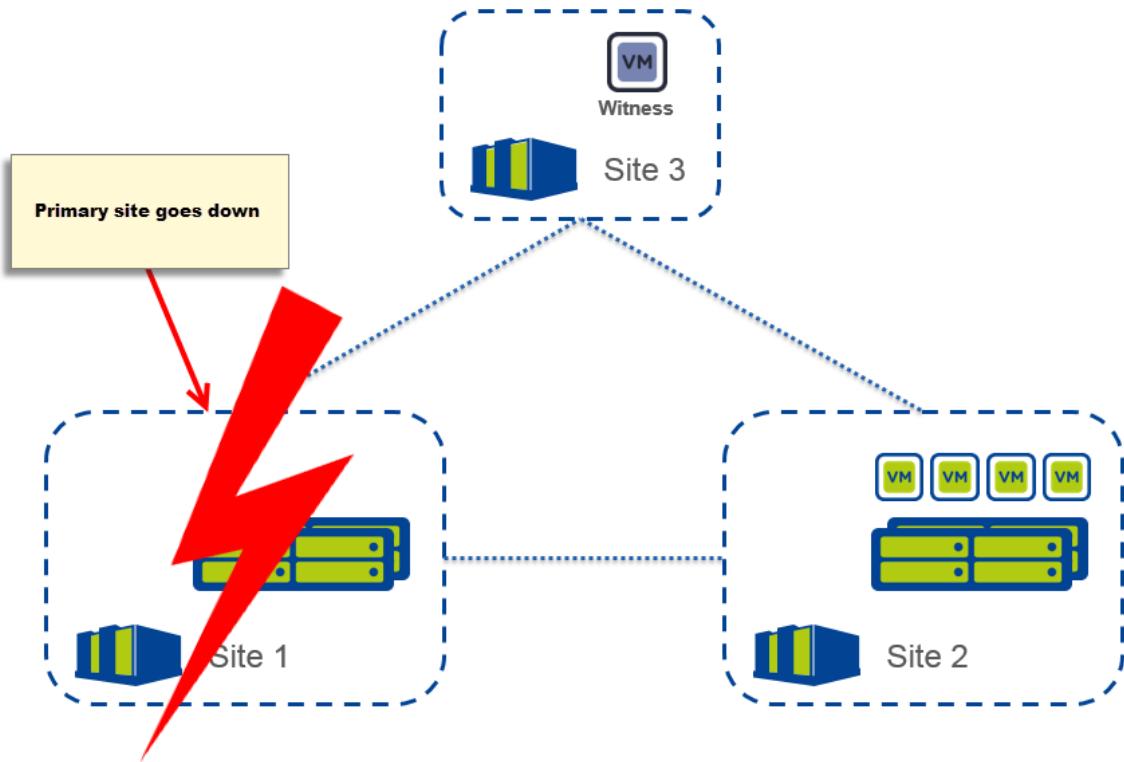


Figure: Metro Availability Primary Site Failure

### Recovering from a Secondary Site Failure

When Site 2 (secondary site) goes down, Metro Availability on the protection domain is disabled automatically. When Site 2 is operational again, the administrator must re-enable the protection domain on Site 1 to resume replication to Site 2.

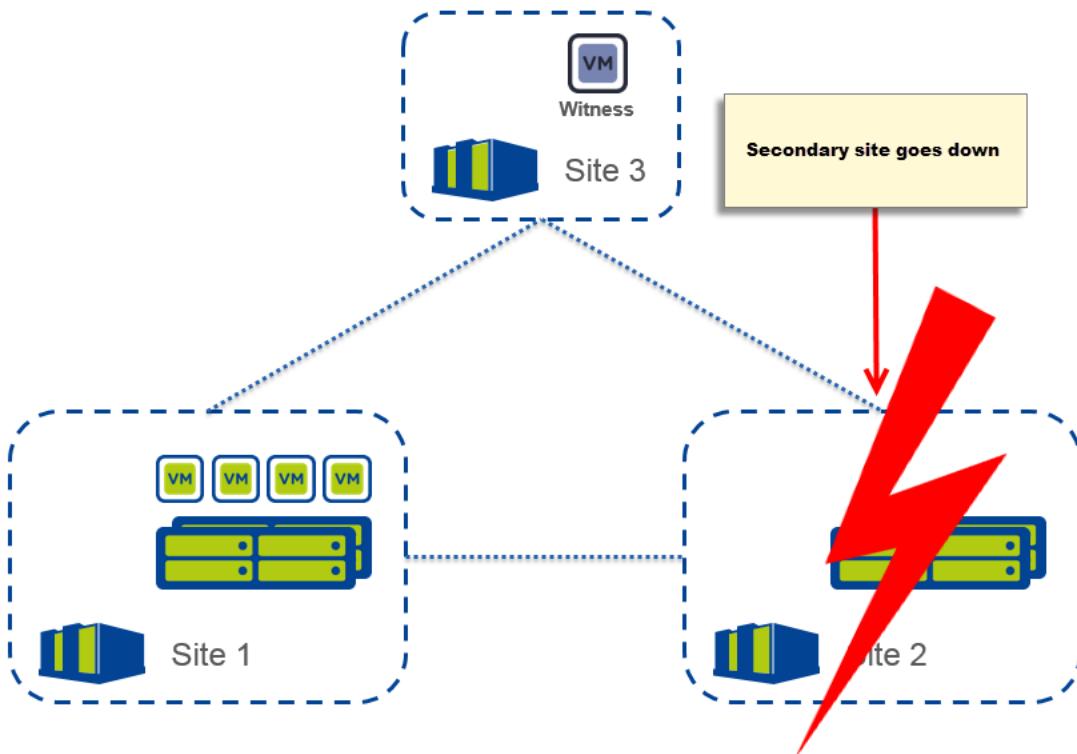


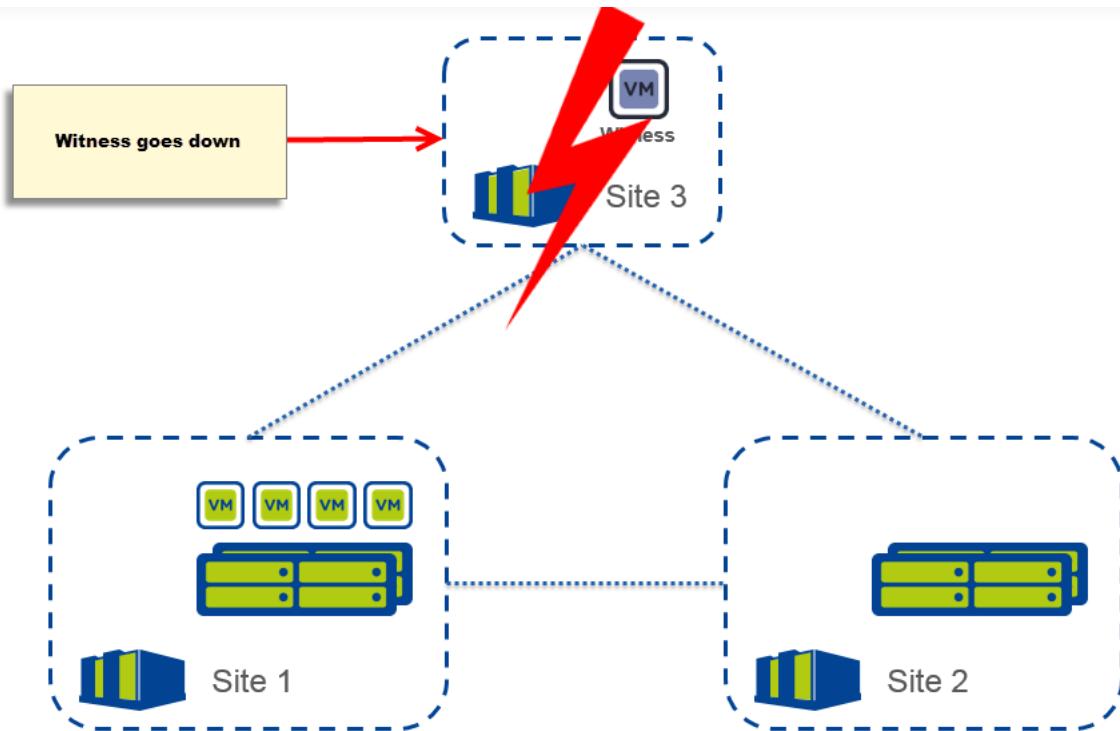
Figure: Metro Availability Secondary Site Failure

### Recovering from a Witness Failure

When the Witness goes down, an alert is generated but Metro Availability is otherwise unaffected. When connection to the Witness is re-established, the Witness process resumes automatically. No administrator intervention is required.

If the Witness VM goes down permanently (unrecoverable), do the following to implement a new Witness VM:

1. Log in to Prism on the primary site.
2. Change the recovery mode from Witness to Automatic (or Manual) for each Metro Availability protection domain that uses the Witness VM (see [Modifying Protection Domain \(Metro Availability\)](#) on page 278).
3. Unregister the Witness VM from the primary site (see [Registering a Witness VM](#) on page 289).
4. Log in to Prism on the secondary site and unregister the Witness VM.
5. When a new Witness VM is installed and ready (see [Installing a Witness VM](#) on page 286), register that Witness VM on both the primary and secondary sites.
6. Disable the target (changed in step 2) Metro Availability protection domains.
7. Change the recovery mode on the target Metro Availability protection domains back to Witness.
8. Re-enable the target Metro Availability protection domains.



*Figure: Witness Failure*

#### Recovering from a Network Failure Between the Metro Sites

If there is a network interruption between Site 1 (primary) and Site 2 (secondary) but the network connections remain good between the sites and the Witness, both Site 1 and Site 2 attempt to acquire the Witness lock. There is a delay built into the Site 2 request, so Site 1 should get the lock first. When Site 1 obtains the lock, the protection domain on Site 1 is disabled automatically. The protection domain on Site 2 remains in "Standby" mode. When the network connection is re-established, the administrator must re-enable the protection domain on Site 1 to resume replication to Site 2.

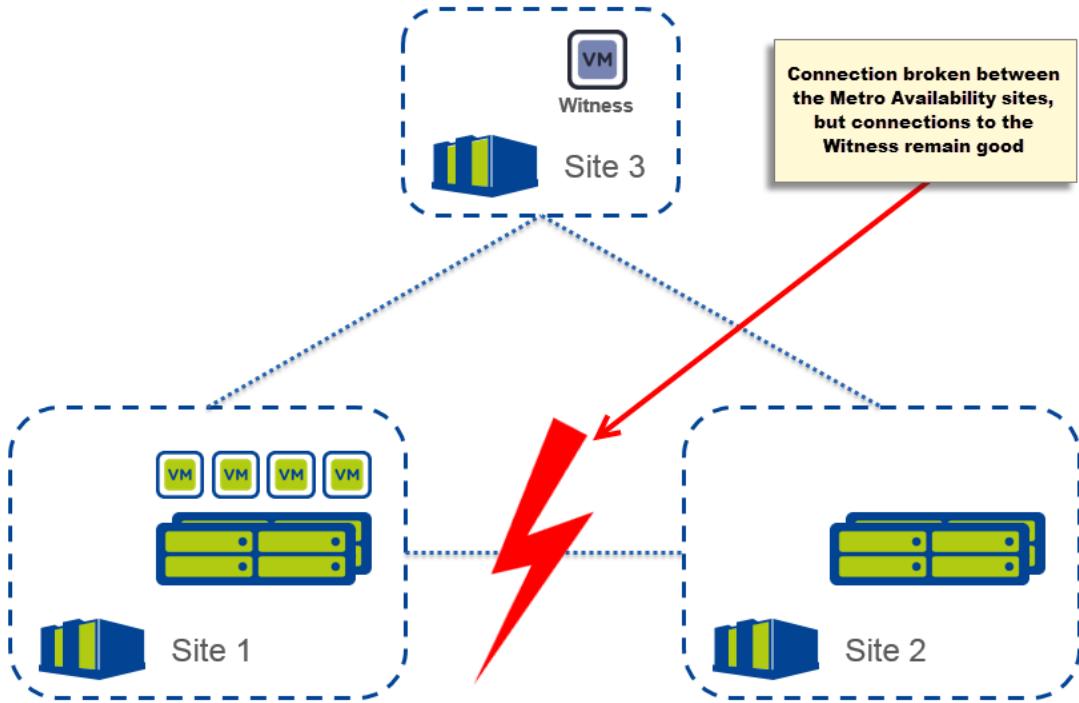


Figure: Network Failure between the Metro Sites

### Recovering from a Double Network Failure (primary site isolated)

When there is a double network failure where the connection is broken both between the Metro pair and between the primary site and the Witness, both Site 1 (primary) and Site 2 (secondary) attempt to acquire the Witness lock. Because Site 1 cannot connect to the Witness, Site 2 will acquire the lock after the built-in delay passes. Site 1 halts all I/O and the VMs are frozen. The storage container automatically becomes active on Site 2. If hypervisor HA (vCenter) is enabled and on the same network as the Witness VM, it restarts the Site 1 VMs on Site 2 after the secondary site is promoted. To re-establish replication (in this case from Site 2 to Site 1) when the connections are restored, do the following:

1. If the Site 1 VMs were restarted on Site 2, set DRS rules so that all VMs have affinities set to Site 2.
2. After restoring network connections to Site 1, kill all the stale VMs still residing on Site 1 as follows:

- a. Run the following command on every host in Site 1 and note down the world ID of the stale VMs:

```
esxcli vm process list
```

- b. Run the following command to kill the stale VMs. Be careful to kill only the VMs identified in the previous step.

```
esxcli vm process kill -w world_id -t force
```

3. Log in to Site 1 using SSH, start the nCLI, reset the failure handling mode for the target protection domain to either Automatic or Manual, and then disable Metro Availability for the protection domain.

```
nutanix@cvm$ ncli
ncli> pd update-failure-handling name=pd_name failure-handling=Automatic local-only=True
ncli> pd metro-avail-disable name=pd_name
```

Replace *pd\_name* with the name of the protection domain. Setting *local-only=True*, which deletes Witness information just from the local store, is necessary whenever any of the connections are down between the Metro sites or between either site and the Witness.

4. Log in to Prism on Site 2 and re-enable Metro Availability for the storage container.

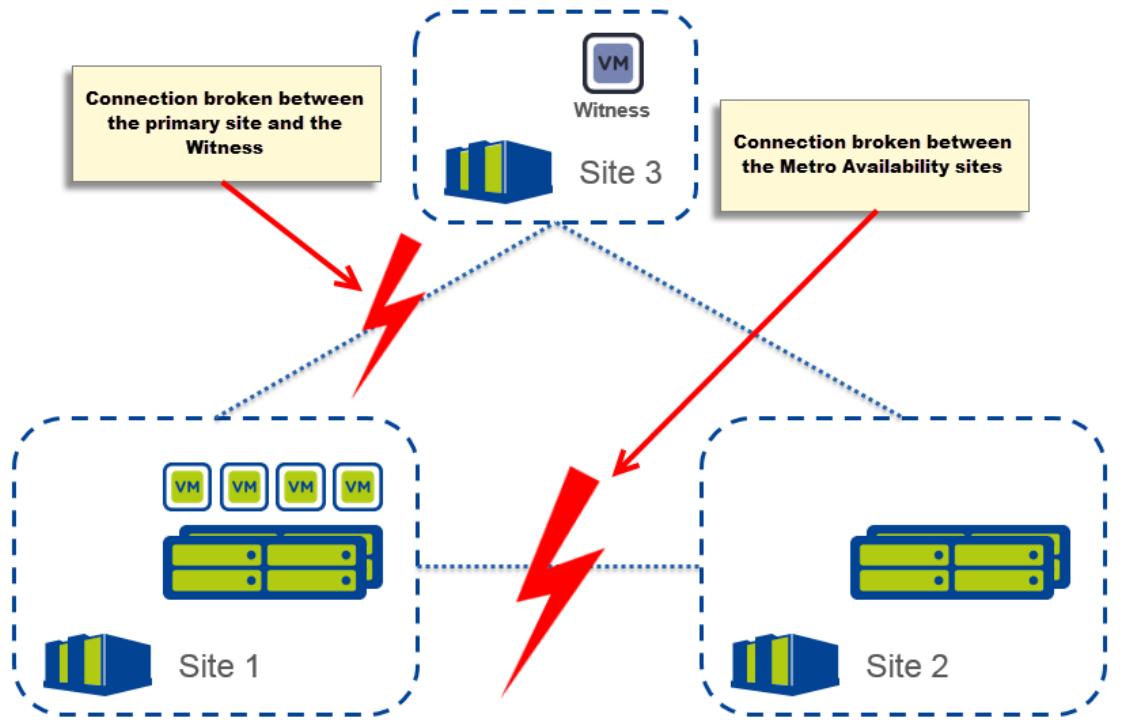
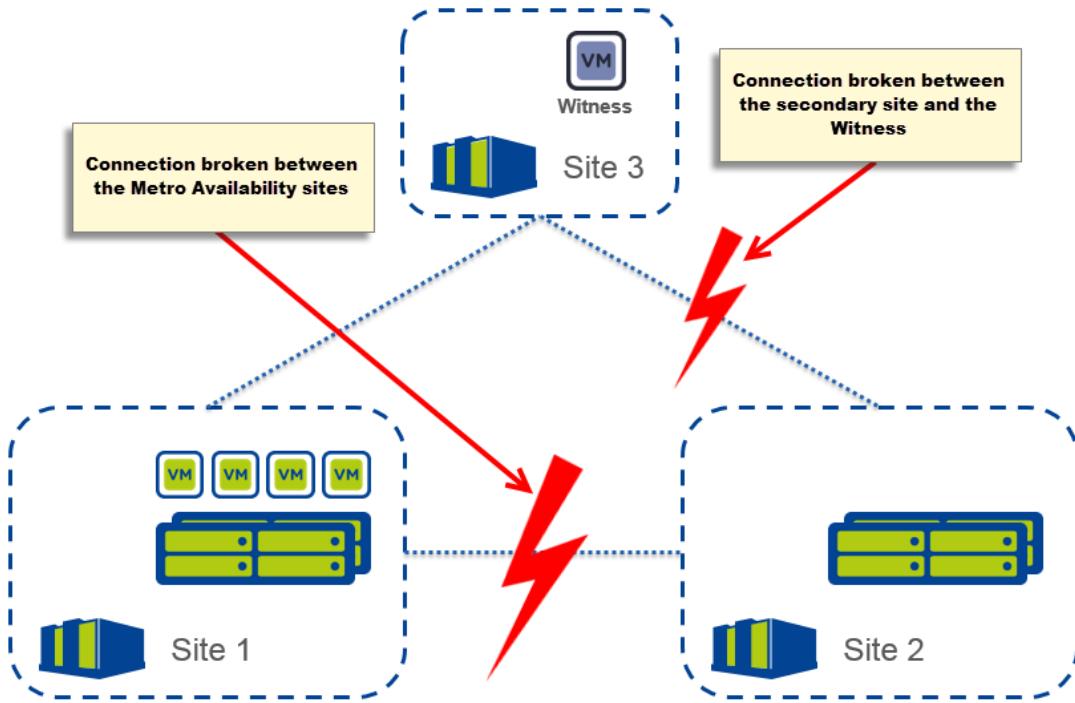


Figure: Network Double Failure (primary site isolated)

#### Recovering from a Double Network Failure (secondary site isolated)

When there is a double network failure where the connection is broken both between the Metro pair and between the secondary site and the Witness, Site 1 gets the Witness lock and Metro Availability on the protection domain is disabled automatically. When the connections are restored, the administrator must re-enable the protection domain on Site 1 to resume replication to Site 2.



*Figure: Network Double Failure (secondary site isolated)*

#### Recovering from a Complete Network Failure (both sites isolated)

When there is a complete network failure where neither Site 1 nor Site 2 can connect to the other site or the Witness, neither site can get the Witness lock, so Site 1 halts all I/O and the VMs are frozen. When the connections are restored, the administrator must perform the same recovery steps described in the primary site double failure section.

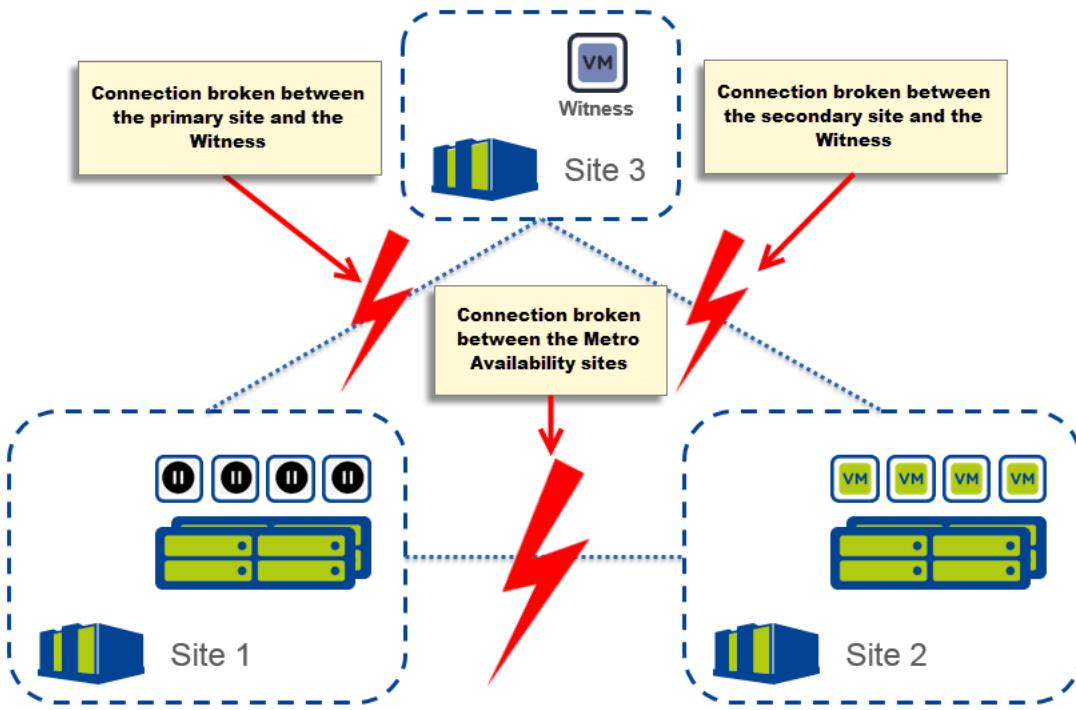


Figure: Network Complete Failure (both sites isolated)

### Additional Recovery Considerations

In addition to the recovery procedures described for each failure scenario, the following recovery considerations might apply:

- If the Witness VM goes down and is no longer recognized when it is restarted or a new Witness VM is created, it might be necessary to re-register the Witness VM.
- If there are any Metro Availability protection domains already in use, (1) change the failure handling to **Automation Resume** or **Manual**, (2) unregister the Witness VM, (3) register the Witness VM again with the default password on both clusters, and then (4) change the failure handling back to **Witness**.
- If the password is changed after the Witness VM is registered, the Witness VM credentials on the cluster must be updated. To do this, enter the following nCLI command:

```
nutanix@cvm$ ncli cluster update-witness id=id_number password=new_password
```

- After a site failure, consider the following:
  - Before promoting a remote cluster to be the primary site, first migrate any VMs on the primary cluster to the remote cluster.
  - It may take some time after the resync of the protection domains before the migration can complete successfully.
  - Review the DRS rules to make sure they do not conflict with a recovery scenario. For example, do not create DRS rules for the VMs to run only on the nodes that belong to a specific cluster (Site 1), because this would prevent the moved VMs from starting on the other cluster (Site 2) after an HA failover.

## Protection Domain Failover and Failback (Metro Availability)

The failover and fallback procedures are dependent on the nature of the failure and the site that has failed. You can perform the planned failover by using vMotion. If a disaster occurs, the recovery procedure is dependent on whether you have witness VM installed and enabled in your cluster or not.



**Note:** If you have witness VM installed and enabled, see [Recovery Procedures \(Witness VM installed\)](#) on page 293 for recovery workflows.

### Failing Over a Protection Domain Manually (Planned Failover)

You can use vMotion to move virtual machines to the standby site provides the highest uptime during planned failovers.

1. Configure the DRS setting to **Manual** to prevent live migration of VMs between sites.
2. Perform vMotion of VMs from site A to B.



**Note:** If any VMs remain on the hosts of site A, they will be disrupted during failover.

3. Change the DRS rules to have VM affinities to the hosts of the site B.
4. After configuring VM affinities, change the DRS setting to **Fully Automated**.
5. Login to the web console of site B, and select the metro availability protection domain and click **Promote**.

If you log in to the web console of site A, the metro availability protection domain will be in the **Decoupled** state. The datastore on the hosts of the site A should remain active, but it is in read-only state. It is not recommended to disable the protection domain on the site A as it can lead to the datastore being readable and writeable on both the sites, which can lead to VM inconsistency.

### Failing Over a Protection domain Manually (Disaster)

Perform the following steps to failover a protection domain in case of disaster (unplanned failover) to remote site (B) from primary site (A). If the site A has failed, all the writes are stopped on the active storage containers of site B.

If the primary site has failed, you can promote storage containers on site B. After you promote the storage containers, the storage containers become active again to the VMware HA cluster. VMware HA updates its compatibility list and virtual machines that reside in that storage container automatically gets powered on. VMware DRS “should run on” affinity rules is overridden and those virtual machines are allowed to restart in the surviving site. “Must run on” affinity rules are enforced and has to be updated to allow virtual machines to restart on site B.

1. Login to the Web console of site B.

2. Click **Promote**.

HA restart process continues for DRS “should” rules.

This operation does the following.

- Restores all VM files from the last acknowledge write before site A failed.
- Registers the VMs on the recovery site (site B) and power on the VMs.
- Marks the failover site protection domain as active.

## Re-enabling Metro Availability Configuration (Manually)

After the primary site recovers, it comes back in decoupled state and the datastores on the hosts of the primary site will be active, but it is in the read-only state. Perform the following steps to failback a protection domain from remote site (B) to primary site (A) for both planned and disaster failovers.

1. Login to the Web console of site A, and click **Disable**.
2. Disable DRS to ensure VMs are not moved to site A.
3. Login to the Web console of the site B and establish the metro availability configuration by clicking **Re-enable**.



**Note:** It changes the direction of the replication. Allow replication to finish.



### Caution:

- Perform the Re-enable operation immediately after clicking Disable on site A because during this phase the containers are mutable and can host the VMs. If an unexpected host failure occurs, it can start an HA event and you cannot prevent both the sites to run VMs easily and to perform writes on them, which can lead to data inconsistency, duplicated IP addresses, etc.
- Do not re-enable in the original metro availability direction because it can lead to inconsistency because of stale data on the original primary site.



**Note:** To revert to original replication direction (from A to B), perform the failover and re-enabling metro availability procedures again.

## Handling Secondary Site Failure Manually

Perform the following procedure to handle secondary site failure. You must have set the DRS rules to **Fully Automated** and configured VM affinities to the hosts of the primary site.

1. If you have configured metro availability with the manual setting, then login to the primary site and disable metro availability by clicking **Disable**.
2. If there are any VMs running on the secondary site (which is against the best practices), these should failover to the hosts of the primary site by using vSphere HA functionality.  
If there is network failure between the primary and secondary sites, there might be some VMs on the secondary site in the paused state.

## Handling Network Isolation (no Witness VM Installed)

Perform the following procedures depending on where the network isolation has occurred.

Context for the current task

1. Network Isolation of the Primary Cluster
  - a. Login to the Web console of the secondary site, and click **Promote**. The vSphere HA will start the VMs on the secondary site.
  - b. Set the DRS rules so that all the VMs have affinities set to the secondary site.
  - c. After restoring the network on the primary you need to destroy all the stale VMs that are still residing on the old primary as follows.

- Run the `esxcli vm process list` on every host of the old primary and note down the world ID of these stale VMs.
  - Run the `esxcli vm process kill -w world_id -t force` to destroy the stale VMs. Ensure that you only destroy the VMs on the datastore of metro availability protection.
- Manually change the protection domain state from **Decoupled** to **Disabled** on the original primary site.
  - Re-enable from the new primary to the intended secondary (old primary).
- 2. Network Isolation of the Secondary Cluster**
- If you have configured metro availability with the manual setting, then login to the primary site and disable metro availability by clicking **Disable**.
  - After restoring the network on the secondary re-enable from the primary site to the secondary site.

## Reconfiguring Data Protection in a Metro Availability and Async DR Configuration

If you are having a metro availability configuration from site A to site B and at the same time performing an Async DR from site A to site C for the same protection domain, and if site A fails you can use the following procedure to reconfigure data protection to keep replication going to site C.

- Login to the Web console of site B, and select the protection domain and click **Promote**.
- Establish Async replication from B to C as follows.
  - Create a remote site on B that points to C.
  - Create a remote site of C that points to B.
  - Create the snapshot schedule on site B by updating the protection domain of site B.



**Note:** This schedule should point to the remote site as site C.

## Upgrade Best Practices and Requirements with Metro Availability Enabled

Following are the best practices and requirements if you are planning to upgrade your cluster and have metro availability enabled.

- Nutanix support upgrade from N-2 versions only. All replications are forward and backward compatible up to N-2 version.
- You do not need to disable replications or disable metro availability during the upgrade process.
- You can upgrade either the primary or secondary site first.
- Cluster can host both active and standby protection domains during an upgrade.

## Cloud Connect (AWS and Azure)

You can configure AWS or Azure as a remote site for backup/restore operations. Before proceeding with configuration of AWS or Azure cloud as a remote site ensure that you have fulfilled all the account requirements of AWS or Azure.

- [Configuring a Remote Site \(AWS\)](#) on page 309
- [Configuring a Remote Site \(Azure\)](#) on page 312

## Cloud Connect Guidelines (AWS and Azure)

The cloud connect feature enables you to back up and restore copies of virtual machines and files to and from an on-premise cluster and a Nutanix Controller VM located on the Amazon Web Service (AWS) or Microsoft Azure cloud. The Nutanix Controller VM is created on an AWS or Azure cloud in a geographical region of your choice. It is a single-node cluster with a 30 terabyte (TB) disk attached to the node, with a usable disk capacity of 20 TB.



**Note:** For 4.6 or lower versions, the disk size of 100 TB gets attached to the node.

Amazon or Azure customers are charged only for capacity that is used (not charged for the full capacity). Once configured through the web console, the remote site cluster is managed and monitored through the Data Protection dashboard like any other remote site you have created and configured. To log in to the Nutanix Controller VM on the cloud, get the IP address from the Data Protection dashboard of the remote site cluster and SSH to the IP address from the source cluster Controller VM.

```
nutanix@cvm$ ssh nutanix@cloud_controller_vm
```

Amazon S3 is used to store data (extents) and Amazon Elastic Block Store (EBS) is used to store metadata. Users then use the Amazon management tools to manage and monitor billing and related usage. When the AWS Remote feature replicates a snapshot data to AWS, the Nutanix Controller VM on AWS creates a bucket on S3 storage. The bucket name will be ntnx-cluster\_id-cluster\_incarnation\_id-disk\_id.

Azure Blob storage is used to store data (extents) and Blob storage backed disk is used to store metadata. Users then use the Azure management tools to manage and monitor billing and related usage.

### Network and Port Requirements and Supported Features

Requirement/Feature	Description/Recommendation
Local cluster	The local cluster requires Internet connectivity and must be able to communicate with the public cloud.
Firewall port access	Ensure that you have configured your firewall to allow communication through the following ports: <ul style="list-style-type: none"><li>• TCP ports 2009/2020 - AOS communications</li><li>• UDP port 53 - DNS</li><li>• HTTPS port 443 - AWS or Azure communication</li><li>• TCP port 22 - SSH communication to Nutanix Controller VM</li></ul>
Name server	This feature requires that you configure a name server in the Prism web console.

Requirement/Feature	Description/Recommendation
VPN	Ensure that you have configured a VPN connection between AWS or Azure subnet and Nutanix local cluster before configuring the cloud remote site through Prism.
AWS Direct Connect	Supported
Azure Express Route	Supported

#### Cloud Connect Features

Feature	Description/Recommendation
Compression	You can choose to enable compression on the local storage container. Compression on wire is enabled by default and is also enabled by default when the remote AWS or Azure storage container is created.
Disaster recovery	Not currently supported.
Hypervisors	AWS and Azure are supported on all the three hypervisors (ESXi, Hyper-V, and AHV).
AOS Version	For AWS, NOS 4.1 or later AOS versions are supported. For Azure, AOS 4.5 or later versions are supported.
Replication type	You can configure multiple AWS or Azure Nutanix Controller VMs, where each Controller VM acts as a separate remote site. You can create instances in multiple AWS or Azure regions.

#### General Limitations and Recommendations

- It is recommended to have only one VM for each protection domain that is configured to replicate to a cloud remote site.
- It is not recommended to configure vStore protection domains and replication for backup with Cloud Connect feature.
- Do not use the Nutanix Web console of the Controller VM that is running on the cloud as it is not supported.
- Do not enable deduplication on the cloud instance.
- It is not recommended to enable deduplication on the source cluster.
- Do not use the *DoNotUse-sp* storage pool on the cloud instance to create containers.
- The credentials that are used for creating the cloud remote site cannot be deleted without deleting the cloud remote site.

#### AWS Account Requirements

Following are the account requirements for the AWS cloud.

## AWS Account Requirements

Requirement	Description/Recommendation
Credentials and permissions	<p>Nutanix recommends that you create a AWS account for the remote site.</p> <p>AWS remote site/cloud connect feature requires AWS credentials (access key and secret access key) for the corresponding AWS user to be configured. You can configure one of the following user types.</p> <ul style="list-style-type: none"> <li>• AWS root user having all the permissions.</li> <li>• Create an IAM user and assign the following permissions.</li> </ul> <p>EC2</p> <ul style="list-style-type: none"> <li>• AWS service: Amazon EC2</li> <li>• Actions: All actions</li> <li>• ARN:*</li> </ul> <p>S3</p> <ul style="list-style-type: none"> <li>• AWS service: Amazon S3</li> <li>• Actions: All actions</li> <li>• ARN:*</li> </ul>
Recommended access type	<p>Prism web console <b>Use VPN Connection</b></p> <ul style="list-style-type: none"> <li>• Nutanix recommends Virtual Private Cloud (VPC) access through an Amazon VPN Connection to the Nutanix Controller VM.</li> <li>• The Amazon VPC/VPN connect assigns a private static IP address to the Nutanix Controller VM which is used with cloud connect and persists if the remote Nutanix cluster restarts. The public IP address might change, but it does not affect any behavior because this address is only used for outbound S3 access.</li> <li>• If you select the <b>Use VPN Connection</b> option, ensure that you have configured: <ul style="list-style-type: none"> <li>• A VPN Connection as part of your Amazon VPC service</li> <li>• A VPN application, device, or server (known as a customer gateway) for your on-premise cluster</li> </ul> </li> </ul>



**Note:** You can also create and use VPC endpoints to simplify access to the Amazon S3 from within a VPC. These endpoints are easy to configure, highly reliable, and provide a secure connection to Amazon S3 that does not require the traffic to go through a public IP address. You do not need to make any change on the cloud Controller VM or local Nutanix cluster. For more information about configuring VPC Endpoint for Amazon S3, see *New – VPC Endpoint for Amazon S3* topic.

Requirement	Description/Recommendation
Alternate access type	<p>Prism web console <b>Create SSH Tunnel</b></p> <ul style="list-style-type: none"> <li>• This scenario is not supported for production use.</li> <li>• You can use a secure session shell (SSH) to access the AWS instance.</li> <li>• If you select SSH connectivity, the Nutanix Controller VM is reachable through its public IP address by using SSH.</li> </ul>
NTP and timezone	<p>Time on your source cluster and AWS instance should be correct. If NTP and timezone are not properly configured, connection to AWS might fail. For more information on configuring timezone and NTP, see <i>AWS documentation</i>.</p>

#### Azure Account Requirements

Following are the account requirements for the Azure cloud.

## Azure Account Requirements

Requirement	Description/Recommendation
Credentials and permissions	<p>Nutanix recommends that you create a dedicated Azure account for the remote site.</p> <p>Azure Remote Site/Cloud Connect uses certificate pair based authentication. You need to upload a client certificate (.cer file) that contains the public certificate and the private key (.pem/.pfx file) on the Nutanix cluster to perform Azure operations.</p> <p>To generate the certificate from the Unix or Linux machines.</p> <ol style="list-style-type: none"><li>1. Log in to the Unix or Linux machine.</li><li>2. Generate .pem file.</li></ol> <pre>\$ openssl req -x509 -nodes -days 365 -newkey rsa:2048 \ -keyout mycert.pem -out mycert.pem</pre> <ol style="list-style-type: none"><li>3. Generate the .cer file.</li></ol> <pre>\$ openssl x509 -inform pem -in mycert.pem -outform der \ -out mycert.cer</pre> <p>After you generate the .cer and .pem files, you need to upload .cer file (public certificate) on Azure portal and .pem file containing the public certificate and the private key on the Nutanix cluster to perform Azure operations..</p> <p>To upload .cer file on the Azure management portal, perform the following steps.</p> <ol style="list-style-type: none"><li>1. Log into the Azure management portal <a href="https://manage.windowsazure.com">https://manage.windowsazure.com</a>.</li></ol> <p> <b>Note:</b> Uploading certificate by using <a href="https://portal.azure.com">https://portal.azure.com</a> is not supported.</p> <ol style="list-style-type: none"><li>2. Go to <b>Settings</b> tab on the left pane.</li><li>3. Click <b>Management Certificate</b> tab.</li><li>4. Click <b>Upload</b>.</li><li>5. Select the .cer file and click <b>Upload</b>.</li></ol> <p>To upload the .pem/.pfx on the Nutanix cluster, see <a href="#">Configuring a Remote Site (Azure)</a> on page 312.</p>

Requirement	Description/Recommendation
Recommended access type	<p>Prism web console <b>Use VPN Connection</b></p> <ul style="list-style-type: none"> <li>Nutanix recommends virtual network access through an Azure VPN Connection to the Nutanix Controller VM.</li> <li>The Azure virtual network/VPN connect assigns a private static IP address to the Nutanix Controller VM that is used with cloud connect and persists if the remote Nutanix cluster restarts. The public IP address might change, but it does not affect any behavior because this address is only used for the outbound Blob store access.</li> <li>If you select the <b>Use VPN Connection</b> option, ensure that you have configured: <ul style="list-style-type: none"> <li>A VPN Connection as part of your Azure virtual network</li> <li>A VPN application, device, or server (known as a customer gateway) for your on-premise cluster</li> </ul> </li> </ul>
Virtual network requirements	<ul style="list-style-type: none"> <li>If you are using the new portal of Azure for creating the virtual network, select <b>Classic</b> as the deployment model from <b>Select a deployment model</b> drop-down menu.</li> <li>During the creation of the virtual network in Azure, select <b>Configure a site-to-site VPN</b> option. Do not select point-to-site VPN connection as it is not supported by Nutanix.</li> <li>Create virtual network referring to a standard Azure region. Do not create affinity-group based virtual network as it is not supported.</li> <li>Create at least one more subnet other than the gateway subnet in the virtual network.</li> <li>Configure a DNS in the virtual network to allow its VM to connect to the Internet.</li> </ul>
Alternate access type	<p>Prism web console <b>Create SSH Tunnel</b></p> <ul style="list-style-type: none"> <li>This scenario is not supported for production use.</li> <li>You can use a secure session shell (SSH) to access the Azure instance.</li> <li>If you select SSH connectivity, the Nutanix Controller VM is reachable through its public IP address by using SSH.</li> </ul>

## Configuring a Remote Site (AWS)

### Before you begin:

- See [Cloud Connect Guidelines \(AWS and Azure\)](#) on page 304.
- See [AWS Account Requirements](#) on page 305.
- Ensure that you have configured a name server on the local Nutanix cluster through the web console. See [Configuring Name Servers](#) on page 570 in the *Web Console Guide*.

- In the [Data Protection dashboard](#), click **+Remote Site > Cloud**. The *Cloud Site* dialog box appears.
- Select the **AWS** option, and click **Next**.
- Click **Add New Key** to set the Amazon credentials for the remote site.
  - Type a name for this set of credentials in the **Name** text box.

- b. Type the **Access Key ID** and **Secret Access Key** in their respective fields.
- c. Click **Save**.
- d. (Optional) Click **Add New Key** to enter another set of Amazon credentials for each additional dedicated Nutanix Controller VM (for example, if you are configuring multiple AWS Nutanix Controller VMs, where each Controller VM is managed individually as a separate remote site).
4. Click **Next** to go to the *Remote Site Settings* dialog box.
5. If you select **VPN/Direct-connect** to configure a VPC/VPN or AWS direct connect connection to the Amazon cloud as follows.

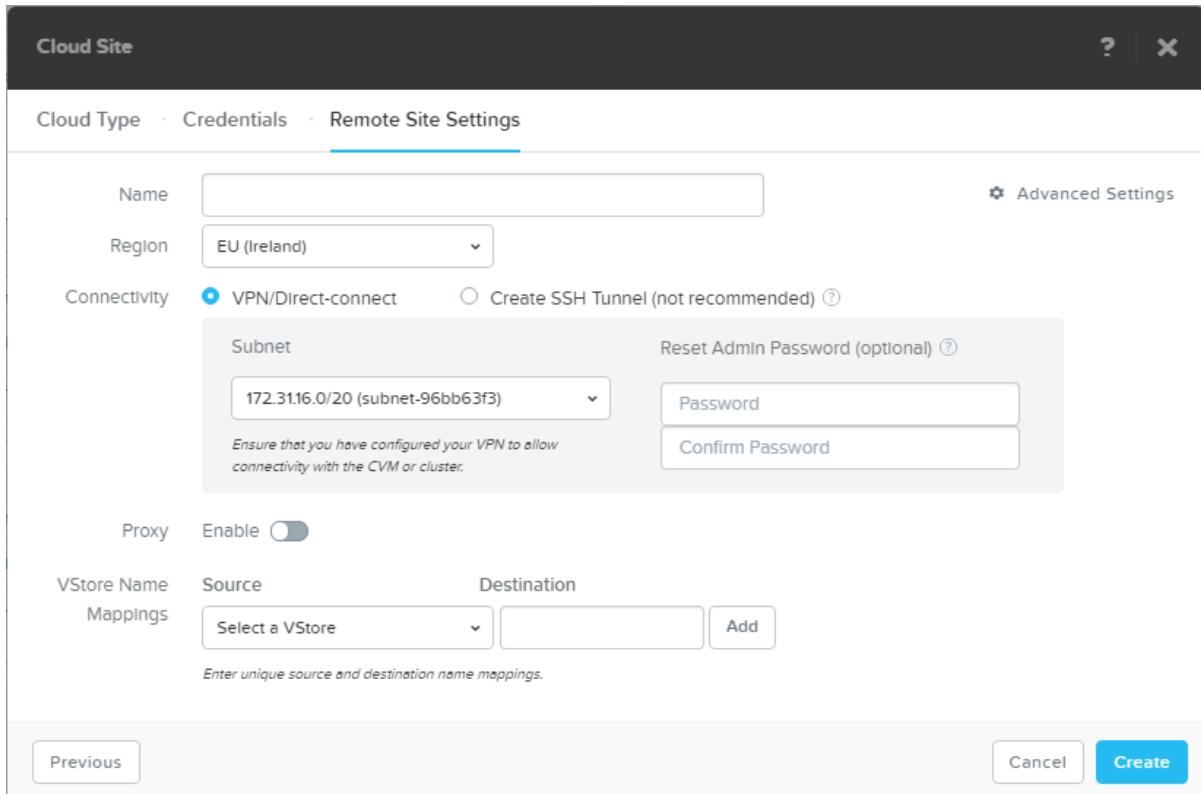


Figure: Remote Site Configuration Wizard for VPN to Amazon AWS

- a. **Name:** Type a remote site name.



**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), Simplified Chinese, decimal digits (0-9), dots (.), hyphens (-), and underscores (\_).

- b. **Region.** From the drop-down menu, select the Amazon region where your Amazon VPC/VPN location is configured.
- c. **Subnet.** This field automatically loads all the subnets on your AWS region. Select the subnet in which you want to create the Controller VM.

- d. **Reset Admin Password (optional).** Create a new administrator password for the nutanix user account on the cloud-based Nutanix cluster.
- e. **Proxy.** Enable to allow addresses in the subnet to be used as a proxy to communicate with other Nutanix components on the remote site. Enabling the proxy is recommended when you have different subnets on primary and secondary sites.
- f. **VStore Name Mappings.** Select a local storage container from the **Source** drop-down menu, type the remote storage container name, and then click **Add**. This entry maps the association between a local source storage container and a remote target storage container at the remote site. Multiple storage containers are supported.
- If you perform restore of snapshots on vStore protection domains, you need to modify the VMDK paths in the VM files and point it to the restored path that is specified as part of the restore operation.
- g. (Optional) Click **Advanced Settings** to configure compression of data.
- **Compress on wire.** Enabled by default. Enable this setting if you want to compress data on the cluster before transmitting it. Data is decompressed on the remote cluster.
- h. Click **Create**.
6. If you select **Create SSH Tunnel** for configuring a SSH tunnel connection to the Amazon cloud, do the following.
- 
- Figure: Remote Site Configuration Wizard for SSH to Amazon AWS*
- a. **Name:** Type a remote site name.



**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), Simplified Chinese, decimal digits (0-9), dots (.), hyphens (-), and underscores (\_).

- b. **Region.** From the drop-down, select the Amazon region where your Amazon location is configured.
- c. **Subnet.** This field automatically loads all the subnets on your AWS region. Select the subnet in which you want to create the Controller VM.
- d. **Set up an Admin Password.** Create a new administrator password for the nutanix user account on the cloud-based Nutanix cluster. This field is required.
- e. **Proxy.** Enable to allow addresses in the subnet to be used as a proxy to communicate with other Nutanix components on the remote site. Enabling the proxy is recommended when you have different subnets on primary and secondary sites.
- f. **Use SSH Tunnel.** Enable an SSH tunnel.
- g. **SSH Port.** Type an SSH port number for the SSH tunnel. Valid range is 3000 to 3099.
- h. **VStore Name Mappings.** Select a local storage container from the **Source** drop-down, type the remote storage container name, then click **Add**. This entry maps the association between a local source storage container and a remote target storage container at the remote site. Multiple storage containers are supported.
- i. (Optional) Click **Advanced Settings** to configure compression of data.
  - **Compress on wire.** Enabled by default. Enable this setting if you want to compress data on the cluster before transmitting it. Data is decompressed on the remote cluster.
- j. Click **Create**.

The Prism web console displays a message similar to `Remote site remote_site_name has been initiated successfully.`

The remote site initiation and creation takes about 10 minutes. You can see the initiation, creation, and results in the web console Progress Monitor.

**What to do next:** You have now created a remote site that can be used just like any other remote site for use with data protection.

#### Configuring a Remote Site (Azure)

##### Before you begin:

- See [Cloud Connect Guidelines \(AWS and Azure\)](#) on page 304.
- See [Azure Account Requirements](#) on page 307.
- Ensure that you have configured a name server on the local Nutanix cluster through the web console. See [Configuring Name Servers](#) on page 570 in the *Web Console Guide*.

1. In the [Data Protection dashboard](#), click **+Remote Site > Cloud**.  
The *Cloud Site* dialog box appears.
2. Select the **Azure** option, and click **Next**.
3. Click **Add New Credential** to set the Azure credentials for the remote site.
  - a. Type a name for this set of credentials in the Name text box.

- b. Enter the **Subscription ID** of your Azure account.
  - c. Select the public certificate of the Azure portal (.pem file) by clicking **Choose File** button.
  - d. (Optional) Click **Add New Credential** to enter another set of Azure credentials for each additional dedicated Nutanix Controller VM (for example, if you are configuring multiple Azure Nutanix Controller VMs, where each Controller VM is managed individually as a separate remote site).
  - e. Click **Save**.
4. Click **Next** to go to the *Remote Site Settings* dialog box.
5. If you select **VPN/Express-route** to configure a VPC/VPN or express route connection to the Azure cloud, do the following.

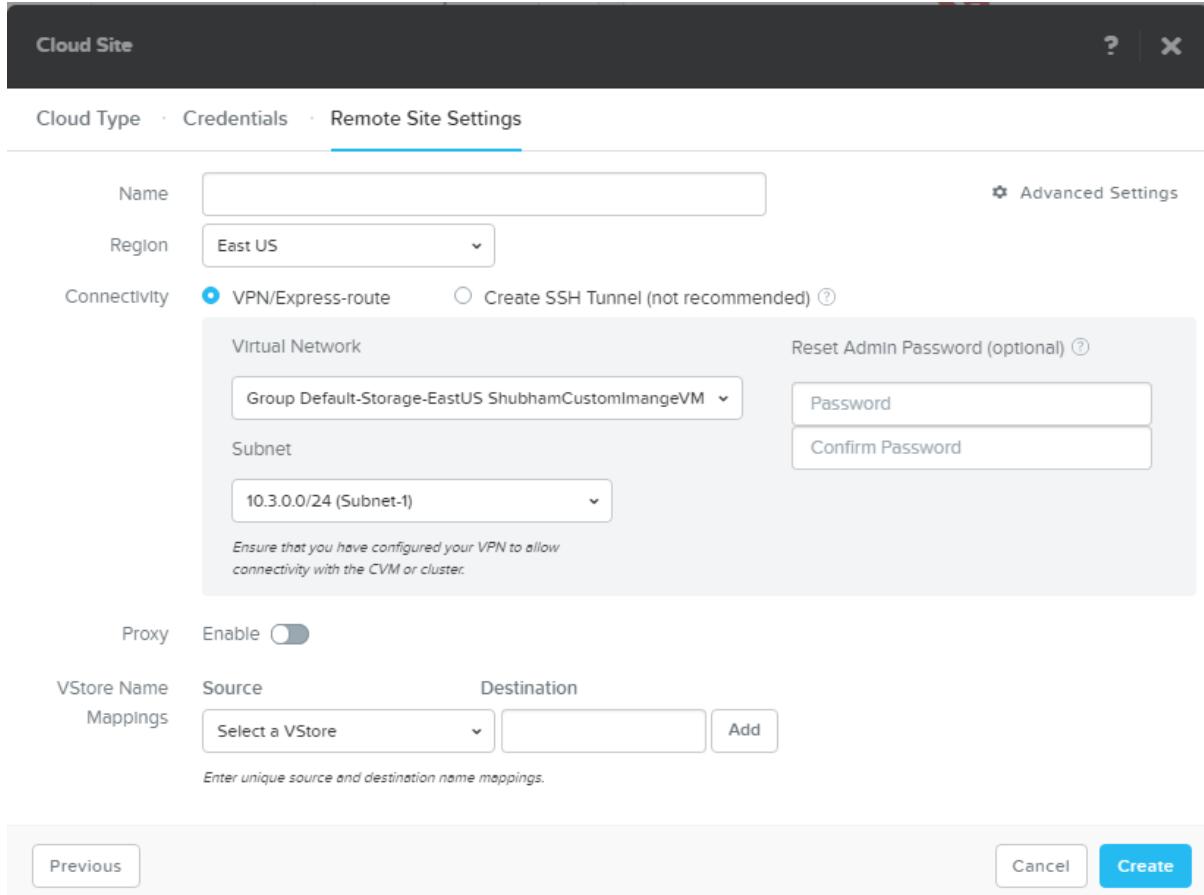


Figure: Remote Site Configuration Wizard for VPN to Microsoft Azure

- a. **Name:** Type a remote site name.



**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), Simplified Chinese, decimal digits (0-9), dots (.), hyphens (-), and underscores (\_).

- b. **Region.** From the drop-down, select the Azure region where your Azure virtual network location is configured.

- c. **Virtual Network:** This field is automatically loads with the virtual network based on your Azure region. Otherwise, select the virtual network from the drop-down menu.
- d. **Subnet.** This field automatically loads all the subnets on your Azure region. Select the subnet in which you want to create the Controller VM.



**Note:** In addition to the gateway subnet, you need to configure additional subnets on the Azure virtual network configuration as the gateway subnet cannot be used to deploy the VMs. If you have configured only the gateway subnet, your VPN tunnel will work but during the configuration of the remote site for the protection domain No subnets available message is displayed on the Prism Web console.

- e. **Reset Admin Password (optional).** Create a new administrator password for the nutanix user account on the cloud-based Nutanix cluster.
  - f. **Proxy.** Enable to allow addresses in the subnet to be used as a proxy to communicate with other Nutanix components on the remote site. Enabling the proxy is recommended when you have different subnets on primary and secondary sites.
  - g. **VStore Name Mappings.** Select a local storage container from the **Source** drop-down menu, type the remote storage container name, and then click **Add**. This entry maps the association between a local source storage container and a remote target storage container at the remote site. Multiple storage containers are supported.  
If you perform restore of snapshots on vStore protection domains, you need to modify the VMDK paths in the VM files and point it to the restored path that is specified as part of the restore operation.
  - h. (Optional) Click **Advanced Settings** to configure compression of data.
    - **Compress on wire.** Enabled by default. Enable this setting if you want to compress data on the cluster before transmitting it. Data is decompressed on the remote cluster.
  - i. Click **Create**.
6. If you select **Create SSH Tunnel** for configuring a SSH tunnel connection to the Azure cloud, do the following.

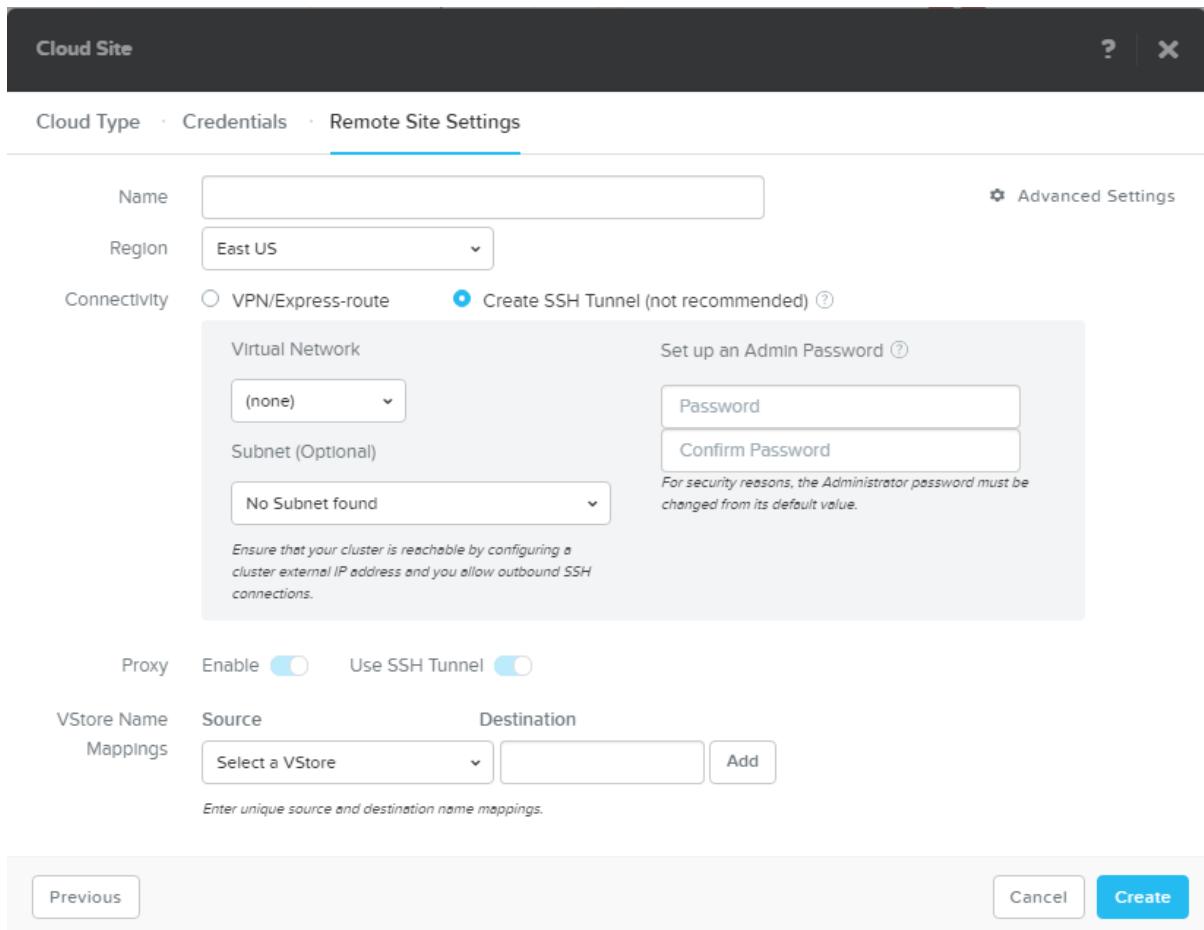


Figure: Remote Site Configuration Wizard for SSH to Azure

- a. **Name:** Type a remote site name.



**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), Simplified Chinese, decimal digits (0-9), dots (.), hyphens (-), and underscores (\_).

- b. **Region.** From the drop-down, select the geographical Azure region.

- c. (Optional) **Virtual Network:** This field automatically loads with the virtual network based on your Azure region. Otherwise, select the virtual network from the drop-down menu.

- d. (Optional) **Subnet.** This field automatically loads all the subnets on your Azure region. Select the subnet in which you want to create the Controller VM.

- e. **Set up an Admin Password.** Create a new administrator password for the nutanix user account on the cloud-based Nutanix cluster. This field is required.

- f. **Proxy.** Enable to allow addresses in the subnet to be used as a proxy to communicate with other Nutanix components on the remote site. Enabling the proxy is recommended when you have different subnets on primary and secondary sites.

- g. **Use SSH Tunnel.** Enable an SSH tunnel.

- h. **SSH Port.** Type an SSH port number for the SSH tunnel. Valid range is 3000 to 3099.
- i. **VStore Name Mappings.** Select a local storage container from the **Source** drop-down menu, type the remote storage container name, and then click **Add**. This entry maps the association between a local source storage container and a remote target storage container at the remote site. Multiple storage containers are supported.
- j. (Optional) Click **Advanced Settings** to configure compression of data.
  - **Compress on wire.** Enabled by default. Enable this setting if you want to compress data on the cluster before transmitting it. Data is decompressed on the remote cluster.
- k. Click **Create**.

The Prism web console displays a message similar to `Remote site remote_site_name has been initiated successfully.`

The remote site initiation and creation takes about 10 minutes. You can see the initiation, creation, and results in the web console Progress Monitor.

**What to do next:** You have now created a remote site that can be used just like any other remote site for use with data protection.

#### Upgrading Nutanix Controller VM on Cloud

If you are planning to upgrade the cloud Nutanix Controller VM on cloud to 5.1.x or later versions, use the following procedure.

For cloud Controller VM upgrade, you must be on the N-2 or later version of AOS release. For example, if you are upgrading to AOS 5.1, your cloud Controller VM must be on AOS 4.7.x or later release.

##### Before you begin:

- Before you start the upgrade process, delete any existing install directory in `/home/nutanix` by running the `nutanix@cvm$ rm -rf /home/nutanix/install` command.
- Download the latest AOS build and metadata JSON file from the Nutanix support portal at the **Downloads** link and copy it to cloud Controller VM at the `/home/nutanix` directory.

1. Run the following command to unzip and extract the upgrade script to the `install/bin` directory.

```
nutanix@cvm$ tar zxf build.tar.gz install/bin/upgrade_cloud_cvm
```

2. Run the following command to upgrade the cloud Controller VM.

```
nutanix@cvm$ install/bin/upgrade_cloud_cvm --installer_file=build_file.tar.gz \
--metadata_file=json_file.json
```



**Note:** If you are upgrading your Nutanix Controller VM on cloud to any previous version (example AOS 5.0 or 4.7), see the relevant topic for the specific release in the *Prism Web Console* guide.

The upgrade procedure may take up to one hour to complete. The cloud Controller VM restarts at the end of the upgrade process. Run the `upgrade_status` command to verify that upgrade is successfully completed.

#### Instance Types for AWS and Azure

Nutanix supports following instance types for AOS 5.0 or later releases. If you are replicating more than 10TB (maximum of 20 TB) of data on both AWS and Azure, you need to update your instance type.

## Supported Instance Types

Cloud Type	Default	Limit	
AWS	For all the regions	m3.2xlarge	Up to 20 TB.
Azure	For all the regions	Standard_D12_v2	Up to 20 TB.



**Note:** If you have upgraded the cloud instance, it is recommended to upgrade the instance type to the one mentioned in the table.

## Recovery Procedures by using Cloud Connect

If for some reason the entities on the primary cluster fails, you can recover the entities by using the snapshots that are being replicated to the AWS or Azure. If your primary cluster fails altogether, you can create a new cluster and use the snapshots residing on the AWS or Azure to recover the cluster.

The process of restoring protected entities from the AWS or Azure is same as the way you restore entities for the normal cluster.

1. To recover the entities, login to the Prism and follow the steps described in the Restoration of Protected Entities, see [Restoration of Protected Entities](#) on page 264.
2. To recover the cluster, see [Recovering from the Remote Snapshots on a Backup or DR Site](#) on page 325 for more information.

## Remote Site Configuration

A remote site is the target location to store data replications for protected domains (see [Configuring a Protection Domain \(Async DR\)](#) on page 256). The remote site can be one of the following:

- another physical cluster (see [Configuring a Remote Site \(Physical Cluster\)](#) on page 317)
- a public cloud provider
  - AWS (see [Configuring a Remote Site \(AWS\)](#) on page 309)
  - Azure (see [Configuring a Remote Site \(Azure\)](#) on page 312)

### Configuring a Remote Site (Physical Cluster)

**Before you begin:** For using network mapping, create the network connections and VLANs on both source and destination cluster. For more information about configuring network connections, see [Configuring Network Connections](#) on page 151.

A remote site is the target location to store data replications for protected domains (see [Configuring a Protection Domain \(Async DR\)](#) on page 256). The remote site can be either another physical cluster or a cluster located in a public cloud. To configure a remote physical cluster that can be used as a replication target, do the following:



**Note:** Do not create multiple remote sites pointing to the single destination cluster. Otherwise, an alert will be generated.

1. In the Data Protection dashboard (see [Data Protection Dashboard](#) on page 237), click the **Remote Site** button and then select **Physical Cluster** from the pull-down list.  
The *Remote Site* dialog box appears.

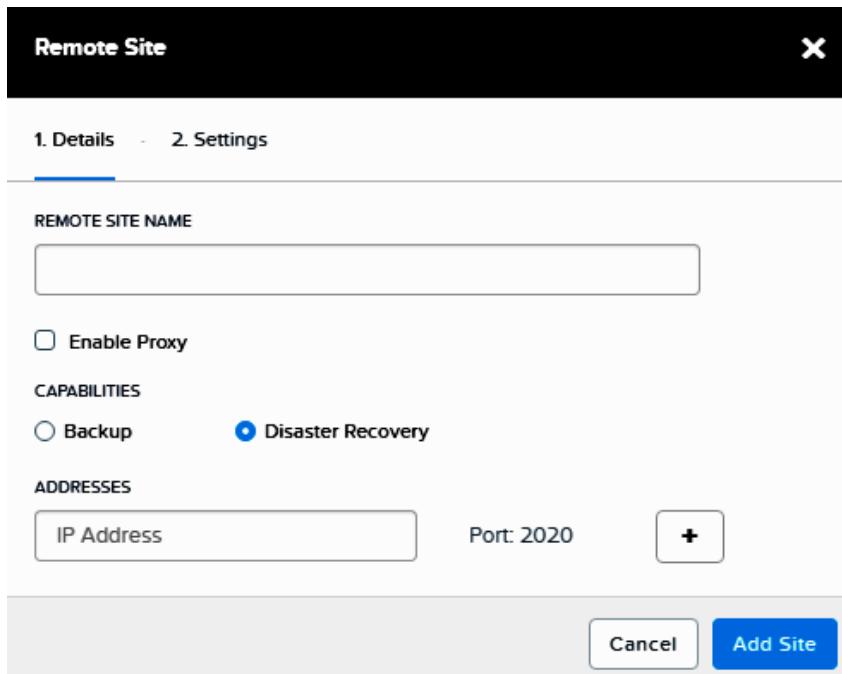


Figure: Remote Site Window

2. Do the following in the indicated fields:

a. **Remote Site Name:** Enter the remote site host name.



**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), Simplified Chinese, decimal digits (0-9), dots (.), hyphens (-), and underscores (\_).

b. **Enable Proxy:** Check the box to enable a proxy.

No proxy is used by default. Enabling this field allows addresses specified in the address list to be used as a proxy to communicate with a Nutanix cluster on the remote site. The proxy should be enabled when the remote Controller VMs are not reachable directly from the source cluster. In this case, the source cluster communicates with the remote proxy IP, which forward the requests to the appropriate remote Controller VMs. The proxy setting on the remote site limits the replication traffic to the defined destination remote site IP rather than to each individual Controller VM IP in the destination cluster. NAT performed by any device in between the two Nutanix clusters is not currently supported.



**Caution:** Do not enable a proxy on remote sites that will be used with a metro availability protection domain.

c. **Use SSH Tunnel:** Check the box to enable an SSH tunnel for secure transmission between the local cluster and the remote site.



**Note:** Use of the SSH tunnel reduces replication throughput because of the CPU overhead for encryption/decryption and is not recommended for production environments. The primary purpose of the SSH tunnel is to provide a secure option when using the cloud connect feature.

d. **Backup:** Select this option to enable backup (only) to this site.

Backup allows the remote site to be used as a backup (replication) target. This means data can be backed up to this site and snapshots can be retrieved from the site to restore locally, but failover protection (that is, running failover VMs directly from the remote site) is not enabled.



**Note:** Use only this option if you are creating single-node replication target remote site.

**e. Disaster Recovery:** Select this option to enable backup to and recovery from this site.

Disaster recovery allows the remote site to be used both as a backup target and as a source for dynamic recovery. This means that failover VMs can be run directly from the remote site.



**Note:** This option is not supported if you are creating single-node replication target remote site.

**f. Addresses:** Enter the virtual IP address of the remote site cluster and port number and then click the **Add** button.

If you do not include a port number, a default port is used. The default address port numbers are 2009 and 2020.



**Note:** Ensure that virtual IP address and the cluster nodes on the remote cluster is in the same subnet.

- To configure additional parameters, click the **Add Site** button and do the following in the indicated fields:

**Remote Site**

**1. Details** - **2. Settings**

**Bandwidth Throttling**

BANDWIDTH THROTTLING

DEFAULT BANDWIDTH LIMIT

Enter the maximum bandwidth in megabytes per second (up to 2 decimal places).

BANDWIDTH THROTTLING POLICIES

No policy found

+ Add Policy

**Compression**

COMPRESS ON WIRE

**Mappings**

VSTORE NAME MAPPING

vStores have not been defined.

Cancel Save

- a. If you want to define a bandwidth policy, set the **Bandwidth Throttling** button to enabled.

The bandwidth throttling policy provides you with an option to set the maximum limit of the network bandwidth. You can specify the policy depending on the usage of your network. For example, you can define a policy that a Nutanix cluster should replicate data from site A to site B at less than 10 MBps between 9 a.m. to 5 p.m. on weekdays because there might be other critical traffic between the two sites at that time.

- b. **Default Bandwidth Limit:** Enter the maximum bandwidth allowed (in MBps) that should be used for replication purpose if no bandwidth policy is applied.



**Note:** Maximum bandwidth of 2048 MBps is only supported for replication purpose.

Leaving the field blank means there is no restriction on bandwidth use.

- c. Click **Add Policy** to configure the bandwidth throttling policy.

The screenshot shows a dialog box titled "Remote Site". At the top, there are tabs for "1. Details" and "2. Settings", with "2. Settings" being the active tab. Below the tabs, the title "Configure Bandwidth Throttling Policy" is displayed. Under "BANDWIDTH LIMIT", there is a text input field with the placeholder "MBPS Up to 2 decimal places". Under "DURATION", there are two radio button options: "All day" (selected) and "Specific duration (Based on the cluster's time zone: US/Pacific)". Under "REPEAT", there is a weekly repeat selector with days Su, M, T, W, Th, F, S, where Su, M, T, W, Th, and F are highlighted in blue. At the bottom right of the dialog are "Cancel" and "Save" buttons.

1. Enter the maximum bandwidth allowed (in MBps) for transmitting the replicated data to the remote site in the **Bandwidth Limit** text box.



**Note:** Maximum bandwidth of 2048 MBps is only supported for replication purpose.

2. Select **All day** (default) to apply the bandwidth specified for the entire day and for the entire week. Otherwise, select the days that you want to apply the bandwidth throttling. To specify the days that you want to apply bandwidth policy for the entire day, click and de-select the days that you do not want to apply the policy.
3. Select **Specific time** and specify the time and also the days that you want to use the bandwidth throttling. For example, you can specify the maximum bandwidth limit of 10 MBps between 9 a.m. to 5 p.m. from Monday to Friday.
4. Click **Save**.

- d. **Compress on Wire:** Click the **Yes** button to enable compression on wire (also known as network compression).

Data compression during transit (on wire) between sites is not used by default. Enabling compression on wire consumes additional CPU resources.

- e. **Network Mapping:** Select the VLAN ID from the source and destination cluster drop-down menu

All the VLANs that are available on the source and destination cluster are mapped in the drop-down menu. For example, if VLAN01 is configured on the source cluster and VLAN02 is configured on the destination cluster. If you select VLAN01 on the source cluster and VLAN02 on the destination cluster, in failover scenario, a VM that is running in VLAN01 on the source cluster is automatically brought up in VLAN02 on the destination cluster.

- f. **vStores:** To specify a vStore, select the source storage container from the pull-down list that contains the VMs to protect, enter the destination storage container name on the remote site, and then click the **Add** button. Repeat for additional vStore entries.

Each **vStores** entry maps the association between a local source storage container and a remote target storage container at the remote site.



**Note:** If you perform restore of snapshots on vStore protection domains, you need to modify the VMDK paths in the VM files and point it to the restored path that is specified as part of the restore operation.

4. When all the field entries are correct, click the **Save** button.



**Note:** The local cluster must also be configured as a remote site on the remote cluster in order to use the remote site as a target location to store data replications. If this is not currently the case, log into the remote cluster and configure the local cluster as a remote site for that cluster.

## Modifying a Remote Site (Physical Cluster or Cloud)

You can monitor or modify an existing remote site (see [Configuring a Remote Site \(Physical Cluster\)](#) on page 317) by testing the network connection, updating the remote site settings, or deleting the remote site configuration. To modify a remote site, do the following:

 **Note:** Before you delete a remote cloud-based site, ensure you have saved any critical data and then delete the remote VM snapshots from the remote site. Otherwise, when you delete the remote site as described in this topic, the remote snapshots are automatically deleted.

1. In the Data Protection dashboard, click the **Table** view.

2. Click the **Remote Site** tab and select the target remote site in the table (top section of screen).

The Summary line (middle of screen) displays the remote site with a set of action links on the right. The actions are **Test Connection**, **Update**, and **Delete**. The following steps describe how to perform each action.

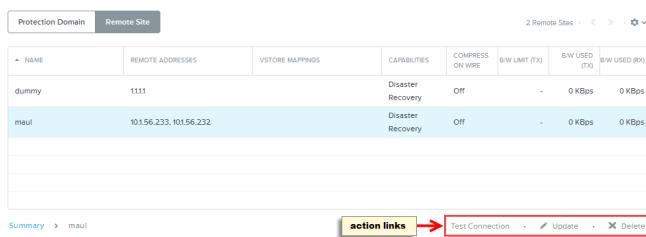


Figure: Remote Site Action Links

3. To verify a network connection, click the **Test Connection** action link.

This invokes an RPC call to the remote site, which checks whether the remote site is alive and accessible. A green check mark  appears if the connection test succeeds; a red  appears if the connection test fails. Check the alert log for potential problems if the test fails.

4. To update the remote site settings (physical cluster), click the **Update** action link. Update the settings in the dialog box as desired and then click the **Save** button.

The Remote Site window appears, which includes the same fields that appear when configuring a remote site (see [Configuring a Remote Site \(Physical Cluster\)](#) on page 317).

5. To update the remote site settings (cloud), click the **Update** action link.

The Remote Site window appears, which includes the same fields that appear when configuring a remote site (see [Cloud Connect Guidelines \(AWS and Azure\)](#) on page 304). Additionally, you can configure bandwidth throttling.

 **Note:** You can only configure bandwidth throttling only while updating the remote site. This option is not available during the configuration of remote site.

- a. If you want to define a bandwidth policy, set the **Bandwidth Throttling** button to enabled.

The bandwidth throttling policy provides you with an option to set the maximum limit of the network bandwidth. You can specify the policy depending on the usage of your network. For example, you can define a policy that a Nutanix cluster should replicate data from site A to site B at less than 10 MBps between 9 a.m. to 5 p.m. on weekdays because there might be other critical traffic between the two sites at that time.

- b. **Default Bandwidth Limit:** Enter the maximum bandwidth allowed (in MBps) that should be used for replication purpose if no bandwidth policy is applied.

 **Note:** Maximum bandwidth of 2048 MBps is only supported for replication purpose.

Leaving the field blank means there is no restriction on bandwidth use.

- c. Click **Add Policy** to configure the bandwidth throttling policy.

The screenshot shows a dialog box titled 'Remote Site' with a tab bar at the top labeled '1. Details' and '2. Settings'. The '2. Settings' tab is selected. Below it, the title 'Configure Bandwidth Throttling Policy' is displayed. Under 'BANDWIDTH LIMIT', there is a text input field with the placeholder 'MBPS Up to 2 decimal places'. Under 'DURATION', there are two radio button options: 'All day' (selected) and 'Specific duration (Based on the cluster's time zone: US/Pacific)'. Under 'REPEAT', there is a weekly repeat selector showing days Su, M, T, W, Th, F, S, where Su, M, T, W, Th, and F are highlighted in blue. At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

1. Enter the maximum bandwidth allowed (in MBps) for transmitting the replicated data to the remote site in the **Bandwidth Limit** text box.



**Note:** Maximum bandwidth of 2048 MBps is only supported for replication purpose.

2. Select **All day** (default) to apply the bandwidth specified for the entire day and for the entire week. Otherwise, select the days that you want to apply the bandwidth throttling. To specify the days that you want to apply bandwidth policy for the entire day, click and de-select the days that you do not want to apply the policy.
  3. Select **Specific time** and specify the time and also the days that you want to use the bandwidth throttling. For example, you can specify the maximum bandwidth limit of 10 MBps between 9 a.m. to 5 p.m. from Monday to Friday.
  4. Click **Save**.
- 
6. To delete a remote site, click the **Delete** action link. A window prompt appears; click the **OK** button to delete the remote site.  
The deleted site disappears from the list of remote sites in the table.

## Network Mapping

Network mapping allows you to control network configuration for the VMs when they are started on the remote site. By using network mapping feature, you can specify network mapping between the source cluster and the destination cluster. The remote site wizard provides you with an option to create one or more network mappings and allows you to select source and destination network from the drop-down list. You can also modify or remove network mappings as part of modifying the remote sites.



**Note:** You need to manually create network mapping on both the sites as part of remote site creation (source and destination cluster).

Periodic synchronization of network mapping between remote sites occurs and it ensures the sanity of the network mapping. Any modification on either site is reflected on another site.



**Note:** Currently, only L2 network configuration mapping is supported.



**Note:** Network mapping is supported for AHV and for cross-hypervisor VM mobility between ESXi and Acropolis. For more information about cross hypervisor VM mobility, see [Nutanix Cross Hypervisor Disaster Recovery](#) on page 331.

If you configure network mapping between source and remote sites, in case of failover the VMs are registered on the remote site with the network configuration that is specified in the network mapping. An example of one of the scenario is as follows.

1. VMs are running on the source cluster on VLAN01.
2. On the remote site (destination cluster), VLAN02 network is present.
3. Network mapping is implemented between VLAN01 and VLAN02.
4. Snapshots are getting replicated from the source cluster to the destination cluster.
5. In case of failover of this protection domain to the remote site, all the VMs which were on VLAN01 on source cluster gets registered with VLAN02 on remote site automatically.

For more information about configuring networking mapping on remote sites, see [Configuring a Remote Site \(Physical Cluster\)](#) on page 317.

### Network Mapping Behavior for AHV-Managed VMs After Failover/Disaster Recovery Migration

In some cases, after failover or DR-related migration to a remote site, a VM is registered without any network configuration or virtual network card (vNIC). A VM can be registered without any network configuration if these conditions are met:

- You have specified a network mapping in the remote site.
- The VM is migrated to the remote site.
- The network where the migrated VM is mapped has changed or no longer exists.

AOS networking mapping helps ensure that migrated VMs are registered on the new network with an IP address in most cases.



**Note:** If a VM is configured with multiple vNICs and no mapping exists for one of the vNICs or AHV is unable to assign an IP to the vNIC on the destination site, the entire registration defaults to "VM registered wthout a vNIC".

### VM IP Address Registration Scenarios

Source IP Address Management (IPAM)	Destination IPAM	Same Subnet?	Destination DHCP Pool?	VM IP Address Registration Result
No	No	Not applicable	Not applicable	VM registered normally
No	Yes	Not applicable	Yes	VM registered with a randomly-selected IP address from the DHCP pool

Source IP Address Management (IPAM)	Destination IPAM	Same Subnet?	Destination DHCP Pool?	VM IP Address Registration Result
Yes	No	Not applicable	Not applicable	VM registered normally
Yes	Yes	Yes	Not applicable	VM registered with original IP address
Yes	Yes	No	No	VM registered without a vNIC
Yes	Yes	No	Yes	VM registered with a randomly-selected IP address from the DHCP pool

## Recovering from the Remote Snapshots on a Backup or DR Site

When you have an existing backup or DR setup in your environment and the primary cluster is unavailable, then you can recover the cluster from the snapshots that are residing on a remote backup or DR site.

- If you have configured a backup site, for example Cloud Connect or Single-Node Replication Target, follow the below procedure.
- If you have configured a DR site, see [Failing Over a Protection Domain](#) on page 267 for recovery procedures.



**Note:** On AHV, if you are recovering from a snapshot that is retrieved from a cloud remote site, the VMs are recovered without any network attached.

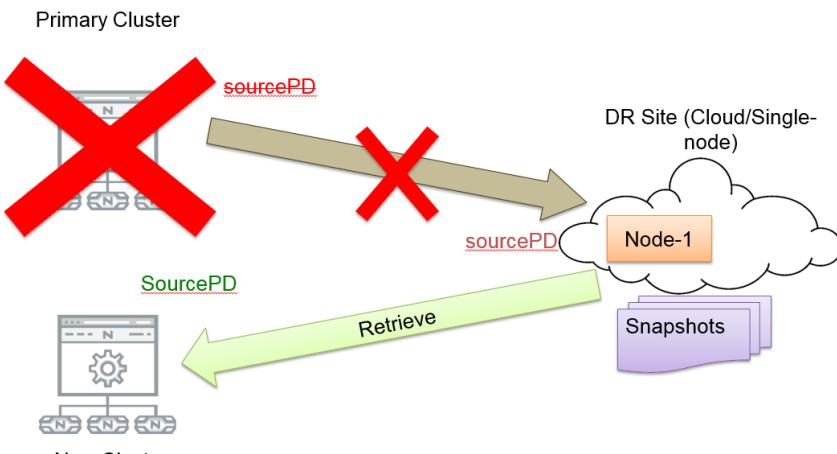


Figure: Cluster Recovery

- Create a new cluster.  
For more information on creating a new cluster, see the *Field Installation Guide*.
- To configure the existing backup site (Cloud Connect or Single-Node Replication Target) on the new cluster, go to **Data Protection > Remote Site** and select **Physical Cluster**. For more information about adding a remote site, see [Remote Site Configuration](#) on page 317.

- For Single-Node Replication Target cluster as backup, you need to perform the same procedure. You need to log into Single-Node Replication Target clusters and configure the new cluster as a remote site for that cluster. For more information about adding a remote site, see [Remote Site Configuration](#) on page 317.
- For Cloud Connect clusters (AWS or Azure) as backup, existing Controller VM located on the AWS or Azure cloud should be configured as remote site as follows.

- Login to the Controller VM of the new cluster and run the following command.

```
nutanix@cvm$ ncli rs create name=remote_site_name_AWS/Azure \
address-list=cvm_ip_AWS/Azure_instance capabilities=backup \
vstore-map=vstore_mapping enable-compression=1 \
cloud-type=AWS/Azure region=region_code_AWS/Azure
```

For example, for AWS:

```
nutanix@cvm$ ncli rs create name=amazon \
address-list=cvm_ip (private IP) of AWS instance capabilities=backup \
vstore-map=Container-1:backup_ctrl enable-compression=1 cloud-type=AWS region=us-east-1
```

- Login to the Controller VM of the AWS or Azure instance and run the following command.

```
nutanix@cvm$ ncli rs create name=new_cluster_name \
address-list=virtual_ip_new_cluster capabilities=backup \
vstore-map=vstore_mapping enable-compression=1
```

For example,

```
nutanix@cvm$ ncli rs create name=test address-list=virtual IP address of new cluster \
capabilities=backup vstore-map=backup_ctrl:Container-1 enable-compression=1
```

- Create a protection domain on the new cluster with the same name as in the primary cluster.

For more information on creating a protection domain, see [Configuring a Protection Domain \(Async DR\)](#) on page 256.

- Select the protection domain, and click the **Remote Snapshots** tab.

You should be able to see the snapshots that you have replicated to the backup site. You can then retrieve and restore from the snapshots on the new cluster.

## Synchronous Replication

Synchronous Replication is a feature where data is synchronously replicated between two sites in metro availability configuration. In an event of a disaster on any one site, real-time data is available on the other site.

The protection domain can be configured for metro availability or for synchronous replication depending on the following:

- Metro availability: The hypervisor is ESXi and the metro availability requirements for a single vSphere cluster across the sites and vSphere HA are satisfied. For more information on metro availability configuration, see Metro Availability tab section of [Data Protection Table View](#) on page 239 topic and to configure metro availability, see [Configuring a Protection Domain \(Metro Availability\)](#) on page 274.
- Synchronous replication: The hypervisor is either ESXi (not setup for metro availability) or Hyper-V.



**Note:** Metro Availability and synchronous replication are now supported across different hardware vendors (NX/SX, Dell, or Lenovo). You can also establish a Metro Availability or synchronous replication relationship between Nutanix NX/SX Series and other non-NX clusters (Dell or Lenovo). However, mixing of NX and non-NX nodes in the same cluster are not supported.

## Configuring Synchronous Replication

1. To establish synchronous replication, configure the protection domain in metro availability configuration between primary and secondary site storage containers. For more information, see [Configuring a Protection Domain \(Metro Availability\)](#) on page 274.

## Best Practices and Requirements

- Avoid whitelisting the primary and secondary clusters on each other.
- Do not have virtual machine in Critical State on any storage container on any host. As the storage is blacklisted, this might impact importing of a VM on a host.
- Do not deploy VMs on the stretched storage container on the secondary site. If you want to deploy VMs on your secondary site, create a new storage container and then deploy the VMs. If you want to establish synchronous replication for these VMs, then this new storage container must be stretched to a remote site.

## Limitations

- All the limitations of metro availability configuration are applicable for synchronous replication. For more information, see Limitations section of [Data Protection Guidelines \(Metro Availability\)](#) on page 271 topic.

## Failover Scenarios for Synchronous Replication in Hyper-V

### VMs are Originally Registered and Running on the Primary Site and Failure Occurred on the Primary Site

If the VMs are originally registered and running on the primary site and a failure occurs on the primary site, then all the VMs can be started on the secondary site.

