Cisco Compute Hyperconverged with Nutanix

Intersight Standalone Mode Installation Field Guide

Document Information

Access the latest version of this document at Cisco Communities: https://community.cisco.com/t5/unified-computing-system-knowledge-base/cisco-compute-hyperconverged-with-nutanix-standalone-field-guide/ta-p/5101084

Revision History

Version	Date	Prism Central version	Foundation Central version	AOS LTS version	AOS STS/eSTS version	LCM Version	Notes
1.0	May 2024	2022.6 or 2023.4	1.6	6.5.5.6	6.7.1	2.7.1	Initial Release for Intersight based deployments with M6 and M7 generation servers.
1.1	July 2024	2022.6 or 2023.4 or 2024.1	1.6	6.5.6	6.8.0.5	3.0.0	Added Witness VM and additional Prism Central on ESXi installation information.

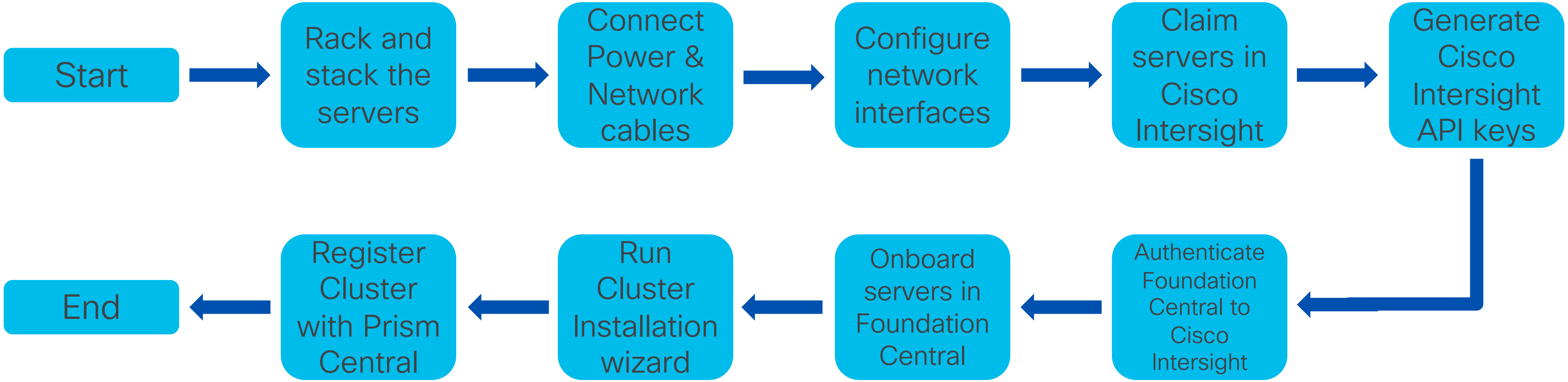
Contents

Installation Overview

This field guide covers the installation of Nutanix clusters on Cisco UCS C-series servers in standalone mode, i.e. not connected to Cisco UCS Fabric Interconnects, but managed by Cisco Intersight and connected to standard Ethernet switches.

Software Prerequisites:

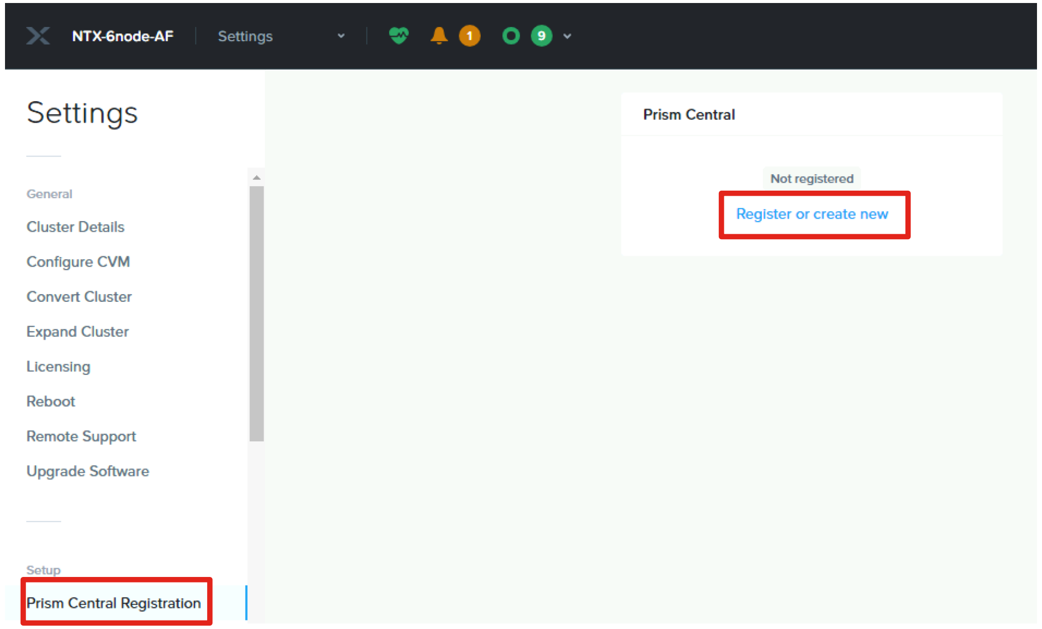
1. Nutanix Prism Central with Foundation Central added from the marketplace
2. Cisco Intersight SaaS account, or the connected or private virtual appliance with sufficient licenses
3. An anonymous web server for hosting installation files, such as the Cisco IMM toolkit VM (optional)
4. NTP sync and DNS name resolution for Cisco Intersight or the Intersight appliance, and Prism Central



Start
Rack and stack the servers
Connect Power & Network cables
Configure network interfaces
Claim servers in Cisco Intersight
Generate Cisco Intersight API keys
Authenticate Foundation Central to Cisco Intersight
Onboard servers in Foundation Central
Run Cluster Installation wizard
Register Cluster with Prism Central
End

Hardware and Software Configuration

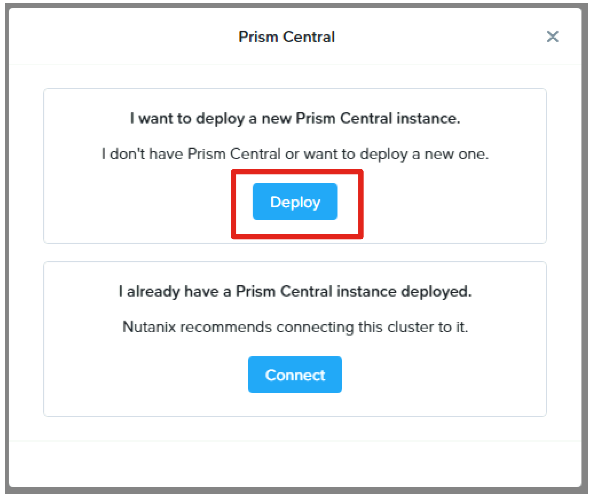
Start Prism Central Installation on a Nutanix Cluster



Prism Central

Not registered

Register or create new

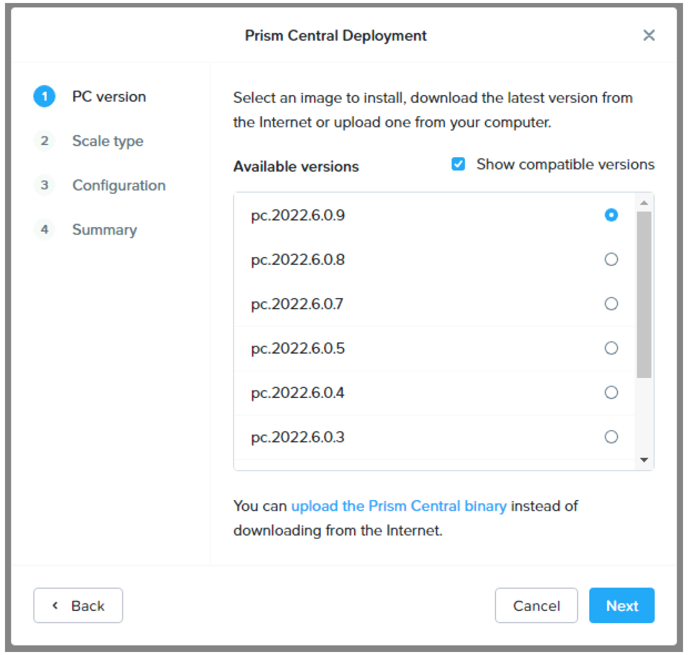


I want to deploy a new Prism Central instance.

I don't have Prism Central or want to deploy a new one.

I already have a Prism Central instance deployed.

Nutanix recommends connecting this cluster to it.



Select an image to install, download the latest version from the Internet or upload one from your computer.

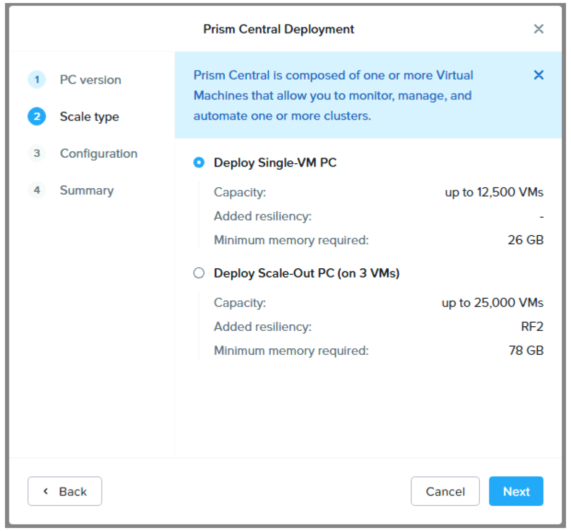
Available versions ☑ Show compatible versions

- pc.2022.6.0.9 ●
- pc.2022.6.0.8 ○
- pc.2022.6.0.7 ○
- pc.2022.6.0.5 ○
- pc.2022.6.0.4 ○
- pc.2022.6.0.3 ○

You can upload the Prism Central binary instead of downloading from the Internet.

If not already done, deploy PC 2023.4 or PC 2024.1 on a Nutanix cluster, or version PC 2022.6 on ESXi.
Prism Central binaries are available here: https://portal.nutanix.com/page/downloads?product=prism
Pay close attention to compatibility information, for example, version 2022.9 or later can only be newly deployed on clusters running AOS 6.6 or later.
Additional upgrade path and compatibility information is available here:
https://portal.nutanix.com/page/documents/upgrade-paths and here:
https://portal.nutanix.com/page/documents/compatibility-interoperability-matrix/interoperability

Prism Central Installation on Nutanix continued



Prism Central Deployment

1 PC version
2 Scale type
3 Configuration
4 Summary

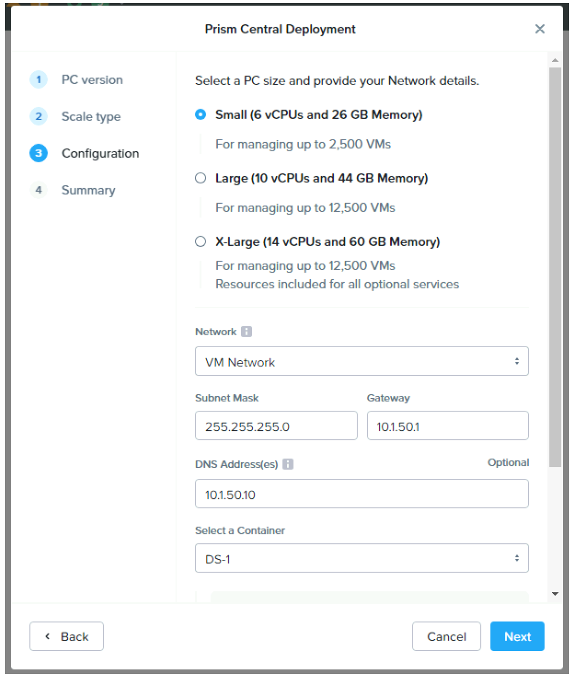
Prism Central is composed of one or more Virtual Machines that allow you to monitor, manage, and automate one or more clusters.

● Deploy Single-VM PC

Capacity:	up to 12,500 VMs
Added resiliency:	-
Minimum memory required:	26 GB

○ Deploy Scale-Out PC (on 3 VMs)

Capacity:	up to 25,000 VMs
Added resiliency:	RF2
Minimum memory required:	78 GB



Prism Central Deployment

1 PC version
2 Scale type
3 Configuration
4 Summary

Select a PC size and provide your Network details.

● Small (6 vCPUs and 26 GB Memory)
For managing up to 2,500 VMs

○ Large (10 vCPUs and 44 GB Memory)
For managing up to 12,500 VMs

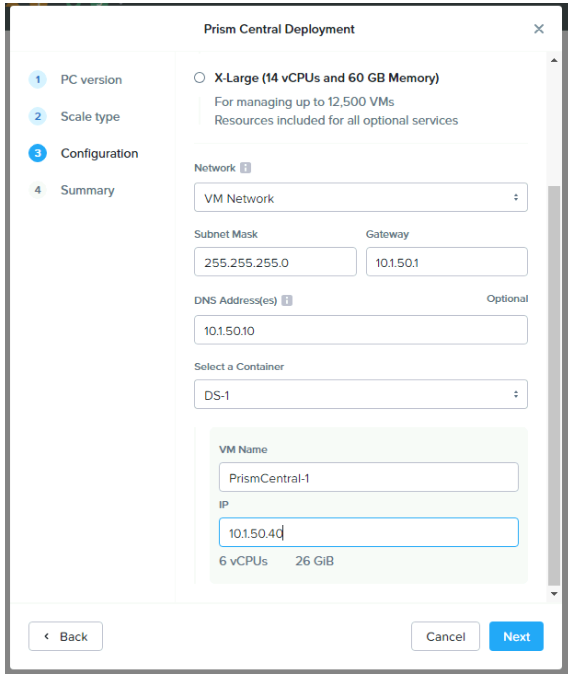
○ X-Large (14 vCPUs and 60 GB Memory)
For managing up to 12,500 VMs
Resources included for all optional services

Network: VM Network

Subnet Mask: 255.255.255.0
Gateway: 10.1.50.1

DNS Address(es) (Optional): 10.1.50.10

Select a Container: DS-1



Prism Central Deployment

1 PC version
2 Scale type
3 Configuration
4 Summary

○ X-Large (14 vCPUs and 60 GB Memory)
For managing up to 12,500 VMs
Resources included for all optional services

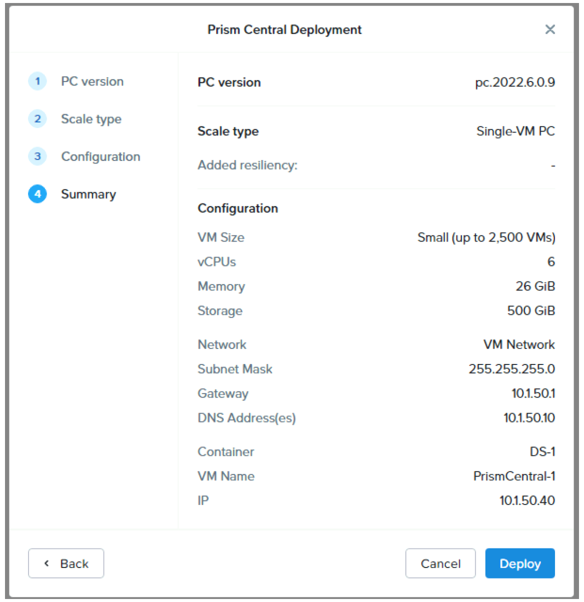
Network: VM Network

Subnet Mask: 255.255.255.0
Gateway: 10.1.50.1

DNS Address(es) (Optional): 10.1.50.10

Select a Container: DS-1

VM Name: PrismCentral-1
IP: 10.1.50.40
6 vCPUs 26 GiB

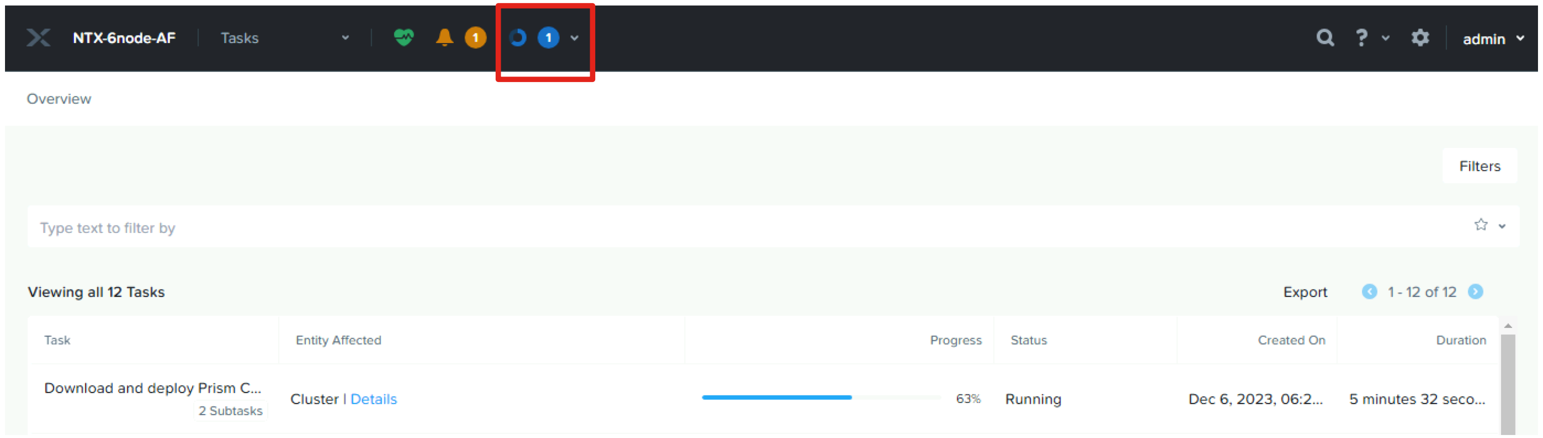


Prism Central Deployment

1 PC version
2 Scale type
3 Configuration
4 Summary

PC version	pc.2022.6.0.9
Scale type	Single-VM PC
Added resiliency:	-
Configuration	
VM Size	Small (up to 2,500 VMs)
vCPUs	6
Memory	26 GiB
Storage	500 GiB
Network	VM Network
Subnet Mask	255.255.255.0
Gateway	10.1.50.1
DNS Address(es)	10.1.50.10
Container	DS-1
VM Name	PrismCentral-1
IP	10.1.50.40