1. Login to the Web console of secondary cluster.
2. Go to **Data Protection > Table > Metro Availability**. The status of protection domain is displayed as Remote Unreachable.
3. Select the protection domain and click **Promote** to make the protection domain on secondary independent of the primary.  
Promoting the secondary site unblocks all the VMs running on the secondary site for the stretched storage container.
4. Register the VMs on the secondary site. For more information about registering the VMs on the primary or secondary site, see [Registering a VM on a Hyper-V Cluster](#) on page 330.
5. Start the VMs.

### VMs are Originally Registered and Running on the Secondary Site and Failure Occurred on the Primary Site

The secondary metro availability is in remote unreachable state and VMs are in hung state as storage is not accessible. All the VMs can be started on the secondary site.

1. Login to the Web console of secondary cluster.
2. Go to **Data Protection > Table > Metro Availability**. The status of protection domain is displayed as Remote Unreachable.
3. Select the protection domain and click **Promote** to make the protection domain on secondary independent of the primary.

All the VMs should start functioning on secondary site after restart.

#### VMs are Originally Registered and Running on the Secondary Site and Failure Occurred on the Secondary Site

All the VMs can be started on the primary site.

1. Login to the Web console of primary cluster.
2. Register the VMs on the primary site. For more information about registering the VMs on the primary or secondary site, see [Registering a VM on a Hyper-V Cluster](#) on page 330.
3. Start the VMs.

### Fallback Scenarios for Synchronous Replication in Hyper-V

#### Fallback VMs that are Currently Running on the Secondary Site but were Originally Registered on the Primary Site

When the primary site recovers, fallback VMs back to the primary site that are currently running on the secondary site. These VMs were originally registered on the primary site when the failure on the primary site had occurred.

1. Login to the Web console of recovered primary cluster and go to **Data Protection > Table > Metro Availability**.  
The status of the protection domain is in Decoupled state.
  2. Select the protection domain and click **Disable**.
-  **Note:** You should not re-enable the protection domain from here because VMs might be running on secondary.
3. Unregister the VMs from the recovered primary cluster. For more information about unregistering the VMs on primary or secondary site, see [Unregistering a VM on a Hyper-V Cluster](#) on page 331.
  4. Login to the Web console of secondary cluster and go to **Data Protection > Table > Metro Availability**.
  5. Select the protection domain and click **Re-enable**. This ensures that the latest content of your VMs is synchronously replicated to the recovered primary site.
  6. Click **Yes**. Wait for the operation to finish. On completion of the operation, the protection domain state changes to Enabled ( In Sync ). The resynchronization time varies on the data that needs to be replicated.
  7. Shutdown the VMs from your current primary site (originally the secondary site).
  8. Select the protection domain and then click **Disable** from your current primary site.
  9. Login to the Web console of your current secondary site (recovered primary site) and go to **Data Protection > Table > Metro Availability**.
  10. Select the protection domain and then click **Promote**.
  11. Register the VMs on this site. For more information about registering the VMs on the primary or secondary site, see [Registering a VM on a Hyper-V Cluster](#) on page 330.
  12. Start the VMs.
  13. Unregister the VMs from where the VMs were originally replicated.

14. To establish the metro availability configuration again, login to the Web console of primary cluster and go to **Data Protection > Table > Metro Availability**.
15. Select the protection domain and click **Re-enable**.
16. Click **Yes**. Wait for synchronization to complete. After the synchronization is completed, the original metro availability configuration is established.

#### **Fallback VMs that are Currently Running on the Secondary Site and were Originally Registered on the Secondary Site**

When the primary site recovers, fallback VMs that were running on the secondary site when the failure on the primary site had occurred. This procedure establishes original synchronous replication configuration.

1. Login to the Web console of the recovered primary cluster and go to **Data Protection > Table > Metro Availability**.
  2. Select the protection domain and click **Disable**.
  3. Login to the Web console of secondary cluster and go to **Data Protection > Table > Metro Availability**.
  4. Select the protection domain and click **Re-enable**.
  5. Click **Yes**. Wait for synchronization to finish.
  6. Shut down the VMs from secondary site.
  7. Select the protection domain and click **Disable**.
  8. Login to the Web console of primary cluster and go to **Data Protection > Table > Metro Availability**.
  9. Select the protection domain and click **Promote**.
  10. Select the protection domain and click **Re-enable**.
- Now you can start the VMs on the secondary site.

#### **Fallback VMs that are Currently Running on the Primary Site but were Originally Registered on the Secondary Site**

When the secondary site recovers, fallback VMs back to the secondary site that are currently running on the primary site. These VMs were originally registered on the secondary site when failure on the secondary site had occurred.

1. Unregister the VMs from the recovered secondary site.
2. Login to the Web console of primary cluster and go to **Data Protection > Table > Metro Availability**.
3. Select the protection domain and click **Re-enable**.
4. Shut down the VMs on the primary site.
5. Unregister the VMs from the primary site.
6. Register the VMs from the secondary site.

## Failing Over a Protection Domain Manually in Synchronous Replication (Planned Failover)

Perform the following procedure to perform the manual failover to the secondary site if you have configured synchronous replication.

1. Power off and remove the VMs from the primary site.



**Note:** Ensure that the container of the primary site does not have any VMs that are running on it.

2. Register and power on the VMs on the secondary site.

3. Promote the secondary site.

The secondary site becomes active. At the same time an alert is displayed on the primary site to disable the metro availability.



**Caution:** If any schedules are enabled on the primary site, ensure that you first disable or remove the schedules.

4. Disable metro availability configuration from the primary site.

5. Re-enable the metro availability configuration from secondary site to the primary site.

This step resynchronizes the metro availability configuration and deletes the data of the primary site container. The roles are successfully reversed, the secondary site will become primary and primary site will become as secondary.

## Registering a VM on a Hyper-V Cluster

You can register the VMs on a Hyper-V cluster by performing following procedure.

1. Generate a compatibility report for the VM that needs to be imported by using the `Compare-VM` cmdlet.
2. Fix incompatibilities that may occur because of incorrect configuration of Nutanix cluster name in the UNC paths (virtual hard disk path) by using the correct Nutanix cluster name.

```
> $report= Compare-VM -Path configuration_file_path -Register
```

Replace `configuration_file_path` with the path to the configuration file of the virtual machine to be compared.

To view the incompatibility report type, `> $report.Incompatibilities | Format-Table -AutoSize`

In the following example, the SMB path incompatibility should be fixed in the configuration XML file of VM to match the destination cluster.

```
> $report= Compare-VM -Path \\winne-smb\Mixed_vms\L4_IO\Virtual Machines\  
\A7351476-4096-91E7-424A57B3FD08.xml -Register  
> $report
```

VM	:Microsoft.HyperV.PowerShell.VirtualMachine
OperationType	:ImportVirtualMachine
Destination	:WINNIE-1
Path	:\\winne-smb\Mixed_vms\L4_IO\Virtual Machines\ \A7351476-4096-91E7-424A57B3FD08.xml
SnapshotPath	:\\winne-smb\Mixed_vms\L4_IO\Snapshots
VhdDestinationPath	:
VhdSourcePath	:
Incompatibilities	:(40010)

To view the incompatibility report type, `> $report.Incompatibilities | fl *`

Message	:Virtual Hard Disk file not found.
MessageId	:40010
Source	:Microsoft.HyperV.PowerShell.HardDiskDrive

Incompatibility occurred while registering a VM on the secondary site (in the example, site WINNIE) and Virtual Hard Disk file file not found - 40010 message is displayed. This occurred because the VM was registered originally on the primary site and not on the secondary site. You must fix this issue before proceeding.

- After all the incompatibilities are fixed, import the virtual machine by using the `Import-VM` cmdlet.

## Unregistering a VM on a Hyper-V Cluster

You can unregister the VMs on a Hyper-V cluster by performing following procedure.



**Note:** To unregister a VM you need to delete the VM. Hence, ensure that the VM has been registered successfully and all the VM files are present on the other site. Also, ensure that the protection domain state on the web console of the site is in the Disabled state.

- Stop the VM.
- If the VM is part of the failover cluster, remove the VM from the cluster by using the `Remove-ClusterGroup` cmdlet.
- Delete the VM by using the `Remove-VM` cmdlet.
- Verify that the VM got unregistered from the host by using `Get-VM` cmdlet.

## Nutanix Cross Hypervisor Disaster Recovery

Cross hypervisor disaster recovery (CH-DR) provides an ability to migrate the VMs from one hypervisor to another (ESXi to AHV or AHV to ESXi) by using the protection domain semantics of protecting VMs, taking snapshots, replicating the snapshots, and then recovering the VMs from the snapshots. To perform these operations, you need to install and configure NGT on all the VMs. See [Enabling and Mounting NGT Simultaneously on Multiple VMs](#) on page 396 for more information. NGT configures the VM with all the required drivers for VM portability. After you prepare the source VMs, they can be recovered in a different hypervisor type.



### Caution:

- If you have configured the static IP addresses for the VMs running on the ESXi hypervisor, you need to manually change the computer name and the IP address after recovering the VMs on the AHV cluster.
- Hypervisor specific properties like multi-writer flags, independent persistent and independent non-persistent disks, changed block tracking (CBT), etc. are not preserved in the CHDR operation.

See [Nutanix Guest Tools Requirements and Limitations](#) on page 390 for more information about general NGT requirements. Requirements specific to this feature are as follows.

- VMs with flat files are only supported. Nutanix does not support vSphere snapshots or delta disk files. If you have delta disks attached to the VM and you proceed with the migration, the VMs will be lost and you have to contact Nutanix support for assistance.
- IDE/SCSI disks are only supported. SATA and PCI disks are not supported.

- VMs running SUSE Linux Enterprise Server (SLES) operating system are not supported.
- Ensure that both the sites are running AOS 4.6 or later release.
- Set the SAN policy to OnlineAll for all the Windows VMs for all the non-boot SCSI disks so that they can be automatically brought online. For more information on setting SAN policy, see [Bringing Multiple SCSI Disks Online](#) on page 333.
- Virtual machines with attached volume groups or shared virtual disks are not supported.
- If the VMs has static IP address configured, you need to manually reconfigure IP address after conversion.

## Recovering Virtual Machines in the Remote Cluster

You can recover the VMs by performing the following procedure.

1. Install and configure NGT on the VMs. For installing and configuring NGT and its requirements and limitations, see [Nutanix Guest Tools](#) on page 390.
  - (Optional) Run `ncli ngt list` to verify communication is active or not.
  - If your VM has SCSI disks, set the SAN policy is to *online all*. Otherwise, only the boot-SCSI disk will be automatically brought online. If the policy is not configured properly and if the VM has an IDE boot disk, all SCSI disks will be offline if you try to power on the VM. To bring multiple disks online after recovery, see [Bringing Multiple SCSI Disks Online](#) on page 333.
  - Snapshots taken after NGT is installed are only supported for recovery operations. You can validate all the snapshots for VM recovery that are replicated to the remote site. Check the **Remote Snapshots** tab on the local cluster and the **Local Snapshots** tab on the remote cluster.
  - If the SCSI devices are enabled for multipathing and fstab contains the device name `/dev/sd*`, then while migrating a VM from ESXi to AHV, VM fails to boot and a message similar to the following Device `/dev/sd*` in use e2fsck can't continue is displayed. See [Blacklisting Devices for Multipathing](#) on page 334 for more information.
2. Create a protection domain and protect the VMs that you want to recover. For more information about creating a protection domain, see [Configuring a Protection Domain \(Async DR\)](#) on page 256.
3. Configure a remote site. During the addition of a remote site, you need to add the L2 network mapping. For more information about configuring a remote site and adding network mapping on a remote site, see [Configuring a Remote Site \(Physical Cluster\)](#) on page 317.



**Note:** If you do not define any network mapping then the VM gets registered without any network configuration.

4. Migrate or take the snapshot of the protection domain and replicate it to the remote site. For more information about migrating, taking and replicating a snapshot, see [Modifying a Protection Domain \(Async DR\)](#) on page 262.
5. Recover the VMs on the remote site by using one of the following methods.

- By using *Planned Failover* procedure (protection domain migration operation ) as described in [Failing Over a Protection Domain](#) on page 267.

Appropriate warnings related to the VMs that cannot be recovered on the remote site are displayed when you try to migrate the protection domain. Click the **Learn more** link for additional information.

- By using *Unplanned Failover* procedure (protection domain activate operation) as described in [Failing Over a Protection Domain](#) on page 267.



**Note:** Before activating the protection domain, verify which VMs are recoverable for the latest snapshot in the **Local Snapshots** tab.

The **Recovery Details** link of the **Local Snapshots** tab provides information whether the VM is recoverable or not on the local cluster. The **Recovery Details** link of the **Remote Snapshots** tab provides information whether the snapshot that is present on the remote cluster is recoverable on the local cluster or not.

- By restoring an individual VM from a snapshot that you have replicated. For more information, see [Restoring an Entity from a Protection Domain](#) on page 265.

The **Recovery Details** tab provides the information whether the VM is recoverable or not.

 <b>Note:</b>
<ul style="list-style-type: none"><li>• If you start the Windows 7 or Windows 2008 R2 VMs after migrating the VMs from ESXi to AHV, a prompt that asks for restart is displayed. It recommended to restart the VMs to install all the required drivers.</li><li>• Do not uninstall Nutanix VM mobility drivers on the VMs post migration as the VMs become unusable after uninstalling mobility drivers.</li></ul>

On successfully recovering the VMs on the remote site, they are ready for use. In case of a failure, see the **Alerts** tab for more information regarding the cause of the failure.

## Bringing Multiple SCSI Disks Online

This tasks describes how to bring multiple SCSI disks online after recovery.

In Windows, the SAN policy determines whether a newly discovered disk is brought online or remains offline, and whether it becomes read/write, or remains read-only. If the SAN policy is not configured properly, only the boot disks are brought online.

When the disks are offline, the partitions or volumes will not be available and drive letters are not assigned. Hence you have to make the disks online.

When you recover a VM with multiple SCSI disks, the non-boot disks are not attached by Windows, but are visible. You need to bring these disks online after recovery.

Perform one of the following steps to bring the disks online.

- Use the Windows Disk Management tool to bring a disk online.
  - a. Go to **Start > Control Panel > System and Security > Administrative Tools > Computer Management > Storage > Disk Management**.
  - b. Right-click the offline disk and select **Online**.
- Use the `diskpart` command-line utility to bring a disk online.
  - a. Open the Windows command prompt and run `diskpart.exe` command.
  - b. List the disks to confirm their status by running the following command.

```
DISKPART> list disk
```

Output might look similar to the following.

Disk #	Status	Size	Free	Dyn	Gpt
Disk 0	Online	34 GB	12 MB		
Disk 1	Offline	1024 MB	0 B		

- c. Bring the disk online by entering the following commands.

```
DISKPART> select disk disk number
DISKPART> ATTRIBUTES DISK CLEAR READONLY
DISKPART> Online
```

Output might look similar to the following.

```
DiskPart successfully onlined the selected disk
```

- Use PowerShell to bring a disk online.

```
> Get-Disk | Where-Object IsOffline -Eq $True | Set-Disk -IsOffline $False
```

## Blacklisting Devices for Multipathing

If the SCSI devices are enabled for multipathing and fstab contains the device name `/dev/sd*`, then while migrating a VM from ESXi to AHV, VM fails to boot and a message similar to the following Device `/dev/sd*` in use e2fsck can't continue is displayed.

To start the VMs, the SCSI devices with name in fstab must be blacklisted from multipathing. You can accomplish this by going into the maintenance mode on the console and performing the following procedure.

1. Mount root file system as a root (rw).

```
$ mount / -o rw,remount
```

2. Blacklist the devices that are causing the issues by adding the following lines to `multipath.conf` file.

```
blacklist{
  devnode "^sd[a-z]"
}
```

3. Restart the VMs.

## Self-Service Restore

The self-service restore (also known as file-level restore) feature allows virtual machine administrators to do a self-service recovery from the Nutanix data protection snapshots with minimal administrator intervention.

The Nutanix administrator should deploy NGT on the VM and then enable this feature. For more information on enabling and mounting NGT, see the [Enabling and Mounting Nutanix Guest Tools](#) on page 393. After the feature is enabled and a disk is attached, the guest VM administrator can recover files within the guest operating system. If the guest VM administrator fails to detach the disk, it gets automatically detached from the VM after 24 hours.



**Note:**

- The Nutanix administrator can enable this feature for a VM only through nCLI, and in-guest actions can be performed only by using NGT.
- Only Async-DR workflow is supported for the self-service restore feature.

## Self-Service Enabled Disks Impact on Disaster Recovery

Disks with this feature enabled running on ESXi are not backed up by the disaster recovery workflows. However original disks of the VMs are backed up. If you replicate the VMs with self-service enabled disks, the following scenarios occur.

- If attaching a self-service disk is attempted for a VM that is part of a protection domain and is getting replicated to a remote site previous to AOS 4.5, an error message is displayed during the disk attach operation.
- If a snapshot with the attached self-service disk is replicated to a remote site previous to AOS 4.5, an alert message is displayed during the replication process.

## Requirements and Limitations of Self-Service Restore

Requirements specific for self-service restore are as follows.



**Note:** This feature requires a Pro (or Ultimate) license.

### Requirements

Privilege	Requirements and Limitations
Guest VM Administrator	<ul style="list-style-type: none"><li>• Linux VMs are not supported.</li></ul>
Nutanix Administrator	<ul style="list-style-type: none"><li>• The <b>disk.enableUUID</b> should be present in the .vmx file for the VMs on ESXi.</li><li>• Guest VM must have configured Nutanix snapshots by adding VM to a protection domain. Self-service restore is not supported for the snapshots that you take from the <b>VM table</b> view.</li><li>• vStore protection domains are not supported.</li><li>• Snapshots that are created in AOS 4.5 or later releases are only supported.</li><li>• Ensure that sufficient logical drive letters are available to bring the disk online.</li><li>• Volume groups are not supported.</li><li>• File Systems. Dynamic disks comprising of NTFS on simple volumes, spanned volumes, striped volumes, mirrored volumes, and RAID-5 volumes are not supported.</li><li>• IDE/SCSI disks are only supported. SATA, PCI, and delta disks are not supported.</li></ul>

## Enabling Self-Service Restore

After enabling NGT for a VM, the Nutanix administrator can enable the self-service restore for a VM.

**Before you begin:** Verify that NGT is enabled and mounted on the VM. For more information, see [Enabling and Mounting Nutanix Guest Tools](#) on page 393.

1. To enable self-service restore, click **Manage Guest Tools**.

- To enable self-service restore feature for the Windows VMs, click **Self Service Restore (SSR)** check box.

The Self-Service Restore feature is enabled of the VM. The guest VM administrator can restore the desired file or files from the VM.

- Click **Submit**.

## Restoring a File as a Guest VM Administrator (Using Web Interface)

After the administrator installs the NGT software inside the Windows guest VM, the Windows guest VM administrator can restore the desired file or files from the VM through the web interface.



**Note:** This option is not available for the Linux VMs.

- Log into the guest VM by using administrator credentials.
- Click the **Nutanix SSR** icon on the desktop.
- Type the administrator credentials of the VM.
  - If the user is an active directory user, use the **domain\_fqdn\_name\user\_name** to log into the SSR UI. Use of NETBIOS domain names or UPNs are currently not supported.  
For example, usage of domain.com\user\_name will work; however, domain\user\_name, user\_name@domain.com will not work.
  - The snapshots that are taken for that day is displayed. You also have an option to select the snapshots for the week, month, and the year. In addition, you can also define a custom range of dates and select the snapshot.

The screenshot shows a list of snapshots taken on September 8, 2016, from 02:21 PM to 09:41 AM. Each snapshot is represented by a small thumbnail icon and a timestamp. The list includes:

- 3293440 02:21 PM
- 3292952 02:17 PM
- 3292840 02:16 PM
- 3292828 02:08 PM
- 3292797 02:01 PM
- 3290796 01:11 PM
- 3290753 00:56 PM
- 3290568 00:01 PM
- 3290574 11:51 AM
- 3290413 10:51 AM
- 3290153 09:41 AM

Figure: Snapshot Selection

- Select the appropriate tab, **This Week, This Month, This Year..**

You can also customize the selection by clicking **Custom Range** tab and selecting the date range in the **From** and **To** fields.

- Select the check box of the disks that you want to attach from the snapshot.

**6.** From the **Disk Action** drop-down menu, select **Mount**.



*Figure: Mounting of Disks*

The selected disk or disks are mounted and the relevant disk label is displayed.

**7.** Go to the attached disk label drive in the VM and restore the desired files.

**8.** To view the list of all the mounted snapshots, select **Mounted Snapshots**.

This page displays the original snapshot drive letters and its corresponding current drive letters. The original drive letters gets assigned to the disk at the time of the snapshot. Mounted drive letters are on which the snapshotted disk is mounted right now.

Mounted Snapshots			
Here you manage snapshot drives that are currently mounted to your virtual machine. We have correlated the original snapshot drive letters with their current drive letters.			
<input type="checkbox"/>	Select All		<input type="button" value="Unmount"/>
<b>Snapshot ID: 3293562 09-08-2016 03:06 PM</b>			
<input checked="" type="checkbox"/>	DISK	ORIGINAL DRIVE LETTERS	MOUNTED DRIVE LETTERS
<input checked="" type="checkbox"/>	Disk 0	C:	H:
<b>Snapshot ID: 3294330 09-08-2016 04:08 PM</b>			
<input type="checkbox"/>	DISK	ORIGINAL DRIVE LETTERS	MOUNTED DRIVE LETTERS
<input type="checkbox"/>	Disk 0	C:	G:

*Figure: List of Mounted Snapshots*

**a.** To detach a disk, click the disk label and click **Unmount**.

You can unmount all the disks at once by clicking **Select All** and then clicking **Unmount**.

**9.** To detach a disk, select the check box of the disk that you want to unmount and then from the **Disk Action** drop-down menu, select **Unmount**.

## Restoring a File as a Guest VM Administrator

After the administrator installs the NGT software inside the guest VM, the guest VM administrator can restore the desired file or files from the VM.

### Before you begin:

- Mount NGT for a VM. For more information about enabling NGT, see [Enabling and Mounting Nutanix Guest Tools](#) on page 393.
- Verify that you have configured your Windows VM to use NGT. For more information, see [Installing NGT on Windows Machines](#) on page 394.

1. Login to the guest VM.
2. Open the command prompt as an administrator.

3. Go to the ngtcli directory in **Program Files > Nutanix**.

```
cd c:\Program Files\Nutanix\ngtcli
```

4. Run the ngtcli.cmd command.

5. List the snapshots and virtual disks that are present for the guest VM by using the following command.

```
ngtcli> ssr ls-snaps
```

The snapshot ID, disk labels, logical drives, and create time of the snapshot is displayed. The guest VM administrator can use this information and take a decision to restore the files from the relevant snapshot that has the data. For example, if the files are present in logical drive "C:" for the snapshot 41 (figure below) and disk label scsi0:0, the guest VM administrator can use this snapshot ID and disk label to attach the disk.

Snapshot Id	Disk Labels	Logical Drives	Create Time
14	scsi0:1 ide0:0 scsi0:0 ide0:1 scsi0:2	I: G: C: F: E:	2015.08.17 01:15 AM
23	scsi0:1 ide0:0 scsi0:0 ide0:1 scsi0:2	I: G: C: F: E:	2015.08.17 01:22 AM
32	scsi0:1 ide0:0 scsi0:0 ide0:1 scsi0:2	I: G: C: F: E:	2015.08.17 01:23 AM
41	scsi0:1 ide0:0 scsi0:0 ide0:1 scsi0:2	I: G: C: F: E:	2015.08.17 01:28 AM

Figure: List Snapshots

To list the snapshots with a specific number, use the following command.

```
ngtcli> ssr ls-snaps snapshot-count=count_value
```

Replace *count\_value* with the number that you want to list.

6. Attach the disk from the snapshots.

```
ngtcli> ssr attach-disk disk-label=disk_label snapshot-id=snap_id
```

For example, to attach a disk with snapshot ID 16353 and disk label scsi0:1, type the command.

```
ngtcli> ssr attach-disk snapshot-id=16353 disk-label= scsi0:1
```

An output similar to the following is displayed.

Communicating with Nutanix Data Protection Service ...			
Waiting for the disk to be attached ...			
Disk attached successfully, bringing the virtual disk online ...			
Hiding system reserved disks if any...			
Snapshot Id	Original Disk Label	Attached Disk Label	Detach Time
16353	scsi0:1 <E:>	scsi0:3 <G:>	2016.01.21 04:27 PM

Figure: Attached Disks

After successfully running the command, a new disk with label "G" is attached to the guest VM.

If sufficient logical drive letters are not present, bringing disks online action fails. In this case, you should detach the current disk, create enough free slots by detaching other self-service disks and re-attach the disk again.

7. Go to the attached disk label drive and restore the desired files.
8. To detach a disk, use the following command.

```
ngtcli> ssr detach-disk attached-disk-label=attached_disk_Label
```

For example, to remove the disk with disk label scsi0:3, type the command.

```
ngtcli> ssr detach-disk attached-disk-label=scsi0:3
```

If the disk is not removed by the guest VM administrator, the disk is automatically removed after 24 hours.

9. To view all the attached disks to the VM, use the following command.

```
ngtcli> ssr list-attached-disks
```

## Restoring a File as a Nutanix Administrator

The Nutanix administrator can also attach or remove the disks from the VM. However, the attached disk does not come online automatically in the VM. The administrators should use the disk management utility to make the disk online.

1. Log into the Controller VM.
2. Retrieve the self-service restore capable snapshots of a VM.

```
ncli> vm list-flr-snapshots vm-id=virtual_machine_id
```

Replace *virtual\_machine\_id* with the ID of the VM.

3. Attach a disk from a self-service restore capable snapshot.

```
ncli> vm attach-flr-disk vm-id=virtual_machine_id snap-id=snapshot_id \
disk-label=disk_Label
```

For example, to attach a disk with VM ID 00051a34-066f-72ed-0000-000000005400::5030468c-32db-c0cc-3e36-515502787dec, snapshot ID 4455 and disk label scsi0:0, type the command.

```
ncli> vm attach-flr-disk vm-id=00051a34-066f-72ed-0000-000000005400::5030468c-32db-
c0cc-3e36-515502787dec snap-id=4455 disk-label=scsi0:0
```

The attached disk does not come automatically online. Administrators should make the disk online by using disk management utility of Windows.

Once the disk is attached, the guest VM administrator can restore the files from the attached disk.

4. To remove a self-service restore disk from a VM.

```
ncli> vm detach-flr-disk vm-id=virtual_machine_id attached-disk-label=attached_disk_Label
```

For example, to remove a disk with VM ID 00051a34-066f-72ed-0000-000000005400::5030468c-32db-c0cc-3e36-515502787dec, and disk label scsi0:0, type the command.

```
ncli> vm detach-flr-disk vm-id=00051a34-066f-72ed-0000-000000005400::5030468c-32db-
c0cc-3e36-515502787dec attached-disk-label=scsi0:0
```

5. View all the self-service restore capable snapshots attached to a VM.

```
ncli> vm list-attached-flr-snapshots vm-id=virtual_machine_id
```

Replace *virtual\_machine\_id* with the ID of the VM.

## Single-Node Replication Target Clusters

Up until AOS 5.0 release, you cannot create a cluster with less than three nodes. From AOS 5.0 or later releases, you can create a cluster by using single node as a replication target. The SMB and ROBO deployments can use this as a replication target for backup and recovery workflows to backup the infrastructure VMs like the DHCP server, DNS server, SQL server, etc. If for some reason VMs on the primary site fails, you can recover the VMs by using the snapshot that is being replicated from the single-node replication target cluster. Since this cluster should only be used as a replication target, options like, Acropolis File Services, restoring VM from the snapshots on the replication target clusters are not available. However, all the other dashboards are available on this cluster for configuring and monitoring purpose. See the [Single-Node Replication Target Requirements and Limitations](#) on page 341 for complete list of requirements and limitations of single-node replication target clusters.



**Note:** If the primary cluster fails, the replication between primary and single-node replication target cluster stops. You cannot recover VMs on the single-node replication target cluster. You cannot run VMs on a single-node replication target cluster. You can use this cluster only for storing backups.

### Single-Node Replication Target Cluster Specifications and Process

Platform: Nutanix provides NX-1155-G5, 1-node 2U rack-mount chassis with 2 SSDs and up to 10 HDDs with a maximum capacity of 60 TB. For complete information about hardware configuration, see *Hardware Administration Guide*.

Read Operation: The read operation is same as that of a normal cluster (three nodes or more).

Write Operation: The write operation is performed to maintain disk-level fault tolerance. When you perform a write operation, the writes are always replicated to two different disks on the same node (in a redundancy factor 2 configuration). This ensures that the cluster tolerates any single SSD or HDD failure.



**Note:** Redundancy factor of 3 is not supported on the single-node replication target cluster.

Disk Failure: The single-node replication target cluster provides redundancy of data at the disk level. Hence if a disk fails, you have the data available on another disk. Metadata is replicated across the two SSDs. In an event of a SSD failure, data and metadata is available on the second SSD.

Disk failure can be categorized into two categories:

- SSD Failure: In an event of an SSD failure or when an SSD is marked for removal, the single-node replication target cluster becomes a Read Only cluster and stops accepting any incoming replication traffic. An alert is displayed in the primary and single-node replication target clusters. Also, the resiliency status of the cluster is changed to the Critical state. The recovery process also slows down. Hence, it is recommended to get the cluster back into the Normal state by adding a new SSD to the cluster. After you remove the faulty disk and replace with the new SSD, this new SSD is automatically detected and the cluster is moved back into the normal state (read/write mode).
- HDD Failure: The HDD failure is handled in the same way as that of a normal cluster and none of the situations that occur when an SSD fails (as described above) occur in case of HDD failure.



**Note:** For more information about recovering from disk failure see the boot/metadata drive documentation for NX-1155-G5.

### Data Resiliency Status

The *Data Resiliency Status* window displays more detailed cluster resiliency status information. This window provides information about the number and type of failures the cluster can withstand safely. For single-node replication target clusters, the **Failures Tolerable** column indicates the number of simultaneous failures of that component type (disk and host instead of host and block) that can be tolerated (0, 1, or 2). When no failure can be tolerated, a message is displayed to highlight the limitation.

Data Resiliency Status		
FAULT DOMAIN TYPE: DISK		
COMPONENT	FAILURES TOLERABLE	MESSAGE
Free Space	1	
FAULT DOMAIN TYPE: HOST		
COMPONENT	FAILURES TOLERABLE	MESSAGE
Static Configuration	0	Not enough nodes (hosts) in the cluster
Free Space	0	Free space on the cluster - 17.62 TB is not enough to tolerate any node failure

**OK**

Figure: Data Resiliency Status

## Single-Node Replication Target Requirements and Limitations

Following are requirements and limitations of the single-node replication target clusters.

### Requirements and Limitations

- Only 1:1 replication is recommended (not n:1 replication).
- It is recommended to have only one VM or VG for each protection domain.
- Only AHV is supported on the single-node replication target cluster. However, the primary cluster can run any hypervisor (ESXi, Hyper-V, or AHV).
- Single-node replication target clusters are supported from AOS 5.0 or later releases. Primary cluster can run on AOS 5.0.x 4.6.x or 4.7.x versions.
- Deduplication is not supported on the single-node replication target clusters.
- Replication of a protection domain on a container with deduplication enabled to a single-node replication target cluster is not recommended.
- Erasure coding is not supported on this cluster.
- The Firmware updates (BMC or BIOS) are not supported on the single-node replication target clusters.
- Metro availability is not supported on this cluster.
- You cannot expand the cluster to add more nodes.
- You cannot use the **Repair Host Boot Disk** from Prism web console to repair SATA DOM.
- You can take only Nutanix native snapshots. You cannot set this cluster as a target for third-party providers like Veeam or CommVault.

## Guidelines for Single-Node Replication Target Clusters

Some guidelines for single-node replication target clusters are as follows.

- You cannot restore VMs from the replicated snapshots on the single-node replication node cluster. You can use this cluster only as a replication target to the primary cluster.
- RPO for single-node replication target cluster is 6 hours with daily change rate of approximately around or less than 1% with a 5 TB of data set.
- You can configure schedule of 7 daily, 4 weekly, and 3 monthly snapshots .
- RTO for single-node replication target cluster is 4 to 5 TB within 24 hours.

## Licensing Requirements

### Licensing Requirements

Cluster	Description
Primary cluster	Primary cluster can be at the Starter License while replicating to the single-node replication target cluster.   <b>Note:</b> Even if the primary cluster is replicating simultaneously to the single-node replication target cluster and a regular Nutanix cluster in the main datacenter, which is set up for either backup or disaster recovery purpose, you can still have Starter License on the primary cluster.
Single-node replication target cluster	Regular Nutanix licensing model is followed on the single-node replication target clusters. For example, Ultimate License will be required if SED Encryption is a requirement on the single-node replication target clusters.

## Imaging Single-Node Replication Target Nodes

You can image single-node replication target nodes by using both Controller VM Foundation and Standalone Foundation.

 **Note:** Imaging by using Standalone Foundation is restricted to Nutanix sales engineers, support engineers, and partners. Contact Nutanix customer support or your partner for help with this procedure.

### Controller VM Foundation

- In Controller VM foundation, you can map the primary cluster nodes (three nodes or more) and the single-node replication target cluster node (one node) during the foundation process itself.  
  
 **Note:** Ensure that primary and single-node replication target cluster is in the same broadcast domain or VLAN.
- You can also create a standalone single-node replication target cluster. If you decide not to map the primary cluster and replication target cluster, you need to add the replication target cluster as a remote site to the primary cluster. For information on the adding the single-node replication target cluster as a remote site, see [Configuring a Remote Site \(Physical Cluster\)](#) on page 317.

## Standalone Foundation

If you use standalone foundation, you cannot perform the mapping of primary cluster and replication target cluster. You need to add the replication target cluster as a remote site to the primary cluster. For more information, see [Configuring a Remote Site \(Physical Cluster\)](#) on page 317.



**Note:** See the *Field Installation Guide* for more information about imaging the nodes.

## Setting Up Single-Node Replication Target Clusters

If you have not mapped the primary cluster and replication target clusters during the foundation process, you can manually set this cluster as a remote site target to store data replications for the protected domains.

The process of setting up the remote site in single-node replication target cluster is same as the way to set up a remote site for the normal cluster except that you have to set up the remote site with backup only capability.

Login to the Prism and follow the steps described in the Configuring a Remote site, see [Configuring a Remote Site \(Physical Cluster\)](#) on page 317.

## Recovery Procedures by using Single-Node Replication Target Clusters

If for some reason the entities on the primary cluster fails, you can recover the entities by using the snapshots that are being replicated to the single-node replication target cluster. If your primary cluster fails altogether, you can create a new cluster and use the snapshots residing in the replication target clusters to recover the cluster.

The process of restoring protected entities from the single-node replication target clusters is same as the way you restore entities for the normal cluster.



**Note:** You can restore data stored on the single-node replication target cluster to the primary site.  
You cannot run VMs on the single-node replication target cluster.

1. To recover the entities, login to the Prism and follow the steps described in the Restoration of Protected Entities, see [Restoration of Protected Entities](#) on page 264.
2. To recover the cluster, see [Recovering from the Remote Snapshots on a Backup or DR Site](#) on page 325 for more information.

## 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 (see [Home Dashboard](#) on page 38).
- In depth health status information for VMs, hosts, and disks is available through the Health dashboard (see [Health Dashboard](#) on page 344).
- You can customize the frequency of the scheduled health checks and how frequently to run them. (see [Configuring Health Checks](#) on page 348).
- You can run NCC health checks directly from the Prism. (see [Running Checks by Using Web Console](#) on page 349).
- You can collect logs for all the nodes and components. (see [Collecting Logs by Using Web Console](#) on page 350).
- For a description of each available health check, see [Alerts/Health checks](#) on page 417.

### 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 (see [Main Menu Options](#) on page 32).



**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 (see [Main Menu Options](#) on page 32).

#### 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 select 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 (see following figure). 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

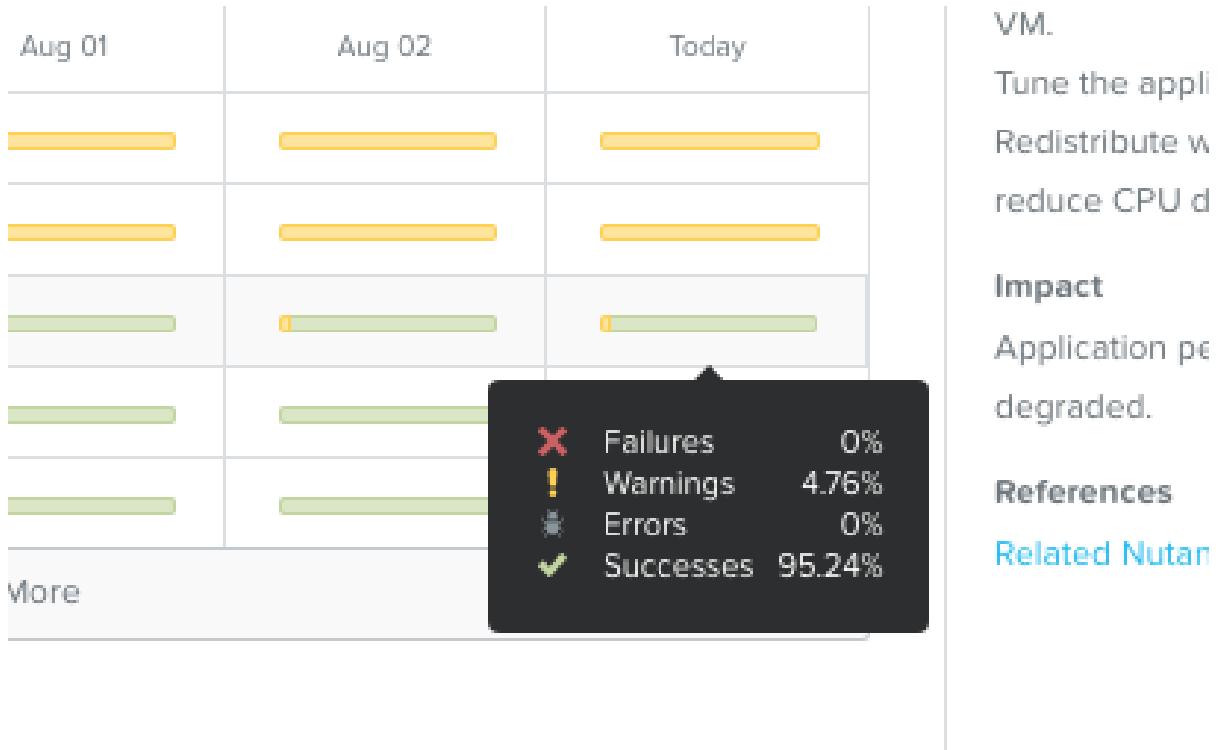


Figure: Hover Information

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.

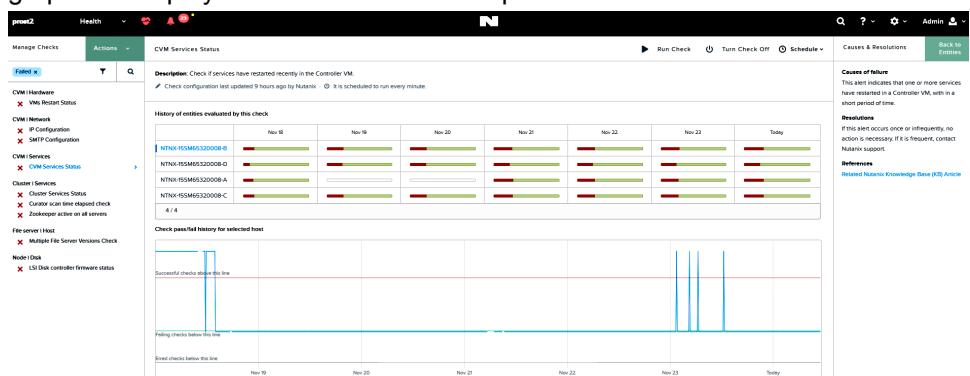


Figure: Filter Categorization



**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 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.

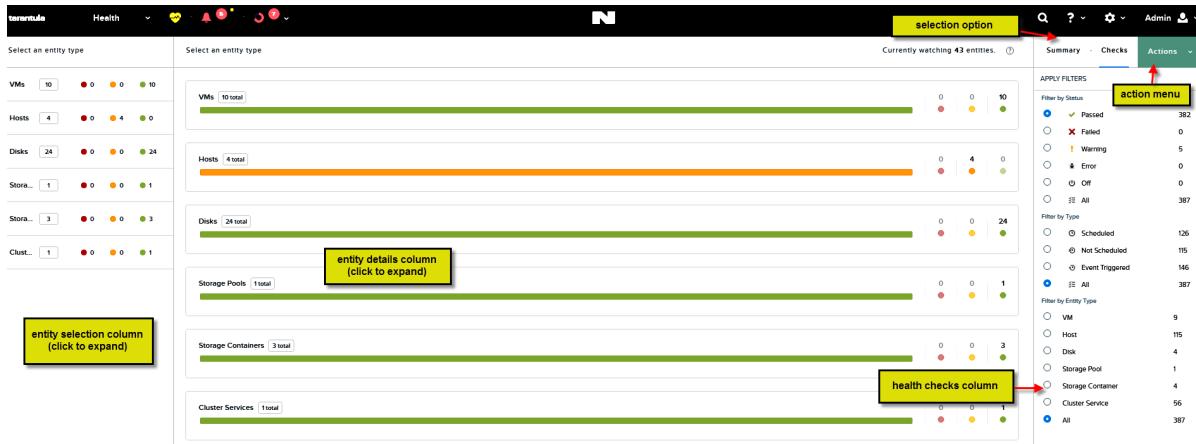


Figure: Health Dashboard

## 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.

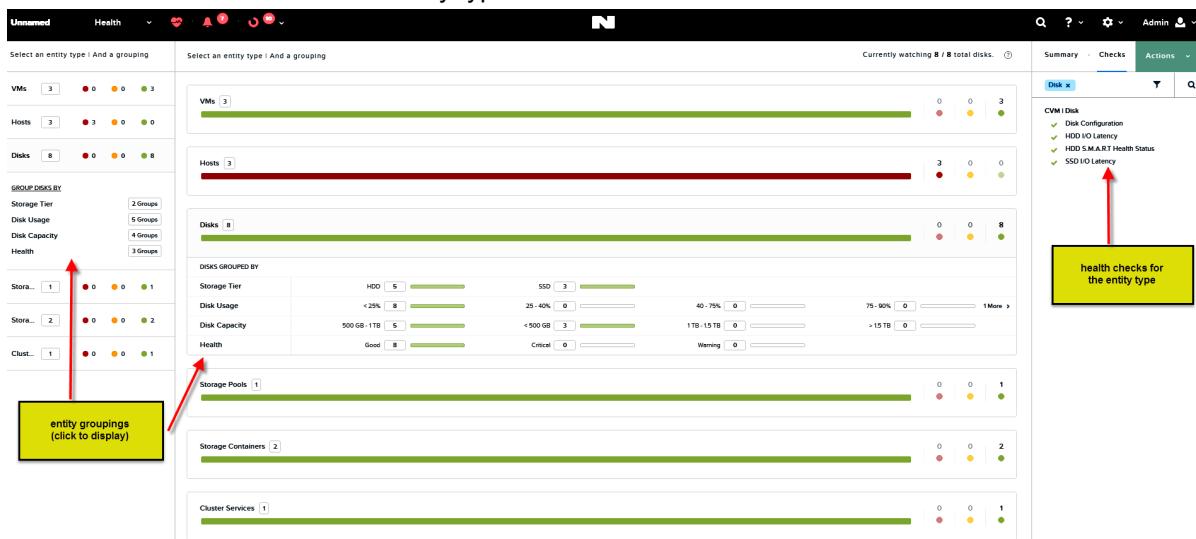


Figure: Health Dashboard Expanded

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.

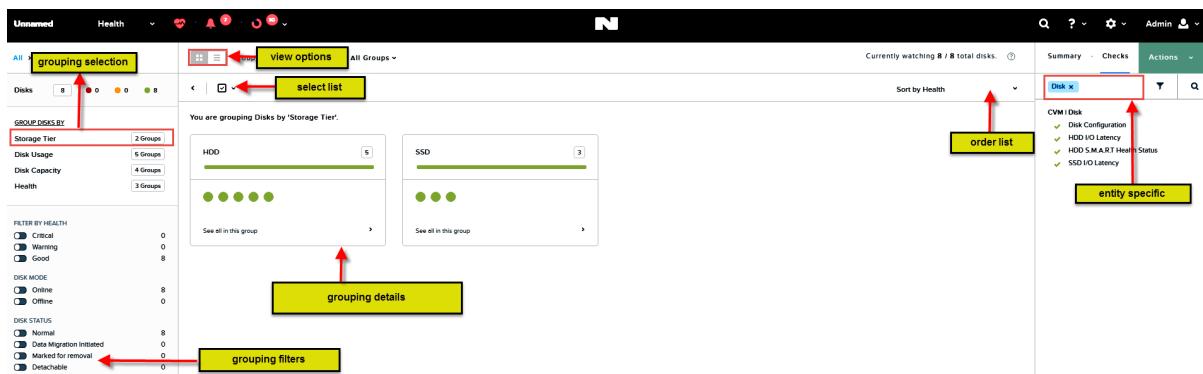


Figure: Health Dashboard Grouping Screen

The middle column provides two viewing options: a diagram view (see figure above) and a table view (see figure below). The table view provides more detailed information in tabular form. You can sort the entries by clicking a column header.

Group Disks by Storage Tier > All Groups						
Currently watching 8 / 8 total disks.						
Sort by Health						
You are grouping Disks by 'Storage Tier'.						
DISK ID	HYPERSERVER IP	TIER	DISK USAGE	DISK IOPS	DISK AVG I/O	LATENCY
00053e42-3a71-8c3b-0000-000000004447-39	10.4.45.80	HDD	0%	0	0 kBps	0 ms
00053e42-3a71-8c3b-0000-000000004447-41	10.4.45.79	HDD	0%	0	0 kBps	0 ms
00053e42-3a71-8c3b-0000-000000004447-42	10.4.45.79	HDD	0%	0	0 kBps	0 ms
00053e42-3a71-8c3b-0000-000000004447-46	10.4.45.78	HDD	0%	0	0 kBps	0 ms
00053e42-3a71-8c3b-0000-000000004447-47	10.4.45.78	HDD	0%	0	0 kBps	0 ms
00053e42-3a71-8c3b-0000-000000004447-40	10.4.45.80	SSD	0%	0	0 kBps	0 ms
00053e42-3a71-8c3b-0000-000000004447-43	10.4.45.79	SSD	0%	0	0 kBps	0 ms
00053e42-3a71-8c3b-0000-000000004447-48	10.4.45.78	SSD	0%	0	0 kBps	0 ms

Figure: Health Dashboard Table View (middle column)

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.

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:

1. In the Health dashboard (see [Health Dashboard](#) on page 344), 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. The following information is displayed:
  - The left column lists the health checks with the selected check highlighted. Click any of the entries to select and highlight that health check.
  - The middle column describes what this health check does, and it provides the run schedule and history across affected entities (hosts, disks, or VMs).
  - The right column describes what failing this health check means (cause, resolution, and impact).

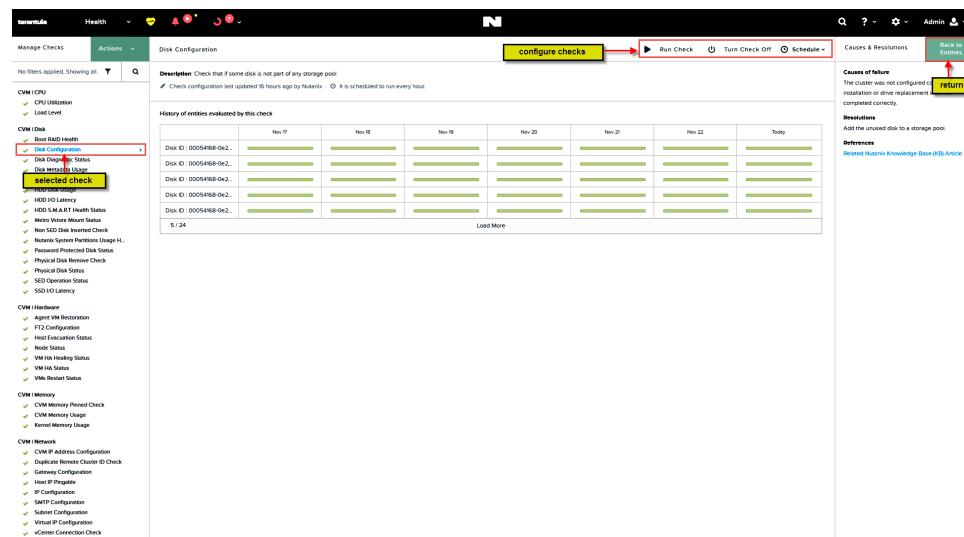


Figure: Health Check Configuration Screen

2. To run a particular check, click **Run Check**.
3. 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.
4. 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.

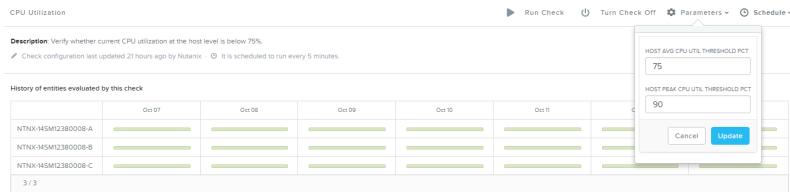


Figure: Health Check Parameters

- To change the schedule for running the health check, click the **Schedule** link for the schedulable checks at the top of the middle column, and select an interval from the drop-down list.

You can choose an interval from 1 minute to 48 hours. Most checks run every minute by default.

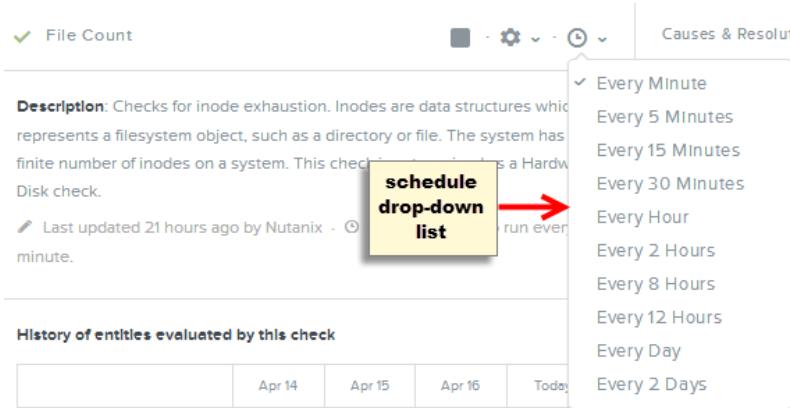


Figure: Health Check Schedule

## Running Checks by Using Web Console

You can now run the NCC checks from the **Home** dashboard of the Prism 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.



**Note:** If you are running checks by using web console, you will not be able to collect the logs at the same time.

- In the Health dashboard, from the **Actions** drop-down menu select **Run Checks**.
- Select 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 were failed or gave warning during the health check runs.
  - 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.
- 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](#) on page 414.

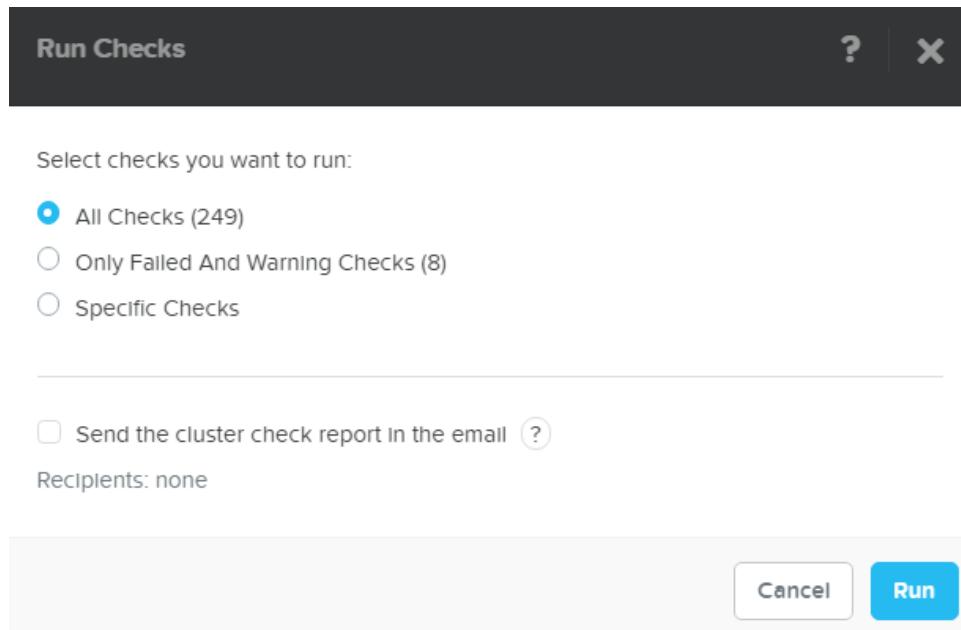


Figure: Run Health Checks

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 Web Console

You can now collect logs directly from the **Home** dashboard of the Prism web console. Logs can be collected 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.



**Note:** If you are collecting logs by using web console, you will not be able to run the health checks by using web console at the same time.

1. In the Health dashboard, from the **Actions** drop-down menu select **Log Collector**.
2. Collect the logs.
  - a. **Collect Logs starting now:** Select this option to collect logs based on number of hours or based on number of days.  
By default this option is selected. In the **For the past** drop-down menu, if you select **Hours**, logs are collected for the past 4 to 23 hours or if you select **Days**, logs are collected depending on your inputs (1 or 2 days)
  - b. **Custom Date Range:** Select this option and provide the date range in the **Start From** and **End By** fields.  
The time field is automatically updated with the current time. However, you also have an option to select the time from when you want to start the collection operation.



**Note:** Logs can be collected for a minimum of 4 hours to a maximum of 2 days.

3. Click **Run Now** to start the operation.

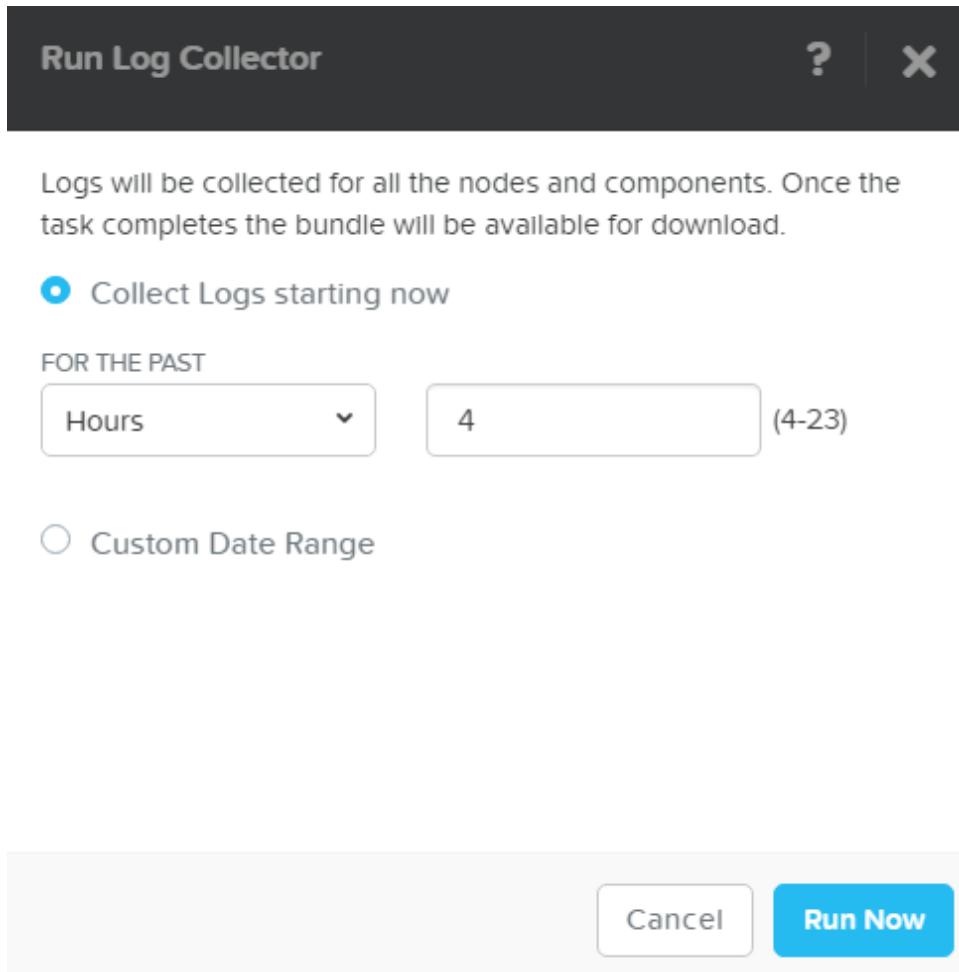


Figure: Run Log Collector

Once the operation finishes, you can download the log bundle for the last two runs from the **Task** dashboard for further analysis.

## 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 (see [VM Dashboard](#) on page 352).
- In Acropolis managed clusters, the web console also allows you to do the following:
  - Create VMs (see [Creating a VM \(AHV\)](#) on page 366).
  - Manage VMs (see [Managing a VM \(AHV\)](#) on page 372).
  - Enable VM high availability (see [Enabling High Availability for the Cluster](#) on page 389).
  - Configure network connections (see [Configuring Network Connections](#) on page 151).
- You can create and manage VMs directly from Prism Element when the hypervisor is ESXi.
  - Create VMs (see [Creating a VM \(ESXi\)](#) on page 377).
  - Manage VMs (see [Managing a VM \(ESXi\)](#) on page 379)

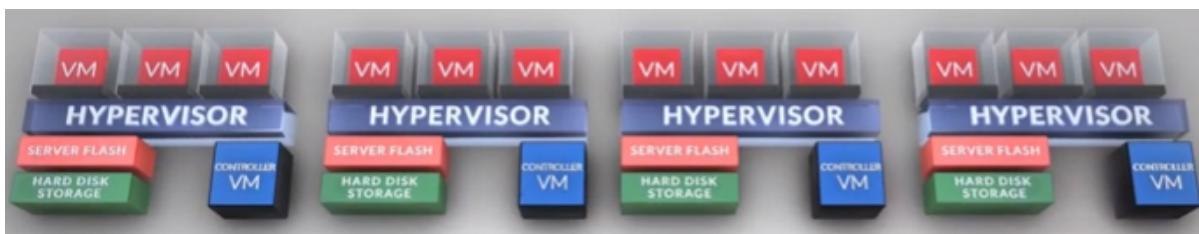


Figure: Node Architecture

## 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 (see [Main Menu Options](#) on page 32), 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 (see [VM Overview View](#) on page 353), or click the **Table** button to display VM information in a tabular form (see [VM Table View](#) on page 354).
- Action buttons.** Click the **Create VM** button on the right to create a virtual machine (see [Creating a VM \(AHV\)](#) on page 366). Click the **Network Config** button to configure a network connection (see [Configuring Network Connections](#) on page 151).



**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 table content.** In the Table view, you can export the table 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 pull-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.



Figure: VM Dashboard Menu

## 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 figure is a sample view, and the table describes each field in this 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.

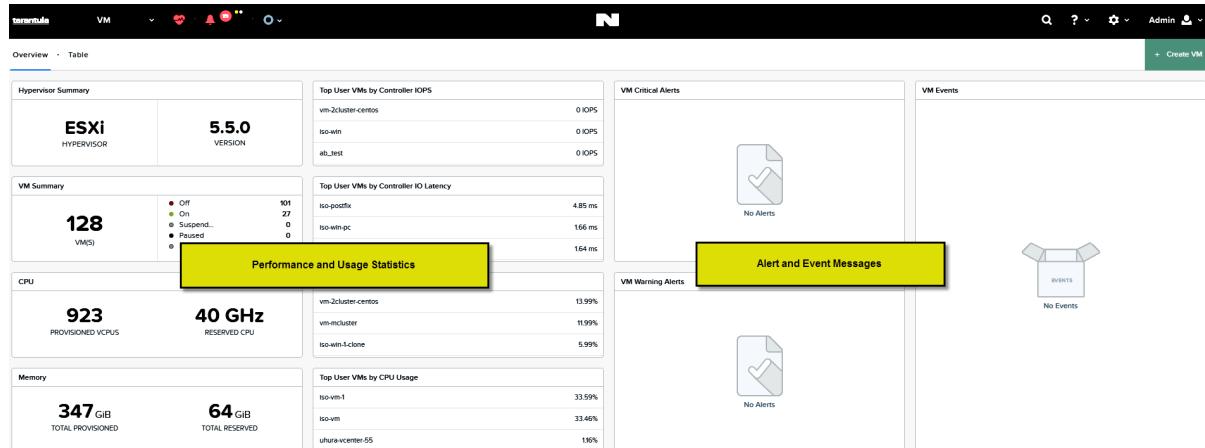


Figure: VM Overview View



**Note:** See [Understanding Displayed Statistics](#) on page 41 for information about how the statistics are derived.

## 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 "view all alerts" button at the bottom of the list (see <a href="#">Alerts Dashboard</a> ).
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 "view all alerts" 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 "view all events" 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:** See [Understanding Displayed Statistics](#) on page 41 for information about how the statistics are derived.

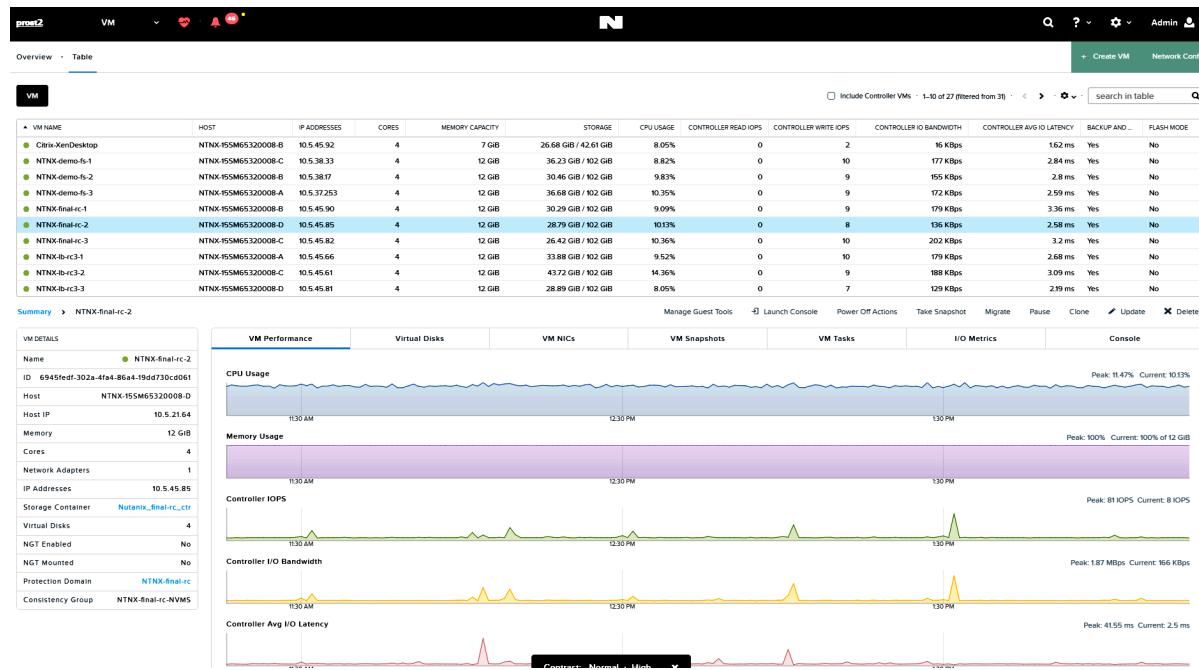


Figure: VM Table View

## VM Table View: Table Fields

Parameter	Description	Values
VM Name	Displays the name given the VM.	(VM name)
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 this VM.	(number)
Memory Capacity	Displays the total amount of memory available to this VM.	xxx [MB GB]
CPU Usage	Displays the percentage of allocated CPU capacity currently being used by this VM.	0 - 100%
Memory Usage	Displays the percentage of allocated memory capacity currently being used by this VM.	0 - 100%

Parameter	Description	Values
[Controller] Read IOPS	Displays read I/O operations per second (IOPS) for this VM.	(number)
	 <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.	
[Controller] Write IOPS	Displays write I/O operations per second for this VM.	(number)
[Controller] IO Bandwidth	Displays I/O bandwidth used per second for this VM.	xxx [Mbps Kbps]
[Controller] Avg IO Latency	Displays the average I/O latency for this 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 (see [Managing a VM \(AHV\)](#) on page 372 for more information about these actions):
  - 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.
  - 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.)
- 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**.



Figure: VM Table View: VM Details

### 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.	(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]
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]

Parameter	Description	Values
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**.

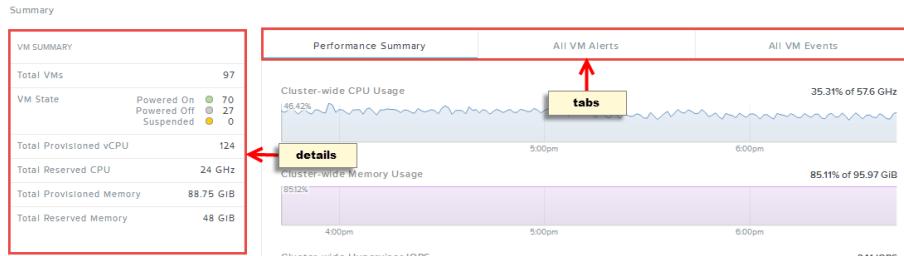


Figure: VM Table View: VM Summary

## 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)

Parameter	Description	Values
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]

## 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 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.

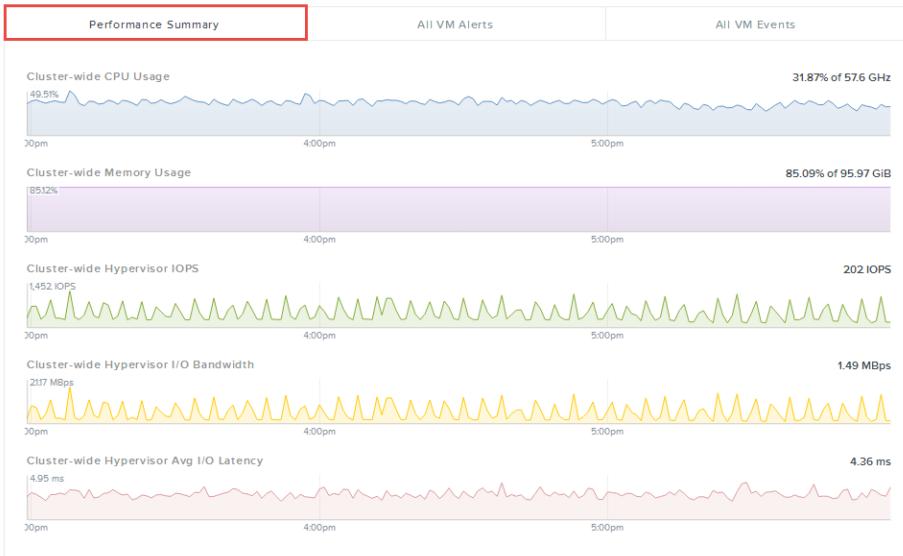
The graphs are rolling time interval performance monitors that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add a monitor to the analysis page by clicking the blue link in the upper right of the graph (see [Analysis Dashboard](#) on page 401). 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.



*Figure: VM Table View: Performance Tab*

## 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 Performance	Virtual Disks	VM NICs	VM Alerts	VM Events	I/O Metrics	Console
Default		Additional Stats				
VIRTUAL DISK	TOTAL CAPACITY	PHYSICAL USAGE	READ IOPS	READ BW	READ LATENCY	WRITE IOPS
/ruthent_ebf_retest_0vm0_0_retest_0vm0.vmdk	10 GB	4.94 GB	0	0 KBps	0 ms	0
/default-container-54681_v_retest_0vm0_0_retest_0vm0.vmdk	10 GB	-	0	0 KBps	0 ms	0

Figure: Virtual Disks Tab

## 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.

VM Performance	Virtual Disks	VM NICs	VM Alerts	VM Events
VIRTUAL NIC	ADAPTER TYPE	MAC ADDRESS	IPV4 ADDRESSES	IPV6 ADDRESSES
Network adapter 1	vmsmoe3	00:50:56:ba:60:c0	10.4.34.49/22	fe80::250:56ff:feba:60c0/64 fe80::250:56ff:feba:7944/64
Network adapter 2	vmsmoe3	00:50:56:ba:79:74	-	-

Figure: VM NICs Tab

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.



Figure: VM NICs Tab: Virtual NIC Stats

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.

Virtual NICs Stats		Host NICs Stats				Physical Switch Interface Stats		
HOST NIC	SPEED (IN KBPS)	MAC ADDRESS	RX PKTS	TX PKTS	DROPPED RX PKTS	DROPPED TX PKTS	RX PKT ERRORS	TX PKT ERRORS
vmmnic0	1250000	00:25:90:e7:8d:0c	79,044	140,094	0	0	0	0
vmmnic3		00:25:90:de:36:c7	0	0	0	0	0	0
vmmnic1		00:25:90:e7:8d:0d	0	0	0	0	0	0
vmmnic2	125000	00:25:90:de:36:c6	334	0	0	0	0	0

Figure: Virtual NICs Tab: Host NIC Stats

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.

Virtual NICs Stats			Host NICs Stats			Physical Switch Interface Stats					
Physical Switch Interface	Switch ID	Index	MTU (in Bytes)	MAC Address	Unicast Rx Pkts	Unicast Tx Pkts	Error Rx Pkts	Error Tx Pkts	Discard Rx Pkts	Discard Tx Pkts	
Ethernet22/3	drt-rf3-swl	22003	9214	0:fc:73:54:fb:e4	23463	24199	0	0	0	0	

Figure: Virtual NICs Tab: Physical Switch Interface Stats

## 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 (see [Alert Messages View](#) on page 411). 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 (see [Event Messages View](#) on page 413). 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 (see [Creating a VM \(AHV\)](#) on page 366) plus a creation time stamp field.

The screenshot shows a modal dialog titled "Snapshot Details". The window is divided into several sections: General Configuration, Compute Details, and Disk details. In the General Configuration section, the NAME is listed as "NTNX-lb-rc3-3". Under Compute Details, the CREATE TIME is "12/16/16, 11:46:35 AM", VCPUs is "4", and NUMBER OF CORES PER VCPU is "12". The MEMORY is listed as "12 GiB". The Disk section shows a table with columns for TYPE, ADDRESS, and PARAMETERS, which is currently empty.

TYPE	ADDRESS	PARAMETERS

Figure: Snapshot Details Window

- Click the **Clone** link to clone a VM from the snapshot (see [Managing a VM \(AHV\)](#) on page 372).
- 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 Performance	Virtual Disks	VM NICs	VM Snapshots	VM Tasks	I/O Metrics	Console
CREATE TIME 12/16/16, 11:46:35 AM	NAME test			ACTIONS Details · Clone · Restore · Delete	1 Snapshot - < > ⌂ 🔍 search in table	Q

Figure: VM Snapshots Tab

## 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.

VM Performance	Virtual Disks	VM NICs	VM Snapshots	VM Tasks	I/O Metrics	Console
OPERATION	ENTITIES			PERCENT COMPLETE PROGRESS STATUS	CREATE TIME	DURATION
Create Snapshot	VM: NTKX-bc3-3 Snapshot: test			100 Succeeded	12/16/16, 11:46:35 AM	Under 1 second
VmSetPowerState	VM: NTKX-bc3-3 Node: NTKX-95M65320008-B			100 Succeeded	12/16/16, 3:17:36 PM	4 seconds
Create Virtual Disk	VM: NTKX-bc3-3			100 Succeeded	12/16/16, 3:17:36 PM	Under 1 second
Create Virtual Disk	VM: NTKX-bc3-3			100 Succeeded	12/16/16, 3:17:36 PM	Under 1 second
Create Virtual Disk	VM: NTKX-bc3-3			100 Succeeded	12/16/16, 3:17:22 PM	11 seconds
Create Virtual Disk	VM: NTKX-bc3-3			100 Succeeded	12/16/16, 3:17:20 PM	Under 1 second
VmSetPowerState	VM: NTKX-bc3-3 Node: NTKX-95M65320008-B			100 Succeeded	12/16/16, 3:17:17 PM	2 seconds
VmSetPowerState	VM: NTKX-bc3-3 Node: NTKX-95M65320008-B			100 Succeeded	12/16/16, 3:14:31 PM	2 seconds
Update	VM: NTKX-bc3-3			100 Succeeded	12/16/16, 3:14:20 PM	Under 1 second
Create	VM: NTKX-bc3-3			100 Succeeded	12/16/16, 3:14:22 PM	Under 1 second

Figure: [All] VM Tasks Tab

## 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.



Figure: I/O Metrics Tab

## 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.

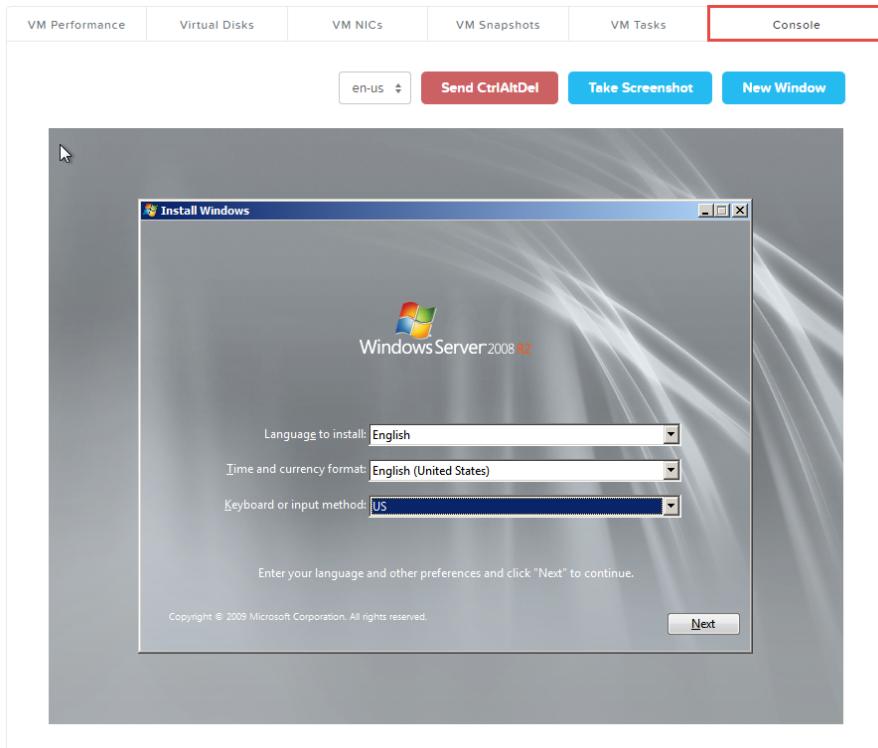


Figure: Console Tab

## VM Management

You can create and manage VMs directly from *Prism Element* when the hypervisor is either ESXi or AHV. Following topics provide more information on creating and managing VM configuration on ESXi and AHV.

- ESXi
  - To create a VM, see [Creating a VM \(ESXi\)](#) on page 377.
  - To manage guest tools, launch VM console, power actions, clone, update, or delete operations, see [Managing a VM \(ESXi\)](#) on page 379.
- AHV
  - To create a VM, see [Creating a VM \(AHV\)](#) on page 366.
  - 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 372.

### Creating a VM (AHV)

In Acropolis managed clusters, you can create a new virtual machine (VM) through the web console.

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:

1. 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.

**Create VM**

?

X

**General Configuration**

NAME

Name

DESCRIPTION

Optional

Use this VM as an agent VM

**Compute Details**

VCPUs

Value

NUMBER OF CORES PER VCPU

1

MEMORY

Value  GiB

**Graphics**

No GPUs have been added.

**Disks**

+ Add New Disk

BOOT	DEVICE	TYPE	ADDRESS	PARAMETERS	⋮	X
	CD-ROM			EMPTY=true; BUS=ide	<input type="button" value="Edit"/>	<input type="button" value="X"/>

**Volume Groups**

Please create a VM before you can add a volume group.

**Network Adapters (NIC)**

You haven't added any NICs yet.

**VM Host Affinity**

You haven't pinned the VM to any hosts yet.

Custom Script

The dialog box is titled 'Create VM' at the top. It contains several sections: 'General Configuration' (with fields for Name and Description, and a checkbox for 'Use this VM as an agent VM'); 'Compute Details' (with fields for VCPUs, Number of Cores per VCPU, and Memory); 'Graphics' (showing a message 'No GPUs have been added.' and a 'Add GPU' button); 'Disks' (listing one entry for a CD-ROM with parameters 'EMPTY=true; BUS=ide'); 'Volume Groups' (with a message 'Please create a VM before you can add a volume group.' and a 'Add Volume Group' button); 'Network Adapters (NIC)' (with a message 'You haven't added any NICs yet.' and a 'Add New NIC' button); and 'VM Host Affinity' (with a message 'You haven't pinned the VM to any hosts yet.' and a 'Set Affinity' button). At the bottom, there is a 'Custom Script' checkbox and a 'Cancel/Save' button.

Figure: Create VM Dialog Box

2. 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. **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 rest of VMs are powered on the host) and must be powered off and migrated after rest of the VMs (for example, during maintenance mode operations).
  - 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 MiBs) to allocate to this VM.
3. (For GPU-enabled AHV clusters only) To configure GPU pass-through for the VM, do the following:
  - a. In the **Graphics** section, click **Add GPU**.
  - b. In the **Add GPU** dialog box, 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. 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.
4. To attach a disk to the VM, click the **Add New Disk** button.  
The Add Disks dialog box appears.

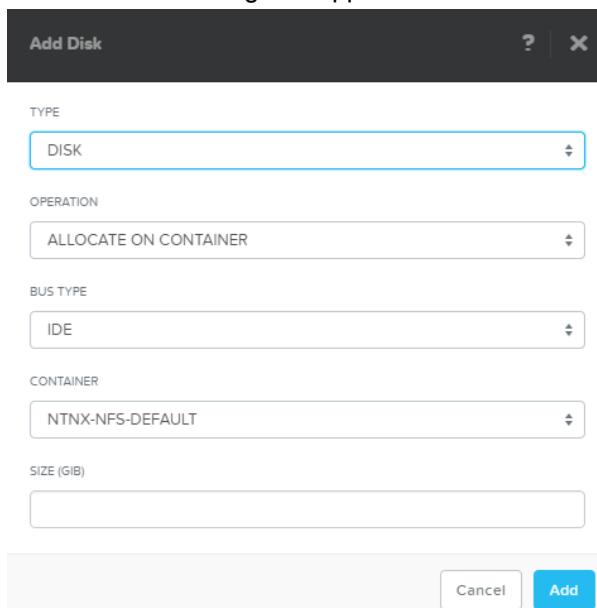


Figure: Add Disk Dialog Box

Do the following in the indicated fields:

- a. **Type:** Select the type of storage device, **DISK** or **CD-ROM**, from the pull-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 pull-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 on the Image Service feature, see the *Image Service* section of *Acropolis App Mobility Fabric Guide*.
- c. Bus Type:** Select the bus type from the pull-down list. The choices are **IDE**, **SCSI**, or **SATA**.
- 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 pull-down list.
- This field appears only when **Allocate on Storage Container** is selected. The list includes all storage containers created for this cluster.
- g. Size:** Enter the disk size in GiBs.
- h.** 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.
- i.** Repeat this step to attach additional 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.

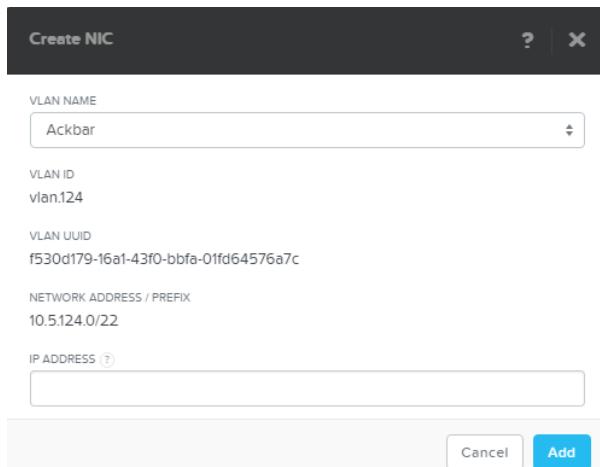


Figure: Create NIC Dialog Box

Do the following in the indicated fields:

- a. **VLAN Name:** Select the target virtual LAN from the pull-down list.  
The list includes all defined networks (see [Configuring Network Connections](#) on page 151).
- b. **VLAN ID:** This is a read-only field that displays the VLAN ID.
- c. **VLAN UUID:** This is a read-only field that displays the VLAN UUID.
- d. **Network Address/Prefix:** This is a read-only field that displays the network IP address and prefix.
- e. **IP Address:** Enter an IP address for the VLAN.

This field appears only if the NIC is placed in a managed network. Entering an IP address in this field is optional when the network configuration provides an IP pool. If the field is left blank, the NIC is assigned an IP address from the pool.

- f. 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.
- g. Repeat this step to create additional network interfaces for the VM.

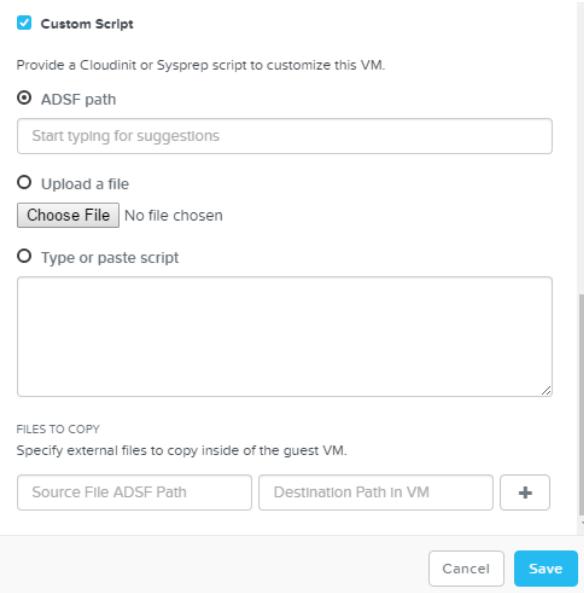
**6.** To configure affinity policy for this VM, click **Set Affinity**.

- 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.

**7.** 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.



*Figure: Create VM Dialog Box (custom script fields)*

8. 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.
9. 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 ADSF prefix (adsf://) followed by the absolute path to the file. For example, if the file is /home/my\_dir/myfile.txt, enter adsf:///home/my\_dir/myfile.txt. Note the use of three slashes.
  - b. In **Destination Path in VM**, enter the absolute path to the target directory.  
You do not have to enter a path prefix in this field.
  - 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.
10. 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 (see [VM Table View](#) on page 354).

## Managing a VM (AHV)

You can use the web console to manage virtual machines (VMs) in Acropolis managed clusters.

After creating a VM (see [Creating a VM \(AHV\)](#) on page 366), you can use the web console to start or shut down the VM, pause or resume 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. To accomplish one or more of these tasks, do the following:

1. In the VM dashboard, click the **Table** view.
2. 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. The possible actions are **Manage Guest Tools**, **Launch Console**, **Power on** (or **Power off**), **Take Snapshot**, **Migrate**, **Pause** (or **Resume**), **Clone**, **Update**, and **Delete**. The following steps describe how to perform each action.

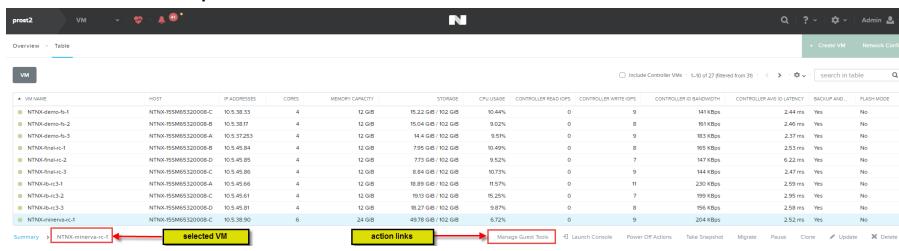


Figure: VM Action Links

3. 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.

- a. Select **Enable Nutanix Guest Tools** check box to enable NGT on the selected VM.

- b. Select **Mount Nutanix Guest Tools** 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.

- c. To enable self-service restore feature for Windows VMs, click **Self Service Restore (SSR)** check box.

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 more information on self-service restore feature, see [Self-Service Restore](#) on page 334.

- d. After you select **Enable Nutanix Guest Tools** check box 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 [Data Protection Guidelines \(Async DR\)](#) on page 250.

- e. 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.

- If you want to enable NGT on multiple VMs simultaneously, see [Enabling and Mounting NGT Simultaneously on Multiple VMs](#) on page 396.

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 need to unmount the ISO, remount the ISO, install the NGT software again, and then upgrade to 4.6 or later version.

4. 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 VM power options that you access from the **Power On Actions** (or **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.

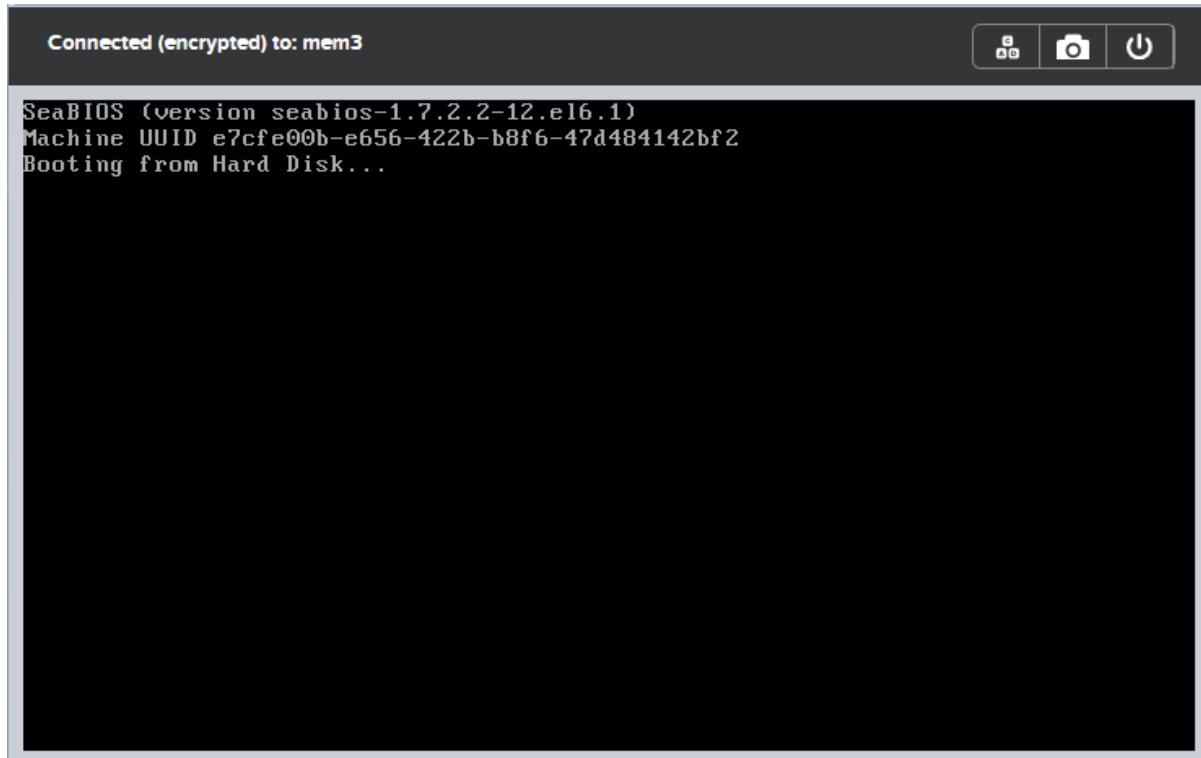


Figure: Virtual Network Computing (VNC) Window

 **Note:** A VNC client may not function properly on all browsers. Some keys are not recognized when the browser is Chrome. (Firefox typically works best.)

5. To start or shut down the VM, click the **Power on** (or **Power off**) action link.

Power on begins immediately, but you are prompted to select an option (**Power Off**, **Power Cycle**, **Reset**, **Guest Shutdown**, or **Guest Reboot**) when powering off.

6. To make a backup of the VM, click the **Take Snapshot** action link.

This displays the Take Snapshot dialog box. Enter a name for the snapshot and then click the **Submit** button to start the backup.

 **Note:** These snapshots (stored locally) cannot be replicated to other sites.

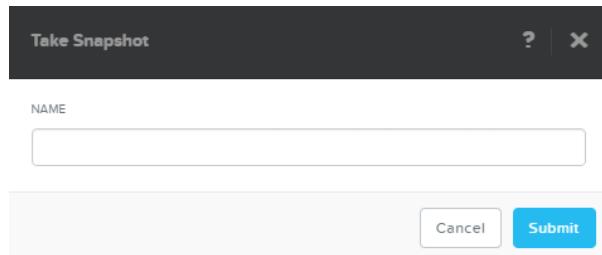


Figure: Take Snapshot Dialog Box

7. 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 pull-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.

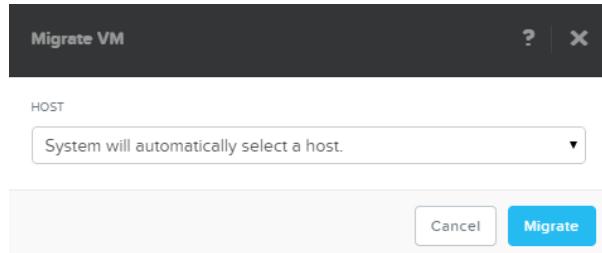
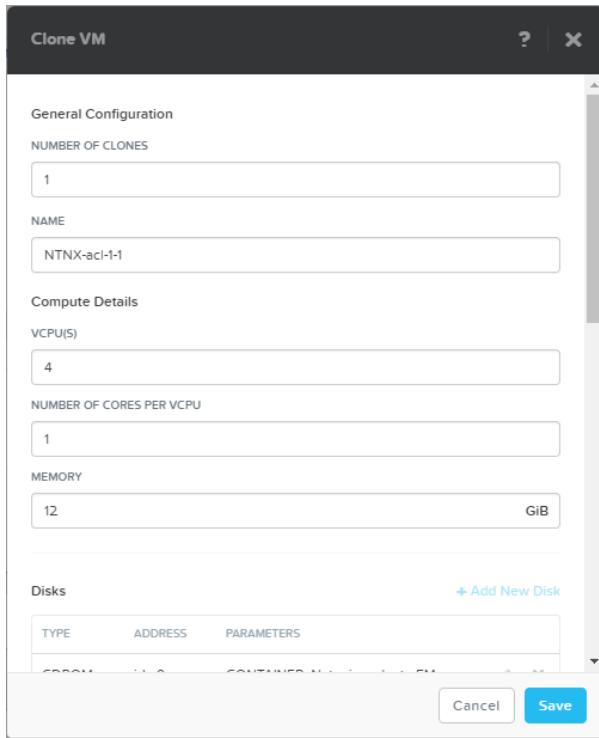


Figure: Migrate VM Dialog Box

8. To pause (or resume) the VM, click the **Pause** (or **Resume**) action link. This option is available only when the VM is powered on.

9. To clone the VM, click the **Clone** action link.

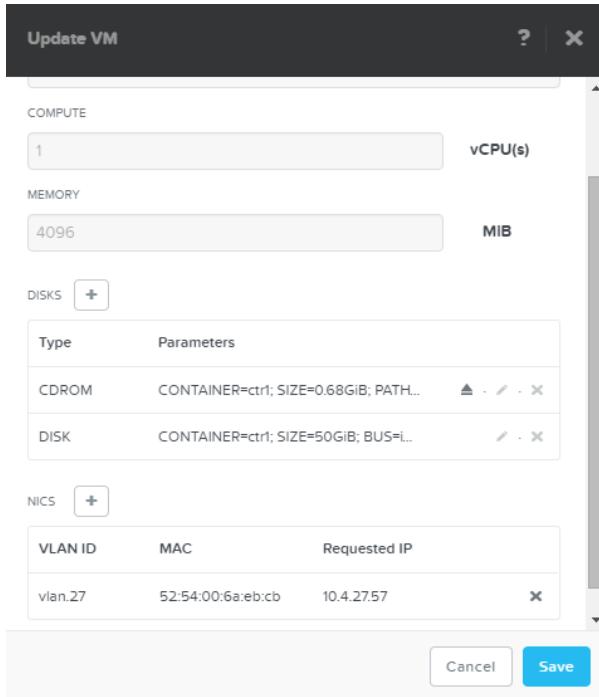
This displays the Clone VM dialog box, which includes the same fields as the Create VM dialog box but with all fields (except the name) filled in with the current VM settings and number of clones needed. Enter a name for the clone and number of clones of the VM that are required and then click the **Save** button to create the clone. You can create a modified clone by changing some of the settings. You can also customize the VM during initialization by providing a custom script and specifying files needed during the customization process (see [Creating a VM \(AHV\)](#) on page 366).



*Figure: Clone VM Dialog Box*

- 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 (see [Creating a VM \(AHV\)](#) on page 366), 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.



*Figure: VM Update Dialog Box*

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 (see [Creating a Volume Group](#) on page 147). 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**.
- a. 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), 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 deselect the **Enable Flash Mode** check box.

11. 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.

## Creating a VM (ESXi)

In ESXi clusters, you can create a new virtual machine (VM) through the web console.

### Before you begin:

- See the requirements and limitations section in the [VM Management through Prism Element \(ESXi\)](#) on page 584 before proceeding.
- Register the vCenter Server with your cluster. For more information, see [Registering a vCenter Server](#) on page 585.

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:

1. In the VM dashboard , click the **Create VM** button.  
The *Create VM* dialog box appears.
2. 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. See the list of supported operating systems in [VM Management through Prism Element \(ESXi\)](#) on page 584 topic.

- 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.
3. To attach a disk to the VM, click the **Add New Disk** button.  
The Add Disks dialog box appears.

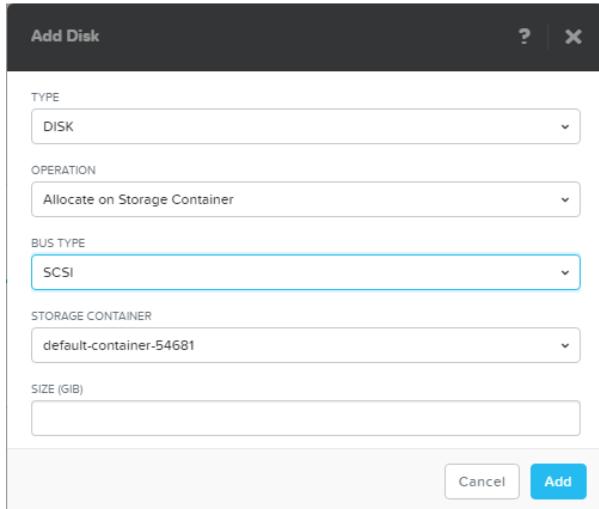


Figure: Add Disk Dialog Box

Do the following in the indicated fields:

- a. **Type:** Select the type of storage device, **DISK** or **CD-ROM**, from the pull-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 pull-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 pull-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.vmdk` in a storage container named `crt1`, enter `/crt1/myvm.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).
- e. **Storage Container:** Select the storage container to use from the pull-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 additional devices to the VM.
4. 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 pull-down list.  
The list includes all defined networks (see *Configuring Network Connections* on page 151).
  - b. **Network Adapter Type:** Select the network adapter type from the pull-down list. See *VM Management through Prism Element (ESXi)* on page 584 for the list of supported adapter types
  - 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 additional network interfaces for the VM.
5. 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 (see *VM Table View* on page 354).

## Managing a VM (ESXi)

You can use the web console to manage virtual machines (VMs) in the ESXi clusters.

### Before you begin:

- See the requirements and limitations section in the *VM Management through Prism Element (ESXi)* on page 584 before proceeding.
- Ensure that you have registered the vCenter Server with your cluster. For more information, see *Registering a vCenter Server* on page 585.

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:

1. In the VM dashboard , click the **Table** view.
2. 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. 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.

VM NAME	HOST	IP ADDRESSES	CORES	MEMORY CAPACITY	STORAGE	CPU USAGE	MEMORY USAGE	CONTROLLER READ IOPS	CONTROLLER WRITE IOPS	CONTROLLER IO BANDWIDTH	CONTROLLER AVG LATENCY	BACKUP AND...	FLASH MODE
uvm_0v0	teramtu-2	10.5.200.95...	8	2 GB	4.11 GB / 12 GB	0.05%	199%	0	0	0 KBps	0 ms	Yes	No
uvm_0v3	teramtu-4	10.5.200.95...	8	2 GB	4.11 GB / 12 GB	0.05%	0.99%	0	0	0 KBps	0 ms	Yes	No
uvm_0v4	teramtu-4	10.5.200.95...	8	2 GB	4.11 GB / 12 GB	0.05%	0%	0	0	0 KBps	0 ms	Yes	No
uvm_0v6	teramtu-3	10.5.200.95...	8	2 GB	4.11 GB / 12 GB	0.05%	199%	0	0	0 KBps	0 ms	Yes	No
uvm_0v9	teramtu-2	8	2 GB	4.17 GB / 12 GB	0.05%	0%	0	0	0	0 KBps	0 ms	Yes	No
uvm_0v9-clone-1-1	teramtu-2	8	2 GB	4.17 GB / 12 GB	0%	0%	0	0	0	0 KBps	0 ms	Yes	No
uvm_0v9-clone-1-10	teramtu-2	8	2 GB	4.17 GB / 12 GB	0%	0%	0	0	0	0 KBps	0 ms	Yes	No
uvm_0v9-clone-1-100	teramtu-2	8	2 GB	4.17 GB / 12 GB	0%	0%	0	0	0	0 KBps	0 ms	Yes	No
uvm_0v9-clone-1-11	teramtu-2	8	2 GB	4.17 GB / 12 GB	0%	0%	0	0	0	0 KBps	0 ms	Yes	No
uvm_0v9-clone-1-12	teramtu-2	8	2 GB	4.17 GB / 12 GB	0%	0%	0	0	0	0 KBps	0 ms	Yes	No

Figure: VM Action Links

### 3. 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.

- Select **Enable Nutanix Guest Tools** check box to enable NGT on the selected VM.

- Select **Mount Nutanix Guest Tools** 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, click **Self Service Restore (SSR)** check box.

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 more information on self-service restore feature, see [Self-Service Restore](#) on page 334.

- After you select **Enable Nutanix Guest Tools** check box 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 [Data Protection Guidelines \(Async DR\)](#) on page 250.

- To mount VMware guest tools, click **Mount VMware Guest Tools** check box.

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.

- 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.
- If you want to enable NGT on multiple VMs simultaneously, see [Enabling and Mounting NGT Simultaneously on Multiple VMs](#) on page 396.

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 need to unmount the ISO, remount the ISO, install the NGT software again, and then upgrade to 4.6 or later version.

4. 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 Chrome. (Firefox typically works best.)

5. To start (or shut down) the VM, click the **Power on** (or **Power off**) action link.

Power on begins immediately, but you are prompted to select an option (**Power Off**, **Reset**, **Guest Shutdown**, or **Guest Reboot**) when powering off.



**Note:** The **Guest Shutdown** and **Guest Reboot** options are available only when VMware guest tools are installed.

6. To pause (or resume) the VM, click the **Suspend** (or **Resume**) action link. This option is available only when the VM is powered on.

7. 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 but with all fields (except the name) filled in with the current VM settings and number of clones needed. Enter a name for the clone and number of clones of the VM that are required and then click the **Save** button to create the clone.

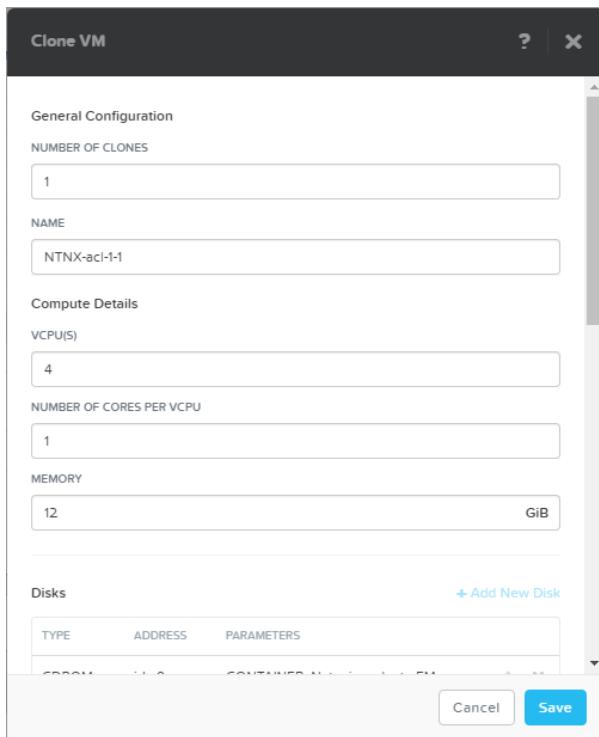


Figure: Clone VM Dialog Box



**Note:** In the Clone window, you cannot update the disks and network interfaces.

8. 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 (see [Creating a VM \(ESXi\)](#) on page 377), and in addition you can enable flash mode for the VM.

- a. 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), 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 deselect the **Enable Flash Mode** check box.

9. 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 Acropolis managed clusters, you can import and configure operating system ISO and disk image files through the web console.

The image service feature allows you 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, vdi, iso, and qcow2 disk formats. To import and configure an image file, do the following:

1. In the task icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Image Configuration**.

The *Image Configuration* window appears.

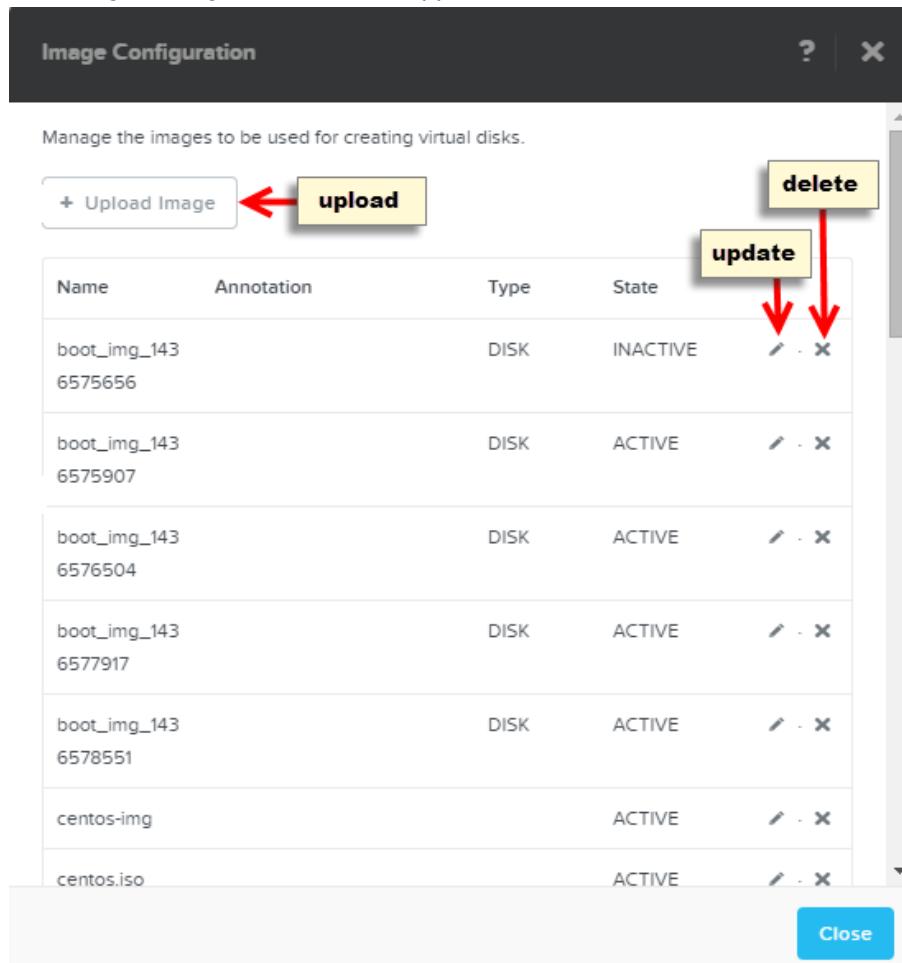


Figure: Image Configuration Window

2. 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:

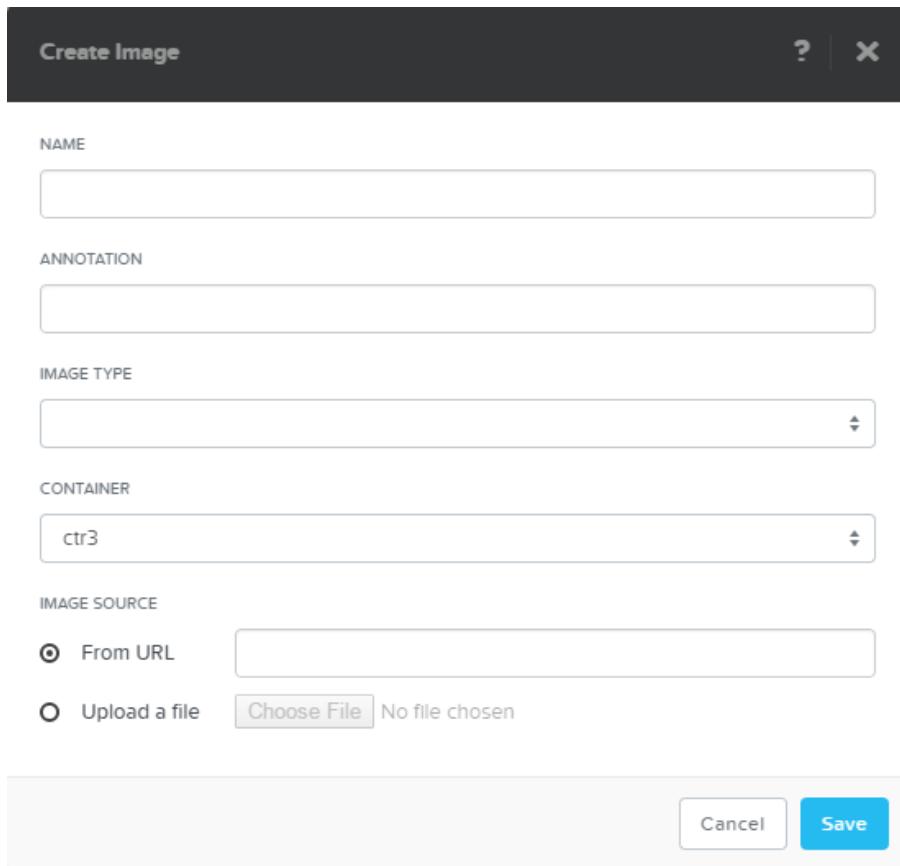


Figure: Create Image Window

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 (see [Creating a Storage Container](#) on page 139).

e. **Image Source:** Do one of the following:

- Click the **From URL** radio button 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://[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 (see [Configuring Name Servers](#) on page 570). A file uploaded through NFS must have 644 permissions.

- Click the **Upload a file** radio button 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.

3. 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.

4. 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 Sysprep documentation at <https://technet.microsoft.com/>.

### 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.

To customize a Linux VM by using Cloud-init, do the following:

1. Log in to the web console by using the Nutanix credentials.
2. In the VM dashboard (see [VM Dashboard](#) on page 352), 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 366. For information about cloning a VM, see [Managing a VM \(AHV\)](#) on page 372.
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. See Image Service in the VM Management chapter of the *Acropolis App Mobility Fabric Guide*.

## Customization of Windows Virtual Machines with System Preparation

To customize a Windows VM by using Sysprep, you need to perform the following tasks:

1. Create a reference image by using Sysprep.
2. 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 web console. If you have files that need to be copied to the temporary ISO image, upload the files to a storage container on the cluster.

### **Creating 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.

To create a reference image, do the following:

1. Log in to the web console by using the Nutanix credentials, and then browse to the VM dashboard (see [VM Dashboard](#) on page 352).
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.



**Note:** Make sure to shut down the VM. Restarting the VM will result 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. To create a reference image from the VM, use Image Service. See Image Service in the VM Management chapter of the Acropolis App Mobility Fabric Guide.

#### **Creating a Customized Virtual Machine from a Reference Image**

To use a reference image, do the following:

1. Log in to the web console by using the Nutanix credentials, and then browse to the VM dashboard (see [VM Dashboard](#) on page 352).
2. Click **Create VM**, and then, in the **Create VM** dialog box, do the following:
  - 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 366.

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. See Image Service in the VM Management chapter of the *Acropolis App Mobility Fabric Guide*.

#### **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.

To customize a fresh installation of Windows by using Sysprep, do the following:

1. Log in to the web console by using the Nutanix credentials, and then browse to the VM dashboard (see [VM Dashboard](#) on page 352).
2. Click **Create VM**, specify the details that are required for installing Windows on the new VM, and then do the following:
  - a. Specify a name for the VM and allocate resources such as vCPUs, memory, and storage.
  - b. In the **Disk** 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 about creating a VM, see [Creating a VM \(AHV\)](#) on page 366.

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. See Image Service in the VM Management chapter of the *Acropolis App Mobility Fabric Guide*.

## VM High Availability in Acropolis

If you have not modified high availability configuration from previous version of AOS releases, best effort VM availability is by default implemented in Acropolis.

If you have not enabled high availability, in case of host failure VMs are restarted from the failed host to any available space on the other hosts in the cluster. Once the failed host joins the cluster again, VMs are migrated back to the host. This type of VM high availability is implemented without reserving any resources. Admission control is not enforced and hence there may not be sufficient capacity available to start all the VMs.



**Note:** Nutanix does not support VMs that are running with 100% remote storage for high availability. The VMs must have at least one local disk that is present on the cluster.

VM high availability can be configured for host based reservations using segment-based reservation method which is the default.



**Note:** If you have enabled VM high availability feature with reserve host method in pre-5.0 release and then upgraded your cluster to AOS 5.0 or later releases, the HA configuration is automatically converted to segment-based reservation method after the upgrade process is completed.

In segment-based reservation, the cluster is divided into segments to ensure enough space is reserved for any host failure. Each segment corresponds to the largest VM that is guaranteed to be restarted in case the failure occurs. The other factor is the number of host failures that can be tolerated. Using these inputs, the scheduler implements admission control to always have enough resources reserved so that the VMs can be restarted upon failure of any host in the cluster.

The segment size ensures that the largest VM can be powered on in HA failover when cluster is fully loaded (if the cluster is fully used except the reserved segments). The number of segments that is reserved is such a way that for each host enough resources are reserved to ensure any host failure in the cluster is tolerated. Multiple VMs may fit into a segment. If anything changes in the cluster, the reservation is computed again. 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 fragmentation of segments. 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 (in case of host upgrade), you might not be protected against further host failures. Maintenance mode uses reservations made for HA for migrating VMs from the host. Although, you are not protected against host failure if you have reservation for HA, hypervisor upgrade occurs without any difficulty because from the perspective of a user it is exactly the same as host failure except that the VMs are migrated (instead of restarted) and hence no runtime state is lost. The HA status goes through the same states as it goes when the host failure had occurred.

Segment-based reservation is the default method that Acropolis uses to enable VM high availability. However, you can update the HA configuration for a host by using the aCLI command. For example,

```
acli> ha.update enable_failover=true num_host_failures_to_tolerate=1  
reservation_type=kAcropolisHAReserveHosts
```



**Note:**

- It is not recommended to use reserved host method to configure HA.
- You will not be able to configure HA to reserved host on a cluster that has VMs with host affinity configured.

In the reserved host method, an entire host is reserved for failover protection. The least used host in the cluster is selected as a reserve host, and all the VMs on that host are migrated off to other hosts in the cluster so that the full capacity of that host is available for VM failover. When a host fails, the reserved host becomes the destination host, and all the VMs from the failed host are restarted on the reserved host. The reserved host now becomes a normal host and you can schedule VMs on this host.



**Note:** At this time, the cluster is not protected for any further host failures if you have configured redundancy factor of 2.

Once the failed host comes back up, the VMs are migrated back from the reserved host to the host that came back up and the cluster is protected against further host failures. The reserved host again becomes empty and you cannot schedule VMs on this host.



**Note:** The number of hosts reserved for VM failover protection depends on the redundancy factor setting of the cluster. A single host is reserved when the redundancy factor is 2, but more than one can be reserved when the redundancy factor is 3.

## Enabling High Availability for the Cluster

In Acropolis managed clusters, you can enable high availability for the cluster to ensure that VMs can be migrated and restarted on another host in case of failure.

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.

1. In the gear icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Manage VM High Availability**.



**Note:** This option does not appear in clusters that do not support this feature.

The *Manage VM High Availability* window appears.

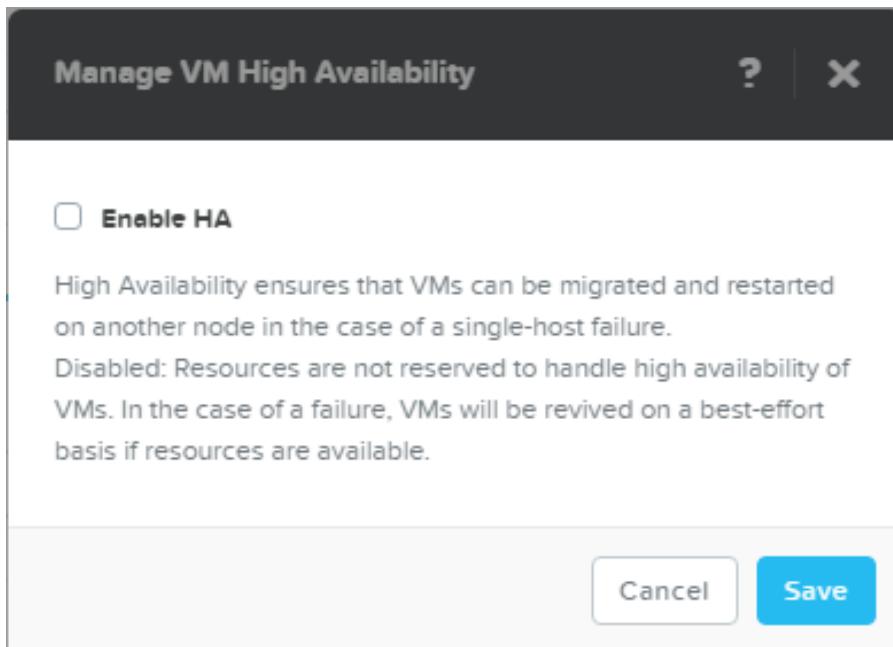


Figure: Manage VM High Availability Window

2. Set the **Enable HA** button to enable.

## Nutanix Guest Tools

Nutanix guest tools (NGT) is a software bundle that you can install in a guest virtual machine (Microsoft Windows or Linux) to enable the advanced functionality provided by Nutanix.

The NGT bundle consists of the following components.

- Nutanix Guest Agent (NGA) service. Communicates with the Nutanix Controller VM.
- File Level Restore CLI. Performs self-service file-level recovery from the VM snapshots. For more information about self-service restore, see [Self-Service Restore](#) on page 334.
- Nutanix VM Mobility Drivers. Facilitates by providing drivers for VM migration between ESXi and AHV, in-place hypervisor conversion, and cross-hypervisor disaster recovery (CH-DR) features. For more information about cross-hypervisor disaster recovery, see [Nutanix Cross Hypervisor Disaster Recovery](#) on page 331. For more information about in-place hypervisor conversion, see [In-Place Hypervisor Conversion](#) on page 586.
- VSS requestor and hardware provider for Windows VMs. Enables application-consistent snapshots of AHV or ESXi Windows VMs. For more information about Nutanix VSS-based snapshots for the Windows VMs, see the best practices section for taking application-consistent snapshots in [Data Protection Guidelines \(Async DR\)](#) on page 250.
- Application-consistent snapshot for Linux VMs. Supports application-consistent snapshots for Linux VMs by running specific scripts on VM quiesce. For more information about Nutanix VSS-based snapshots for the Linux VMs, see the best practices section for taking application-consistent snapshots in [Data Protection Guidelines \(Async DR\)](#) on page 250.

## Nutanix Guest Tools Requirements and Limitations

All the features that use NGT should conform to the following requirements.

## **General Requirements and Limitations**

- Virtual IP address must be configured on the Nutanix cluster. If the virtual IP address of the cluster changes, it will impact all the NGT instances that are running in your cluster. For more information, see [\*Impact of Changing Virtual IP Address of the Cluster\*](#) on page 44.
- VMs must have at least one empty IDE CD-ROM slot to attach the ISO.
- Port 2074 should be open to communicate with the NGT-Controller VM service.
- Hypervisor: ESXi 5.1 or later release, AHV (20160215 or later version).
- VMs should be connected to a network that can be accessed by using the virtual IP address of the cluster.

## Operating Systems Supported

### Operating System Supported for NGT

Operating System	Version	Requirements and Limitations
Windows	<ul style="list-style-type: none"><li>Windows 2008 R2 or later versions</li><li>Windows 7 or later versions</li></ul>	<ul style="list-style-type: none"><li>Only 64-bit operating system is supported.</li></ul> <p> <b>Note:</b></p> <ul style="list-style-type: none"><li>For AOS 5.1 and pre-AOS 5.1 releases, on Windows 7 and Windows 2008 R2 operating systems, you must install SHA-2 code signing support update before installing NGT. For more information on installing SHA-2 support for Windows, <a href="#">Microsoft Documentation</a>.</li></ul> <p> <b>Note:</b> From AOS 5.1.1 release onwards, SHA-1 and SHA-2 support is provided in Nutanix mobility drivers. Hence, you do not need to manually install SHA-2 support for Windows.</p> <ul style="list-style-type: none"><li>For Windows Server Edition VMs, ensure that Microsoft VSS services is enabled before starting the NGT installation.</li></ul>

Operating System	Version	Requirements and Limitations
Linux	<ul style="list-style-type: none"> <li>CentOS 6.5 and 7.0</li> <li>Red Hat Enterprise Linux (RHEL) 6.5 or later and RHEL 7.0 or later.</li> <li>Oracle Linux 6.5 and 7.0</li> <li>SUSE Linux Enterprise Server (SLES) 11 SP4 and 12</li> <li>Ubuntu 14.04</li> </ul>	<ul style="list-style-type: none"> <li>SLES operating system is only supported for application consistent snapshot with VSS feature. SLES operating system is not supported for cross-hypervisor disaster recovery feature.</li> </ul>

## Enabling and Mounting Nutanix Guest Tools

By using the Nutanix web console, you can enable and mount NGT on a VM.

1. Log in to the web console.
2. Go to table view of the **VM** dashboard.
3. Click **Manage Guest Tools**.

You can enable NGT applications (self-service restore, Volume Snapshot Service and application-consistent snapshots) also as part of manage guest tools.

- a. Select **Enable Nutanix Guest Tools** check box to enable NGT on the selected VM.

- b. Select **Mount Nutanix Guest Tools** 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.

- c. To enable self-service restore feature for Windows VMs, click **Self Service Restore (SSR)** check box.

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 more information on self-service restore feature, [Self-Service Restore](#) on page 334.

- d. After you select **Enable Nutanix Guest Tools** check box 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 [Data Protection Guidelines \(Async DR\)](#) on page 250.

- e. 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.

- If you want to enable NGT on multiple VMs simultaneously, see [Enabling and Mounting NGT Simultaneously on Multiple VMs](#) on page 396.

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 need to unmount the ISO, remount the ISO, install the NGT software again, and then upgrade to 4.6 or later version.

## Installing NGT on Windows Machines

After mounting NGT on a VM, you can configure your Windows machine to use NGT.

1. Log into the Windows guest VM.
2. In the explorer window, double-click the Nutanix icon labeled **X**.



**Note:** If you have mounted the NGT when VM is powered off, after powering on the VM this functionality does not work. You need to open the CD (right-click the CD and click **Open**) and then double-click setup.exe file.

3. Accept the license agreement and follow the prompts to configure NGT on the virtual machine. After installation finishes, Nutanix guest agents are installed on the VM and you can use all the NGT features (self-service restore after you manually enable the feature, cross-hypervisor disaster recovery, application-consistent snapshots with VSS on AHV, or in-place hypervisor conversion from ESXi to AHV).



**Note:** The Nutanix VSS HW Provider does not get automatically registered after installation. The process of registration starts after you take the snapshot of the VM and it automatically unregisters after the operation finishes.



**Caution:** If Nutanix VM mobility driver version gets upgraded on AHV during the installation process, a prompt that asks for reboot will be displayed. It is recommended to restart the VMs to upgrade the VM mobility driver version successfully.

## Installing NGT on Windows Machines (Silent Install)

You can use silent installer to install NGT on multiple windows machines simultaneously. You can achieve this by writing a custom script that uses the silent installer package. You can also install NGT on Windows machines silently (with reduced clicks) by using NGT silent installer package. The NGT silent installer package consists of the following components.

- Custom module that performs checks and fulfills all the prerequisites.

- Nutanix VM mobility
- Python
- Microsoft Visual C++ 2008/2012 x64 redistributable setup for Windows Server operating systems
- Nutanix VSS package
- Nutanix guest agent package

1. Open the command prompt and go to the drive on which NGT is mounted.

2. Install NGT by using silent installer.



**Caution:** On AHV, VMs might get restarted depending on the command that you use to install NGT by using silent installer. You can use any of the following commands for ESXi as VMs running on ESXi are not affected.

→ `drive:\> setup.exe /quiet ACCEPTEULA=yes /norestart`

Use this command to ensure that VMs are not restarted after installing NGT. Note that if you use this command drivers will not be updated. You need to manually restart the VMs to update the drivers.

→ `drive:\> setup.exe /quiet ACCEPTEULA=yes`

If you use this command, VMs are restarted and drivers are automatically updated.



**Note:** If the mobility driver version on the VM is same as the one that NGT is installing, then the VMs are not restarted.

Logs are generated in the **Event Viewer** and in the **%TEMP%** directory starting with **Nutanix\_Guest\_Tools\_timestamp**. Event Viewer logs for all the components are installed as part of the NGT installation.



**Note:** If you get any warnings after running this command, these warnings are treated as errors and are captured in the logs. If you want to ignore the warnings and complete the installation, you can use the flag `IGNOREALLWARNINGS=yes` in the command `drive:\> setup.exe /quiet ACCEPTEULA=yes IGNOREALLWARNINGS=yes`. If you enable this flag, all the warnings are ignored and the silent installation proceeds smoothly.

3. (Optional) Install NGT by using silent installer with a log parameter.

`drive:\> 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 **Event Viewer** and in the path that has been provided. No logs are generated in the **%TEMP%** directory. Ensure that the path you provided is capable of having new data written on it.



**Caution:** If Nutanix VM mobility driver version gets upgraded on AHV for Windows VMs during the silent installation process, then the VM will be restarted automatically after the NGT installation completes.

### Installing NGT on Linux Machines

After mounting NGT on a VM, you can configure your Linux machine to use NGT. Graphical Linux deployments auto-discover the CD-ROM and mount the CD-ROM appropriately. For non-graphical Linux deployments, use the following procedure.

**Before you begin:** Verify that Python 2.6 or 2.7 along with `python-setuptools` package is installed properly on your Linux machines.

1. Log into the Linux VM.

2. Create a temporary folder (`/mnt`) and mount the content of the CD in the temporary folder.

```
$ sudo mount /dev/sr0 /mnt
```

3. Run the `install_ngt.py` script.

```
$ sudo /mnt/installer/linux/install_ngt.py
```

After the installation finishes, Nutanix guest agents are installed on the VM and you can use the NGT features (cross-hypervisor disaster recovery, application-consistent snapshots with VSS on AHV, or in-place hypervisor conversion from ESXi to AHV).

## Enabling and Mounting NGT Simultaneously on Multiple VMs

You can enable and mount NGT simultaneously on multiple VMs by using the master VM image.

1. Install NGT on the master VM and ensure that the NGT service is communicating properly with the Controller VM.
2. Clone the required amount of VMs from the master VM.
3. For every cloned VM, login to the Controller VM and run the command.

```
ncli> ncli ngt mount vm-id=clone_vm_id
```

Replace `clone_vm_id` with the ID of the cloned VM.

4. Power on the cloned VM.

The Nutanix Guest Agent running in the VM:

- Detects that a new NGT CD-ROM ISO is attached.
- Copies all the relevant configuration files.
- Starts communicating with the Controller VM.
- Ejects the CD-ROM automatically.

## NGA and Controller VM Communication

After the installation of NGT is completed, the Nutanix Guest Agent (NGA) in the VM starts periodic communication with the NGT-Controller VM service over SSL connections.

NGA also publishes information about the VM to the NGT-Controller VM service, for example, guest OS type, status of VM mobility and VSS services, etc. Each Nutanix cluster is configured as a Certificate Authority (CA). When NGT is enabled on a VM, a certificate pair is generated for the specific VM and it is embedded in an ISO that is configured for this VM. The security certificates are installed inside the VM as part of the installation process.

The NGA service running inside the VM initiates an SSL connection to the virtual IP port 2074 of the Controller VM to communicate with the NGT-Controller VM service. No firewall change is required from the VM side. However the VM should be able to reach port 2074 through SSL on the Controller VM.

NGT provides three levels of security for the VM communication.

- SSL certificates
- Capability based authorization
- System/BIOS UUID of the VM should be same as seen by the hypervisor

Communication is successful only if all the three conditions are met. For example, if a VM that has NGT installed is cloned, then the new VM will not be able to communicate with the Controller VM.

## CD-ROM Eject Functionality of NGT

After the NGT software is installed on a VM, CD-ROM is auto-ejected from the VM in the following two stages.

1. CD-ROM is automatically ejected from the guest immediately after the installation of NGT is successfully completed.
2. NGA then indicates to the NGT-Controller VM service that the installation is complete, and the CD-ROM is detached from the VM through the hypervisor and destroyed. This operation depends on the periodicity of the VM and Controller VM communication and may take up to 10 minutes.



### Note:

- There can be a time difference between these operations. Hence there may be a possibility that the CD-ROM shows up as empty inside a VM, but from the NGT-Controller VM service **Tools Mounted** may be displayed as true. If this situation occurs, verify the hypervisor reported values.
- If the NGT software version in the ISO is greater than the installed version inside the VM, the CD-ROM does not get automatically ejected. This helps with the upgrade of the NGT software inside the VM.

## Nutanix Guest Tools Usage in Disaster Recovery

If a VM that is protected by the Nutanix data protection feature and has NGT enabled for it or vice-versa, the relevant NGT information including capabilities is added as part of the disaster recovery snapshot record.

If you migrate a VM to a remote site, restore it in place, or clone it from a snapshot, the NGT information is preserved for the restored VM. A new NGT ISO image containing only the relevant configuration information (SSL certificates, Controller VM IP address, etc.) is created for the recovered VM and the image is automatically attached to the VM.

When the VM is powered on, the NGA service running on the VM copies the relevant configuration information and detaches the CD-ROM automatically. If a VM snapshot that has NGT enabled is getting replicated to a remote cluster that does not support NGT (for example, AOS version previous to 4.5 release), an alert is raised.

Restoring a VM on the remote site or retrieving the snapshot back to the local or source cluster results in loss of NGT information or functionality. Hence the Nutanix administrator must enable NGT again for the restored VM.

## Upgrading NGT

If you have upgraded your AOS, you can also upgrade your NGT. NGT is not automatically upgraded. Following are some of the general guidelines of upgrading NGT.

### NGT Upgrade

- After upgrading AOS, you can choose to upgrade NGT. You need to manually upgrade NGT by new version of NGT on a VM. For more information about mounting NGT on a VM, see [Enabling and Mounting Nutanix Guest Tools](#) on page 393.
- If Nutanix VM mobility driver version gets upgraded on AHV for Windows VMs during the silent installation process, then the VM will be restarted automatically after the NGT installation completes.
- If Nutanix VM mobility driver version gets upgraded on AHV for Windows VMs during the GUI installation process, a prompt that asks for reboot will be displayed. It is recommended to restart the VMs to upgrade the VM mobility driver version successfully.

## Disabling and Removing Nutanix Guest Tools

You can use the Nutanix web console to disable NGT for a VM.

If you disable NGT, only communication between VM and NGT-Controller VM service is stopped. To completely remove NGT from the database you have to use the nCLI command.

### 1. To disable NGT.

- a. Log in to the web console.
- b. Go to table view of the **VM** dashboard.
- c. Select the VM on which you want to disable NGT.
- d. Click **Manage Guest Tools**.
- e. De-select the **Enable Nutanix Guest Tools** option.
- f. Click **Submit**.

Disabling NGT rejects any form of communication between the VM and NGT-Controller VM. The NGT software does not get uninstalled from the VM.

### 2. To uninstall NGT.

- a. Uninstall NGT from a VM by following the regular uninstall procedure of Windows and Linux.

For the Windows VMs, uninstalling the NGT software inside a VM does not uninstall the VM Mobility drivers. This ensures that the VM always have the required drivers for mobility purpose. For example, the VM might be migrated from one hypervisor to another and if drivers are uninstalled, the VM might not be able to start properly.

### 3. To delete the NGT entity.

- a. Log into the Controller VM.
- b. Run the following command.

```
ncli> ngt delete vm-id=virtual_machine_id
```

Replace *virtual\_machine\_id* with the ID of the virtual machine. Deleting the NGT entity clears any relevant NGT information for the VM.

If you delete the VMs on which NGT is enabled, the NGT entity is cleaned up automatically and the ISO files are also deleted.

## Affinity Policies for AHV

As an administrator in an Acropolis managed cluster, you can specify scheduling policies for virtual machines on an AHV cluster. By defining these policies, you can control placement of the virtual machines on the hosts within a cluster.

You can define two types of affinity policies.

## VM-Host Affinity Policy

The VM-host affinity policy controls the placement of the VMs. You can use this policy to specify that a selected VM can only run on the members of the affinity host list. This policy checks and enforces where a VM can be hosted when you power on or migrate the VM.



### Note:

- The VM-host affinity policy is a mandatory policy. This policy limits Acropolis HA and Acropolis Dynamic Scheduling (ADS) in such a way that a virtual machine cannot be powered on or migrated to a host that does not conform to requirements of the affinity policy.
- The VM-host anti-affinity policy is not supported.

You can use the VM-host affinity policy to meet the compliance and licensing requirements. For example, if you are paying for Oracle licenses only on a few sockets on a set of hosts within a larger cluster, you can use the VM-host affinity policy to ensure that the Oracle application on a VM is running on a specific host, thereby ensuring that you are not in violation of the Oracle licensing. This affinity policy is not violated even during the host HA events, even if it is possible to start the VM on the remaining 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 \(AHV\)](#) on page 366.

## VM-VM Anti-Affinity Policy

You can use this policy to specify anti-affinity between the virtual machines. The VM-VM anti-affinity policy keeps the specified virtual machines apart in such a way that when a problem occurs with one host, you should not lose both the virtual machines. However, this is a preferential policy. This policy does not limit the Acropolis Dynamic Scheduling (ADS) feature to take necessary action in case of resource constraints.



### Note:

- Currently, you can only define VM-VM anti-affinity policy by using aCLI. For more information, see [Configuring VM-VM Anti-Affinity Policy](#) on page 399.
- The VM-VM affinity policy is not supported.



**Note:** If a VM is cloned that has the affinity policies configured, then the policies are not automatically applied to the cloned VM. However, if a VM is restored from a DR snapshot, the policies are automatically applied to the VM.

## 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.
- The VM-host affinity cannot be configured on a cluster that has the HA configured by using reserved host method.
- You cannot remove the VM-host affinity for a powered on VM from Prism. You can use the `vm.affinity_unset vm_list` acli command to perform this operation.

## Configuring VM-VM Anti-Affinity Policy

Perform the following procedure to configure the VM-VM anti-affinity policy.

To configure VM-VM anti-affinity policies, you must first define a group and then add all the VMs on which you want to define VM-VM anti-affinity policy.



**Note:** Currently, the VM-VM affinity policy is not supported.

1. Log in to the Controller VM in your cluster through an SSH session and access the Acropolis command line.

2. Create a group.

```
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 anti-affinity to the group.

```
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.

4. Configure VM-VM anti-affinity policy.

```
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 attempted to be started on the different hosts. However, this is a preferential policy. This policy does not limit the Acropolis Dynamic Scheduling (ADS) feature to take necessary action in case of resource constraints.

### Removing VM-VM Anti-Affinity Policy

Perform the following procedure to remove the VM-VM anti-affinity policy.

1. Log in to the Controller VM in your cluster through an SSH session and access the Acropolis command line.

2. Remove the VM-VM anti-affinity policy.