Warning: You must provide valid DNS servers in order for the connection to Cisco Intersight to work properly

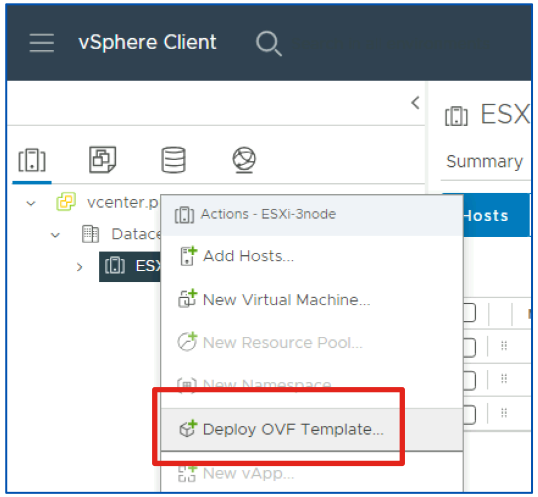


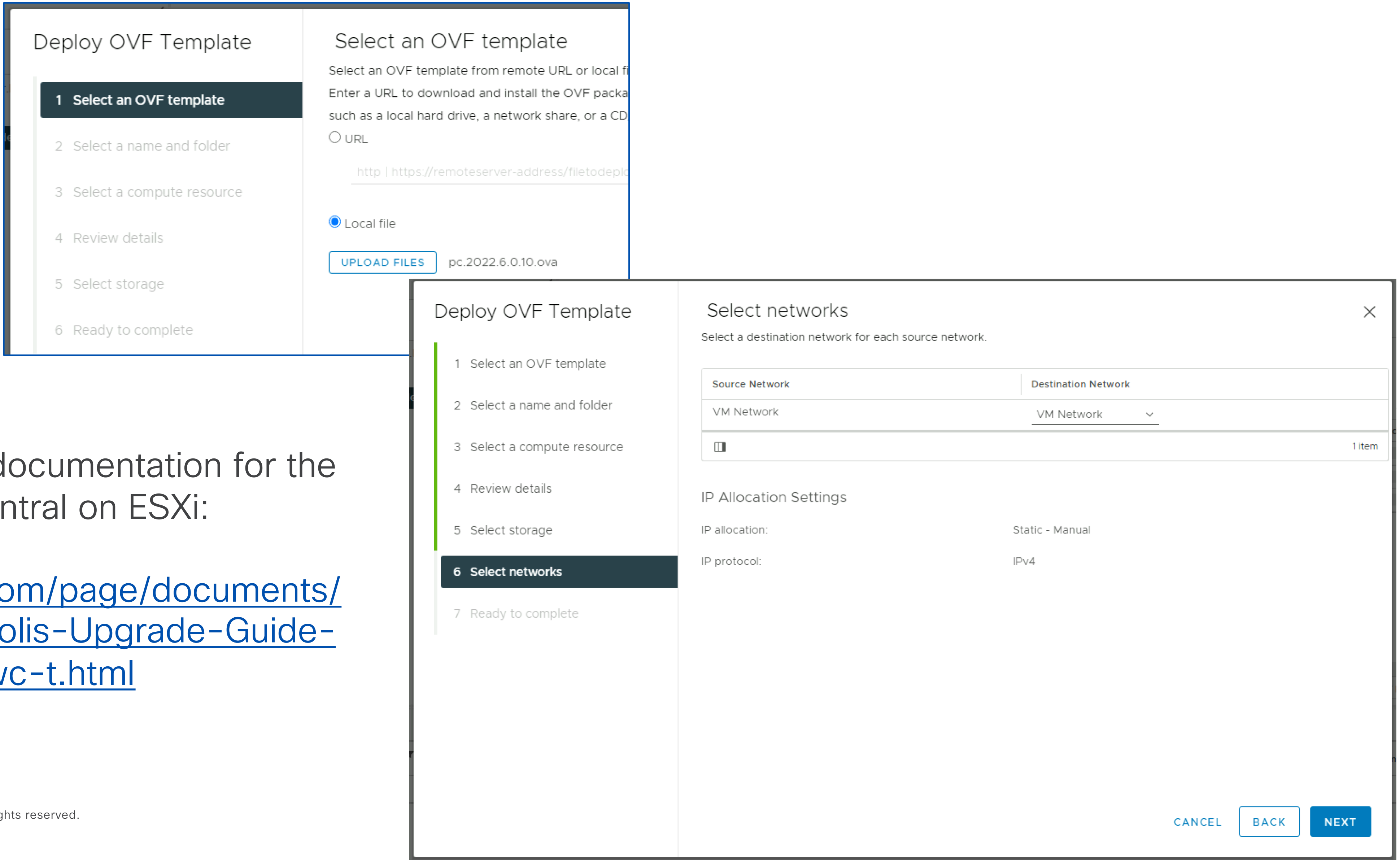
Viewing all 12 Tasks

Task	Entity Affected	Progress	Status	Created On	Duration
Download and deploy Prism C... 2 Subtasks	Cluster | Details	63%	Running	Dec 6, 2023, 06:2...	5 minutes 32 seco...

Note: Deployment can take 30+ minutes

Start Prism Central Installation on ESXi infrastructure





Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local fi
Enter a URL to download and install the OVF packa
such as a local hard drive, a network share, or a CD

○ URL

http | https://remoteserver-address/filetodeplc

● Local file

UPLOAD FILES pc.2022.6.0.10.ova

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Select networks
7 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network

1 item

IP Allocation Settings

IP allocation:	Static - Manual
IP protocol:	IPv4

Refer to the following documentation for the installation of Prism Central on ESXi:

https://portal.nutanix.com/page/documents/details?targetId=Acropolis-Upgrade-Guide-v6_5:upg-vm-install-wc-t.html

Prism Central Installation on ESXi continued

Power on the VM then open the local vSphere console. Log on as user nutanix, password nutanix/4u and edit the network interface with a static IP address:

```
$ sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Add or edit the NETMASK, IPADDR and GATEWAY lines, change BOOTPROTO to none, then save the changes and reboot:

```
NETMASK="xxx.xxx.xxx.xxx"
IPADDR="xxx.xxx.xxx.xxx"
BOOTPROTO="none"
GATEWAY="xxx.xxx.xxx.xxx”
```

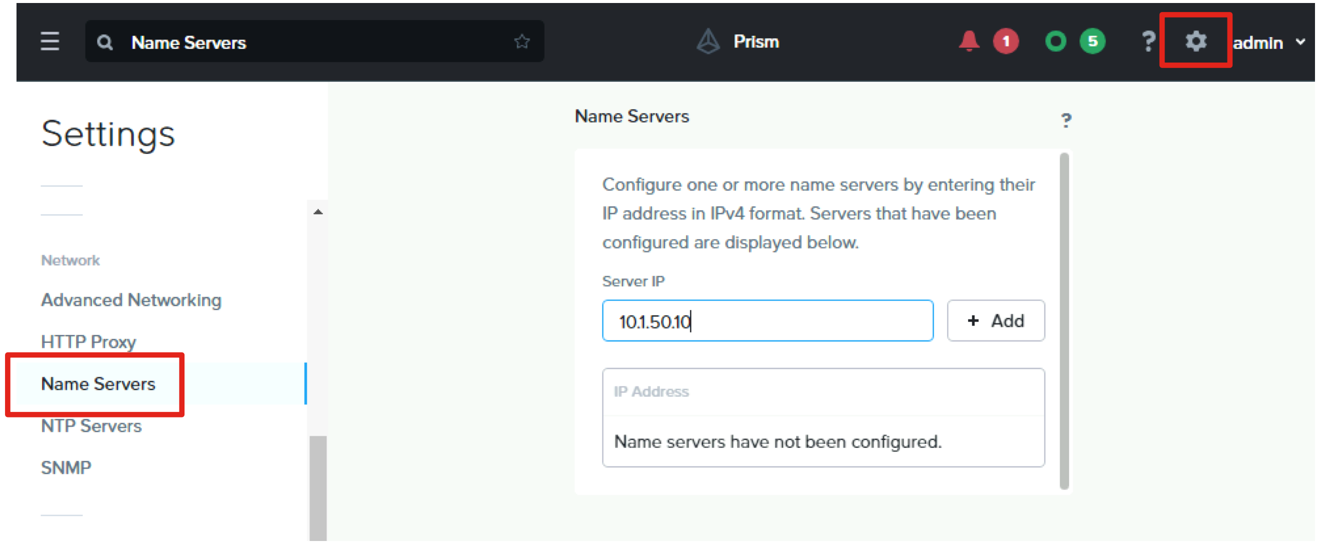
Edit the /etc/hosts file to remove all lines containing any entry similar to “127.0.0.1 NTNX-10-3-190-99-A-CVM” then save the changes and reboot:

```
$ sudo vi /etc/hosts
$ sudo reboot
```

After the reboot, log on to the console and create the Prism Central cluster:

```
$  cluster --cluster_function_list="multicluster" -s <static_ip_address> create
```

Configure DNS in Prism Central



Name Servers

Configure one or more name servers by entering their IP address in IPv4 format. Servers that have been configured are displayed below.

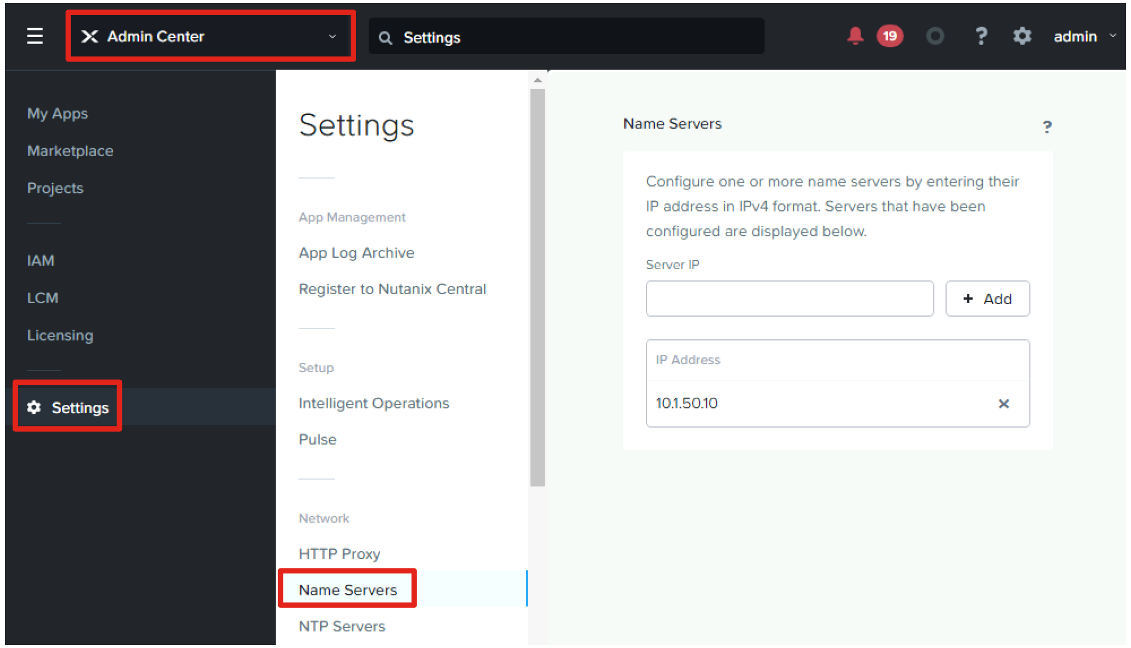
Server IP: 10.1.50.10

+ Add

IP Address

Name servers have not been configured.

Version 2022.6.x



Name Servers

Configure one or more name servers by entering their IP address in IPv4 format. Servers that have been configured are displayed below.

Server IP

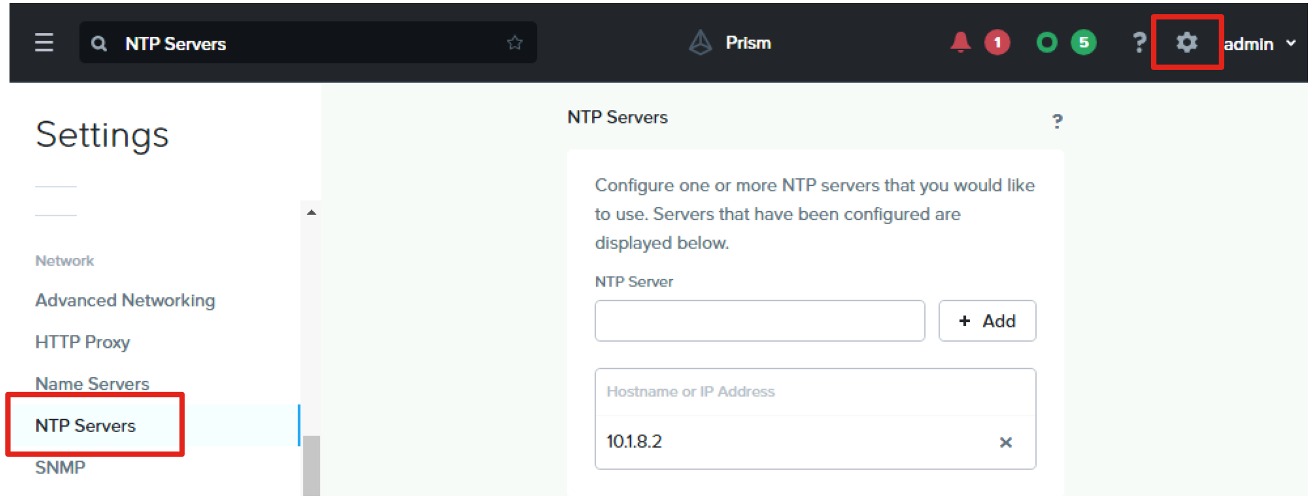
+ Add

IP Address
10.1.50.10

Version 2023.4+

Alert: If Foundation Central was installed before configuring or changing the DNS and NTP server addresses, the Prism Central VM must be rebooted before attempting to install a cluster.

Configure NTP in Prism Central



NTP Servers

Configure one or more NTP servers that you would like to use. Servers that have been configured are displayed below.

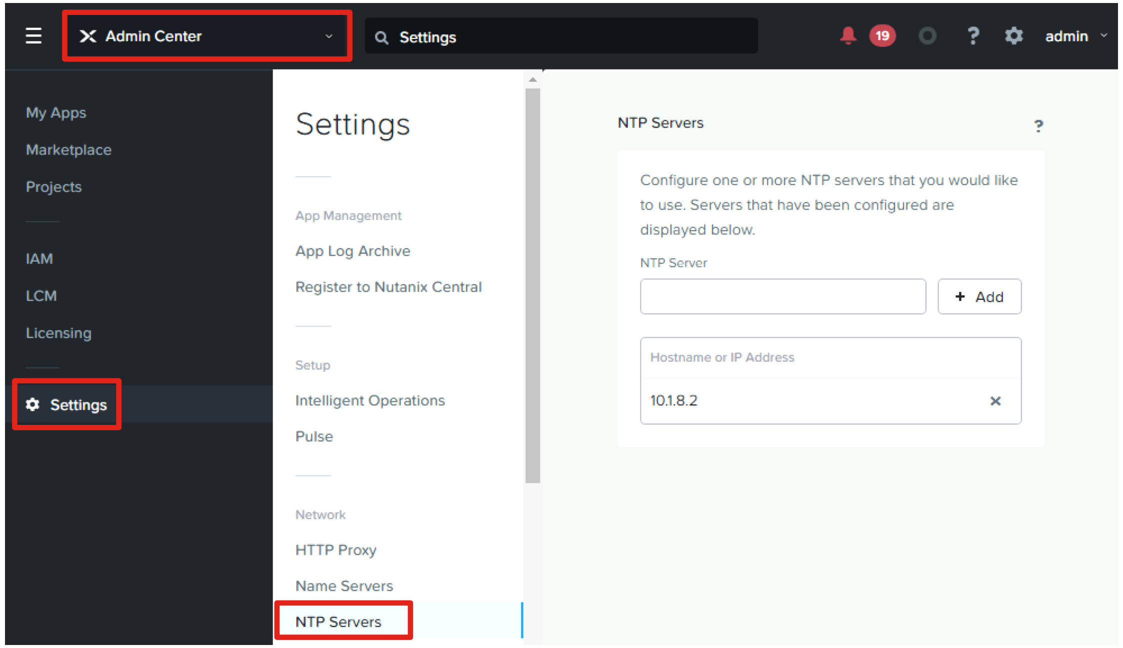
NTP Server

+ Add

Hostname or IP Address

10.1.8.2 ×

Version 2022.6.x



NTP Servers

Configure one or more NTP servers that you would like to use. Servers that have been configured are displayed below.

NTP Server

+ Add

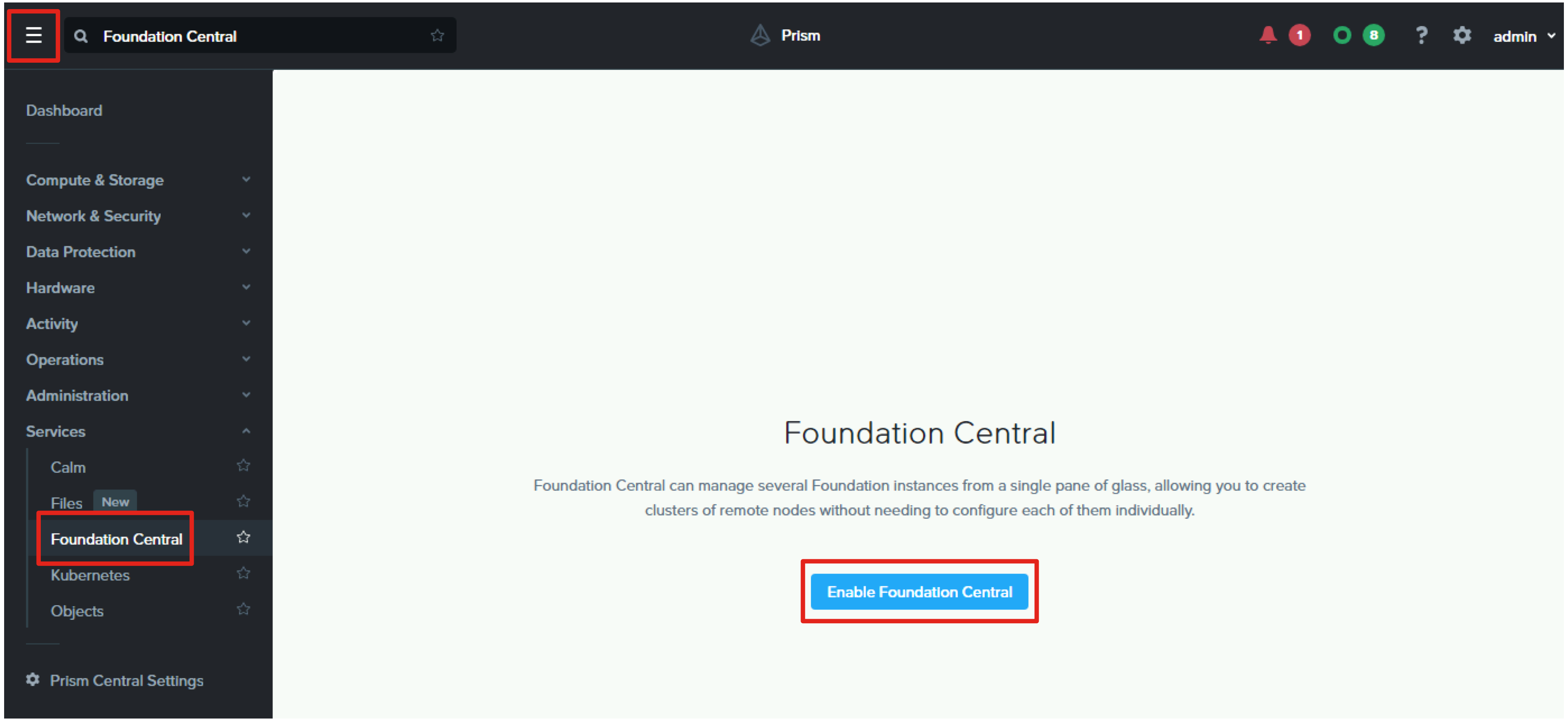
Hostname or IP Address

10.1.8.2 ×

Version 2023.4+

Alert: If Foundation Central was installed before configuring or changing the DNS and NTP server addresses, the Prism Central VM must be rebooted before attempting to install a cluster.

Install Foundation Central in Prism Central 2022.6.x

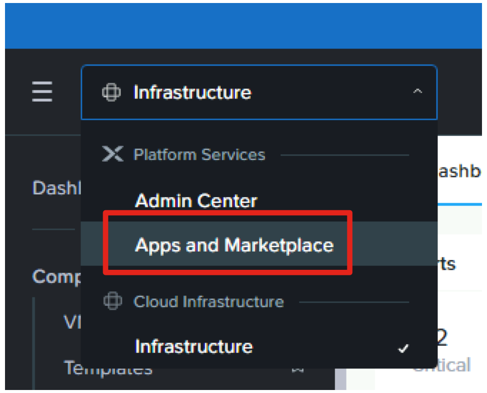


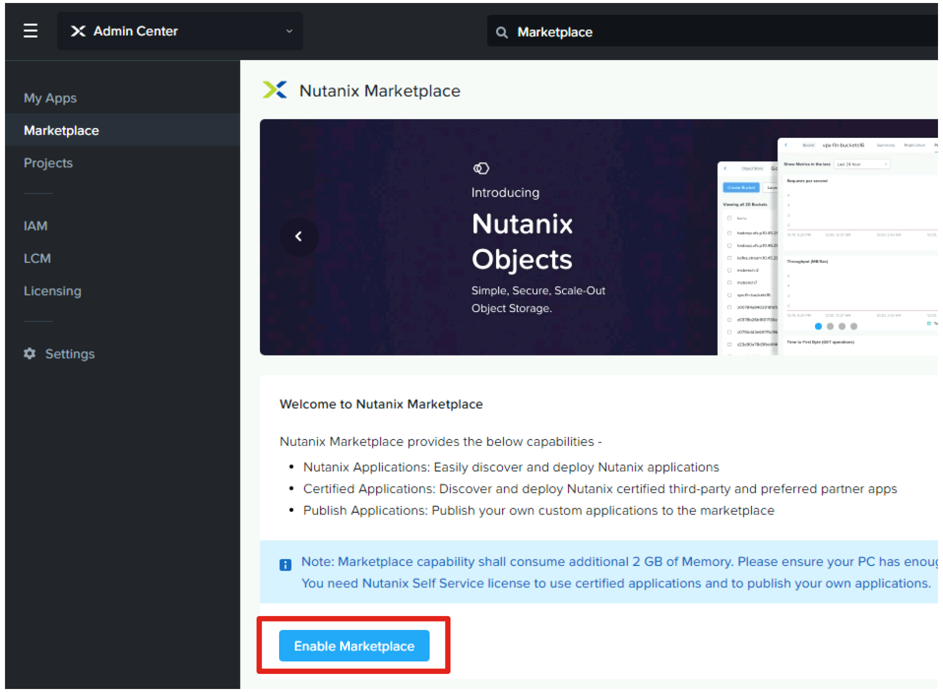
Foundation Central

Foundation Central can manage several Foundation instances from a single pane of glass, allowing you to create clusters of remote nodes without needing to configure each of them individually.

Enable Foundation Central

Install Foundation Central in Prism Central 2023.4+



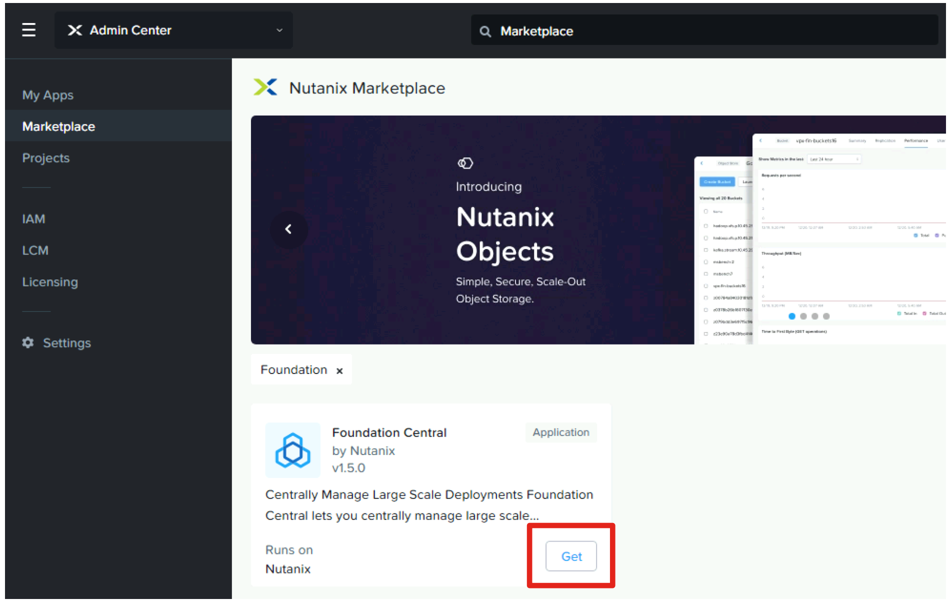


Welcome to Nutanix Marketplace

Nutanix Marketplace provides the below capabilities -

- Nutanix Applications: Easily discover and deploy Nutanix applications
- Certified Applications: Discover and deploy Nutanix certified third-party and preferred partner apps
- Publish Applications: Publish your own custom applications to the marketplace

Note: Marketplace capability shall consume additional 2 GB of Memory. Please ensure your PC has enoug
You need Nutanix Self Service license to use certified applications and to publish your own applications.



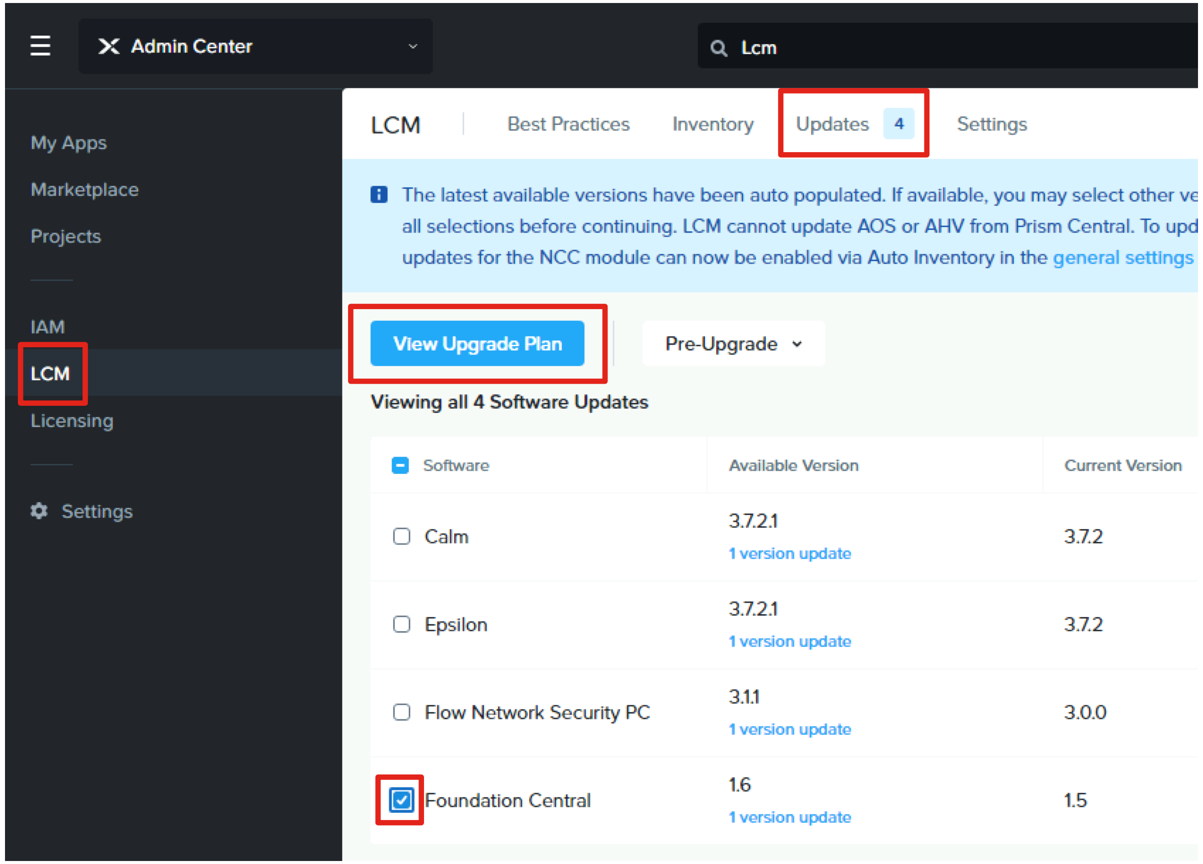
Foundation Central
by Nutanix
v1.5.0

Centrally Manage Large Scale Deployments Foundation Central lets you centrally manage large scale...

Runs on
Nutanix

Note: You must register the cluster that hosts the Prism Central 2023.4+ VM with Prism Central before you can successfully enable the marketplace. The required version of Foundation Central is v.1.6.0+

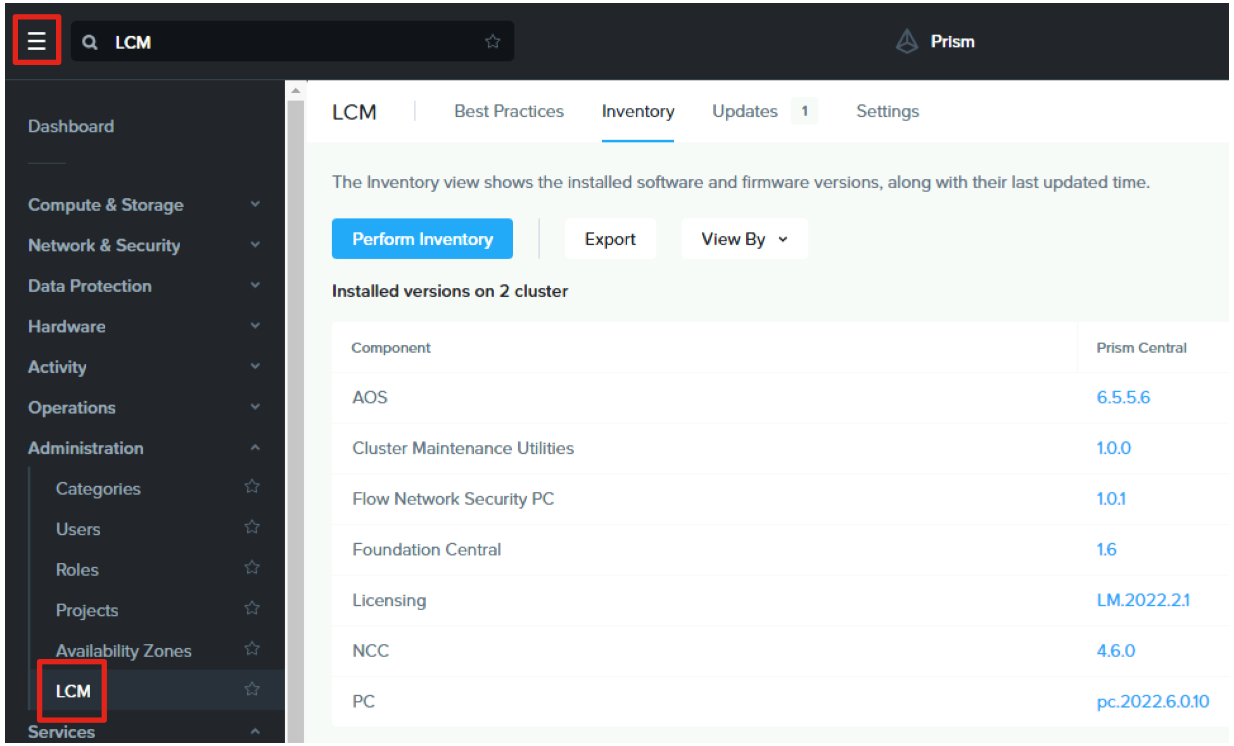
Use LCM to upgrade Foundation Central



The latest available versions have been auto populated. If available, you may select other ve all selections before continuing. LCM cannot update AOS or AHV from Prism Central. To upd updates for the NCC module can now be enabled via Auto Inventory in the general settings

Viewing all 4 Software Updates

Software	Available Version	Current Version
□ Calm	3.7.2.1 1 version update	3.7.2
□ Epsilon	3.7.2.1 1 version update	3.7.2
□ Flow Network Security PC	3.1.1 1 version update	3.0.0
☑ Foundation Central	1.6 1 version update	1.5



The Inventory view shows the installed software and firmware versions, along with their last updated time.

Installed versions on 2 cluster

Component	Prism Central
AOS	6.5.5.6
Cluster Maintenance Utilities	1.0.0
Flow Network Security PC	1.0.1
Foundation Central	1.6
Licensing	LM.2022.2.1
NCC	4.6.0
PC	pc.2022.6.0.10

Note: You must register the cluster that hosts the Prism Central VM with Prism Central before you can successfully run LCM. You may need to run an inventory task once to update LCM, then run an inventory again to scan the system for available updates. The required version of Foundation Central is v.1.6.0+

Upgrade Foundation Central via CLI

In some cases, older versions of Foundation Central running on ESXi may not be upgradeable via LCM and must be upgraded via the CLI. For more information, refer to the following page: https://portal.nutanix.com/page/documents/details?targetId=Field-Installation-Guide-Cisco-HCI-ISM:v1-upgrade-fc-cli-t.html

1. Download the Foundation Central 1.6 dark site bundle and upload it to the Prism Central VM in the /home/nutanix folder.
2. Log on to the CLI of the Prism Central VM as user nutanix and extract the compressed file contents:

```
  $ mkdir /home/nutanix/fc_installer
  $ tar -xf /home/nutanix/lcm_foundation-central_1.6.tar.gz -C /home/nutanix/fc_installer/
```

3. Stop Foundation Central:

```
  $ genesis stop foundation_central
```

4. Remove the existing Foundation Central files:

```
  $ sudo rm -rf /home/docker/foundation_central/*
```

5. Extract the new Foundation Central files to the correct folder:

```
  $ sudo tar -xJf
/home/nutanix/fc_installer/builds/foundation-central-builds/1.6/foundation-central-installer.tar.xz -C
/home/docker/foundation_central/
```

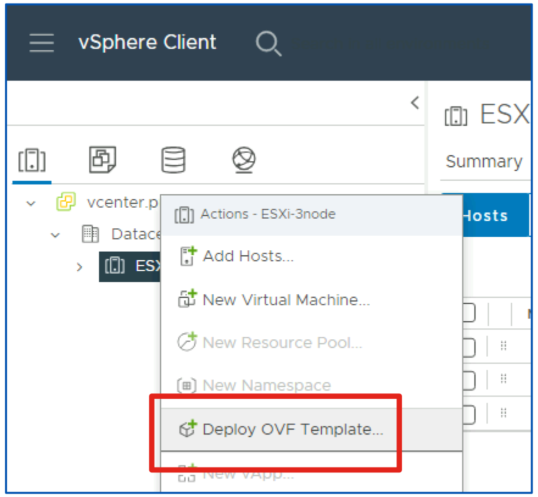
6. Set the directory ownership and permissions:

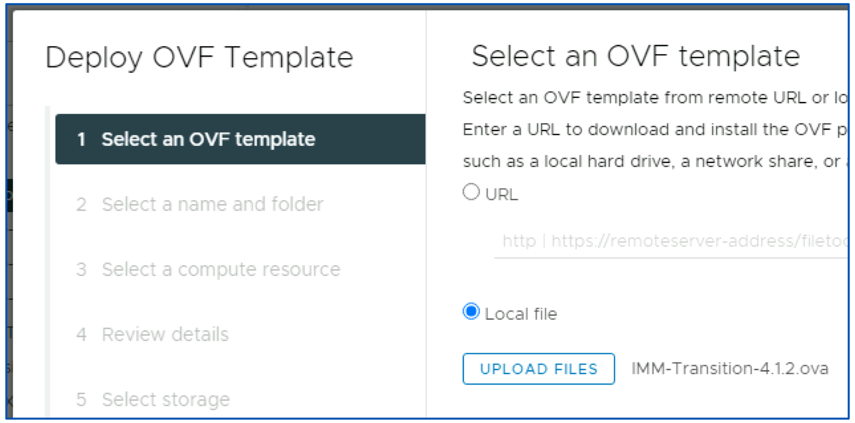
```
  $ sudo chown -R nutanix:nutanix /home/docker/foundation_central/*
```

7. Start the Foundation Central service:

```
  $ cluster start
```

Deploy Cisco IMM Transition Toolkit (optional)




Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage

Select an OVF template

Select an OVF template from remote URL or lo

Enter a URL to download and install the OVF p

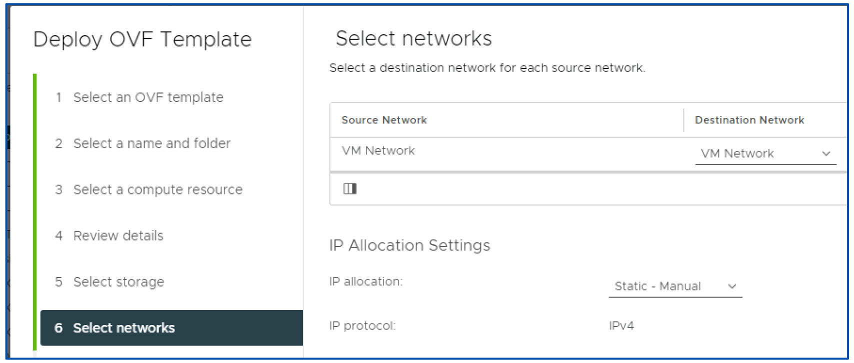
such as a local hard drive, a network share, or

○ URL

http | https://remoteserver-address/fileto

● Local file

UPLOAD FILES IMM-Transition-4.1.2.ova


Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Select networks

Select networks

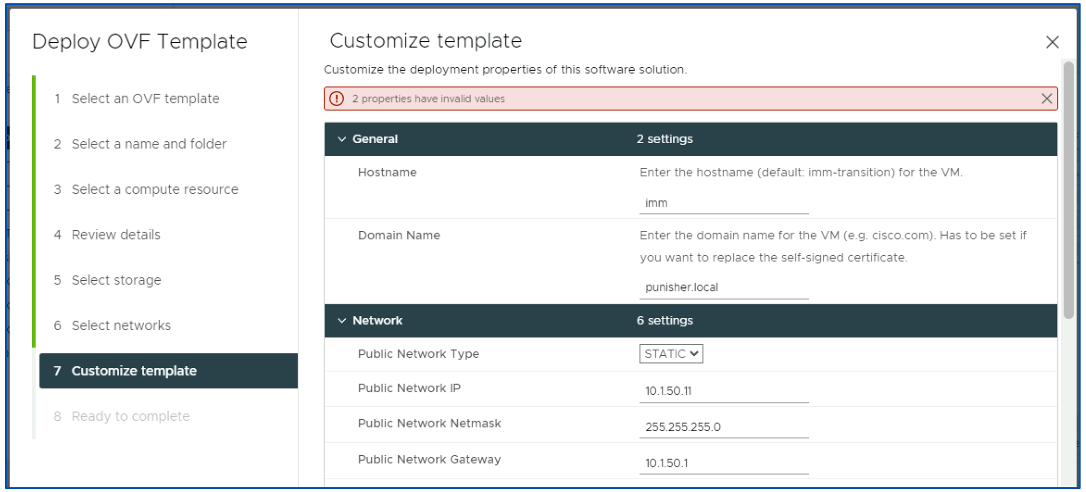
Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4


Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Select networks
7 Customize template
8 Ready to complete

Customize template

Customize the deployment properties of this software solution.

2 properties have invalid values

General — 2 settings

Hostname: Enter the hostname (default: imm-transition) for the VM.
imm

Domain Name: Enter the domain name for the VM (e.g. cisco.com). Has to be set if you want to replace the self-signed certificate.
punisher.local

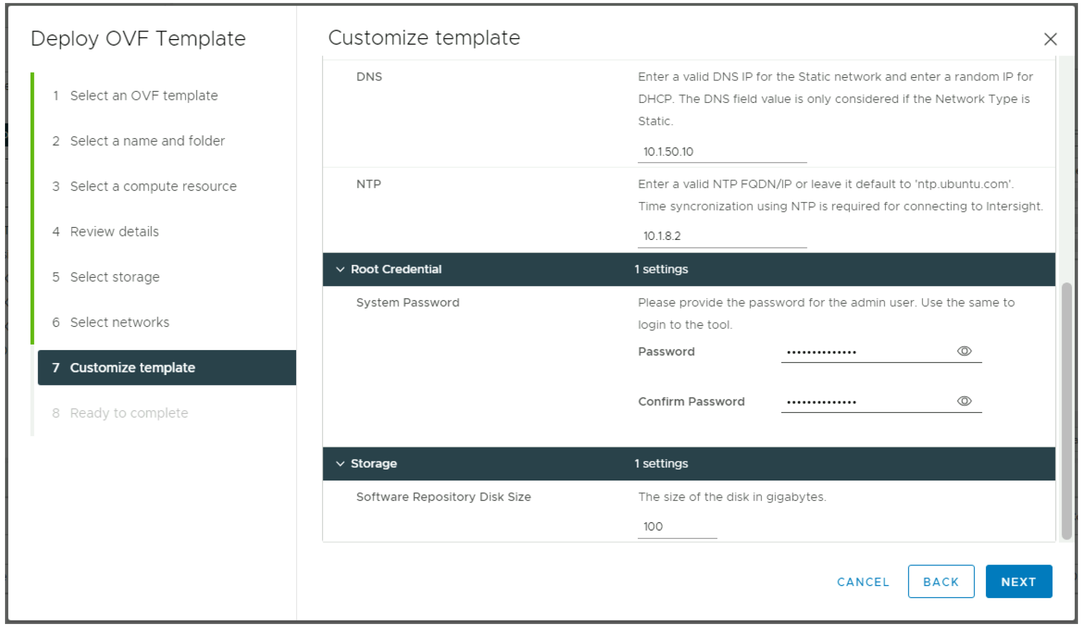
Network — 6 settings

Public Network Type: STATIC

Public Network IP: 10.1.50.11

Public Network Netmask: 255.255.255.0

Public Network Gateway: 10.1.50.1


Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Select networks
7 Customize template
8 Ready to complete

Customize template

DNS: Enter a valid DNS IP for the Static network and enter a random IP for DHCP. The DNS field value is only considered if the Network Type is Static.
10.1.50.10

NTP: Enter a valid NTP FQDN/IP or leave it default to 'ntp.ubuntu.com'. Time syncronization using NTP is required for connecting to Intersight.
10.1.8.2

Root Credential — 1 settings

System Password: Please provide the password for the admin user. Use the same to login to the tool.
Password: •••••••••••••••
Confirm Password: •••••••••••••••

Storage — 1 settings

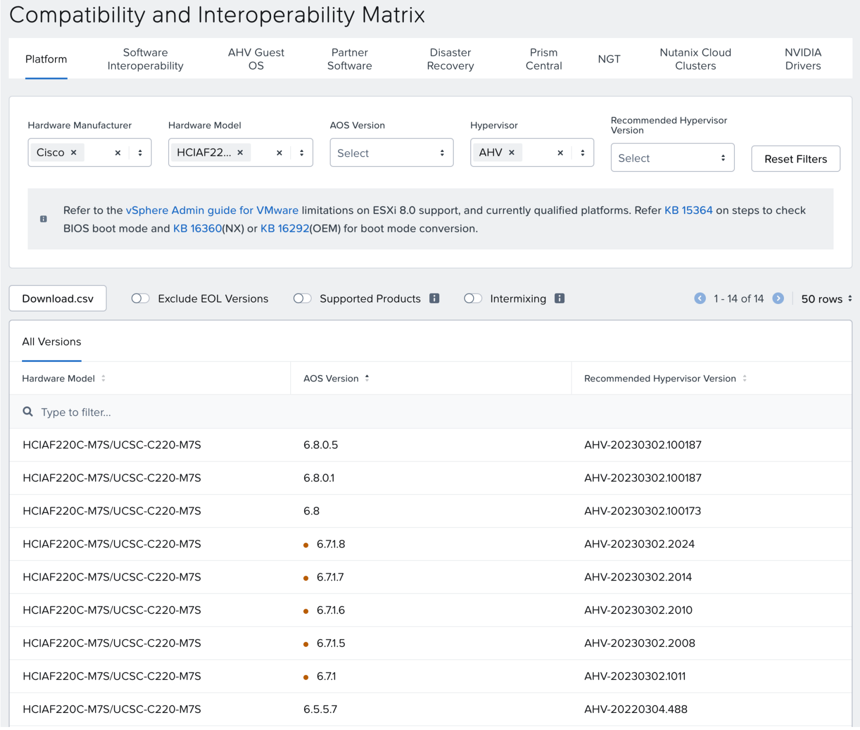
Software Repository Disk Size: The size of the disk in gigabytes.
100

During installation, the factory installed software can be used or the servers can optionally be re-imaged. If so, the Cisco IMM Toolkit provides an easy HTTP server which can host the AOS, AHV and ESXi installation files. Any anonymous HTTP server can be used. Download the latest IMM Transition Toolkit OVA from here: https://ucstools.cloudapps.cisco.com/#/downloadApp

Download AOS Software and Verify Compatibility

Consult the Nutanix Compatibility and Interoperability matrix here:
https://portal.nutanix.com/page/documents/compatibility-interoperability-matrix

Download a supported Nutanix AOS STS or LTS image and the AHV installer here:
https://portal.nutanix.com/page/downloads/list



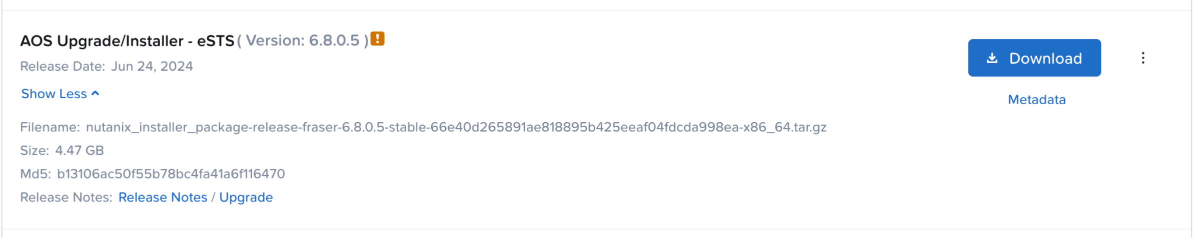
Compatibility and Interoperability Matrix

Hardware Manufacturer: Cisco
Hardware Model: HCIAF22...
AOS Version: Select
Hypervisor: AHV
Recommended Hypervisor Version: Select

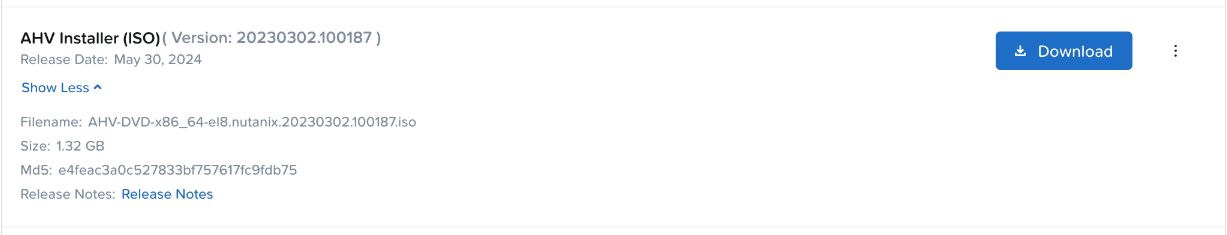
Refer to the vSphere Admin guide for VMware limitations on ESXi 8.0 support, and currently qualified platforms. Refer KB 15364 on steps to check BIOS boot mode and KB 16360(NX) or KB 16292(OEM) for boot mode conversion.

○ Exclude EOL Versions ○ Supported Products ○ Intermixing

Hardware Model	AOS Version	Recommended Hypervisor Version
HCIAF220C-M7S/UCSC-C220-M7S	6.8.0.5	AHV-20230302.100187
HCIAF220C-M7S/UCSC-C220-M7S	6.8.0.1	AHV-20230302.100187
HCIAF220C-M7S/UCSC-C220-M7S	6.8	AHV-20230302.100173
HCIAF220C-M7S/UCSC-C220-M7S	● 6.7.1.8	AHV-20230302.2024
HCIAF220C-M7S/UCSC-C220-M7S	● 6.7.1.7	AHV-20230302.2014
HCIAF220C-M7S/UCSC-C220-M7S	● 6.7.1.6	AHV-20230302.2010
HCIAF220C-M7S/UCSC-C220-M7S	● 6.7.1.5	AHV-20230302.2008
HCIAF220C-M7S/UCSC-C220-M7S	● 6.7.1	AHV-20230302.1011
HCIAF220C-M7S/UCSC-C220-M7S	6.5.5.7	AHV-20220304.488



AOS Upgrade/Installer - eSTS (Version: 6.8.0.5) !
Release Date: Jun 24, 2024
Filename: nutanix_installer_package-release-fraser-6.8.0.5-stable-66e40d265891ae818895b425eeaf04fdcda998ea-x86_64.tar.gz
Size: 4.47 GB
Md5: b13106ac50f55b78bc4fa41a6f116470
Release Notes: Release Notes / Upgrade



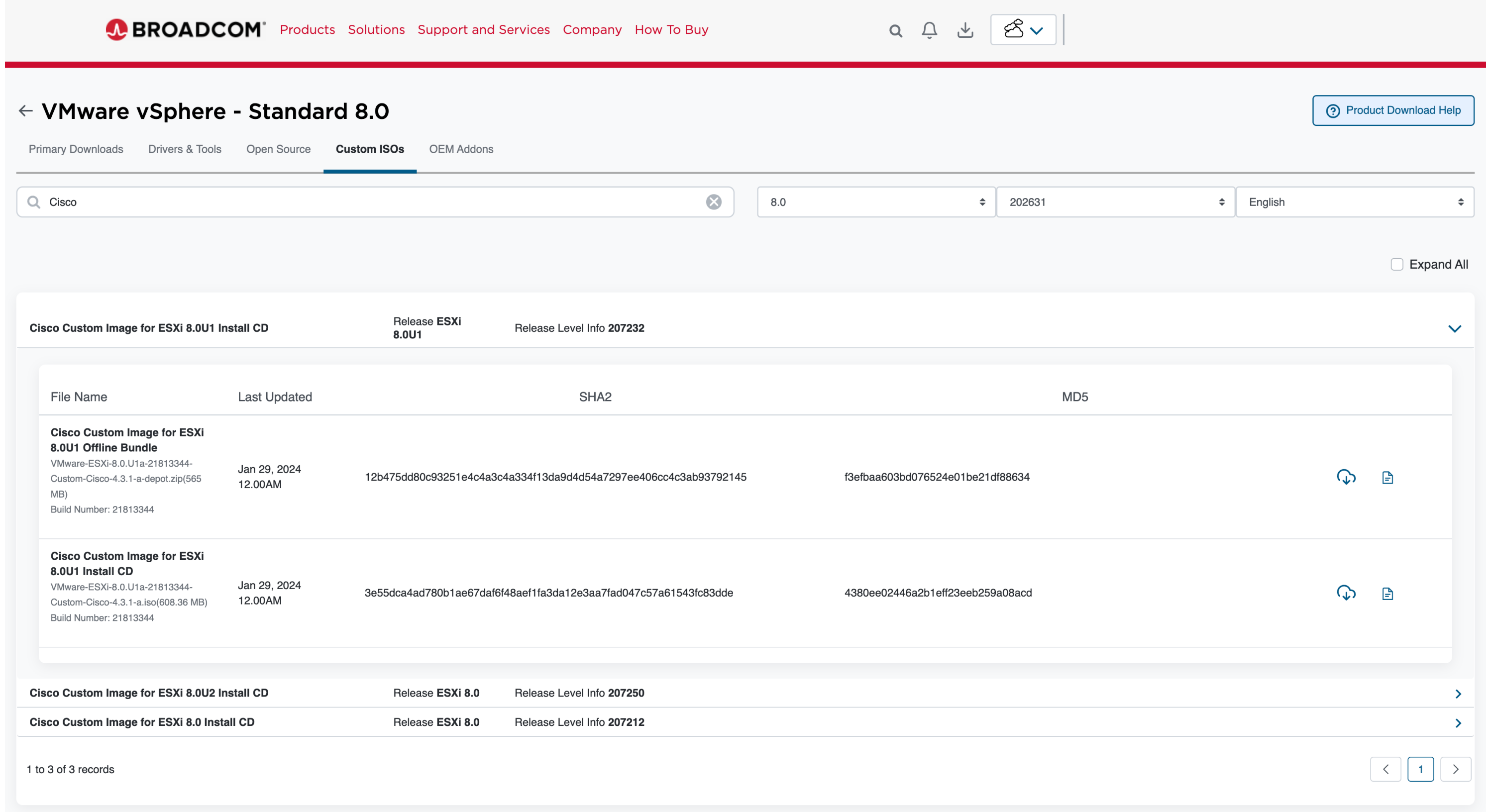
AHV Installer (ISO) (Version: 20230302.100187)
Release Date: May 30, 2024
Filename: AHV-DVD-x86_64-el8.nutanix.20230302.100187.iso
Size: 1.32 GB
Md5: e4feac3a0c527833bf757617fc9fdb75
Release Notes: Release Notes

Note: Starting with AOS 6.8 the AOS installer file no longer includes the AHV installer, so the AHV installer file must be downloaded separately and used during the installation.

Download VMware Software

Download the supported and compatible Cisco custom ESXi ISOs here: https://support.broadcom.com/group/ecx/productfiles?subFamily=VMware%20vSphere&displayGroup=VMware%20vSphere%20-%20Standard&release=8.0&os=&servicePk=202631&language=EN

Note: ESXi 8.0 is only supported with AOS short-term support versions (STS) at this time.



VMware vSphere - Standard 8.0

Search: Cisco | 8.0 | 202631 | English

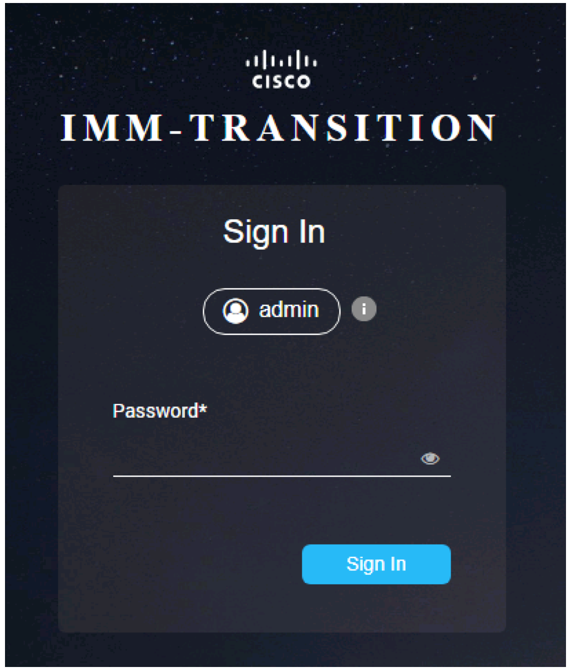
Name	Release	Release Level Info
Cisco Custom Image for ESXi 8.0U1 Install CD	Release **ESXi 8.0U1**	Release Level Info **207232**

File Name	Last Updated	SHA2	MD5
Cisco Custom Image for ESXi 8.0U1 Offline Bundle VMware-ESXi-8.0.U1a-21813344-Custom-Cisco-4.3.1-a-depot.zip(565 MB) Build Number: 21813344	Jan 29, 2024 12.00AM	12b475dd80c93251e4c4a3c4a334f13da9d4d54a7297ee406cc4c3ab93792145	f3efbaa603bd076524e01be21df88634
Cisco Custom Image for ESXi 8.0U1 Install CD VMware-ESXi-8.0.U1a-21813344-Custom-Cisco-4.3.1-a.iso(608.36 MB) Build Number: 21813344	Jan 29, 2024 12.00AM	3e55dca4ad780b1ae67daf6f48aef1fa3da12e3aa7fad047c57a61543fc83dde	4380ee02446a2b1eff23eeb259a08acd

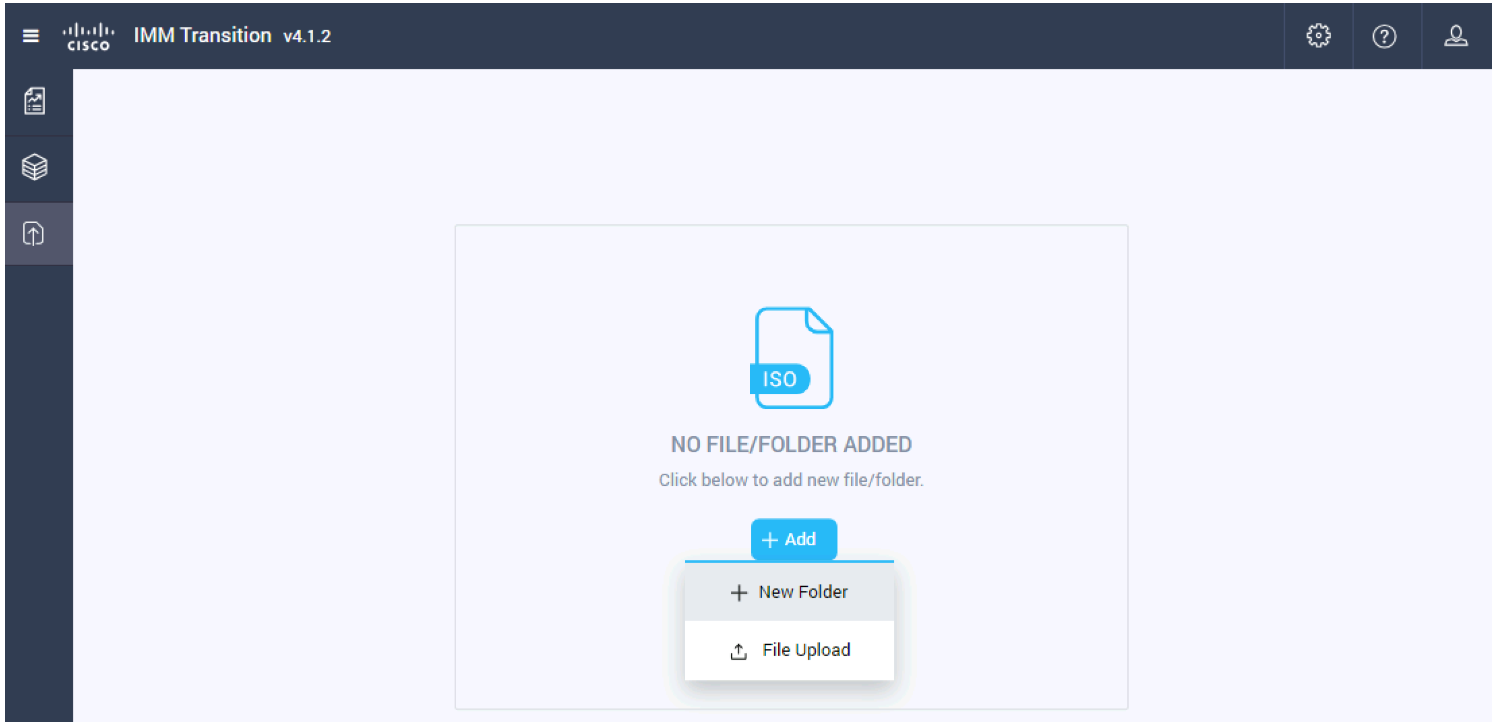
Name	Release	Release Level Info
Cisco Custom Image for ESXi 8.0U2 Install CD	Release **ESXi 8.0**	Release Level Info **207250**
Cisco Custom Image for ESXi 8.0 Install CD	Release **ESXi 8.0**	Release Level Info **207212**

1 to 3 of 3 records

Upload Files to IMM Transition Toolkit

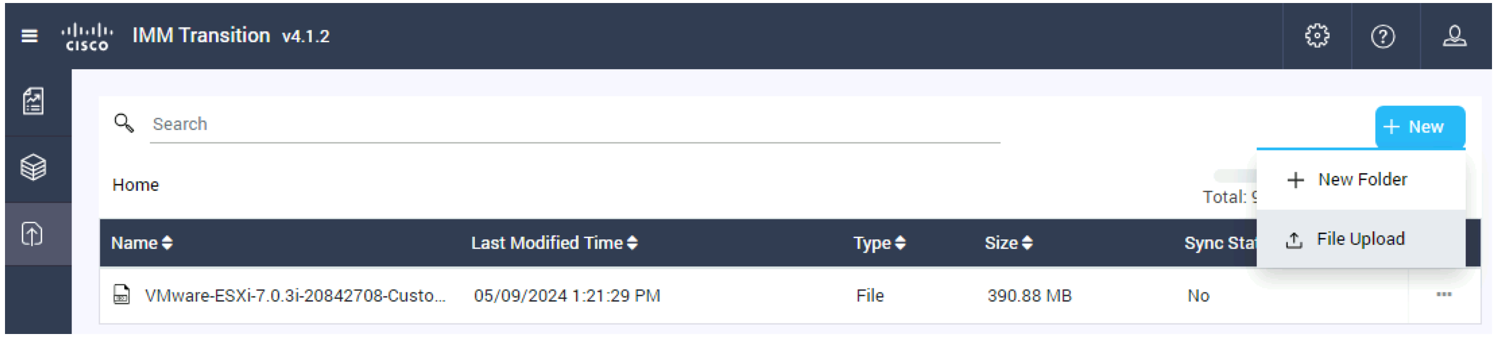


Log in via a web browser. Create a folder for storing the Nutanix installation files if desired.
Click on File Upload, then drag-and-drop the AOS, AHV and/or ESXi installation files you will use for the cluster installations.



NO FILE/FOLDER ADDED

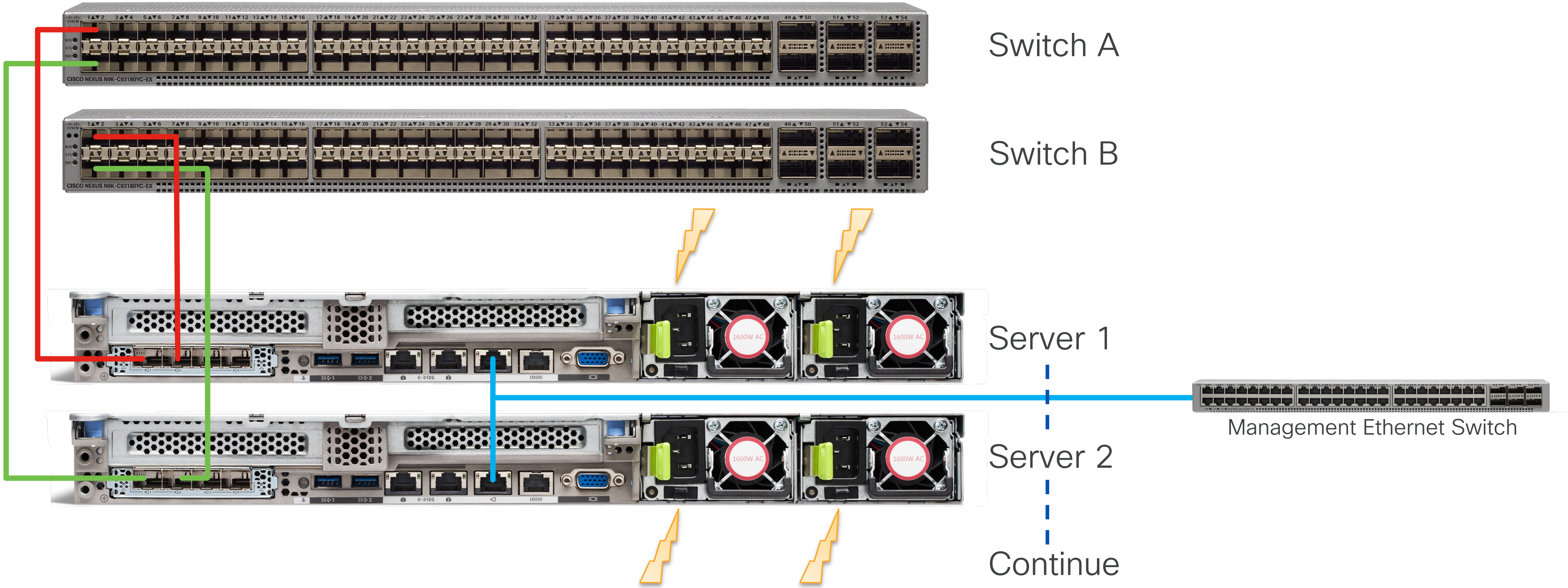
Click below to add new file/folder.



Name	Last Modified Time	Type	Size	Sync Stat
VMware-ESXi-7.0.3i-20842708-Custo...	05/09/2024 1:21:29 PM	File	390.88 MB	No

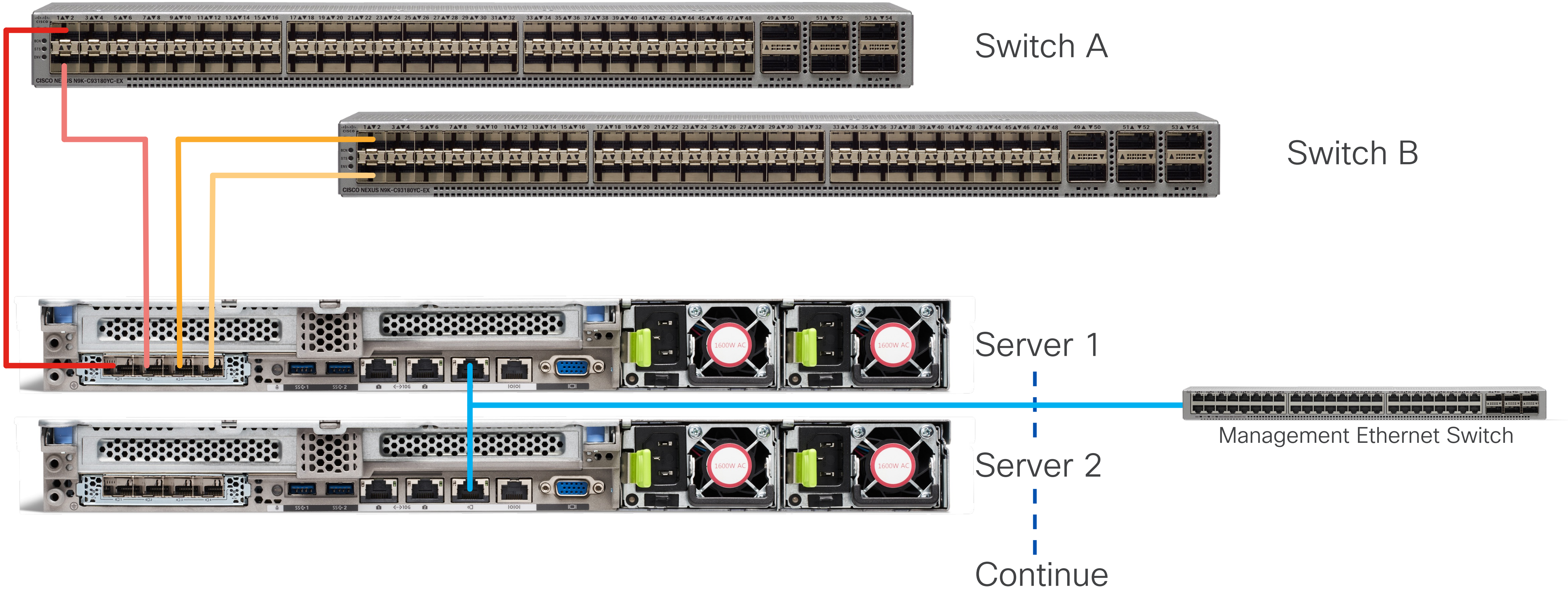
Server Cabling – 2 Port Adapters or 2 Cable Method

Note: Dual switches or a stacked dual switch config with 2 cables per server is the minimum recommended network configuration. The card can be a Cisco VIC MLoM card, a Cisco VIC PCIe card or a third-party PCIe NIC. Connect the dedicated CIMC interfaces to a management switch or access ports for management traffic on a dedicated VLAN.



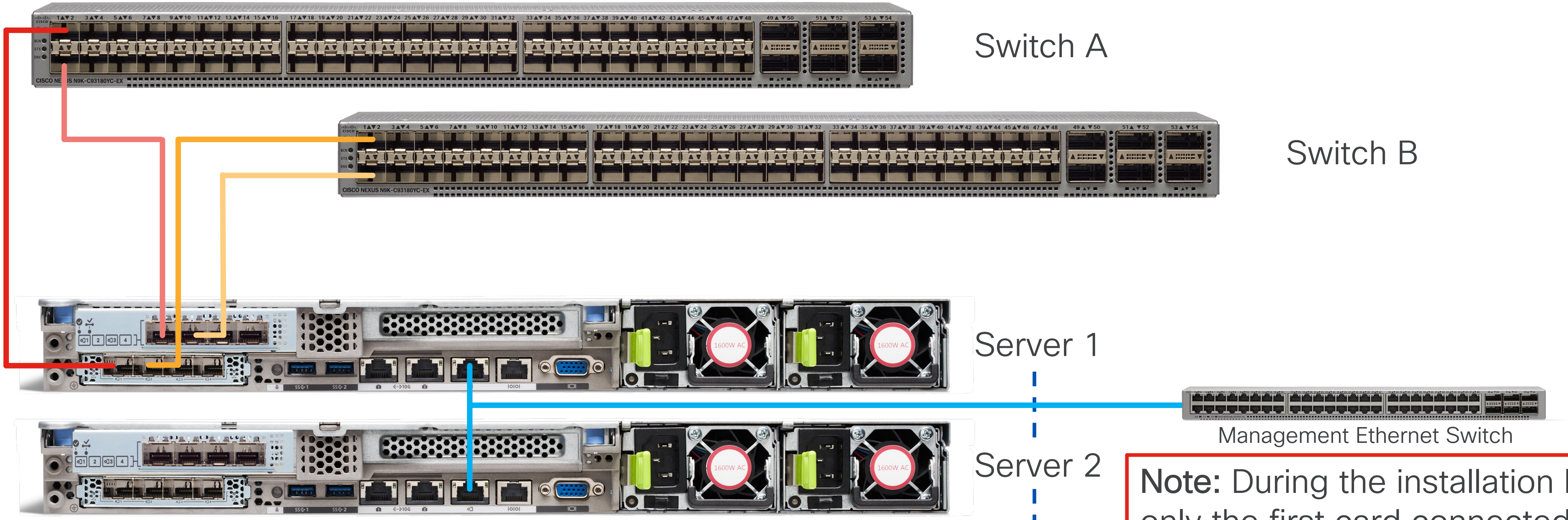
Server Cabling – 4 Port Adapters or 4 cable method

Note: When using 4 ports per server, use ports 1 and 2 to switch A, ports 3 and 4 to switch B. Repeat this pattern for all servers. The card can be a Cisco VIC MLoM card, a Cisco VIC PCIe card or a third-party PCIe NIC. Connect the dedicated CIMC interfaces to a management switch or access ports for management traffic on a dedicated VLAN.



Alternate Server Cabling – Dual VIC/NIC

Note: When using 4 ports in a dual VIC or NIC config per server, use port 1 from each VIC or NIC to switch A and port 2 from each VIC or NIC to switch B. The cards can be Cisco VIC MLoM and PCIe cards or two third-party PCIe NICs. Repeat this pattern for all servers. Connect the dedicated CIMC interfaces to a management switch or access ports for management traffic on a dedicated VLAN.



Note: During the installation leave only the first card connected, then connect the cables to the second cards after the installation is completed.

Warning: Do not mix Cisco VIC cards with 3rd-party NICs

Network Port Configurations

- Network ports can be in access mode or trunk mode
- Use trunk mode when multiple VLANs will be presented to the servers, i.e. one for management and others for guest VM traffic. Providing a VLAN ID during installation will place the host ports into trunk mode.
- Use access mode when all traffic will use one VLAN. Leaving the VLAN ID blank during installation will place the host ports into access mode.
- Cisco VIC cards with interfaces set to access mode will always carry a VLAN ID header with no ID set. Some 3rd-party switches may not function properly in this configuration and may need their interfaces set to be trunks with a native VLAN ID set instead of access mode.
- Management interfaces for the CIMC ports should be access ports in the appropriate VLAN.
- Even if LACP is planned for use, do not configure port-channels prior to installation, they will be configured later after the cluster is installed.
- MTU 9216 is not required but recommended in case jumbo frames are ever used in the future.

Trunk ports