```
acli> vm_group.antiaffinity_unset group_name
```

Replace *group\_name* with the name of the group.

The 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).

## 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 (see [Analysis Dashboard](#) on page 401).

### 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 (see [Main Menu Options](#) on page 32).

#### 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 **Scale** 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.

The following figure is a sample view, and the table describes each field in this view. 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:** See [Understanding Displayed Statistics](#) on page 41 for information about how the metrics are measured.

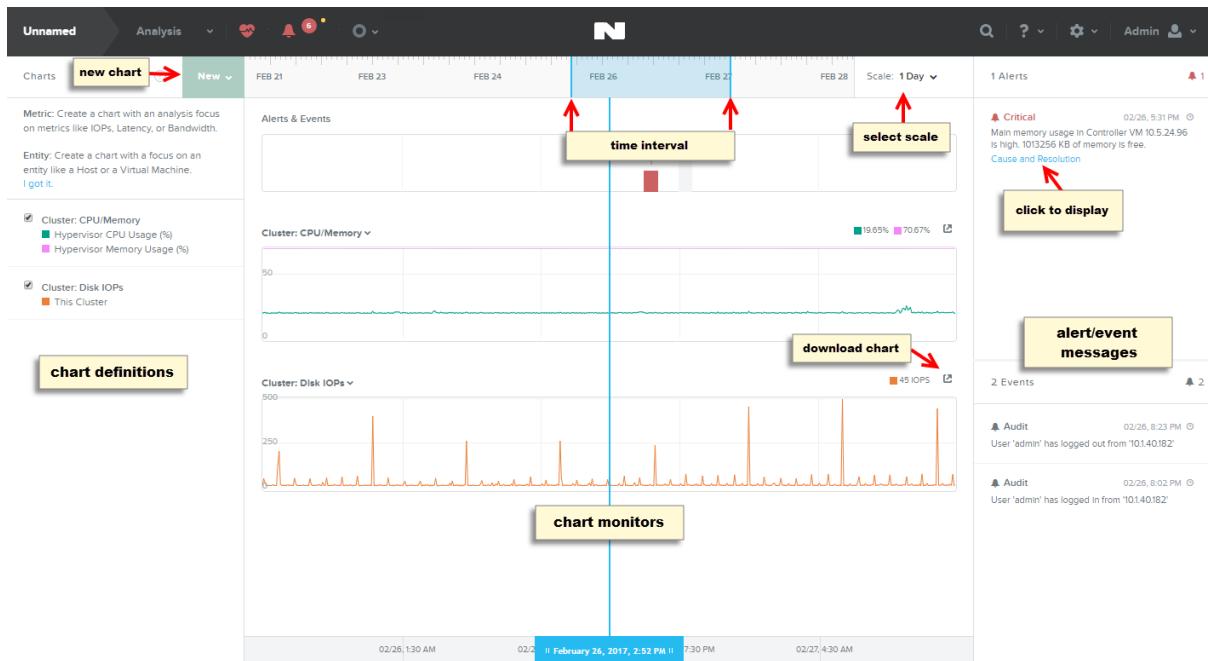


Figure: Analysis Dashboard

## 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 (see <a href="#">Creating a Metric Chart</a> on page 404).
New Entity Chart	Allows you to create a chart that tracks one or more metrics for a single entity (see <a href="#">Creating an Entity Chart</a> on page 403).
(range time line and monitor period)	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>Scale</b> field pull-down menu (far right of time line). To customize the monitor period, drag the time line end points to the desired times on the time line.
Alerts & Events Monitor	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).

Name	Description
(defined chart monitors)	<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> <p style="text-align: center;"> <span>Export Chart Data (CSV)...</span>  <span>Export Chart Data (JSON)...</span>  <span>Chart Link...</span> </p>
Alerts	<p>Displays the alert messages that occurred during the time interval (see <a href="#">Alerts Dashboard</a>). Clicking a message causes the monitor line to move to the time when that alert occurred.</p>
Events	<p>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.</p>

## Creating an Entity Chart

An entity chart monitors the performance of one or more metrics for a single entity. To create an entity chart definition, do the following:

1. In the Analysis dashboard (see [Analysis Dashboard](#) on page 401), click the **New Entity Chart** button. The *New Entity Chart* dialog box appears.
2. 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, 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 pull-down list. (Repeat to include additional metrics.)

For descriptions of the available metrics, see [Chart Metrics](#) on page 405.

3. 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.

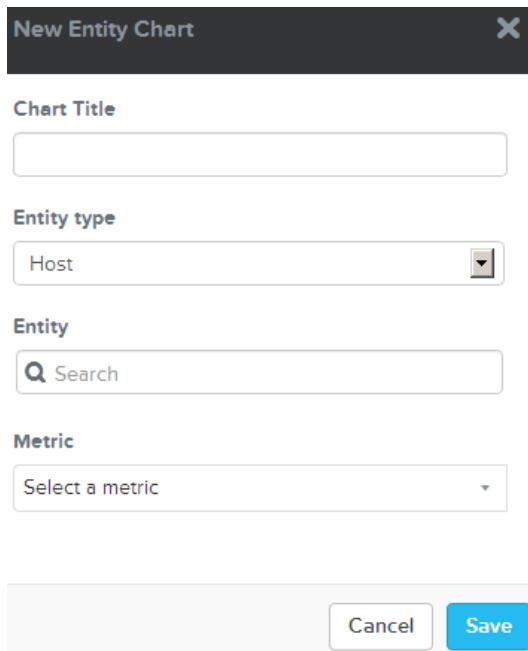


Figure: New Entity Chart Window

## Creating a Metric Chart

A metric chart monitors the performance of a single metric for one or more entities. To create a metric chart definition, do the following:

1. In the Analysis dashboard (see [Analysis Dashboard](#) on page 401), click the **New Metric Chart** button.

The *New Metric Chart* dialog box appears.

2. 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 405.

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.

3. 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.

New Metric Chart X

**Chart Title**

**Metric**  
 ▼

**Entity type**  
 ▼

**Entity**  
 Q

Cancel Save

Figure: New Metric Chart Window

## Chart Metrics

These metrics can be added to charts.

Metric	Description
Content Cache Hit Rate (%)	Content cache hits over all lookups. ID: <code>CONTENT_CACHE_HIT_PPM</code>
Content Cache Hits	Number of hits on the content cache. ID: <code>CONTENT_CACHE_NUM_HITS</code>
Content Cache Logical Memory Usage	Logical memory (in bytes) used to cache data without deduplication. ID: <code>CONTENT_CACHE_LOGICAL_MEMORY_USAGE_BYTES</code>
Content Cache Logical SSD Usage	Logical SSD memory (in bytes) used to cache data without deduplication. ID: <code>CONTENT_CACHE_LOGICAL_SSD_USAGE_BYTES</code>
Content Cache Lookups	Number of lookups on the content cache. ID: <code>CONTENT_CACHE_NUM_LOOKUPS</code>
Content Cache Memory Saved	Memory (in bytes) saved due to content cache deduplication. ID: <code>CONTENT_CACHE_SAVED_MEMORY_USAGE_BYTES</code>

Metric	Description
Content Cache Physical Memory Usage	Real memory (in bytes) used to cache data by the content cache. ID: CONTENT_CACHE_PHYSICAL_MEMORY_USAGE_BYTES
Content Cache Reference Count	Average number of content cache references. ID: CONTENT_CACHE_NUMDEDUP_REF_COUNT_PPH
Content Cache SSD Usage	Real SSD usage (in bytes) used to cache data by the content cache. ID: CONTENT_CACHE_PHYSICAL_SSD_USAGE_BYTES
Content Cache SSD Usage Saved	SSD usage (in bytes) saved due to content cache deduplication. ID: CONTENT_CACHE_SAVED_SSD_USAGE_BYTES
Deduplication Fingerprints Cleared	Number of written bytes for which fingerprints have been cleared. ID: DEDUP_FINGERPRINT_CLEARED_BYTES
Deduplication Fingerprints Written	Number of written bytes for which fingerprints have been added. ID: DEDUP_FINGERPRINT_ADDED_BYTES
Disk I/O Bandwidth	Data transferred per second in KB/second from disk. ID: STATS_BANDWIDTH
Disk I/O Bandwidth - Read	Read data transferred per second in KB/second from disk. ID: STATS_READ_BANDWIDTH
Disk I/O Bandwidth - Write	Write data transferred per second in KB/second from disk. ID: STATS_WRITE_BANDWIDTH
Disk I/O Latency	I/O latency in milliseconds from disk. ID: STATS_AVG_IO_LATENCY
Disk IOPS	Input/Output operations per second from disk. ID: STATS_NUM_IOPS
Disk IOPS - Read	Input/Output read operations per second from disk. ID: STATS_NUM_READ_IOPS
Disk IOPS - Write	Input/Output write operations per second from disk. ID: STATS_NUM_WRITE_IOPS
Hypervisor CPU Ready Time (%)	
Hypervisor CPU Usage (%)	Percent of CPU used by the hypervisor. ID: STATS_HYP_CPU_USAGE
Hypervisor I/O Bandwidth	Data transferred per second in KB/second from Hypervisor. ID: STATS_HYP_BANDWIDTH

Metric	Description
Hypervisor I/O Bandwidth - Read	Read data transferred per second in KB/second from Hypervisor. ID: <code>STATS_HYP_READ_BANDWIDTH</code>
Hypervisor I/O Bandwidth - Write	Write data transferred per second in KB/second from Hypervisor. ID: <code>STATS_HYP_WRITE_BANDWIDTH</code>
Hypervisor I/O Latency	I/O latency in milliseconds from Hypervisor. ID: <code>STATS_HYP_AVG_IO_LATENCY</code>
Hypervisor I/O Latency - Read	I/O read latency in milliseconds from Hypervisor. ID: <code>STATS_HYP_AVG_READ_IO_LATENCY</code>
Hypervisor I/O Latency - Write	I/O write latency in milliseconds from Hypervisor. ID: <code>STATS_HYP_AVG_WRITE_IO_LATENCY</code>
Hypervisor IOPS	Input/Output operations per second from Hypervisor. ID: <code>STATS_HYP_NUM_IOPS</code>
Hypervisor IOPS - Read	Input/Output read operations per second from Hypervisor. ID: <code>STATS_HYP_NUM_READ_IOPS</code>
Hypervisor IOPS - Write	Input/Output write operations per second from Hypervisor. ID: <code>STATS_HYP_NUM_WRITE_IOPS</code>
Hypervisor Memory Usage (%)	Percent of memory used by the hypervisor. ID: <code>STATS_HYP_MEMORY_USAGE</code>
Logical Usage	Logical usage of storage (before compression/deduplication). ID: <code>STATS_UNTRANSFORMED_USAGE</code>
Physical Usage	Actual usage of storage. ID: <code>STATS_TRANSFORMED_USAGE</code>
Read IOPS (%)	Percent of IOPS that are reads. ID: <code>STATS_READ_IO_PPM</code>
Replication Bandwidth - Received	Replication data received per second in KB/second ID: <code>STATS REP BW RECEIVED</code>
Replication Bandwidth - Transmitted	Replication data transferred per second in KB/second ID: <code>STATS REP BW TRANSFERRED</code>
Replication Bytes - Received	Number of bytes received. ID: <code>STATS REP NUM RECEIVED BYTES</code>
Replication Bytes - Total Received	Total number of bytes received. ID: <code>STATS REP TOT RECEIVED BYTES</code>

Metric	Description
Replication Bytes - Total Transmitted	Total number of bytes transmitted. ID: <code>STATS_REP_TOT_TRANSMITTED_BYTES</code>
Replication Bytes - Transmitted	Number of bytes transmitted. ID: <code>STATS_REP_NUM_TRANSMITTED_BYTES</code>
Storage Controller Bandwidth	Data transferred in KB/second from the Storage Controller. ID: <code>STATS_CONTROLLER_BANDWIDTH</code>
Storage Controller Bandwidth - Read	Read data transferred in KB/second from the Storage Controller. ID: <code>STATS_CONTROLLER_READ_BANDWIDTH</code>
Storage Controller Bandwidth - Write	Write data transferred in KB/second from the Storage Controller. ID: <code>STATS_CONTROLLER_WRITE_BANDWIDTH</code>
Storage Controller IOPS	Input/Output operations per second from the Storage Controller ID: <code>STATS_CONTROLLER_NUM_IOPS</code>
Storage Controller IOPS - Read	Input/Output read operations per second from the Storage Controller ID: <code>STATS_CONTROLLER_NUM_READ_IOPS</code>
Storage Controller IOPS - Read (%)	Percent of Storage Controller IOPS that are reads. ID: <code>STATS_CONTROLLER_READ_IO_PPM</code>
Storage Controller IOPS - Write	Input/Output write operations per second from the Storage Controller ID: <code>STATS_CONTROLLER_NUM_WRITE_IOPS</code>
Storage Controller IOPS - Write (%)	Percent of Storage Controller IOPS that are writes. ID: <code>STATS_CONTROLLER_WRITE_IO_PPM</code>
Storage Controller Latency	I/O latency in milliseconds from the Storage Controller. ID: <code>STATS_CONTROLLER_AVG_IO_LATENCY</code>
Storage Controller Latency - Read	Storage Controller read latency in milliseconds. ID: <code>STATS_CONTROLLER_AVG_READ_IO_LATENCY</code>
Storage Controller Latency - Write	Storage Controller write latency in milliseconds. ID: <code>STATS_CONTROLLER_AVG_WRITE_IO_LATENCY</code>
Storage container own usage	
Swap In Rate	
Swap Out Rate	
Write IOPS (%)	Percent of IOPS that are writes. ID: <code>STATS_WRITE_IO_PPM</code>

## Exporting Performance Data

This topic describes how to view and export the performance chart.

Performance data is stored for three months in the UI. You can export the performance data results in CSV or JSON format.



**Note:** Performance data is available for 3 months.

1. Log into the Prism Web Console.
2. Navigate to the Analysis Dashboard. Click **Home > Analysis**.  
The *Analysis* page displays.
3. Set the scale to **1 Month**. The **1 Month** scale shows the data in monthly segments.

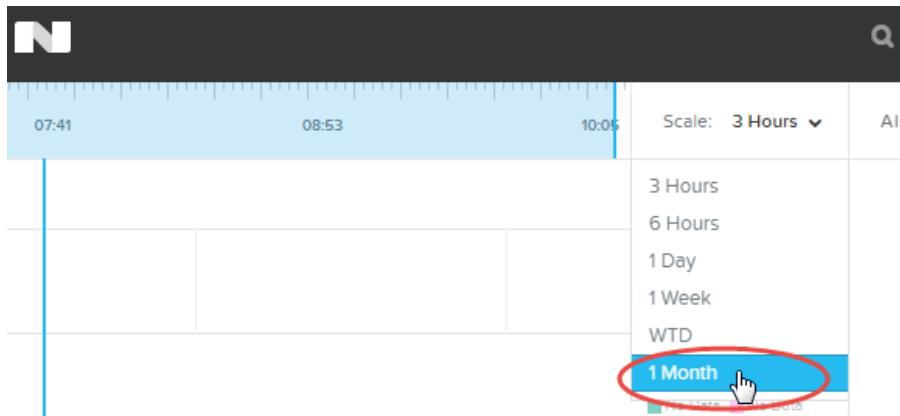


Figure: Set Performance Data Scale

4. Export the performance data into a CSV or JSON format. Click the drop-down arrow next to the cluster chart you want to export.

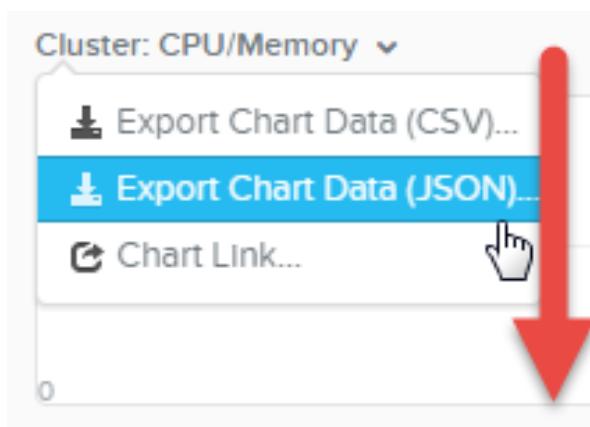


Figure: Export Performance Data

## Alert and Event Monitoring

The web console provides several mechanisms to monitor events in the cluster.

- *Dashboard views.* You can display alert and event message views to monitor activity in the cluster (see [Alerts Dashboard](#) on page 410).
- *Alert policies.* You can customize the list of events that generate an alert (see [Configuring Alert Policies](#) on page 416).
- *Email notification.* You can enable email notification and set up a list of users who are notified when alerts are generated (see [Configuring Alert Emails](#) on page 414).

When alerting is enabled, some potentially high impact events also generate a case automatically with Nutanix customer support. Events that might generate a Nutanix support case include hardware problems such as clock, power supply, or disk failures; monitoring problems such as Stargate outages or Curator scan failures; and data processing problems such as disabled compression or deduplication.

### Alerts Dashboard

The Alerts dashboard displays alert and event messages. To view the Alerts dashboard, select **Alerts** from the pull-down list on the far left of the main menu.

#### Menu Options

In addition to the main menu (see [Main Menu Options](#) on page 32), the Alert screen includes a menu bar with the following options:

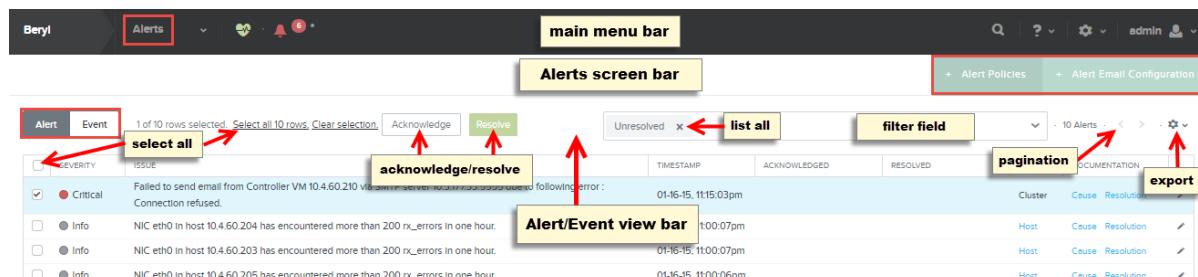


Figure: Alerts Dashboard Menu

- *View selector.* The Alerts dashboard provides two viewing modes.
  - Click the **Alert** button on the left to display the alert messages (see [Alert Messages View](#) on page 411).
  - Click the **Event** button to display the event messages (see [Event Messages View](#) on page 413).
- *Action buttons.* Click the **Alert Policies** button to specify what events should generate an alert and how frequently the system should check for each event type (see [Configuring Alert Policies](#) on page 416). Click the **Alert Email Configuration** button to enable alert emails and specify email addresses to which alerts should go (see [Configuring Alert Emails](#) on page 414).

- **Acknowledge/Resolve indicators.** When the far left column box is checked for one or more issues, an **Acknowledge** option appears in the alert/event view bar, and a **Resolve** option also appears for alerts. Clicking one or both of these options applies those options to all checked messages. You can click the **select all xx rows** link in the alert/event view bar to select all the rows in the table. Clicking the far left column header selects all the displayed issues on that page.
- **List all issues.** Only unresolved alert messages or unacknowledged event messages are displayed by default. To list both resolved and unresolved alert messages, click the **Unresolved X** button in the filter box. To list both acknowledged and unacknowledged event messages, check the **Include Acknowledged** box.
- **Filter options (alerts only).** In the Alerts view click in the filter box to display a drop-down of filtering options. Enter the desired filtering parameters in the following fields and then click the **Apply Filter** button to display a filtered list:
  - **Severity:** Select the alert severity level (All, Critical, Warning, Info) from the pull-down list.
  - **Resolution:** Select the resolution status (All, Unresolved, Auto Resolved, Manually Resolved) from the pull-down list.
  - **From:** Select the start time of the interval in the date and time fields.
  - **To:** Select the stop time of the interval in the date and time fields.

The figure shows a user interface for filtering alerts. At the top are two dropdown menus: 'Severity' set to 'All' and 'Resolution' set to 'Unresolved'. Below these are two date and time input fields labeled 'From' and 'To', each with a small calendar icon. At the bottom is a blue rectangular button labeled 'Apply Filter'.

*Figure: Alerts Filter Box*

- **Pagination.** Messages are displayed 20 per page. When there are more than 20 messages, left and right paging arrows appear on the right of the alert/event view bar along with the total message count and the message numbers for the current page.
- **Export messages.** You can export the messages to a file in either CSV or JSON format by clicking the gear icon  on the right of the alert/event view bar and selecting either **Export CSV** or **Export JSON** from the pull-down menu. This exports the messages for the current tab, either all the alerts or all the events. (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.

## Alert Messages View

The Alert messages view displays a list of alert messages. The following figure is a sample view, and the table describes each field in this view. You can order the alerts by clicking on a column header, which switches the entries alphabetically or by date based on the values in that column.



**Note:** See [Alerts/Health checks](#) on page 417 for a list of alert messages and corrective actions.

SEVERITY	issue	TIMESTAMP	ACKNOWLEDGED	RESOLVED	ENTITIES	DOCUMENTATION
<input checked="" type="checkbox"/> Critical	Failed to send email from Controller VM 10.4.60.210 via SMTP server 10.3.177.33:5555 due to following error : Connection refused.	01-16-15, 11:15:03pm	By admin (01-22, 05:17:30pm)		Cluster	Cause Resolution
<input type="checkbox"/> Info	NIC eth0 in host 10.4.60.204 has encountered more than 200 rx_errors in one hour.	01-16-15, 11:00:07pm			Host	Cause Resolution
<input type="checkbox"/> Info	NIC eth0 in host 10.4.60.203 has encountered more than 200 rx_errors in one hour.	01-16-15, 11:00:07pm			Host	Cause Resolution
<input type="checkbox"/> Info	NIC eth0 in host 10.4.60.205 has encountered more than 200 rx_errors in one hour.	01-16-15, 11:00:06pm			Host	Cause Resolution
<input type="checkbox"/> Info	NIC eth0 in host 10.4.60.206 has encountered more than 200 rx_errors in one hour.	01-16-15, 11:00:06pm			Host	Cause Resolution
<input type="checkbox"/> Critical	There have been 10 or more cluster services restarts within 15 minutes in the Controller VM 10.4.60.207.	01-16-15, 04:29:07pm			Host	Cause Resolution
<input type="checkbox"/> Critical	Controller VM 10.4.60.207 has been rebooted on Fri Jan 16 16:27:00 2015.	01-16-15, 04:29:04pm			Host	Cause Resolution
<input type="checkbox"/> Critical	Stargate on Controller VM 10.4.60.207 is down for 331 seconds.	01-16-15, 04:22:45pm			Host	Cause Resolution
<input type="checkbox"/> Critical	Hypervisor 10.4.60.203 is not reachable from Controller VM 10.4.60.208 in the last six attempts.	01-16-15, 04:22:07pm			Host	Cause Resolution
<input type="checkbox"/> Critical	Hypervisor 10.4.60.203 is not reachable from Controller VM 10.4.60.208 in the last three attempts.	01-16-15, 04:19:06pm			Host	Cause Resolution

Figure: Alerts View

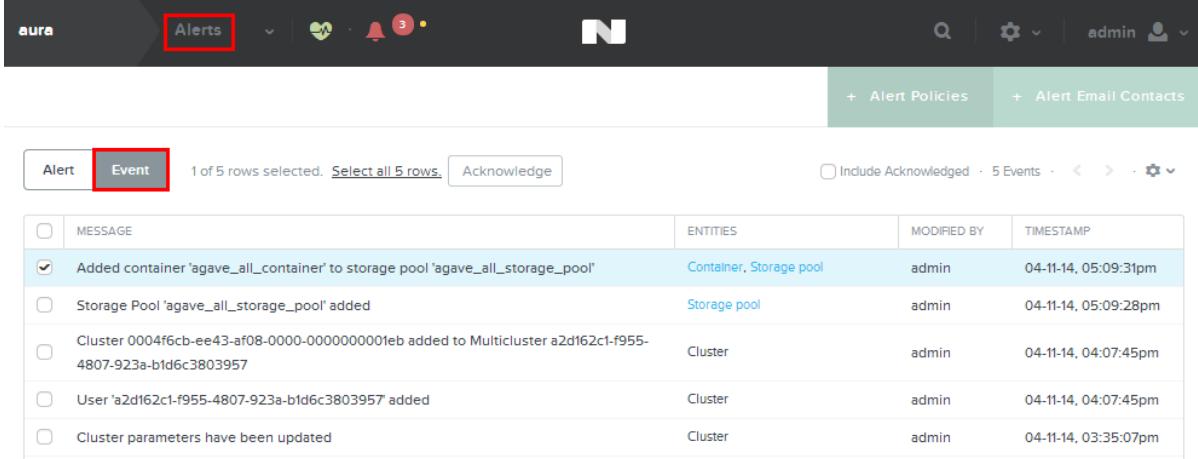
### Alerts View Fields

Parameter	Description	Values
(selection box)	Click this box to select the message for acknowledgement or resolution (see <a href="#">Alerts Dashboard</a> on page 410).	n/a
Severity	Displays the severity level of this condition. There are three levels:  <i>Critical</i> A "critical" alert is one that requires immediate attention, such as a failed Controller VM.  <i>Warning</i> A "warning" alert is one that might need attention soon, such as an issue that could lead to a performance problem.  <i>Informational</i> An "informational" alert highlights a condition to be aware of, for example, a reminder that the support tunnel is enabled.	Critical, Warning, Informational
Issue	Displays the alert message.	(message text)
Timestamp	Displays the date and time when the alert occurred.	(time and date)
Acknowledged	Indicates whether a user has acknowledged the alert. To acknowledge an alert, check the box in the far left column and then click <b>Acknowledge</b> in the screen menu bar. The field value changes from blank or <b>No</b> to the user name and time the alert was acknowledged.	(user and time), No

Parameter	Description	Values
Resolved	Indicates whether a user has set the alert as resolved. To resolve an alert, check the box in the far left column and then click <b>Resolved</b> in the screen menu bar. The field value changes from blank or <b>No</b> to the user name and time the alert was resolved.	(user and time), No
Entities	Displays the name of the entity to which this alert applies, for example <b>host</b> or <b>cluster</b> .	(entity name)
Documentation	Displays <b>Cause</b> and <b>Resolution</b> links that pop up an explanation of the alert cause and resolution when you hover the cursor over the link.	(test description of cause or resolution)
 (pencil icon)	Clicking the pencil icon opens the <i>Update Alert Policy</i> window at that message (see <a href="#">Configuring Alert Policies</a> on page 416).	n/a

## Event Messages View

The Event messages view displays a list of event messages. Event messages describe cluster actions such as adding a storage pool or taking a snapshot. The following figure is a sample view, and the table describes each field in this view. You can order the events by clicking on a column header, which switches the entries alphabetically or by date based on the values in that column.



MESSAGE	ENTITIES	MODIFIED BY	TIMESTAMP
<input checked="" type="checkbox"/> Added container 'agave_all_container' to storage pool 'agave_all_storage_pool'	Container, Storage pool	admin	04-11-14, 05:09:31pm
<input type="checkbox"/> Storage Pool 'agave_all_storage_pool' added	Storage pool	admin	04-11-14, 05:09:28pm
<input type="checkbox"/> Cluster 0004f6cb-ee43-af08-0000-000000001eb added to Multicluster a2d162c1-f955-4807-923a-b1d6c3803957	Cluster	admin	04-11-14, 04:07:45pm
<input type="checkbox"/> User 'a2d162c1-f955-4807-923a-b1d6c3803957' added	Cluster	admin	04-11-14, 04:07:45pm
<input type="checkbox"/> Cluster parameters have been updated	Cluster	admin	04-11-14, 03:35:07pm

Figure: Events View

## Events View Fields

Parameter	Description	Values
(selection box)	Click this box to select the message for acknowledgement or resolution (see <a href="#">Alerts Dashboard</a> on page 410).	n/a
Message	Displays the event message.	(message text)
Entities	Displays the name of the entity to which this alert applies, for example <b>host</b> or <b>cluster</b> .	(entity name)

Parameter	Description	Values
Modified by	Displays the name of the user who initiated the action, for example <b>admin</b> .	(user name)
Timestamp	Displays the date and time when the event occurred.	(time and date)

## Configuring Alert Emails

E-mail notification of alerts is enabled by default and sends alert messages automatically to Nutanix customer support through customer-opened ports 80 or 8443. To customize who should receive the alert e-mails (or to disable e-mail notification), do the following:

**1.** Do one of the following:

- In the gear icon pull-down list of the main menu, select **Alert Email Configuration**.
- In the Alerts dashboard, click the **Alert Email Configuration** button.

The *Alert Email Configuration* window appears.

**2.** In the **Settings** tab do the following.

- a. Select the **Email Every Alert** box to send an email whenever the event occurs.
- b. Select the **Email Daily Digest** box to send a cumulative (24 hour) list of alerts once a day. You can check one or both boxes. If neither box is checked, no alert emails are sent.
- c. Select the **Nutanix Support** box to send alert notification to Nutanix customer support. Note that an alert notification to the Nutanix customer support is sent only if you have selected the **Email Every Alert** option.
- d. To send alert notifications to others, enter their email addresses in a comma separated list in the field below the **Nutanix Support** box.
- e. Click the **Apply** button to apply the changes and continue the configuration (or click the **Save** button to apply the changes and close the window).

The **Connection Status** section displays mail transport status information. In this example, default Nutanix tunnel is used for mail service. For more information on configuring the SMTP server settings window (see [Configuring an SMTP Server](#) on page 573).

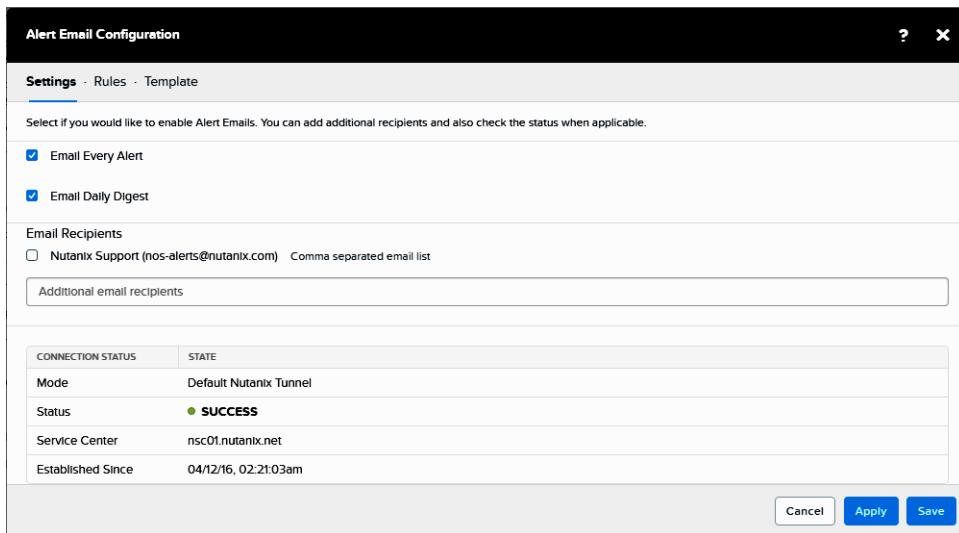


Figure: Alert Email Configuration Window

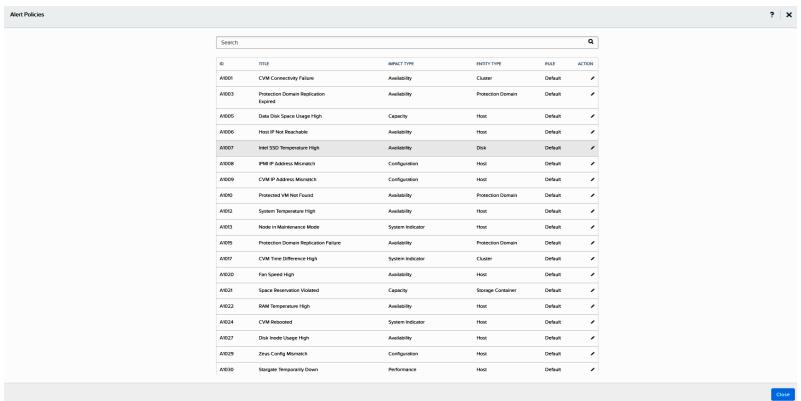
3. To create a custom alert email rule, click the **Rules** tab and the **New Rule** button, and then configure the rule as follows:
  - a. Specify the conditions for generating the alert:
    - **Severity:** Select one or more of the severities from the pull-down list (Critical, Warning, Info, All).
    - **Category:** Select one or more of the categories from the pull-down list (Availability, Capacity, Configuration, Performance, System Indicator, All).
  - b. Specify who should receive the alert email.
    - **Email Addresses:** Enter recipient email addresses as a comma separate list in the box.
    - **Global Recipient List:** Click this box to add everyone on the global recipient list. This is in addition to any users listed in the **Email Addresses** field.
  - c. Click the **Apply** button to apply the rule.
  - d. Repeat these steps to apply additional custom rules.
4. To create a template for the email messages, click the **Template** tab and do the following:
  - a. In the **Prepend content to the email subject** field, enter the desired text.  
This text will appear at the beginning of the subject field in each alert email. If the field is left blank, no prepended text will appear in the subject.
  - b. In the **Append content to the email body** field, enter the desired text.  
This text will appear at the end of the message body in each alert email. If the field is left blank, no appended text will appear in the message body.
  - c. Click the **Save** button to apply the changes and close the window (or click the **Apply** button to apply the changes and continue the configuration).

## Configuring Alert Policies

The system comes with default alert policies, but you can customize which events should trigger an alert and how frequently to check for those events. To customize the alert policies, do the following:

1. In the gear icon  pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Alert Policies**.

The Alert Policies window appears. This screen displays a list of alert events. Enter a string in the search box at the top or use the scroll bar on the right to search through the list.



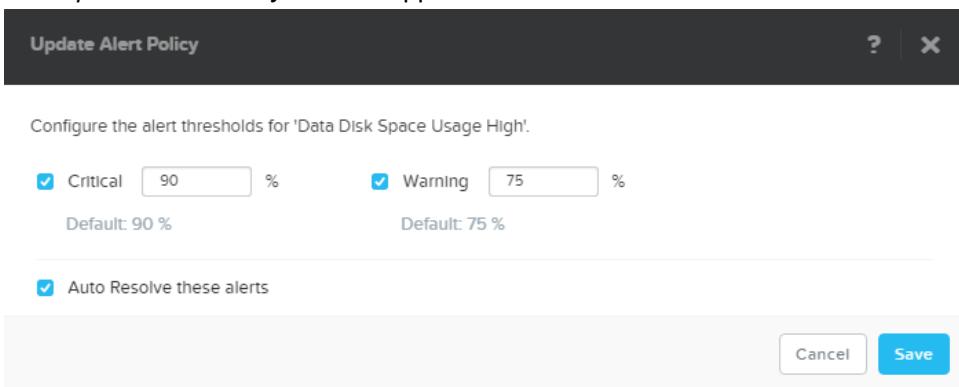
ID	Title	Impact Type	Entity Type	Rate	Action
AE001	CWV Connectivity Failure	Availability	Cluster	Default	<input checked="" type="checkbox"/>
AE003	Protection Domain Replication Failed	Availability	Protection Domain	Default	<input checked="" type="checkbox"/>
AE004	Data Disk Space Usage High	Capacity	Host	Default	<input checked="" type="checkbox"/>
AE006	Host IP Not Reachable	Availability	Host	Default	<input checked="" type="checkbox"/>
AE007	Intel SSD Temperature High	Availability	Disk	Default	<input checked="" type="checkbox"/>
AE008	IPMI IP Address Mismatch	Configuration	Host	Default	<input checked="" type="checkbox"/>
AE009	CWV IP Address Mismatch	Configuration	Host	Default	<input checked="" type="checkbox"/>
AE010	Protocol IP Not Found	Availability	Protection Domain	Default	<input checked="" type="checkbox"/>
AE012	System Temperature High	Availability	Host	Default	<input checked="" type="checkbox"/>
AE013	Node in Maintenance Mode	System Indicator	Host	Default	<input checked="" type="checkbox"/>
AE015	Protection Domain Replication Failure	Availability	Protection Domain	Default	<input checked="" type="checkbox"/>
AE017	CWV Time Difference High	System Indicator	Cluster	Default	<input checked="" type="checkbox"/>
AE018	Fan Speed High	Availability	Host	Default	<input checked="" type="checkbox"/>
AE019	Space Reservation Violated	Capacity	Storage Container	Default	<input checked="" type="checkbox"/>
AE022	RAID Temperature High	Availability	Host	Default	<input checked="" type="checkbox"/>
AE024	CWV Resolved	System Indicator	Host	Default	<input checked="" type="checkbox"/>
AE027	Disk Health Usage High	Availability	Host	Default	<input checked="" type="checkbox"/>
AE029	Zeta Config Mismatch	Configuration	Host	Default	<input checked="" type="checkbox"/>
AE030	Navigate Temporarily Down	Performance	Host	Default	<input checked="" type="checkbox"/>

Figure: Alert Policies Window

2. To modify the alert policy for an event, click the title or pencil icon for that alert.

All the alerts are enabled (box checked) by default. 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 75%) and a critical alert when a second threshold is reached (90%). 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).

The *Update Alert Policy* window appears.



Configure the alert thresholds for 'Data Disk Space Usage High'.

<input checked="" type="checkbox"/> Critical	90	%	<input checked="" type="checkbox"/> Warning	75	%
Default: 90 %			Default: 75 %		
<input checked="" type="checkbox"/> Auto Resolve these alerts					
			<input type="button" value="Cancel"/>	<input type="button" value="Save"/>	

Figure: Update Alert Policy

3. Do the following in the indicated fields:

- a. Severity value(s): **Critical**, **Warning**, and/or **Info**: Uncheck (or check) the box next to the severity to disable (or re-enable) this as an alert.

All the alerts are enabled (box checked) by default. 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 75%) and a critical alert when a second threshold is reached (90%). 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.)

- c. Click the **Save** button to save the changes and return to the *Alert Policies* page.
4. Repeat the previous step for any additional alert policies that you want to update.
5. When the alert policies are correct, click the **Close** button.

## Alerts/Health checks

### Cluster

#### High vDisk count in the cluster [1032] [A1182]

Name	vDisk Count Check
Description	Checks for high vDisk count in the cluster
Alert message	Number of <code>vdisk_type</code> in the cluster is above the threshold <code>(vdisk_count/vdisk_threshold)</code>
Cause	Aggressive replication/snapshot schedules may generate large number of vDisks on the remote site
Impact	The cluster may become unstable due to increased load on core Nutanix services
Resolution	Immediately contact Nutanix support for assistance

#### All flash nodes mixed with non-all-flash nodes [1054] [A1191]

Name	All-flash Node Intermixed Check
Description	Checks that all-flash nodes do not coexist with non-all-flash nodes in a cluster
Alert message	Cluster <code>cluster_id</code> has both all-flash nodes and non-all-flash nodes
Cause	All-flash nodes and non-all-flash nodes are put into the same cluster
Impact	The cluster may experience performance degradation or instability.
Resolution	Remove either all-flash nodes or non-all-flash nodes from the cluster

### Cluster In Read-Only Mode [1058] [A1195]

---

Name	Cluster In Read-Only Mode
Description	Single-node cluster is in read-only mode.
Alert message	Single node cluster with CVM <i>service_vm_external_ip</i> is running in read-only mode due to <i>reason</i> .
Cause	One of the metadata SSDs has failed.
Impact	Native backups are disabled.
Resolution	Replace the failed SSD. Refer to the Nutanix documentation for instructions.

---

### VM Memory Pressure [3024]

---

Name	VM Memory Pressure
Description	Checks balloon driver reclaimed memory is at most within {vm_balloon_reclaim_threshold_mb} MB of the target.
Cause	Ballooning driver could not reclaim enough memory.
Impact	VM and cluster performance is degraded.
Resolution	Increase memory, reduce memory intensive VMs or reduce the total number of VMs.

---

### CVM Time Difference High [3025] [A1017]

---

Name	Time Drift Check
Description	Check that the time drift between CVMs is less than {time_drift_threshold_sec}.
Alert message	Wall clock time has drifted by more than <i>time_difference_limit_secs</i> seconds between the Controller VMs <i>lower_time_ip</i> and <i>higher_time_ip</i> .
Cause	Timedrift exceeds threshold.
Impact	The cluster may experience downtime.
Resolution	Check network configuration or connectivity.

---

### Upgrade bundle available [3031] []

---

Name	Upgrade Bundle Available
Description	Bundle available for upgrade
Alert message	Bundle <i>bundle_name</i> is available for <i>upgrade_type</i> upgrade.
Cause	Newer bundle available for upgrade
Impact	Cluster is running on older version.
Resolution	Upgrade the cluster with newer bundle. Refer to the Nutanix documentation for instructions.

---

### Cluster services are down [3032] []

---

Name	Cluster Services Down Check
Description	Check that no services are down in the cluster.
Alert message	Cluster Service: <i>service_name</i> is down on the Controller VM <i>ip_address</i> .
Cause	One or more services in the cluster are down.
Impact	Cluster performance may be significantly degraded. In the case of multiple services with the same condition, the cluster may become unable to serve I/O requests.
Resolution	If this check occurs once or infrequently, no action is necessary. If it is frequent, contact Nutanix support.

---

### Alert Manager Service Check [3033]

---

Name	Alert Manager Service Check
Description	Check if Alert Manager service is available.
Cause	This check usually indicates that the Alert Manager service is not healthy, but there could be other causes.
Impact	Cluster issues may stay unnoticed.
Resolution	If this alert occurs once or infrequently, no action is necessary. If it is frequent, contact Nutanix support.

---

### Cluster Service Restarting Frequently [3034] []

---

Name	Cluster Services Status
Description	Check if services have restarted recently across the cluster.
Alert message	There have been <i>threshold</i> or more service restarts of <i>service</i> within one day across all Controller VM(s).
Cause	This alert indicates that one or more services in the cluster were restarted.
Impact	Cluster performance may be significantly degraded. In the case of multiple services with the same condition, the cluster may become unable to service I/O requests.
Resolution	If this alert occurs once or infrequently, no action is necessary. If it is frequent, contact Nutanix support.

---

### IPMI IP Not Reachable [3062] [A1041]

---

Name	IPMI IP Pingable
Description	Check that all ipmi ips are pingable from local SVM.
Alert message	IPMI interface <i>target_ip</i> is not reachable from Controller VM <i>source_ip</i> in the last 6 attempts.
Cause	The IPMI interface is down or there is a network connectivity issue.
Impact	The host is unreachable through the IPMI interface.

---

Resolution	Ensure that the IPMI interface is functioning and that physical networking, VLANs, and virtual switches are configured correctly.
------------	-----------------------------------------------------------------------------------------------------------------------------------

#### **Host IP Not Reachable [3065] [A1006]**

Name	Host IP Pingable
Description	Check that all host ips are pingable from local SVM.
Alert message	Hypervisor <i>target_ip</i> is not reachable from Controller VM <i>source_ip</i> in the last 6 attempts.
Cause	The hypervisor host is down or there is a network connectivity issue.
Impact	Cluster compute and storage capacity are reduced. Until data stored on this host is replicated to other hosts in the cluster, the cluster has one less copy of guest VM data.
Resolution	Ensure that the hypervisor host is running and that physical networking, VLANs, and virtual switches are configured correctly.

#### **NIC Link Down [3067] [A1082]**

Name	NIC Link Status
Description	Checks whether any nic is down.
Alert message	Link on NIC <i>nic_name</i> of host <i>host_ip</i> is down. NIC description: <i>nic_description</i>
Cause	The NIC is disconnected from the switch, or the switch port is failing.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Ensure that the NIC is connected to the switch and that the switch port is functioning properly.

#### **Inter CVM Latency [6005]**

Name	Inter CVM Latency
Description	Check that other CVMs are pingable in less than {ping_time_threshold_ms} milliseconds.
Cause	At least one other CVM has high ping latency higher than {ping_time_threshold_ms} milliseconds.
Impact	If problem persists I/O performance will be degraded.
Resolution	Check network connectivity/configuration.

#### **Remote Support Enabled [6206] [A1051]**

Name	Remote Support Status
Description	Checks if remote support tunnel to Nutanix HQ is enabled on this cluster.

---

Alert message	Remote support tunnel to Nutanix HQ is enabled on this cluster.
Cause	Nutanix support staff are able to access the cluster to assist with any issue.
Impact	Nutanix support staff are able to access the cluster to assist with any issue.
Resolution	No action is necessary.

---

#### **CVM IP Address Mismatch [6207] [A1009]**

---

Name	CVM IP Address Configuration
Description	Checks that cvm IP address is in sync with zeus configuration
Alert message	IP address of Controller VM <i>zeus_ip_address</i> has been updated to <i>invalid_ip_address</i> . The Controller VM will not be part of the cluster once the change comes into effect, unless zeus configuration is updated.
Cause	The IP address configured in the cluster does not match the actual setting of the Controller VM.
Impact	Cluster compute and storage capacity are reduced. Until data stored on this host is replicated to other hosts in the cluster, the cluster has one less copy of guest VM data.
Resolution	Follow the IP address change procedure in the Nutanix documentation.

---

#### **Zeus Config Mismatch [6208] [A1029]**

---

Name	Hypervisor IP Address Configuration
Description	Checks that hypervisor IP address is in sync with zeus configuration
Alert message	Hypervisor IP address on Controller VM <i>svm_ip_address</i> was updated from <i>zeus_ip_address</i> to <i>invalid_ip_address</i> without following the Nutanix IP Reconfiguration procedure.
Cause	The IP address configured in the cluster does not match the actual setting of the hypervisor.
Impact	The hypervisor host is unreachable from other Controller VMs in the cluster.
Resolution	Follow the IP address change procedure in the Nutanix documentation.

---

#### **ESXi SIOC status check [6448]**

---

Name	ESXi SIOC status check
Description	Checks if the ESX Storage IO Controller (SIOC) feature is disabled
Cause	ESX SIOC feature may be enabled
Impact	ESX SIOC feature should be disabled on all Nutanix datastores
Resolution	ESX SIOC feature needs to be disabled

---

### **IPMI IP Address Mismatch [15013] [A1008]**

---

Name	IPMI IP Address Configuration
Description	Checks that IPMI IP address is in sync with zeus configuration
Alert message	IPMI IP address on Controller VM <i>svm_ip_address</i> was updated from <i>zeus_ip_address</i> to <i>invalid_ip_address</i> without following the Nutanix IP Reconfiguration procedure.
Cause	The IP address configured in the cluster does not match the actual setting of the IPMI interface.
Impact	The host is unreachable through the IPMI interface.
Resolution	Follow the IP address change procedure in the Nutanix documentation.

---

### **IPMI sensor values check [15021]**

---

Name	IPMI sensor values check
Description	Check that all IPMI sensor values are within threshold
Cause	IPMI sensors are not within threshold.
Impact	Cannot monitor hardware health.
Resolution	Review KB article 1524.

---

### **IPMI connectivity check [15022]**

---

Name	IPMI connectivity check
Description	Check that IPMI is working on all nodes
Cause	Refer to KB 1502.
Impact	IPMI could be unavailable.
Resolution	Refer to KB 1502.

---

### **IPMI sel assertions check [15023]**

---

Name	IPMI sel assertions check
Description	Check for IPMI SEL assertions in the past 24 hours
Cause	IPMI events logged in the last 24 hours.
Impact	Host might have restarted.
Resolution	Refer to KB 1590.

---

### **Number of orphaned egroups is over the recommended threshold. [20013] []**

---

Name	Garbage egroups check
------	-----------------------

---

Description	Check that the number of orphaned egroups are below the recommended threshold.
Alert message	Orphaned egroups are high
Cause	Number of orphaned groups is over the recommended threshold.
Impact	Space is underutilized.
Resolution	Review KB 1574.

---

#### **Snapshot chain height exceeds threshold [20014] [ ]**

Name	Snapshot chain height check
Description	Check that snapshot chain height is less than 25
Alert message	Snapshot chain height has exceeded the threshold limit.
Cause	Snapshot chain height exceeds threshold of 25.
Impact	Some VMs might experience increased latencies.
Resolution	Review KB 1732.

---

#### **Oplog episodes check [20015]**

Name	Oplog episodes check
Description	Check that oplog episode count is within threshold
Cause	Oplog episode count is high for one or more vDisks.
Impact	Oplog draining to extent store might get slower, impacting random writes latency.
Resolution	One or more VMs have an unusual burst of write IO.
Resolution	Review KB 1541.

---

#### **Automatic Dedup disabled check [20016]**

Name	Automatic Dedup disabled check
Description	Check that Dedup is not automatically disabled.
Cause	Deduplication on the Storage Container is disabled by Stargate service.
Impact	Space savings may not be observed on the Storage Container.
Resolution	Review KB 1730.

---

#### **Compression disabled check [20017]**

Name	Compression disabled check
Description	Check whether compression is automatically disabled.
Cause	Metadata usage has exceeded the 60GB or 20 percent default threshold.

---

Impact	
Resolution	Contact Nutanix support to manually reenable compression.

---

#### **Linked clones on Dedup check [20018]**

Name	Linked clones on Dedup check
Description	Verifies if there are shared disks on a Storage Container that has deduplication enabled that may be linked clones.
Cause	There are shared disks on a Storage Container that has deduplication enabled that may be linked clones.
Impact	Using both linked clones and deduplication on the same Storage Container may cause metadata bloat.
Resolution	For non-linked clone VMs that use deduplication, place the VMs in separate Storage Containers.

---

#### **Dedup and compression on Storage Container [20019]**

Name	Dedup and compression on Storage Container
Description	Check that only one of dedup and compression is enabled on the Storage Containers
Cause	If dedup and compression enabled on the Storage Containers only compression will take effect unless NOS is above 4.5.
Impact	Deduplication is not in effect.
Resolution	Enable either Dedup or compression on the Storage Container depending on the type of data.

---

#### **Cassandra service status check [21009]**

Name	Cassandra service status check
Description	Check that all Cassandra nodes are online and functioning normally
Cause	Cassandra service is not running in one or more hosts.
Impact	Cluster resilience might degrade.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Contact Nutanix support.

---

#### **Cassandra service crashed [21010] []**

Name	Cassandra service restarts check
Description	Check if Cassandra service is crashing continuously.

---

---

Alert message	Cassandra service has recently crashed. Contact Nutanix support for assistance.
Cause	Cassandra service is restarting frequently in the last 30 minutes.
Impact	Data resiliency is compromised.
Resolution	Contact Nutanix support.

---

#### **Cassandra service is running out of memory [21011] []**

---

Name	Cassandra memory usage
Description	Check if the Cassandra service is running out of memory.
Alert message	Cassandra service is running out of memory. Contact Nutanix support for assistance.
Cause	Cassandra has crossed memory threshold more than 5 times in the last 3 minutes.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Contact Nutanix support.

---

#### **Cassandra Keyspace/Column family check [21013]**

---

Name	Cassandra Keyspace/Column family check
Description	Check that there are no undefined Keyspace or CF in Cassandra
Cause	
Impact	
Resolution	

---

#### **Cassandra Waiting For Disk Replacement [21014] []**

---

Name	Cassandra Waiting For Disk Replacement
Description	Metadata disk not replaced for Disk Replace Op
Alert message	Disk <i>disk_id</i> for node <i>service_vm_external_ip</i> not replaced. Node performing disk replace: <i>ip_address_doing_ring_change</i>
Cause	Disk not replaced for Disk Replace Op.
Impact	Disk Replacement operation will not proceed to completion.
Resolution	Ensure that a replacement disk is present on the node undergoing disk replace. If it is and the alert persists, contact Nutanix support.

---

#### **ESXi RAM disk full check [101040]**

---

Name	ESXi RAM disk full check
------	--------------------------

---

Description	Check for ramdisk full condition
Cause	pynfs server is using legacy setting to write log file on root partition of ESXi ramdisk.
Impact	ESXi host may be disconnected from vCenter.
Impact	Local datastore may go offline and will be unavailable.
Resolution	Clean up the growing file and change the pynfs server settings.
Resolution	Review KB 1718 for additional details.

---

#### **ESXi RAM disk root usage [101041]**

Name	ESXi RAM disk root usage
Description	Check that RAM disk root directory usage below 85%
Cause	ESXi ramdisk root usage exceeds 85%.
Impact	Host might be inaccessible if ramdisk is full.
Resolution	Refer to KB 1846.

---

#### **Discoverable disks check [101042]**

Name	Discoverable disks check
Description	Check if disks are discoverable
Cause	HyperV utilities in the host are unable to detect controllers and disks.
Impact	NA
Resolution	The host may need a reboot. Review KB 2712 for mitigation steps.

---

#### **Ext4 journal sequence check [101043]**

Name	Ext4 journal sequence check
Description	Check if Ext4 journal sequence below threshold for all partitions
Cause	Ext4 journal sequence is less than the default threshold.
Impact	
Resolution	Upgrade to NOS 3.5.2 or higher.

---

#### **Duplicate disk id check [101044]**

Name	Duplicate disk id check
Description	Check for duplicate disk ids
Cause	Multiple disks with same disk id were found.
Impact	This can interfere with cluster functionality.

Resolution      Review KB 1876.

---

#### CVM startup dependency check [101045]

Name	CVM startup dependency check
Description	Checks if available unreserved space on any Storage Container is below 10 percent of the maximum capacity.
Cause	Unreserved available space is below threshold.
Impact	Virtual Machines might go to a stunned state if the available unreserved capacity drops to zero.

Resolution

---

#### Descriptors to deleted files check [101046]

Name	Descriptors to deleted files check
Description	Check if there are file descriptors to deleted files
Cause	
Impact	

Resolution

---

#### High disk space usage [101047]

Name	High disk space usage
Description	Check disk space usage on the cluster
Cause	High disk usage in the cluster.
Impact	Cluster can not tolerate single node failure.

Resolution      Review KB article 1863.

---

#### Offline disk in cluster [101048] []

Name	Disk online check
Description	Check for offline disks
Alert message	Disk mounted at <i>mount_path</i> on CVM <i>cvm_ip</i> is marked offline.
Cause	A disk may have failed or was manually removed.

Impact      Cluster performance may be degraded.

Resolution      Review KB 1536.

---

#### Incomplete disk removal [101049]

---

Name	Incomplete disk removal
Description	Check for incomplete disk removal
Cause	Cluster Health detected an incomplete disk removal operation.
Impact	Data integrity might be compromised.
Resolution	If the disk removal has not been manually triggered contact Nutanix Support.

---

#### SED protection consistency check [101050]

---

Name	SED protection consistency check
Description	Checks that all the drives in the system can authenticate to their internal security agents
Cause	
Impact	
Resolution	Contact Nutanix Support.

---

#### Automatic disabling of Deduplication [101051]

---

Name	Automatic disabling of Deduplication
Description	Check that On disk Dedup is not automatically disabled
Cause	Deduplication was disabled due to high metadata size, CVM RAM or SSD requirements are not met.
Impact	Deduplication is disabled.
Resolution	Ensure the RAM and SSD requirement are met and enable dedup from prism or CLI.

---

#### Field Advisory 35 check [101052]

---

Name	Field Advisory 35 check
Description	Check that 'vdisk_corrupt_replica_autofix_mode' is set to auto
Cause	vdisk_corrupt_replica_autofix_mode is not set to auto.
Impact	Data integrity might be compromised.
Resolution	Review KB 2880 and contact Nutanix Support to schedule an AOS upgrade.

---

#### Sanity check on local.sh [101053]

---

Name	Sanity check on local.sh
Description	Validate local.sh file configuration.
Cause	pynfs server is using legacy setting to write log file on root partition of ESXi ramdisk.

---

---

Impact	ESXi host may be disconnected from vCenter.
Impact	Local datastore may go offline and will be unavailable.
Resolution	Clean up the growing file and change the pynfs server settings.
Resolution	Review KB 1718 for details.

---

#### **Host FQDN resolution [103069]**

---

Name	Host FQDN resolution
Description	Check FQDN resolution of host IPs
Cause	Unable to reach name server or name server doesn't have correct entry.
Impact	Unable to resolve "host FQDN to IP" or "IP to host FQDN".
Resolution	Check if hostname to IP and IP to hostname resolution is working.

---

#### **NTP server FQDN resolution [103070]**

---

Name	NTP server FQDN resolution
Description	Check NTP Server FQDN resolution
Cause	Unable to reach name server or name server doesn't have correct entry.
Impact	Unable to resolve NTP server FQDN.
Resolution	Check if ntp server name resolution is working.

---

#### **SMTP server FQDN resolution [103071]**

---

Name	SMTP server FQDN resolution
Description	Check SMTP server FQDN resolution
Cause	Unable to reach name server or name server doesn't have correct entry.
Impact	Unable to resolve SMTP server FQDN.
Resolution	Check if smtp server name resolution is working.

---

#### **NSC(Nutanix Service Center) server FQDN resolution [103072]**

---

Name	NSC(Nutanix Service Center) server FQDN resolution
Description	Check NSC server FQDN resolution
Cause	Unable to reach name server or name server doesn't have correct entry.
Impact	Unable to resolve NSC(Nutanix Service Center) server FQDN.
Resolution	Check if cluster has Internet access and correct name server setting exists.

---

#### CVM Not Uplinked to Active 10Gbps Link [103073] []

---

Name	CVM 10 GB uplink check
Description	Check that CVM uplinked to active 10Gbps link
Alert message	CVM is not uplinked to active 10Gbps link.
Cause	CVM is not uplinked to active 10Gbps link.
Impact	Performance may degrade.
Resolution	Verify bonds do not contain a 1Gbe link.
Resolution	Review KB 1584.

---

#### Storage routed to alternate CVM check [103074]

---

Name	Storage routed to alternate CVM check
Description	Check if storage is routed to an alternate CVM
Cause	Stargate traffic reroute is engaged on host of the cluster.
Impact	Due to stargate traffic reroute, the data resilience and performance may get impacted
Resolution	Check the following cases: 1. CVM is completely down. 2. Stargate is not running or CVM is partly down. 3. Stargate is crashing.

---

#### NIC driver and firmware version check [103075]

---

Name	NIC driver and firmware version check
Description	Check if Quad port NIC driver version is above min recommended version
Cause	Quad-port nic card on Nutanix Haswell platform is not running min recommended driver or firmware version.
Impact	NIC is not on the latest driver / firmware version.
Resolution	Upgrade to the latest version of driver and firmware version for the Quad d port nic card.

---

#### Incorrect NTP Configuration [103076] []

---

Name	NTP configuration check
Description	Check that NTP is configured properly on CVM/Hypervisor
Alert message	NTP is not properly configured or the NTP server(s) cannot be reached from <i>cvm_ip</i> .
Cause	Detected problems with NTP configuration.
Impact	Metadata operations or alerts might not work properly.
Resolution	Review KB 2999.

---

#### **VM IDE bus check [103079]**

---

Name	VM IDE bus check
Description	Check UVMs with IDE disk
Cause	Detected VMs running in the cluster on IDE bus.
Impact	VMs Performance degradation.
Resolution	Review KB 2998.

---

#### **CVM memory check [103080]**

---

Name	CVM memory check
Description	Check CVM Memory
Cause	CVM memory is lesser than the recommended threshold with the current feature set.
Impact	
Resolution	

---

#### **CVM same timezone check [103085]**

---

Name	CVM same timezone check
Description	Check that all CVMs are in the same timezone
Cause	Some of the Controller VMs in the cluster are not in the same timezone.
Impact	It is recommended to have all the CVMs in the same timezone to avoid potential issues.
Resolution	Make sure all Controller VMs are in the same time zone. If they are not, then set the timezone using KB 1050

---

#### **Cluster NCC version check [103086]**

---

Name	Cluster NCC version check
Description	Check that NCC version is consistent on the cluster
Cause	NCC version is different across the CVMs.
Impact	Some NCC checks can not be executed on all CVMs.
Resolution	Upgrade NCC to the desired version to keep it consistent across CVMs.

---

#### **CVM is unreachable [103088] []**

---

Name	Inter-CVM connectivity check
Description	Check that all CVMs are reachable via ping
Alert message	CVM is unreachable

---

Cause	The Controller VM is down or there is a network connectivity issue.
Impact	Storage may be unavailable and/or performance issues may be observed.
Resolution	If the Controller VM does not respond to ping, turn it on. Ensure that physical networking, VLANs, and virtual switches are configured correctly.

---

#### Duplicate CVM IP check [103089]

Name	Duplicate CVM IP check
Description	Check for duplicate CVM IP
Cause	One (or more) of your Nutanix cluster Controller VM external(eth0) interfaces conflicts with other hosts on the same network.
Impact	
Resolution	Review KB 3025.

---

#### FusionIO PCIE-SSD: ECC errors check [106013]

Name	FusionIO PCIE-SSD: ECC errors check
Description	Check ECC errors on FIO drives
Cause	If the check reports a non-zero value, it does not necessarily indicate the card is defective.
Impact	Card might be replaced pre-maturely.
Resolution	Run this command a second time and confirm the findings.

---

#### Intel Drive: ECC errors [106014]

Name	Intel Drive: ECC errors
Description	Check for IO errors on an Intel PCIe drive
Cause	Intel SSD that has reached its maximum number of reads/writes.
Cause	Failure in the physical interface in the server or drive.
Impact	The respective drives may need to be replaced immediately. System performance may also degrade.
Resolution	Replace the drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

#### Boot device connection check [106015]

Name	Boot device connection check
Description	Check connection to the boot device
Cause	Boot device may have lost connection.

Impact

Resolution      Check boot device status.

---

#### **Boot device status check [106016]**

Name	Boot device status check
Description	Check status of the boot device
Cause	
Impact	
Resolution	Check boot device connection using vmkfstool -P bootbank / readbank on ESXI host.

---

#### **LSI Disk controller firmware status [106018]**

Name	LSI Disk controller firmware status
Description	Check LSI Firmware Revision
Cause	LSI Disk Controller is running a superseded version of firmware.
Impact	LSI Disk Controller firmware issues can result in a node to hang and disk instability.
Resolution	Upgrade LSI Controller Firmware.

---

#### **SATA controller [106020]**

Name	SATA controller
Description	Check SATA controller ports
Cause	The SATA controller is experiencing errors.
Impact	The system may experience issues while accessing physical storage within the node.
Resolution	Review KB 2312.
Resolution	Contact Nutanix support.

---

#### **Intel SSD S3610 on {ip\_address} has configuration problems. [106021] []**

Name	Intel SSD Configuration
Description	Check if node has supported configuration for Intel SSD S3610
Alert message	Intel SSD S3610 on host <i>ip_address</i> has configuration problems: <i>alert_msg</i> .
Cause	SSD S3610 is installed on an NX-1020 or NX-9040 node. SSD S3610 is installed on a cluster whose AOS version is before 4.1.1.4. SSD S3610 is not properly down-formatted.
Impact	SSD S3610 drive performance and write endurance are degraded.

---

---

Resolution	Remove SSD S3610 from the NX-1020 or NX-9040 nodes. Upgrade AOS to at least version 4.1.1.4. Contact Nutanix support to replace with a new drive. Refer to the Nutanix documentation for instructions.
------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

#### **SSD Firmware Check [106022]**

---

Name	SSD Firmware Check
Description	Check SSD firmware version
Cause	SSD firmware version is below the recommended version.
Impact	Intel S3610 SSDs running firmware version 0110 could be marked offline for upto a minute.
Resolution	Upgrade SSD firmware to the recommended version or above. Refer to KB 2588 for details.

---

#### **DIMM degradation check [106023]**

---

Name	DIMM degradation check
Description	Check DIMM for potential failures
Cause	
Impact	
Resolution	

---

#### **DIMMs same memory speed [106024]**

---

Name	DIMMs same memory speed
Description	Check that DIMM speeds are the same
Cause	Speeds of the DIMMs are different.
Impact	Performance may be affected.
Resolution	Review KB 2723.

---

#### **Hardware FRU information correctness [106025]**

---

Name	Hardware FRU information correctness
Description	Check that FRU fields are programmed to correct value
Cause	Hardware information may be incorrectly configured.
Impact	No functional Impact.
Resolution	Contact Nutanix support to correctly configure the FRU fields.

---

#### CVM virtual hardware version check [106027]

---

Name	CVM virtual hardware version check
Description	Check CVM virtual hardware version
Cause	One or more CVM is using old/different virtual hardware version
Impact	Virtual hardware version 7 might cause performance issue
Resolution	Use the recommended minimum Virtual machine hardware version of 8.
Resolution	All CVMs should be on same virtual hardware version.

---

#### DIMMs of different types in one memory channel [106028] []

---

Name	DIMMs Interoperability Check
Description	DIMMs Interoperability Check
Alert message	Memory channels on host <i>ip_address</i> have multiple types of DIMMs: <i>err_msg</i>
Cause	DIMMs of different types are in the same memory channel.
Impact	Unsupported configuration.
Resolution	Ensure that all DIMMs in a memory channel are of the same type. Verify capacity, model, and manufacturer of DIMMs.

---

#### ESXi version compatibility [106415]

---

Name	ESXi version compatibility
Description	Check ESX version compatibility with NOS
Cause	ESXi on the cluster is not of the recommended version.
Impact	Identified ESXi version on the cluster is either incompatible or has issues with CBT/VADP APIs.
Resolution	Upgrade ESXi on the cluster.
Resolution	Refer to KB 1729 for more details.

---

#### BMC firmware version check [106416]

---

Name	BMC firmware version check
Description	Check BMC Firmware Version
Cause	BMC firmware version is older than the recommended version.
Impact	Baseboard management controller (BMC) might not work properly.
Resolution	Upgrade the BMC firmware. Refer to the Nutanix documentation for instructions.

---

#### **ESXi TCP delayed ACK check [106417]**

---

Name	ESXi TCP delayed ACK check
Description	Check TCP delayed ack settings
Cause	'TCP Delayed ACK' is enabled on ESXi
Impact	'TCP Delayed ACK' is enabled on ESXi.
Resolution	Upgrade NOS to at least 3.5.5 or 4.0.1.
Resolution	Run "vsish -e set /net/tcpip/instances/defaultTcpipStack/sysctl/_net_inet_tcp_delayed_ack 0".

---

#### **ESXi Driver compatibility check [106418]**

---

Name	ESXi Driver compatibility check
Description	Check compatibility of the installed ixgbe driver with NOS
Cause	Intel ixgbe driver is on qualified driver version earlier than 3.21.4.
Impact	Qualified driver for products based on the Intel 82599 and x540 10 Gigabit Ethernet Controllers.
Resolution	Upgrade driver to 3.21.4(steps in KB1555) for products based on the Intel 82599 and x540 10GigE network interface controllers for use with both ESXi 5.5 and 6.0.

---

#### **ESXi services check [106419]**

---

Name	ESXi services check
Description	Check if ESXi services are up on the host
Cause	One of ssh, ntpd, shell, vpxa, lbtd, DCUI, sfcbd services are not running.
Impact	Cluster connectivity, cluster synchronization, adding host to cluster, accessing console may be impacted.
Resolution	Check following services on the ESX host: SSH, ntpd, vpxa, lbtd, DCUI, sfcbd services.

---

#### **ESXi VAAI plugin installed [106421]**

---

Name	ESXi VAAI plugin installed
Description	Check if the latest version of VAAI Plugin is installed
Cause	Incorrect ESXi VAAI plugin version for AOS version.
Impact	Suboptimal storage performance due to lack of supported VAAI primitives (VMware KB 1021976).
Resolution	Review KB 1868.

---

### **ESXi VAAI plugin enabled [106422]**

---

Name	ESXi VAAI plugin enabled
Description	Check if VAAI Plugin is enabled
Cause	ESXi VAAI plugin is not enabled.
Impact	Suboptimal storage performance due to lack of storage hardware acceleration (VMware KB 1021976).
Resolution	Review KB 1868.

---

### **Some storage containers have a high number of NFS files [106426] []**

---

Name	NFS file count check
Description	Check that NFS datastore file count below threshold 20000
Alert message	Some storage containers have a high number of NFS files
Cause	Number of files for respective storage containers has increased beyond 20K. This is expected with large VDI setups.
Impact	High number of NFS files may cause vpxa services on esxi hosts to restart.
Resolution	Reduce the number of files if you observe vpxa instability.

---

### **hostd Service Not Running [106427] []**

---

Name	VMware hostd service check
Description	Check if hostd access is available
Alert message	hostd service is not running.
Cause	VMware hostd service may not be running.
Impact	If hostd service is not running, AOS upgrade will fail.
Resolution	Check hostd status and restart it manually.

---

### **CVM port group renamed [106428]**

---

Name	CVM port group renamed
Description	Check that CVM port group name has not changed
Cause	CVM port group is renamed on the ESXi hosts.
Impact	NCC checks dependent on the default port group might fail executing the checks.
Resolution	Refer to KB 1904

---

### **ESXi Scratch Configuration [106429]**

---

Name	ESXi Scratch Configuration
------	----------------------------

---

Description	Check ESXi Scratch settings
Cause	Host contains a scratch location that is not properly configured or the locker.conf cannot be read.
Impact	If scratch space is not available, temporary data is stored on a RAM disk with limited space, causing issues and log files not being updated.
Resolution	Manually configure the scratch location.
Resolution	Review KB 2046.

---

#### **ESXi configured VMK check [106430]**

Name	ESXi configured VMK check
Description	Check that correct vmk is chosen
Cause	Host Management IP in esx.conf does not match the host ip in zeus config.
Impact	A cluster upgrade or node addition operation might fail
Impact	The cluster will choose the wrong ESXi interface as management server IP address when a node is added.
Resolution	Review KB 2049 and KB 2522

---

#### **Ivy Bridge performance check [106441]**

Name	Ivy Bridge performance check
Description	Check Ivy Bridge performance degradation scenarios on ESXi
Cause	
Impact	Performance issues may be observed at Applications or OS level.
Resolution	Review KB 2729.

---

#### **VMKNICs subnets check [106442]**

Name	VMKNICs subnets check
Description	Check if vmknics have different subnets
Cause	vmknics have ip address configured in the same subnet
Impact	vmknics in the same ip subnet on the same esxi host is unsupported.
Resolution	Correct the IP addressing in the network.
Resolution	Review KB 2722 for more details.

---

#### **ESXi CPU model and UVM EVC mode check [106444]**

Name	ESXi CPU model and UVM EVC mode check
------	---------------------------------------

---

---

Description	Check CPU model and UVM EVC mode on ESXi
Cause	Some SMEP enabled VMs detected.
Impact	Performance might be degraded for the affected VMs.
Resolution	Review KB 3000. ESXi upgrade might be required.

---

#### **ESXi APD handling check [106445]**

---

Name	ESXi APD handling check
Description	Check if APD handling is disabled.
Cause	APD handling is enabled.
Impact	
Resolution	Refer KB 3328 for steps to disable APD handling.

---

#### **ESXi NFS heartbeat timeout check [106446]**

---

Name	ESXi NFS heartbeat timeout check
Description	Check if NFS heartbeat timeout is set to recommended value.
Cause	NFS heartbeat parameter is set NOT set to 30 secs.
Impact	This parameter essentially decides the amount of time ESXI waits before aborting a heartbeat request. If set incorrectly, it may cause ESXI to perceive the datastore status incorrectly.
Resolution	Refer KB 3328 for steps to disable APD handling.

---

#### **Incorrect Kerberos Setup [106450] []**

---

Name	Hyper-V Kerberos setup check
Description	Check if Kerberos is set up correctly
Alert message	Kerberos is not set up correctly.
Cause	Kerberos is not setup correctly.
Impact	Kerberos authentication is impacted.
Resolution	Check Kerberos setup.
Resolution	Review KB 3030 for additional details.

---

#### **Hyper-V VMQ Check [106451]**

---

Name	Hyper-V VMQ Check
Description	Check if VMQ is disabled on host
Cause	VMQ is enabled on Hyper-V host.

---

---

Impact	Enabling VMQ on NICs with a faulty driver can cause VMs to fail during live migration.
Resolution	Nutanix recommends that you disable VMQ. To do so, find the VMQ status: Get-NetAdapterVmq and for the component for which VMQ is enabled, disable VMQ. Disable-NetAdapterVmq -name <component>.

---

#### **Hyper-V Host pending reboots check [106452]**

---

Name	Hyper-V Host pending reboots check
Description	Check that host has no pending reboots
Cause	Host has pending reboot.
Impact	Hyper-v Hosts pending reboots after Windows cluster aware or other updates/hyperv controller utilities fail to show any disks attached even though the disks are physically attached.
Resolution	Restart the Hyper-v Host.

---

#### **Orphaned shadow copies [106453]**

---

Name	Orphaned shadow copies
Description	Check if no orphan shadows copies are present
Cause	Detected orphaned volumed shadow copies.
Impact	Performance degradation
Resolution	Remove orphaned VSS copies, review KB 2798.

---

#### **Domain join check [106454]**

---

Name	Domain join check
Description	Check if host is joined to a domain
Cause	Node(s) is/are not joined to a domain.
Impact	The host will not be manageable using Hyper-V Manager or SCVMM.
Resolution	Refer to KB 2231.
Resolution	Join the cluster and nodes to a domain.

---

#### **Hyper-V services check [106455]**

---

Name	Hyper-V services check
Description	Check if essential services are running on the host.
Cause	NutanixHAService/DiskMonitoerService/NutanixHostAgent not running properly.
Impact	Cluster cannot do disk monitoring and storage traffic re-routing if the Controller VM is unreachable or down.

---

---

Resolution	Verify status of Nutanix services. Review KB2242 for detailed information.
------------	----------------------------------------------------------------------------

---

#### **Window update check [106456]**

Name	Window update check
Description	Check if automatic Windows updates are disabled on the host
Cause	Windows update mode is set to automatic.
Impact	Hyper-V hosts can reboot in an uncontrolled manner because of automatic windows updates.
Resolution	Set the update mode to Manual. Refer to KB article 2253

---

#### **MS Failover cluster check [106457]**

Name	MS Failover cluster check
Description	Check if the Hyper-V failover cluster is properly configured
Cause	Hyper-V failover cluster is not configured with host disk drives.
Impact	It can cause outage as it will prevent disks from being available to CVMs after CVM and Host reboot.
Resolution	Refer to KB 2282.

---

#### **Required Windows features check [106458]**

Name	Required Windows features check
Description	Check if the required Windows features are installed and the banned Windows features are not installed
Cause	Required windows roles are not enabled on the host.
Impact	Recommended features are not enabled.
Resolution	Review KB 2244.

---

#### **Host networking check [106459]**

Name	Host networking check
Description	Check if networking is properly configured on the host
Cause	The Nutanix-specific virtual network switches are not correctly configured.
Impact	Nutanix services will not come up in the Controller VM.
Resolution	Create the missing vmswitches/network adapters.

---

#### **Hyper-V host power scheme [106460]**

---

Name	Hyper-V host power scheme
Description	Check if high performance profile is enabled on the host
Cause	Power scheme on the host is not configured to High Performance.
Impact	Hosts can experience increased latency and performance might be degraded.
Resolution	Review KB 2217.

---

#### **Nutanix Utilities [106461]**

---

Name	Nutanix Utilities
Description	Check if high performance profile is enabled on the host
Cause	Required Nutanix utilities are not found on the host.
Impact	Some Nutanix Services will fail to start.
Resolution	Review KB 2254.

---

#### **CVM configuration check [106462]**

---

Name	CVM configuration check
Description	Check if the CVM is properly configured
Cause	A problem with the CVM configuration has been detected.
Impact	CVM services may not start after reboot.
Resolution	Review KB 2283 and 2219.

---

#### **Storage access from Host [106463]**

---

Name	Storage access from Host
Description	Check if storage is accessible from the host
Cause	Storage is not properly configured on the host.
Impact	All storage I/O might go to a single node.
Resolution	Review KB 2263.

---

#### **WinRM service check [106464]**

---

Name	WinRM service check
Description	Check if the winrm service on the host is listening on port 5985
Cause	WinRM service not running in one or more Hyper-V hosts.
Impact	WinRM service not running in one or more Hyper-V hosts.

---

---

Resolution	Ensure that the WinRM service is running and listening on the port 5986.
Resolution	Review KB 2243 for more details.

---

#### **Crash dumps check [106465]**

---

Name	Crash dumps check
Description	Check crash dumps on the host
Cause	Dedicated kernel crash dump is not enabled.
Cause	Kernel crash dump exists on the host.
Impact	Host kernel crash dump may not work correctly.
Resolution	Review KB 2249.

---

#### **High Availability Routes check [106466]**

---

Name	High Availability Routes check
Description	Check if HA routes are setup correctly in the host in pre 4.0 releases.
Cause	The External switch may have to be recreated.
Impact	HA will be unavailable.
Resolution	You can recover the routes by running genesis restart on the Controller VM.

---

#### **UTC clock check [106467]**

---

Name	UTC clock check
Description	Check if UTC Clock is enabled
Cause	UTC clocks on the node are not enabled or CVMs are not in sync.
Impact	
Resolution	Review KB 2711.

---

#### **User VMs status [106468]**

---

Name	User VMs status
Description	Check if the user virtual machines are properly configured
Cause	User VMs are in critical state.
Impact	User VMs in critical state can not be accessible.
Resolution	Review KB 2259.

---

### CVM Panics check [106469]

---

Name	CVM Panics check
Description	Check CVM Serial Console Log for panics.
Cause	
Impact	
Resolution	

---

### Host Missing Critical Windows Updates [106470] []

---

Name	Critical Windows updates check
Description	Check if required windows updates are installed
Alert message	Host is missing critical Windows Updates.
Cause	Host is missing critical Windows Updates.
Impact	Host might experience problems regarding storage / live migration.
Resolution	Install hotfixes KB 2975719 and KB 3087856.
Resolution	Review KB 3011 for more information.

---

### HyperV VSS file limit check [106473]

---

Name	HyperV VSS file limit check
Description	Check VSS containers have file count within limit.
Cause	VSS can fail on containers with higher file count.
Impact	VSS may fail on the container.
Resolution	Reduce the number of files in the container below the file limit.

---

### Remote Site Time Sync [110001]

---

Name	Remote Site Time Sync
Description	Checks whether Time drift between remote site is below {remote_site_sync_warn_threshold_sec} seconds.
Cause	Time drift between source and remote cluster is above {remote_site_sync_warn_threshold_sec}.
Impact	Remote replication may fail to complete as expected.
Resolution	Use NTP to sync time

---

### Remote site connectivity not normal. [110002] []

---

Name	Remote Site Connectivity
------	--------------------------

---

Description	Check if connectivity to remote sites is normal.
Alert message	Connectivity to remote site <i>remote_name</i> is not normal.
Cause	Remote site may not have the local site configured as a remote.
Cause	Remote site might be stale (destroyed and re-created).
Cause	Cluster services at remote site might not be running.
Cause	Network connectivity to remote site might have been lost.
Cause	Firewall/VPN on source cluster, remote cluster, or both may prevent connection establishment.
Impact	Remote replication may fail to complete as expected.
Resolution	Configure the local site as a remote on the remote site.
Resolution	Remove and re-add the remote site on the local cluster.
Resolution	Ensure that cluster services at remote site are running.
Resolution	Check network connectivity to remote site.
Resolution	Check firewall/VPN on source cluster and remote cluster to allow them to connect to each other.

---

#### Remote Site MTU settings [110005]

Name	Remote Site MTU settings
Description	Check MTU setting for connecting to remote cluster
Cause	MTU size mismatch on CVMs between remote sites.
Impact	Degraded replication performance may be observed if MTU size is not consistent between remote sites.
Resolution	Review KB 1949.

---

#### Remote Site configuration [110006]

Name	Remote Site configuration
Description	Check remote site configuration on local and remote sites
Cause	Remote site is not properly configured.
Impact	Nutanix snapshot replication might fail to the remote site.
Resolution	Review KB 3335.

---

#### Remote Site virtual external IP(VIP) [110007]

Name	Remote Site virtual external IP(VIP)
Description	Check if remote site configuration on remote sites has virtual ip of this cluster
Cause	Remote Cluster may not be using the virtual external IP address (VIP) of the local cluster for remote site connectivity.

---

---

Impact	CVM shutting down on a remote site results in replication problems.
Resolution	Add the virtual external IP address (VIP) of the local cluster to the remote site configuration of the remote cluster. Add the virtual external IP address (VIP) of the remote cluster to the remote site configuration of the local cluster.

---

#### AWS cloud instance not configured properly. [110008] []

---

Name	AWS Instance Check
Description	Verify that the AWS cloud instances have recommended configuration.
Alert message	AWS cloud instance at remote <i>remote_name</i> not configured properly.
Cause	AWS instance does not have at least two 190GB+ disks.
Impact	Curator scans may fail.
Resolution	Make sure that AWS instance has at least two 190GB+ disks.

---

#### Old generation AWS instance configured. [110009] []

---

Name	AWS Instance Type Check
Description	Checks whether old generation AWS instance is configured for remote site.
Alert message	old generation AWS instance is configured for remote site <i>remote_name</i> . Follow KB 3861 to change the instance type to m3.2xlarge and cloud CVM configuration for better RPO/RTO.
Cause	Present AWS instance has slow replication performance.
Impact	Present AWS instance has slow replication performance.
Resolution	Follow the KB 3861 to change the instance type to m3.2xlarge and cloud CVM configuration.

---

#### AOS version of cloud remote site is less than source cluster. [110010] []

---

Name	Cloud Remote Version Check
Description	Check AOS version for cloud remote site.
Alert message	AOS version of cloud remote site <i>remote_name</i> : ( <i>remote_nos_version</i> ) is less than that of source cluster( <i>src_nos_version</i> ).
Cause	AOS version of cloud remote site is lower than that of source cluster.
Impact	Performance improvements made in new AOS version will not be available for cloud CVM.
Resolution	Upgrade cloud remote site.

---

---

**Cloud cluster does not have all recommended gflags set. [110012] []**

---

Name	Cloud Gflags Check
Description	Check if cloud remote sites have recommended gflags set.
Alert message	Cloud cluster does not have all recommended gflags set.
Cause	Cluster may have been upgraded to a newer version.
Impact	Some of the improvements made in new release will not be enabled.
Resolution	Set recommended gflags. The <code>cloud_connect_fix</code> script can be run.

---

**Egroup count on cloud disk is higher than the recommended threshold. [110013] []**

---

Name	Cloud Egroup Count check
Description	Check if egroup count on cloud remote is within threshold.
Alert message	Egroup count on cloud disk is higher than the recommended threshold.
Cause	Large amount of data may have been stored on cloud appliance.
Impact	Slow performance can be seen.
Resolution	Spread the PDs to be replicated among multiple cloud CVMs.

---

**Active Backup Schedule Check [110200]**

---

Name	Active Backup Schedule Check
Description	Checks if a backup schedule exists for protection domain protecting some entities.
Cause	No backup schedule exists for protection domain protecting some entities.
Cause	Backup schedules exists for protection domain not protecting any entity.
Impact	No backups will be made.
Resolution	Configure a backup schedule for protection domain protecting some entities.
Resolution	Delete backup schedule(s) for protection domain not protecting any entity.

---

**Storage Container Mount Configuration [110201]**

---

Name	Storage Container Mount Configuration
Description	Verify that the Storage Containers are mounted on all nodes.
Cause	Storage Containers are not mounted on all nodes.
Impact	Registration of VMs may fail during restoration from backup.
Resolution	Mount the Storage Containers on all nodes.

---

### **Local Backup Configuration [110204]**

---

Name	Local Backup Configuration
Description	Verify if recovery is possible from a local backup.
Cause	Backup schedule is not configured properly.
Cause	Backup is not happening as expected.
Impact	Recovery from local backup may not be possible.
Resolution	Verify backup schedule configuration.
Resolution	Verify if backups are happening without error.

---

### **Replication Snapshot Rate [110205]**

---

Name	Replication Snapshot Rate
Description	Checks if replication is lagging behind snapshot generation rate
Cause	Replication is lagging behind snapshot generation rate
Impact	Restore from remote cluster will be affected.
Resolution	Check if the replication link is healthy and is configured with sufficient bandwidth.

---

### **Shared Link Clone Check [110209]**

---

Name	Shared Link Clone Check
Description	Checks if linked clones are spread across multiple consistency groups.
Cause	Linked clones are spread across multiple consistency groups
Impact	No backups will be made.
Resolution	Group linked clones under same consistency group

---

### **Cluster Certificate Expiring [110215] [A1115]**

---

Name	SED CA Certificate
Description	Check if CA certificates are about to expire.
Alert message	Cluster CA certificate <i>certificate_name</i> expires on <i>expiration_date</i> .
Cause	Certificates have defined expiration dates.
Impact	If the cluster's certificate expires, it will be unable to verify trust of server certificates.
Resolution	Get a new signed certificate.

---

### **Cloud remote check [110220]**

---

Name	Cloud remote check
------	--------------------

---

---

Description	Check backup and on-wire compression settings for cloud remote sites
Cause	
Impact	
Resolution	Contact Nutanix support.

---

#### **Cloud cluster does not have recommended configuration locally [110221] []**

---

Name	Cloud local check
Description	Check that cloud cluster has recommended configuration locally.
Alert message	Cloud cluster does not have recommended configuration locally. Verify that cloud cluster has recommended configuration locally and then proceed.
Cause	AWS cluster does not have exactly two storage pools (backup-sp and DoNotUse-sp).
Cause	Storage Pool backup-sp does not have exactly one disk with CLOUD storage tier.
Cause	Some remote sites configured on cloud do not have onwire compression enabled.
Impact	
Resolution	Contact Nutanix support.

---

#### **Secondary PDs Not in Sync [110222] []**

---

Name	Metro Availability Secondary PD sync check
Description	Check if secondary metro PD is in sync with primary
Alert message	Secondary Protection domains are no more in sync with primary Protection domains.
Cause	Link between primary and secondary is not healthy.
Impact	Secondary protection domain is no more in sync.
Resolution	Review KB 3032.

---

#### **Backup snapshots on metro secondary check [110223]**

---

Name	Backup snapshots on metro secondary check
Description	Check if there are any backup snapshots on a metro secondary which can be used to reclaim space
Cause	A local snapshot of the Storage Container saved on the standby cluster in a metro availability configuration.
Impact	Snapshot exists on remote site and Free space on cluster is less than 15 percent.
Resolution	Upgrade the cluster to NOS 4.1.4 or later/Acropolis base software 4.5 or later.

---

#### **Checkpoint snapshot on Metro configured Protection Domain [110224]**

---

Name	Checkpoint snapshot on Metro configured Protection Domain
Description	Check that last auto checkpoint snapshot was taken in the last 4 hours
Cause	Automatic checkpoint snapshot might not be created or created with delay.
Impact	Time for data replication and resync will be longer when Metro Availability is re-enabled.
Resolution	Create a schedule manually for checkpoint snapshot.
Resolution	Review KB.

---

#### **Data Protection Linked Clone check [110225]**

---

Name	Data Protection Linked Clone check
Description	Check Linked clones
Cause	Linked Clone Detected on NOS <3.5.3 with Data Protection/Disaster Recovery enabled.
Impact	Running Linked Clones on a NOS pre 3.5.3 cluster is not supported and may cause problems.
Resolution	Disable Linked Clones, Data Protection, or upgrade NOS to 3.5.3 or higher.

---

#### **Host based snapshots check [110226]**

---

Name	Host based snapshots check
Description	Check for checkpoints on VMs protected by Nutanix Protection Domains
Cause	Checkpoints are found on the VMs protected by Nutanix Protection Domains.
Impact	Nutanix's native protection domain snapshots will fail on the VMs that have Checkpoints.
Resolution	Remove all the checkpoints taken on the VMs.

---

#### **ESX VM Virtual Hardware Version Compatible [110227]**

---

Name	ESX VM Virtual Hardware Version Compatible
Description	Check Virtual hardware version compatibility of protected VMs
Cause	Virtual hardware version of the VM is not compatible with the maximum virtual hardware version supported by any of the nodes at the remote site.
Impact	VMs will not be registered on the remote site hosts upon PD failover.
Resolution	Upgrade the hypervisor version on the remote site to support virtual hardware version for the VM.

---

#### Duplicate VM names [110228]

---

Name	Duplicate VM names
Description	Check for duplicate VM names
Cause	Duplicate named VMs are found.
Impact	Duplicate named VMs will not be protected by protection domains.
Resolution	Review KB 1907.

---

#### Protection Domains File share [110229]

---

Name	Protection Domains File share
Description	Check for files/VMs protected by multiple protection domains
Cause	Some files/VMs are being protected by multiple protection domains.
Impact	Migrating such a PD would remove the VMs from the inventory.
Resolution	Review KB 2034.

---

#### Vstore PDs with multiple CGs [110231]

---

Name	Vstore PDs with multiple CGs
Description	Check for multiple consistency groups in PDs
Cause	This is probably a result of SRA-SRM workflows creating multiple CGs in respective PDs.
Impact	Having more than one consistency group for a Storage Container level protection domain can result in issues when snapshot restore or DR failover actions are initiated.
Resolution	Contact Nutanix support.

---

#### Unhealthy data replication [110232]

---

Name	Unhealthy data replication
Description	Check if Data Replication is healthy.
Cause	Cluster is running NOS 4.1.1 or higher with snapshots from older version or the cluster is running with snapshots with NOS version less than 4.1.1
Impact	Inability to restore from snapshots.
Resolution	Upgrade the NOS version to 4.1.1 or higher and delete the older snapshots.
Resolution	Review KB 2089 for more information.

---

#### Snapshot file location check [110233]

---

Name	Snapshot file location check
------	------------------------------

---

---

Description	Check snapshot file location
Cause	VM protected by Nutanix Protection Domain has a trailing backslash in the snapshot file location.
Impact	Nutanix snapshots might be skipped for these VMs if they are protected by Nutanix Protection Domains.
Resolution	Review 2069.

---

#### **Latest Snapshot contains all the UVMs [110234]**

---

Name	Latest Snapshot contains all the UVMs
Description	Check that all VMs are protected by snapshot
Cause	Snapshot doesn't include all the VMs protected by that protection domain.
Impact	Some VMs are not protected.
Resolution	Review KB 3336.

---

#### **Detected VMs with non local data [110237]**

---

Name	Detected VMs with non local data
Description	Metro Availability VMs are accessing data from local cluster.
Cause	Detected VMs polling data from remote location.
Impact	Performance degradation
Resolution	Review KB 2093.

---

#### **Metro protection domain active on both sites [110239]**

---

Name	Metro protection domain active on both sites
Description	Check that Metro protection domain active on both sites
Cause	Metro protection domain is active on both sites.
Impact	Synchronous replication will not happen when both sites are in Active State.
Resolution	Disable Metro protection from the primary site and then reenable.

---

#### **No Checkpoint Snapshots on Metro PD in Last Hour [110240] []**

---

Name	Automatic checkpoint schedule for Metro Protection Domain
Description	Check that Metro PDs have associated checkpoint snapshots
Alert message	Checkpoint snapshots are not taken on the Metro configured protection domain in the last one hour.
Cause	No snapshot checkpoints are taken on Metro protection domain in the last one hour

---

Impact	Having checkpoint snapshots will help minimize the data replication and resync time when Metro configured protection domains is re-enabled in the same or reverse direction.
Resolution	Review KB 3031.

---

#### **Files in a stretched VMs should be in the same Storage Container [110241]**

Name	Files in a stretched VMs should be in the same Storage Container
Description	Check that VMs are consistently stretched
Cause	VM that is protected by Metro protection domain has some of its files in a different Storage Container from the Metro protected Storage Container.
Impact	VMs might not be properly recovered on the remote site.
Resolution	If the VM resides on a Metro enabled Storage Container, move all its associated files to the same Storage Container.

---

#### **Vstore VM Files Consistency Check [110253]**

Name	Vstore VM Files Consistency Check
Description	Check that VMs in a Vstore are consistently protected
Cause	VM that is protected by Vstore protection domain has some of its files in a different Storage Container from the Vstore protected Storage Container.
Impact	VMs might not be properly recovered on the remote site.
Resolution	If the VM resides on a Vstore protection enabled Storage Container, move all its associated files to the same Storage Container.

---

#### **E-mail alerts check [111000]**

Name	E-mail alerts check
Description	Check email alerts
Cause	E-mail alerts disabled
Impact	Alerts will not be sent through email, asup cases might not be created.
Resolution	Review smtp configuration.
Resolution	Review KB 1586.

---

#### **E-mail alerts contacts configuration [111001]**

Name	E-mail alerts contacts configuration
Description	Check email contacts
Cause	E-mail alerts do not have contacts configured.

---

---

Impact	Alerts are enabled, but no contacts are configured.
Resolution	Configure emails contacts where alerts should be sent.

---

#### Cassandra nodes up [111002]

---

Name	Cassandra nodes up
Description	Check that all Cassandra nodes are running
Cause	
Impact	Meta data load is inconsistent.
Resolution	If no other Cassandra checks are failing, repair nodetool by following KB 1369. If other Cassandra checks are failing, contact Nutanix support.

---

#### Cassandra tokens consistent [111003]

---

Name	Cassandra tokens consistent
Description	Check that all Cassandra nodes are consistent
Cause	
Impact	Meta data load is inconsistent.
Resolution	If no other Cassandra checks are failing, repair nodetool by following KB 1369. If other Cassandra checks are failing, contact Nutanix support.

---

#### Cassandra metadata balanced across CVMs [111004]

---

Name	Cassandra metadata balanced across CVMs
Description	Check that Cassandra metadata balanced across CVMs
Cause	Metadata is not distributed evenly among nodes in the cluster.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Correct imbalance by using the nCLI command 'cluster cassandra-token-range-skewfixer-start'.

---

#### Zookeeper fault tolerance check [111007]

---

Name	Zookeeper fault tolerance check
Description	Checks if Zookeeper services have the desired fault tolerance level
Cause	Zookeeper and/or Zookeeper monitor services are down on one or more nodes
Impact	The cluster may not be able to continue operating in the case of a node or block failure.
Resolution	Contact Nutanix support

---

**Time since last Curator scan is beyond threshold [111008] []**

---

Name	Curator scan time elapsed check
Description	Check if time since last Curator Scan is beyond threshold.
Alert message	Time since last Curator scan is beyond threshold. Contact Nutanix support for assistance.
Cause	Background cluster maintenance tasks are not occurring.
Impact	Cluster operation may be affected.
Resolution	Contact Nutanix Support.

---

**Zookeeper Not Active on All CVMs [111009] []**

---

Name	Zookeeper active on all CVMs
Description	Checks if number of active zookeepers is equal to the total number of zookeeper CVMs
Alert message	zookeeper is not active on all CVMs.
Cause	Zookeeper service is not running on all CVMs.
Impact	Cluster resiliency is affected.
Resolution	Contact Nutanix support.

---

**Zookeeper nodes distributed in multi-block cluster [111010]**

---

Name	Zookeeper nodes distributed in multi-block cluster
Description	Checks if zookeeper nodes are distributed in a multi block cluster
Cause	Zookeeper service has nodes running in the same block.
Impact	Cluster is not block aware.
Resolution	Review KB 1587.

---

**Zookeeper Alias Check [111011]**

---

Name	Zookeeper Alias Check
Description	Check Zookeeper alias information configuration
Cause	ZK aliases in one or more sources do not match with the Zookeeper server config maintained by Zookeeper.
Impact	Nutanix utilities or Nutanix cluster services may not work as expected.
Resolution	Ensure the ZK aliases are consistent across all locations.

---

**GPU drivers installed [111015]**

---

Name	GPU drivers installed
------	-----------------------

---

---

Description	Check if drivers are installed
Cause	GPU driver may be corrupt or missing or not functioning properly.
Impact	GPU card (NVIDIA) may not function properly.
Resolution	Confirm that GPU is installed and re-install or upgrade the driver.
Resolution	Review KB 2714.

---

#### **Host passwordless SSH [111019]**

---

Name	Host passwordless SSH
Description	Check passwordless SSH into local hypervisor
Cause	
Impact	
Resolution	

---

#### **Non default gflags check [111020]**

---

Name	Non default gflags check
Description	Check for non-default gflag values
Cause	One or more gflags are set to non-default values.
Impact	System is running with non default value of gflag and upgrade will evaporate the gflag values and set it back to normal.
Resolution	Review KB 1530.

---

#### **Degraded Node check [111021]**

---

Name	Degraded Node check
Description	Check if any node is in degraded state
Cause	
Impact	
Resolution	Contact Nutanix support.

---

#### **Name server configuration [111022]**

---

Name	Name server configuration
Description	Check for DNS Server configuration
Cause	Name server is not configured on CVMs and hypervisor hosts or is not able to resolve queries.
Impact	Name resolution will not work.

---

---

Resolution	Verify if Name server is configured on CVMs and on hypervisor hosts and if it can resolves queries. Review KB 3005 for more details.
------------	--------------------------------------------------------------------------------------------------------------------------------------

---

#### **HTTP proxy check [111023]**

---

Name	HTTP proxy check
Description	Check if HTTP proxy is working
Cause	No proxy configured.
Cause	Unable to connect to proxy on the port.
Impact	
Resolution	Check the proxy server setting like network, port, user credentials, etc

---

#### **LDAP configuration [111024]**

---

Name	LDAP configuration
Description	Check LDAP configuration.
Cause	LDAP not correctly configured in the cluster.
Impact	Directory users might not be able to log properly.
Resolution	Review KB 2997.

---

#### **Pulse configuration [111025]**

---

Name	Pulse configuration
Description	Check for auto support configuration
Cause	Pulse is not configured.
Impact	Pulse emails will not be sent.
Resolution	Verify if Pulse is configured, if emails can be send via SMTP server or connections to nsc01.nutanix.net/nsc02.nutanix.net hosts are successfull.
Resolution	Review KB 1585 for more details.

---

#### **Snapshots space utilization status [111026]**

---

Name	Snapshots space utilization status
Description	Check that space occupied by snapshots is below the threshold
Cause	Snapshots disk space utilization exceeds the threshold.
Impact	Snapshots occupies most of the disk space on the cluster.
Resolution	Review KB 1853.

---

#### **Virtual IP check [111027]**

---

Name	Virtual IP check
Description	Check if virtual ip is configured and reachable
Cause	
Impact	
Resolution	

---

#### **Remote syslog server check [111028]**

---

Name	Remote syslog server check
Description	Check remote syslog server connectivity
Cause	Remote syslog server is not reachable.
Impact	remote syslog will not be receiving log output from cluster.
Resolution	Check for network problem with rsyslog server or upstream network.

---

#### **Internal port configuration [111029]**

---

Name	Internal port configuration
Description	Check if internal config port is disabled
Cause	Port 7777 is enabled on CVM.
Impact	This configuration is not recommended for security reasons.
Resolution	Disable port 7777 on the CVMs.

---

#### **Deduplication efficiency check [111030]**

---

Name	Deduplication efficiency check
Description	Check that value of content_cache_dedup_ref_count is low
Cause	Deduplication is not working efficiently. Usually occurs when deduplication is enabled after Storage Container has been in use.
Impact	Space saved by deduplication is not optimal.
Resolution	Move guest VMs from one Storage Container to another to generate deduplication fingerprint, or use vdisk_manipulator tool to create fingerprint on a specific vdisk.

---

#### **Storage Pool SSD tier usage [111031]**

---

Name	Storage Pool SSD tier usage
Description	Check that storage pool SSD tier usage under ILM threshold
Cause	Storage Pool SSD utilization consistently above 75%.

---

---

Impact	Performance degradation.
Resolution	Delete unnecessary data.
Resolution	Review knowledge article 2882 for more information.

---

#### **Cluster version check [111032]**

---

Name	Cluster version check
Description	Check that cluster runs GA version of NOS
Cause	Non GA version of NOS/AOS detected.
Impact	Cluster is on Non GA version.
Resolution	Review KB 2720.

---

#### **Hardware configuration validation [111033]**

---

Name	Hardware configuration validation
Description	Check that /etc/nutanix/factory_config.json is valid
Cause	factory_config.json does not contain valid configuration.
Impact	Service degradation.
Resolution	Review KB 3001.

---

#### **File permissions check [111034]**

---

Name	File permissions check
Description	Check /tmp permissions
Cause	Proper permissions are not set on /tmp directory in the CVM.
Impact	Some Nutanix services will fail to read/write data into /tmp directory which results in service crashes.
Resolution	Set /tmp directory permissions to 1777. Run the command "sudo chmod 1777 /tmp"

---

#### **Advanced Encryption Standard (AES) enabled [111035]**

---

Name	Advanced Encryption Standard (AES) enabled
Description	Checks AES enabled on CPUs.
Cause	Intel's Advanced Encryption Standard (AES) is disabled on the node.
Impact	If AES is disabled, AHV might fail to boot properly on the node.
Resolution	Enable AES on the node. Review KB 3513.

---

### **Hypervisor version check [111037]**

---

Name	Hypervisor version check
Description	Check whether the same hypervisor version running on all cluster nodes.
Cause	Hypervisor version is not same across all hosts.
Impact	It is recommended to keep the hypervisor version same across all the hosts in the cluster.
Resolution	Keep hypervisor versions same across the hosts in the cluster.

---

### **Zookeeper connections check [111038]**

---

Name	Zookeeper connections check
Description	Check that Zookeeper is correctly configured for a cluster
Cause	
Impact	
Resolution	Review KB 1587.

---

### **Field Advisory 31 check [111043]**

---

Name	Field Advisory 31 check
Description	Determine if cluster is affected by Field Advisory 31.
Cause	Cluster is affected by Field Advisory 31.
Impact	Data corruption
Resolution	Follow recommended resolutions given in FA31 and KB2320.

---

### **Check that cluster virtual IP address is part of cluster external subnet [111044] []**

---

Name	Check that cluster virtual IP address is part of cluster external subnet
Description	Check that cluster virtual IP address is part of cluster external subnet
Alert message	Cluster virtual IP address <i>vip</i> is in a different subnet from the cluster external subnet <i>external_subnet</i>
Cause	Cluster virtual IP address is in a different subnet from the cluster external subnet
Impact	Data protection in between remote sites will be affected.
Resolution	Ensure that cluster virtual IP address is part of cluster external subnet

---

### **Mellanox NIC Speed is not 10GbE and 40 GbE or both 10GbE and 40GbE NICs are installed on one node [111047] []**

---

Name	Mellanox NIC Status check
------	---------------------------

---

---

Description	Checks if Mellanox NICs are down or if any Mellanox NIC has speed other than 10GbE or 40GbE. Checks if both 10GbE and 40GbE Mellanox NICs are installed on one node.
Alert message	Mellanox NIC on host <i>host_ip</i> has problem: <i>alert_msg</i>
Cause	The NIC is disconnected from the switch, or the switch port is not functioning correctly, or both 10GbE and 40GbE Mellanox NICs are installed on one node.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Ensure that the NIC is connected to the switch and that the switch port is functioning properly. Ensure that only 10GbE or 40GbE Mellanox NIC is installed on one node.

---

#### Cluster running out of CPU capacity (low runway). [120089] []

---

Name	cluster_cpu_running_out_alert_insights
Description	Predict high CPU resource usage.
Alert message	Cluster <i>cluster_name</i> is running out of CPU resource in approximately <i>data_int</i> days.
Cause	Cluster CPU running out.
Impact	Application performance on cluster may be degraded.
Resolution	Add more nodes to the cluster to increase cluster CPU capacity, reduce CPU-intensive VMs, or reduce the total number of VMs on cluster.

---

#### Cluster running out of Memory capacity (low runway). [120094] []

---

Name	cluster_memory_running_out_alert_insights
Description	Predict high memory resource usage.
Alert message	Cluster <i>cluster_name</i> is running out of Memory resource in approximately <i>data_int</i> days.
Cause	Cluster memory running out.
Impact	Application performance on cluster may be degraded.
Resolution	Add more memory to nodes if applicable, add more nodes to the cluster to increase cluster memory capacity, reduce memory-intensive VMs, or reduce the total number of VMs.

---

#### Cluster running out of storage capacity (low runway). [120113] []

---

Name	cluster_storage_running_out_alert_insights
Description	Predict high storage space usage on cluster.
Alert message	Cluster <i>cluster_name</i> is running out of storage capacity in approximately <i>data_int</i> days.
Cause	Cluster storage running out.

---

---

Impact	The cluster will run out of storage space, and may become unable to service I/O requests.
Resolution	Add more nodes to the cluster to increase cluster storage capacity, remove storage intensive VMs, or reduce the total number of VMs on the cluster.

---

#### Cannot Remove Password Protected Disk(s) [130003] [A1106]

---

Name	Password Protected Disk Status
Description	Cannot remove password protected disk(s)
Alert message	Cannot remove password protected disks <i>disk_id_list</i> from the configuration as they cannot be cleaned.
Cause	Either the disks are offline, pulled out or the corresponding node is down.
Impact	The disks cannot be removed from the configuration.
Resolution	Ensure the disks are accessible.

---

#### Metadata Drive AutoAdd Disabled [130004] [A1079]

---

Name	Metadata Drive AutoAdd Disabled Check
Description	Metadata Drive AutoAdd Disabled
Alert message	Automatic addition of Metadata drive on CVM <i>service_vm_id</i> with IP address <i>ip_address</i> has been disabled by CVM.
Cause	This node has been removed from metadata store after being automatically added recently. Automatic addition of this node to the metadata store has now been disabled.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Automatic addition will be re-enabled when the node is manually added to the metadata store. If the node was down for an extended period of time and is now running, add it back to the metadata store by going to host details. Otherwise, contact Nutanix support.

---

#### Node detached from metadata ring [130005] [A1055]

---

Name	Metadata Drive Ring Check
Description	Node detached from metadata ring
Alert message	Metadata drive on CVM <i>ip_address</i> is now detached from ring due to <i>reason</i> .
Cause	Either a metadata drive has failed, the node was down for an extended period of time, or an unexpected subsystem fault was encountered, so the node was removed from the metadata store.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.

---

Resolution	If the metadata drive has failed, replace the metadata drive as soon as possible. Refer to the Nutanix documentation for instructions. If the node was down for an extended period of time and is now running, add it back to the metadata store by going to host details. Otherwise, contact Nutanix support.
------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

#### Metadata Dynamic Ring Change Operation Stuck [130006] [A1117]

Name	Metadata DynRingChangeOp Status
Description	Dynamic Ring Change operation not making progress
Alert message	<i>operation for node ip_address is not progressing. Node performing the operation: ip_address_doing_ring_change</i>
Cause	A node in the cluster is unhealthy.
Impact	Node addition and node removal operations will not proceed to completion.
Resolution	Ensure that all nodes in the cluster are healthy. If they are and the alert persists, contact Nutanix support.

#### Metadata Dynamic Ring Change Operation Too Slow [130007] [A1116]

Name	Metadata DynRingChangeOp Slow Check
Description	Dynamic Ring Change operation too slow
Alert message	<i>operation for node ip_address is progressing slowly. Total elapsed time: elapsed_time_mins min(s). Node performing the operation: ip_address_doing_ring_change</i>
Cause	A node in the cluster is unhealthy, or the cluster contains an extraordinarily large amount of data.
Impact	Cluster performance may be degraded.
Resolution	Ensure that all nodes in the cluster are healthy. If they are and the alert persists, contact Nutanix support.

#### Metadata drive failed [130008] [A1037]

Name	Metadata Drive Failed Check
Description	Metadata Drive Failed
Alert message	Metadata service on CVM ip_address is running in forwarding mode due to reason.
Cause	Either a metadata drive has failed, node removal has been initiated, or an unexpected subsystem fault has been encountered.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.

### Large Metadata Size Detected [130009] [A1119]

---

Name	Metadata Size
Description	Large metadata size detected
Alert message	Node <i>ip_address</i> contains a large amount of metadata.
Cause	A node in the cluster contains a large amount of metadata and has exceeded thresholds.
Impact	Cluster performance may be degraded.
Resolution	Ensure that all nodes in the cluster are healthy. If they are and the alert persists, contact Nutanix support.

---

### Metadata Drive Detached [130011] [A1054]

---

Name	Metadata Drive Detached Check
Description	Metadata Drive Detached
Alert message	Metadata drive on CVM <i>ip_address</i> is marked to be detached from ring due to <i>reason</i> .
Cause	Either a metadata drive has failed, the node was down for an extended period of time, or an unexpected subsystem fault was encountered, so the node is marked to be removed from the metadata store.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	If the metadata drive has failed, replace the metadata drive as soon as possible. Refer to the Nutanix documentation for instructions. If the node was down for an extended period of time and is now running, add it back to the metadata store by going to host details. Otherwise, contact Nutanix support.

---

### Metadata Ring Imbalance [130012] [A1072]

---

Name	Metadata Imbalance Check
Description	Cassandra Metadata Imbalance
Alert message	Metadata ring imbalance for <i>num_partitions</i> partitions. The partitions are <i>partition_list</i>
Cause	One or more nodes have a disproportionately larger token range size. This imbalance can cause performance bottlenecks on the node(s) affected.
Impact	Node performance may be significantly degraded.
Resolution	Execute cassandra ring skew fix operation using the NCLI command 'cluster cassandra-token-range-skew-fixer-start'.

---

### Curator Job Running Too Long [130015] [A1120]

---

Name	Curator Job Status
------	--------------------

---

---

Description	Curator Job Running Too Long
Alert message	Curator job <i>name</i> with id <i>execution_id</i> has been running for a long time i.e. <i>elapsed_time_secs</i> seconds.
Cause	Various
Impact	Background cluster maintenance tasks might get affected in the future. The root cause should be addressed as soon as possible.
Resolution	Contact Nutanix support if this issue persists.

---

#### **Curator Scan Failure [130016] [A1081]**

---

Name	Curator Scan Status
Description	Curator Scan Failure
Alert message	Curator <i>scan_type</i> scans have repeatedly failed to complete.
Cause	Various
Impact	Background cluster maintenance tasks are not occurring. While cluster operation will not be immediately affected, the root cause should be addressed as soon as possible.
Resolution	Contact Nutanix support.

---

#### **Duplicate IP Address Detected [130017] [A1096]**

---

Name	IP Configuration
Description	Duplicate IP Address Detected
Alert message	Detected IP address conflict for cluster virtual IP address <i>duplicate_ip</i> .
Cause	The cluster virtual IP address may be configured on another host.
Impact	The cluster is not accessible through the virtual IP address. Other services that use the virtual IP address, such as remote replication or SCCM, may be affected.
Resolution	Either configure a different cluster virtual IP address or unconfigure the IP address from the other host.

---

#### **Duplicate Remote Cluster ID [130018] [A1038]**

---

Name	Duplicate Remote Cluster ID Check
Description	Duplicate Remote Cluster ID
Alert message	Remote cluster ' <i>remote_name</i> ' is disabled because the name conflicts with remote cluster ' <i>conflicting_remote_name</i> '.
Cause	Two remote sites with different names or different IP addresses have same cluster ID. This can happen in two cases: (a) A remote cluster is added twice under two different names (through different IP addresses) or (b) Two clusters have the same cluster ID.
Impact	Protected data is not replicated to the remote site.

---

---

Resolution	In case (a) remove the duplicate remote site. In case (b) verify that the both clusters have the same cluster ID and contact Nutanix support.
------------	-----------------------------------------------------------------------------------------------------------------------------------------------

---

#### **IP Address Not Hosted [130023] [A1097]**

---

Name	Virtual IP Configuration
Description	IP Address Not Hosted
Alert message	Unable to host virtual IP address <i>ip_address</i> .
Cause	The network configuration is corrupted.