```
interface Ethernet1/6
  switchport mode trunk
  switchport trunk allowed vlan 11-13
  spanning-tree port type edge trunk
  mtu 9216
```

Access ports

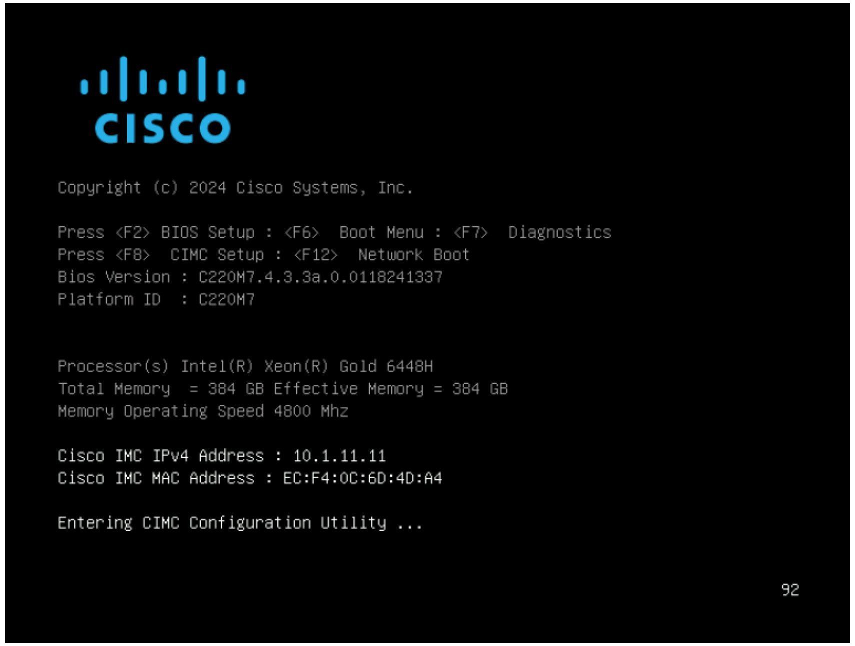
```
interface Ethernet1/6
  switchport mode access
  switchport access vlan 11
  mtu 9216
```

Trunk ports with native VLAN

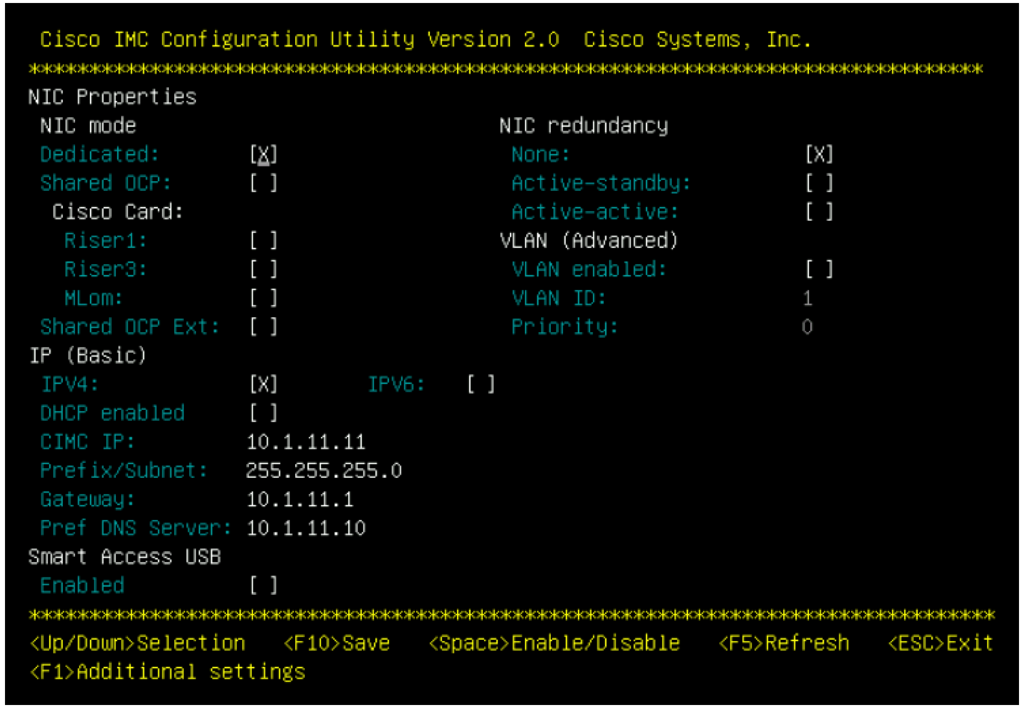
```
interface Ethernet1/6
  switchport mode trunk
  switchport trunk allowed vlan 11-13
  switchport trunk native vlan 11
  spanning-tree port type edge trunk
  mtu 9216
```

CIMC Configuration

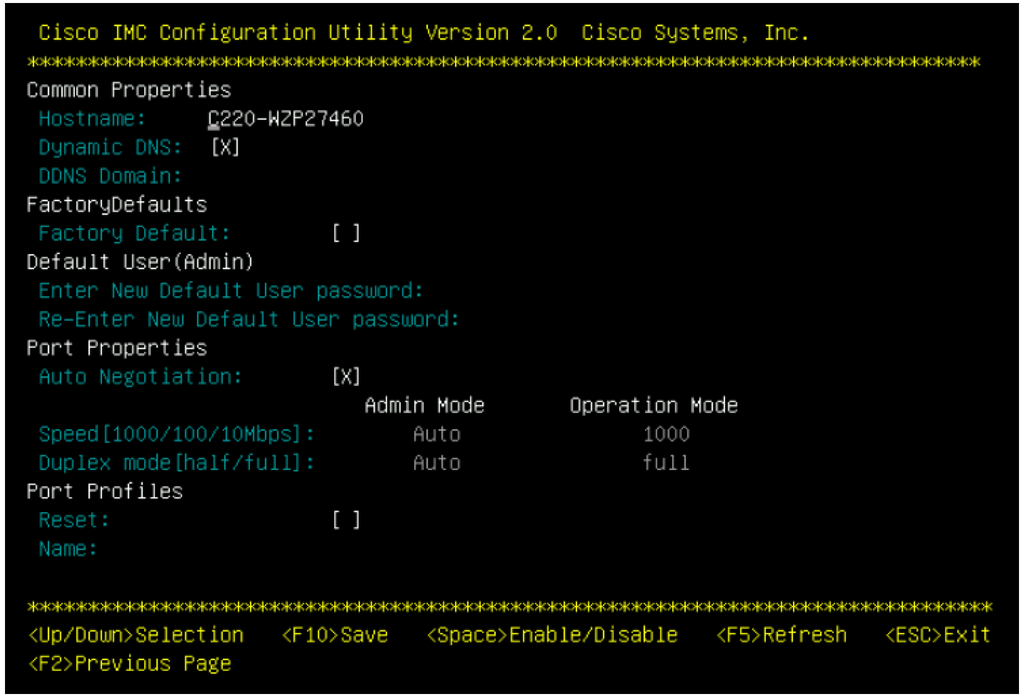
- Connect the KVM dongle and a crash cart to the server
- Press F8 during boot to configure the CIMC
- Default username: admin password: password
- Set to use the dedicated CIMC interface with no redundancy, a static IP address and valid DNS
- Press F1 to go to the second screen to change the password, press F10 to save



```
Copyright (c) 2024 Cisco Systems, Inc.

Press <F2> BIOS Setup : <F6>  Boot Menu : <F7>  Diagnostics
Press <F8>  CIMC Setup : <F12>  Network Boot
Bios Version : C220M7.4.3.3a.0.0118241337
Platform ID  : C220M7


Processor(s) Intel(R) Xeon(R) Gold 6448H
Total Memory  = 384 GB Effective Memory = 384 GB
Memory Operating Speed 4800 Mhz

Cisco IMC IPv4 Address : 10.1.11.11
Cisco IMC MAC Address : EC:F4:0C:6D:4D:A4

Entering CIMC Configuration Utility ...

                                                            92
```

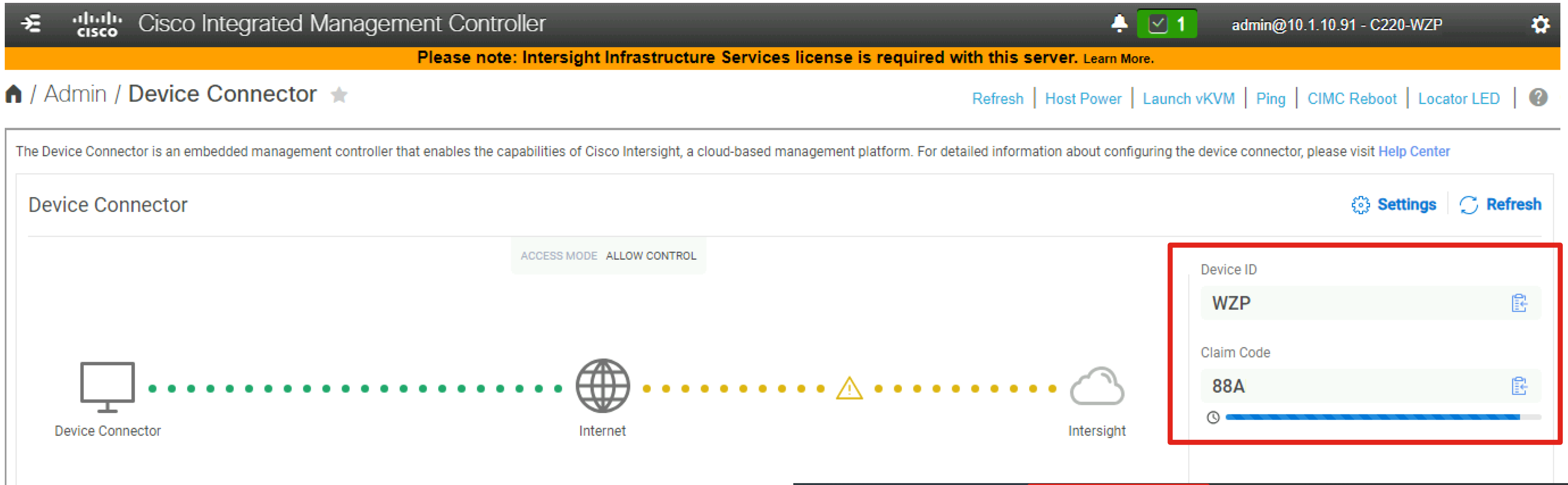


```
 Cisco IMC Configuration Utility Version 2.0  Cisco Systems, Inc.
********************************************************************************
NIC Properties
 NIC mode                                NIC redundancy
 Dedicated:        [X]                    None:                  [X]
 Shared OCP:       [ ]                    Active-standby:        [ ]
  Cisco Card:                             Active-active:         [ ]
   Riser1:         [ ]                   VLAN (Advanced)
   Riser3:         [ ]                    VLAN enabled:          [ ]
   MLom:           [ ]                    VLAN ID:               1
 Shared OCP Ext:   [ ]                    Priority:              0
IP (Basic)
 IPV4:             [X]       IPV6:    [ ]
 DHCP enabled      [ ]
 CIMC IP:          10.1.11.11
 Prefix/Subnet:    255.255.255.0
 Gateway:          10.1.11.1
 Pref DNS Server:  10.1.11.10
Smart Access USB
 Enabled           [ ]
********************************************************************************
<Up/Down>Selection   <F10>Save   <Space>Enable/Disable   <F5>Refresh   <ESC>Exit
<F1>Additional settings
```



```
 Cisco IMC Configuration Utility Version 2.0  Cisco Systems, Inc.
********************************************************************************
Common Properties
 Hostname:     C220-WZP27460
 Dynamic DNS:  [X]
 DDNS Domain:
FactoryDefaults
 Factory Default:       [ ]
Default User(Admin)
 Enter New Default User password:
 Re-Enter New Default User password:
Port Properties
 Auto Negotiation:      [X]
                                 Admin Mode       Operation Mode
 Speed[1000/100/10Mbps]:            Auto              1000
 Duplex mode[half/full]:            Auto              full
Port Profiles
 Reset:                 [ ]
 Name:

********************************************************************************
<Up/Down>Selection   <F10>Save   <Space>Enable/Disable   <F5>Refresh   <ESC>Exit
<F2>Previous Page
```

Claim Servers in Cisco Intersight



Cisco Integrated Management Controller

admin@10.1.10.91 - C220-WZP

Please note: Intersight Infrastructure Services license is required with this server. Learn More.

/ Admin / Device Connector

Refresh | Host Power | Launch vKVM | Ping | CIMC Reboot | Locator LED |

The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit Help Center

Device Connector

Settings Refresh

ACCESS MODE ALLOW CONTROL

Device ID

WZP

Claim Code

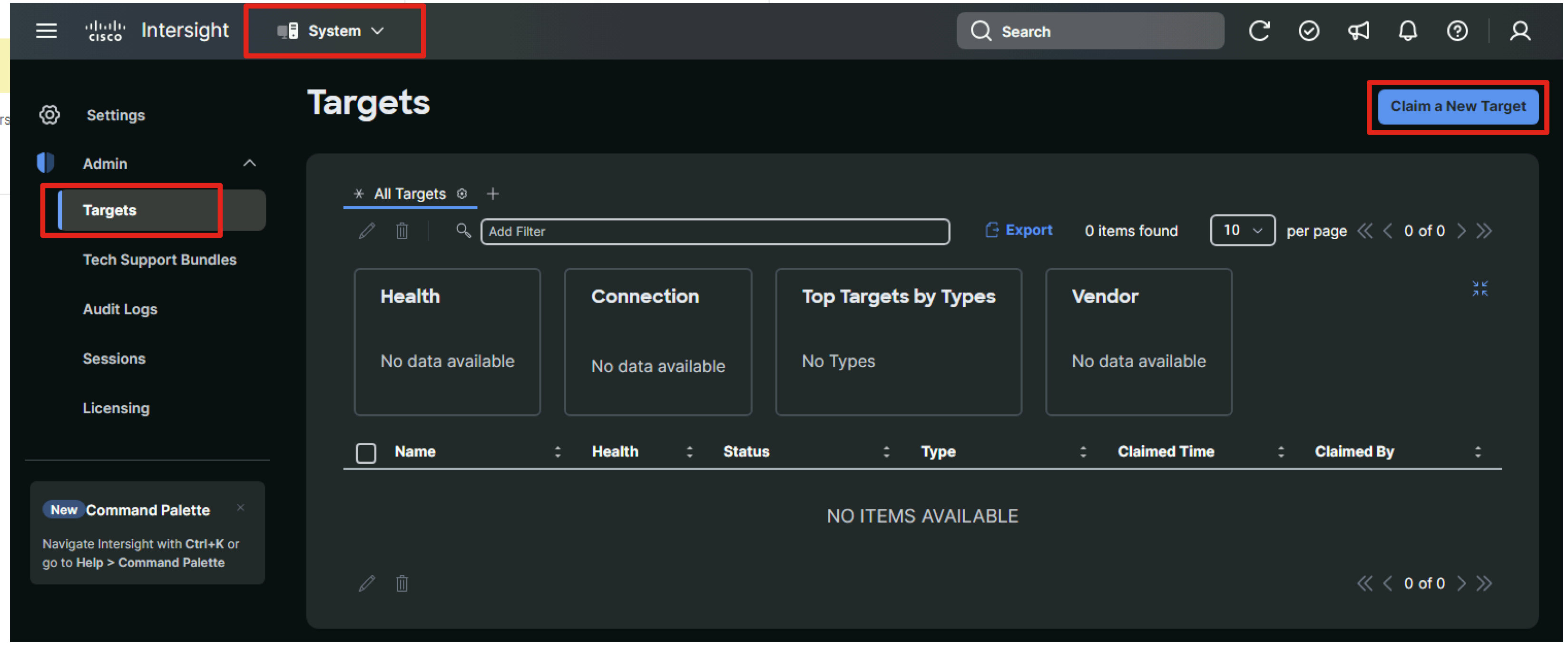
88A

Not Claimed

The connection to the Cisco Intersight Portal is successful, but device is still not claimed. To claim the device open Cisco Inters
or go to the Targets page and click Claim a New Device for existing account.

1.0.11-3533

Log in to the CIMC interface with a web browser using the IP address you set. Retrieve the Device ID and the Claim Code from the CIMC web UI, under Admin > Device Connector



Intersight | System

Search

Settings

Admin

Targets

Tech Support Bundles

Audit Logs

Sessions

Licensing

New Command Palette

Navigate Intersight with Ctrl+K or go to Help > Command Palette

Targets

Claim a New Target

All Targets

Add Filter | Export | 0 items found | 10 per page | 0 of 0

Health	Connection	Top Targets by Types	Vendor
No data available	No data available	No Types	No data available

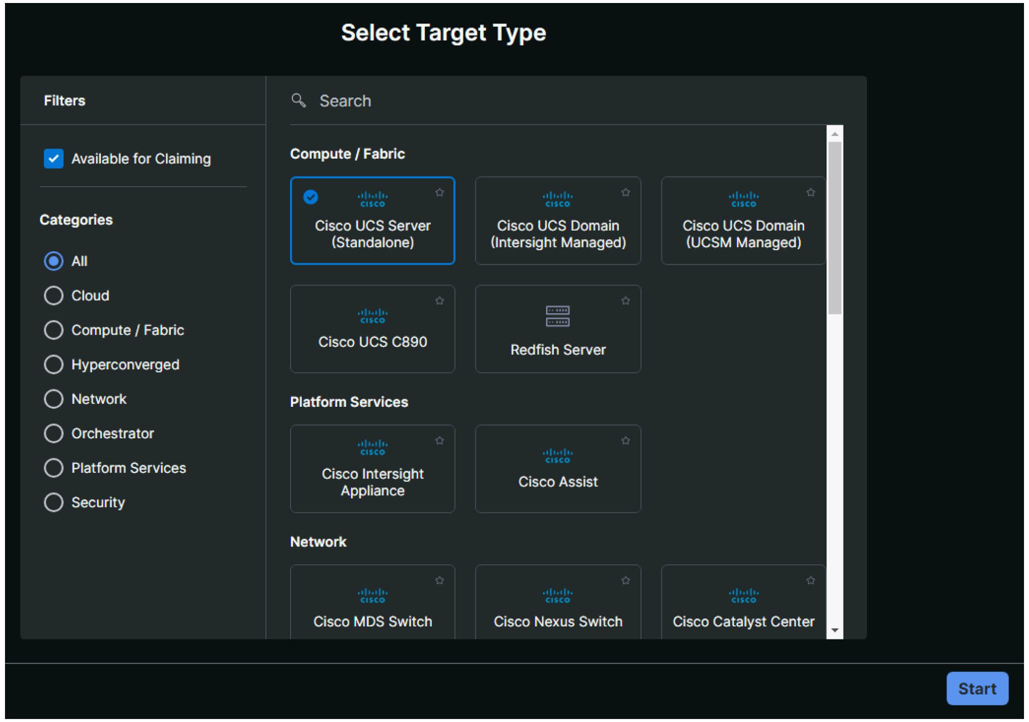
Name	Health	Status	Type	Claimed Time	Claimed By

NO ITEMS AVAILABLE

0 of 0

In Cisco Intersight, go to the System area, click on Targets, then Claim a New Target

Claim Servers in Cisco Intersight Continued

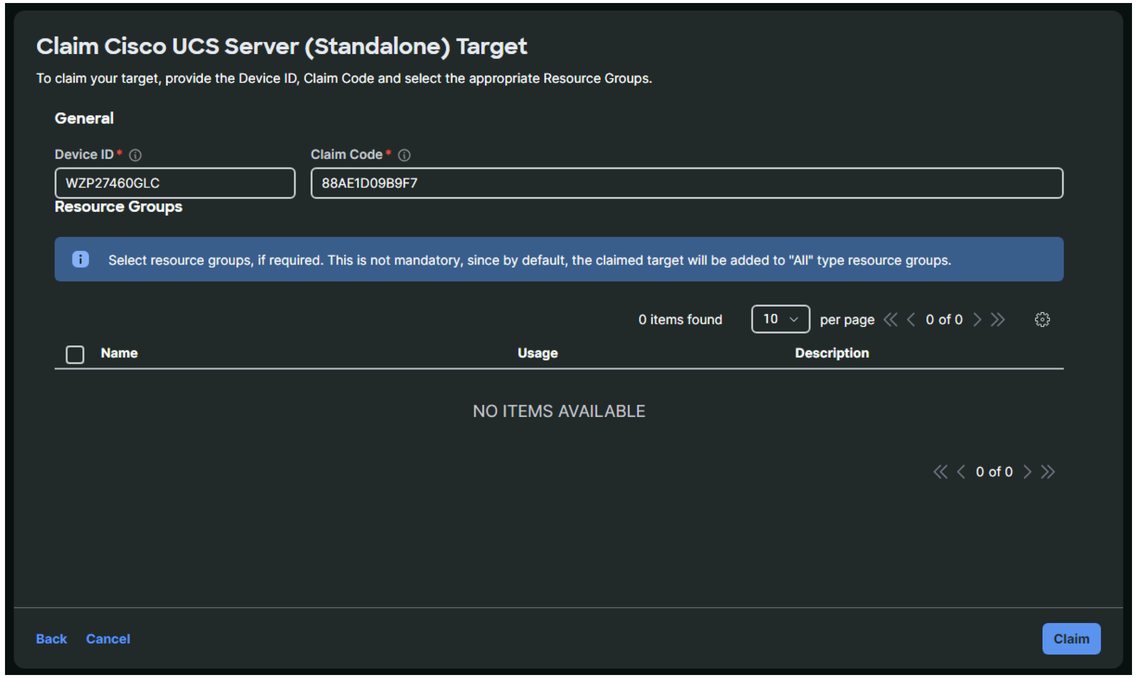


Select Target Type

☑ Available for Claiming

Categories: ● All

Compute / Fabric: ☑ Cisco UCS Server (Standalone)



Claim Cisco UCS Server (Standalone) Target

To claim your target, provide the Device ID, Claim Code and select the appropriate Resource Groups.

General

Device ID *: WZP27460GLC

Claim Code *: 88AE1D09B9F7

Resource Groups

Select resource groups, if required. This is not mandatory, since by default, the claimed target will be added to "All" type resource groups.

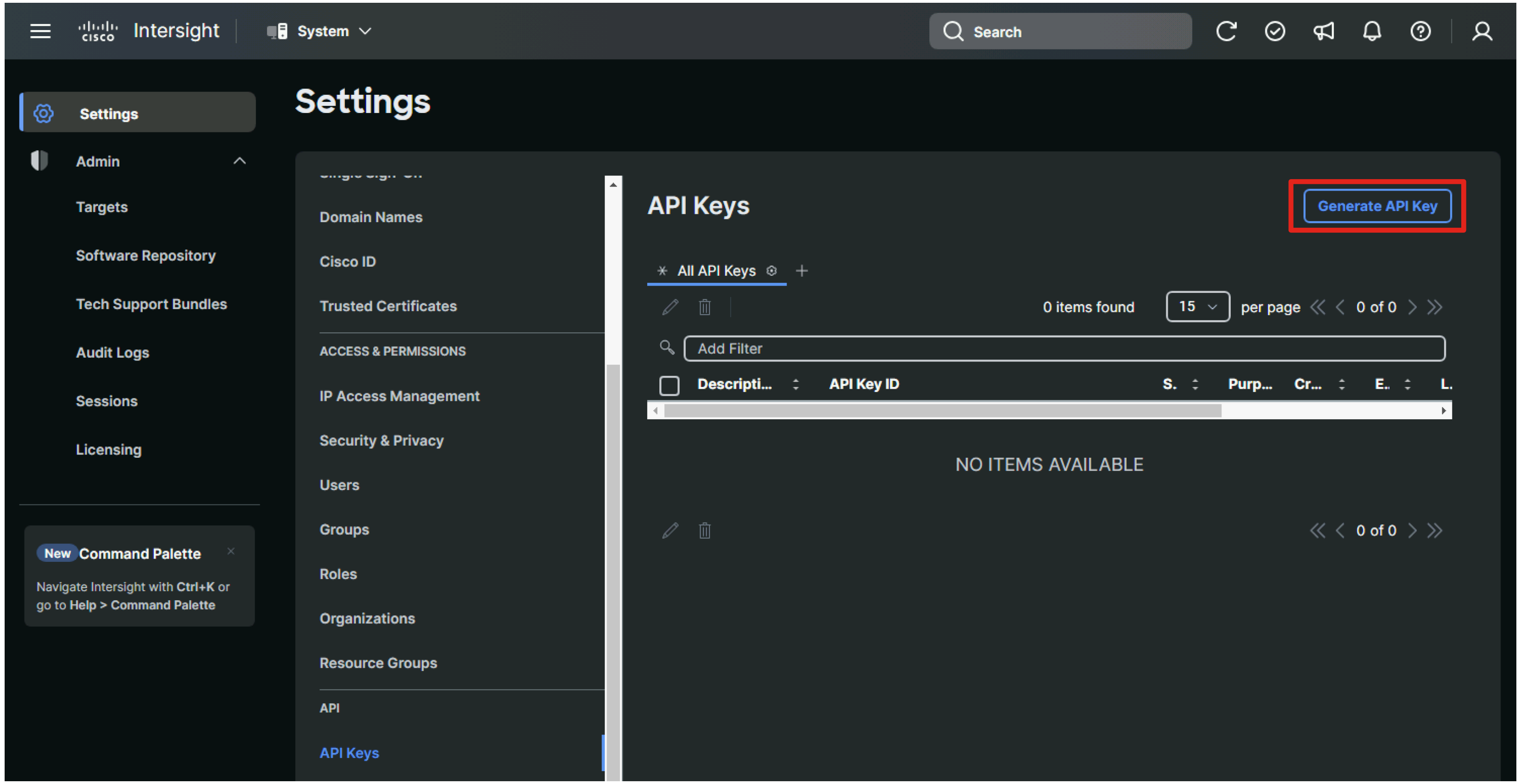
0 items found 10 per page 0 of 0

NO ITEMS AVAILABLE

Select Cisco UCS Server (Standalone), then enter the Device ID and Claim Code, then click Claim. Repeat for all the servers to be used in your new cluster.

Note: When using the Cisco Intersight Virtual Appliance, the servers’ CIMC IP addresses and their usernames and passwords are used to claim the servers instead of the Device IDs and Claim Codes.

Generate API Keys

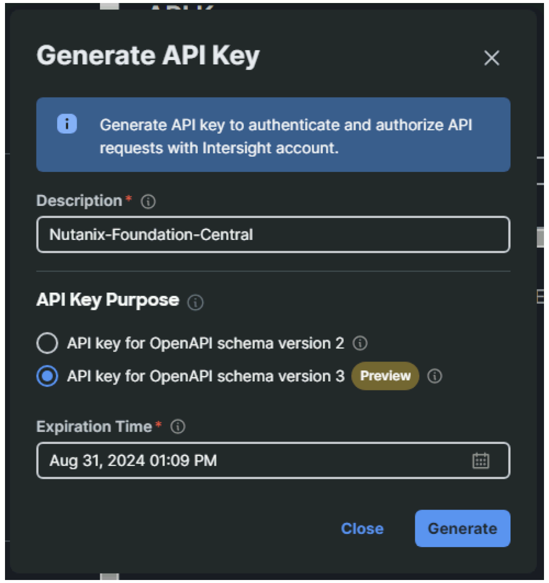


Settings

API Keys

0 items found 15 per page 0 of 0

NO ITEMS AVAILABLE



Generate API Key

Generate API key to authenticate and authorize API requests with Intersight account.

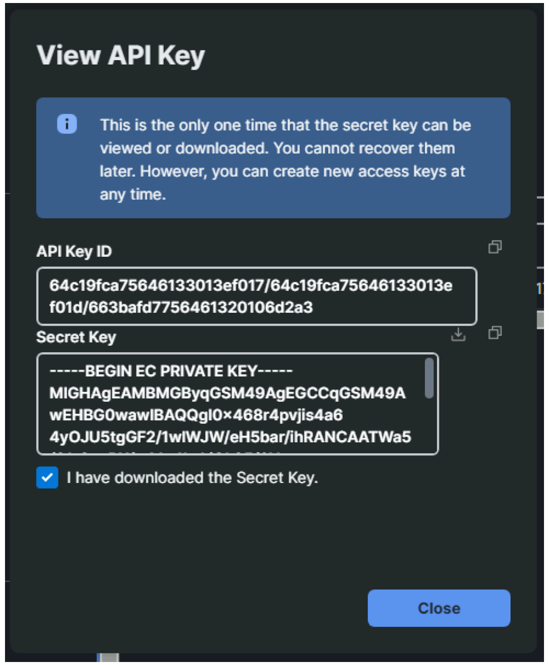
Description *
Nutanix-Foundation-Central

API Key Purpose

○ API key for OpenAPI schema version 2

● API key for OpenAPI schema version 3 Preview

Expiration Time *
Aug 31, 2024 01:09 PM



View API Key

This is the only one time that the secret key can be viewed or downloaded. You cannot recover them later. However, you can create new access keys at any time.

API Key ID

```
64c19fca75646133013ef017/64c19fca75646133013ef01d/663bafd7756461320106d2a3
```

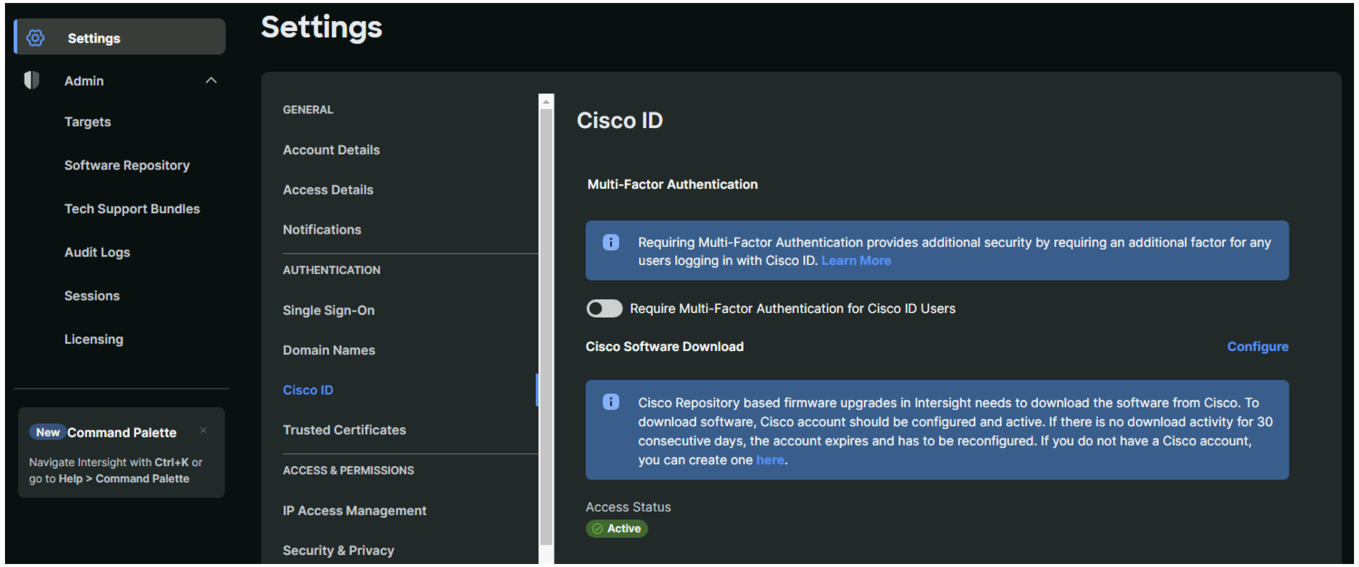
Secret Key