Impact	The cluster is not accessible through the virtual IP address. Other services that use the virtual IP address, such as remote replication or SCCM, may be affected.
Resolution	Contact Nutanix support.

---

#### **SMTP Error [130060] [A1080]**

---

Name	SMTP Configuration
Description	Failed to send email
Alert message	Failed to send email from Controller VM <i>ip_address</i> via SMTP server <i>smtp_host:smtp_port</i> due to following error : <i>error</i> .
Cause	The cluster cannot send Pulse and alert emails to Nutanix support with the current configuration.
Impact	Nutanix support cannot proactively monitor cluster health and offer assistance before issues become acute.
Resolution	Ensure an SMTP server is configured and reachable from the cluster. If no SMTP server is configured, ensure that the firewalls allow the cluster to send email messages through the Nutanix SMTP servers (nsc01.nutanix.net and nsc02.nutanix.net) on port 80.

---

#### **Remote site latency is high [130075] [A1168]**

---

Name	RemoteSiteHighLatency
Description	Latency to a stretch remote site is high
Alert message	Latency to remote site ' <i>remote_name</i> ' has been more than ' <i>remote_site_high_latency_threshold_ms</i> ' ms , for ' <i>sustained_high_latency_secs</i> ' seconds
Cause	Various
Impact	Replication will fail
Resolution	Check if remote site is reachable.

---

#### Possible degraded Node [130087] []

---

Name	Node Degradation Status
Description	Services on node possibly not making progress.
Alert message	Possible degraded Node <i>ip_address</i> .
Cause	Various
Impact	Services on the node are running but possibly not making progress.
Resolution	Contact Nutanix support.

---

#### CPS Deployment Evaluation Mode [130093] []

---

Name	CPS Deployment Evaluation Mode
Description	Checks if the CPS deployment is running in evaluation mode.
Alert message	CPS deployment of cluster with cluster id <i>cluster_id</i> is running in evaluation mode. Please apply a license by following the CPS deployment guide.
Cause	CPS is running in evaluation mode.
Impact	The deployment cannot be in evaluation and the user has to apply a license.
Resolution	Apply a license to the deployment.

---

#### Stretch connectivity is lost [130119] []

---

Name	Stretch Connectivity Lost
Description	Stretch connectivity is lost
Alert message	Stretch connectivity from local site ' <i>Local_stargate_handler</i> ' to remote site ' <i>remote_name</i> ' is lost due to ' <i>reason</i> '
Cause	Remote site(s) not reachable
Impact	Metro connection of the remote site is unavailable
Resolution	Check remote site(s) connectivity and reenable if necessary

---

#### Alert raised on cloud remote site {remote\_name}: {alert\_message} [130135] []

---

Name	Cloud Remote Alert
Description	Alert generated on cloud remote site.
Alert message	Alert raised on cloud remote site <i>remote_name</i> : <i>alert_message</i>
Cause	Various
Impact	Various
Resolution	Resolve the issue stated in the alert. If you cannot resolve the issue, please contact Nutanix support.

---

#### **File Server Space Usage High [160000] []**

---

Name	File Server Space Usage
Description	File Server Space Usage High
Alert message	File Server space usage for <i>file_server_name</i> is at <i>usage_pct</i> %.
Cause	File Server Storage utilization is high.
Impact	If storage usage keeps growing, the shares will be marked as read-only.
Resolution	Expand File Server storage size, or ask users to delete unused files.

---

#### **File Server Space Usage Critical. [160001] []**

---

Name	File Server Space Usage Critical
Description	File Server Space Usage Critical
Alert message	File Server space usage for <i>file_server_name</i> is at <i>usage_pct</i> %.
Cause	File Server storage utilization has reached a critical value.
Impact	The shares will be marked as read-only until there is more free space on the File Server.
Resolution	Expand the File Server storage size, or ask users to delete unused files.

---

#### **File Server Unreachable. [160002] []**

---

Name	File Server Unavailable Check
Description	File server is unreachable.
Alert message	File server <i>file_server_name</i> is unreachable.
Cause	File server VMs are not reachable.
Impact	No operations can be executed against the file server.
Resolution	Contact Nutanix support.

---

#### **File Server storage is not available. [160003] []**

---

Name	File Server Storage Status
Description	file server storage is not available.
Alert message	Storage for File Server <i>file_server_name</i> is unavailable.
Cause	file server storage is unavailable due to network connectivity issues between file server VM and Controller VM.
Impact	Read and write operations on the file server will fail.
Resolution	Contact Nutanix support.

---

**File Server scale-out failed. [160004] []**

---

Name	File Server Scale-out Status
Description	File Server scale-out failed.
Alert message	File Server <i>file_server_name</i> scale-out failed because of <i>reason</i>
Cause	See details in the alert message.
Impact	Unable to scale-out the file server.
Resolution	Contact Nutanix support.

---

**File Server could not join the AD Domain [160005] []**

---

Name	File Server Join Domain Status
Description	File Server could not join the AD Domain
Alert message	File Server <i>file_server_name</i> could not join the Domain because <i>reason</i>
Cause	See details in the alert message. Error could be due to one of the following reasons:AD is not reachable, or Domain credentials are invalid, or Entity with the specified File Server name already exists in the domain
Impact	No operations can be performed on the File Server as it has not joined the domain
Resolution	The resolution will depend on the cause, and could be either to check that the Domain is actually reachable or to provide the correct administrator credentials or to provide a different name for the File Server to avoid conflicts in the name.

---

**Node failed to join domain. [160006] []**

---

Name	File Server Node Join Domain Status
Description	The node could not join the domain.
Alert message	The node could not join the domain for file server <i>file_server_name</i> as <i>reason</i>
Cause	AD is not reachable or Domain administrator credentials are invalid or a file server with the same name already exists in AD.
Impact	The node could not join the domain.
Resolution	Provide the correct domain administrator credentials or a different name for the file server.

---

**File Server Time Difference High [160007] []**

---

Name	FSVM Time Drift Status
Description	The time drift between the file server VMs is beyond the acceptable range
Alert message	Time drift between the file server VMs ( <i>lower_time_ip</i> and <i>higher_time_ip</i> ) is more than the acceptable value of <i>time_difference_limit_secs</i>
Cause	NTP is not configured correctly or the NTP service is not functioning.

---

---

Impact	The AFS cluster may become inaccessible
Resolution	Check that the NTP service is running and is reachable from the file server VMs

---

#### **File server unreachable check [160008] []**

---

Name	File Server Network Reachable
Description	Checks that File server is reachable
Alert message	File server <i>file_server_name</i> is unreachable
Cause	File server Network is unreachable
Impact	File server operations will not work.
Resolution	Contact Nutanix support.

---

#### **File server down check [160009] []**

---

Name	File Server Reachable
Description	Checks that File server is down
Alert message	File server <i>file_server_name</i> is down
Cause	All File server VMs are powered off
Impact	File server operations will not work.
Resolution	Contact Nutanix support

---

#### **File server mutiple VMs on single node check [160010] []**

---

Name	File Server VM Status
Description	Checks that multiple File server VMs are running on a single node
Alert message	File server <i>file_server_name</i> has mutiple VMs on single node
Cause	File server VMs are running on a single node
Impact	Single node failure may bring down the File server
Resolution	Contact Nutanix support.

---

#### **File server services down check [160011] []**

---

Name	File Server Status
Description	Checks that all File server services are running
Alert message	File server <i>file_server_name</i> services are down
Cause	One or more services are not running on File server VMs.
Impact	File server operations will not work.

---

---

Resolution	Contact Nutanix support.
------------	--------------------------

---

**File Server storage cleanup failed [160012] []**

---

Name	File Server Storage Cleanup Failure
Description	Failed to clean up storage for the File Server
Alert message	Storage message for the File Server <i>file_server_name</i> is not cleaned up
Cause	Acropolis service may be down on the cluster
Impact	File server storage will not be released
Resolution	Delete the volume groups associated with the file server using the 'acli vg.delete' command.

---

**File server cannot connect with AD server [160013] []**

---

Name	File Server AD Connectivity Failure
Description	File server cannot connect with AD server with configured information
Alert message	File server <i>file_server_name</i> cannot connect with AD server
Cause	The machine account credentials may have been changed, or there is a network connectivity issue for the AD server.
Impact	File server is in non-operational state. Client connectivity with file-server is disabled.
Resolution	Check that the AD server is reachable.
Resolution	Try leaving and joining the domain again.

---

**File Server performance optimization recommended [160015] []**

---

Name	File Server Performance Optimization Recommended
Description	File server has a recommendation to optimize performance by using scale-up, scale-out or rebalance.
Alert message	A recommendation is available to optimize the performance on one or more nodes of file server <i>file_server_name</i> .
Cause	File server has one or more nodes under extensive load.
Impact	File server performance may be impacted and new client connections may be refused.
Resolution	Run 'Performance optimization' for the specified file server.

---

**User Quota Assignment Failed [160016] []**

---

Name	File Server Quota allocation failed for user
Description	Failed to assign the specified quota to the user

---

Alert message	Failed to apply quota for user: <i>user_name</i> on share: <i>share_name</i> of File Server <i>file_server_name</i>
Cause	The user has used more space on the File Server than the specified quota value.
Impact	User has no quota limit
Resolution	Notify user to reduce their usage below the quota value, or increase the quota allocation for the user.

---

#### **Share utilization reached configured limit [160017] []**

---

Name	Share Utilization Reached Configured Limit
Description	Share is no longer writeable.
Alert message	Utilization on <i>share_name</i> on file server <i>file_server_name</i> has reached the configured limit
Cause	Share utilization reached its configured limit
Impact	Writes to the share will fail until one of the actions is taken.
Resolution	Ask users to free up space or increase storage allocation to the share.

---

#### **File Server failed to get updated CVM IP address. [160018] []**

---

Name	File Server CVM IP update failed
Description	File server cvm ip update failed.
Alert message	The file server <i>file_server_name</i> could not get updated CVM IP address.
Cause	Failed to contact file server .
Impact	File server is not reachable
Resolution	Contact Nutanix support.

---

#### **Appropriate Site Not Found in Active Directory [160019] []**

---

Name	File Server Site Not Found
Description	Unable to determine an appropriate site in Active Directory
Alert message	File server <i>file_server_name</i> 's client network is not mapped to a site on the Active Directory.
Cause	File server client network is not part of any site in Active Directory.
Impact	File server may take a long time to join the domain, depending on which domain controller is selected.
Resolution	Add the client network of file server to a local site in Active Directory for optimal performance.

---

**File Server DNS Updates Pending [160020] []**

---

Name	File Server DNS Updates Pending
Description	DNS updates are pending after a file server operation.
Alert message	File server <i>file_server_name</i> 's DNS updates are pending after the join or leave domain operation.
Cause	Failed to add or remove DNS entries
Impact	The File Server cannot be used by clients by until the DNS entries are manually created or remove as specified.
Resolution	Find a list of pending DNS entries in 'file server DNS' tab on file server page and add or remove the specified DNS mappings on the DNS server manually.

---

**File Server activation failed [160021] []**

---

Name	File Server Activation Failed
Description	File Server Activation Failed
Alert message	File server <i>file_server_name</i> activation failed due to <i>reason</i>
Cause	Check alert message for details
Impact	File Server is not usable.
Resolution	Try to activate file server again, and if the failure persists, then contact Nutanix support.

---

**File Server PD activates on multiple sites [160022] []**

---

Name	File Server PD Active On Multiple Sites
Description	Checks that File Server PD Active On Multiple Sites
Alert message	File server <i>file_server_name</i> protection domain <i>protection_domain_name</i> activates on multiple site(s) <i>remote_site_names</i>
Cause	File Server PD activates on multiple sites
Impact	File server operations might not work
Resolution	Deactivate PD on other sites

---

**Failed to set VM-to-VM anti-affinity rule [160023] []**

---

Name	Failed To Set VM-to-VM Anti Affinity Rule
Description	Failed to set VM-to-VM anti affinity rule
Alert message	Failed to set VM-to-VM anti-affinity rule for <i>file_server_name</i> . <i>reason_and_resolution_msg</i>
Cause	Contact Nutanix support.
Impact	More than one FSVM may be deployed on a single physical host, which will cause data unavailability in case that host fails.

---

---

Resolution	Various. Check alert message for details.
------------	-------------------------------------------

---

**File server home share creation failed [160024] []**

---

Name	File Server Home Share Creation Failed
Description	Failed to create home share during file server creation.
Alert message	Failed to create Home share for <i>file_server_name</i> because <i>message</i>
Cause	Check alert message for details
Impact	The default home share is not created.
Resolution	Check alert message to understand cause of failure and take action accordingly.

---

**Discovery of iSCSI targets failed. [160025] []**

---

Name	File Server Iscsi Discovery Failure
Description	Failed to discover iSCSI targets on the CVM during the discovery process.
Alert message	Discovery of iSCSI targets failed for file server <i>file_server_name</i>
Cause	The 'external_data_services_ip' or the CVM IP addresses are not reachable from the file server VM.
Impact	Share operations and file server HA will fail.
Resolution	Check the configured IP addresses and ensure connectivity from the file server VM's storage network to the external_data_services_ip and the CVM IPs.

---

**File Server upgrade failed [160026] []**

---

Name	File Server Upgrade Failed
Description	File Server Upgrade Failed.
Alert message	Upgrade of file server <i>file_server_name</i> failed due to <i>reason</i> .
Cause	Check alert message for details
Impact	File server has not been upgraded.
Resolution	Try again. If the failure persists, contact Nutanix support

---

**File server invalid snapshot [160027] []**

---

Name	File Server Invalid Snapshot Warning
Description	Checks that File server is in healthy state to take snapshot
Alert message	File server <i>file_server_name</i> is not healthy and leads to invalid snapshot
Cause	File Server NVMs might deleted
Impact	File server operations will not work and creates the bad snapshots

---

---

Resolution	Cancel the snapshot schedule
Resolution	Avoid taking snapshot and migration
Resolution	Contact Nutanix support.

---

#### Incompatible File Server [160028] []

---

Name	Incompatible File Server Activation
Description	File Server version incompatible with AOS
Alert message	File server <i>file_server_name</i> is incompatible with AOS
Cause	Version of activated file server is incompatible with AOS
Impact	File server configuration cannot be edited. In addition, next AOS upgrade will fail.
Resolution	Upgrade file server to new AFS release

---

#### File server entities not protected [160029] []

---

Name	File Server Entities Not Protected
Description	Checks all File server entities are protected
Alert message	Some of File server <i>file_server_name</i> entities are not protected
Cause	Some of the File Server entities are not protected
Impact	File server migration might fails and creates the bad snapshots
Resolution	Contact Nutanix support.

---

#### Multiple File server versions are present in the cluster. [160030] []

---

Name	Multiple File Server Versions Check
Description	Checks whether multiple File server versions are running in the cluster
Alert message	File Servers are on different versions. Please upgrade all File Servers to the same version as soon as possible.
Cause	File server(s) were powered off or not reachable during the last fileserver upgrade.
Impact	FileServer upgrade may not upgrade some file servers.
Resolution	Upgrade individual File Server.

---

#### File server upgrade task is not progressing. [160031] []

---

Name	File Server Upgrade Task Stuck Check
Description	Check that file server task is progressing.
Alert message	File server <i>file_server_name</i> upgrade task is not progressing.

---

---

Cause	Various. Check alert message for details.
Impact	File server upgrade may fail to complete.
Resolution	Contact Nutanix support

---

#### **File Server in heterogeneous state. [160032] []**

---

Name	File Server In Heterogeneous State
Description	File server in heterogeneous state.Nodes do not match in their CPU or memory configuration.
Alert message	File server <i>file_server_name</i> is in heterogeneous state , as upgrade failed due to <i>reason</i>
Cause	Various. Check alert message for details.
Impact	Performance of the file server is less than optimal.
Resolution	Contact Nutanix support

---

#### **File Server PD enabled on non-compatible Remote Site [160033] []**

---

Name	Remote Site Not File Server Capable
Description	Checks File server remote sites are file server capable
Alert message	File server <i>file_server_name</i> protection domain <i>protection_domain_name</i> enabled on non-compatiable Remote site <i>remote_site_name</i>
Cause	Remote site is not File server capable
Impact	File server migration/failover will fail
Resolution	Upgrade remote site cluster NOS to 5.0 and above version

---

#### **Failed to correct File Server data and meta data inconsistencies [160034] []**

---

Name	Failed To Run File Server Metadata Fixer Successfully
Description	Failed to Run File Server Metadata Fixer tool successfully
Alert message	Failed to run File Server <i>file_server_name</i> Metadata fixer task successfully. <i>reason_and_resolution_msg</i>
Cause	Metadata fixer task might timedout
Impact	Some of the top level directory might not shown on file server
Resolution	Rerun the Metadata fixer scli command on File server

---

#### **File server share deletion failed [160035] []**

---

Name	File Server Share Deletion Failed
------	-----------------------------------

---

---

Description	Failed to delete share.
Alert message	Failed to delete share <i>share_name</i> on File Server <i>file_server_name</i> . <i>message</i>
Cause	{cause_message}
Impact	Contents of share may not have been fully deleted after delete request.
Resolution	{message}

---

#### **File server compatibility check skipped [160036] []**

---

Name	Skipped File Server Compatibility Check
Description	File server compatibility check skipped
Alert message	File server compatibility check skipped
Cause	File server compatibility check was skipped during AOS upgrade
Impact	Some management functions of the file server may not be available.
Resolution	Upgrade file servers that reside on the cluster.

---

#### **Snapshot Invalid for Clone [160037] []**

---

Name	File Server Clone - Snapshot invalid
Description	Pre-asterix.2 snapshot is invalid for clone
Alert message	Snapshot Invalid for Clone <i>pd_name</i> . <i>reason_and_resolution_msg</i>
Cause	Clone feature needs snapshot taken from asterix.2 onwards
Impact	Pre-asterix.2 snapshots cannot be cloned
Resolution	Take/Use new snapshot

---

#### **Failed to add one or more file server administrator users or groups [160038] []**

---

Name	Failed to add one or more file server admin users or groups
Description	Failed to add one or more users or groups as file server administrators
Alert message	File server <i>file_server_name</i> : <i>failure_msg</i> Update file server administrators on the file server page
Cause	One or more users or groups could not be resolved on Active Directory.
Impact	File server administrator users or groups may not function as administrators
Resolution	Update file server administrators on the file server page

---

#### **Maximum connections limit reached on a file server VM [160039] []**

---

Name	Maximum connections limit reached on a file server VM
------	-------------------------------------------------------

---

---

Description	Maximum connections limit reached on a file server VM
Alert message	File server VM <i>fsvm_name</i> on file server <i>file_server_name</i> has reached maximum connections limit.
Cause	File server has one or more nodes under extensive load.
Impact	File server performance may be impacted and new client connections may be refused.
Resolution	Run 'Performance optimization' for the specified file server.

---

#### **File Server Clone failed [160040] []**

---

Name	File Server Clone Failed
Description	File Server Clone Failed
Alert message	File server <i>file_server_name</i> clone failed due to <i>reason</i>
Cause	Check alert message for details
Impact	Clone File Server not available.
Resolution	Check alert message, Retry clone operation after rectifying, and if the failure persists, then contact Nutanix support.

---

#### **File Server rename failed [160041] []**

---

Name	File Server Rename Failed
Description	File Server Rename Failed
Alert message	File server rename from <i>file_server_name</i> to <i>file_server_new_name</i> failed due to <i>reason</i>
Cause	Check alert message for details
Impact	Rename File Server not available.
Resolution	Check alert message, Retry rename operation after rectifying, and if the failure persists, then contact Nutanix support.

---

#### **Workload Status [170000]**

---

Name	Workload Status
Description	Checks for the abrupt workload changes.
Cause	VDisk is accessed uniformly across its entire dataset.
Impact	The performance of VMs on the cluster may be degraded.
Resolution	Disable the processes that cause the entire dataset to be accessed.

---

### Cluster Connectivity Status [200000] []

Name	Cluster Connectivity Status
Description	Tests whether the cluster connectivity is fine
Alert message	<i>component</i> data from cluster <i>cluster_name</i> is not up-to-date.
Cause	Cluster network connectivity or CVM services could be down.
Impact	Cluster data shown in the Prism Central is not up to date.
Resolution	Ensure that cluster network connectivity is up and all CVM services are up.

### Dynamic scheduling failure. [200201] [A200201]

Name	Acropolis Dynamic Scheduler Status
Description	One or more nodes have resource contention. This imbalance can cause performance bottlenecks on the node(s) affected.
Alert message	Dynamic scheduling failure. <i>reason</i>
Cause	Cluster may have insufficient CPU or Controller VM resources.
Cause	Cluster may have insufficient resources to satisfy VM group affinity policies or VM host affinity policies.
Impact	Cluster performance may be significantly degraded.
Resolution	Shut down unneeded VMs to free cluster resources.
Resolution	Expand the cluster to add resources.

### PC vCPU Availability Check [200301] []

Name	PC vCPU Availability Check
Description	Checks if the number of vCPUs is sufficient for the number of VM entities in Prism Central.
Alert message	The PC does not have enough vCPUs for the number of VM entities it has.
Cause	Too many VMs in Prism Central for the number of vCPUs in the PC VM.
Impact	Prism Central performance may be degraded.
Resolution	Reduce the number of VM entities in Prism Central or provide more vCPUs for the PC VM.

### PC Sufficient Disk Space Check [200302] []

Name	PC Sufficient Disk Space Check
Description	Checks if the amount of storage is sufficient for the number of VM entities in Prism Central.
Alert message	The PC does not have enough storage for the number of VM entities it has.
Cause	Too many VMs in Prism Central for the amount of storage in Prism Central.

---

Impact	Prism Central may run out of disk space to store data.
Resolution	Reduce the number of VM entities in Prism Central or provide more storage for Prism Central.

---

#### PC Memory Availability Check [200303] []

---

Name	PC Memory Availability Check
Description	Checks if the amount of memory is sufficient for the number of VM entities in Prism Central.
Alert message	The PC does not have enough memory for the number of VM entities it has.
Cause	Too many VMs in Prism Central for the amount of memory in the PC VM.
Impact	Services running in Prism Central may run out of memory and crash.
Resolution	Reduce the number of VM entities in Prism Central or provide more memory for the PC VM.

---

#### PC VM Limit Check [200304] []

---

Name	PC VM Limit Check
Description	Checks if the number of VM entities is within the limit.
Alert message	The PC cannot handle this many VM entities.
Cause	Too many VMs in Prism Central.
Impact	Prism Central performance may be degraded.
Impact	Prism Central may run out of disk space to store data.
Impact	Services running in Prism Central may run out of memory and crash.
Resolution	Reduce the number of VM entities in Prism Central.

---

### Controller VM

#### CVM Boot Raid Degraded [1019] [A1107]

---

Name	Boot RAID Health
Description	Check the health of boot RAID volumes.
Alert message	Boot RAID volumes on CVM <i>service_vm_external_ip</i> are degraded.
Cause	RAID volume can be in an abnormal state due to power loss or temporary or permanent drive failure.
Impact	Can be indicate boot drive failure. The CVM would be inoperable with an additional failure.
Resolution	Verify boot disk status from the web console Hardware page and replace the disk if required.

---

### **Abnormal Host Boot RAID State [1020] [A1105]**

---

Name	Host Boot RAID State
Description	Check the health of boot RAID volumes.
Alert message	Hypervisor RAID volume ' <i>volume_Label</i> ' is in abnormal state ' <i>volume_state</i> ' on host <i>host_ip</i> .
Cause	RAID volume can be in an abnormal state due to power loss or temporary or permanent drive failure.
Impact	Can be indicate boot drive failure. The CVM would be inoperable with an additional failure.
Resolution	Use iDRAC to examine RAID status to decide whether to replace a drive.

---

### **CVM RAM Usage High [3023] [A1056]**

---

Name	CVM Memory Usage
Description	Check that CVM memory usage is not high.
Alert message	Main memory usage in Controller VM <i>ip_address</i> is high. <i>available_memory_kb</i> KB of memory is free.
Cause	The RAM usage on the Controller VM has been high.
Impact	Cluster performance may be significantly degraded.
Resolution	Contact Nutanix Support for diagnosis. RAM on the Controller VM may need to be increased.

---

### **CVM NTP Time Synchronized [3026]**

---

Name	CVM NTP Time Synchronized
Description	Checks that the CVM is able to synchronize time with one of the configured NTP servers.
Cause	CVM is not synchronizing time with an NTP server.
Impact	Workflows involving Kerberos may fail if the time difference between the Controller VM and the NTP server is greater than 5 minutes.
Resolution	Check that NTP servers are configured and reachable.

---

### **Kernel Memory Usage High [3027] [A1034]**

---

Name	Kernel Memory Usage
Description	Checks whether CVM's kernel memory usage is higher than expected
Alert message	Controller VM <i>ip_address</i> 's kernel memory usage is higher than expected.
Cause	Various
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.

---

---

Resolution	Contact Nutanix support.
------------	--------------------------

---

**CVM Rebooted [3028] [A1024]**

---

Name	CVM Rebooted Check
Description	Check that Cvm is not rebooted recently
Alert message	Controller VM <i>ip_address</i> has been rebooted on <i>reboot_timestamp_str</i> .
Cause	Cvm is rebooted.
Impact	During the time the Controller VM is down, cluster compute and storage capacity are reduced.
Resolution	Check cvm status.

---

**CVM Services Restarting Frequently [3029] [A1032]**

---

Name	CVM Services Status
Description	Check if services have restarted recently in the Controller VM.
Alert message	There have been 10 or more cluster services restarts within 15 minutes in the Controller VM <i>ip_address</i> .
Cause	This alert indicates that one or more services have restarted in a Controller VM, with in a short period of time.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	If this alert occurs once or infrequently, no action is necessary. If it is frequent, contact Nutanix support.

---

**CVM CPU Utilization [3041]**

---

Name	CVM CPU Utilization
Description	Checks CPU usage is above {cvm_peak_cpu_util_threshold_pct}
Cause	CPU utilization above {cvm_peak_cpu_util_threshold_pct}.
Impact	High I/O latency may be experienced by some workloads.
Resolution	Reduce CPU intensive processes.

---

**Jumbo Frames Enabled [3063] [A1095]**

---

Name	NIC MTU Configuration
Description	Check MTU of the CVM network interfaces.
Alert message	Controller VM <i>service_vm_external_ip</i> has NIC <i>nic_name</i> with MTU set to <i>mtu</i> instead of <i>desired_mtu</i> .

---

---

Cause	MTU is not set correctly on eth0/eth1
Impact	If MTU is not set correctly in the Controller VMs, all Nutanix services timeout causing the storage to be unavailable.
Resolution	Set MTU to the right value

---

#### CVM Connectivity Failure [3064] [A1001]

---

Name	CVM Passwordless Connectivity
Description	Check that SVM has passwordless connection to each other.
Alert message	Controller VM <i>target_ip</i> is not reachable from Controller VM <i>source_ip</i> in the last 3 attempts.
Cause	SVM has no passwordless connection to each other
Impact	Cluster compute and storage capacity are reduced. Until data stored on this host is replicated to other hosts in the cluster, the cluster has one less copy of guest VM data.
Resolution	Check SVM network configuration

---

#### CVM NIC Speed Low [6008] [A1058]

---

Name	TenGig Adaptor Status
Description	Checks whether CVM is uplinked to 10 GbE NIC.
Alert message	Controller VM <i>service_vm_external_ip</i> is running on the network interface(s) <i>nic_list</i> , which is/are slower than 10 Gbps. This will degrade the system performance.
Cause	CVM not uplinked to 10 GbE NIC.
Cause	1 GbE NIC is part of the bond.
Cause	ESX hypervisor may be lockdown.
Impact	The Controller VM is not configured to use the 10 GbE NIC or is configured to share load with a slower NIC.
Resolution	Check network configuration.
Resolution	Check if ESX hypervisor is lockdown, and unlock it if it is lockdown.

---

#### CVM Host Subnet Mismatch [6202] [A1048]

---

Name	CVM Subnet
Description	Checks that host and cvm share the same subnet.
Alert message	Controller VM <i>svm_ip</i> with network address <i>svm_subnet</i> is in a different network than the Hypervisor <i>hypervisor_ip</i> , which is in the network <i>hypervisor_subnet</i> .
Cause	The Controller VM and the hypervisor are not on the same subnet.
Impact	Controller VM high availability will not apply in the case of Controller VM failure, leading to guest VM unavailability.

---

---

Resolution	Reconfigure the cluster. Either move the Controller VMs to the same subnet as the hypervisor hosts or move the hypervisor hosts to the same subnet as the Controller VMs.
------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

#### **Invalid Drive Configuration [6209] [A1164]**

---

Name	Invalid Drive Configuration
Description	Checks whether combination of SSDs and HDDs is valid.
Alert message	Invalid drive configuration seen on <i>ip_address</i> - <i>num_ssd</i> SSDs and <i>num_hdd</i> HDDs.
Cause	Combination of SSDs and HDDs on the node is not valid.
Impact	Cluster performance may be significantly degraded.
Resolution	Add or remove SSDs or HDDs to create a valid configuration.

---

#### **CPU Average Load High on Controller VM. [6511] []**

---

Name	Node Avg Load - Non Critical
Description	Verify system load average for the past 5 minutes is below {cvm_load_average_threshold}.
Alert message	Average CPU load on Controller VM <i>ip_address</i> is high (above average load threshold value <i>high_value</i> )
Cause	I/O workload on the cluster is high.
Impact	High I/O latencies may be experienced by some workloads.
Resolution	Redistribute VMs to reduce load on the affected Controller VM.
Resolution	Tune the applications to reduce CPU demand.
Resolution	Reduce the number of VMs on the host.

---

#### **HDD IO Latency [6514]**

---

Name	HDD IO Latency
Description	Verify whether the average time for I/O requests to the HDDs managed by the Controller VM is below {HDD_latency_threshold_ms} ms.
Cause	I/O workload on the cluster is high.
Impact	High I/O latencies may be experienced by some workloads.
Resolution	Redistribute VMs to reduce load on the affected Controller VM.

---

#### **CPU Average Load Critically High on Controller VM. [6516] []**

---

Name	Node Avg Load - Critical
------	--------------------------

---

---

Description	Verify system load average for the past 5 minutes is below {cvm_load_average_threshold_critical}.
Alert message	Average CPU load on Controller VM <i>ip_address</i> is critically high (above critical average load threshold value <i>critical_high_value</i> )
Cause	Critically high load on the system.
Impact	Low performance may be experienced due to cluster-wide I/O latency.
Resolution	Contact Nutanix Support for assistance.

---

#### **Controller VM Certificate Expiring [110214] [A1114]**

---

Name	SED Node Certificate
Description	Check if node certificates are about to expire.
Alert message	Certificate for key management server <i>key_management_server_name</i> for Controller VM <i>service_vm_external_ip</i> expires on <i>expiration_date</i> .
Cause	Certificates have defined expiration dates.
Impact	If the node's certificate expires then it will be unable to authenticate with external servers.
Resolution	Get a new signed certificate.

---

#### **Kerberos Clock Skew Failure [130024] [A1083]**

---

Name	Kerberos Clock Skew Status
Description	Kerberos Clock Skew Failure
Alert message	Kerberos authentication failure occurred on Controller VM <i>ip_address</i> due to clock skew between the Controller VM and the Domain Controller (reason: <i>reason</i> ).
Cause	There is considerable clock skew between the Controller VM and the Domain Controller.
Impact	The Controller VM cannot manage the host, which may lead to node instability.
Resolution	Ensure that the time on the Controller VM is synchronized with the time of the host. It can be accomplished by configuring the NTP server properly.

---

#### **Metadata Volume Snapshot Persistent Failure [130026] [A1087]**

---

Name	Metadata Volume Snapshot Persistent
Description	Metadata Volume Snapshot Persistent Failure
Alert message	The last <i>failure_count</i> metadata volume snapshots have failed. <i>reason</i>
Cause	The EBS snapshot service is unavailable, possibly because AWS could not be reached.
Impact	If the cloud instance fails, backups of the guest VM may be unavailable.
Resolution	Contact Nutanix support.

---

#### Metadata Volume Snapshot Timeout [130027] [A1088]

---

Name	Metadata Volume Snapshot Status
Description	Metadata Volume Snapshot Timeout Failure
Alert message	Metadata volume snapshot could not be created in <i>duration_mins</i> minutes.
Cause	Metadata volume snapshot frequency is too high.
Impact	If the cloud instance fails, backups of the guest VM may be unavailable.
Resolution	Contact Nutanix support.

---

#### Physical Disk Drive Has Failed [130035] [A1104]

---

Name	Physical Disk Status
Description	Physical drive has failed.
Alert message	Drive <i>disk_id</i> with serial <i>disk_serial</i> in drive bay <i>disk_Location</i> on Controller VM <i>service_vm_external_ip</i> has failed.
Cause	The drive has failed.
Impact	Cluster storage capacity is reduced.
Resolution	Replace the failed drive. Refer to the Nutanix documentation for instructions.

---

#### Physical Disk Removed From Slot [130036] [A1103]

---

Name	Physical Disk Remove Check
Description	Physical disk removed from slot
Alert message	Disk with serial <i>disk_serial</i> was removed from drive bay <i>disk_Location</i> on Controller VM <i>service_vm_external_ip</i>
Cause	A drive was physically removed from a slot.
Impact	Migration of data from the disk will start.
Resolution	No action is necessary.

---

#### Self Encrypting Drive Operation Failure [130051] [A1111]

---

Name	SED Operation Status
Description	Self encrypting drive operation failure
Alert message	Self Encrypted Drive operation <i>operation</i> has failed for disk <i>disk_id</i> with serial <i>disk_serial</i> on node <i>service_vm_external_ip</i> .
Cause	A self encrypting drive operation could not be performed.
Impact	The desired action could not be performed.
Resolution	Retest key management server configuration to ensure connectivity and that certificates are valid then retry the command, or contact Nutanix support.

---

### **Stargate Temporarily Down [130054] [A1030]**

---

Name	Stargate Status
Description	Stargate Temporarily Down.
Alert message	Stargate on Controller VM <i>ip_address</i> is down for <i>downtime</i> seconds.
Cause	Various
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Contact Nutanix support.

---

### **Unsupported Configuration For Redundancy Factor 3 [130055] [A1092]**

---

Name	FT2 Configuration
Description	Unsupported Configuration For Redundancy Factor 3.
Alert message	Controller VM <i>service_vm_id</i> with IP address <i>service_vm_external_ip</i> has <i>actual_ram_size_gbGB</i> RAM which does not meet the configuration requirement of <i>min_ram_required_gbGB</i> RAM to support 'Redundancy Factor 3' feature.
Cause	To support 'Redundancy Factor 3' feature all controller VMs in the cluster must meet the minimum requirements for RAM.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Increase RAM on the Controller VM to meet the minimum requirement. Contact Nutanix support for assistance.

---

### **Stargate Responsive [130069]**

---

Name	Stargate Responsive
Description	Check if any Stargate process is still running after being killed.
Cause	Stargate got into an unresponsive state.
Impact	Nutanix datastore may become inaccessible.
Resolution	Restart the Stargate process.

---

### **Disk Diagnostic Failure [130089] [A1139]**

---

Name	Disk Diagnostic Status
Description	Drive diagnostic has failed.
Alert message	Drive <i>disk_id</i> with serial <i>disk_serial</i> in drive bay <i>disk_Location</i> on Controller VM <i>service_vm_external_ip</i> has failed diagnostic test.
Cause	The drive has failed.
Impact	Cluster storage capacity is reduced.

---

---

Resolution	Replace the drive. Refer to the Nutanix documentation for instructions.
------------	-------------------------------------------------------------------------

---

DR

#### **Protected VMs Not On Nutanix Storage [110216] []**

---

Name	Protected VMs Storage Configuration
Description	Protected VMs have invalid storage configuration.
Alert message	Protection domain <i>pd_name</i> protects VM <i>vm_name</i> which is not on Nutanix storage.
Cause	Not all protected VMs are on Nutanix storage.
Impact	RPO will be affected.
Resolution	Verify that all protected VMs are on Nutanix storage

---

#### **VM is protected in multiple PDs. [110217] []**

---

Name	Protection Domains sharing VMs
Description	VMs are protected in multiple Protection Domains.
Alert message	VM <i>vm_name</i> is protected in multiple protection domains <i>pd_names</i> .
Cause	VMs are protected in multiple Protection Domains.
Impact	Recovery of VMs will fail.
Resolution	Verify that VMs are not protected in multiple Protection Domains.

---

#### **Unsupported number of VMs protected as part of Metro/Vstore Protection Domain. [110219] []**

---

Name	Unsupported number of VMs in the Metro or Vstore PD
Description	Unsupported number of VMs in Metro/Vstore Protection Domain.
Alert message	Metro/Vstore PD <i>pd_name</i> protects <i>num_vms</i> VMs which is more than <i>supported_num_vms</i> , supported number of VMs for a Metro PD.
Cause	Unsupported number of VMs in Metro/Vstore Protection Domain.
Impact	Metro/Vstore Protection Domain backup performance will be degraded.
Resolution	Verify that number of VMs are protected in a Metro or Vstore Protection Domains is not over the supported number.

---

#### **NGT installation required. [110242] []**

---

Name	Cross Hypervisor NGT Installation Check
Description	Some VMs in protection domain replicating to cross-hypervisor remote site do not have NGT installed.

---

Alert message	Some VMs in cross-hypervisor protection domain <i>pd_name</i> do not have NGT installed.
Cause	Some VMs in protection domain replicating to cross-hypervisor remote site do not have NGT installed.
Impact	Recovery of VMs on the remote site might fail.
Resolution	Verify that NGT is installed on all the VMs of the protection domain that you want to recover on the remote site.

---

#### Too many files in the Consistency Group. [110243] []

Name	Metro/Vstore Consistency Group File Count Check
Description	Checks if too many files are being protected by a single consistency group of any Metro/Vstore protection domain.
Alert message	The consistency group <i>cg_name</i> (part of protection domain <i>pd_name</i> ) protects <i>num_files</i> files, which exceeds the currently set threshold of <i>threshold_num_files</i> .
Cause	Too many files are being protected by a single consistency group of a Metro/Vstore protection domain.
Impact	Performance on Metro-protected or Vstore-protected Storage Container may be degraded.
Resolution	Delete some VMs/files from the consistency group, or move to another Storage Container and protect the new Storage Container.
Resolution	Change alert threshold from the alert policies section.
Resolution	If needed, contact Nutanix Support for assistance.

---

#### Too many files in the Protection Domain. [110244] []

Name	Metro/Vstore Protection Domain File Count Check
Description	Checks if too many files are being protected by any Metro/Vstore protection domain.
Alert message	The protection domain <i>pd_name</i> protects <i>num_files</i> files, which exceeds the currently set threshold of <i>threshold_num_files</i> .
Cause	Too many files are being protected by a Metro/Vstore protection domain.
Impact	Performance on Metro-protected or Vstore-protected Storage Container may be degraded.
Resolution	Delete some VMs/files from the protection domain, or move to another Storage Container and protect the new Storage Container.
Resolution	Change alert threshold from the alert policies section.
Resolution	If needed, contact Nutanix Support for assistance.

---

**Found old clones on cluster. [110245] []**

---

Name	Clone Age Check
Description	Check for any clones restored from protection domain snapshots that are too old.
Alert message	Found <i>count</i> clones related to protection domain <i>pd_name</i> which are older than the currently configured threshold of <i>clone_age_threshold</i> days.
Cause	Clones were not removed automatically.
Impact	Storage performance may be degraded.
Resolution	Remove any clones restored from protection domain snapshots that are too old.

---

**Too many clones on cluster. [110246] []**

---

Name	Clone Count Check
Description	Check if there are too many clones restored from protection domain snapshots.
Alert message	Found <i>count</i> clones related to protection domain <i>pd_name</i> which is more than the currently configured threshold of <i>clone_count_threshold</i> .
Cause	Clones were not removed automatically.
Impact	Storage performance may be degraded.
Resolution	Remove any clones restored from protection domain snapshots that are too old.

---

**Protecting VMs that are using shared VHDX disks is unsupported. [110247] []**

---

Name	Check VHDX Disks
Description	Check if VMs with shared VHDX disks are not part of any protection domain.
Alert message	Protecting VMs that are using shared VHDX disks is unsupported.
Cause	VMs with shared VHDX disks are protected, which is an unsupported configuration.
Impact	Snapshotting shared VHDX disks that are connected to protected VMs may fail.
Resolution	Unprotect VMs that use shared VHDX disks.

---

**Symlinks found on metro/vstore protected container. [110248] []**

---

Name	Metro Vstore Symlinks Check
Description	Check for symlinks in metro/vstore protection domain.
Alert message	Symlinks found on metro/vstore protected container <i>ctr_name</i> , which might lead to cluster instability.
Cause	Symlinks present in metro/vstore protection domain.
Impact	Snapshot operations on the metro/vstore protected container may fail, leading to replication failures.
Resolution	Remove symlinks from metro/vstore protected container.

---

#### Remote Stargate Version Check [110249]

---

Name	Remote Stargate Version Check
Description	Check for the AOS version running on Metro remote site.
Cause	Stargate running on Metro remote site is out of date.
Impact	Metro cluster may not be available due to crashing Stargate.
Resolution	Contact Nutanix support.

---

#### Aged third-party backup snapshots present [110250] []

---

Name	Aged Third-party Backup Snapshot Check
Description	Check for aged third-party backup snapshots.
Alert message	Protection Domain <i>pd_name</i> has <i>num_snapshot</i> aged third-party backup snapshot(s) and may unnecessarily consume storage space in the cluster.
Cause	Third-party backup snapshots are present in the cluster longer than the configured threshold.
Impact	Aged snapshots may unnecessarily consume storage space in the cluster.
Resolution	Contact Nutanix support.

---

#### Replications are scheduled on entities from the storage containers that have deduplication enabled. [110251] []

---

Name	Replication of deduped entities to non-compliant remote sites
Description	Replications are scheduled on entities from the storage containers that have deduplication enabled
Alert message	Protection domain <i>pd_name</i> with entities from the storage containers <i>dedup_ctrs</i> that have deduplication enabled are being replicated to single-node backup or cloud remote sites <i>remote_names</i> .
Cause	Protection domain with entities from the storage containers that have deduplication enabled are being replicated to a single-node backup or cloud remote site.
Impact	Performance of replications and retrievals will be affected.
Resolution	Either disable deduplication on the storage containers, or use a multi-node AOS cluster as a replication target.

---

#### Protection domain contains more than one entity. [110252] []

---

Name	PD Entity Count Check
Description	Check if PDs being replicated to cloud backup site contain more than one entity.
Alert message	Do not protect more than one entity in a protection domain <i>pd_name</i> if you are replicating to the backup-only remote site <i>remote_name</i> . <i>cloud_node</i>
Cause	PD being replicated to cloud backup site contains more than one entity.

---

Impact	Selective retrieval of any single VM will take longer. Replication schedules will be staggered because of large snapshots.
Resolution	Ensure that PDs replicating to cloud backup site contains single entity.

---

#### Secure Tunnel To Remote Site Down [130000] [A1090]

Name	Remote Site Tunnel Status
Description	Secure Tunnel To Remote Site Down.
Alert message	Secure tunnel to remote site <i>remote_name</i> is down.
Cause	Incorrect remote site configuration or network connectivity issue.
Impact	Replication to remote site will fail.
Resolution	Check if the IP address specified in the remote site is reachable.

---

#### Metro Availability Is Disabled [130002] [A1124]

Name	Metro Connectivity
Description	Metro availability is disabled.
Alert message	Metro availability for the protection domain ' <i>protection_domain_name</i> ' to the remote site ' <i>remote_name</i> ' is disabled because of ' <i>reason</i> '.
Cause	Remote site unreachable.
Impact	Metro availability operation is disabled.
Resolution	Check if cluster service is healthy at remote cluster.

---

#### Duplicate Remote Cluster ID [130018] [A1038]

Name	Duplicate Remote Cluster ID Check
Description	Duplicate Remote Cluster ID
Alert message	Remote cluster ' <i>remote_name</i> ' is disabled because the name conflicts with remote cluster ' <i>conflicting_remote_name</i> '.
Cause	Two remote sites with different names or different IP addresses have same cluster ID. This can happen in two cases: (a) A remote cluster is added twice under two different names (through different IP addresses) or (b) Two clusters have the same cluster ID.
Impact	Protected data is not replicated to the remote site.
Resolution	In case (a) remove the duplicate remote site. In case (b) verify that the both clusters have the same cluster ID and contact Nutanix support.

---

#### Entities Restored But Unprotected [130019] [A1134]

Name	Restored Entities Protected
------	-----------------------------

---

---

Description	Entities Restored But Unprotected
Alert message	Some entities became unprotected after restoring <i>protection_domain_name</i> . Count: <i>num_entities</i> . Entity names: <i>entity_names</i> . Reason: <i>reason</i> .
Cause	Some other protected entities conflict with the entities being recovered.
Impact	Some entities became unprotected after restoring the snapshot.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

#### Entities Skipped During Restore [130020] [A1132]

---

Name	Entities Restored Check
Description	Entities Skipped During Restore
Alert message	Some entities skipped during restore of <i>protection_domain_name</i> . Count: <i>num_entities</i> . Entity names: <i>entity_names</i> . Reason: <i>reason</i> .
Cause	Existing files conflict with the files to be recovered.
Impact	Not all entities could be restored from the snapshot.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

#### Invalid Consistency Group [130022] [A1136]

---

Name	Consistency Group Configuration
Description	Invalid Consistency Group
Alert message	Failed to create a snapshot of protection domain <i>protection_domain_name</i> as some files in consistency group <i>consistency_group_name</i> overlap other consistency groups.
Cause	VMs with common files are not in the same consistency group.
Impact	Snapshot will fail.
Resolution	Put VMs with common files in the same consistency group.

---

#### Metadata Volume Snapshot Persistent Failure [130026] [A1087]

---

Name	Metadata Volume Snapshot Persistent
Description	Metadata Volume Snapshot Persistent Failure
Alert message	The last <i>failure_count</i> metadata volume snapshots have failed. <i>reason</i>
Cause	The EBS snapshot service is unavailable, possibly because AWS could not be reached.
Impact	If the cloud instance fails, backups of the guest VM may be unavailable.
Resolution	Contact Nutanix support.

---

#### Metadata Volume Snapshot Timeout [130027] [A1088]

Name	Metadata Volume Snapshot Status
Description	Metadata Volume Snapshot Timeout Failure
Alert message	Metadata volume snapshot could not be created in <i>duration_mins</i> minutes.
Cause	Metadata volume snapshot frequency is too high.
Impact	If the cloud instance fails, backups of the guest VM may be unavailable.
Resolution	Contact Nutanix support.

#### Metro Availability Configuration Failed [130028] [A1123]

Name	Metro Availability
Description	Metro availability start failed
Alert message	Failed to establish Metro Availability for the protection domain ' <i>protection_domain_name</i> ' to the remote site ' <i>remote_name</i> '. Reason: ' <i>reason</i> '.
Cause	Various
Impact	Metro availability operation could not be started.
Resolution	Contact Nutanix support if this issue persists.

#### Stale NFS Mount [130029] [A1135]

Name	Metro Vstore Mount Status
Description	Stale NFS mount
Alert message	Unable to process NFS requests for vstore id <i>vstore_id</i> due to <i>reason</i> .
Cause	Stale NFS file handle.
Impact	Unable to process NFS requests.
Resolution	Unmount the datastore from all hosts and remount again.

#### Protected VM Is Not Nutanix Backup And Recovery Compliant [130037] [A1109]

Name	Protected VM CBR Capability
Description	Protected VM is not Nutanix backup and recovery compliant.
Alert message	Protected VM with name ' <i>vm_name</i> ' and internal ID ' <i>vm_id</i> ' in protection domain ' <i>protection_domain_name</i> ' cannot be backed up and restored by Nutanix.
Cause	The VM found in the protection domain has been modified to include files that are not on a Nutanix Storage Container.
Impact	Any data associated with the VM may not be backed up or replicated to a remote site.
Resolution	Remove or detach files from the VM that are not on Nutanix Storage Containers and make the VM Nutanix backup and recovery compliant.

#### **Protected VM Not Found [130038] [A1010]**

---

Name	Protected VM Not Found
Description	Protected VM not Found
Alert message	Unable to locate VM with name ' <i>vm_name</i> ' and internal ID ' <i>vm_id</i> ' protected by protection domain ' <i>protection_domain_name</i> '.
Cause	The protected VM cannot be found and may have been deleted.
Impact	Any data associated with the VM may not be backed up or replicated to a remote site.
Resolution	Remove the VM from the protection domain.

---

#### **Protection Domain Activation [130040] [A1043]**

---

Name	PD Active
Description	Protection Domain Activation
Alert message	Unable to make protection domain ' <i>protection_domain_name</i> ' active on remote site ' <i>remote_name</i> ' due to ' <i>reason</i> '.
Cause	Various
Impact	Protected VMs could not be started during failover to a remote site.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

#### **Protection Domain Change Mode Failure [130041] [A1060]**

---

Name	PD Change Mode Status
Description	Protection Domain Change Mode Failure
Alert message	Protection domain <i>protection_domain_name</i> activate/deactivate failed.
Cause	Protection domain cannot be activated or migrated.
Cause	Protection domain with same name might be active on remote site.
Impact	Protected VMs could not be started during failover to a remote site.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

#### **Failed To Change State Of One Or More VMs [130042] [A1094]**

---

Name	PD VM Action Status
Description	Failed to change state of one or more VMs.
Alert message	Failed to <i>action</i> one or more VMs in protection domain <i>protection_domain_name</i> .
Cause	The hypervisor may have insufficient resources or the configuration of the VM restored from the snapshot may be invalid.

---

Impact	If VMs failed to stop, no snapshot can be taken for the protection domain. If VMs failed to start, the VMs will not be powered on for use.
Resolution	Check error reported by the hypervisor management software. If you cannot resolve the error, contact Nutanix support.

---

#### Registration Of One Or More VMs Failed [130043] [A1093]

Name	PD VM Registration Status
Description	Registration of one or more VMs failed
Alert message	Failed to register one or more VMs during activation of protection domain <i>protection_domain_name</i> .
Cause	VMs in the snapshot have invalid VM configuration or the local hypervisor reported an error.
Impact	VMs restored from the snapshot will not be unavailable.
Resolution	Check the existence of the VM in the snapshot and check any errors reported in the hypervisor management software. If you cannot resolve the error, contact Nutanix support.

---

#### Protection Domain Full Replication Performed [130044] [A1108]

Name	PD Full Replication Status
Description	Full Replication was done.
Alert message	The replication for snapshot with id <i>snap_id</i> of protection domain <i>protection_domain_name</i> to remote site <i>remote_name</i> will be a full replication.
Cause	A reference snapshot could not be found.
Impact	The replication may take longer.
Resolution	No action is necessary.

---

#### Protection Domain Replication Expired [130045] [A1003]

Name	PD Replication Expiry Status
Description	Protection Domain Replication Expired
Alert message	Protection domain <i>protection_domain_name</i> replication to the remote site <i>remote_name</i> has expired before it is started.
Cause	Replication is taking too long to complete before the snapshots expire.
Impact	The snapshot that was scheduled to be replicated could not be replicated. Data that is expected to be protected may not be protected.
Resolution	Review replication schedules taking into account bandwidth and overall load on systems. Confirm retention time on replicated snapshots.

---

#### Protection Domain Replication Failure [130046] [A1015]

---

Name	PD Replication Status
Description	Protection Domain Replication Failure
Alert message	Protection domain <i>protection_domain_name</i> replication to remote site <i>remote_name</i> failed. <i>reason</i>
Cause	Various
Impact	Snapshots of protected VMs were not replicated to the remote site.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

#### Skipped Replication Of The Snapshot [130047] [A1113]

---

Name	PD Replication Skipped Status
Description	Skipped replication of the snapshot.
Alert message	Replication was skipped for protection domain <i>protection_domain_name</i> of snapshot <i>snapshot_name</i> to remote site <i>remote_name</i> . <i>reason</i>
Cause	Snapshot replication was skipped because a newer snapshot is available.
Impact	Snapshot is not present on the remote site.
Resolution	If this issue persists, consider reducing the replication frequency.

---

#### Protection Domain Receive Snapshot Failure [130048] [A1127]

---

Name	PD Snapshot Retrieval
Description	Protection Domain Receive Snapshot Failure.
Alert message	Snapshot receive for protection domain <i>protection_domain_name</i> from remote site <i>remote_name</i> failed. <i>reason</i>
Cause	Various
Impact	The snapshot receive operation requested by the user could not be completed.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

#### Protection Domain Snapshot Failure [130049] [A1064]

---

Name	PD Snapshot Status
Description	Protection Domain Snapshot Failure.
Alert message	Protection domain <i>protection_domain_name</i> snapshot <i>snapshot_id</i> failed because <i>reason</i> .
Cause	Protection domain cannot be snapshotted.
Cause	Metro protection domain has more entities than supported.

---

Impact	A requested snapshot of guest VMs and files in the protection domain did not succeed.
Resolution	Make sure all VMs and files are available.
Resolution	In case of Metro protection domain, make sure number of entities are within the supported limit.

---

#### **Remote Site Is Unhealthy [130050] [A1125]**

Name	Remote Site Health
Description	Remote site is unhealthy.
Alert message	Remote ' <i>remote_name</i> ' is unhealthy due to reason ' <i>reason</i> '.
Cause	Various
Impact	Replication to remote site can fail.
Resolution	Check if the IP address specified in the remote site is reachable.

---

#### **Snapshot Partially Crash Consistent [130052] [A1110]**

Name	Snapshot Crash Consistent
Description	Snapshot partially crash consistent.
Alert message	Failed to create an application-consistent snapshot for one or more VMs in snapshot <i>snapshot_name</i> of protection domain <i>protection_domain_name</i> . A crash-consistent snapshot has been created for these VMs instead.
Cause	VSS or hypervisor error
Impact	Recovery may take longer and involve manual steps.
Resolution	No action is necessary if this issue is intermittent. If this error persists, contact Nutanix support.

---

#### **VM Action Error [130057] [A1033]**

Name	VM Action Status
Description	VM Action Error
Alert message	Failed to <i>action</i> VM with name ' <i>vm_name</i> ' and internal ID ' <i>vm_id</i> ' due to <i>reason</i>
Cause	A VM could not be restored because of a hypervisor error, or could not be deleted because it is still in use.
Impact	The requested VM action (restore or delete) could not be completed.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

---

**VM Virtual Hardware Version Not Compatible [130058] [A1133]**

---

Name	VM Virtual Hardware Version Compatible
Description	VM Virtual Hardware Version not Compatible
Alert message	Virtual hardware version of the VM <i>vm_name</i> is not supported by any of the nodes on the remote site <i>remote_name</i> . Protection domain: <i>protection_domain_name</i> . VM id: <i>vm_id</i> . Reason: <i>reason</i> .
Cause	Virtual hardware version of the VM is not compatible with the maximum virtual hardware version supported by any of the nodes at the remote site.
Impact	VM may not register properly on the remote site on restore/clone.
Resolution	Upgrade the hypervisor version on the remote site to support virtual hardware version for the VM.

---

**Remote Site {remote\_name} Network Mapping Missing [130062] [A1156]**

---

Name	Remote Site Network Configuration
Description	No Network Mapping Specified.
Alert message	No network mapping specified for remote site <i>remote_name</i> .
Cause	No network mapping specified when remote site is created.
Impact	When the VM is restored or cloned on the remote site, networking configuration may not be recovered.
Resolution	Specify network mapping for the remote site.

---

**Remote Site {remote\_name} Network Mapping Invalid [130063] [A1157]**

---

Name	Remote Site Network Mapping Configuration
Description	Invalid Network Mapping Specified.
Alert message	Invalid network mapping specified for remote site <i>remote_name</i> : <i>reason</i> .
Cause	Either the source or destination network configuration is not present in network mapping specified in the remote site, or the networks specified in the network mapping do not exist.
Impact	When the VM is restored or cloned on the remote site, networking configuration may not be recovered.
Resolution	Create network mapping with the networks present on the source and the destination cluster for the remote site.

---

**Protected Volume Group not Found [130070] [A1162]**

---

Name	Protected Volume Group Not Found
Description	Protected Volume Group not Found

---

---

Alert message	Unable to locate volume group with name ' <i>vg_name</i> ' and internal ID ' <i>vg_uuid</i> ' protected by protection domain ' <i>protection_domain_name</i> '.
Cause	The protected volume group cannot be found and may have been deleted.
Impact	Any data associated with the volume group may not be backed up or replicated to a remote site.
Resolution	Remove the volume group from the protection domain.

---

#### Volume Group Action Error [130071] [A1163]

---

Name	Volume Group Action Status
Description	Volume Group Action Error
Alert message	Failed to <i>action</i> volume group with name ' <i>vg_name</i> ' and internal ID ' <i>vg_uuid</i> ' because <i>reason</i> in protection domain ' <i>protection_domain_name</i> '
Cause	A volume group could not be restored or could not be deleted because it is still in use.
Impact	The requested volume group action (restore or delete) could not be completed.
Resolution	Detach the volume group from VMs and external initiators before recovery.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

#### VSS Snapshot Failed [130073] [A130073]

---

Name	VSS Snapshot Status
Description	VSS snapshot failed.
Alert message	VSS snapshot failed for the VM(s) <i>vm_names</i> protected by the protection domain <i>name</i> in the snapshot <i>snapshot_id</i> because <i>reason</i> .
Cause	Guest is not able to quiesce VM due to internal error.
Impact	Crash consistent snapshot is taken instead of application consistent snapshot.
Resolution	Look at the logs in the guest VM. If the VM failed to quiesce, reduce the load on the VM and try again.

---

#### Nutanix Guest Tools Not Installed [130074] [A130074]

---

Name	NGT Configuration
Description	Nutanix Guest Tools not installed.
Alert message	Vss is enabled but Nutanix Guest Tools are not installed on the guest VM(s) <i>vm_names</i> protected by <i>protection_domain_name</i> .
Cause	VSS is enabled but Nutanix Guest Tools are not installed on the VM(s).
Impact	Crash consistent snapshot is taken instead of application consistent snapshot.
Resolution	Install Nutanix Guest Tools on the guest VM(s).

---

### Protection Domain might have symlinks. [130077] [A130077]

---

Name	Snapshot Symlink Check
Description	Protection domain snapshot has symlinks.
Alert message	Protection Domain <i>protection_domain_name</i> might have symlinks that have been skipped in the snapshot.
Cause	The protection domain might have symlinks that have been skipped in the snapshot.
Impact	The symlinks in the protection domain have been skipped in the snapshot.
Resolution	Delete the symlinks or protect the entities individually.

---

### Entity Restore Aborted [130078] [A130078]

---

Name	EntityRestoreAbort
Description	Entity restore aborted.
Alert message	Restoring VMs failed for snapshot <i>snapshot_id</i> protected by <i>protection_domain_name</i> because <i>reason</i> .
Cause	Unable to restore VMs due internal error.
Impact	Snapshot expiry is removed to prevent data loss, and needs to be removed manually.
Resolution	Restart the restore process. If this error persists, contact Nutanix support.

---

### Skipped Replication Of The Snapshot [130079] []

---

Name	Remote Site Snapshot Replication Status
Description	Skipped replication of the snapshot.
Alert message	Replication was skipped for protection domain <i>protection_domain_name</i> to remote site <i>remote_name</i> . <i>reason</i>
Cause	Snapshot replication was skipped because the remote is not fully upgraded.
Impact	Snapshot is not present on the remote site.
Resolution	Wait for the completion of the upgrade process on the remote before initiating snapshot schedules.

---

### Nutanix Guest Tools Agent is not reachable on the VM [130081] [A130081]

---

Name	VSS VM Reachable
Description	VM not reachable.
Alert message	VM(s) <i>vm_names</i> Guest Agent Service is not reachable, protected by <i>protection_domain_name</i> .
Cause	The communication link to the VMs Nutanix Guest Agent service seems to be down
Impact	Crash consistent snapshot is taken instead of application consistent snapshot.

---

---

Resolution	Please check and restart Nutanix Guest Agent service inside the VM
------------	--------------------------------------------------------------------

---

**Nutanix Guest Tools is not supported on remote site [130082] [A130082]**

Name	Remote Site NGT Support
Description	Remote site does not support NGT.
Alert message	Remote site <i>remote_site</i> does not support Nutanix Guest Tools. <i>reason</i> .
Cause	Remote cluster is not upgraded
Impact	Nutanix Guest Tools information for the VM will be lost.
Resolution	Upgrade the remote cluster.

---

**Protected Vms Not Found [130083] [A130083]**

Name	Protected VMs Not Found
Description	Protected Vms Not Found
Alert message	Unable to locate VM(s) <i>vm_names</i> protected by protection domain ' <i>protection_domain_name</i> '.
Cause	Protected VM(s) cannot be found and may have been deleted.
Impact	Any data associated with the VMs may not be backed up or replicated to a remote site.
Resolution	Remove VM(s) from the protection domain.

---

**Protected Volume Groups Not Found [130084] [A130084]**

Name	Protected Volume Groups Not Found
Description	Protected Volume Groups Not Found
Alert message	Unable to locate volume group(s) <i>vg_names</i> protected by protection domain ' <i>protection_domain_name</i> '.
Cause	Protected volume group(s) cannot be found and may have been deleted.
Impact	Any data associated with the volume group(s) may not be backed up or replicated to a remote site.
Resolution	Remove volume group(s) from the protection domain.

---

**VSS Software or (pre\_freeze/post\_thaw) Scripts Not Installed [130085] [A130085]**

Name	VSS Scripts Not Installed
Description	VSS software or pre_freeze/post_thaw Scripts Not Installed
Alert message	VSS is enabled but VSS software or pre_freeze/post_thaw scripts are not installed on the guest VM(s) <i>vm_names</i> protected by <i>protection_domain_name</i> .

---

Cause	VSS is enabled but VSS software or pre_freeze/post_thaw scripts are not installed on the VM(s).
Impact	Crash consistent snapshot is taken instead of application consistent snapshot.
Resolution	Install VSS software or (pre_freeze/post_thaw) scripts on the guest VM(s).

#### VStore Snapshot Status [130086] []

Name	VStore Snapshot Status
Description	VStore Snapshot Status
Alert message	Snapshot status for vstore <i>vstore_name</i> : <i>reason</i> .
Cause	Various
Impact	The requested VStore snapshot action could not be completed.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

#### Failed to snapshot entities [130088] [A130088]

Name	Failed To Snapshot Entities
Description	Failed to snapshot entities
Alert message	Failed to snapshot the entities <i>entity_names</i> in the protection domain <i>protection_domain_name</i> , snapshot <i>snapshot_id</i> .
Cause	Conflicting hypervisor tasks might be running on the entities.
Impact	The entities are not captured in the snapshot.
Resolution	

#### Related Entity Protection Status [130090] []

Name	Related Entity Protection Status
Description	Protection status of a related entity.
Alert message	<i>error_message</i> .
Cause	Related entity is not protected in the same protection domain.
Impact	Related VM/Volume Group will not be snapshotted and recovered.
Resolution	Protect the related entity in the same consistency group.

#### Remote Site Operation Mode ReadOnly [130092] [A1189]

Name	Remote Site Operation Mode ReadOnly
Description	Operation Mode of Remote Site changed to kReadOnly.

---

Alert message	Remote site <i>remote_name</i> moved to read-only state, outgoing replications to this remote will fail.
Cause	Probable SSD Failure on remote site in case of single node backup cluster.
Cause	Cloud virtual appliance ran out of memory in case of cloud connect.
Cause	Data stored on cloud appliance exceeded 20TB.
Impact	All outgoing replications to remote site will be aborted.
Resolution	Need to replace the failed SSD on remote site.
Resolution	Delete some remote snapshots to reduce memory or data usage in case of cloud connect and wait for some time.
Resolution	Please refer to Nutanix cloud connect documentation and increase the cloud CVM size if applicable.

---

#### **Failed to reconfigure Nutanix Guest Tools during VMs recovery for protection domain [130095] []**

---

Name	Failed To Recover NGT Information
Description	Failed to enable Nutanix Guest Tools during VMs recovery for protection domain.
Alert message	Failed to reconfigure Nutanix Guest Tools for VMs in protection domain <i>protection_domain_name</i> due to <i>reason</i> .
Cause	Nutanix Guest Tools service might be down.
Impact	VM
Resolution	Enable and mount Nutanix Guest Tools, and restart Nutanix Guest Agent service within the VM, for VMs in protection domain. If you cannot resolve the error, contact Nutanix support.

---

#### **Failed to reconfigure Nutanix Guest Tools for the recovered VM [130096] []**

---

Name	Failed To Recover NGT Information for VM
Description	Failed to reconfigure Nutanix Guest Tools for a VM in protection domain.
Alert message	Failed to reconfigure Nutanix Guest Tools for VM <i>vm_name</i> in protection domain <i>protection_domain_name</i> .
Cause	Virtual IP address of the cluster might not have been configured.
Cause	Error in generating certificate for VM.
Cause	Guest VM information could not be retrieved.
Impact	VM
Resolution	Configure the virtual IP address of the cluster (if not configured).
Resolution	Enable and Mount Nutanix Guest Tools on the failed VM, and restart the Nutanix Guest Agent service within the VM.
Resolution	Resolve the issue. If you cannot resolve the error, contact Nutanix support.

---

### Failed to reconfigure Nutanix Guest Tools for a VM in protection domain [130097] []

---

Name	Failed To Mount NGT ISO On Recovery of VM
Description	Failed to mount ISO image as part of Nutanix Guest Tools reconfiguration for a VM in protection domain
Alert message	Failed to reconfigure Nutanix Guest Tools for VM <i>vm_name</i> in protection domain <i>protection_domain_name</i> due to ISO mount failure.
Cause	Virtual IP address of the cluster might not have been configured.
Cause	Controller VM Nutanix Guest Tools version is lower than guest VM Nutanix Guest Tools version.
Cause	Guest VM information could not be retrieved.
Cause	NGT ISO could not be mounted.
Impact	VM
Resolution	Configure the virtual IP address of the cluster (if not configured).
Resolution	Mount Nutanix Guest Tools ISO on the failed VM, and restart Nutanix Guest Agent service within the VM.
Resolution	Resolve the issue. If you cannot resolve the error, contact Nutanix support.

---

### External iSCSI Attachments Not Snapshotted [130099] [A130099]

---

Name	External iSCSI Attachments Not Snapshotted
Description	External iSCSI Attachments Not Snapshotted.
Alert message	<i>error_message</i> . Volume Group external iSCSI attachments cannot be snapshotted for these VMs.
Cause	VMs have duplicate IQNs.
Cause	VMs have configured iSCSI target IP addresses that do not belong to the local Nutanix cluster.
Cause	IQN could not be resolved to VM ID.
Impact	Volume group external iSCSI attachments cannot be snapshotted and restored for these VMs.
Resolution	Make sure all VMs in the protection domain have different IQNs.
Resolution	Remove iSCSI target IP addresses that do not belong to the local Nutanix cluster from the VMs.
Resolution	Install Nutanix Guest Tools on all the VMs using volume group external iSCSI attachments.

---

### Volume Group Attachments Not Restored [130101] [A130101]

---

Name	Volume Group Attachments Not Restored
Description	Volume Group Attachments Not Restored.
Alert message	<i>error_message</i> for the protection domain ' <i>protection_domain_name</i> '.

---

---

Cause	Acropolis failed to attach volume groups to the VMs.
Impact	VMs will not be able to access volume group iSCSI disks.
Resolution	Manually attach volume groups to the VMs.

---

#### **Self service restore operation failed [130102] [A130102]**

---

Name	Self service restore operation Failed
Description	Self service restore operation failed
Alert message	Unable to ' <i>operation</i> ' disk from ' <i>vm_name</i> ' and internal ID ' <i>vm_id</i> ' due to ' <i>reason</i> '.
Cause	Snapshot disk could not be recovered.
Cause	Recovered disk could not be attached to the VM.
Cause	Self-service restore disk could not be detached from VM.
Impact	In the case of attachment failure, the user will not be able to restore files from snapshot.
Impact	In the case of detachment failure, the guest VM will have an extraneous disk attached.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

#### **Cloud remote site failed to start. [130108] [A130108]**

---

Name	Cloud Remote Site failed to start
Description	Cloud remote site failed to start.
Alert message	Cloud remote site ' <i>remote_name</i> ' failed to start due to reason ' <i>reason</i> '.
Cause	Various
Impact	All operations to cloud remote site will fail.
Resolution	Contact Nutanix support.

---

#### **Operation forwarded to cloud remote failed. [130109] [A130109]**

---

Name	Cloud Remote Operation Failure
Description	Cloud Remote Operation Failure.
Alert message	<i>failure_message</i> on cloud remote site ' <i>remote_name</i> ' due to reason ' <i>reason</i> '
Cause	Cloud remote site could not be reached
Impact	Operations forwarded to the cloud remote site will fail.
Resolution	Contact Nutanix support.

---

#### **Witness is not configured [130114] []**

---

Name	Witness Not Configured
Description	Witness is not configured
Alert message	Failed to <i>operation</i> for the protection domain ' <i>protection_domain_name</i> ' to the remote site ' <i>remote_name</i> '. Reason: Witness is not configured
Cause	Witness is not configured
Impact	Metro availability operation failed
Resolution	Configure Witness

---

#### **Witness is not reachable [130115] []**

---

Name	Witness Not Reachable
Description	Witness is not reachable
Alert message	Failed to <i>operation</i> for the protection domain ' <i>protection_domain_name</i> ' to the remote site ' <i>remote_name</i> '. Reason: Witness is not reachable or the Witness credentials are incorrect
Cause	Witness or the network is down
Cause	Witness credentials are incorrect
Impact	Metro availability failures will not be automatically handled
Resolution	Check if Witness is up on the network
Resolution	Check Witness credentials

---

#### **Metro Availability Is Promoted [130116] []**

---

Name	Automatic Promote Metro Availability
Description	Metro availability is promoted.
Alert message	Metro availability for the protection domain ' <i>protection_domain_name</i> ' to the remote site ' <i>remote_name</i> ' is promoted on standby cluster because of ' <i>reason</i> '.
Cause	Remote site unreachable.
Impact	Metro availability is promoted on standby cluster.
Resolution	Check if cluster service is healthy at remote cluster.

---

#### **Failed to update Metro Availability failure handling [130117] []**

---

Name	Updating Metro Failure Handling Failed
Description	Error in updating failure-handling on Metro Availability protection domain.
Alert message	Error in updating Metro Availability failure handling for the protection domain ' <i>protection_domain_name</i> ' to the remote site ' <i>remote_name</i> '. Reason: ' <i>reason</i> '.

---

---

Cause	Various
Impact	Metro Availability failure-handling could not be updated.
Resolution	Contact Nutanix support if this issue persists.

---

#### Failed to update Metro Availability failure handling on the remote site [130118] []

---

Name	Updating Metro Failure Handling Remote Failed
Description	Error in updating failure handling on the remote Metro Availability protection domain
Alert message	Error in updating Metro Availability failure handling on the remote site ' <i>remote_name</i> ' for the protection domain ' <i>protection_domain_name</i> '. Reason: ' <i>reason</i> '.
Cause	Various
Impact	Failure handling on this Metro Availability protection domain might be affected
Resolution	Perform a local-only update of failure handling on the remote site by using ncli

---

#### Authentication failed in Witness [130123] []

---

Name	Authentication Failed in Witness
Description	Authentication failed in Witness
Alert message	Failed to <i>operation</i> for the protection domain ' <i>protection_domain_name</i> ' to the remote site ' <i>remote_name</i> '. Reason: Authentication failure in Witness
Cause	Witness configured with incorrect credentials
Impact	Metro availability failures will not be automatically handled
Resolution	Configure Witness with correct credentials

---

#### Metro Availability Is Promoted [130125] []

---

Name	Manual Promote Metro Availability
Description	Metro availability is promoted.
Alert message	Metro availability for the protection domain ' <i>protection_domain_name</i> ' to the remote site ' <i>remote_name</i> ' is promoted on standby node.
Cause	An administrator promoted metro availability.
Impact	Metro availability is promoted on standby node.
Resolution	Reenable to get the benefit of Metro protection domain.

---

#### Metro Availability Is Disabled [130126] []

---

Name	Manual Break Metro Availability
------	---------------------------------

---

Description	Metro availability is disabled.
Alert message	Metro availability for the protection domain ' <i>protection_domain_name</i> ' to the remote site ' <i>remote_name</i> ' is disabled.
Cause	An administrator disabled metro availability.
Impact	Metro availability operation is disabled.
Resolution	Reenable to get the benefit of Metro protection domain.

---

**VMs in the standby site of a Metro Availability protection domain are running at suboptimal performance. [130129] []**

Name	Metro Protection domain VMs running at Sub-optimal performance
Description	VMs in the standby site of a Metro Availability protection domain are running at suboptimal performance.
Alert message	<i>num_of_vms</i> VMs on the remote site ' <i>remote_name</i> ' of protection domain ' <i>protection_domain_name</i> ' will be at sub-optimal performance.
Cause	VMs are hosted at the standby site of the Metro Availability protection domain.
Impact	Experience of decreased performance
Resolution	Host the VMs at the active site of the Metro Availability protection domain.

---

**Protection domain contains more than specified VMs [130130] []**

Name	Protection Domain VM Count Check
Description	Protection domain contains multiple VMs.
Alert message	It is not recommended to protect more than 1 VM in a protection domain <i>protection_domain_name</i> if you are replicating to the backup only remote site <i>remote_name</i> .
Cause	Replicating a protection domain with multiple VMs to a backup only remote site.
Impact	Selective retrieval of any 1 VM will take longer time as we need to retrieve the whole snapshot packed all VMs in the protection domain. replication schedules will be staggered due to large snapshot.
Resolution	Protect each VM in a separate protection domain.

---

**Snapshot contains entities from the storage container that have deduplication enabled. [130131] []**

Name	Replication Of Deduped Entity
Description	Snapshot contains entities from the storage container that have deduplication enabled.
Alert message	Do not replicate protection domain <i>protection_domain_name</i> comprising entities from the storage container that have deduplication enabled to a <i>remote_site_type</i> remote site <i>remote_name</i> .
Cause	Replicating a snapshot with entities from the storage container that have deduplication enabled to a single node backup or cloud remote site.

---

Impact	Performance of replications and retrievals will be affected.
Resolution	Either disable dedup on the Storage Containers, or use a multi-node NOS cluster as a replication target.

---

#### vStore is being replicated to backup only remote site. [130134] []

Name	Vstore Replication To Backup Only Remote
Description	vStore is being replicated to backup only remote site.
Alert message	vStore protection domain <i>protection_domain_name</i> is being replicated to backup only remote site <i>remote_name</i> .
Cause	vStore is being replicated to backup only remote site.
Impact	Low RTO can be seen as selective retrieve of VMs is not supported and snapshot of whole protection domain, having all the VMs in it, has to be retrieved.
Resolution	One VM per protection domain is the recommended configuration to achieve higher RTO.

---

#### Replication of protection domain {protection\_domain\_name} has not progressed. [130137] []

Name	Protection Domain Replication Stuck
Description	Replication of protection domain has not progressed.
Alert message	Replication of protection domain <i>protection_domain_name</i> to remote site <i>remote_name</i> for the snapshot <i>snapshot_id</i> has not made any progress in last one hour.
Cause	Network outage with remote.
Cause	Remote cluster does not have enough free disk space available.
Impact	Snapshots of protection domain will not be available on the remote site.
Resolution	Check network connection with remote.
Resolution	Make sure that the remote cluster has enough disk space available.

---

#### Guest VM

##### VM IO Latency [2001]

Name	VM IO Latency
Description	Checks that the Average I/O Latency is below {avg_io_latency_threshold_ms}ms.
Cause	Average I/O Latency is above {avg_io_latency_threshold_ms}ms.
Impact	Application performance on the VM may be degraded.
Resolution	Add capacity to cluster.

---

#### **VM Swap Rate [3020]**

---

Name	VM Swap Rate
Description	Checks whether Swap rate for VM is below {vm_swap_threshold_mbps} Mb/sec.
Cause	Swap rate is high - possible thrashing.
Impact	VM performance is degraded.
Resolution	Increase memory, reduce memory intensive VMs or reduce the total number of VMs.

---

#### **VM Memory Usage High [3021]**

---

Name	VM Memory Usage High
Description	Checks memory usage is above {vm_avg_mem_util_threshold_pct}
Cause	Memory usage is above {vm_avg_mem_util_threshold_pct}
Impact	Application performance on the VM may be degraded.
Resolution	Check network configuration/connections.

---

#### **Datastore VM Count High [3030] [A1170]**

---

Name	Datastore VM Count Check
Description	Checks for high VM count on datastores
Alert message	The number of VMs on Datastore: <i>datastore</i> is <i>vm_count</i>
Cause	High number of VMs on at least one datastore
Impact	HA service might be affected as VMware HA protects only 2048 VMs per datastore.
Resolution	Move some VMs to another datastore

---

#### **VM CPU Utilization [3040]**

---

Name	VM CPU Utilization
Description	Checks CPU usage is above {vm_peak_cpu_util_threshold_pct}
Cause	CPU utilization above {vm_peak_cpu_util_threshold_pct}.
Impact	Application performance on the VM may be degraded.
Resolution	Reduce CPU intensive processes.

---

#### **VM Transmit Packet Drop Check [3060]**

---

Name	VM Transmit Packet Drop Check
Description	Checks transmitted packet drop rate is above {vm_tx_drop_threshold}
Cause	Transmitted packet drop rate above {vm_tx_drop_threshold}

---

---

Impact	Application performance on the VM may be degraded.
Resolution	Check network configuration/connections.

---

#### VM Receive Packet Drop Check [3061]

---

Name	VM Receive Packet Drop Check
Description	Checks received packet drop rate is above {vm_rcv_drop_threshold}
Cause	Received packet drop rate above {vm_rcv_drop_threshold}
Impact	Application performance on the VM may be degraded.
Resolution	Check network configuration/connections.

---

#### VM has non-ASCII name. [106472] []

---

Name	Non-ASCII VM Names
Description	Check if any VMs have non-ASCII names.
Alert message	VM <i>vm_name</i> has non-ASCII name, which may cause snapshotting problems.
Cause	Some VMs have non-ASCII names.
Impact	Snapshot operations may fail.
Resolution	Update the VM names to consist only of ASCII characters.

---

#### Node Failure [130030] [A1137]

---

Name	Node Status
Description	Node Failure
Alert message	Host <i>hypervisor_address</i> appears to have failed. High Availability is restarting VMs on <i>failover_host_info</i> .
Cause	Host is not accessible.
Impact	VMs will restart on another host.
Resolution	Check for network connectivity or a hardware failure.

---

#### Protected VM Not Found [130038] [A1010]

---

Name	Protected VM Not Found
Description	Protected VM not Found
Alert message	Unable to locate VM with name ' <i>vm_name</i> ' and internal ID ' <i>vm_id</i> ' protected by protection domain ' <i>protection_domain_name</i> '.
Cause	The protected VM cannot be found and may have been deleted.
Impact	Any data associated with the VM may not be backed up or replicated to a remote site.

---

---

Resolution	Remove the VM from the protection domain.
------------	-------------------------------------------

---

**VM Action Error [130057] [A1033]**

---

Name	VM Action Status
Description	VM Action Error
Alert message	Failed to <i>action</i> VM with name ' <i>vm_name</i> ' and internal ID ' <i>vm_id</i> ' due to <i>reason</i> .
Cause	A VM could not be restored because of a hypervisor error, or could not be deleted because it is still in use.
Impact	The requested VM action (restore or delete) could not be completed.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

**Failure To Restart VMs For HA Event [130064] [A1145]**

---

Name	VMs Restart Status
Description	Failure to restart VMs for HA event
Alert message	Failed to restart one or more VMs that were running on failed host <i>hypervisor_address</i> .
Cause	Not enough memory or CPU resources within the cluster.
Impact	Some VMs will remain powered off.
Resolution	Shut down unneeded VMs to free cluster resources; expand the cluster to add resources; or wait until the failed host recovers. Once resources are available, power on the VMs.

---

**HA Host Evacuation Failure [130065] [A1146]**

---

Name	Host Evacuation Status
Description	Failure to evacuate host while entering maintenance mode or reserving host for HA.
Alert message	Failed to evacuate some VMs from host <i>hypervisor_address</i> while <i>reason</i> .
Cause	Not enough memory/CPU resources within the cluster.
Impact	The host will not enter requested state.
Resolution	Shut down unneeded VMs to free cluster resources or expand the cluster to add resources.

---

**HA Healing Failure [130067] [A1155]**

---

Name	VM HA Healing Status
Description	HA healing failure

---

---

Alert message	Could not restore VM High Availability.
Cause	Not enough memory/CPU resources within the cluster.
Impact	VMs are no longer protected against host failure.
Resolution	Shut down unneeded VMs to free cluster resources or expand the cluster to add resources.

---

#### Vm High Availability Failure [130068] [A130068]

---

Name	VM HA Status
Description	High Availability Failure
Alert message	VMs are no longer protected against host failure. Reason: <i>reason</i>
Cause	Not enough memory/CPU resources within the cluster.
Impact	VMs are no longer protected against host failure.
Resolution	Shut down unneeded VMs to free cluster resources or expand the cluster to add resources.

---

#### iSCSI Configuration Failed [130100] [A130100]

---

Name	iSCSI Configuration Failed
Description	iSCSI Configuration Failed
Alert message	Failed to re-configure iSCSI settings on the recovered VM ' <i>vm_name</i> '. <i>reason</i> .
Cause	Nutanix Guest Tools failed to execute some iSCSI commands on the guest VM.
Impact	iSCSI disks may become unavailable on the guest VM.
Resolution	If IQN and iSCSI target IP addresses of the VM have been updated by Nutanix Guest Agent, Discover and connect to new targets after rebooting the VM.
Resolution	Manually configure iSCSI settings on the guest VM.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

#### Nutanix Guest Tools mount failed. [130103] [A130103]

---

Name	NGT Mount Failure
Description	Nutanix Guest Tools mount failed.
Alert message	Nutanix Guest Tools mount failed. <i>reason</i> .
Cause	Failed to attach ISO image to the VM, please check the logs for exact cause of failure.
Impact	Nutanix Guest Tools is not mounted on VM.
Resolution	Check the logs for error information or contact Nutanix support.

---

---

**NGT version of the VM is incompatible with the NGT version of the cluster. [130104] [A130104]**

---

Name	NGT Version Incompatible
Description	NGT version of the VM is incompatible with the NGT version of the cluster.
Alert message	<i>message.</i>
Cause	VM is restored from the snapshot.
Impact	Nutanix Guest Tools features will not work.
Resolution	Uninstall NGT, Mount the NGT ISO, and then re-install NGT on the VM.

---

**VSS Snapshot is not supported for the VM. [130105] [A130105]**

---

Name	VSS Snapshot Not Supported
Description	VSS snapshot is not supported for the VM.
Alert message	VSS snapshot is not supported for the VM ' <i>vm_name</i> ', because <i>reason</i> .
Cause	VM has unsupported configuration.
Impact	Hypervisor based application consistent snapshot is taken on ESX. Crash consistent snapshot is taken for other hypervisors.
Resolution	Please look at the alert message and fix the invalid configuration.

---

**VSS Snapshot Aborted. [130106] [A130106]**

---

Name	VSS Snapshot Aborted
Description	VSS snapshot is aborted by the Guest VM.
Alert message	VSS snapshot is aborted for the VM ' <i>vm_name</i> ', because <i>reason</i> .
Cause	Guest VM aborted VSS snapshot operation.
Impact	Crash consistent snapshot is taken.
Resolution	Please look at the alert message and fix the issue.

---

**Recovered VM Disk Configuration Update Failed [130107] [A130107]**

---

Name	Disk Configuration Update Failed
Description	Disk Configuration Update Failed
Alert message	Failed to make some disks online on the recovered VM ' <i>vm_name</i> '. <i>reason</i> .
Cause	Nutanix Guest Tools failed to automatically bring the disks online.
Impact	Disks may become offline on the recovered VM.
Resolution	Manually bring the disks online on the recovered VM.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

#### **Execution of the PostThaw Script Failed [130113] [A130113]**

---

Name	PostThaw Script Execution Failed
Description	Execution of the PostThaw Script Failed
Alert message	Failed to execute the post_thaw script during the creation of the application consistent snapshot with uuid ' <i>snapshot_uuid</i> ' for the VM ' <i>vm_name</i> '. Error : <i>error_message</i> .
Cause	Guest VM failed to execute the post_thaw script during the creation of the application consistent snapshot.
Impact	Some of the applications that got stopped by the pre_freeze script may not start after application consistent snapshot is created for the VM.
Resolution	Manually run the post_thaw script on the guest VM.
Resolution	Fix the cause of the script failure to avoid any further execution failures.
Resolution	Resolve the specified reason for the failure. If you still cannot resolve the error, contact the Nutanix support.

---

#### **Application-consistent snapshot not taken for the VM. [130127] [A130127]**

---

Name	Application Consistent Snapshot Skipped
Description	Application-consistent snapshot not taken for the VM.
Alert message	Application-consistent snapshot not taken for the VM ' <i>vm_name</i> ', because <i>reason</i> .
Cause	VMware tools is not installed on the VM.
Cause	VMware tools is not running inside the VM.
Impact	Crash consistent snapshot is taken for the VM.
Resolution	Install the VMware tools inside the VM (if not installed).
Resolution	Start the VMware tools inside the VM (if not running).
Resolution	Resolve the issue. If you cannot resolve the error, contact Nutanix support.

---

#### **VM Registration Warning [130132] [A130132]**

---

Name	VM Registration Warning
Description	VM Registration caused warning
Alert message	VM with name ' <i>vm_name</i> ' has been recovered successfully, however the following issue was observed - <i>reason</i>
Cause	Processor features may not be compatible
Impact	VM registered successfully during disaster recovery but with warnings.
Resolution	No action is necessary.

---

### Storage Device Health Bad [1005] [A1069]

---

Name	SmartCtl Health
Description	Smartctl health bad.
Alert message	Smartctl reports attribute <i>attribute</i> having value <i>value</i> for device <i>device</i> on CVM <i>service_vm_external_ip</i> .
Cause	Smartctl health bad.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Check or replace disk.

---

### Intel SSD Wear High [1007] [A1042]

---

Name	Intel PCIe SSD Wearout Status
Description	Check for wear out on Intel PCIe SSDs
Alert message	Intel 910 SSD device <i>device</i> on the Controller VM <i>ip_address</i> has worn out beyond <i>thresholdPB</i> of writes.
Cause	The drive is close to the maximum write endurance.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace the drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

### Intel SSD Temperature High [1008] [A1007]

---

Name	Intel PCIe SSD Temperature
Description	Check the temperature on Intel PCIe SSDs
Alert message	Intel 910 SSD device <i>device</i> temperature exceeded <i>temperatureC</i> on the Controller VM <i>ip_address</i> .
Cause	The device is overheating.
Impact	The device may fail or be permanently damaged.
Resolution	Ensure that the fans in the block are functioning properly and that the environment is cool enough.

---

### Fusion IO Wear High [1010] [A1014]

---

Name	Fusion IO Wear Status
Description	Checks whether fusion io drive has worn out beyond write limit
Alert message	Fusion-io drive has worn out beyond write limit in Controller VM <i>ip_address</i> .
Cause	The drives are approaching the maximum write endurance and are beginning to fail.

---

Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace the drives as soon as possible.

---

#### Fusion IO Wear High [1011] [A1026]

Name	Fusion IO Die Status
Description	Checks whether fusion-io drive die failure has occurred
Alert message	Fusion-io drive die failures have occurred in Controller VM <i>ip_address</i> .
Cause	The drive is failing.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace the drives as soon as possible.

---

#### Fusion IO Temperature High [1012] [A1047]

Name	Fusion IO Temperature
Description	Checks whether temperature exceeded on fusion-io drive
Alert message	Fusion-io drive device temperature exceeded <i>temperatureC</i> on Controller VM <i>ip_address</i>
Cause	The device is overheating.
Impact	The device may fail or be permanently damaged.
Resolution	Ensure that the fans in the block are functioning properly and that the environment is cool enough.

---

#### Fusion IO Reserve Low [1013] [A1039]

Name	Fusion IO Reserve Pct
Description	Checks whether fusion io reserves are down
Alert message	Fusion-io drive device reserves are down to <i>reserve%</i> on Controller VM <i>ip_address</i> .
Cause	The drive is beginning to fail.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Consider replacing the drive.

---

#### Fusion IO Disk Failed [1014] [A1126]

Name	Fusion IO Disk Status
------	-----------------------

---

---

Description	Checks whether fusion-io drive has failed
Alert message	Fusion-io drive <i>device</i> has FAILED on Controller VM <i>ip_address</i> .
Cause	The drive had failed.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace the drive as soon as possible.

---

#### SATA DOM has failed. [1025] [A1165]

---

Name	SATADOM Status
Description	Checks that host SATA DOM is functioning.
Alert message	SATA DOM on host <i>ip_address</i> has failed.
Cause	SATA DOM has lost power connection.
Cause	SATA DOM has failed.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Check the SATA DOM physical connection.
Resolution	Replace the SATA DOM as soon as possible. Refer to the Nutanix documentation for instructions.

---

#### SATA DOM not reachable. [1030] [A1177]

---

Name	SATADOM Connection Status
Description	Checks that host SATA DOM is reachable.
Alert message	SATA DOM on host <i>ip_address</i> cannot be reached.
Cause	SATA DOM has lost power connection.
Cause	SATA DOM is not installed.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Check if SATA DOM is installed.
Resolution	Check the SATA DOM physical connection.
Resolution	Replace the SATA DOM as soon as possible. Refer to the Nutanix documentation for instructions.

---

#### SATA DOM has worn out. [1031] [A1180]

---

Name	SATADOM Wearout Status
Description	Checks the wearout of SATA DOM via SMART data.

---

---

Alert message	SATA DOM on host <i>ip_address</i> has PE cycles above 4500 or PE cycles above 3000 and daily PE cycles above 15.
Cause	SATA DOM has been in use for a long time.
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace SATA DOM as soon as possible. Refer to the Nutanix documentation for instructions.

---

#### SATA DOM needs firmware version upgrade to S170119. [1033] [A1183]

---

Name	SATA DOM 3ME Date and Firmware Status
Description	Checks the firmware version of SATA DOM.
Alert message	SATA DOM on host <i>ip_address</i> has old firmware version: <i>alertView</i>
Cause	SATA DOM firmware version is not the latest version.
Impact	Impacted by Shift read retry issue. The problem can cause node to fail to boot.
Resolution	Update the firmware to the latest version.

---

#### SATA DOM has Guest VM. [1034] [A1184]

---

Name	SATA DOM Guest VM Check
Description	Checks that no guest VM is installed on SATA DOM.
Alert message	SATA DOM on host <i>ip_address</i> contains a guest VM, which will accelerate the degradation of the SATA DOM.
Cause	A guest VM is installed on SATA DOM.
Cause	A VM is incorrectly configured.
Impact	Degradation of the SATA DOM will be accelerated, leading to unavailability of the node.
Resolution	Remove guest VMs from SATA DOM.
Resolution	Reconfigure guest VMs on the host machine.

---

#### SATADOM-SL 3IE3 has high wear. [1035] [A1185]

---

Name	SATADOM-SL 3IE3 Wearout Status
Description	Checks the wearout of SATADOM-SL 3IE3 via SMART data.
Alert message	SATADOM-SL 3IE3 on host <i>ip_address</i> has device life smaller than 5%
Cause	SATADOM-SL 3IE3 Device Life too short (<5).
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.

---

---

Resolution	Replace SATADOM-SL 3IE3 as soon as possible. Refer to the Nutanix documentation for instructions.
------------	---------------------------------------------------------------------------------------------------

---

**{model} firmware version is not the latest firmware version. [1055] [A1192]**

---

Name	SATA DOM Firmware Status
Description	Checks the firmware version of SATA DOM.
Alert message	<i>model</i> on host <i>ip_address</i> has firmware version <i>fwv</i> , need to upgrade to firmware version <i>lfwv</i> .
Cause	SATA DOM firmware version is not the latest version.
Impact	The node may fail to start.
Resolution	Update the firmware to the latest version.

---

**Samsung PM1633 drive has worn out. [1056] [A1193]**

---

Name	Samsung PM1633 Wearout Status
Description	Checks the status of Samsung PM1633 drive via SMART data.
Alert message	Samsung PM1633 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Samsung PM1633 drive revision is wrong or Samsung PM1633 drive has been in use for a long time and close to the maximum write endurance.
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace Samsung PM1633 drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

**Toshiba PM3 drive has worn out. [1057] [A1194]**

---

Name	Toshiba PM3 Status
Description	Checks the status of Toshiba PM3 drive via SMART data.
Alert message	Toshiba PM3 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Toshiba PM3 drive revision is wrong or Toshiba PM3 drive has been in use for a long time and close to the maximum write endurance.
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace Toshiba PM3 drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

**NVMe Drive has errors. [1059] [A1196]**

---

Name	NVMe Status Check
Description	Check that host NVMe drive is functioning properly.
Alert message	NVMe Drive on host <i>ip_address</i> has errors: <i>alert_msg</i>
Cause	NVMe Drive is damaged or worn out.
Impact	Cluster performance may be degraded. The integrity of data from NVMe drive may be harmed.
Resolution	Replace the problematic NVMe drive as soon as possible.

---

**Toshiba PM4 drive has worn out. [1060] [A1197]**

---

Name	Toshiba PM4 Status
Description	Check the status of Toshiba PM4 drive.
Alert message	Toshiba PM4 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Toshiba PM4 drive revision is unsupported or Toshiba PM4 drive has been in use for a long time and close to the maximum write endurance.
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace Toshiba PM4 drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

**Hypervisor Boot Drive Wear High [1061] [A1198]**

---

Name	Hyve Boot Disk Status
Description	Check Hyve boot disk status
Alert message	Hypervisor boot drive on the Controller VM <i>ip_address</i> has problem: <i>alert_msg</i>
Cause	The drive is close to the maximum write endurance.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace the drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

**More than one type of Toshiba PM4 drives installed on the node. [1062] [A1199]**

---

Name	Toshiba PM4 Config
Description	Check the Configuration of Toshiba PM4 drives.
Alert message	Toshiba PM4 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>

---

---

Cause	More than one type of Toshiba PM4 drives are installed on the node.
Impact	Toshiba PM4 drives may not function properly.
Resolution	Keep only one type of Toshiba PM4 drives.

---

#### **Toshiba PM4 drives not compatible with NOS or Foundation version on the node. [1063] [A1200]**

---

Name	Toshiba PM4 Version Compatibility
Description	Check the compatibility of Toshiba PM4 drives with NOS and Foundation versions.
Alert message	Toshiba PM4 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Toshiba PM4 drives are not compatible with the current NOS or foundation version.
Impact	Toshiba PM4 drives may not function properly.
Resolution	Upgrade NOS or Foundation version.

---

#### **Firmware version of Toshiba PM4 drives is old. [1064] [A1201]**

---

Name	Toshiba PM4 FW Version
Description	Check the firmware of Toshiba PM4 drives.
Alert message	Toshiba PM4 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Firmware version of Toshiba PM4 drives is not the latest version.
Impact	Toshiba PM4 drives may not function properly.
Resolution	Upgrade Toshiba PM4 firmware version.

---

#### **Samsung PM1633 drives not compatible with NOS or Foundation version on the node. [1065] [A1202]**

---

Name	Samsung PM1633 Version Compatibility
Description	Check the compatibility of Samsung PM1633 drives with NOS and Foundation versions.
Alert message	Samsung PM1633 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Samsung PM1633 drives are not compatible with the current NOS or foundation version.
Impact	Samsung PM1633 drives may not function properly.
Resolution	Upgrade NOS or Foundation version.

---

#### **Firmware version of Samsung PM1633 drives is old. [1066] [A1203]**

---

Name	Samsung PM1633 FW Version
------	---------------------------

---

Description	Check the firmware of Samsung PM1633 drives.
Alert message	Samsung PM1633 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Firmware version of Samsung PM1633 drives is not the latest version.
Impact	Samsung PM1633 drives may not function properly.
Resolution	Upgrade Samsung PM1633 firmware version.

---

#### NIC Flaps [3066] [A1067]

Name	NIC Flapping Check
Description	Check that all nics have no flapping.
Alert message	NIC <i nic_name=""> in host <i host_ip=""> has flapped <i nic_flap_count=""> times in one hour.</i></i></i>
Cause	A physical networking component is failing.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Check all physical networking components (including switch,cables, and NIC) and replace the failed component.

---

#### NIC Error Rate High [6011] [A1065]

Name	NIC Error Rate Check
Description	Check that each NIC has fewer than {nic_error_threshold} errors during span of execution (3600 seconds)
Alert message	NIC <i nic_name=""> in host <i host_ip=""> has encountered many <i error_type="">.</i></i></i>
Cause	NIC error rate high.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Check NIC health.

---

#### SSD IO Latency [6515]

Name	SSD IO Latency
Description	Checks that the Average SSD I/O Latency is below {SSD_latency_threshold_ms}ms.
Cause	I/O load on the cluster is high.
Impact	High I/O latencies may be experienced by some workloads.
Resolution	Redistribute VMs to reduce load on the affected Controller VM.

---

### **Fan Speed Low [15006] [A1045]**

---

Name	Fan Speed Low Check
Description	Check that fan speed is not low
Alert message	<i>fan_id</i> has stopped or its speed is low on Controller VM <i>ip_address</i> .
Cause	A fan has failed.
Impact	The device may fail or be permanently damaged.
Resolution	Replace the fan as soon as possible. Refer to the Nutanix documentation for instructions.

---

### **Fan Speed High [15007] [A1020]**

---

Name	Fan Speed High Check
Description	Check that fan speed is not too high
Alert message	Speed of <i>fan_id</i> exceeded <i>fan_rpm</i> RPM on Controller VM <i>ip_address</i> .
Cause	The device is overheating to the point of imminent failure.
Impact	The device may fail or be permanently damaged.
Resolution	Ensure that the fans in the block are functioning properly and that the environment is cool enough.

---

### **RAM Fault [15008] [A1052]**

---

Name	Ram Fault Status
Description	Check if current available memory has gone below the installed size.
Alert message	DIMM fault detected on host <i>ip_address</i> . The node is running with <i>current_memory_gb</i> GB whereas <i>installed_memory_gb</i> GB was installed.
Cause	A DIMM has failed.
Impact	Memory capacity on the node is reduced.
Resolution	Replace the failed DIMM as soon as possible. Refer to the Nutanix documentation for instructions.

---

### **CPU Temperature High [15010] [A1049]**

---

Name	CPU Temperature
Description	Check that cpu temperature is not too high.
Alert message	Temperature of <i>cpu_id</i> exceeded <i>temperatureC</i> on Controller VM <i>ip_address</i>
Cause	The device is overheating to the point of imminent failure.

---

Resolution	Ensure that the fans in the block are functioning properly and that the environment is cool enough.
------------	-----------------------------------------------------------------------------------------------------

---

#### **RAM Temperature High [15011] [A1022]**

---

Name	DIMM Temperature
Description	Check that DIMM temperature is not high.
Alert message	Temperature of <i>dimm_id</i> exceeded <i>temperatureC</i> on Controller VM <i>ip_address</i>
Cause	DIMM temperature is high.
Impact	The device may fail or be permanently damaged.
Resolution	Check ram temperature.

---

#### **System Temperature High [15012] [A1012]**

---

Name	System Temperature
Description	Check that system temperature is not high
Alert message	System temperature exceeded <i>temperatureC</i> on Controller VM <i>ip_address</i>
Cause	The device is overheating to the point of imminent failure.
Impact	The device may fail or be permanently damaged.
Resolution	Ensure that the fans in the block are functioning properly and that the environment is cool enough.

---

#### **GPU Temperature High [15014] [A1070]**

---

Name	GPU Temperature
Description	Check that gpu temperature is not high
Alert message	Temperature of <i>gpu_id</i> exceeded <i>temperatureC</i> on host <i>ip_address</i>
Cause	The device is overheating to the point of imminent failure.
Impact	The device may fail or be permanently damaged.
Resolution	Ensure that the fans in the block are functioning properly and that the environment is cool enough.

---

#### **Hardware Clock Failure [15015] [A1059]**

---

Name	Hardware Clock Status
Description	Check if Hardware clock has failed
Alert message	Hardware clock in host <i>host_ip</i> has failed.
Cause	The RTC clock on the host has failed or the RTC battery has died.

---

---

Impact	The host may fail after restart and remain unavailable until it is replaced.
Resolution	Replace the node. Refer to the Nutanix documentation for instructions.

---

#### IPMI Error [15016] [A1050]

---

Name	IPMI SDR Status
Description	Checks whether IPMI SDR has failures.
Alert message	Controller VM <i>ip_address</i> is unable to fetch IPMI SDR repository.
Cause	The IPMI interface is down.
Cause	There is a network connectivity issue.
Cause	The hypervisor password does not match what is configured in the cluster.
Cause	The cluster did not correctly fail back after a Controller VM was temporarily down.
Impact	Nutanix support staff are able to access the cluster to assist with any issue.
Resolution	Ensure that the IPMI interface is functioning.
Resolution	Ensure that physical networking, VLANs, and virtual switches are configured correctly.
Resolution	Ensure that the hypervisor password configured in the cluster matches the actual hypervisor password.
Resolution	If the alert persists, contact Nutanix support.

---

#### GPU Fault [15017] [A1071]

---

Name	GPU Status
Description	Check that GPU have not faulted.
Alert message	<i>gpu_model</i> GPU fault detected on host <i>host_ip</i> . The node is running with <i>current_gpu_count</i> GPU(s) whereas <i>installed_gpu_count</i> GPU(s) were installed.
Cause	The device is failing.
Impact	Graphics acceleration is not available to guest VMs.
Resolution	Replace the device. Refer to the Nutanix documentation for instructions.

---

#### Power Supply Down [15018] [A1046]

---

Name	Power Supply Status
Description	Check that Power supply has no errors.
Alert message	<i>power_source</i> is down on block <i>block_position</i>
Cause	The power supply has failed.
Impact	The block does not have power supply redundancy. It will continue to function with one power supply.

---

---

Resolution	Replace the power supply as soon as possible. Refer to the Nutanix documentation for instructions.
------------	----------------------------------------------------------------------------------------------------

---

#### High number of correctable ECC errors in last 1 day. [15019] [A1187]

---

Name	Correctable ECC Errors One Day
Description	Check for number of correctable ECC errors for last one day in the IPMI system event log.
Alert message	Memory module <i>dimm_id</i> has <i>num_correctable_ecc_errors</i> correctable ECC errors (run time <i>run_time_num</i> , post time <i>post_time_num</i> ) in sel log on the host <i>host_ip</i> in last <i>num_days</i> days
Cause	A memory module in the node is failing.
Impact	The node may stop running, reducing cluster capacity.
Resolution	Replace the failing memory module as soon as possible. Refer to the Nutanix documentation for instructions.

---

#### High number of correctable ECC errors in last 10 days. [15020] [A1188]

---

Name	Correctable ECC Errors 10 Days
Description	Check for number of correctable ECC errors for last 10 days in the IPMI system event log.
Alert message	Memory module <i>dimm_id</i> has <i>num_correctable_ecc_errors</i> correctable ECC errors (run time <i>run_time_num</i> , post time <i>post_time_num</i> ) in sel log on the host <i>host_ip</i> in last <i>num_days</i> days
Cause	A memory module in the node is failing.
Impact	The node may stop running, reducing cluster capacity.
Resolution	Replace the failing memory module as soon as possible. Refer to the Nutanix documentation for instructions.

---

#### CPU Voltage Abnormal [15024] []

---

Name	CPU Voltage
Description	Check that CPU voltage is within normal range.
Alert message	Voltage of <i>cpu_id</i> not within normal range on Controller VM <i>ip_address</i>
Cause	Server board component problem may cause the CPU voltage to be too high or too low.
Impact	The device may fail or be permanently damaged.
Resolution	Replace the node. Refer to the Nutanix documentation for instructions.

---

#### **RAM Voltage Abnormal [15025] []**

---

Name	DIMM Voltage
Description	Check that DIMM voltage is within normal range.
Alert message	Voltage of <i>dimm_id</i> is not within normal range on Controller VM <i>ip_address</i>
Cause	Memory problem and server board problem may cause DIMM voltage to be too high or too low.
Impact	The device may fail or be permanently damaged.
Resolution	Replace the memory. If the problem persists, replace the node. Refer to the Nutanix documentation for instructions

---

#### **CPU-VRM Temperature High [15026] []**

---

Name	CPU-VRM Temperature
Description	Check that CPU-VRM temperature is not too high.
Alert message	Temperature of CPU-VRM <i>cpu_vrm_id</i> exceeded <i>temperatureC</i> on Controller VM <i>ip_address</i>
Cause	Server board component problem may cause the CPU-VRM to be overheating.
Impact	The device may fail or be permanently damaged.
Resolution	Replace the node. Refer to the Nutanix documentation for instructions.

---

#### **RAM-VRM Temperature High [15027] []**

---

Name	DIMM-VRM Temperature
Description	Check that DIMM-VRM temperature is not high.
Alert message	Temperature of DIMM-VRM <i>dimm_vrm_id</i> exceeded <i>temperatureC</i> on Controller VM <i>ip_address</i>
Cause	Server board component problem may cause DIMM-VRM temperature to be high.
Impact	The device may fail or be permanently damaged.
Resolution	Replace the node. Refer to the Nutanix documentation for instructions.

---

#### **CPU Temperature Reading Error [15028] []**

---

Name	CPU Temperature Fetch
Description	Check that CPU temperature can be fetched.
Alert message	Failed to fetch temperature of <i>cpu_id</i> on Controller VM <i>ip_address</i>
Cause	CPU temperature sensor may be unstable or BMC firmware may be reporting temperature inaccurately.
Impact	CPU temperature cannot be monitored.

---

Resolution	Check BMC SEL log. If CPU temperature in SEL log is 0, check CPU temperature sensor. If CPU temperature in SEL is not 0, ensure that the BMC firmware version is correct.
------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

#### **SM863 drive has worn out. [106017] [ ]**

---

Name	Samsung SM863 SSD status check
Description	Check the status of SM863 and SM863a SSD drive
Alert message	<code>dev_type</code> drive <code>dev_name</code> on host <code>ip_address</code> has the following problems: <code>err_msg</code>
Cause	SM863a SSD drive revision is unsupported or SM863 and SM863a has been in use for a long time and close to maximum write endurance.
Impact	Cluster performance may be significantly degraded or or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace SM863 or SM863a SSD drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

#### **SAS Connectivity Not Normal [106019] [ ]**

---

Name	SAS Connectivity
Description	Check SAS connectivity
Alert message	SAS cables missing or not properly connected on host.
Cause	SAS cables are not properly connected.
Impact	Cluster performance may be significantly degraded.
Resolution	Ensure that SAS cables are properly connected.

---

#### **Haswell and Broadwell CPUs are in the same chassis. [106026] [A1190]**

---

Name	CPU type on chassis check
Description	Checks whether CPUs within a chassis are of the same type.
Alert message	Chassis <code>chassis_id</code> has both Haswell & Broadwell CPUs and this may affect the performance and stability of the nodes in the chassis. Chassis cpu info: <code>chassis_cpu_info</code>
Cause	A node of a different type was added to the chassis.
Impact	Having nodes of different CPU types in the same chassis is not supported.
Resolution	Remove the node that has a different CPU type from the chassis. Before moving a node to a chassis, make sure its CPU type is the same as that of other nodes in the chassis.

---

**Micron5100 drive has worn out. [106029] []**

---

Name	Micron5100 SSD status check
Description	Check the status of Micron5100 SSD drive
Alert message	Micron5100 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Micron5100 SSD drive revision is unsupported or is close to maximum write endurance.
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace Micron5100 SSD drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

**SM863a drives not compatible with NOS or Foundation version on the node. [106030] []**

---

Name	Samsung SM863a version compatibility check
Description	Check the compatibility of SM863a drives with NOS and Foundation versions.
Alert message	<i>dev_type</i> drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	SM863a drives are not compatible with the current NOS or foundation version.
Impact	SM863a drives may not function properly.
Resolution	Upgrade NOS or Foundation version.

---

**Firmware version of SM863 drives is old. [106031] []**

---

Name	Samsung SM863/SM863a FW version check
Description	Check the firmware of SM863 or SM863a drives.
Alert message	<i>dev_type</i> drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Firmware version of SM863 drives is not the latest one.
Impact	SM863a drives may not function properly.
Resolution	Upgrade SM863 firmware version.

---

**Fewer than two non-Samsung PM863a drives installed on the node. [106032] []**

---

Name	Samsung PM863a config check
Description	Check the types of disk drives on a node that has PM863a drives installed.
Alert message	Host machine <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Fewer than two non-Samsung PM863a drives are installed on the node.
Impact	Invalid Samsung PM863a drive configuration.
Resolution	Install at least two non-Samsung PM863a drive.

---

**PM863a drives not compatible with AOS or Foundation version on the node. [106033] []**

---

Name	Samsung PM863a version compatibility check
Description	Check the compatibility of PM863a drives with AOS and Foundation versions.
Alert message	PM863a drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	PM863a drives are not compatible with the current AOS or foundation version.
Impact	Expand cluster and foundation workflows will not work.
Resolution	Upgrade AOS or Foundation version.

---

**Firmware version of PM863a drives is old. [106034] []**

---

Name	Samsung PM863a FW version check
Description	Check firmware of PM863a drives.
Alert message	PM863a drive <i>dev_name</i> of model <i>dev_model</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Firmware version of PM863a drives is not the latest one.
Impact	PM863a drives may not function properly.
Resolution	Upgrade PM863a firmware version.

---

**PM863a drive has worn out. [106035] []**

---

Name	Samsung PM863a status check
Description	Check the status of PM863a SSD
Alert message	PM863a drive <i>dev_name</i> of model <i>dev_model</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	PM863a is approaching maximum write endurance.
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace PM863a SSD as soon as possible. Refer to the Nutanix documentation for instructions.

---

**M10 GPU check [111040]**

---

Name	M10 GPU check
Description	Check number of M10 GPUs on a node
Cause	
Impact	
Resolution	Contact Nutanix support.

---

#### M60 GPU check [111041]

---

Name	M60 GPU check
Description	Check number of M60 GPUs on a node
Cause	
Impact	
Resolution	Contact Nutanix support.

---

#### Node Failure [130030] [A1137]

---

Name	Node Status
Description	Node Failure
Alert message	Host <i>hypervisor_address</i> appears to have failed. High Availability is restarting VMs on <i>failover_host_info</i> .
Cause	Host is not accessible.
Impact	VMs will restart on another host.
Resolution	Check for network connectivity or a hardware failure.

---

#### Non Self Encryption Drive Disk Inserted [130031] [A1122]

---

Name	Non SED Disk Inserted Check
Description	Non Self Encrypting Drive disk inserted
Alert message	Non encrypted disk with serial <i>disk_serial</i> was added in drive bay <i>disk_Location</i> on Controller VM <i>service_vm_external_ip</i> . It is not usable because the rest of the cluster is protected using encrypted drives.
Cause	A cluster with self-encrypting drives has a non-self encrypting drive installed.
Impact	The new disk was not mounted because the cluster cannot be fully secured without all drives supporting encryption.
Resolution	Ensure all installed drives are of self-encrypting type. If more help is needed call Nutanix support.

---

#### Disk Bad [130033] [A1044]

---

Name	Disk Offline Status
Description	Disk Bad
Alert message	Disk <i>disk_position</i> with id <i>disk_id</i> on node <i>node_position</i> of block <i>block_position</i> is marked offline due to IO errors. Serial number of the disk is <i>disk_serial</i> in host <i>host_ip</i> of block <i>block_serial</i> .
Cause	The drive has failed.
Impact	Cluster storage capacity is reduced.

---

---

Resolution	Replace the failed drive. Refer to the Nutanix documentation for instructions.
------------	--------------------------------------------------------------------------------

---

**Physical Disk Drive Has Failed [130035] [A1104]**

---

Name	Physical Disk Status
Description	Physical drive has failed.
Alert message	Drive <i>disk_id</i> with serial <i>disk_serial</i> in drive bay <i>disk_Location</i> on Controller VM <i>service_vm_external_ip</i> has failed.
Cause	The drive has failed.
Impact	Cluster storage capacity is reduced.
Resolution	Replace the failed drive. Refer to the Nutanix documentation for instructions.

---

**Physical Disk Removed From Slot [130036] [A1103]**

---

Name	Physical Disk Remove Check
Description	Physical disk removed from slot
Alert message	Disk with serial <i>disk_serial</i> was removed from drive bay <i>disk_Location</i> on Controller VM <i>service_vm_external_ip</i>
Cause	A drive was physically removed from a slot.
Impact	Migration of data from the disk will start.
Resolution	No action is necessary.

---

**Disk Diagnostic Failure [130089] [A1139]**

---

Name	Disk Diagnostic Status
Description	Drive diagnostic has failed.
Alert message	Drive <i>disk_id</i> with serial <i>disk_serial</i> in drive bay <i>disk_Location</i> on Controller VM <i>service_vm_external_ip</i> has failed diagnostic test.
Cause	The drive has failed.
Impact	Cluster storage capacity is reduced.
Resolution	Replace the drive. Refer to the Nutanix documentation for instructions.

---

## Network

**IPMI IP Not Reachable [3062] [A1041]**

---

Name	IPMI IP Pingable
Description	Check that all ipmi ips are pingable from local SVM.

---

---

Alert message	IPMI interface <i>target_ip</i> is not reachable from Controller VM <i>source_ip</i> in the last 6 attempts.
Cause	The IPMI interface is down or there is a network connectivity issue.
Impact	The host is unreachable through the IPMI interface.
Resolution	Ensure that the IPMI interface is functioning and that physical networking, VLANs, and virtual switches are configured correctly.

---

#### **CVM Connectivity Failure [3064] [A1001]**

---

Name	CVM Passwordless Connectivity
Description	Check that SVM has passwordless connection to each other.
Alert message	Controller VM <i>target_ip</i> is not reachable from Controller VM <i>source_ip</i> in the last 3 attempts.
Cause	SVM has no passwordless connection to each other
Impact	Cluster compute and storage capacity are reduced. Until data stored on this host is replicated to other hosts in the cluster, the cluster has one less copy of guest VM data.
Resolution	Check SVM network configuration

---

#### **Host IP Not Reachable [3065] [A1006]**

---

Name	Host IP Pingable
Description	Check that all host ips are pingable from local SVM.
Alert message	Hypervisor <i>target_ip</i> is not reachable from Controller VM <i>source_ip</i> in the last 6 attempts.
Cause	The hypervisor host is down or there is a network connectivity issue.
Impact	Cluster compute and storage capacity are reduced. Until data stored on this host is replicated to other hosts in the cluster, the cluster has one less copy of guest VM data.
Resolution	Ensure that the hypervisor host is running and that physical networking, VLANs, and virtual switches are configured correctly.

---

#### **NIC Link Down [3067] [A1082]**

---

Name	NIC Link Status
Description	Checks whether any nic is down.
Alert message	Link on NIC <i>nic_name</i> of host <i>host_ip</i> is down. NIC description: <i>nic_description</i>
Cause	The NIC is disconnected from the switch, or the switch port is failing.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Ensure that the NIC is connected to the switch and that the switch port is functioning properly.

---

### Inter CVM Latency [6005]

---

Name	Inter CVM Latency
Description	Check that other CVMs are pingable in less than {ping_time_threshold_ms} milliseconds.
Cause	At least one other CVM has high ping latency higher than {ping_time_threshold_ms} milliseconds.
Impact	If problem persists I/O performance will be degraded.
Resolution	Check network connectivity/configuration.

---

### CVM NIC Speed Low [6008] [A1058]

---

Name	TenGig Adaptor Status
Description	Checks whether CVM is uplinked to 10 GbE NIC.
Alert message	Controller VM <i>service_vm_external_ip</i> is running on the network interface(s) <i>nic_list</i> , which is/are slower than 10 Gbps. This will degrade the system performance.
Cause	CVM not uplinked to 10 GbE NIC.
Cause	1 GbE NIC is part of the bond.
Cause	ESX hypervisor may be lockdown.
Impact	The Controller VM is not configured to use the 10 GbE NIC or is configured to share load with a slower NIC.
Resolution	Check network configuration.
Resolution	Check if ESX hypervisor is lockdown, and unlock it if it is lockdown.

---

### CVM Host Subnet Mismatch [6202] [A1048]

---

Name	CVM Subnet
Description	Checks that host and cvm share the same subnet.
Alert message	Controller VM <i>svm_ip</i> with network address <i>svm_subnet</i> is in a different network than the Hypervisor <i>hypervisor_ip</i> , which is in the network <i>hypervisor_subnet</i> .
Cause	The Controller VM and the hypervisor are not on the same subnet.
Impact	Controller VM high availability will not apply in the case of Controller VM failure, leading to guest VM unavailability.
Resolution	Reconfigure the cluster. Either move the Controller VMs to the same subnet as the hypervisor hosts or move the hypervisor hosts to the same subnet as the Controller VMs.

---

### Transmit Packet Drop Check [6404]

---

Name	Transmit Packet Drop Check
------	----------------------------

---

Description	Checks that the host transmitted packets drop rate is below {host_tx_drop_threshold}.
Cause	Transmitted packet drop rate is above {host_tx_drop_threshold}.
Impact	Cluster performance may be degraded.
Resolution	Check network hardware/configuration.

---

#### **Receive Packet Drop Check [6405]**

Name	Receive Packet Drop Check
Description	Checks that the high received packets drop rate is below {host_rcv_drop_threshold}.
Cause	Received packet drop rate is above {host_rcv_drop_threshold}.
Impact	Cluster performance may be degraded.
Resolution	Check network hardware/configuration.

---

#### **Unable to connect to vCenter. [6449] []**

Name	vCenter Connection Check
Description	Check if vCenter connection is established.
Alert message	vCenter connection is not established.
Cause	vCenter server is unreachable on port 80.
Impact	Certain VM operations might fail.
Resolution	Confirm that vCenter server is reachable on port 80.

---

#### **Key Management Server Unavailable [110213] [A1099]**

Name	Key Management Server Availability
Description	Check Key Management Server is available.
Alert message	Cannot connect to key management server <code>key_management_server_name</code> from Controller VM <code>service_vm_external_ip</code> .
Cause	The node cannot connect to a key management server either because of hardware failures, certificate validation failure, or network issues.
Impact	Secure clusters may not be able to unlock their drives on boot or change passwords.
Resolution	Ensure the key management server and nodes in a cluster have network connectivity to each other and all certificates are valid.

---

#### **Mellanox NIC Speed is not 10GbE and 40 GbE or both 10GbE and 40GbE NICs are installed on one node [111047] []**

Name	Mellanox NIC Status check
------	---------------------------

---

---

Description	Checks if Mellanox NICs are down or if any Mellanox NIC has speed other than 10GbE or 40GbE. Checks if both 10GbE and 40GbE Mellanox NICs are installed on one node.
Alert message	Mellanox NIC on host <i>host_ip</i> has problem: <i>alert_msg</i>
Cause	The NIC is disconnected from the switch, or the switch port is not functioning correctly, or both 10GbE and 40GbE Mellanox NICs are installed on one node.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Ensure that the NIC is connected to the switch and that the switch port is functioning properly. Ensure that only 10GbE or 40GbE Mellanox NIC is installed on one node.

---

## Node

### SATA DOM has failed. [1025] [A1165]

---

Name	SATADOM Status
Description	Checks that host SATA DOM is functioning.
Alert message	SATA DOM on host <i>ip_address</i> has failed.
Cause	SATA DOM has lost power connection.
Cause	SATA DOM has failed.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Check the SATA DOM physical connection.
Resolution	Replace the SATA DOM as soon as possible. Refer to the Nutanix documentation for instructions.

---

### SATA DOM not reachable. [1030] [A1177]

---

Name	SATADOM Connection Status
Description	Checks that host SATA DOM is reachable.
Alert message	SATA DOM on host <i>ip_address</i> cannot be reached.
Cause	SATA DOM has lost power connection.
Cause	SATA DOM is not installed.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Check if SATA DOM is installed.
Resolution	Check the SATA DOM physical connection.
Resolution	Replace the SATA DOM as soon as possible. Refer to the Nutanix documentation for instructions.

---

**SATA DOM has worn out. [1031] [A1180]**

---

Name	SATADOM Wearout Status
Description	Checks the wearout of SATA DOM via SMART data.
Alert message	SATA DOM on host <i>ip_address</i> has PE cycles above 4500 or PE cycles above 3000 and daily PE cycles above 15.
Cause	SATA DOM has been in use for a long time.
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace SATA DOM as soon as possible. Refer to the Nutanix documentation for instructions.

---

**SATA DOM needs firmware version upgrade to S170119. [1033] [A1183]**

---

Name	SATA DOM 3ME Date and Firmware Status
Description	Checks the firmware version of SATA DOM.
Alert message	SATA DOM on host <i>ip_address</i> has old firmware version: <i>alert_msg</i>
Cause	SATA DOM firmware version is not the latest version.
Impact	Impacted by Shift read retry issue. The problem can cause node to fail to boot.
Resolution	Update the firmware to the latest version.

---

**SATA DOM has Guest VM. [1034] [A1184]**

---

Name	SATA DOM Guest VM Check
Description	Checks that no guest VM is installed on SATA DOM.
Alert message	SATA DOM on host <i>ip_address</i> contains a guest VM, which will accelerate the degradation of the SATA DOM.
Cause	A guest VM is installed on SATA DOM.
Cause	A VM is incorrectly configured.
Impact	Degradation of the SATA DOM will be accelerated, leading to unavailability of the node.
Resolution	Remove guest VMs from SATA DOM.
Resolution	Reconfigure guest VMs on the host machine.

---

**SATADOM-SL 3IE3 has high wear. [1035] [A1185]**

---

Name	SATADOM-SL 3IE3 Wearout Status
Description	Checks the wearout of SATADOM-SL 3IE3 via SMART data.
Alert message	SATADOM-SL 3IE3 on host <i>ip_address</i> has device life smaller than 5%
Cause	SATADOM-SL 3IE3 Device Life too short (<5).

---

---

Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace SATADOM-SL 3IE3 as soon as possible. Refer to the Nutanix documentation for instructions.

---

**{model} firmware version is not the latest firmware version. [1055] [A1192]**

---

Name	SATA DOM Firmware Status
Description	Checks the firmware version of SATA DOM.
Alert message	<i>model</i> on host <i>ip_address</i> has firmware version <i>fwv</i> , need to upgrade to firmware version <i>lfwv</i> .
Cause	SATA DOM firmware version is not the latest version.
Impact	The node may fail to start.
Resolution	Update the firmware to the latest version.

---

**Samsung PM1633 drive has worn out. [1056] [A1193]**

---

Name	Samsung PM1633 Wearout Status
Description	Checks the status of Samsung PM1633 drive via SMART data.
Alert message	Samsung PM1633 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Samsung PM1633 drive revision is wrong or Samsung PM1633 drive has been in use for a long time and close to the maximum write endurance.
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace Samsung PM1633 drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

**Toshiba PM3 drive has worn out. [1057] [A1194]**

---

Name	Toshiba PM3 Status
Description	Checks the status of Toshiba PM3 drive via SMART data.
Alert message	Toshiba PM3 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Toshiba PM3 drive revision is wrong or Toshiba PM3 drive has been in use for a long time and close to the maximum write endurance.
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.

---

---

Resolution	Replace Toshiba PM3 drive as soon as possible. Refer to the Nutanix documentation for instructions.
------------	-----------------------------------------------------------------------------------------------------

---

#### NVMe Drive has errors. [1059] [A1196]

---

Name	NVMe Status Check
Description	Check that host NVMe drive is functioning properly.
Alert message	NVMe Drive on host <i>ip_address</i> has errors: <i>alert_msg</i>
Cause	NVMe Drive is damaged or worn out.
Impact	Cluster performance may be degraded. The integrity of data from NVMe drive may be harmed.
Resolution	Replace the problematic NVMe drive as soon as possible.

---

#### Toshiba PM4 drive has worn out. [1060] [A1197]

---

Name	Toshiba PM4 Status
Description	Check the status of Toshiba PM4 drive.
Alert message	Toshiba PM4 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Toshiba PM4 drive revision is unsupported or Toshiba PM4 drive has been in use for a long time and close to the maximum write endurance.
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace Toshiba PM4 drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

#### More than one type of Toshiba PM4 drives installed on the node. [1062] [A1199]

---

Name	Toshiba PM4 Config
Description	Check the Configuration of Toshiba PM4 drives.
Alert message	Toshiba PM4 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	More than one type of Toshiba PM4 drives are installed on the node.
Impact	Toshiba PM4 drives may not function properly.
Resolution	Keep only one type of Toshiba PM4 drives.

---

#### Toshiba PM4 drives not compatible with NOS or Foundation version on the node. [1063] [A1200]

---

Name	Toshiba PM4 Version Compatibility
------	-----------------------------------

---

---

Description	Check the compatibility of Toshiba PM4 drives with NOS and Foundation versions.
Alert message	Toshiba PM4 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Toshiba PM4 drives are not compatible with the current NOS or foundation version.
Impact	Toshiba PM4 drives may not function properly.
Resolution	Upgrade NOS or Foundation version.

---

#### **Firmware version of Toshiba PM4 drives is old. [1064] [A1201]**

---

Name	Toshiba PM4 FW Version
Description	Check the firmware of Toshiba PM4 drives.
Alert message	Toshiba PM4 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Firmware version of Toshiba PM4 drives is not the latest version.
Impact	Toshiba PM4 drives may not function properly.
Resolution	Upgrade Toshiba PM4 firmware version.

---

#### **Samsung PM1633 drives not compatible with NOS or Foundation version on the node. [1065] [A1202]**

---

Name	Samsung PM1633 Version Compatibility
Description	Check the compatibility of Samsung PM1633 drives with NOS and Foundation versions.
Alert message	Samsung PM1633 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Samsung PM1633 drives are not compatible with the current NOS or foundation version.
Impact	Samsung PM1633 drives may not function properly.
Resolution	Upgrade NOS or Foundation version.

---

#### **Firmware version of Samsung PM1633 drives is old. [1066] [A1203]**

---

Name	Samsung PM1633 FW Version
Description	Check the firmware of Samsung PM1633 drives.
Alert message	Samsung PM1633 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Firmware version of Samsung PM1633 drives is not the latest version.
Impact	Samsung PM1633 drives may not function properly.
Resolution	Upgrade Samsung PM1633 firmware version.

---

### **Wsmans Connectivity lost [6210] [A1186]**

---

Name	WSMan Connectivity Check
Description	Checks if CVM can connect to the host using WSMAN.
Alert message	Wsmans Remote Shell Connectivity lost between CVM and the host.
Cause	Password is not updated in the cluster configuration.
Impact	The CVM cannot connect to the host to manage it.
Resolution	Update the correct password in the cluster configuration.

---

### **CVM memory reservation is incorrectly configured. [6211] []**

---

Name	CVM Memory Pinned Check
Description	Verify CVM memory reservation and pinning.
Alert message	CVM memory reservation is incorrectly configured on CVM with IP <i>service_vm_external_ip</i>
Cause	CVM memory reservation is configured incorrectly.
Impact	This can potentially result in cluster instability.
Resolution	Please contact Nutanix Support to verify memory resolution.

---

### **Host CPU Utilization [6409]**

---

Name	Host CPU Utilization
Description	Checks cpu contention at the host level is below {host_avg_cpu_util_threshold_pct}.
Cause	High CPU utilization.
Impact	I/O performance may be degraded.
Resolution	Reduce CPU intensive VMs or reduce the total number of VMs.

---

### **Host Swap Rate [6413]**

---

Name	Host Swap Rate
Description	Checks whether Swap rate at the host level is below {host_swap_threshold_mbps} Mb/sec.
Cause	Swap rate is high - possible thrashing.
Impact	VM performance is degraded.
Resolution	Increase memory, reduce memory intensive VMs or reduce the total number of VMs.

---

### **VM migration compromised [6447] []**

---

Name	EVC Configuration Check
------	-------------------------

---

Description	Checks whether VMWare EVC configuration can cause VM migration problems
Alert message	VM migration might be compromised due to VMware EVC configuration
Cause	Not all hosts have the same EVC baseline applied
Cause	EVC mode not enabled on all hosts
Cause	Host CPUs in the cluster belong to multiple processor families, and EVC mode is disabled
Impact	vMotion may not be possible from a host with newer generation CPUs to a host with older generation CPUs
Resolution	Apply the same EVC baseline on all hosts
Resolution	Enable EVC mode on all hosts
Resolution	Enable EVC mode

---

#### **Metadata disk(s) not mounted on CVM [101055] []**

Name	Metadata Disk Mounted Check
Description	Check that all metadata disks are mounted.
Alert message	Metadata disk(s) on Controller VM <i>svm_ip_address</i> are not mounted: <i>unmounted_disks</i>
Cause	Metadata disk(s) not mounted on CVM.
Impact	Cluster performance may be significantly degraded. If this condition continues, there is a potential for data corruption and/or loss.
Resolution	Contact Nutanix Support to mount the metadata disk.

---

#### **SM863 drive has worn out. [106017] []**

Name	Samsung SM863 SSD status check
Description	Check the status of SM863 and SM863a SSD drive
Alert message	<i>dev_type</i> drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	SM863a SSD drive revision is unsupported or SM863 and SM863a has been in use for a long time and close to maximum write endurance.
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace SM863 or SM863a SSD drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

#### **Haswell and Broadwell CPUs are in the same chassis. [106026] [A1190]**

Name	CPU type on chassis check
Description	Checks whether CPUs within a chassis are of the same type.

---

Alert message	Chassis <i>chassis_id</i> has both Haswell & Broadwell CPUs and this may affect the performance and stability of the nodes in the chassis. Chassis cpu info: <i>chassis_cpu_info</i>
Cause	A node of a different type was added to the chassis.
Impact	Having nodes of different CPU types in the same chassis is not supported.
Resolution	Remove the node that has a different CPU type from the chassis. Before moving a node to a chassis, make sure its CPU type is the same as that of other nodes in the chassis.

---

#### **Micron5100 drive has worn out. [106029] []**

Name	Micron5100 SSD status check
Description	Check the status of Micron5100 SSD drive
Alert message	Micron5100 drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Micron5100 SSD drive revision is unsupported or is close to maximum write endurance.
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace Micron5100 SSD drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

#### **SM863a drives not compatible with NOS or Foundation version on the node. [106030] []**

Name	Samsung SM863a version compatibility check
Description	Check the compatibility of SM863a drives with NOS and Foundation versions.
Alert message	<i>dev_type</i> drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	SM863a drives are not compatible with the current NOS or foundation version.
Impact	SM863a drives may not function properly.
Resolution	Upgrade NOS or Foundation version.

---

#### **Firmware version of SM863 drives is old. [106031] []**

Name	Samsung SM863/SM863a FW version check
Description	Check the firmware of SM863 or SM863a drives.
Alert message	<i>dev_type</i> drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Firmware version of SM863 drives is not the latest one.
Impact	SM863a drives may not function properly.
Resolution	Upgrade SM863 firmware version.

---

**Fewer than two non-Samsung PM863a drives installed on the node. [106032] []**

---

Name	Samsung PM863a config check
Description	Check the types of disk drives on a node that has PM863a drives installed.
Alert message	Host machine <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Fewer than two non-Samsung PM863a drives are installed on the node.
Impact	Invalid Samsung PM863a drive configuration.
Resolution	Install at least two non-Samsung PM863a drive.

---

**PM863a drives not compatible with AOS or Foundation version on the node. [106033] []**

---

Name	Samsung PM863a version compatibility check
Description	Check the compatibility of PM863a drives with AOS and Foundation versions.
Alert message	PM863a drive <i>dev_name</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	PM863a drives are not compatible with the current AOS or foundation version.
Impact	Expand cluster and foundation workflows will not work.
Resolution	Upgrade AOS or Foundation version.

---

**Firmware version of PM863a drives is old. [106034] []**

---

Name	Samsung PM863a FW version check
Description	Check firmware of PM863a drives.
Alert message	PM863a drive <i>dev_name</i> of model <i>dev_model</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	Firmware version of PM863a drives is not the latest one.
Impact	PM863a drives may not function properly.
Resolution	Upgrade PM863a firmware version.

---

**PM863a drive has worn out. [106035] []**

---

Name	Samsung PM863a status check
Description	Check the status of PM863a SSD
Alert message	PM863a drive <i>dev_name</i> of model <i>dev_model</i> on host <i>ip_address</i> has the following problems: <i>err_msg</i>
Cause	PM863a is approaching maximum write endurance.
Impact	Cluster performance may be significantly degraded or the cluster may become unusable. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.

---

Resolution	Replace PM863a SSD as soon as possible. Refer to the Nutanix documentation for instructions.
------------	----------------------------------------------------------------------------------------------

---

#### **BMC BIOS version check [111039]**

---

Name	BMC BIOS version check
Description	Check BMC/Bios version of all nodes
Cause	
Impact	
Resolution	Contact Nutanix support.

---

#### **Mellanox NIC Driver version check [111045]**

---

Name	Mellanox NIC Driver version check
Description	Check if Mellanox port NIC driver version is above min recommended version
Cause	
Impact	
Resolution	Contact Nutanix support.

---

#### **Storage Container running out of storage capacity (low runway). [120116] [A120116]**

---

Name	storage_container_usage_running_out_alert_insights
Description	Predict high storage space usage on Storage Container.
Alert message	Storage Container <i>container_name</i> on cluster <i>cluster_name</i> will run out of storage resource in approximately <i>data_int</i> days.
Cause	Storage Container storage is running out.
Impact	The Storage Container will run out of storage space and may be unable to service I/O requests.
Resolution	Add more nodes to the cluster to increase cluster storage capacity, remove storage intensive VMs, or reduce the total number of VMs on the cluster.

---

#### **Node running out of CPU capacity (low runway). [120241] []**

---

Name	node_cpu_running_out_alert_insights
Description	Predict high CPU resource usage.
Alert message	Node <i>node_name</i> on cluster <i>cluster_name</i> is running out of CPU resource in approximately <i>data_int</i> days.
Cause	Node CPU running out.
Impact	Application performance on node may be degraded.

---

---

Resolution	Reduce CPU intensive VMs on node or reduce the total number of VMs on the node.
------------	---------------------------------------------------------------------------------

---

**Node running out of Memory capacity (low runway). [120242] []**

---

Name	node_memory_running_out_alert_insights
Description	Predict high memory resource usage.
Alert message	Node <i>node_name</i> on cluster <i>cluster_name</i> is running out of Memory resource in approximately <i>data_int</i> days.
Cause	Node memory is overutilized.
Impact	Application performance on node may be degraded.
Resolution	Add more memory to the node if applicable, remove memory-intensive VMs, or reduce the total number of VMs on the node.

---

**Certificate Creation Error [130013] [A1112]**

---

Name	Certificate Creation Status
Description	Certificate signing request creation failure
Alert message	Failed to create a certificate signing request on node <i>service_vm_external_ip</i> in the cluster.
Cause	Either the OpenSSL library had a failure or a non-supported subject field, subject value, or subject alternative name was provided.
Impact	Without a CSR then data at rest encryption cannot be enabled.
Resolution	Ensure that the certificate signing request fields are valid and retry the command, or contact Nutanix support if the OpenSSL configuration file is missing or corrupted.

---

**Agent VM Restoration Failure [130091] []**

---

Name	Agent VM Restoration
Description	Failure to Restore Agent VM
Alert message	Failed to restore agent VM with UUID <i>vm_uuid</i> .
Cause	Not enough memory/CPU resources on this node.
Impact	VMs on this host may not function correctly because of the missing agent VM.
Resolution	Shut down unneeded VMs to free cluster resources or expand the cluster to add resources.

---

**VM group Snapshot and Current Mismatch [130110] [A130110]**

---

Name	VM group Snapshot and Current Mismatch
Description	Check that snapshot to restore matches current VM group

---

---

Alert message	VM group <i>vm_group_uuid</i> Snapshot and Current Mismatch: <i>message</i>
Cause	VM group changed after snapshot was created.
Impact	VMs might be scheduled to run on same host instead of different host.
Resolution	Recreate VM snapshot to ensure up-to-date VM group information.

---

#### Metro takeover - old primary site is hosting VM(s) [130111] []

---

Name	Metro Old Primary Site Hosting VMs
Description	Metro takeover - old primary site is hosting VMs
Alert message	old primary site ' <i>remote_name</i> ' for protection domain ' <i>protection_domain_name</i> ' is hosting VM(s) while secondary is taking over.
Cause	The old primary site is hosting VMs while the secondary is taking over the metro protection domain.
Impact	VM performance might be degraded.
Resolution	Unregister the VMs hosted on the old primary and register them on the secondary site.

---

#### Protection domain is in decoupled state [130112] []

---

Name	Protection Domain Decoupled Status
Description	Protection domain is in decoupled state
Alert message	Protection domain ' <i>protection_domain_name</i> ' protecting Storage Container ' <i>container_name</i> ' is in decoupled state
Cause	Standby site has been promoted to primary
Impact	Metro availability for the protection domain on the primary is unavailable
Resolution	Reenable metro availability from the remote site

---

#### Other

#### Orphan VM Snapshot Check [3200]

---

Name	Orphan VM Snapshot Check
Description	Checks for VM snapshots whose associated VMs are removed.
Cause	The VM associated with a snapshot has been removed.
Impact	Cluster storage resources are consumed by unneeded data.
Resolution	Delete the snapshots based on the VM that has been removed.

---

#### **Network adapter setting check [103068]**

---

Name	Network adapter setting check
Description	Check Network adapter setting
Cause	Network adapter is not set to not connect on power on
Impact	CVM may not boot up after the host reboot.
Resolution	Check if "ethernet0.startConnected = "true"" is present in the CVM's .vmx file.

---

#### **PYNFS dependency check [106431]**

---

Name	PYNFS dependency check
Description	Check PYNFS dependency
Cause	PYNFS is in use and is not present.
Impact	CVM may not boot up after the host reboot.
Resolution	Validate PYNFS configuration.

---

#### **localcli check [106432]**

---

Name	localcli check
Description	Check that esxcli command not used in rc local script
Cause	esxcli command is used in rc local script.
Impact	CVM may not boot up after the host reboot.
Resolution	Check if 'esxcli' is used instead of 'localcli' in /etc/rc.local.d/local.sh.

---

#### **vim command check [106433]**

---

Name	vim command check
Description	Check that vim-cmd vmsvc/power.on command is present in local script
Cause	vim-cmd vmsvc/power.on\ command not present in local script.
Impact	CVM may not boot up after the host reboot.
Resolution	Check if 'vim-cmd vmsvc/power.on' entry is present in 'local.sh'.

---

#### **Autobackup check [106436]**

---

Name	Autobackup check
Description	Check that /sbin/auto-backup.sh has run successfully
Cause	/sbin/auto-backup.sh has not run successfully.
Impact	CVM may not boot up after the host reboot.

---

---

Resolution	Make sure '/bootbank/state.tgz' has a newer timestamp.
------------	--------------------------------------------------------

---

**EOF check [106437]**

---

Name	EOF check
Description	Check that there is no line "EOF" at end of rc local script
Cause	"EOF" statement at end of rc local.
Impact	CVM may not boot up after the host reboot.
Resolution	Check that 'local.sh' does not have 'EOF'

---

**RC local script exit statement present [106438]**

---

Name	RC local script exit statement present
Description	Check that top level exit statement is not present in RC local script
Cause	Top level exit statement present in script rc local preventing script lines from being run.
Impact	CVM may not boot up after the host reboot.
Resolution	Check if 'local.sh' has an 'exit' statement. Generate INFO if the exit statement is NOT within the if..fi statement

---

**.dvsData directory in local datastore [106439]**

---

Name	.dvsData directory in local datastore
Description	Check that .dvsData directory is present on pynfs mounted local datastore
Cause	.dvsData directory is not persistent yet.
Impact	CVM may not boot up after the host reboot.
Resolution	Check if .dvsData directory exists in the local datastore.

---

**NGT CA Setup Check [111046]**

---

Name	NGT CA Setup Check
Description	Checks that the NGT CA setup is same on all nodes.
Cause	/home/ngt/ca.tar does not have the same checksum on all CVMs.
Impact	NGT operations may not function properly.
Resolution	Contact Nutanix support.

---

**RPO script validation on storage heavy cluster [111048]**

---

Name	RPO script validation on storage heavy cluster
------	------------------------------------------------

---

---

Description	Check that RPO validation script is installed and running on storage heavy cluster.
Cause	RPO validation scripts are not installed.
Impact	RPO may not met.
Resolution	Install RPO validation script on storage heavy cluster.
Resolution	Contact Nutanix support.

---

#### Metro Availability Prechecks Failed [130124] []

---

Name	Metro Availability Prechecks Failed
Description	Metro availability prechecks failed
Alert message	Prechecks for <i>operation</i> failed for the protection domain ' <i>protection_domain_name</i> ' to the remote site ' <i>remote_name</i> '. Reason: ' <i>reason</i> '.
Cause	Various
Impact	Metro availability operation could not be started.
Resolution	Contact Nutanix support if this condition persists

---

#### Recovery Point Objective Cannot Be Met [130138] []

---

Name	Recovery Point Objective Cannot Be Met
Description	Recovery Point Objective Cannot Be Met
Alert message	Recovery point objective cannot be met because ' <i>reason</i> '
Cause	Various
Impact	Recovery plan could be affected.
Resolution	Contact Nutanix support if this condition persists

---

## Storage

#### Data Disk Space Usage High [1003] [A1005]

---

Name	Data Disk Usage
Description	Check that current amount of disk usage is above {disk_usage_threshold_pct}.
Alert message	Disk space usage for <i>mount_path</i> on <i>entity ip_address</i> is <i>disk_usage%</i> which exceeds the threshold of <i>disk_usage_threshold%</i> . <i>action_str</i>
Cause	Disk usage exceeds threshold {disk_usage_threshold_pct}.
Impact	Cluster performance may be significantly degraded. In the case of multiple disks reaching 95% usage, the cluster may become unable to service I/O requests.
Resolution	Reduce disk usage or replace disk.

---

### Disk Inode Usage High [1004] [A1027]

---

Name	Inode Usage
Description	Check that current inode usage is above {inode_usage_threshold_pct}.
Alert message	Inode usage for one or more disks on Controller VM <i>svm_ip_address</i> has exceeded <i>inode_usage_threshold%</i> .
Cause	Inode usage exceeds threshold {inode_usage_threshold_pct}.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Reduce disk usage or replace disk.

---

### Storage Device Health Bad [1005] [A1069]

---

Name	SmartCtl Health
Description	Smartctl health bad.
Alert message	Smartctl reports attribute <i>attribute</i> having value <i>value</i> for device <i>device</i> on CVM service <i>vm_external_ip</i> .
Cause	Smartctl health bad.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Check or replace disk.

---

### Intel SSD Wear High [1007] [A1042]

---

Name	Intel PCIe SSD Wearout Status
Description	Check for wear out on Intel PCIe SSDs
Alert message	Intel 910 SSD device <i>device</i> on the Controller VM <i>ip_address</i> has worn out beyond <i>thresholdPB</i> of writes.
Cause	The drive is close to the maximum write endurance.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace the drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

### Intel SSD Temperature High [1008] [A1007]

---

Name	Intel PCIe SSD Temperature
Description	Check the temperature on Intel PCIe SSDs
Alert message	Intel 910 SSD device <i>device</i> temperature exceeded <i>temperatureC</i> on the Controller VM <i>ip_address</i> .

---

---

Cause	The device is overheating.
Impact	The device may fail or be permanently damaged.
Resolution	Ensure that the fans in the block are functioning properly and that the environment is cool enough.

---

#### Disk Unused [1009] [A1063]

---

Name	Disk Configuration
Description	Check that if some disk is not part of any storage pool
Alert message	Device with disk id <i>disk_id</i> on Controller VM <i>service_vm_external_ip</i> is not part of any storage pool.
Cause	The cluster was not configured correctly during installation or drive replacement was not completed correctly.
Impact	The cluster was not configured correctly during installation or drive replacement was not completed correctly
Resolution	Add the unused disk to a storage pool.

---

#### Fusion IO Wear High [1010] [A1014]

---

Name	Fusion IO Wear Status
Description	Checks whether fusion io drive has worn out beyond write limit
Alert message	Fusion-io drive has worn out beyond write limit in Controller VM <i>ip_address</i> .
Cause	The drives are approaching the maximum write endurance and are beginning to fail.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace the drives as soon as possible.

---

#### Fusion IO Wear High [1011] [A1026]

---

Name	Fusion IO Die Status
Description	Checks whether fusion-io drive die failure has occurred
Alert message	Fusion-io drive die failures have occurred in Controller VM <i>ip_address</i> .
Cause	The drive is failing.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace the drives as soon as possible.

---

### Fusion IO Temperature High [1012] [A1047]

---

Name	Fusion IO Temperature
Description	Checks whether temperature exceeded on fusion-io drive
Alert message	Fusion-io drive <i>device</i> temperature exceeded <i>temperatureC</i> on Controller VM <i>ip_address</i>
Cause	The device is overheating.
Impact	The device may fail or be permanently damaged.
Resolution	Ensure that the fans in the block are functioning properly and that the environment is cool enough.

---

### Fusion IO Reserve Low [1013] [A1039]

---

Name	Fusion IO Reserve Pct
Description	Checks whether fusion io reserves are down
Alert message	Fusion-io drive <i>device</i> reserves are down to <i>reserve%</i> on Controller VM <i>ip_address</i> .
Cause	The drive is beginning to fail.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Consider replacing the drive.

---

### Fusion IO Disk Failed [1014] [A1126]

---

Name	Fusion IO Disk Status
Description	Checks whether fusion-io drive has failed
Alert message	Fusion-io drive <i>device</i> has FAILED on Controller VM <i>ip_address</i> .
Cause	The drive had failed.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace the drive as soon as possible.

---

### Hypervisor Disk Space Usage High [1015] [A1161]

---

Name	Host Disk Usage
Description	Checks that host disk usage is not high.
Alert message	Disk space usage for <i>mount_path</i> on <i>entity</i> on host <i>ip_address</i> has exceeded <i>threshold%</i> .
Cause	Too much data is stored on the node.

---

Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Delete unneeded data or add nodes to the cluster.

---

#### **Storage Pool Space Usage Exceeded [1016] [A1128]**

Name	StoragePool Space Usage
Description	Check high space usage on storagepools
Alert message	Storage Pool space usage for <i>storage_pool_name</i> is at <i>usage_pct</i> . <i>alert_msg</i>
Cause	Excessive space usage in the storage pool.
Impact	Storage pool will run out of space, and the cluster may become unable to service I/O requests.
Resolution	Add more storage or delete some data to free storage space.

---

#### **Storage Container Space Usage Exceeded: NCC Check [1017] [A1130]**

Name	Storage Container Space Usage
Description	Check high space usage on Storage Containers
Alert message	Storage Container space usage for <i>container_name</i> is at <i>usage_pct</i> .
Cause	Excessive space usage in the Storage Container.
Impact	Storage Container will run out of space, and the cluster may become unable to service I/O requests.
Resolution	Delete some data to free storage space from the Storage Container.

---

#### **System Partitions Space Usage High [1021] [A1031]**

Name	System Partition Usage
Description	Check that current amount of disk usage is above {home_nutanix_usage_threshold_pct}.
Alert message	Disk space usage for <i>mount_path</i> on entity <i>ip_address</i> has exceeded <i>threshold</i> %.
Cause	Disk usage exceeds threshold {home_nutanix_usage_threshold_pct}.
Impact	The space reservations on the cluster can no longer be met. Writes by guest VMs may fail if expected storage space is not available.
Resolution	Reduce disk usage or replace disk.

---

#### **Flash Mode Configuration has exceeded the threshold limit [1022] [A1158]**

Name	Flash Mode Configuration
------	--------------------------

---

Description	Check the total configured size of flash-mode-enabled vDisks with respect to the threshold limit.
Alert message	Flash-mode-enabled vDisks are configured to use more flash tier space than the allotted limit.
Cause	Flash-mode-enabled vDisks are configured to use more flash tier space than the allotted limit.
Impact	Flash mode policies may not be enforced properly.
Resolution	Reduce the number of flash-mode-enabled vDisks or increase the capacity of the flash tier.

---

#### **Flash Mode Usage Limit Exceeded [1023] [A1159]**

Name	Flash Mode Usage
Description	Check the amount of usage by flash-mode-enabled vDisks with respect to the threshold limit.
Alert message	Flash Mode usage has exceeded the threshold limit.
Cause	Flash-mode-enabled vDisks are using more flash tier space than the allotted limit.
Impact	System may down-migrate flash mode data.
Resolution	Reduce the number of flash-mode-enabled vDisks or increase the capacity of the flash tier.

---

#### **Flash-mode-enabled VM Power Status [1024] [A1160]**

Name	Flash Mode Enabled VM Power Status
Description	Check if any flash-mode-enabled VMs are Powered Off.
Alert message	One or more Powered Off flash-mode-enabled VMs detected.
Cause	One or more flash-mode-enabled VMs are Powered Off.
Impact	Flash tier space might be getting wasted.
Resolution	Disable Flash Mode on the Powered Off VMs, or power them on.

---

#### **High Garbage due to erasure coding [1026] [A1174]**

Name	Erasure Code Garbage
Description	Checks if erasure coding garbage is below a safe threshold.
Alert message	Garbage due to erasure coding on <i>container_name</i> is currently <i>usage</i> which is above the safety threshold.
Cause	Suboptimal performance of erasure coding is generating garbage that is consuming additional storage space.
Impact	Erasure coding on Nutanix clusters may experience suboptimal storage savings.

---

---

Resolution	Review KB 2912 for corrective actions. Contact Nutanix support to discuss possible fixes before enabling or disabling erasure coding.
------------	---------------------------------------------------------------------------------------------------------------------------------------

---

#### **Erasure coding on Acropolis base software versions less than 4.5.2 may perform suboptimally. [1027] [A1175]**

---

Name	Erasure Code Configuration
Description	Checks erasure coding is enabled on cluster with version < 4.5.2
Alert message	Erasure Coding is enabled on Nutanix clusters with Acropolis base software version less than 4.5.2.
Cause	Erasure coding was enabled on the cluster
Impact	Erasure coding on Nutanix clusters with version < 4.5.2 may experience suboptimal storage savings.
Resolution	Upgrade to Acropolis base software 4.5.2 or higher. See KB 2912 for details.

---

#### **Invalid erasure code delay parameter. [1028] [A1176]**

---

Name	Erasure-Code-Delay Configuration
Description	Validate the EC param value for erasure-code-delay
Alert message	The erasure coding parameter erasure-code-delay for Storage Container <i>container_name msg</i>
Cause	Invalid setting for erasure-code-delay
Impact	Current Erasure coding parameter value can lead to poor performance and suboptimal storage savings.
Resolution	Please fix the erasure-code-delay value. See KB 2912 for details.

---

#### **Storage Pool Flash Mode Configuration [1029] [A1173]**

---

Name	Storage Pool Flash Mode Configuration
Description	Flash Mode is not supported when multiple storage pools are in use.
Alert message	Flash Mode configuration with Multiple Storage Pools detected.
Cause	Multiple Storage Pools and Flash Mode are in use together.
Impact	This configuration is not supported.
Resolution	Disable Flash Mode for all VMs and Volume Groups, or consolidate all Storage Pools into one.

---

#### **Hypervisor Boot Drive Wear High [1061] [A1198]**

---

Name	Hyve Boot Disk Status
Description	Check Hyve boot disk status

---

Alert message	Hypervisor boot drive on the Controller VM <i>ip_address</i> has problem: <i>alert_msg</i>
Cause	The drive is close to the maximum write endurance.
Impact	Cluster performance may be significantly degraded. In the case of multiple nodes with the same condition, the cluster may become unable to service I/O requests.
Resolution	Replace the drive as soon as possible. Refer to the Nutanix documentation for instructions.

---

#### **Erasure coding pending check [101054]**

Name	Erasure coding pending check
Description	Check if EC undo is pending on any of the Storage Containers
Cause	
Impact	
Resolution	Contact Nutanix Support

---

#### **SAS Connectivity Not Normal [106019] []**

Name	SAS Connectivity
Description	Check SAS connectivity
Alert message	SAS cables missing or not properly connected on host.
Cause	SAS cables are not properly connected.
Impact	Cluster performance may be significantly degraded.
Resolution	Ensure that SAS cables are properly connected.

---

#### **Storage Container Replication Factor Low [110210] [A1074]**

Name	Storage Container RF Status
Description	Check that the Storage Container region replication factor is not low
Alert message	Replication factor of <i>container_region</i> on Storage Container <i>container_name</i> is set to 1.
Cause	Replication factor on the Storage Container was changed to 1.
Impact	Only one copy of guest VM data exists on the cluster. If any node fails, the data stored on that node is unavailable. If any drive fails, the data stored on that drive is unrecoverable.
Resolution	Change the replication factor on the Storage Container with the nCLI command "container edit name='ctr_name' rf='2'" (or higher if appropriate for your environment).

---

### Compression Disabled [130014] [A1121]

Name	Compression Status
Description	Compression is Disabled.
Alert message	Disabling compression for future writes. Calculated metadata usage of <i>metadata_usage</i> bytes exceeds safety limit of <i>metadata_limit</i> bytes on Controller VM <i>service_vm_id</i> . The metadata disk size is <i>metadata_disk_size</i> .
Cause	Compression metadata usage has exceeded the safety limits. Compression metadata usage can increase due to variety of reasons such as having too many snapshots simply because too much of data is stored.
Impact	Advantages of compression are not available.
Resolution	Once the metadata size is brought under the safety limit (for example, by removing unneeded snapshots, or by expanding the cluster size), contact Nutanix support to manually enable compression.

### Fingerprinting Disabled [130021] [A1068]

Name	Finger Printing Status
Description	Fingerprinting Disabled
Alert message	Disabling fingerprinting (deduplication) for future writes. Calculated metadata usage of <i>metadata_usage</i> bytes exceeds safety limit of <i>metadata_limit</i> bytes on Controller VM <i>service_vm_id</i> . The metadata disk size is <i>metadata_disk_size</i> .
Cause	The metadata disk is used for metadata and data. Once the metadata portion on the disk exceeds the safety threshold we disable fingerprinting (deduplication) of future writes. Metadata sizes can increase due to a variety of reasons such as having too many snapshots, or simply because too much data is fingerprinted.
Impact	The advantages of deduplication are not available.
Resolution	Once the metadata size is brought under the safety limit (for example, by removing unneeded snapshots, or by expanding the cluster size), contact Nutanix support to manually enable fingerprinting.

### Metadata Usage High [130025] [A1101]

Name	Metadata Usage
Description	Metadata Usage High.
Alert message	Metadata usage on Controller VM <i>service_vm_external_ip</i> has exceeded <i>critical_pct</i> .
Cause	The cluster either has too many snapshots or too much data is being fingerprinted.
Impact	Cluster performance may be significantly degraded.
Resolution	Reduce metadata size by removing unneeded snapshots, creating snapshots less frequently, creating snapshots of fewer VMs, or expanding the cluster size.

#### Non Self Encryption Drive Disk Inserted [130031] [A1122]

---

Name	Non SED Disk Inserted Check
Description	Non Self Encrypting Drive disk inserted
Alert message	Non encrypted disk with serial <i>disk_serial</i> was added in drive bay <i>disk_Location</i> on Controller VM <i>service_vm_external_ip</i> . It is not usable because the rest of the cluster is protected using encrypted drives.
Cause	A cluster with self-encrypting drives has a non-self encrypting drive installed.
Impact	The new disk was not mounted because the cluster cannot be fully secured without all drives supporting encryption.
Resolution	Ensure all installed drives are of self-encrypting type. If more help is needed call Nutanix support.

---

#### On-Disk Dedup Disabled [130032] [A1089]

---

Name	On-Disk Dedup Status
Description	On-Disk Dedup Disabled
Alert message	Disabling further on-disk deduplication (fingerprinting). Controller VM with <i>ram_sizeGB</i> RAM and <i>ssd_sizeGB</i> SSD does not meet the minimum requirements of <i>required_ram_sizeGB</i> RAM and <i>required_ssd_sizeGB</i> SSD to support on-disk deduplication feature.
Cause	To support on-disk deduplication (fingerprinting) feature, the Controller VM must meet the minimum requirements for RAM and SSD. When this safety threshold is not satisfied, on-disk deduplication is disabled.
Impact	The advantages of on-disk deduplication are not available.
Resolution	Once the Controller VMs are upgraded to meet the minimum requirements on RAM and SSD, on-disk deduplication can be enabled. Contact Nutanix support for assistance.

---

#### Disk Bad [130033] [A1044]

---

Name	Disk Offline Status
Description	Disk Bad
Alert message	Disk <i>disk_position</i> with id <i>disk_id</i> on node <i>node_position</i> of block <i>block_position</i> is marked offline due to IO errors. Serial number of the disk is <i>disk_serial</i> in host <i>host_ip</i> of block <i>block_serial</i> .
Cause	The drive has failed.
Impact	Cluster storage capacity is reduced.
Resolution	Replace the failed drive. Refer to the Nutanix documentation for instructions.

---

#### Physical Disk Drive Has Failed [130035] [A1104]

---

Name	Physical Disk Status
------	----------------------

---

Description	Physical drive has failed.
Alert message	Drive <i>disk_id</i> with serial <i>disk_serial</i> in drive bay <i>disk_Location</i> on Controller VM <i>service_vm_external_ip</i> has failed.
Cause	The drive has failed.
Impact	Cluster storage capacity is reduced.
Resolution	Replace the failed drive. Refer to the Nutanix documentation for instructions.

---

#### **Physical Disk Removed From Slot [130036] [A1103]**

Name	Physical Disk Remove Check
Description	Physical disk removed from slot
Alert message	Disk with serial <i>disk_serial</i> was removed from drive bay <i>disk_Location</i> on Controller VM <i>service_vm_external_ip</i>
Cause	A drive was physically removed from a slot.
Impact	Migration of data from the disk will start.
Resolution	No action is necessary.

---

#### **Space Reservation Violated [130053] [A1021]**

Name	Space Reservation Status
Description	Space Reservation Violated
Alert message	Space reservation configured on vdisk <i>vdisk_name</i> belonging to Storage Container id <i>container_id</i> could not be honored due to insufficient disk space resulting from a possible disk or node failure.
Cause	A drive or a node has failed.
Impact	The space reservations on the cluster can no longer be met. Writes by guest VMs may fail if expected storage space is not available.
Resolution	Change space reservations to total less than 90% of the available storage, and replace the drive or node as soon as possible. Refer to the Nutanix documentation for instructions.

---

#### **vDisk Block Map Usage High Critical [130056] [A1061]**

Name	vDisk Block Map Usage
Description	vDisk Block Map Usage High Critical.
Alert message	Too many snapshots have been allocated in the system. This may cause perceivable performance degradation.
Cause	Too many vdisks or snapshots are present in the system.
Impact	Cluster performance may be significantly degraded.

---

---

Resolution	Remove unneeded snapshots and vdisks. If using remote replication, try to lower the frequency of taking snapshots. If you cannot resolve the error, contact Nutanix support.
------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

#### **Protected Volume Group not Found [130070] [A1162]**

---

Name	Protected Volume Group Not Found
Description	Protected Volume Group not Found
Alert message	Unable to locate volume group with name ' <i>vg_name</i> ' and internal ID ' <i>vg_uuid</i> ' protected by protection domain ' <i>protection_domain_name</i> '.
Cause	The protected volume group cannot be found and may have been deleted.
Impact	Any data associated with the volume group may not be backed up or replicated to a remote site.
Resolution	Remove the volume group from the protection domain.

---

#### **Volume Group Action Error [130071] [A1163]**

---

Name	Volume Group Action Status
Description	Volume Group Action Error
Alert message	Failed to <i>action</i> volume group with name ' <i>vg_name</i> ' and internal ID ' <i>vg_uuid</i> ' because <i>reason</i> in protection domain ' <i>protection_domain_name</i> '
Cause	A volume group could not be restored or could not be deleted because it is still in use.
Impact	The requested volume group action (restore or delete) could not be completed.
Resolution	Detach the volume group from VMs and external initiators before recovery.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

#### **vDisk Block Map Usage High Warning [130072] []**

---

Name	vDisk Block Map Usage Warning
Description	vDisk Block Map Usage High.
Alert message	Too many snapshots have been allocated in the system. This may cause perceivable performance degradation.
Cause	Too many vdisks or snapshots are present in the system.
Impact	Cluster performance may be significantly degraded.
Resolution	Remove unneeded snapshots and vdisks. If using remote replication, try to lower the frequency of taking snapshots. If you cannot resolve the error, contact Nutanix support.

---

#### **Unable to remount datastore [130076] []**

---

Name	Datastore Remount Status
Description	Unable to remount datastore
Alert message	Unable to <i>operation</i> Datastore ' <i>datastore_name</i> ' <i>host_info</i> .
Cause	Various
Impact	VM HA and DRS functionality might be impaired.
Resolution	Please refer to KB2898 at the Nutanix Portal.

---

#### **Protected Vms Not Found [130083] [A130083]**

---

Name	Protected VMs Not Found
Description	Protected Vms Not Found
Alert message	Unable to locate VM(s) <i>vm_names</i> protected by protection domain ' <i>protection_domain_name</i> '.
Cause	Protected VM(s) cannot be found and may have been deleted.
Impact	Any data associated with the VMs may not be backed up or replicated to a remote site.
Resolution	Remove VM(s) from the protection domain.

---

#### **Protected Volume Groups Not Found [130084] [A130084]**

---

Name	Protected Volume Groups Not Found
Description	Protected Volume Groups Not Found
Alert message	Unable to locate volume group(s) <i>vg_names</i> protected by protection domain ' <i>protection_domain_name</i> '.
Cause	Protected volume group(s) cannot be found and may have been deleted.
Impact	Any data associated with the volume group(s) may not be backed up or replicated to a remote site.
Resolution	Remove volume group(s) from the protection domain.

---

#### **VStore Snapshot Status [130086] []**

---

Name	VStore Snapshot Status
Description	VStore Snapshot Status
Alert message	Snapshot status for vstore <i>vstore_name</i> : <i>reason</i> .
Cause	Various
Impact	The requested VStore snapshot action could not be completed.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

### Disk Diagnostic Failure [130089] [A1139]

---

Name	Disk Diagnostic Status
Description	Drive diagnostic has failed.
Alert message	Drive <i>disk_id</i> with serial <i>disk_serial</i> in drive bay <i>disk_Location</i> on Controller VM <i>service_vm_external_ip</i> has failed diagnostic test.
Cause	The drive has failed.
Impact	Cluster storage capacity is reduced.
Resolution	Replace the drive. Refer to the Nutanix documentation for instructions.

---

### Related Entity Protection Status [130090] []

---

Name	Related Entity Protection Status
Description	Protection status of a related entity.
Alert message	<i>error_message</i> .
Cause	Related entity is not protected in the same protection domain.
Impact	Related VM/Volume Group will not be snapshotted and recovered.
Resolution	Protect the related entity in the same consistency group.

---

### iSCSI Configuration Failed [130100] [A130100]

---

Name	iSCSI Configuration Failed
Description	iSCSI Configuration Failed
Alert message	Failed to re-configure iSCSI settings on the recovered VM ' <i>vm_name</i> '. <i>reason</i> .
Cause	Nutanix Guest Tools failed to execute some iSCSI commands on the guest VM.
Impact	iSCSI disks may become unavailable on the guest VM.
Resolution	If IQN and iSCSI target IP addresses of the VM have been updated by Nutanix Guest Agent, Discover and connect to new targets after rebooting the VM.
Resolution	Manually configure iSCSI settings on the guest VM.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

---

### Recovered VM Disk Configuration Update Failed [130107] [A130107]

---

Name	Disk Configuration Update Failed
Description	Disk Configuration Update Failed
Alert message	Failed to make some disks online on the recovered VM ' <i>vm_name</i> '. <i>reason</i> .
Cause	Nutanix Guest Tools failed to automatically bring the disks online.
Impact	Disks may become offline on the recovered VM.

---

Resolution	Manually bring the disks online on the recovered VM.
Resolution	Resolve the stated reason for the failure. If you cannot resolve the error, contact Nutanix support.

#### System-Defined Flash Mode Usage Limit Exceeded [130120] []

Name	System Defined Flash Mode Usage Limit
Description	Check that usage for flash-mode-enabled vDisks is within system limits.
Alert message	System has down-migrated the data of flash-mode-enabled vDisks.
Cause	Too many vDisks are assigned to the flash tier, or the vDisks assigned to the flash tier are too large.
Impact	The advantages of flash mode may not be available.
Resolution	Reduce the number of flash-mode-enabled vDisks or increase the capacity of the flash tier.

#### Storage Container Space Usage Exceeded: AOS Check [130121] []

Name	High Space Usage on Storage Container
Description	Check high space usage on Storage Containers
Alert message	Storage Container space usage for <i>container_name</i> is at <i>usage_pct</i> %.
Cause	Excessive space usage in the Storage Container.
Impact	Storage Container will run out of space, and the cluster may become unable to service I/O requests.
Resolution	Delete some data to free storage space from the Storage Container.

#### NFS metadata size overshoot [130122] []

Name	NFS Metadata Size Overshoot
Description	NFS Metadata Usage High
Alert message	NFS metadata usage is too high. Calculated metadata usage of <i>metadata_usage</i> bytes exceeds safety limit of <i>metadata_limit</i> bytes on Controller VM <i>service_vm_id</i> .
Cause	Either NFS datastore is used as a file store which is not supported, or too many files are present in the datastore.
Impact	Cluster performance and stability may be significantly degraded.
Resolution	If NFS datastore is used as a file store, remove the corresponding files and wait for up to 24 hours to allow compaction.

## Task Status

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

### Task Page Navigation

- To view the Task dashboard, select **Task** from the pull-down list on the far left of the main menu.
- 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.
- 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

### View Task Status

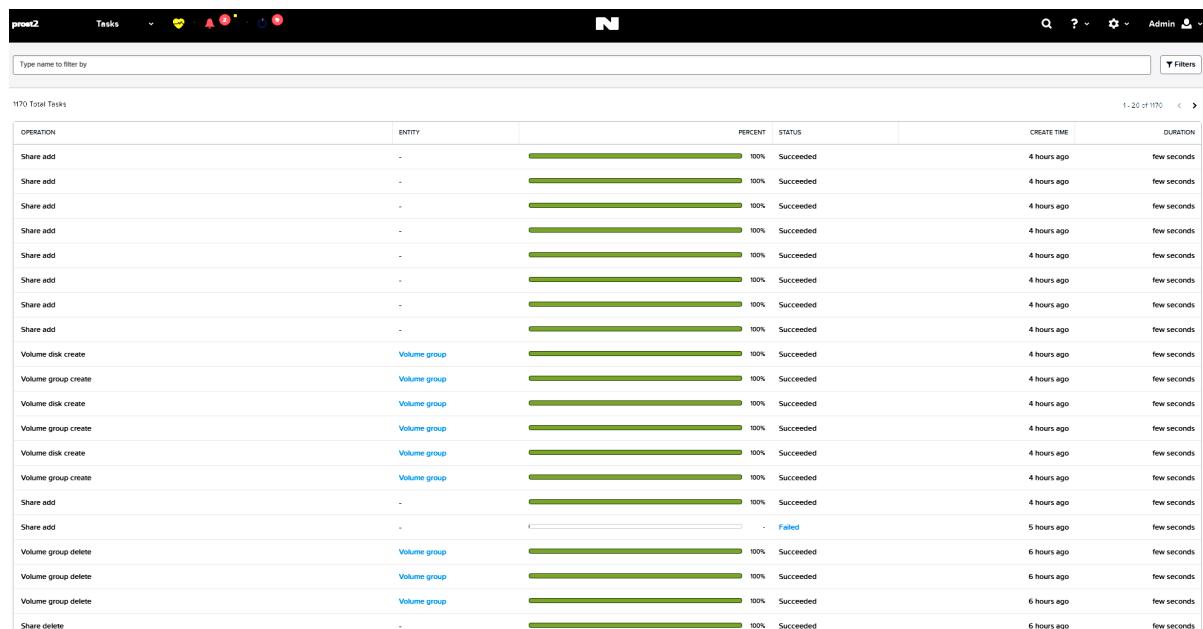


Figure: Task Dashboard

The following table describes the fields in the tasks list.

## Tasks List Fields

Parameter	Description	Values
Operation	Specifies which type of operation the task is performing.	upgrade <other>
Entity	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
Create Time	Displays when the task began.	seconds, minutes, hours
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 (see [Configuring Name Servers](#) on page 570)
- If Acropolis is enabled, you can configure one or more network connections (see [Configuring Network Connections](#) on page 151).
- You can create a whitelist of IP addresses that are allowed access (see [Configuring a Filesystem Whitelist](#) on page 569).
- You can specify one or more NTP servers for setting the system clock (see [Configuring NTP Servers](#) on page 572).
- You can configure one or more network switches for statistics collection (see [Configuring Network Switch Information](#) on page 155).
- You can specify an SMTP mail server (see [Configuring an SMTP Server](#) on page 573).
- You can configure SNMP (see [Configuring SNMP](#) on page 574).
- You can configure a login banner page (see [Configuring a Banner Page](#) on page 583).

### Configuring a Filesystem Whitelist

A whitelist is a set of addresses that are allowed access to the cluster. Whitelists are used to allow appropriate traffic when unauthorized access from other sources is denied.



**Warning:** 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 whitelist, do the following:

1. In the gear icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Filesystem Whitelists**.  
The *Filesystem Whitelists* dialog box appears.
2. To add an address to the whitelist, enter the IP address and netmask value (in the form ip\_address/netmask) in the **IP Address/Netmask** field and then click the **Add** button to the right of that field.  
The entry is added to the **Whitelist Entry** list (below the **IP Address/Netmask** field).
3. To delete an entry from the whitelist, click the garbage pail 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.
4. Click the **Close** button to close the *Filesystem Whitelists* window.  
An NFS whitelist is created when the hypervisor is ESXi or AHV. A CIFS whitelist is created when the hypervisor is Hyper-V.

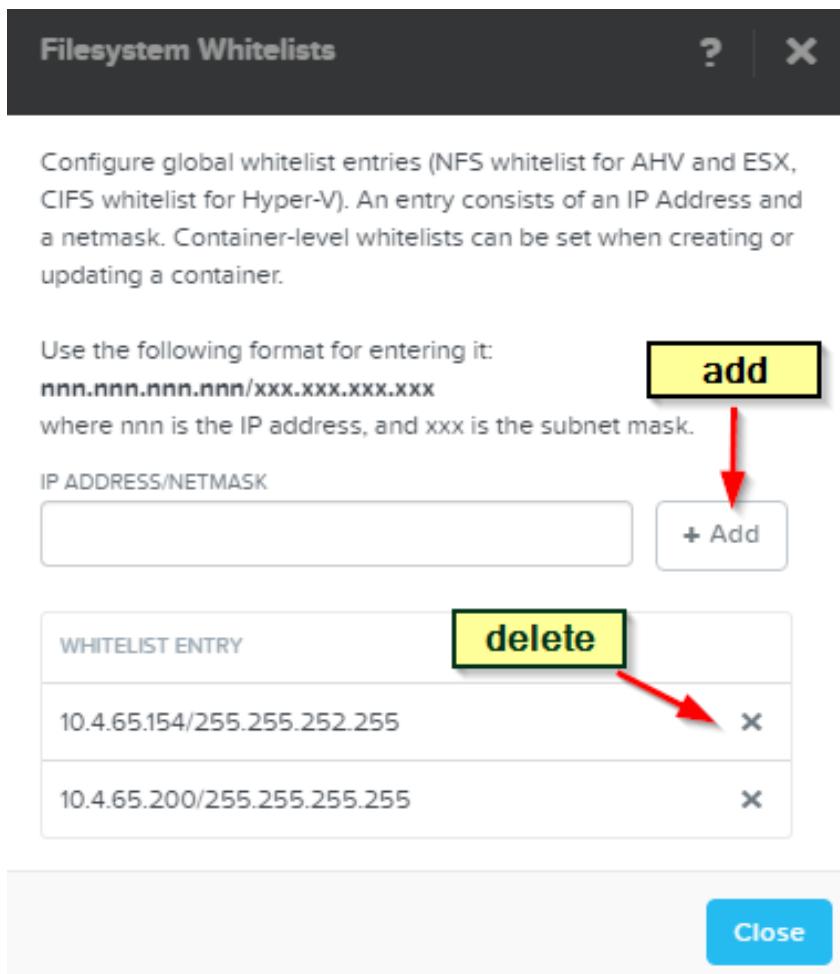


Figure: NFS Whitelists Window

## Configuring Name Servers

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:

1. In the gear icon  pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Name Servers**.  
The **Name Servers** dialog box appears.
2. 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.
3. To delete a name server entry, click the cross 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.
4. Click the **Close** button to close the **Name Servers** window.

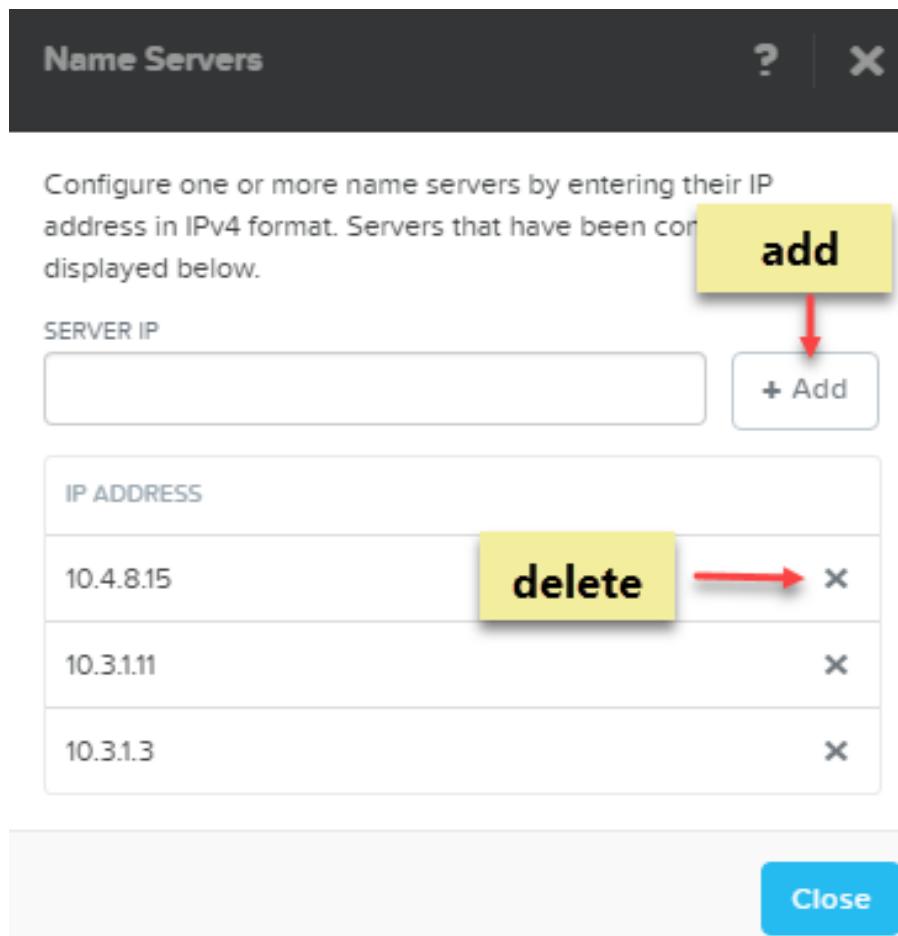


Figure: Name Servers Window

## 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, prefer a time source maintained by the 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 <http://support.ntp.org/bin/view/Support>SelectingOffsiteNTPServers> for various recommendations.

- 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

To add (or delete) an NTP server entry, do the following:

1. In the gear icon  pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **NTP Servers**.  
The **NTP Servers** dialog box appears.
2. 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).
3. 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.
4. Click the **Close** button to close the **NTP Servers** window.

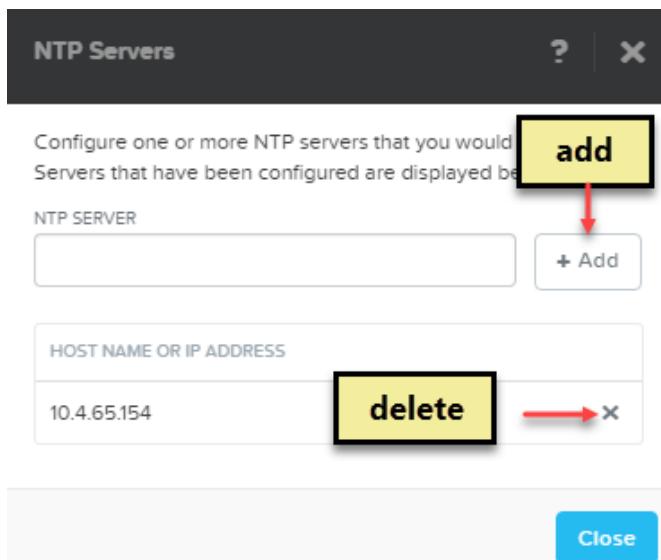


Figure: NTP Servers Window

## Configuring an SMTP Server

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 and to exchange emails with Nutanix technical support. To configure an SMTP server entry, do the following:

1. In the gear icon  pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **SMTP Server**.  
The *SMTP Server Settings* dialog box appears.
  2. 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).
    - c. **Security Mode:** Enter the desired security mode from the pull-down list.  
The options are NONE (unencrypted), STARTTLS (use TTL 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 (*user@domain*) depending on the authentication process.
    - e. **Password:** Enter the user password.
- a. From Email Address (optional):** Enter an e-mail address that appears as the sender address.  
By default, alert (see [Configuring Alert Emails](#) on page 414) and cluster status information (see [Configuring Pulse](#) on page 634) 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.

- When all the fields are correct, click the **Save** button.

The screenshot shows the 'SMTP Server Settings' dialog box. At the top, it says 'Configure the SMTP server that the Nutanix software should use to send email such as alerts.' Below this are several input fields:

- HOST NAME OR IP ADDRESS:** An empty text input field.
- PORT:** An empty text input field.
- SECURITY MODE:** A dropdown menu set to 'NONE'.
- USER:** An empty text input field.
- PASSWORD:** An empty text input field.
- FROM EMAIL ADDRESS:** An empty text input field.

At the bottom of the dialog are three buttons: 'Clear' (grayed out), 'Cancel' (grayed out), and 'Save' (highlighted in blue).

Figure: SMTP Server Settings Window

## Configuring SNMP

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. To configure SNMP v3 (versions 1 and 2 are not supported), do the following:

- In the gear icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **SNMP**.  
The *SNMP Configuration* dialog box appears.

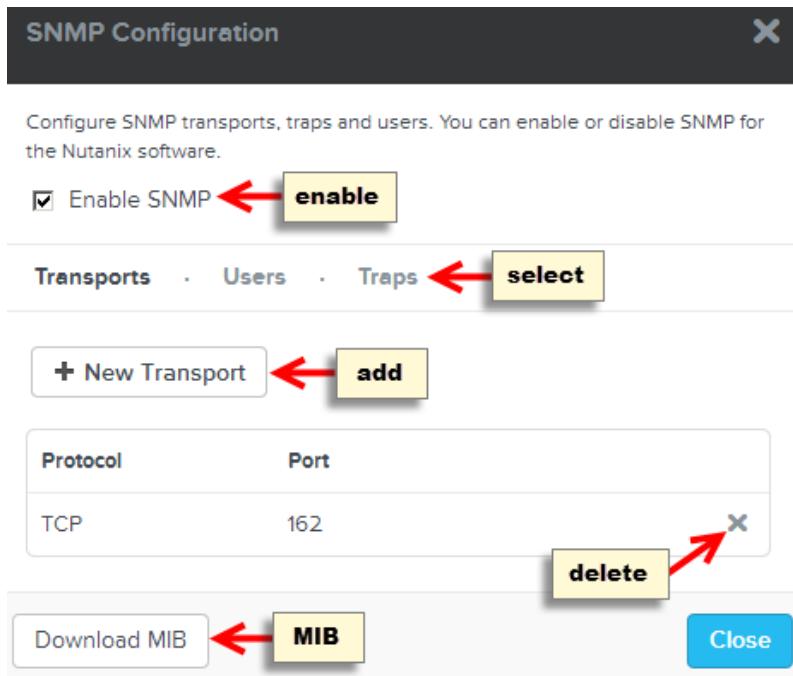


Figure: SNMP Configuration Window

- To enable SNMP for this cluster, check the **Enable SNMP** box. To disable SNMP, uncheck the box.

**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.

- To view the Nutanix MIB (NUTANIX-MIB.txt), click the **Download 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.
- 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:

The screenshot shows the 'Transports' tab selected in the navigation bar. Below it, there is a 'Protocol' dropdown menu set to 'TCP'. Below the dropdown is a 'Port' input field containing '162'. At the bottom of the dialog are two buttons: 'Cancel' and 'Save'.

Figure: SNMP Transport Fields

- a. **Protocol:** Select the protocol to use from the pull-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.
- 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.

5. To add an SNMP user entry, click the **Users** tab and the **New User** button and then do the following in the indicated fields:

TRANSPORTS		USERS	TRAPS
USERNAME			
PRIV TYPE	PRIV KEY		
AES			
AUTH TYPE	AUTH KEY		
SHA			

Figure: SNMP User 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.
  - d. **Auth Type:** Select the authentication hash function type from the pull-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.
  - 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.
6. 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:

Address	Inform
<input type="text"/>	<input type="button" value="False"/>
Port	Transport Protocol
<input type="text"/>	<input type="button" value="UDP"/>
Engine ID	Trap Username
<input type="text"/>	<input type="button" value="jwm"/>

Figure: SNMP Trap Fields

a. **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.

b. **Port:** Enter the port number to use.

The standard SNMP port number is 161.

c. **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.

d. **Inform:** Select **True** from the pull-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.

e. **Transport Protocol:** Select the protocol to use from the pull-down list.

The options are **TCP**, **TCP6**, **UDP**, and **UDP6**.

f. **Trap Username:** Select a user from the pull-down list.

All users added previously (see step 5) appear in the pull-down list. You cannot add a trap receiver entry until at least one user has been added.

g. 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.

h. To test all configured SNMP traps, click the **Traps** tab, and then click **Test All**.

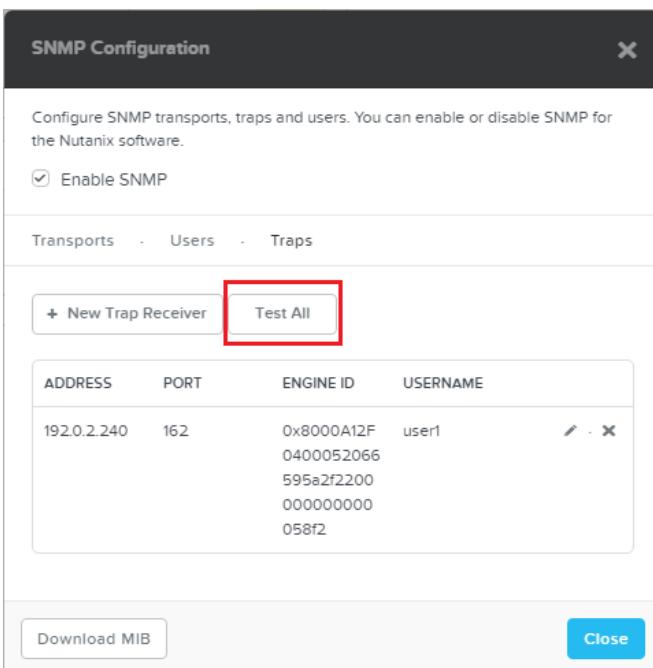


Figure: Test All Button

The Nutanix cluster sends test alerts to all the SNMP trap receivers configured on the cluster.

7. 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.
8. 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.
9. Click the **Close** button to close the *SNMP Configuration* window.

## Nutanix MIB

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.

The following table describes the Nutanix MIB fields. The table is subdivided by the MIB sections.

#### Nutanix MIB Fields

Name	Description	Data Type
<i>Cluster Information Fields</i>		
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 "started" and "stopped".	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
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
<i>Software Version Information Fields</i>		
svtIndex	Unique index that is used to identify an entry in the software version information table.	Signed 32-bit integer
svtControllerVMId	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
<i>Service Status Information Fields</i>		
cstIndex	Unique index that is used to identify an entry in the service status information table.	Signed 32-bit integer

Name	Description	Data Type
cstControllerVMId	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
<i>Hypervisor Information Fields</i>		
hypervisorIndex	Number that is used to uniquely identify an entry in the hypervisor information table.	Signed 32-bit integer
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
hypervisorCpuUsagePercent	Percentage of CPU resources in use by the hypervisor instance.	Unsigned 32-bit integer
hypervisorMemory	Total memory available to the hypervisor instance, in bytes.	Unsigned 64-bit integer
hypervisorMemoryUsagePercent	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).	Unsigned 64-bit integer
hypervisorIOBandwidth	I/O bandwidth of the hypervisor in kilobytes per second (KBps).	Unsigned 64-bit integer
hypervisorRxBytes	Total number of bytes received by the hypervisor.	Unsigned 64-bit integer
hypervisorTxBytes	Total number of bytes transmitted by the hypervisor.	Unsigned 64-bit integer
hypervisorRxDropCount	Total number of packets dropped by the hypervisor when receiving data.	Unsigned 64-bit integer
hypervisorTxDropCount	Total number of packets dropped by the hypervisor when transmitting data.	Unsigned 64-bit integer
<i>Virtual Machine Information Fields</i>		
vmlIndex	Number that is used to uniquely identify an entry in the VM information table.	Signed 32-bit integer

Name	Description	Data Type
vmId	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
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.	Unsigned 64-bit integer
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 ( $\mu\text{s}$ ).	Unsigned 64-bit integer
vmlOBandwidth	I/O bandwidth of the VM in kilobytes per second (KBps).	Unsigned 64-bit integer
vmRxBytes	Total number of bytes received by the VM.	Unsigned 64-bit integer
vmTxBytes	Total number of bytes transmitted by the VM.	Unsigned 64-bit integer
vmRxDropCount	Total number of packets dropped by the VM when receiving data.	Unsigned 64-bit integer
vmTxDropCount	Total number of packets dropped by the VM when transmitting data.	Unsigned 64-bit integer
<i>Disk Information Fields</i>		
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
dstControllerVmId	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

Name	Description	Data Type
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
dstNumFreeInodes	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 ( $\mu$ s).	Unsigned 64-bit integer
dstIOPBandwidth	I/O bandwidth of the disk in kilobytes per second (Kbps).	Unsigned 64-bit integer
dstNumberIops	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
<i>Controller VM Resource Information Fields</i>		
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
<i>Storage Pool Information Fields</i>		
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
spitAvgLatencyUsecs	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
<i>Storage Container Information Fields</i>		
ctIndex	Number that is used to uniquely identify an entry in the storage container information table.	Signed 32-bit integer

Name	Description	Data Type
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
<i>Alerts Information Fields</i>		
ntxAlertCreationTime	Time of alert creation. The value is the number of seconds since the UNIX epoch (01/01/1970).	Unsigned 64-bit integer
ntxAlertDisplayMsg	<p>Alert message text. All Nutanix SNMP alerts are generated with the same SNMP OID. The differentiating factor is the description of the event, which is included in the alert. The following sample alerts have the same SNMP OID but different event descriptions:</p> <pre> DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (110276) 0:18:22.76 ... SNMPv2-SMI::enterprises.41263.999.2 = STRING: "Failed to send email from Controller VM 192.0.2.244 via SMTP server 192.0.2.242:2525 due to following error : Connection refused." </pre> <pre> DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (156330) 0:26:03.30 ... SNMPv2- SMI::enterprises.41263.999.2 = STRING: "Controller VM 192.0.2.243 has been rebooted on Mon Sep 21 21:30:00 2015." </pre> <p>The set of alert messages that the SNMP agent includes in traps is the same as the set of alert messages that is exposed through the web console. For a list of the alert messages and corrective actions, see <a href="#">Alerts/Health checks</a> on page 417.</p>	Display string

## 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.

To configure a banner page, do the following:

1. In the gear icon  pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Welcome Banner**.  
The *Edit Welcome Banner* dialog box appears.
2. 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.
3. Click the **Preview** button to display the banner in the pane on the right.
4. If the banner is not correct, update the HTML code as needed until the preview pane displays the desired message.
5. 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 unchecking (checking) the **Enable Banner** box.

The following figure is a sample banner page configuration.



**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.

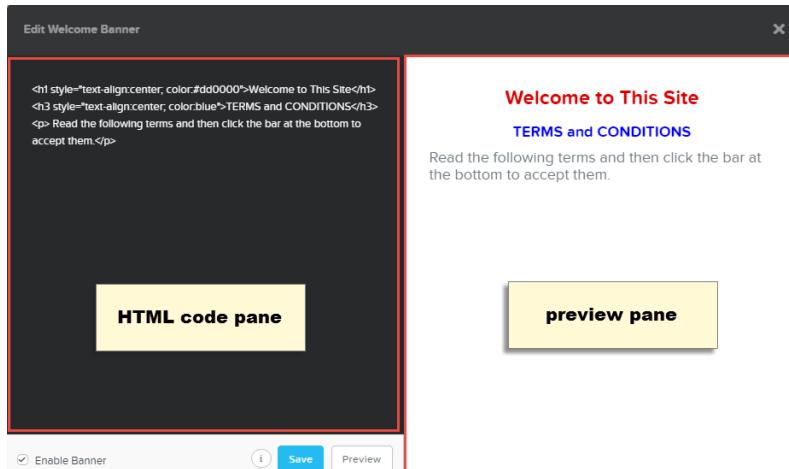


Figure: Welcome Banner Window

## VM Management through Prism Element (ESXi)

From AOS 5.0 or later releases, 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 vCenter Server](#) on page 585.

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 reboot.
- 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 cluster with the new IP address.

## Requirements and Limitations

- SCSI, IDE, and SATA disks are supported. PCI disks are not supported.
- The E1000, 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.

## Registering a vCenter Server

To perform core VM management operations directly from Prism without switching to vCenter Server, you need to register your cluster with the vCenter Server.

Following are some of the important points about registering vCenter Server.

- Nutanix does not store vCenter Server credentials.
- Whenever a new node is added to cluster, vCenter Server registration for the new node is automatically performed.
- If you change the vCenter Server credentials, all the operations will start to fail. You need to unregister and then register the vCenter Server again. For unregistering vCenter Server from the cluster, see [Unregistering a Cluster from the vCenter Server](#) on page 586.

1. Log into the Prism web console.
2. From the settings menu, select **vCenter Registration**.
  - The vCenter Server that is managing the hosts in the cluster is auto-discovered and its IP address is auto-populated in the **Address** field.
  - The port number field is also auto-populated with 443. Do not change the port number.

- Type the administrator user name and password of the vCenter Server in the **Admin Username** and **Admin Password** fields.
- Click **Register**.

During the registration process a certificate is generated to communicate with the vCenter Server. If the registration is successful, relevant message is displayed in the **Tasks** dashboard.

### Unregistering a Cluster from the vCenter Server

To unregister the vCenter Server from your cluster, perform the following procedure.

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 should register the vCenter Server again with the new IP address with the cluster.

- Log into the Prism web console.
- From the settings menu, click **vCenter Registration**.  
A message that cluster is already registered to the vCenter Server is displayed.
- Type the administrator user name and password of the vCenter Server in the **Admin Username** and **Admin Password** fields.
- Click **Unregister**.  
If the credentials are correct, the vCenter Server is unregistered from the cluster and a relevant message is displayed in the **Tasks** dashboard.

## 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 in the AHV cluster. After the conversion finishes, you need to manually start the VMs on the AHV cluster. You can also convert the cluster back to ESXi. This conversion from AHV to ESXi is a file system restore. 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.

### Requirements and Limitations for In-Place Hypervisor Conversion

Following are the general prerequisites along with requirements and limitations for the in-place hypervisor conversion feature.

#### Prerequisites

- Ensure that HA and DRS is disabled.
- All the nodes in the cluster should be running AOS 4.6 or later versions (4.6.2 or later for Lenovo platforms).
- Ensure that you have saved 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.
- This feature is supported on multi-hypervisor clusters (combination of ESXi nodes with one AHV node).

## General Limitations

- This feature is not supported if you have metro availability protection domains in your environment.
- Conversion back from ESXi to AHV fails if you have converted the cluster using free ESXi license.
- Cluster conversion fails if you have Acropolis File Services deployed in your cluster.

## ESXi Supported Versions

### Supported ESXi Versions

Version	Support
5.1	All versions of 5.1.x are supported
5.5	All versions of 5.5.x are supported
6.0	6.0, 6.0 Update 1, and 6.0 Update 2

## ESXi Network Requirements and Limitations

### Network Requirements and Limitations

Component	Description
NIC	Two 10 GB or two 1 GB NICs are required on each host for conversion. Ensure that the NICs that are in the uplink set are homogenous.
vSwitch	<ul style="list-style-type: none"><li>• Each host should have only one external vSwitch. If you have more than one external vSwitch conversion validation fails.</li><li>• One active and multiple passive failover configuration of NICs on vSwitch is supported.</li><li>• Active/active load balancing policies are not supported and will be 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 switch	Not supported
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 the AHV, these changes may not be maintained after converting the cluster back to ESXi.
- All the powered off VMs end up on a single host. The network configuration that you might have defined for the VMs may not be maintained.
- MAC address of the VMs are not preserved because the MAC address is provided by the hypervisor (ESXi and AHV) and both the hypervisors follow different conventions.
- After migration to AHV, NIC adapter 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**

- All the operating systems that are supported by NGT are supported by this feature. See [Nutanix Guest Tools Requirements and Limitations](#) on page 390 for more information.
- Only VMs with flat disks are supported. The delta disks are not supported.
- IDE/SCSI disks are only supported. SATA and PCI disks are not supported.
- Set the SAN policy to OnlineAll for all the Windows VMs for all the non-boot SCSI disks so that they can be automatically brought online. For more information on setting SAN policy, see [Bringing Multiple SCSI Disks Online](#) on page 333.
- Install NGT on all the VMs. See [Enabling and Mounting Nutanix Guest Tools](#) on page 393 for more information.
- Folders with NFS mounts and VMware tags in vSphere for categorisation may not be supported.
- Ensure that you do not have VMs with UEFI boot firmware enabled.
- Virtual machines with attached volume groups or shared virtual disks are not supported.
- VMs running SUSE Linux Enterprise Server (SLES) operating system are not supported.
- After conversion of the cluster back to ESXi from AHV, the VMs are converted to the maximum hardware version that is supported by that specific ESXi version.
- 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.
- Do not power on the VMs while the conversion is in progress.
- If the VMs have static IP address configured, you need to manually reconfigure IP address after conversion.

## In-Place Hypervisor Conversion Process

### **ESXi to AHV**

After you start the conversion process, all the nodes in the cluster are converted one by one to AHV. The current state of ESXi host is saved for reverting to ESXi. Internally foundation converts the ESXi host to AHV. First all the Controller VMs are migrated to AHV. After Controller VMs come up on the AHV side, VMs that are running on ESXi are migrated to AHV. After migration of VMs is completed, you need to manually start the VMs on AHV. Once all the hosts and VMs are migrated to AHV, you can start using the AHV cluster.

### **Port Groups and VLAN Transformation**

All the ESXi port groups, any VLAN IDs, and virtual machines that belong to a particular group are captured, a corresponding Acropolis virtual network for every unique ESXi port group on the cluster is created, a corresponding VLAN ID is assigned, and then the VMs are transferred into the right virtual network. 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.

### **VM Conversion**

After you install NGT on the VMs and start the conversion, the VM conversion occurs simultaneously. The process is as follows.

- Validation:** All the existing VMs in the cluster are validated and if some VMs cannot be converted, an error message is displayed with a valid reason.
- Start:** A record of the conversion is created to track the progress of the conversion.
- Preparing Node for VM conversion:** All the information about VMs registered on a node is gathered depending on the node UUID. If the VMs are protected, they are automatically unprotected. All the

information relevant to the VMs is stored in the master conversion record. The source VM files are not modified.

- **Perform VM Conversion:** The hypervisor type of the node to that of the hypervisor type in the node conversion record is verified. Depending on the information stored in the conversion record for a specific node, all the VMs are converted and registered on a specific node. The network mapping configuration that you have specified is used to convert the virtual networks to the target site. This process is performed for each protection domain.

At the completion of conversion, the source VM files are deleted.

### 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.



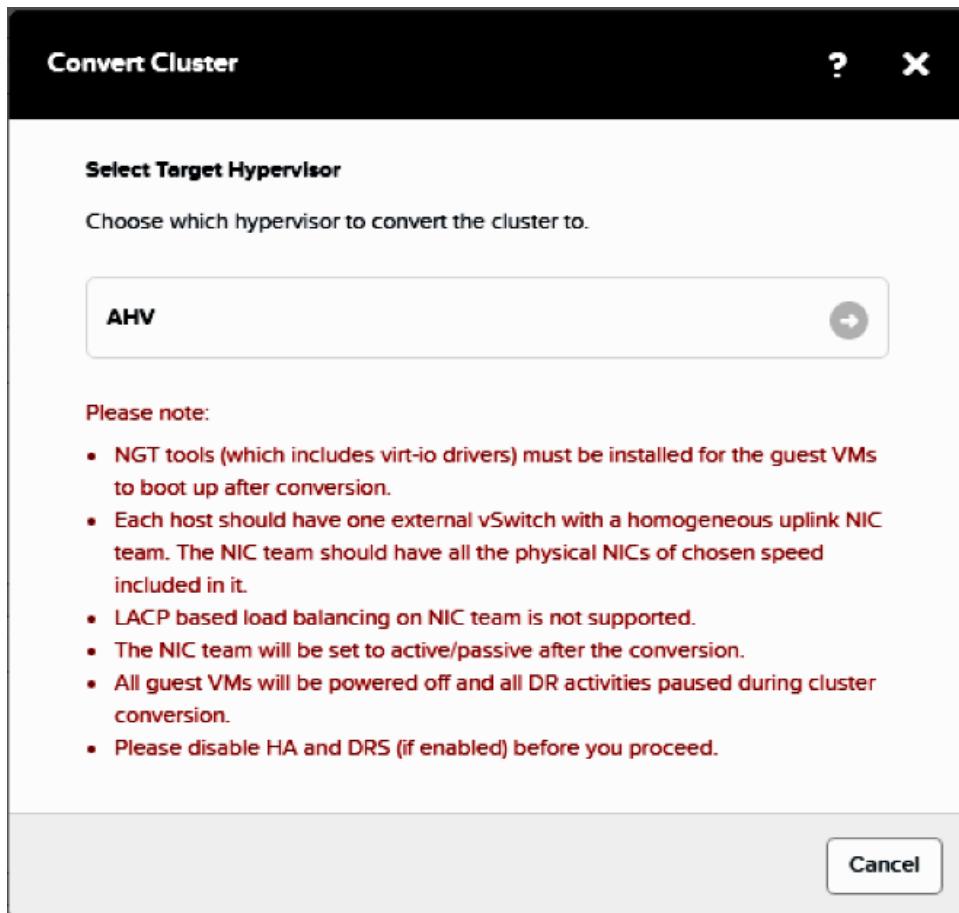
**Note:** The image that you provide should be of the same major ESXi version that you have used during ESXi to AHV conversion.

### Converting Cluster (ESXi to AHV)

Perform the following procedure to convert the cluster from ESXi to AHV.

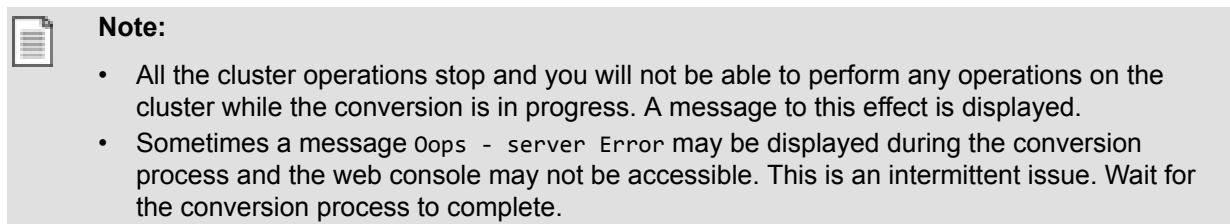
**Before you begin:** Verify that you have met all the networking and virtual machine requirements as described in [Requirements and Limitations for In-Place Hypervisor Conversion](#) on page 586.

1. Log into the web console.
2. From the wheel icon, click **Convert Cluster**.
3. Select **AHV** as the hypervisor and click the right-arrow icon.



The conversion process does not proceed unless you meet all the requirements that are listed in this pane. After you meet all the requirements, validation is performed and once the validation is successful the conversion process proceeds.

4. Click **Convert Cluster** button to start the conversion process.



5. 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. You can also track the progress of the conversion by logging again into the web console.

# SWITCHING HYPERVISOR TO AHV

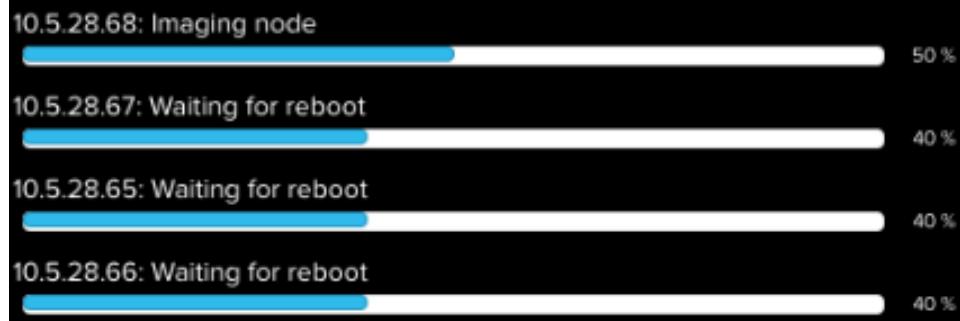


Figure: Conversion Progress

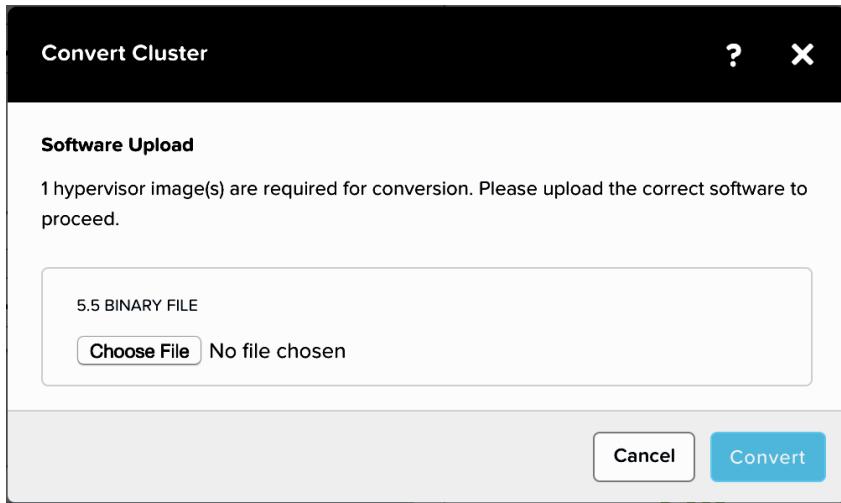
## Converting Cluster (AHV to ESXi)

Perform the following procedure to convert the cluster back to ESXi from AHV.

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:** 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 586 topic.

1. Log into the web console.
2. From the wheel icon, click **Convert Cluster**.
3. Select **ESXi** as the hypervisor and click the right-arrow icon.  
The conversion process does not proceed unless you meet all the requirements that are listed in this pane. After you meet all the requirements, validation is performed and once the validation is successful the conversion process proceeds.
4. Click **Convert Cluster** button to start the conversion process.
5. (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.

**6. Click Convert Cluster.**

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.

**7. 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.

#### Aborting Cluster Conversion

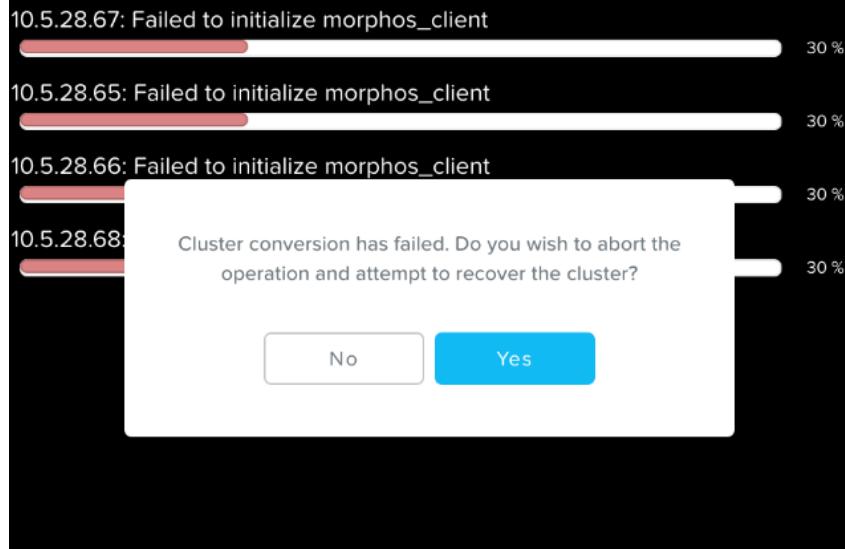
If any issues occur with the cluster conversion process, a message to abort the cluster conversion is displayed and then you can abort the cluster conversion operation and get the cluster to its pre-conversion state.

**Before you begin:** Ensure that you have saved the ESXi ISO at the foundation/isos/hypervisor/esx/ location. This ISO image will be used to bring the cluster back to its pre-conversion state if you abort the cluster conversion operation from ESXi to AHV.

If any issues occur during the conversion process, a message is displayed to abort the conversion operation.

Click **Yes** when a message to abort the cluster conversion is displayed.

# SWITCHING HYPERVISOR TO AHV



The cluster goes back to its original state. You need to manually power on the VMs after you perform this operation.

## Internationalization (i18n)

The following table lists all the supported and unsupported entities in UTF-8 encoding.

### Internationalization Support

Supported Entities	Unsupported Entities
Cluster name	Acropolis file server
Storage Container name	Share path
Storage pool	Internationalized domain names
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, iSCSCI initiator, vLAN name)

Supported Entities	Unsupported Entities
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 594.

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 [Creating a User Account](#) on page 626.

### Guidelines 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 change the language settings of the Prism. You can change the language setting of the cluster to Simplified Chinese or Japanese language. You also have an option to change the calendar, date, and time format to the selected region.

1. In the gear icon pull-down list of the main menu, select **Language Settings**.

By default **English** language is selected.

- To change the language setting of the cluster to Simplified Chinese, select **Simplified Chinese** from the drop-down menu.
- To change the language setting of the cluster to Japanese, select **Japanese** from the drop-down menu.

→ To change the locale settings (date, time, calendar), select the appropriate region from the **Region** drop-down menu.

By default, the locale is set to the language setting that you have set in the **Language** drop-down menu. However, you can change the **Region** to display the date, time, or calendar in some other format. This format for date, time, and calendar is applied for the entire cluster.

## 2. Click **Save**.

The language and locale settings (date, time, calendar) is changed according to the selection. For example, in the below screen shot, once you click **Save** the language setting for the cluster is changed to Chinese and locale setting is changed to Russian.

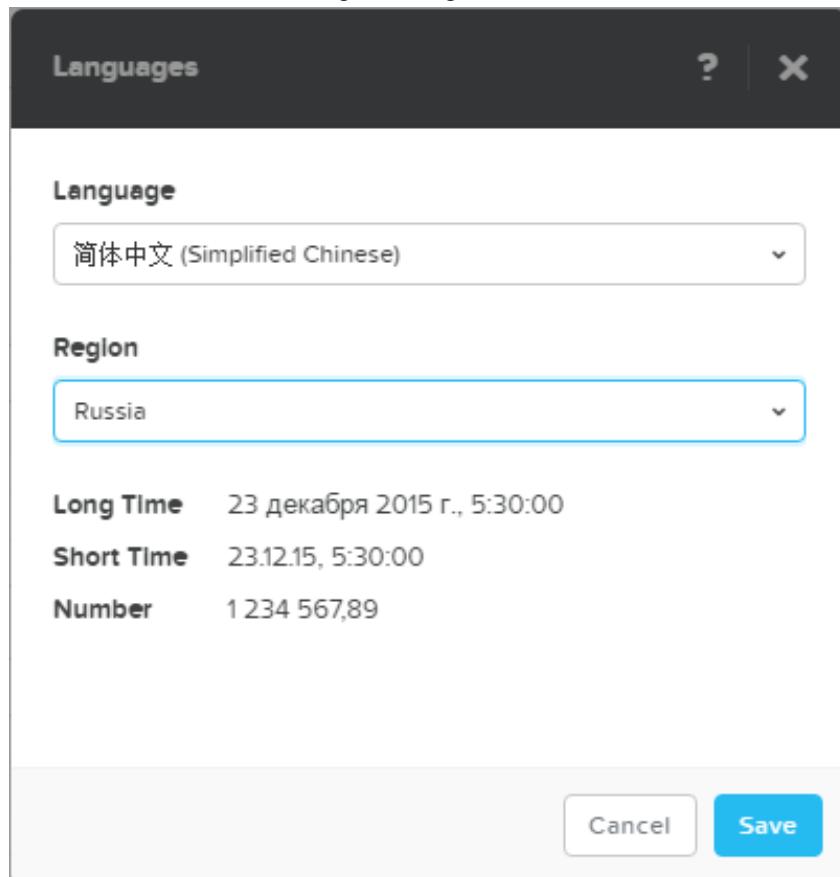


Figure: Locale Settings

For more information on the entities that are supported, see [Internationalization \(i18n\)](#) on page 593. Also, the user interface is localized according to the selection. For more information about localization, see [Localization \(L10n\)](#) on page 594.

## Hyper-V Setup

### Joining the Cluster and Hosts to a Domain

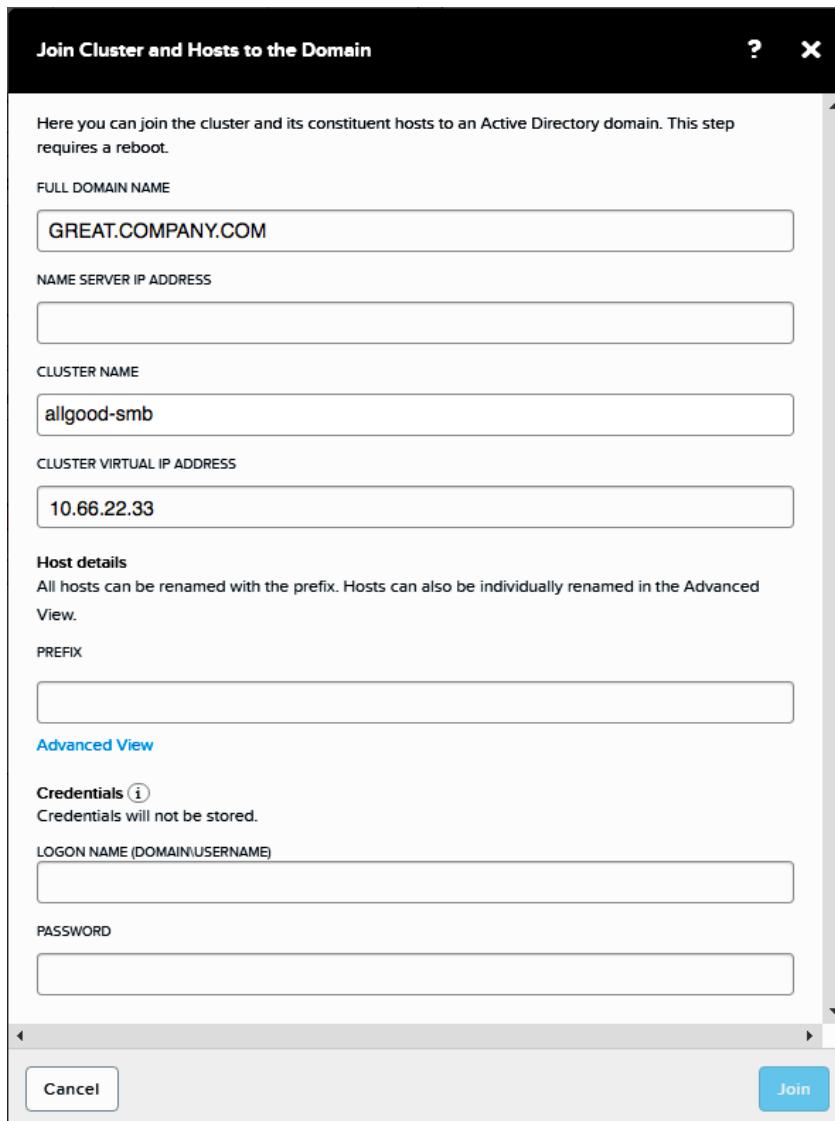
After completing foundation of the cluster, you need to join the cluster and its constituent hosts to the Active Directory domain. The joining of cluster and hosts to the domain facilitates centralized administration

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. To configure VLANs for the Controller VM, see the *Advanced Setup Guide*.
- Ensure that you have valid credentials of the domain account that has the privileges to create a new or modify an existing computer accounts in the Active Directory domain. 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)* section.

1. Log into the Web console by using one of the Controller VM IP address or by using cluster virtual IP address.
2. From the gear icon, select **Join Cluster and Hosts to the Domain**.



3. Type the fully qualified name of the domain that you want to join the cluster and its constituent hosts to in the **Full Domain Name** text box.
4. Type the IP address of the name server in the **Name Server IP Address** text box that can resolve the domain name that you have entered in the **Full Domain Name** text box.

- Type a name for the cluster in the **Cluster Name** text box.

The maximum length of the cluster name should not be more than 15 characters and it should be a valid NetBIOS name.

- Type the virtual IP address of the cluster in the **Cluster Virtual IP Address** text box.

If you have not already configured the virtual IP address of the cluster, you can configure it by using this field.

- Type the prefix that should be used to name the hosts (according to your convention) in the **Prefix** text box.

- 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 the **Advanced** link 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, type 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.

This logon name must be in the format **DOMAIN\USERNAME**. The credentials are required to join the cluster and its constituent hosts to the domain. Nutanix does not store the credentials.

- When all the information is correct, click **Join**.

The cluster is joined to the domain. All the hosts are renamed and joined to the domain and are restarted. Wait for about 5 to 10 minutes before proceeding to allow the hosts and Controller VMs time to start. After the cluster is ready, the logon page is displayed.

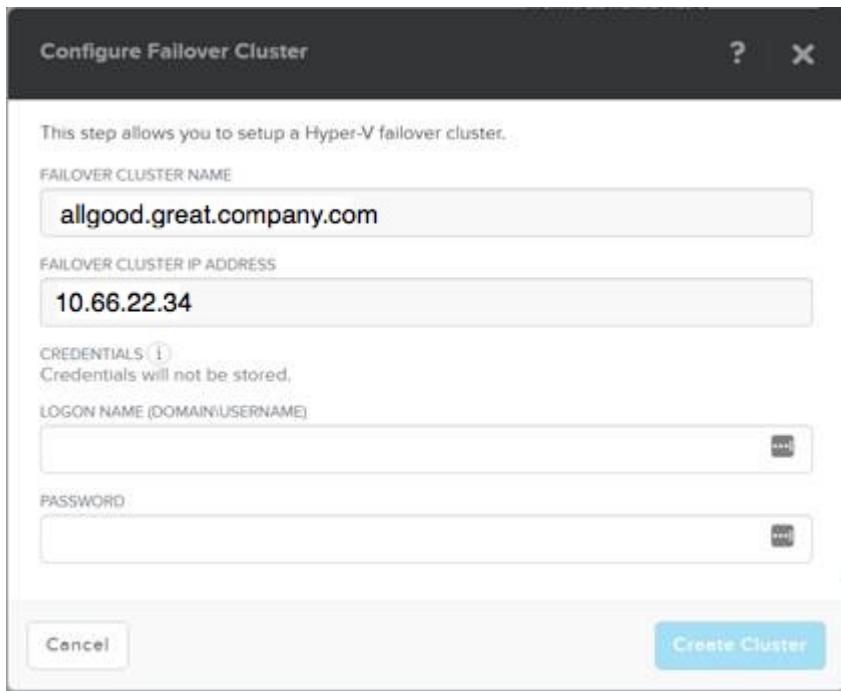
**What to do next:** Create a Microsoft failover cluster. For more information, see [Creating a Failover Cluster for Hyper-V](#) on page 597.

## Creating a Failover Cluster for Hyper-V

**Before you begin:** Join the hosts to the domain as described in "Joining the Cluster and Hosts to a Domain" in the Hyper-V Administration for Acropolis guide or the Prism Web Console guide.

Use this procedure to create a failover cluster that includes all the hosts in the cluster.

- Log into the Web console by using one of the Controller VM IP address or by using cluster virtual IP address.
- From the gear icon, select **Configure Failover Cluster**.



3. Type the failover cluster name in the **Failover Cluster Name** text box.

The maximum length of the failover cluster name should not be more than 15 characters and it should be a valid NetBIOS name.

4. Type an IP address for the Hyper-V failover cluster in the **Failover Cluster IP Address** text box.

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 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 or modify an existing computer accounts in the Active Directory domain.

This 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.

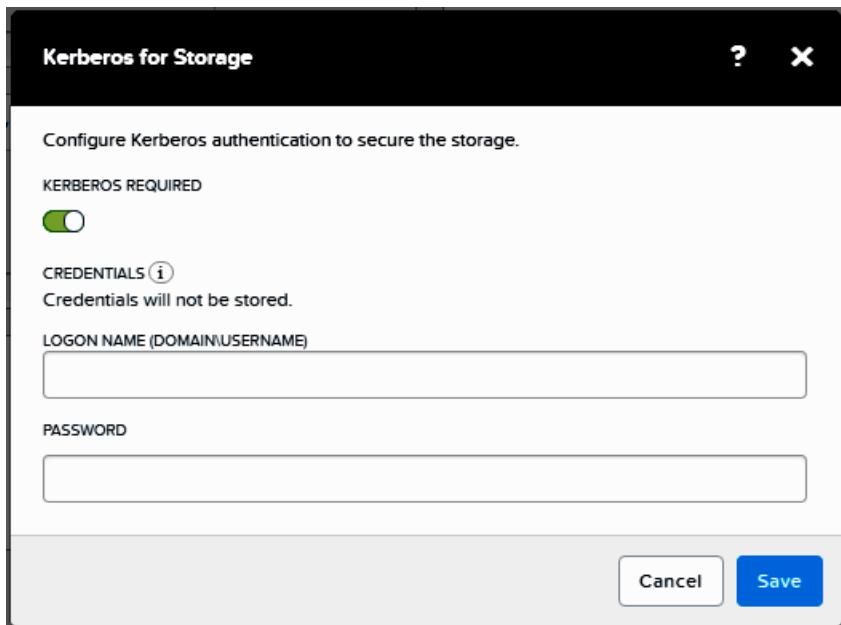
## Enabling Kerberos for Hyper-V

Perform the following procedure to configure Kerberos to secure the storage.

### Before you begin:

- Join the hosts to the domain as described in [Joining the Cluster and Hosts to a Domain](#) on page 595.
- Verify that you have configured service account for delegation. For more information on enabling delegation, see [Microsoft documentation](#).

1. Log into the Web console by using one of the Controller VM IP addresses or by using cluster virtual IP address.
2. From the gear icon, click **Kerberos Management**.



3. Set **Kerberos Required** button to enabled.
4. In the **Credentials** field, type the logon name and password of the domain account that has the privileges to create modify the virtual computer object representing the cluster in the Active Directory. The credentials are required for enabling Kerberos.  
This logon name must be in the format *DOMAIN\USERNAME*. Nutanix does not store the credentials.
5. Click **Save**.

#### Configuring the Nutanix Storage Cluster Object and Hyper-V Computer Objects by Using Kerberos and SMB Signing

Perform the following procedure to complete the configuration of the Nutanix storage cluster object by using Kerberos and SMB signing.

1. 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
```
2. Log on to Domain Controller and perform the following.
  - a. Right-click the Nutanix storage cluster object and go to **Properties**. For example, in the following screenshot, right-click **Kats1**.  
**Kats1** is the name of the Nutanix storage cluster object.

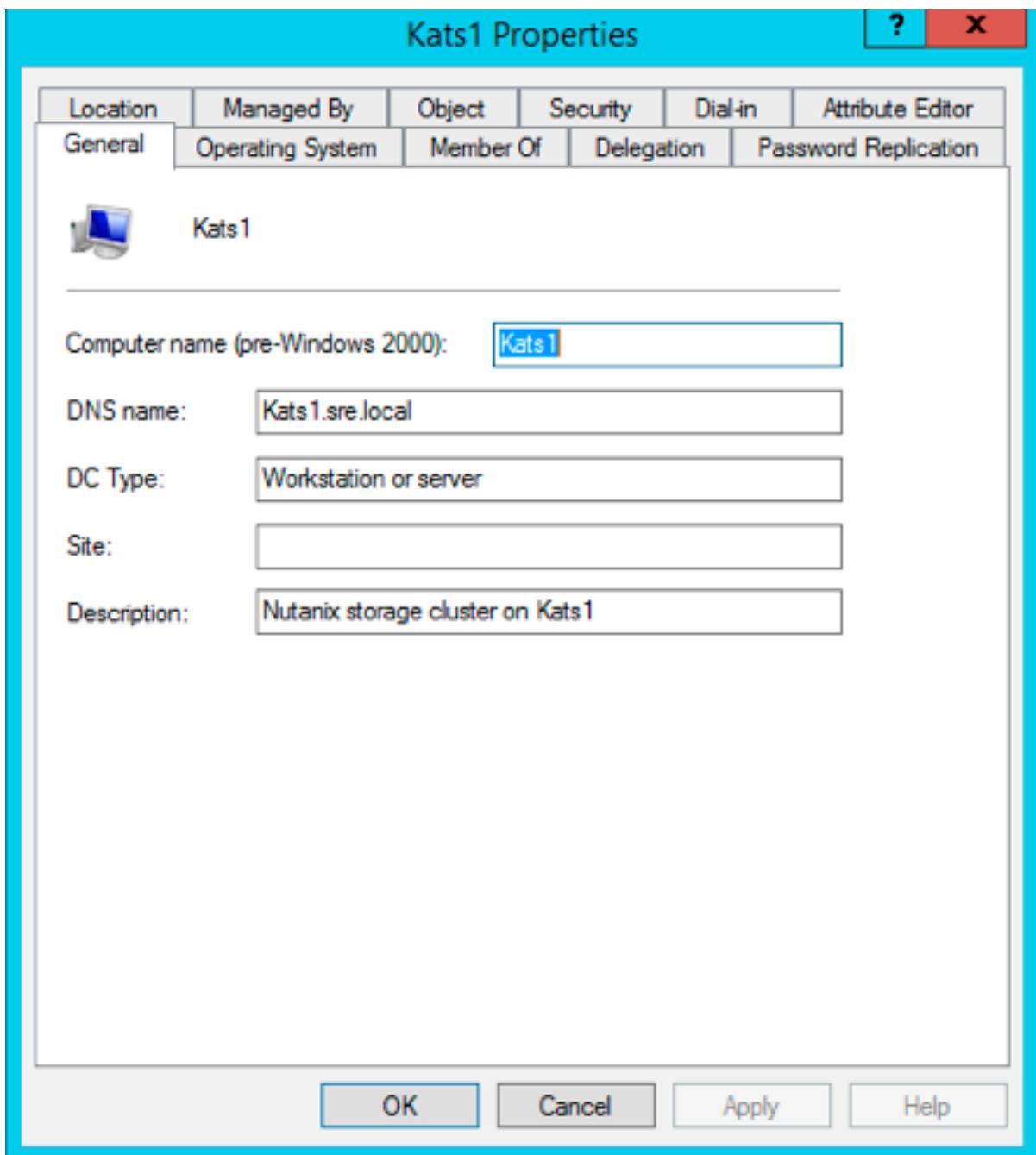


Figure: Nutanix Cluster Storage Object Properties

- b. In the **Delegation** tab, select the **Trust this computer for delegation to specified services only** option, and then select **Use Kerberos Only**.
- c. Click **Add**, select your Hyper-V hosts, and then add **cifs** and **Microsoft Virtual System Migration Service** for all the hosts. For example, in the following screenshot, there are three Hyper-V hosts: **Kats1-1**, **Kats1-2**, and **Kats1-3**.

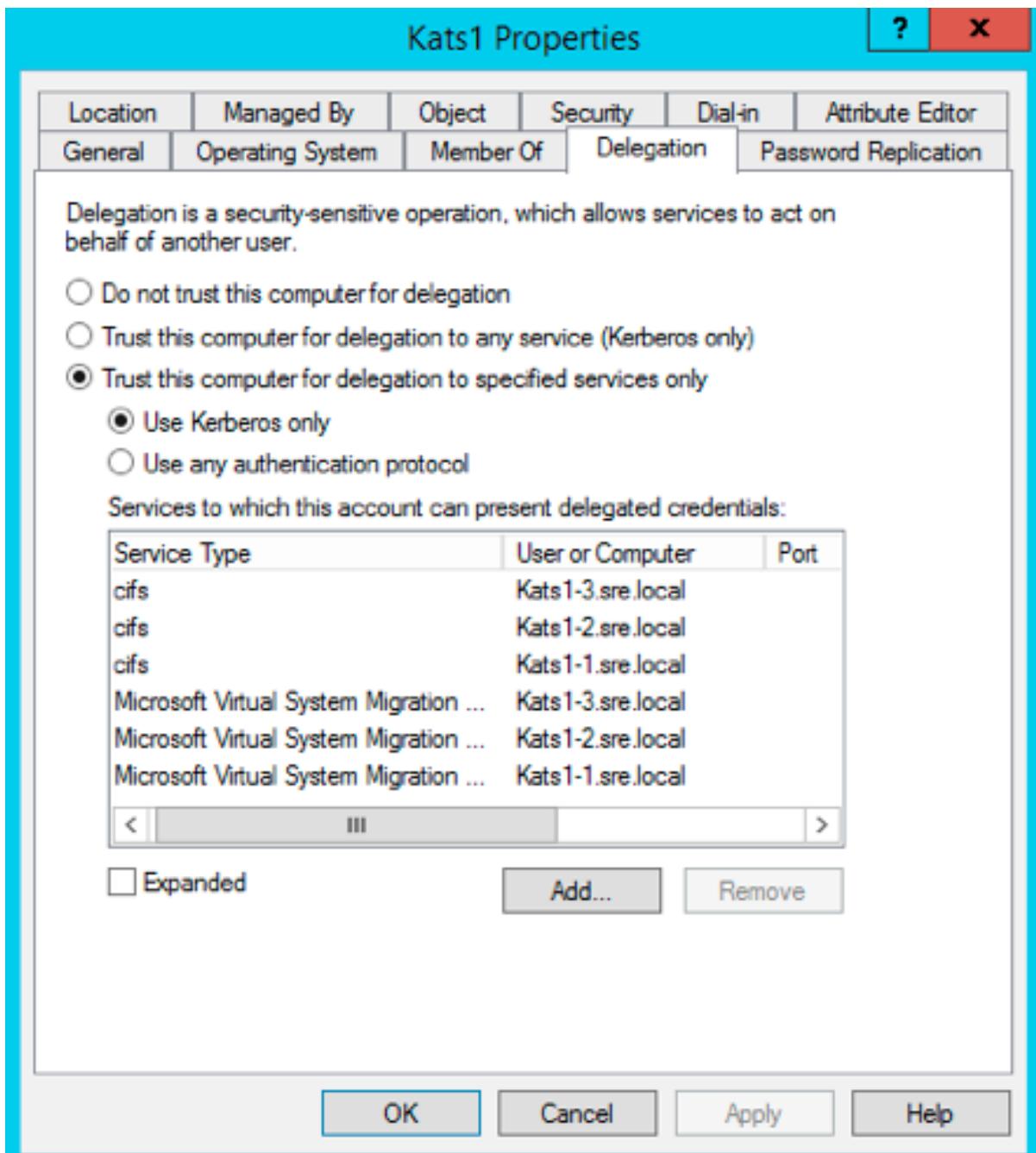


Figure: Adding cifs and Microsoft Virtual System Migration Service

3. 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 Kerberos Only**.
  - b. Click **Add** to add the **cifs** of the Nutanix storage cluster object.

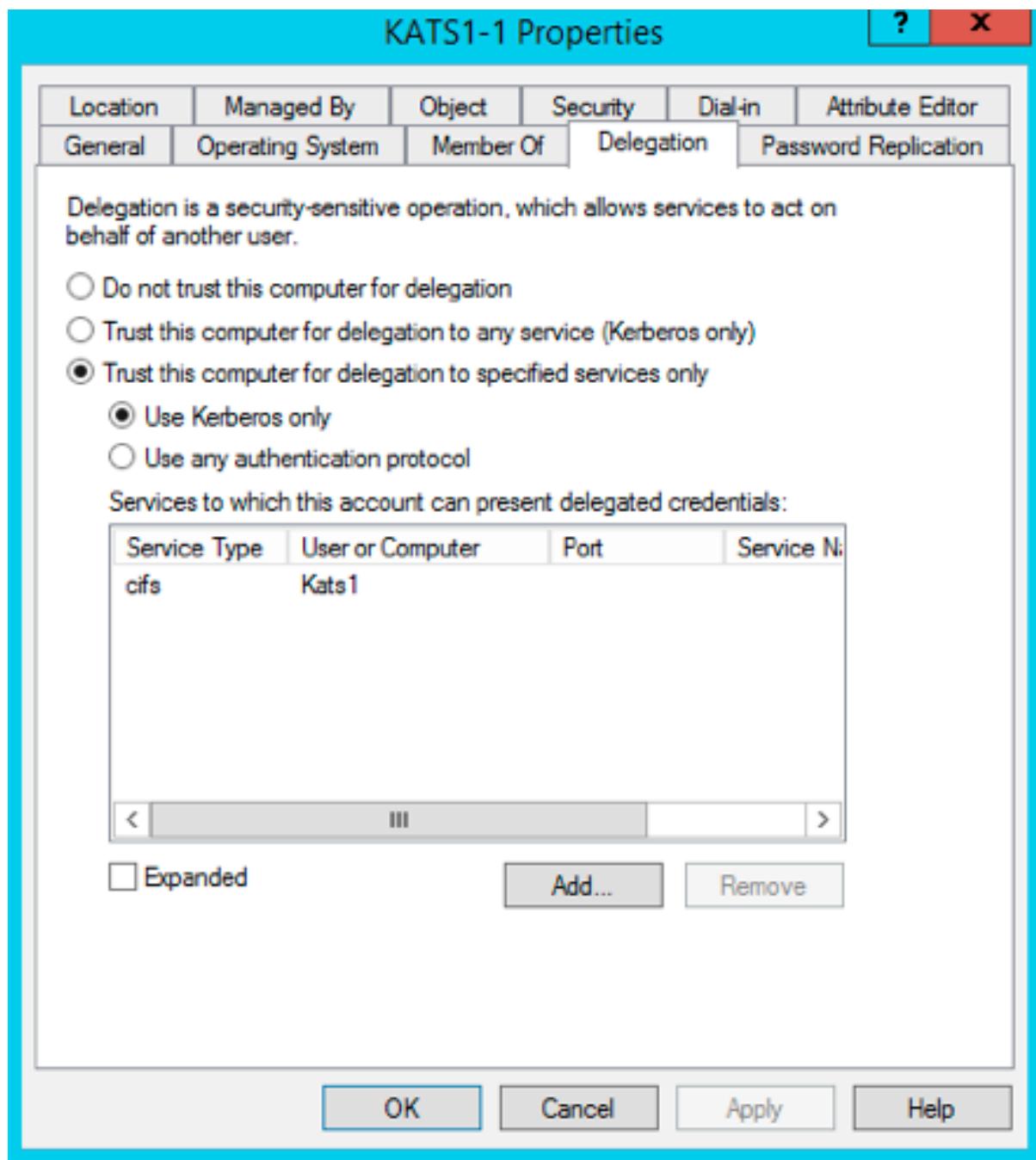


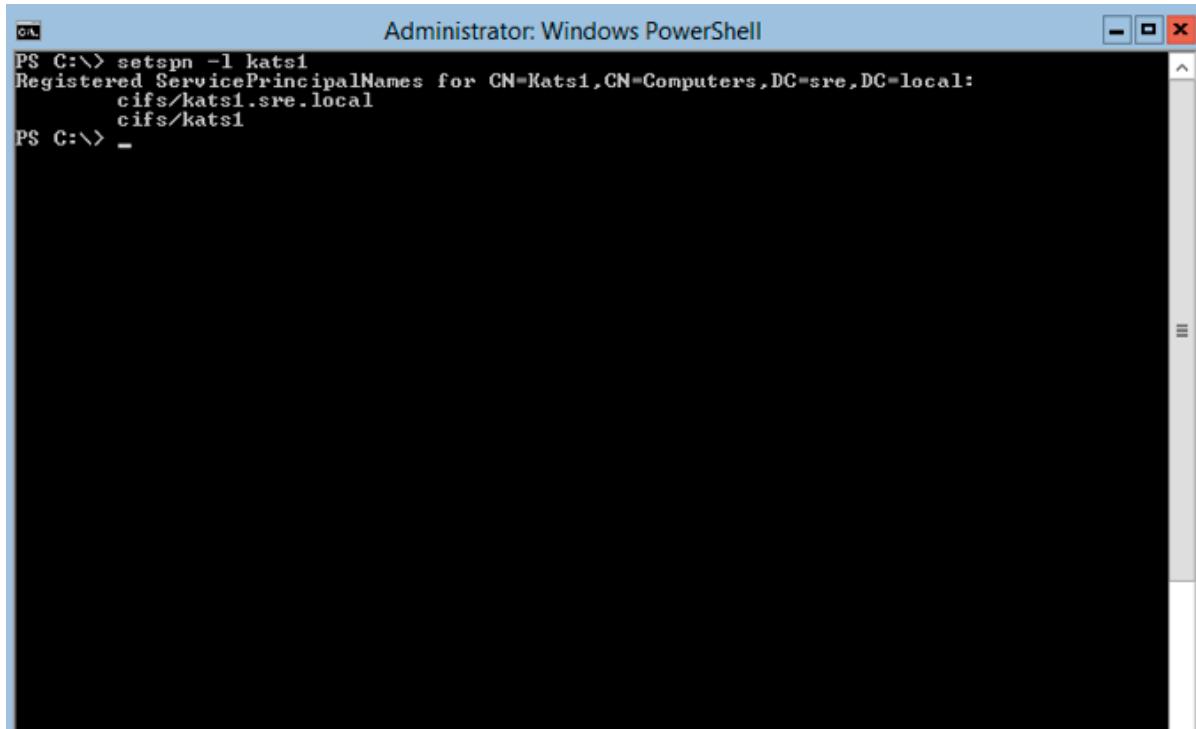
Figure: Adding the cifs of the Nutanix storage cluster object

4. 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.

An output similar to the following is displayed.

A screenshot of an Administrator: Windows PowerShell window. The command 'setspn -l kats1' is run, and the output shows registered ServicePrincipalNames for the object CN=Kats1,CN=Computers,DC=sre,DC=local, specifically cifs/kats1.sre.local and cifs/kats1.

```
Administrator: Windows PowerShell
PS C:\> setspn -l kats1
Registered ServicePrincipalNames for CN=Kats1,CN=Computers,DC=sre,DC=local:
  cifs/kats1.sre.local
  cifs/kats1
PS C:\> _
```

Figure: SPN Registration

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/kats1 kats1
> Setspn -S cifs/kats1.sre.local kats1
```

## Security Management

Nutanix provides several mechanisms to maintain security in a cluster.

- User accounts control access, and the web console allows you to set the authentication method (see [Configuring Authentication](#) on page 604).
- Nutanix uses SSL to secure communication with a cluster, and the web console allows you to install SSL certificates (see [Installing an SSL Certificate](#) on page 612).
- Nutanix supports key-based SSH access to a cluster, but you have the option to disable such access (see [Controlling Cluster Access](#) on page 615).
- Nutanix provides an option to configure the cluster for enhanced data-at-rest security through the use of self-encrypting drives (see [Data-at-Rest Encryption](#) on page 616).

### Configuring Authentication

Nutanix supports user authentication. To configure authentication types and directories and to enable client authentication or to enable client authentication only, do the following:



**Caution:** The web console (and nCLI) does not allow the use of the not secure SSLv2 and SSLv3 ciphers. To eliminate the possibility of an SSL Fallback situation and denied access to the web console, disable (uncheck) SSLv2 and SSLv3 in any browser used for access. However, TLS must be enabled (checked).

1. In the gear icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Authentication**.

The *Authentication Configuration* window appears.

The screenshot shows the 'Authentication Configuration' window with the following interface elements and data:

- Header:** 'Authentication Configuration' with a gear icon, a question mark icon, and a close button.
- Toolbar:** 'Directory List' (highlighted with a red box and a 'select' callout), 'Authentication Types', and 'Client'.
- Buttons:** '+ New Directory' (highlighted with a red box and an 'add' callout), 'edit' (with a red arrow pointing to it), and 'delete' (with a red arrow pointing to it).
- Table:** A list of authentication directories with columns: NAME, DOMAIN, URL, and TEST.
- Data:**

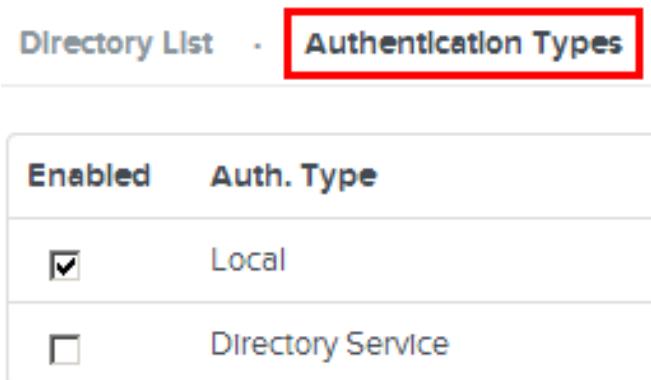
NAME	DOMAIN	URL	TEST
domain1	domain1.example.com	ldap://domain.example.com	Test
domain2	domain2.example.com	ldaps://domain2.example.com	Test
- Buttons:** 'Close' at the bottom right.

Figure: Authentication Window

 **Note:** The following steps combine three distinct procedures, enabling authentication (step 2), configuring one or more directories for LDAP/S authentication (steps 3-5), and enabling client authentication (step 6). Perform the steps for the procedures you need. For example, perform step 6 only if you intend to enforce client authentication.

2. To enable server authentication, click the **Authentication Types** tab and then check the box for either **Local** or **Directory Service** (or both). After selecting the authentication types, click the **Save** button.

The **Local** setting uses the local authentication provided by Nutanix (see [User Management](#) on page 626). This method is employed when a user enters just a login name without specifying a domain (for example, `user1` instead of `user1@nutanix.com`). The **Directory Service** setting validates `user@domain` entries and validates against the directory specified in the **Directory List** tab. Therefore, you need to configure an authentication directory if you select **Directory Service** in this field.



The screenshot shows a window titled "Authentication Types". At the top, there are two tabs: "Directory List" and "Authentication Types", with "Authentication Types" being the active tab and highlighted with a red border. Below the tabs is a table with two columns: "Enabled" and "Auth. Type". There are two rows: the first row has a checked checkbox in the "Enabled" column and the text "Local" in the "Auth. Type" column; the second row has an unchecked checkbox in the "Enabled" column and the text "Directory Service" in the "Auth. Type" column.

Enabled	Auth. Type
<input checked="" type="checkbox"/>	Local
<input type="checkbox"/>	Directory Service

Figure: Authentication Window: Authentication Types

 **Note:** The Nutanix admin user can log on to the management interfaces, including the web console, even if the **Local** authentication type is disabled.

3. To add an authentication directory, click the **Directory List** tab and then the **New Directory** button. A set of fields is displayed. Do the following in the indicated fields:

- a. **Name:** Enter a directory name.

This is a name you choose to identify this entry; it need not be the name of an actual directory.

- b. **Domain:** Enter the domain name.

Enter the domain name in DNS format, for example, `nutanix.com`.

- c. **Directory URL:** Enter the URL address to the directory.

The URL format is as follows for an LDAP entry (the only type supported currently):

`ldap://host:Ldap_port_num`. The host value is either the IP address or fully qualified domain name. The default LDAP port number is 389. Nutanix also supports LDAPS (port 636) and LDAP/S Global Catalog (ports 3268 and 3269). The following are example configurations appropriate for each port option:



**Note:** LDAPS support does not require custom certificates or certificate trust import.

- Port 389 (LDAP). Use this port number (in the following URL form) when the configuration is single domain, single forest, and not using SSL.  
`ldap://ad_server.mycompany.com:389`
- Port 636 (LDAPS). Use this port number (in the following URL form) when the configuration is single domain, single forest, and using SSL. This requires all Active Directory Domain Controllers have properly installed SSL certificates.  
`ldaps://ad_server.mycompany.com:636`
- Port 3268 (LDAP - GC). Use this port number when the configuration is multiple domain, single forest, and not using SSL.
- Port 3269 (LDAPS - GC). Use this port number when the configuration is multiple domain, single forest, and using SSL.



**Note:** When constructing your LDAP/S URL to use a Global Catalog server, ensure that the Domain Control IP address or name being used is a global catalog server within the domain being configured. If not, queries over 3268/3269 may fail.

**d. Directory Type:** Select **Active Directory** from the pull-down list.

Active Directory (AD) is a directory service implemented by Microsoft for Windows domain networks. It is the only option currently available.



**Note:**

- Users with the "User must change password at next logon" attribute enabled will not be able to authenticate to the web console (or nCLI). Ensure users with this attribute first login to a domain workstation and change their password prior to accessing the web console. Also, if SSL is enabled on the Active Directory server, make sure that Nutanix has access to that port (open in firewall).
- 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 the [Internationalization \(i18n\)](#) on page 593 section.

**e. Connection Type:** Select **LDAP** from the pull-down list.

Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining distributed directory information services. It is the only option currently available.

**f. When all the fields are correct, click the **Save** button (lower right).**

This saves the configuration and redisplays the Authentication Configuration dialog box. The configured directory now appears in the **Directory List** tab.

**g. Repeat this step for each authentication directory you want to add.**



**Note:** All users in an authenticated directory are granted full administrator permissions by default. You can refine the granted permissions by specifying roles for the users in that directory (see [Assigning Role Permissions](#) on page 610).

The screenshot shows a web-based configuration interface for authentication. At the top, there are tabs: 'Directory List' (which is highlighted with a red border), 'Authentication Types', and 'Client'. Below these tabs, there are several input fields and dropdown menus. The 'Name' field is empty. The 'Domain' field is also empty. The 'Directory URL' field is empty. Under 'Directory Type', the option 'Active Directory' is selected. Under 'Connection Type', the option 'LDAP' is selected. The overall layout is clean and organized, typical of a network management or configuration tool.

Figure: Authentication Window: Directory List

4. To edit a directory entry, click the **Directory List** tab and then click the pencil icon for that entry. After clicking the pencil icon, the Directory List fields reappear (see step 3). Enter the new information in the appropriate fields and then click the **Save** button.
5. To delete a directory entry, click the **Directory List** tab and then click the X icon for that entry. After clicking the X icon, a window prompt appears to verify the delete action; click the **OK** button. The entry is removed from the list.
6. To enable client authentication, do the following:
  - a. Click the **Client** tab.
  - b. Select the **Configure Client Chain Certificate** check box.

The screenshot shows the 'Client' tab selected in the navigation bar. Below the tab, there is a single checkbox labeled 'Configure Client Chain Certificate'. A note below the checkbox states: 'Forces the authentication of all clients of the REST API (including the Prism UI and NCLI). Requires a client chain certificate.' The overall interface is simple and focused on enabling specific security features.

Figure: Authentication Window: Client Tab (1)

- c. Click the **Choose File** button, browse to and select a client chain certificate to upload, and then click the **Open** button to upload the certificate.

**Note:** Uploaded certificate files must be PEM encoded. The web console restarts after the upload step.

Configure Client Chain Certificate  
Force the authentication of all clients of the REST API (including the Prism UI and NCLI).  
Requires a client chain certificate.

CLIENT CHAIN CERTIFICATE

No file chosen

Figure: Authentication Window: Client Tab (2)

d. To enable client authentication, click **Enable Client Authentication**.

e. To modify client authentication, do one of the following:

 **Note:** The web console restarts when you change these settings.

- Click **Enable Client Authentication** to disable client authentication.
- Click **Remove** to delete the current certificate. (This also disables client authentication.)

Configure Client Chain Certificate  
Force the authentication of all clients of the REST API (including the Prism UI and NCLI).  
Requires a client chain certificate.

CLIENT CHAIN CERTIFICATE

UNIVERSAL\_CA\_CHAIN.CER

Enable Client Authentication

Figure: Authentication Window: Client Tab (3)

Client authentication ensures that the Nutanix cluster gets a valid certificate from the user. Normally, a one-way authentication process occurs where the server provides a certificate so the user can verify the authenticity of the server (see [Installing an SSL Certificate](#) on page 612). When client authentication is enabled, this becomes a two-way authentication where the server also verifies the authenticity of the user. A user must provide a valid certificate when accessing the console either by installing the certificate on his or her local machine or by providing it through a smart card reader.

-  **Note:** The CA must be the same for both the client chain certificate and the certificate on the local machine or smart card.
-  **Note:** Client authentication is not available on Prism Central (see [Multi-Cluster Management](#) on page 105).

7. To specify a service account that the web console can use to log in to Active Directory and authenticate Common Access Card (CAC) users, select the **Configure Service Account** check box, and then do the following in the indicated fields:

Enable Client Authentication

Configure Service Account [Edit](#)

Configure to enable swipe access authentication instead of two-step token authentication.

DIRECTORY
AD1
SERVICE USERNAME
<input type="text" value="user.name@domain.com"/>
SERVICE PASSWORD
<input type="password"/>

**Note:** Enabling CAC Authentication will also enable Client Authentication.

Enable CAC Authentication

Figure: Common Access Card Authentication

- a. **Directory:** Select the authentication directory that contains the CAC users that you want to authenticate.  
This list includes the directories that are configured on the **Directory List** tab.
- b. **Service Username:** Enter the user name in the *user.name@domain.com* format that you want the web console to use to log in to the Active Directory.
- c. **Service Password:** Enter the password for the service user name.
- d. Click **Enable CAC Authentication**.



**Note:** The web console restarts after you change this setting.

If you map a Prism role to a CAC user and not to an Active Directory group or organizational unit to which the user belongs, specify the EDIPI (User Principal Name, or UPN) of that user in the role mapping. A user who presents a CAC with a valid certificate is mapped to a role and taken directly to the web console home page. The web console login page is not displayed.

 **Note:** If you have logged on to Prism by using CAC authentication, to successfully log out of Prism, close the browser after you click **Log Out**.

8. Click the **Close** button to close the *Authentication Configuration* dialog box.

## Assigning Role Permissions

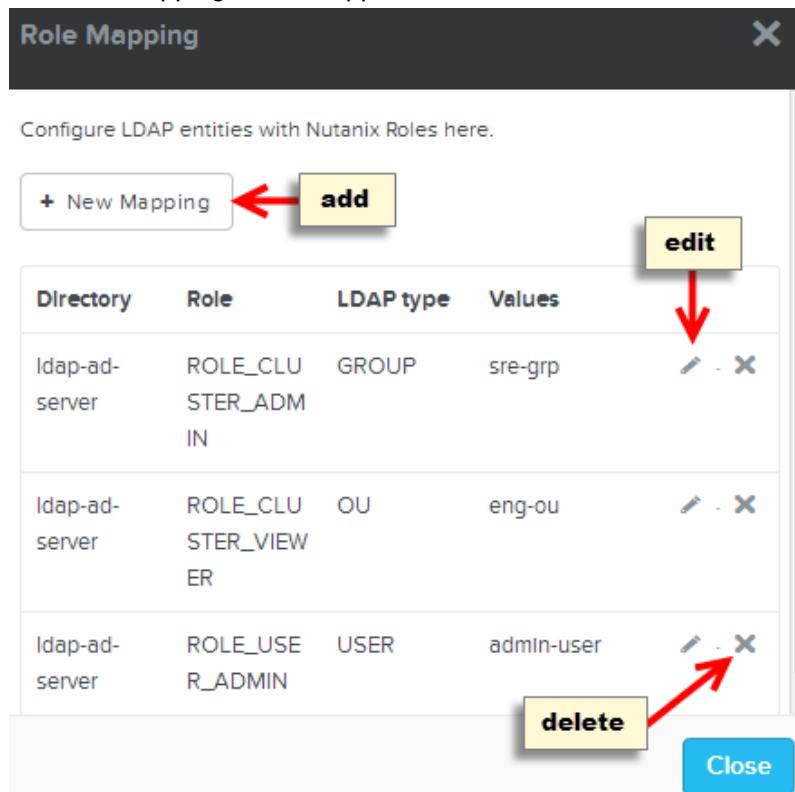
When user authentication is enabled for a directory service (see [Configuring Authentication](#) on page 604), all authorized users have full administrator permissions by default. You must refine the authentication process by assigning a role (with associated permissions) to organizational units (OUs), groups, or individuals within a directory.

If you are using Active Directory, you must also assign roles to entities or users, especially before upgrading from a previous AOS version.

To assign roles, do the following:

1. In the gear icon  pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Role Mapping**.

The *Role Mapping* window appears.



Directory	Role	LDAP type	Values	Actions
ldap-ad-server	ROLE_CLU	GROUP	sre-grp	 
ldap-ad-server	ROLE_CLU	OU	eng-ou	 
ldap-ad-server	ROLE_USE	USER	admin-user	 

Figure: Role Mapping Window

2. To create a role mapping, click the **New Mapping** button.

The *Create Role Mapping* window appears. Do the following in the indicated fields:

- a. **Directory:** Select the target directory from the pull-down list.

Only directories previously defined when configuring authentication appear in this list. If the desired directory does not appear, add that directory to the directory list (see [Configuring Authentication](#) on page 604) and then return to this procedure.

- b. **LDAP Type:** Select the desired LDAP entity type from the pull-down list.

The entity types are **GROUP**, **USER**, and **OU**.

- c. **Role:** Select the user role from the pull-down list.

There are three roles from which to choose:

- **Viewer:** This role allows a user to view information only. It does not provide permission to perform any administrative tasks.
- **Cluster Admin:** This role allows a user to view information and perform any administrative task (but not create or modify user accounts).
- **User Admin:** This role allows the user to view information, perform any administrative task, and create or modify user accounts.

- d. **Values:** Enter the case-sensitive entity names (in a comma separated list with no spaces) that should be assigned this role.

The values are the actual names of the organizational units (meaning it applies to all users in those OUs), groups (all users in those groups), or users (each named user) assigned this role. For example, entering value "admin-gp, support-gp" when the LDAP type is **GROUP** and the role is **Cluster Admin** means all users in the admin-gp and support-gp groups should be assigned the cluster administrator role.



**Note:** Do not include a domain in the value, for example enter just admin-gp, not admin-gp@nutanix.com. However, when users log into the web console, they need to include the domain in their user name (see [Logging Into the Web Console](#) on page 29).

- e. When all the fields are correct, click **Save**.

This saves the configuration and redisplays the *Role Mapping* window. The new role map now appears in the list.



**Note:** All users in an authorized service directory have full administrator permissions when role mapping is not defined for that directory. However, after creating a role map, any users in that directory that are not explicitly granted permissions through the role mapping are denied access (no permissions).

- f. Repeat this step for each role map you want to add.

You can create a role map for each authorized directory. You can also create multiple maps that apply to a single directory. When there are multiple maps for a directory, the most specific rule for a user applies. For example, adding a **GROUP** map set to **Cluster Admin** and a **USER** map set to **Viewer** for select users in that group means all users in the group have administrator permission except those specified users who have viewing permission only.

**Create Role Mapping**

Enter the attributes for this role mapping.

Directory	ad-server1
LDAP Type	GROUP
Role	Cluster Admin
Values	qa-group,eng-group

Figure: Create Role Mapping Window

3. To edit a role map entry, click the pencil icon  for that entry. After clicking the pencil icon, the *Edit Role Mapping* window appears, which contains the same fields as the *Create Role Mapping* window (see step 2). Enter the new information in the appropriate fields and then click the **Save** button.
4. To delete a role map entry, click the "X" icon for that entry. After clicking the X icon, a window prompt appears to verify the delete action; click the **OK** button. The entry is removed from the list.
5. Click the **Close** button to close the *Role Mapping* window.

## Installing an SSL Certificate

Nutanix supports SSL certificate-based authentication for console access. To install a self-signed or custom SSL certificate, do the following:



**Note:** Nutanix recommends that customers replace the default self-signed certificate with a CA signed certificate. The [Controller VM Security Operations Guide](#) includes more information about certificates, such as generating a private key and certificate signing request (CSR).

1. In the gear icon  pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **SSL Certificate** to open the *SSL Certificate* dialog box.
2. To replace (or install) a certificate, click the **Replace Certificate** button.

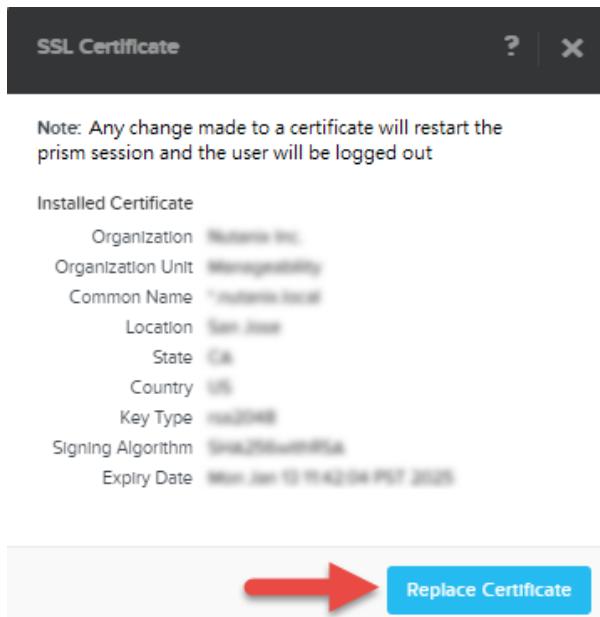


Figure: SSL Certificate Window

3. To create a new self-signed certificate, click the **Regenerate Self Signed Certificate** option and then click the **Apply** button.

A dialog box appears to verify the action; click the **OK** button. This generates and applies a new RSA 2048-bit self-signed certificate for the Prism user interface.

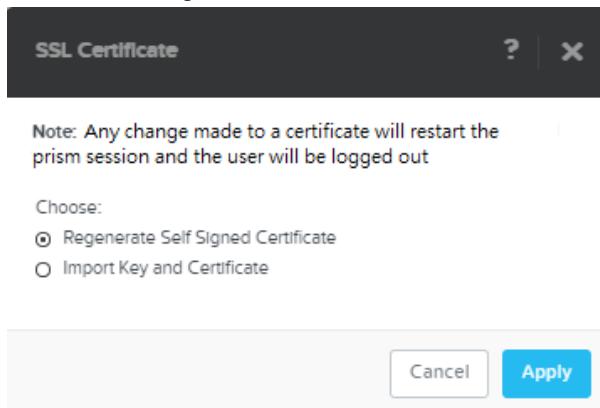


Figure: SSL Certificate Window: Regenerate

4. To apply a custom certificate that you provide, do the following:

- a. Click the **Import Key and Certificate** option and then click the **Next** button.

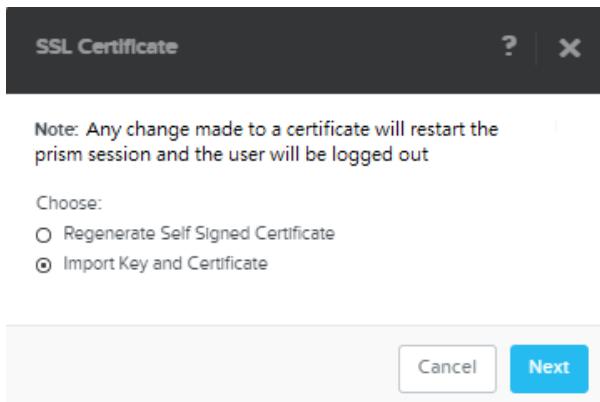


Figure: SSL Certificate Window: Import

- b. Do the following in the indicated fields, and then click the **Import Files** button.

**Note:** All three imported files for the custom certificate must be PEM encoded.

- **Private Key Type:** Select the appropriate type for the signed certificate from the pull-down list (RSA 2048 bit, EC DSA 256 bit, or EC DSA 384 bit).
- **Private Key:** Click the **Browse** button and select the private key associated with the certificate to be imported.
- **Public Certificate:** Click the **Browse** button and select the signed public portion of the server certificate corresponding to the private key.
- **CA Certificate/Chain:** Click the **Browse** button and select the certificate or chain of the signing authority for the public certificate.

The screenshot shows the "SSL Certificate" window again. It includes a note about RSA 2048 bit guidelines and dropdown menus for selecting file types. The "PRIVATE KEY TYPE" dropdown is set to "RSA 2048 bit". Below it are sections for "PRIVATE KEY", "PUBLIC CERTIFICATE", and "CA CERTIFICATE/CHAIN", each with a "Choose File" button and a "No file chosen" message. At the bottom right are "Cancel" and "Import Files" buttons.

Figure: SSL Certificate Window: Select Files

In order to meet the high security standards of NIST SP800-131a compliance, the requirements of the RFC 6460 for NSA Suite B, and supply the optimal performance for encryption, the certificate import process validates the correct signature algorithm is used for a given key/cert pair. Refer to the following table to ensure the proper set of key types, sizes/curves, and signature algorithms. These are the ONLY supported configurations. All private keys must follow the supported list, and the CA must sign all public certificates with proper type, size/curve, and signature algorithm for the import process to validate successfully.

### Supported Key Configurations

Key Type	Size/Curve	Signature Algorithm
RSA	2048	SHA256-with-RSAEncryption
EC DSA 256	prime256v1	ecdsa-with-sha256
EC DSA 384	secp384r1	ecdsa-with-sha384

You can use the `cat` command to concatenate a list of CA certificates into a chain file.

```
$ cat signer.crt inter.crt root.crt > server.cert
```

Order is essential. The total chain should begin with the certificate of the signer and end with the root CA certificate as the final entry.

**Results:** After generating or uploading the new certificate, the interface gateway restarts. If the certificate and credentials are valid, the interface gateway uses the new certificate immediately, which means your browser session (and all other open browser sessions) will be invalid until you reload the page and accept the new certificate. If anything is wrong with the certificate (such as a corrupted file or wrong certificate type), the new certificate is discarded, and the system reverts back to the original default certificate provided by Nutanix.



**Note:** The system holds only one custom SSL certificate. If a new certificate is uploaded, it replaces the existing certificate. The previous certificate is discarded.

## Controlling Cluster Access

Key-based SSH access to a cluster is supported. Adding a key through the Prism web console provides key-based access to the cluster, Controller VM, and hypervisor host. Each node employs a public/private key pair, and the cluster is made secure by distributing and using these keys. Create a key pair (or multiple key pairs) and add the public keys to enable key-based SSH access. However, when site security requirements do not allow such access, you can remove all public keys to prevent SSH access.

To control key-based SSH access to the cluster, do the following:



**Note:** Use this procedure to lock down access to the Controller VM and hypervisor host. In addition, it is possible to lock down access to the hypervisor.

1. In the gear icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Cluster Lockdown**.  
The *Cluster Lockdown* dialog box appears. Enabled public keys (if any) are listed in this window.

2. To disable (or enable) remote login access, uncheck (check) the **Enable Remote Login with Password** box.  
Remote login access is enabled by default.
  3. To add a new public key, click the **New Public Key** button and then do the following in the displayed fields:
    - a. **Name:** Enter a key name.
    - b. **Key:** Enter (paste) the key value into the field.
    - c. Click the **Save** button (lower right) to save the key and return to the main *Cluster Lockdown* window.

There are no public keys available by default, but you can add any number of public keys.
  4. To delete a public key, click the **X** on the right of that key line.
-  **Note:** Deleting all the public keys and disabling remote login access locks down the cluster from SSH access.
5. Click the **Close** button to close the *Cluster Lockdown* window.

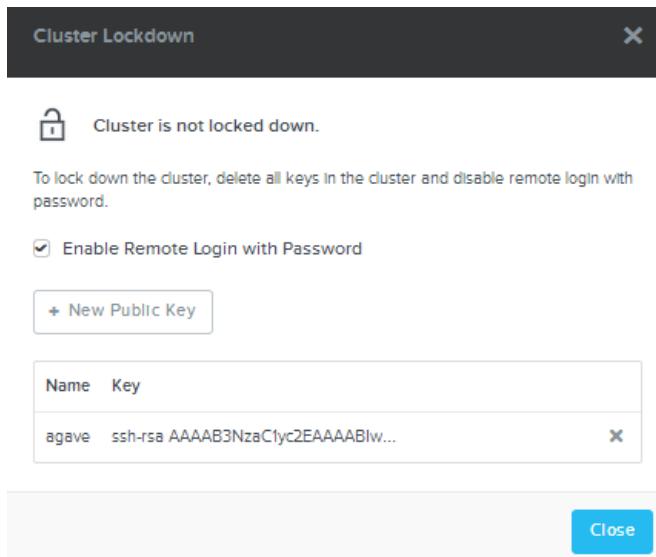


Figure: Cluster Lockdown Window

## Data-at-Rest Encryption

Nutanix provides an option to secure data while it is at rest using self encrypted drives and key-based access management.

For customers who require enhanced data security, Nutanix provides a data-at-rest security option that supports the following features:

- Data is encrypted on all drives at all times.
- Data is inaccessible in the event of drive or node theft.
- Data on a drive can be securely destroyed.
- A key authorization method allows password rotation at arbitrary times.
- Protection can be enabled or disabled at any time.
- No performance penalty is incurred despite encrypting all data.



**Note:** This solution provides enhanced security for data on a drive, but it does not secure data in transit.

## Data Encryption Model

To accomplish these goals, Nutanix implements a data security configuration that uses self-encrypting drives (SEDs) with keys maintained through a separate key management device. Nutanix uses open standards (TCG and KMIP protocols) and FIPS validated SED drives for interoperability and strong security.

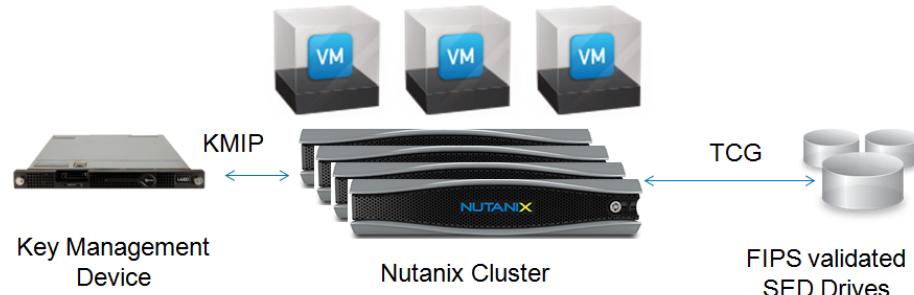


Figure: Cluster Protection Overview

This configuration involves the following workflow:

1. The security implementation begins by installing SEDs for all data drives in a cluster.

The drives are FIPS 140-2 Level 2 validated and use FIPS 140-2 validated cryptographic modules.

It is easiest to create a new cluster that includes SED data drives only, but an existing cluster can be converted to support data-at-rest encryption by replacing the existing drives with SEDs (after migrating all the VMs/vDisks off of the cluster while the drives are being replaced).



**Note:** Contact Nutanix customer support for assistance before attempting to convert an existing cluster. A non-protected cluster can contain both SED and standard drives, but Nutanix does not support a mixed cluster when protection is enabled. All the disks in a protected cluster must be SED drives.

2. Data on the drives is always encrypted, but read or write access to that data is open by default.

However, when data protection for the cluster is enabled, the Controller VM must provide the proper key to access data on a SED. The Controller VM communicates with the SEDs through a Trusted Computing Group (TCG) Security Subsystem Class (SSC) Enterprise protocol.

A symmetric data encryption key (DEK) such as AES 256 is applied to all data being written to or read from the disk. The key is known only to the drive controller and never leaves the physical subsystem, so there is no way to access the data directly from the drive.

Another key, known as a key encryption key (KEK), is used to encrypt/decrypt the DEK and authenticate to the drive. (Some vendors call this the authentication key or PIN.)

Each drive has a separate KEK that is generated through the FIPS compliant random number generator present in the drive controller. The KEK is 32 bytes long to resist brute force attacks. The KEKs are sent to the key management server for secure storage and later retrieval; they are not stored locally on the node (even though they are generated locally).

Each node maintains a set of certificates and keys in order to establish a secure connection with the key management server.

3. Keys are stored in a key management server that is outside the cluster, and the Controller VM communicates with the key management server using the Key Management Interoperability Protocol (KMIP) to upload and retrieve drive keys.

Only one key management server device is required, but it is recommended that multiple devices are employed so the key management server is not a potential single point of failure. Configure the key manager server devices to work in clustered mode so they can be added to the cluster configuration as a single entity that is resilient to a single failure.

- When a node experiences a full power off and power on (and cluster protection is enabled), the controller VM retrieves the drive keys from the key management server and uses them to unlock the drives.

If the Controller VM cannot get the correct keys from the key management server, it cannot access data on the drives.

If a drive is re-seated, it becomes locked.

If a drive is stolen, the data is inaccessible without the KEK (which cannot be obtained from the drive). If a node is stolen, the key management server can revoke the node certificates to ensure they cannot be used to access data on any of the drives.

## Preparing for Data-at-Rest Encryption

Because data-at-rest encryption relies on a key management server outside the Nutanix cluster, preparation steps outside the web console are required.

You can perform steps 2, 4, and 5 through the web console (see [Configuring Data-at-Rest Encryption](#) on page 619). Steps 1 and 3 must come from the key management server and a Certificate Authority (CA).

Nutanix does not provide a key management server but supports key management servers from several vendors including SafeNet KeySecure and Vormetric. See the *Acropolis Release Notes* for a complete list of the supported key management servers. For instructions on how to configure a key management server, refer to the documentation from the appropriate vendor.

### 1. Configure a key management server.

The key management server devices must be configured into the network so the cluster has access to those devices. For redundant protection, it is recommended that you employ at least two key management server devices, either in active-active cluster mode or stand-alone.



**Note:** The key management server must support KMIP version 1.0 or later.



**Caution:** Do not host a key management server VM on the encrypted cluster that is using it.

→ SafeNet

Ensure that **Security > High Security > Key Security > Disable Creation and Use of Global Keys** is checked.

→ Vormetric

Set the appliance to compatibility mode. Suite B mode causes the SSL handshake to fail.

### 2. Generate a certificate signing request (CSR) for each node in the cluster.

- The **Common Name** field of the CSR is populated automatically with `unique_node_identifier.nutanix.com` to identify the node associated with the certificate.



**Note:** If a custom common name (CN) is needed, contact Nutanix customer support for assistance.

- A **UID** field is populated with a value of **Nutanix**. This can be useful when configuring a Nutanix group for access control within a key management server, since it is based on fields within the client certificates.



**Note:** Some vendors when doing client certificate authentication expect the client **username** to be a field in the CSR. While the CN and UID are pre-generated, many of the user populated fields can be used instead if desired. If a node-unique field such as CN is chosen, users must be created on a per node basis for access control. If a cluster-unique field is chosen, customers must create a user for each cluster.

### 3. Send the CSRs to a certificate authority (CA) and get them signed.

→ Safenet

The SafeNet KeySecure key management server includes a local CA option to generate signed certificates, or you can use other third-party vendors to create the signed certificates.

To enable FIPS compliance, add user nutanix to the CA that signed the CSR. Under **Security > High Security > FIPS Compliance** click **Set FIPS Compliant**.



**Note:** Some CAs strip the **UID** field when returning a signed certificate.

### 4. Upload the signed SSL certificates (one for each node) and the certificate for the CA to the cluster. These certificates are used to authenticate with the key management server.

### 5. Generate keys (KEKs) for the SED drives and upload those keys to the key management server.

## Configuring Data-at-Rest Encryption

Nutanix offers an option to use self-encrypting drives (SEDs) to store data in a cluster. When SEDs are used, there are several configuration steps that must be performed to support data-at-rest encryption in the cluster.

**Before you begin:** A separate key management server is required to store the keys outside of the cluster. Each key management server device must be configured and addressable through the network. It is recommended that multiple key manager server devices be configured to work in clustered mode so they can be added to the cluster configuration as a single entity (see step 4) that is resilient to a single failure.

To configure cluster encryption, do the following:

1. In the gear icon pull-down list of the main menu (see *Main Menu Options* on page 32), select **Data-at-Rest Encryption**.

The *Data-at-Rest Encryption* page appears. Initially, encryption is not configured, and a message to that effect appears.

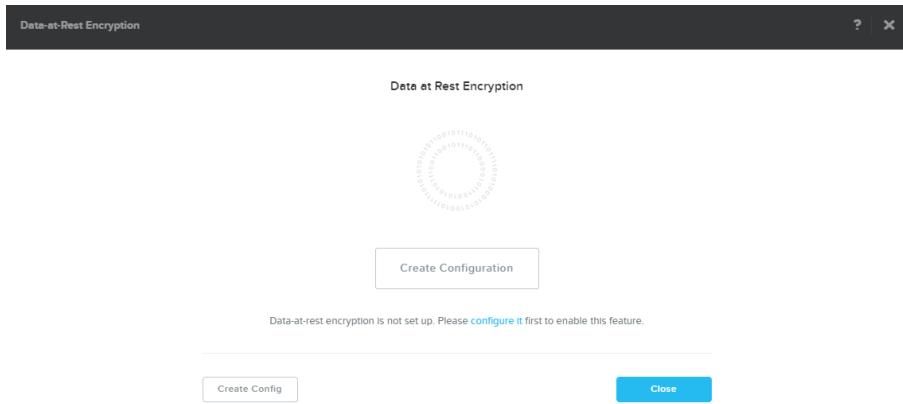


Figure: Data-at-Rest Encryption Screen (initial)

**2. Click the Create Configuration button.**

Clicking the **Continue Configuration** button, **configure it** link, or **Edit Config** button does the same thing, which is display the Data-at-Rest Encryption configuration page.

**3. In the Certificate Signing Request Information section, do the following:**

EMAIL ginger@nutanix.com	ORGANIZATION ntnx	ORGANIZATIONAL UNIT OU
COUNTRY CODE US	CITY la	STATE CA

Figure: Certificate Signing Request Section

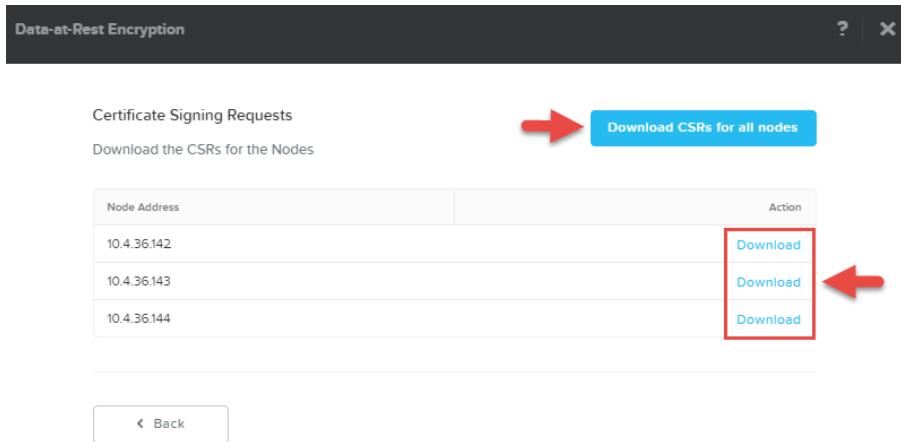
- a. Enter appropriate credentials for your organization in the **Email**, **Organization**, **Organizational Unit**, **Country Code**, **City**, and **State** fields and then click the **Save CSR Info** button.**

The entered information is saved and is used when creating a certificate signing request (CSR). To specify more than one **Organization Unit** name, enter a comma separated list.



**Note:** You can update this information until an SSL certificate for a node is uploaded to the cluster, at which point the information cannot be changed (the fields become read only) without first deleting the uploaded certificates.

- b. Click the **Download CSRs** button, and then in the new screen click the **Download CSRs for all nodes** to download a file with CSRs for all the nodes or click a **Download** link to download a file with the CSR for that node.**



*Figure: Download CSRs Screen*

- Send the files with the CSRs to the desired certificate authority.

The certificate authority creates the signed certificates and returns them to you. Store the returned SSL certificates and the CA certificate where you can retrieve them in step 5.

- The certificates must be X.509 format. (DER, PKCS, and PFX formats are not supported.)
- The certificate and the private key should be in separate files.

#### 4. In the *Key Management Server* section, do the following:

The screenshot shows a table with one row for 'kms1'. The 'Status' column shows 'Upload' and the 'Address' column shows '10.1.40.22 : 5696'. A red arrow points to the 'Manage Certificates' link in the 'Actions' column. Another red arrow points to the 'Add New Key Management Server' button at the bottom left.

*Figure: Key Management Server Section*

- Click the **Add New Key Management Server** button.
- In the *Add a New Key Management Server* screen, enter a name, IP address, and port number for the key management server in the appropriate fields.  
The port is where the key management server is configured to listen for the KMIP protocol. The default port number is 5696.
  - If you have configured multiple key management servers in cluster mode, click the **Add Address** button to provide the addresses for each key management server device in the cluster.
  - If you have stand-alone key management servers, click the **Save** button. Repeat this step (**Add New Key Management Server** button) for each key management server device to add.

**Note:** If your key management servers are configured into a master/slave (active/pассивный) relationship and the architecture is such that the slave cannot accept write requests, do not add the slave into this configuration. The system sends requests (read

(or write) to any configured key management server, so both read and write access is needed for key management servers added here.

**Note:** To prevent potential configuration problems, always use the **Add Address** button for key management servers configured into cluster mode. Only a stand-alone key management server should be added as a new server.

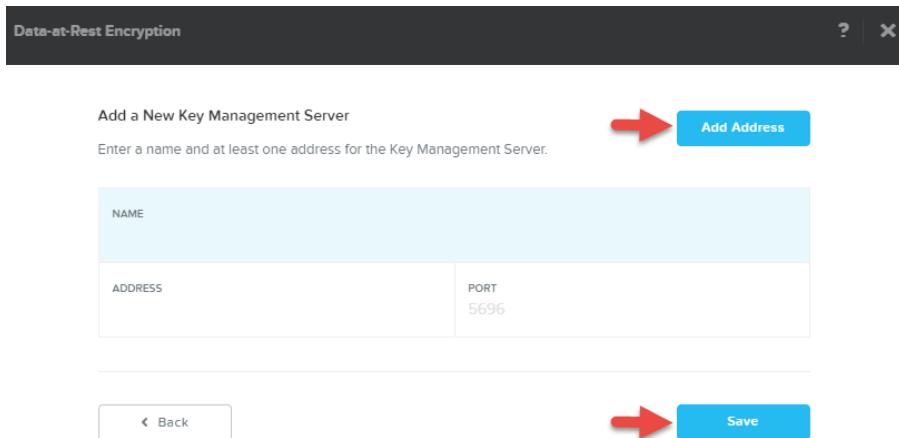


Figure: Add Key Management Server Screen

- c. To edit any settings, click the pencil icon for that entry in the key management server list to redisplay the add page and then click the **Save** button after making the change. To delete an entry, click the X icon.
5. In the *Add a New Certificate Authority* section, enter a name for the CA, click the **Upload CA Certificate** button, and select the certificate for the CA used to sign your node certificates (see step 3c). Repeat this step for all CAs that were used in the signing process.

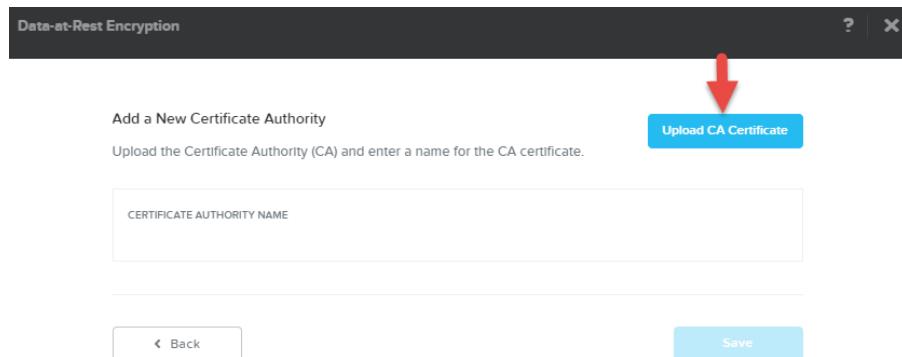
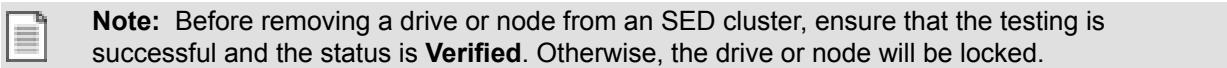
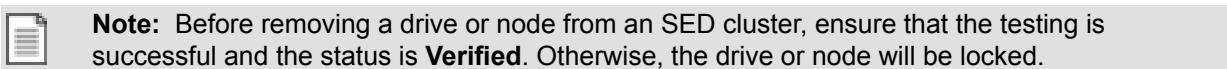


Figure: Certificate Authority Section

6. Go to the *Key Management Server* section (see step 4) and do the following:
  - a. Click the **Manage Certificates** button for a key management server.
  - b. In the *Manage Signed Certificates* screen, upload the node certificates either by clicking the **Upload Files** button to upload all the certificates in one step or by clicking the **Upload** link (not shown in the figure) for each node individually.
  - c. Test that the certificates are correct either by clicking the **Test all nodes** button to test the certificates for all nodes in one step or by clicking the **Test CS** (or **Re-Test CS**) link for each node individually. A status of **Verified** indicates the test was successful for that node.



- a. Repeat this step for each key management server.



The screenshot shows the 'Data-at-Rest Encryption' interface. At the top, there's a note about verifying drives/nodes. Below it, the 'Upload Signed Certificates' section has two main buttons: 'all nodes actions' (highlighted with a yellow box and red arrows) and 'single node actions' (highlighted with a red box and arrow). A table lists four nodes with their addresses, statuses (Waiting for Upload), and actions (Test CS • Delete). At the bottom are 'Back' and 'Submit' buttons.

Figure: Upload Signed Certificates Screen

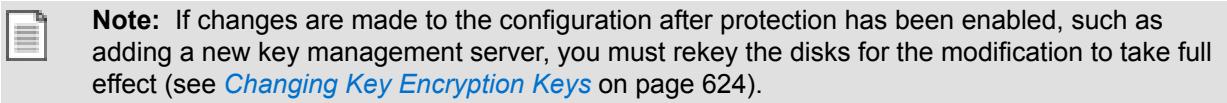
7. When the configuration is complete, click the **Protect** button on the opening page to enable encryption protection for the cluster.

A clear key icon appears on the page.

The screenshot shows the 'Cluster Encryption' interface. It features a key icon, a note about encrypting the cluster for safety, and a status message: 'Encryption State of Cluster: All disks are in an unprotected state'. At the bottom are 'Protect' and 'Edit Config' buttons, with a red arrow pointing to the 'Protect' button.

Figure: Data-at-Rest Encryption Screen (unprotected)

The key turns gold when cluster encryption is enabled.



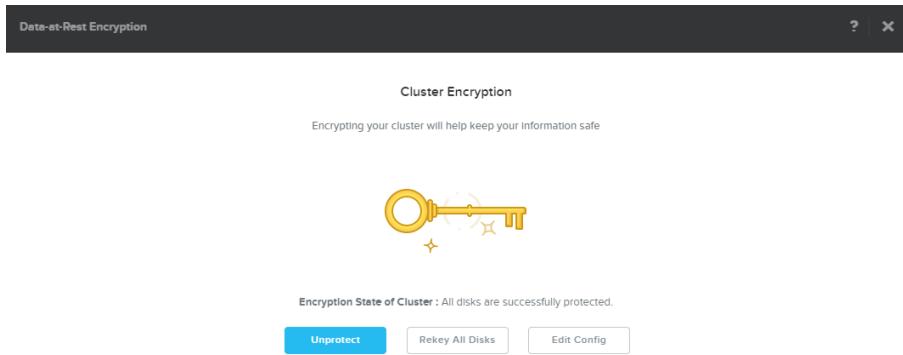


Figure: Data-at-Rest Encryption Screen (protected)

## Enabling/Disabling Encryption

Data on a self encrypting drive (SED) is always encrypted, but enabling/disabling data-at-rest encryption for the cluster determines whether a separate (and secured) key is required to access that data.

To enable or disable data-at-rest encryption after it has been configured for the cluster (see [Configuring Data-at-Rest Encryption](#) on page 619), do the following:



**Note:** The key management server must be accessible to disable encryption.

1. In the gear icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Data at Rest Encryption**.
2. In the *Cluster Encryption* page, do one of the following:
  - If cluster encryption is enabled currently, click the **Unprotect** button to disable it.
  - If cluster encryption is disabled currently, click the **Protect** button to enable it.

Enabling cluster encryption enforces the use of secured keys to access data on the SEDs in the cluster; disabling cluster encryption means the data can be accessed without providing a key.

## Changing Key Encryption Keys

The key encryption key (KEK) can be changed at any time. This can be useful as a periodic password rotation security precaution or when a key management server or node becomes compromised. If the key management server is compromised, only the KEK needs to be changed, because the KEK is independent of the drive encryption key (DEK). There is no need to re-encrypt any data, just to re-encrypt the DEK.

To change the KEKs for a cluster, do the following:

1. In the gear icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Data at Rest Encryption**.
2. In the *Cluster Encryption* page, press the **Rekey All Disks** button.  
This step resets the KEKs for all the self encrypting disks in the cluster.



**Note:** The **Rekey All Disks** button appears only when cluster protection is active.

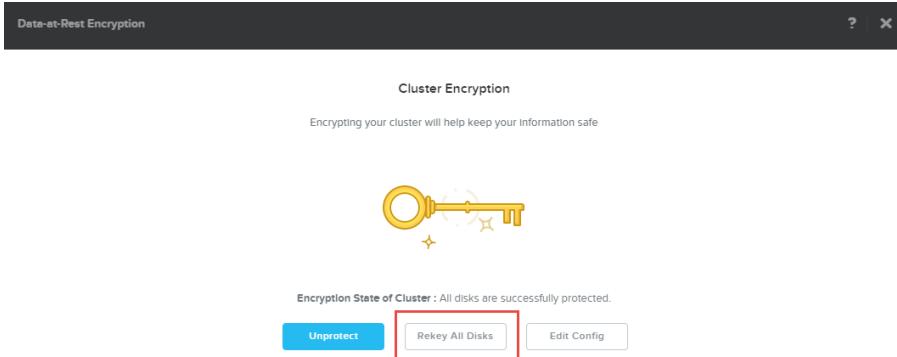
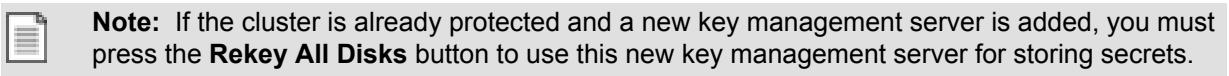


Figure: Cluster Encryption Screen

## Destroying Data on a SED

Data on a self encrypting drive (SED) is always encrypted, and the data encryption key (DEK) used to read the encrypted data is known only to the drive controller. All data on the drive can effectively be destroyed (that is, become permanently unreadable) by having the controller change the DEK. This is known as a crypto-erase.

To crypto-erase a SED, do the following:

1. Go to the Hardware dashboard and select the **Diagram** tab (see *Hardware Diagram View* on page 168).
2. Select the target disk in the diagram (upper section of screen) and then click the **Remove Disk** button (at the bottom right of the following diagram).

As part of the disk removal process, the DEK for that disk is automatically cycled on the drive controller. The previous DEK is lost and all new disk reads are indecipherable. The key encryption key (KEK) is unchanged, and the new DEK is protected using the current KEK.

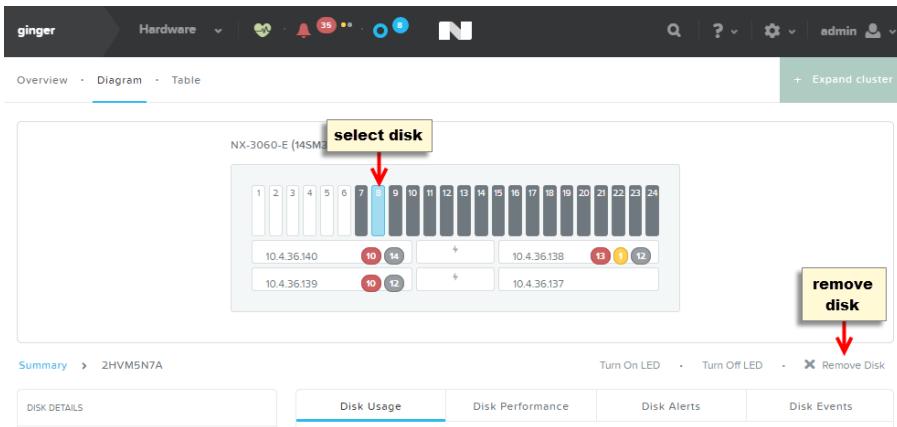
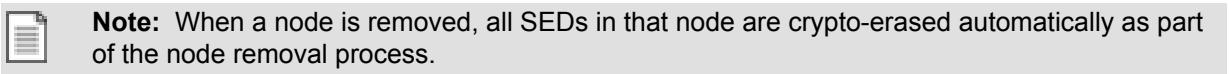


Figure: Removing a Disk

## User Management

Nutanix user accounts can be created or updated as needed.

- The web console allows you to add (see [Creating a User Account](#) on page 626), edit (see [Updating a User Account](#) on page 628), or delete (see [Deleting a User Account](#) on page 632) local user accounts at any time.
- You can also configure user accounts through Active Directory and LDAP (see [Configuring Authentication](#) on page 604). 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 the [Internationalization \(i18n\)](#) on page 593 section.



**Note:** In addition to the Nutanix user account, there are IPMI, Controller VM, and hypervisor host users. Passwords for these accounts cannot be changed through the web console.

### Creating a User Account

The admin user is created automatically when you get a Nutanix system, but you can add more users as needed. Note that you cannot delete the admin user. To create a new user, do the following:



**Note:** You can also configure user accounts through Active Directory and LDAP (see [Configuring Authentication](#) on page 604).

- In the gear icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **User Management**.  
The *User Management* dialog box appears.

USERNAME	NAME	EMAIL	ROLES	ENABLED
admin			Cluster Admin, User Admin, Viewer	Yes
lab	lab viewonly	lab@corp.nutanix.com	Viewer	Yes

Figure: User Management Window

2. To add a user, click the **New User** button and do the following in the displayed fields:
  - a. **Username:** Enter a user name.
  - b. **First Name:** Enter a first name.
  - c. **Last Name:** Enter a last name.
  - d. **Email:** Enter the user email address.
  - e. **Password:** Enter a password (maximum of 255 characters).  
A second field to verify the password is not included, so be sure to enter the password correctly in this field.
  - f. **Language:** Select the language setting for the user.  
By default **English** is selected. You have an option to select **Simplified Chinese** or **Japanese**. Depending the language that you select here, the cluster locale will be updated for the new user. For example, if you select **Simplified Chinese**, next time when the new user that you have created logs in, the user interface will be displayed in Simplified Chinese.
  - g. **Roles:** Assign a role to this user.  
There are three options:
    - Checking the **User Administrator** box allows the user to view information, perform any administrative task, and create or modify user accounts. (Checking this box automatically checks the **Cluster Admin** box as well to indicate this user has full permissions. However, a user administrator has full permissions regardless of whether the cluster administrator box is checked.)
    - Checking the **Cluster Administrator** box allows the user to view information and perform any administrative task (but not create or modify user accounts).
    - Leaving both boxes unchecked allows the user to view information, but it does not provide permission to perform cluster or user administrative tasks.
- h. 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 appearing in the list.



**Note:** To return to the *User Management* window without saving, click the **Back** button; to cancel out of the *User Management* window (without saving), click the **Cancel** button.

3. Click the **Close** button to close the *User Management* window.

**Create User**

Enter the attributes for this user. Passwords must be at least eight characters long. Username is the name that is used by the user to sign into the Nutanix console.

USERNAME

FIRST NAME

LAST NAME

EMAIL

PASSWORD

LANGUAGE

ROLES  
 User Admin [?](#)  
 Cluster Admin

[◀ Back](#) [Cancel](#) [Save](#)

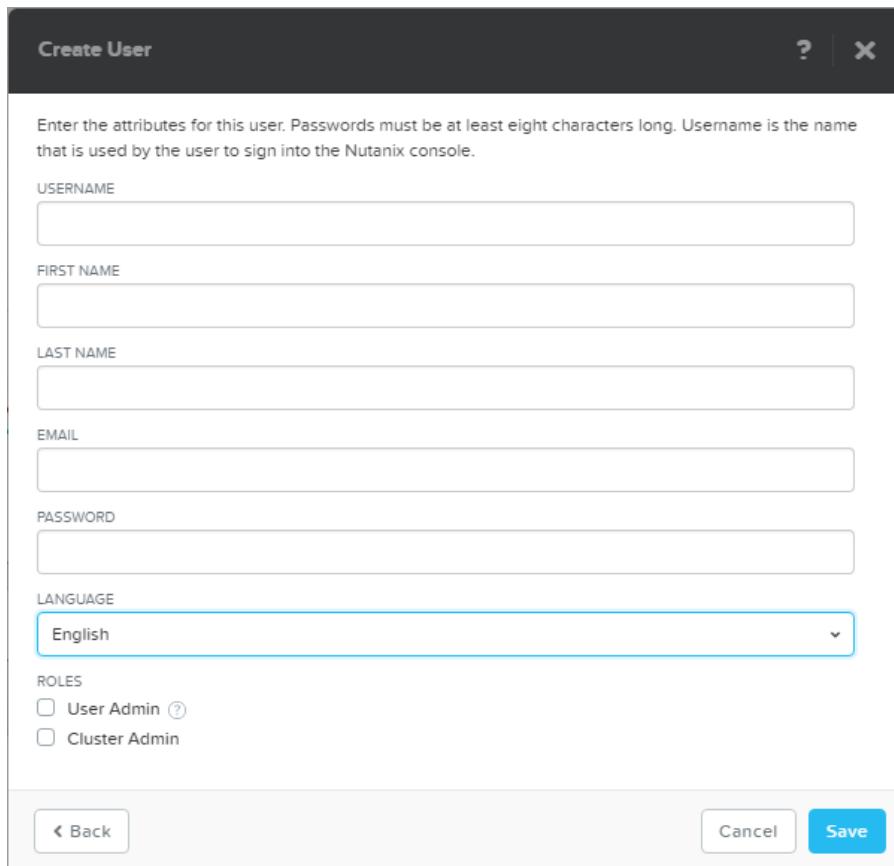


Figure: Create User Window

## Updating a User Account

To update credentials for an existing user, do the following:



**Note:** To update your account credentials (that is, the user you are currently logged in as), see [Updating My Account](#) on page 630. Changing the password for a different user is not supported; you must log in as that user to change the password.

1. In the gear icon  pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **User Management**.  
The *User Management* dialog box appears.

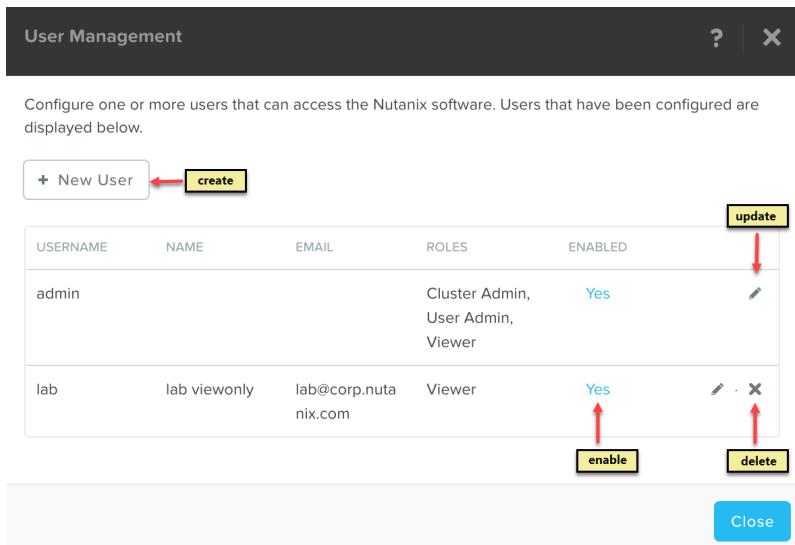


Figure: User Management Window

2. To disable login access, click the **Yes** value in the **Enabled** field for that user; to enable the account, click the **No** value.  
A **Yes** value means the login is enabled; a **No** value means it is disabled. A user account is enabled (login access activated) by default.
  3. To edit the user credentials, click the pencil icon for that user and update one or more of the values as desired in the displayed fields:
    - a. **Username:** The username is fixed when the account is created and cannot be changed.
    - b. **First Name:** Enter a different first name.
    - c. **Last Name:** Enter a different last name.
    - d. **Email:** Enter a different email address.
    - e. **Roles:** Change the role assigned to this user.  
There are three options:
      - Checking the **Cluster Admin** box allows a user to view information and perform any administrative task (but not create or modify user accounts).
      - Checking the **User Admin** box allows the user to view information, perform any administrative task, and create or modify user accounts. (Checking this box automatically checks the **Cluster Admin** box as well to indicate this user has full permissions. However, a user administrator has full permissions regardless of whether the cluster administrator box is checked.)
      - Leaving both boxes unchecked allows the user to view information, but it does not provide permission to perform cluster or user administrative tasks.
  - 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 appearing in the list.
-  **Note:** To return to the *User Management* window without saving, click the **Back** button; to cancel out of the *User Management* window (without saving), click the **Cancel** button.
4. Click the **Close** button to close the *User Management* window.

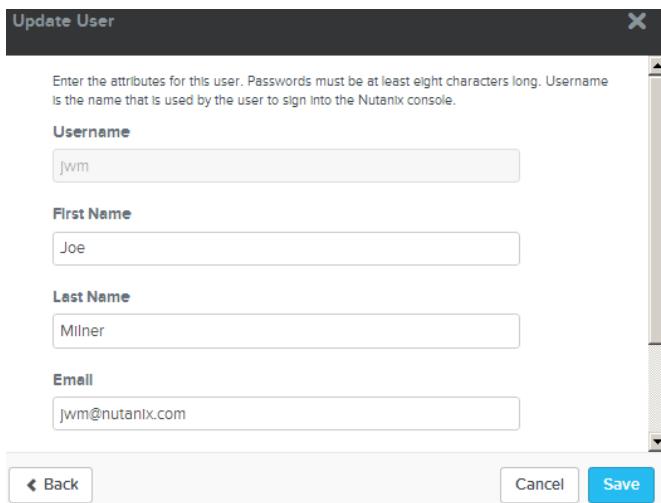


Figure: Update User Window

## Updating My Account

To update your account credentials (that is, credentials for the user you are currently logged in as), do the following:

1. To update your password, select **Change Password** from the user icon  pull-down list of the main menu (see [Main Menu Options](#) on page 32).  
The *Change Password* dialog box appears. Do the following in the indicated fields:
  - a. **Current Password:** Enter the current password.
  - b. **New Password:** Enter a new password.
  - c. **Confirm Password:** Re-enter the new password.
  - d. When the fields are correct, click the **Save** button (lower right). This saves the new password and closes the window.

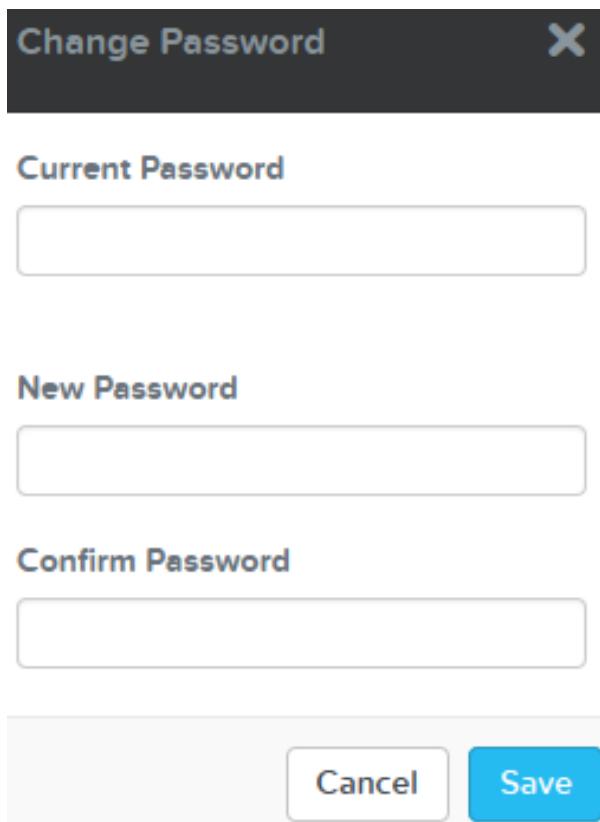


Figure: Change Password Window

2. To update other details of your account, select **Update Profile** from the user icon pull-down list. The *Update Profile* dialog box appears. Do the following in the indicated fields:
  - a. **Username:** The username is fixed when the account is created and cannot be changed.
  - b. **First Name:** Enter a different first name.
  - c. **Last Name:** Enter a different last name.
  - d. **Email:** Enter a different user email address.
  - e. **Language:** Select a language for your account.

f. When all the fields are correct, click the **Save** button (lower right). This saves the changes and closes the window.

**Update Profile**

Profile settings for **admin**.

**General**

FIRST NAME      LAST NAME

Nutanix      Company

EMAIL ADDRESS

x@x.com

LANGUAGE

English

---

**Portal Connection**

API KEY

PUBLIC KEY      Optional

Your keys can be managed from the [API Keys](#) page on the Support Portal.

Cancel      Save

Figure: Update Profile Window

## Deleting a User Account

To delete an existing user, do the following:

1. In the gear icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **User Management**.  
The *User Management* dialog box appears.

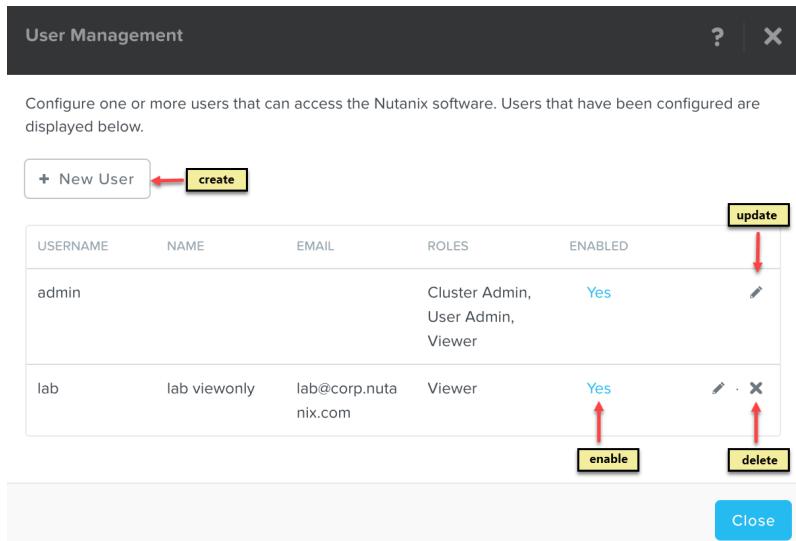


Figure: User Management Window

2. Click the **X** icon for that user. Note that you cannot delete the admin user. A window prompt appears to verify the action; click the **OK** button. The user account is removed and the user no longer appears in the list.
3. Click the **Close** button to close the *User Management* window.

## Support Services

Nutanix provides support services in several ways.

- Nutanix technical support can monitor your clusters and provide assistance when problems occur (see [Pulse Access Requirements](#) on page 636, [Controlling Remote Connections](#) on page 636, [Configuring HTTP Proxy](#) on page 637, and [Configuring Pulse](#) on page 634).
- Nutanix technical support maintains a portal that you can access to request assistance, download AOS updates, or view documentation (see [Accessing the Nutanix Support Portal](#) on page 639).
- Nutanix supports a REST API that allows you to request information or run administration scripts for a Nutanix cluster (see [Accessing the REST API Explorer](#) on page 642).

### Configuring Pulse

The feature known as *Pulse* provides diagnostic system data to Nutanix support teams to deliver proactive, context-aware support for Nutanix solutions. The Nutanix cluster automatically and unobtrusively collects this information with no effect on system performance. Pulse shares only basic system-level information necessary for monitoring the health and status of a Nutanix cluster. Information includes:

- system alerts
- current Nutanix software version
- Nutanix processes and Controller VM information
- hypervisor details such as type and version

When Pulse is enabled, Pulse sends a message once every hour to a Nutanix support server by default. Pulse also collects the most important data like system-level statistics and configuration information more frequently to automatically detect issues and help make troubleshooting easier. With this information, Nutanix support can apply advanced analytics to optimize your implementation and to address potential problems.



**Note:** Pulse sends messages through ports 80/8443/443, or if this is not allowed, through your mail server (see [Pulse Access Requirements](#) on page 636).



**Note:** When logging in to Prism the first time after installation or an upgrade, the system checks whether Pulse is enabled. If it is not, a message appears recommending that you enable Pulse. To enable Pulse, click the **Continue** button in the message and follow the prompts; to continue without enabling Pulse, check the **Disable Pulse (not recommended)** box and then click the **Continue** button.

You can enable (or disable) Pulse at any time. To configure Pulse, do the following:

1. In the gear icon pull-down list of the main menu (see [Main Menu Options](#) on page 32), select **Pulse**.  
The *Pulse* dialog box appears.

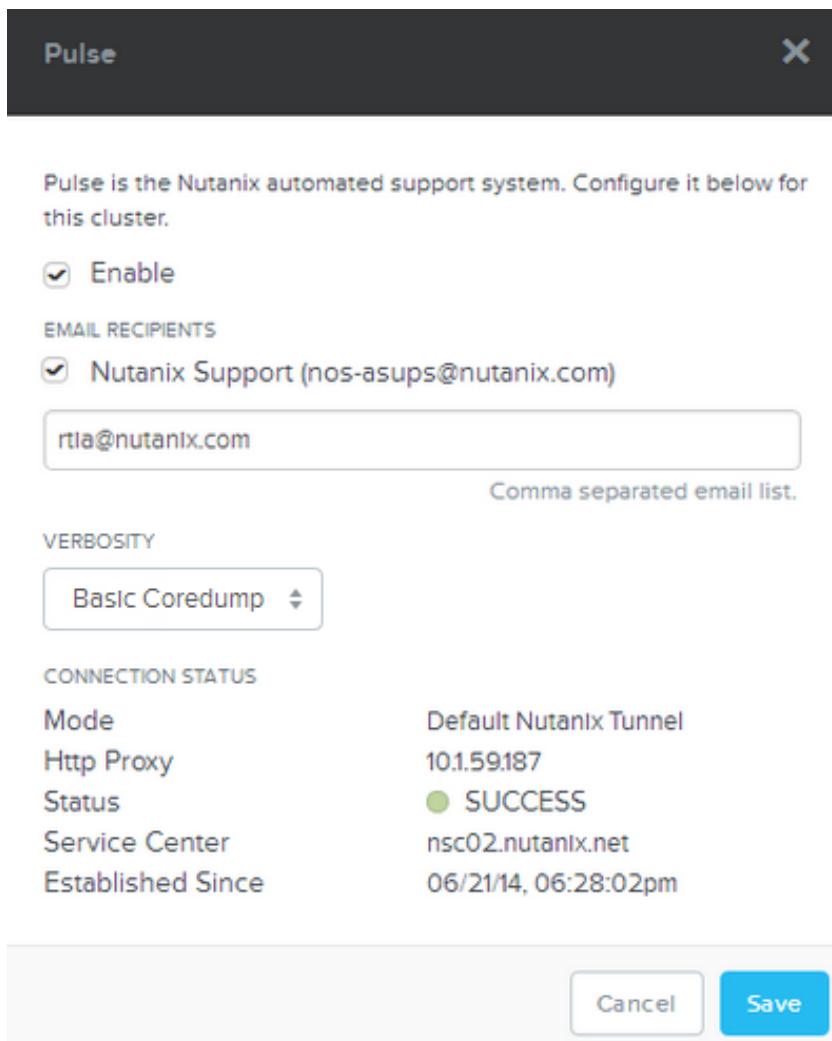


Figure: Pulse Window

2. To enable (disable) this feature, check (uncheck) the **Enable** box.
3. To add (remove) Nutanix customer support as a recipient of the cluster information, check (uncheck) the box next to **Nutanix Support (nos-asups@nutanix.com)** in the **Email Recipients** field.

Cluster information is e-mailed automatically to Nutanix customer support at **nos-asups@nutanix.com** when this feature is enabled. If you do not want Nutanix customer support to receive the cluster information, you can uncheck this box at any time (or restart the e-mails by checking it again).
4. To send the cluster information to additional recipients, enter one or more e-mail addresses in the **Additional Email Recipients** field.

In addition to (or instead of) sending the cluster information to Nutanix customer support, you can e-mail the information to yourself or others by entering recipient e-mail addresses in this field. Use a comma to separate multiple addresses.
5. Specify the amount of data to send by selecting an option from the **Verbosity** field pull-down list. The options are as follows:
  - **Nothing:** Do not collect any data. Setting the verbosity to **Nothing** is the same as unchecking the **Enable Emails** box; either action disables this feature (no e-mails are sent).
  - **Basic:** Collect basic statistics only. Basic statistics include Zeus, Stargate, Cassandra, and Curator subsystem information; Controller VM information; hypervisor and VMs information; and cluster configuration and performance information.

- **Basic Coredump** (default setting): Collect basic statistics plus core dump data. The core dump data is a summary of information extracted from the core dump files including the time stamp when it was created, the file name, and the fatal message.

**6.** Check the **Connection Status** field for connection information.

This field appears only when the feature is enabled, and it provides the following information:

- **Mode**: Displays the mode of e-mail transport, which is either Default Nutanix Tunnel (see *Controlling Remote Connections* on page 636 to enable tunnel) or SMTP Server (see *Configuring an SMTP Server* on page 573).
- **Http Proxy**: Displays the IP address for an HTTP proxy. This field appears only when a proxy is enabled (see *Configuring HTTP Proxy* on page 637).
- **Status**: Displays the transport mechanism status, which is **Success** when the default tunnel or an SMTP server is active or **Failure** when neither is available.
- **Service Center**: Displays the Nutanix service center address for this cluster, which is either nsc01.nutanix.net or nsc02.nutanix.net.
- **Established Since**: Displays the date and time when the connection was established.

**7.** Click the **Save** button to save the new setting and close the window.

## Pulse Access Requirements

In order to successfully send Pulse and alert messages from a cluster to the Nutanix support servers, Pulse requires the following access:

- Messages are sent from the Zeus (cluster configuration manager) leader, so the firewall must allow the Zeus leader IP address. Because the Zeus leader can change, it is recommended that the IP address for all Controller VMs in the cluster be open in the firewall.
- Each Controller VM in your cluster sends Pulse data to insights.nutanix.com over port 443 once every hour over HTTPS. Ensure that port 443 is open in your firewall to send cluster metrics.
- Ports 80 and 8443 are the default ports that the cluster uses to connect to the Nutanix support servers nsc01.nutanix.net and nsc02.nutanix.net. Nutanix recommends that you open both ports. If one port is disabled, the cluster will automatically try to connect on the other. Pulse (and alert) messages are not HTTP formatted, so if you use a firewall that only allows HTTP traffic through port 80, Pulse requires access through port 8443. Pulse uses the SSH protocol for communication through the firewall.
- If your security policy does not allow ports 80 and 8443 to be opened, Pulse can use your SMTP server to send messages and alert notifications if you have configured an SMTP server (see *Configuring an SMTP Server* on page 573). In this case the cluster only needs access to your SMTP server (not the Internet) to send the messages. If you do not use an SMTP server, another option is to implement an HTTP proxy as part of your overall support scheme.

## Controlling Remote Connections

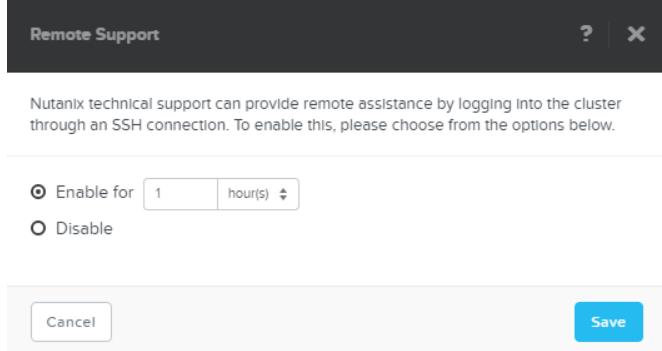
Nutanix technical support can remotely assist with problems by logging into the cluster through an SSH connection. This remote connection is disabled by default, but it may be enabled during the site installation procedure or at a later date through the web console. To enable (or disable) Nutanix technical support remote access to your cluster through this connection, do the following:

1. In the gear icon  pull-down list of the main menu (see *Main Menu Options* on page 32), select **Remote Support**.  
The *Remote Support Services* dialog box appears.
2. Select (click the radio button for) the desired access state.

- To allow remote access (temporarily) for Nutanix support, select **Enable** and enter the number and duration (hours or minutes) in the two boxes. When remote support is enabled temporarily, an icon appears in the screen header that includes a dynamic countdown until remote support is disabled.



- To prevent remote access by Nutanix support, select **Disable**.
3. Click the **Save** button to save the new setting and close the window.



*Figure: Remote Support Services Window*

 **Note:** The remote connection requires access to and from nsc01.nutanix.net and nsc02.nutanix.net at either port 80 or 8443 across all Controller VM IP addresses in the cluster. The firewall must be configured to allow this access in order to enable the Nutanix support remote connection.

## Configuring HTTP Proxy

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:

- In the gear icon  pull-down list of the main menu (see *Main Menu Options* on page 32), select **HTTP Proxy**.  
The *HTTP Proxy* dialog box appears.

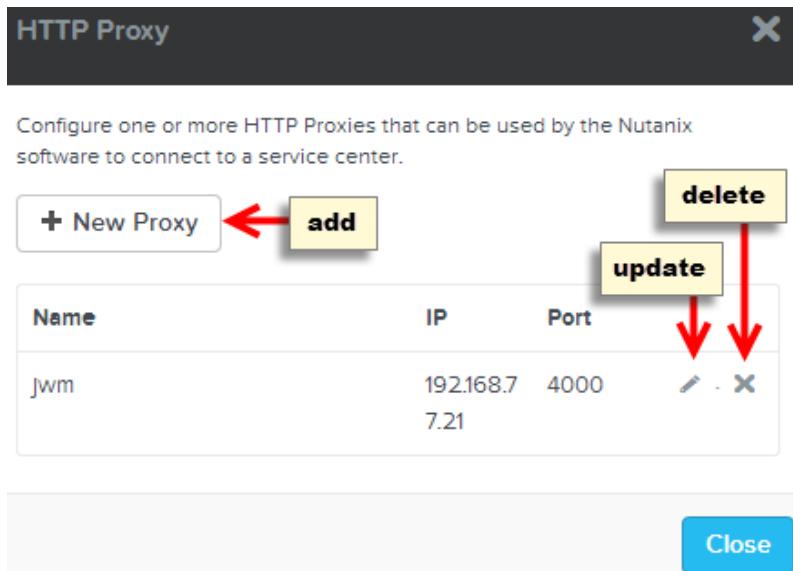


Figure: HTTP Proxy Window

2. 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.
- 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 HTTP proxy entry appearing in the list.

 **Note:** To return to the *HTTP Proxy* window without saving, click the **Cancel** button.

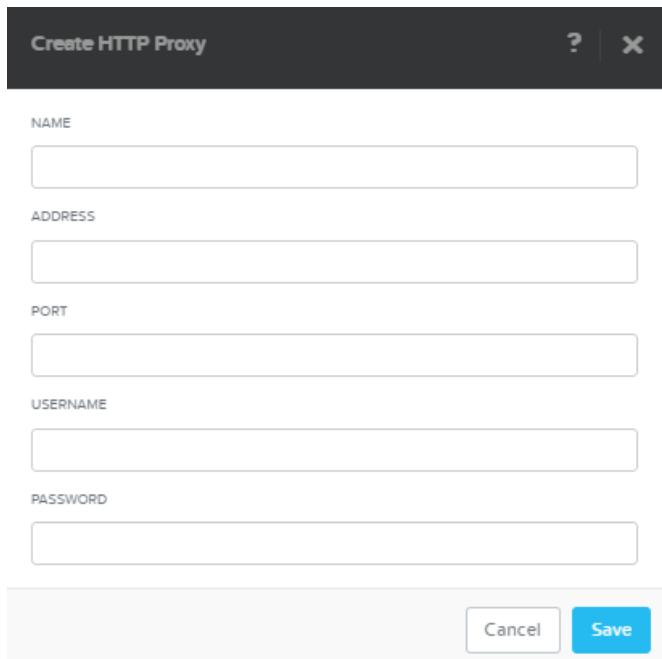


Figure: Create HTTP Proxy Window

3. 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.
4. 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.
5. Click the **Close** button to close the window.

## Accessing the Nutanix Support Portal

Nutanix provides a variety of support services and materials through its support portal.

1. To access the Nutanix support portal, select **Support Portal** from the question mark icon pull-down list.  
The login screen for the Nutanix support portal appears in a new tab or window.
2. Enter your support account user name and password.  
The Nutanix support portal home page appears.
3. Select the desired service from the screen options.  
You can select an option from one of the main menu pull-down lists 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.

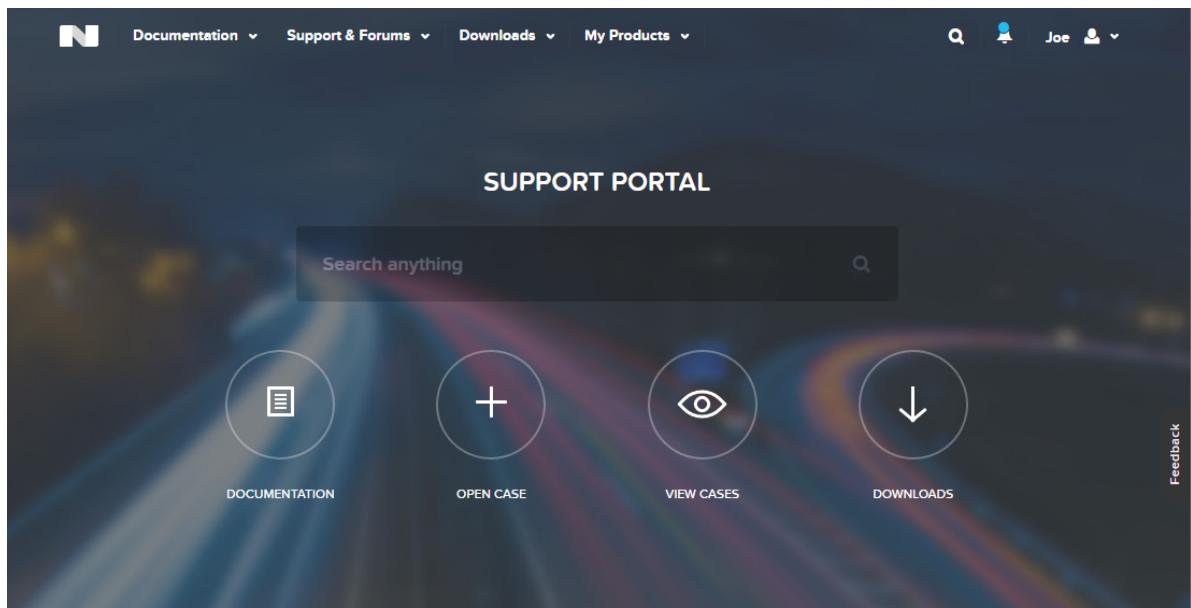


**Note:** Some options have restricted access and are not available to all users.

## Main Menu Options

Category	Option	Description
Documentation	Product Documentation	Displays a page from which you can view the Nutanix product manuals.
	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).
Support & Forums	Webinar Recordings	Displays a page with links to a selection of Nutanix training webinars.
	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.
Downloads	Terms & Conditions	Displays a page from which you can view various warranty and terms and conditions documents.
	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.

Category	Option	Description
	Phoenix	Displays a page from which you can download Phoenix ISO files.
	Foundation	Displays a page from which you can download Foundation releases.
My Products	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.



#### Popular KB Articles

- [SIOC in Stats Mode can cause storage unavailability on Nutanix](#)
- [Upgrade ESXi 5.1/ESXi 5.5 to ESXi 5.5 Update 1 patch 4 build-1881737 \(NFS bug fixed/Heartbleed patch\)](#)
- [Updated 10 Gigabit Ethernet Driver For ESXi 5.5](#)

#### Announcements

- [Register now for .NEXT Conference 2016!](#)
- [AOS 4.6.1 is now available!](#)
- [Prism Central 4.6.1 is now available!](#)
- [Nutanix Cluster Check 2.2.3 is now available!](#)

Figure: Nutanix Support Portal

## 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 Nutanix 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/>.

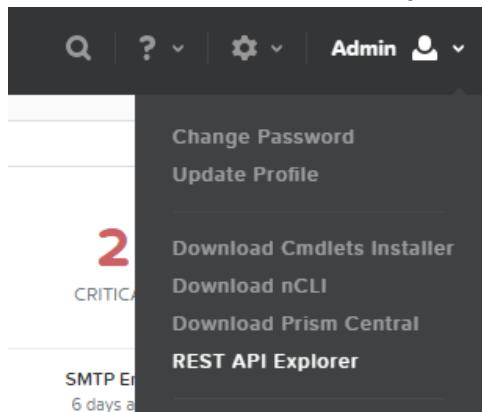
## Accessing the REST API Explorer

Nutanix provides a utility with the 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.

The v1 and v2 APIs can both be viewed in the REST API Explorer.

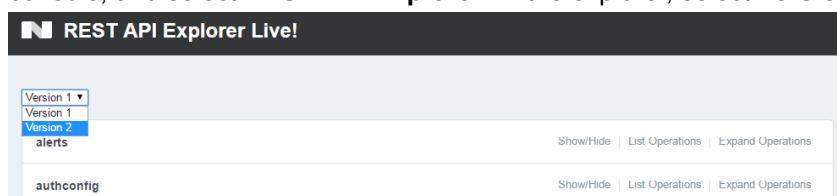
### 1. Open the explorer for the desired version of the API.

- v1: Connect to the Nutanix 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 1** from the menu.



*Figure: User menu*

- v2: Connect to the Nutanix 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.



*Figure: API version selection*

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

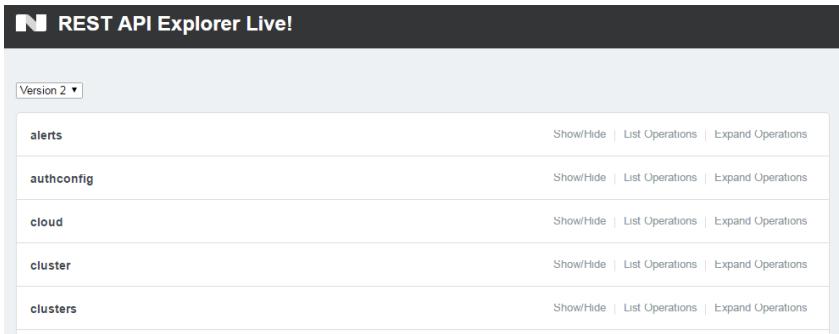


Figure: REST API Explorer

 **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](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.

- Find the line for the object you want to explore and click **Expand Operations**. For this example, you will operate on a storage pool.

Method	Path	Description
GET	/cluster/	Get Cluster details.
PATCH	/cluster/	Modify Cluster params.
PUT	/cluster/	Update Cluster params.
POST	/cluster/metro_witness	Add Witness VM details
GET	/cluster/metro_witness/	Get Witness VM config
GET	/cluster/name_servers	Get the list of Name Servers.
POST	/cluster/name_servers	Add name server.
DELETE	/cluster/name_servers/{nameServer}	Delete the specified Name Server.

Figure: Cluster Operations

- Click **GET** on the first line to show the details for this API call.

Implementation Notes  
Get the details of the cluster.

Response Class (Status 200)  
Model Model Schema

```
{
  "alert_summary": {
    "alert_summaries": {},
    "count": 0
  },
  "all_hyperv_nodes_in_failover_cluster": true,
  "block_serials": [
    "string"
  ],
  "cloudcluster": true,
  "cluster_data_state": {
    ...
  }
}
```

Response Content Type application/json ▾  
Try it out!

Figure: Get Cluster Details

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 screenshot shows the Prism Web Console API Explorer interface. At the top, there is a dropdown menu for 'Response Content Type' set to 'application/json'. Below it is a button labeled 'Try it out!' and a 'Hide Response' link. The 'Curl' section contains a command: 'curl -X GET --header "Accept: application/json" "https://10.52.47.9440/PrismGateway/services/rest/v2.0/cluster?". The 'Request URL' field shows the full URL: 'https://10.52.47.9440/PrismGateway/services/rest/v2.0/cluster/'. The 'Response Body' section displays a JSON error message:

```
{  
  "message": "An Authentication object was not found in the SecurityContext",  
  "detailed_message": "org.springframework.security.authentication.AuthenticationCredentialsNotFoundException: An Authentication object was not found in the SecurityContext",  
  "error_code": {  
    "code": 1100,  
    "help_url": "http://my.nutanix.com"  
  }  
}
```

The 'Response Code' field shows '401'. The 'Response Headers' section includes a timestamp and some X-headers:

```
{"date": "Fri, 26 Aug 2016 23:02:23 GMT",  
 "x-content-type-options": "nosniff",  
 "x-permitted-cross-domain-policies": "master-only",  
 "exception": "An Authentication object was not found in the SecurityContext"}
```

*Figure: Get Cluster Details Response*

The test displays the request URL required for scripting, as well as sample responses expected from the API call.

## Help Resources

There are several information sources that you can access at any time when you need help:

- Context-sensitive help documentation (see [Accessing Online Help](#) on page 645).
- Health dashboard tutorial (see the Menu Options section in [Health Dashboard](#) on page 344).
- Customer support portal (see [Accessing the Nutanix Support Portal](#) on page 639).
- Nutanix community forum (see [Accessing the Nutanix Next Community](#) on page 647).
- REST API explorer (see [Accessing the REST API Explorer](#) on page 642).
- Glossary of terms (see [Glossary](#) on page 648).

### Accessing Online Help

The web console includes online help documentation that you can access at any time.

1. To open the online help, choose one of the following from the question mark icon  pull-down list of the main menu (see [Main Menu Options](#) on page 32):
  - 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.

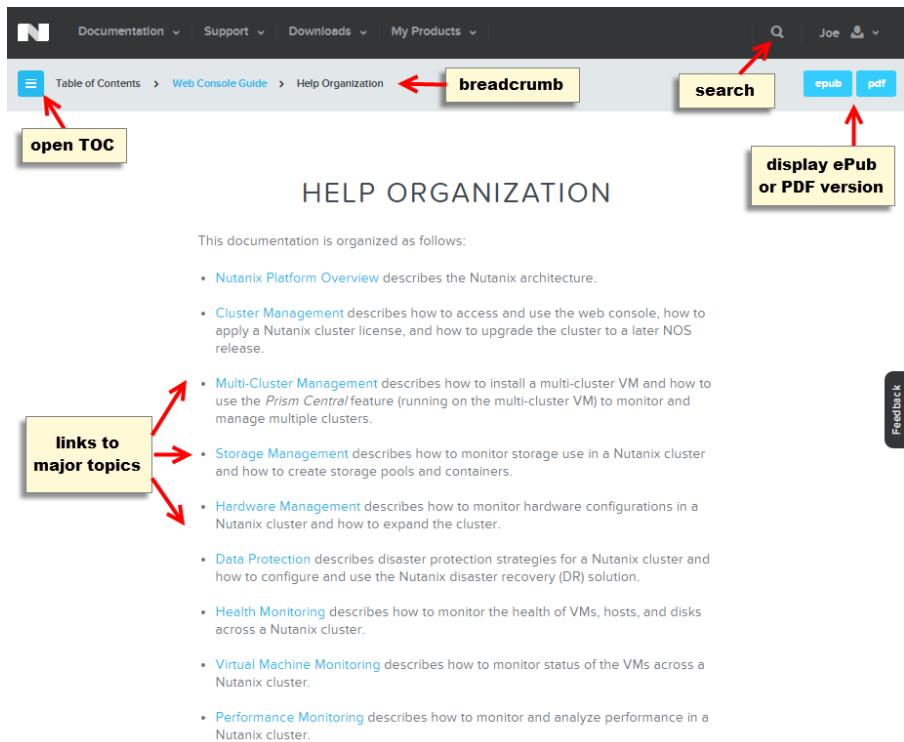


Figure: Help Organization Page

## 2.

To select a topic from the table of contents, click the  icon 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.

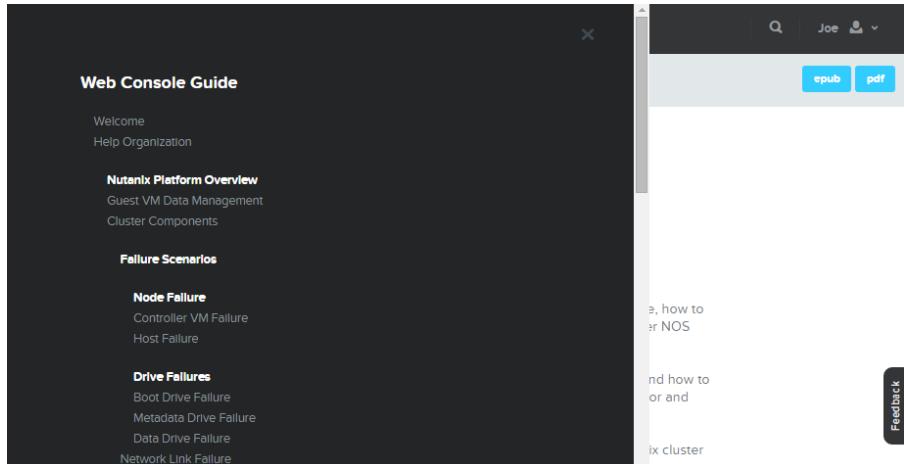


Figure: Table of Contents Pane

## 3.

To display all the help contents as a single document (*Web Console Guide*), click the **epub** or **pdf** button in the upper right.

You can view the *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.

## 4.

To search for a topic, click the  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.

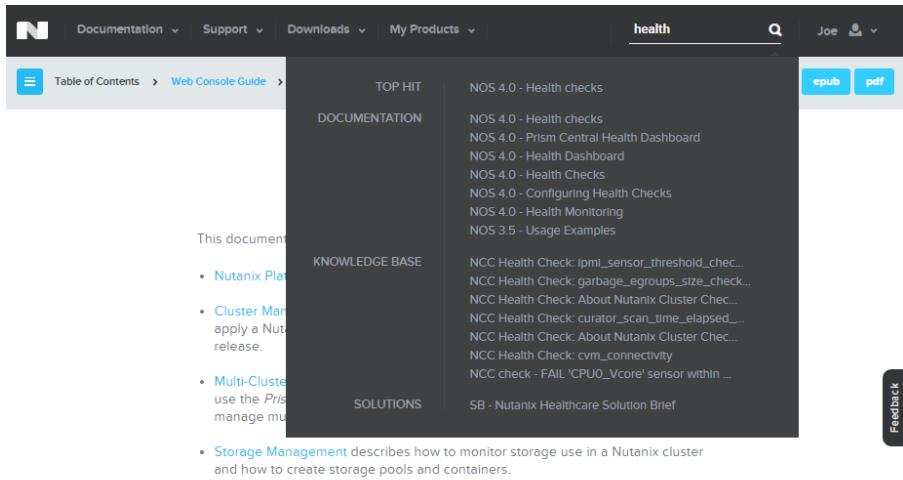


Figure: Search Results Example

## 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.

To access the Nutanix next community forum, select **Nutanix Next Community** from the question mark icon pull-down list of the main menu (see *Main Menu Options* on page 32). 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.

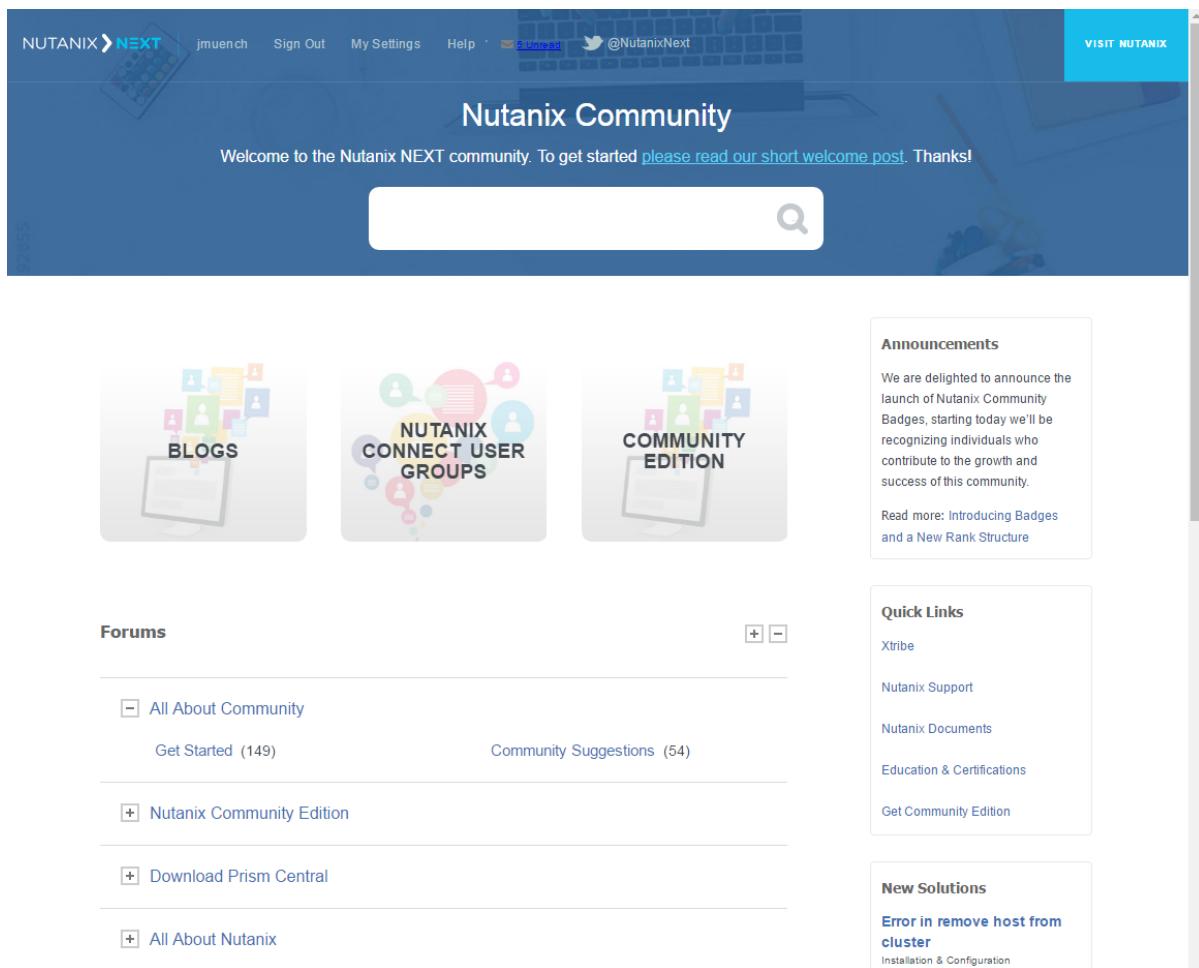


Figure: Next Community Screen

## Glossary

### aCLI

Acropolis command-line interface.

### Acropolis

The Nutanix converged software fabric for virtualization and storage management. It consists of the Acropolis base software, Acropolis Distributed Storage Fabric, AHV, App Mobility Fabric, Prism, and Acropolis APIs.

### Acropolis App Mobility Fabric

Provides virtualization management, volume management, and other distributed management functions for Acropolis.

## AHV

Nutanix-specific hypervisor host providing core server virtualization and optimized for Nutanix cluster and guest VM use.

## block

A set of Nutanix nodes contained in a single enclosure.

## block fault tolerance

When certain conditions are met, redundant copies of any data required to serve I/O are placed on nodes that are not in the same block. In the case where multiple nodes in a block fail, the cluster can continue to run because cluster configuration data exists on other blocks. Guest VMs can continue to run because redundant copies of guest VM data and metadata exist on other blocks.

## clone

A writeable copy of a vDisk.

## Cloud Connect

A feature that enables you to back up and restore copies of virtual machines and files to and from an on-premise cluster and a Nutanix Controller VM located on the Amazon Web Service (AWS) or Microsoft Azure cloud. The cloud-based cluster is managed as a remote site from the Prism Web Console or nCLI.

## cluster

A group of nodes contained in one or more Nutanix blocks.

## cold data

Data that did not have many rewrites or overwrites for a long time. For example, snapshots, file servers, archives, or backups.

## compression

An optional storage container setting that enables one of two types of compression.

## compression, inline

Data is compressed as it is written. This type of compression is recommended for workloads that perform batch processing.

## compression, post-process

Data is compressed after it is written. The delay time between write and compression is configurable. Because every workload has a different I/O profile, Nutanix has no recommended delay value. This type of compression is recommended for most workloads.

## consistency group

A subset of VMs in a protection domain. All VMs within a consistency group for that protection domain will be snapshotted in a crash-consistent manner. For all VMs in a consistency group, a snapshot creates one snapshot for all VMs in the group.

## Controller VM

A Nutanix VM that manages storage and other cluster functions on a node.

## data resiliency

A measure of the types of failures a cluster can withstand; affected by block awareness and redundancy factor.

## datastore

A logical storage container for files necessary for VM operations.

## deduplication

The sharing of identical guest VM data on premium tiers (RAM and Flash) for improved performance or on capacity tiers (HDD) for storage space savings. Enabled by properties of a storage container or vDisk.

## Distributed Storage Fabric

All storage functionality, including snapshots and clones, data protection, disaster recovery, data path redundancy, replication factors, deduplication, compression, erasure coding, and so on.

## Enterprise Cloud Platform

The Nutanix solution that natively converges compute, virtualization and storage into a resilient, software-defined solution with rich machine intelligence

## erasure coding

Optional algorithm included in the Acropolis base software to help reduce the storage used for fault tolerance. It helps to increase the effective or usable capacity on a cluster, depending on cluster size and data coldness.

## failback

Planned failover initiated from recovery site.

## failover

Moving VMs from a primary site to a recovery site.

## failover, disaster

Failover when the primary site is down.

**failover, planned**

Failover when both sites are up.

**guest VM**

A VM running on a Nutanix cluster that executes a workload, such as VDI or Exchange, as opposed to a VM that is involved in cluster operations, such as a Controller VM.

**host**

An instance of the hypervisor that runs on a Nutanix node.

**image service**

A workflow in the Prism web console that enables a user to upload ISO or disk images (in ESXi or Hyper-V format) to a Nutanix AHV cluster by specifying a remote repository URL or by uploading a file from a local machine.

**local replication**

Multiple copies of data within a storage container. These copies exist for fault tolerance: if a physical disk fails, the cluster can recover data from another copy. The cluster manages the replicated data, and the copies are not visible to the user.

**local snapshot**

Snapshots stored on the same cluster where they originated.

**nCLI**

Nutanix command-line interface.

**node**

A physical server contained in a Nutanix block; runs a hypervisor host.

**oplog**

A write cache on a faster, more expensive storage tier.

**Prism**

Web-based management interface for managing Nutanix clusters.

**Prism Central**

Centralized management tool that runs as a separate VM configured as a single-node cluster to monitor and manage multiple clusters through a single web console.

## Prism Element

A single cluster being managed by and available through the Prism Central web console.

## protection domain

A group of VMs to be backed up locally on a cluster or replicated on the same schedule to one or more clusters. Protection domains may be associated with remote sites. Protection domain names must be unique across sites. A VM can be in at most one protection domain.

## protection domain, active

A protection domain that manages live VMs and makes, replicates, and expires snapshots.

## protection domain, inactive

A protection domain that receives snapshots from a remote cluster.

## redundancy factor

The number of nodes plus 1 that the cluster can tolerate being down at one time. By default, Nutanix clusters have a redundancy factor of 2, which means that they can tolerate 1 node being down. They are configurable to redundancy factor 3 to enable tolerating 2 nodes being down.

## remote replication, one-to-one

Replicates a production cluster with one idle cluster as a DR target.

## remote replication, reciprocal

Cross replication within running (non-idle) production clusters.

## remote site

A pair of clusters that can replicate data to each other. A configured remote site can also be located in the cloud (based on Amazon AWS or Microsoft Azure, for example).

## remote snapshot

A snapshot copied asynchronously from one cluster to another.

## replication factor

The number of copies of data kept by a storage container. The default is 2. Storage Containers on clusters with redundancy factor of 3 can have replication factor of 3.

## reserved capacity

A property of a storage container or vDisk that guarantees that a certain amount of storage space is available.

## schedule

A property of a protection domain that specifies the intervals to take snapshots and how long the snapshots should be retained. A schedule optionally specifies which remote site to replicate to.

## Self-Service Restore

Allows a user to restore a file within a virtual machine from the Nutanix protected snapshot with minimal Nutanix administrator intervention.

## shadow clone

A cache of a vDisk on all the nodes in the cluster. When a vDisk is read by multiple VMs (such as the base image for a VDI clone pool), the cluster creates shadow clones of the vDisk.

## snapshot

A read-only copy of the state and data of a VM at a point in time. Snapshots for a VM are crash consistent, which means that the VMDK on-disk images are consistent with a single point in time. That is, the snapshot represents the on-disk data as if the VM crashed. The snapshots are not, however, application consistent, meaning that application data is not quiesced at the time of snapshot, unless the protection domain is configured to use application-consistent snapshots.

## storage container

A subset of available storage within a storage pool.

## storage pool

A group of physical disks from one or more tiers.

## storage replication adapter

A Nutanix-provided module that allows VMware Site Replication Manager (SRM) to use native remote replication.

## tier

A type of physical storage in a Nutanix node.

## vDisk

Data associated with a VM represented as a set of files on a datastore.

## 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.

## VM mobility

The ability to export your existing VMs from one non-AHV cluster to an AHV cluster. This option requires that you install the Nutanix VM Mobility installer on all the VMs. The Nutanix VM Mobility installer deploys the drivers that are required at the destination AHV cluster. After you prepare the source VMs, they can be exported to the AHV cluster.

## vStore

A separate mount point within a storage container which has its own NFS namespace. This namespace maps to a protection domain. Each vStore is exported as a device through the Nutanix SRA.

# Copyright

Copyright 2017 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.

## License

The provision of this software to you does not grant any licenses or other rights under any Microsoft patents with respect to anything other than the file server implementation portion of the binaries for this software, including no licenses or any other rights in any hardware or any devices or software that are used to communicate with or in connection with this software.

## Conventions

Convention	Description
<code>variable_value</code>	The action depends on a value that is unique to your environment.
<code>ncli&gt; command</code>	The commands are executed in the Nutanix nCLI.
<code>user@host\$ command</code>	The commands are executed as a non-privileged user (such as nutanix) in the system shell.
<code>root@host# command</code>	The commands are executed as the root user in the vSphere or Acropolis host shell.
<code>&gt; command</code>	The commands are executed in the Hyper-V host shell.
<code>output</code>	The information is displayed as output from a command or in a log file.

## Default Cluster Credentials

Interface	Target	Username	Password
Nutanix web console	Nutanix Controller VM	admin	Nutanix/4u
vSphere Web Client	ESXi host	root	nutanix/4u
vSphere client	ESXi host	root	nutanix/4u
SSH client or console	ESXi host	root	nutanix/4u
SSH client or console	AHV host	root	nutanix/4u

Interface	Target	Username	Password
SSH client or console	Hyper-V host	Administrator	nutanix/4u
SSH client	Nutanix Controller VM	nutanix	nutanix/4u
SSH client	Nutanix Controller VM	admin	Nutanix/4u
SSH client or console	Acropolis OpenStack Services VM (Nutanix OVM)	root	admin

## Version

**Last modified:** September 14, 2017 (2017-09-14 14:06:38 GMT+5.5)