```
-----BEGIN EC PRIVATE KEY-----
MIGHAgEAMBMGByqGSM49AgEGCCqGSM49A
wEHBG0wawIBAQQgI0×468r4pvjis4a6
4yOJU5tgGF2/1wIWJW/eH5bar/ihRANCAATWa5
```

☑ I have downloaded the Secret Key.

Generate an API key using schema version 3 for use by Foundation Central. Be sure to copy the API Key ID and copy and save the Secret Key file. It will only be shown once.

Cisco Intersight Software Download Permissions



Cisco ID

Multi-Factor Authentication

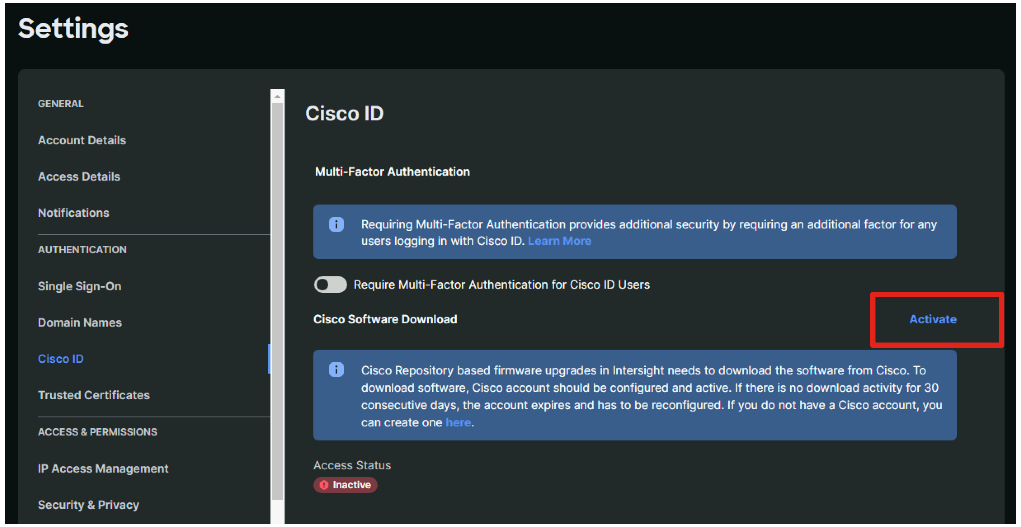
Requiring Multi-Factor Authentication provides additional security by requiring an additional factor for any users logging in with Cisco ID. Learn More

Require Multi-Factor Authentication for Cisco ID Users

Cisco Software Download

Cisco Repository based firmware upgrades in Intersight needs to download the software from Cisco. To download software, Cisco account should be configured and active. If there is no download activity for 30 consecutive days, the account expires and has to be reconfigured. If you do not have a Cisco account, you can create one here.

Access Status: Active



Cisco ID

Multi-Factor Authentication

Requiring Multi-Factor Authentication provides additional security by requiring an additional factor for any users logging in with Cisco ID. Learn More

Require Multi-Factor Authentication for Cisco ID Users

Cisco Software Download

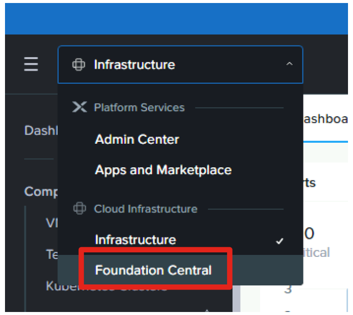
Cisco Repository based firmware upgrades in Intersight needs to download the software from Cisco. To download software, Cisco account should be configured and active. If there is no download activity for 30 consecutive days, the account expires and has to be reconfigured. If you do not have a Cisco account, you can create one here.

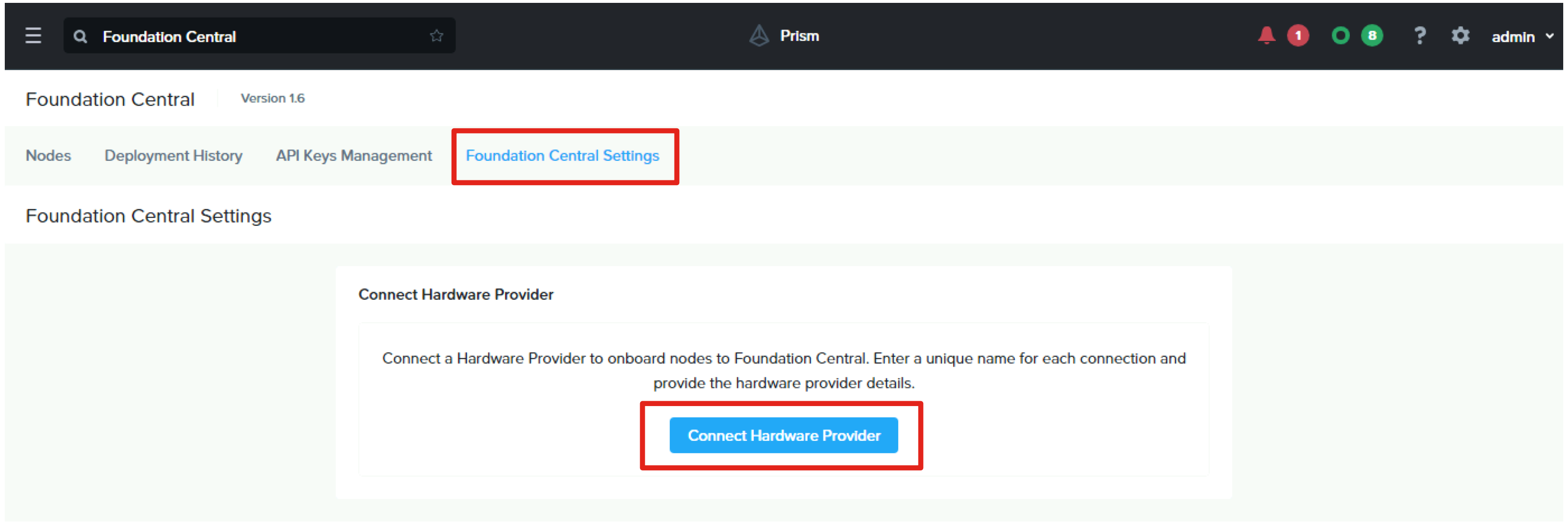
Access Status: Inactive

Ensure your Cisco ID is granted access to download software from CCO. If not, click the Activate link and enter your CCO login credentials.

Nutanix Installation

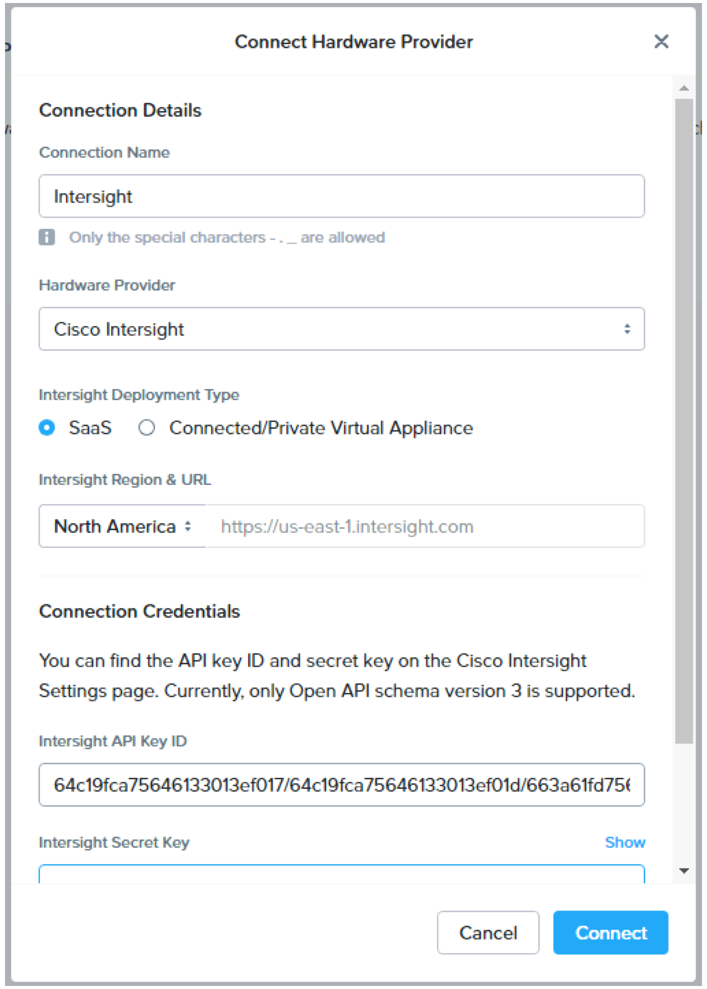
Connect Foundation Central to Cisco Intersight




Foundation Central
Prism
admin
Foundation Central
Version 1.6
Nodes
Deployment History
API Keys Management
Foundation Central Settings
Foundation Central Settings
Connect Hardware Provider

Connect a Hardware Provider to onboard nodes to Foundation Central. Enter a unique name for each connection and provide the hardware provider details.

Connect Hardware Provider



Connect Hardware Provider

Connection Details

Connection Name: Intersight

Only the special characters - . _ are allowed

Hardware Provider: Cisco Intersight

Intersight Deployment Type: ● SaaS ○ Connected/Private Virtual Appliance

Intersight Region & URL: North America https://us-east-1.intersight.com

Connection Credentials

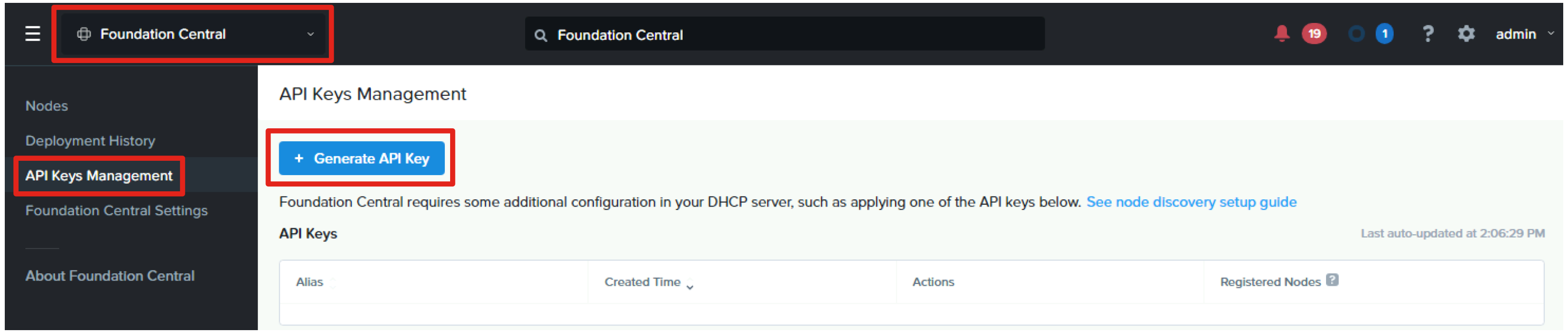
You can find the API key ID and secret key on the Cisco Intersight Settings page. Currently, only Open API schema version 3 is supported.

Intersight API Key ID: 64c19fca75646133013ef017/64c19fca75646133013ef01d/663a61fd75

Intersight Secret Key Show

Note: Only one connection to Cisco Intersight is allowed at a time.

Generate an API Key for Foundation Central



API Keys Management

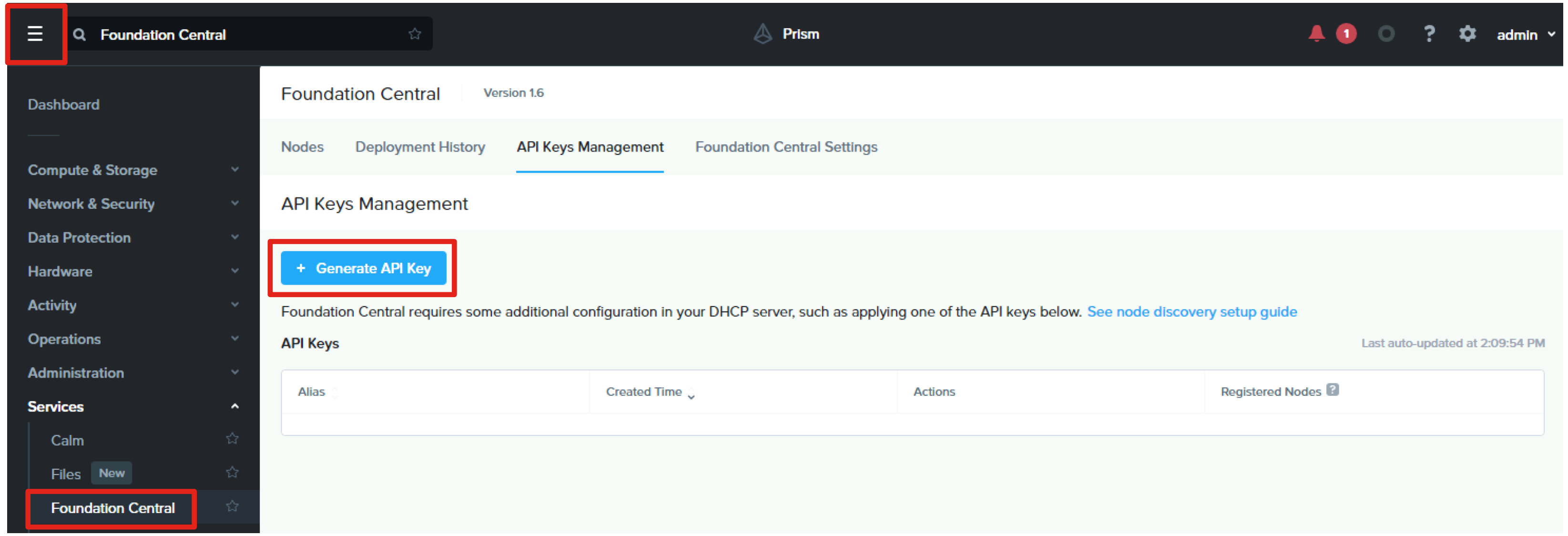
Foundation Central requires some additional configuration in your DHCP server, such as applying one of the API keys below. See node discovery setup guide

API Keys

Last auto-updated at 2:06:29 PM

Alias	Created Time	Actions	Registered Nodes

or



Foundation Central Version 1.6

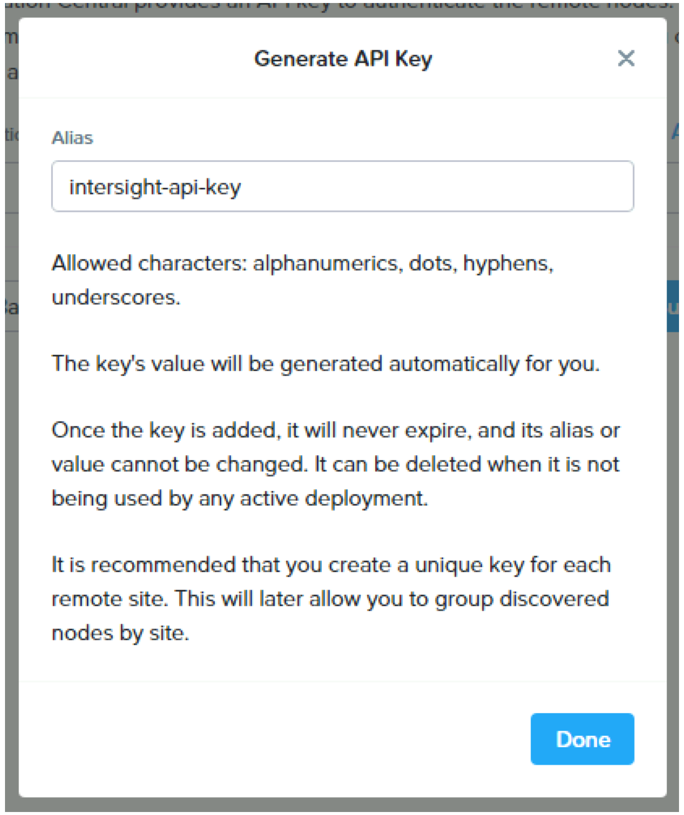
API Keys Management

Foundation Central requires some additional configuration in your DHCP server, such as applying one of the API keys below. See node discovery setup guide

API Keys

Last auto-updated at 2:09:54 PM

Alias	Created Time	Actions	Registered Nodes



Generate API Key

Alias

intersight-api-key

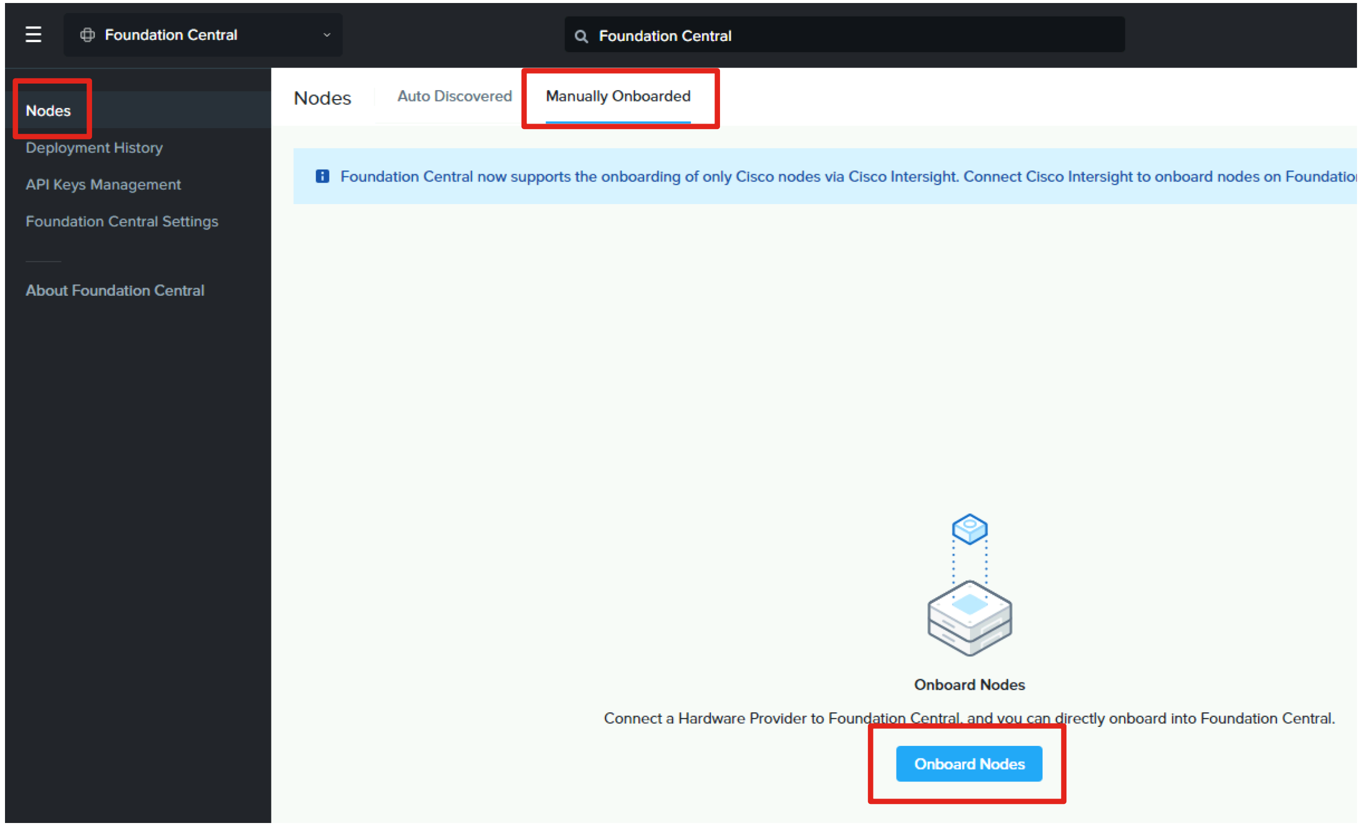
Allowed characters: alphanumerics, dots, hyphens, underscores.

The key's value will be generated automatically for you.

Once the key is added, it will never expire, and its alias or value cannot be changed. It can be deleted when it is not being used by any active deployment.

It is recommended that you create a unique key for each remote site. This will later allow you to group discovered nodes by site.

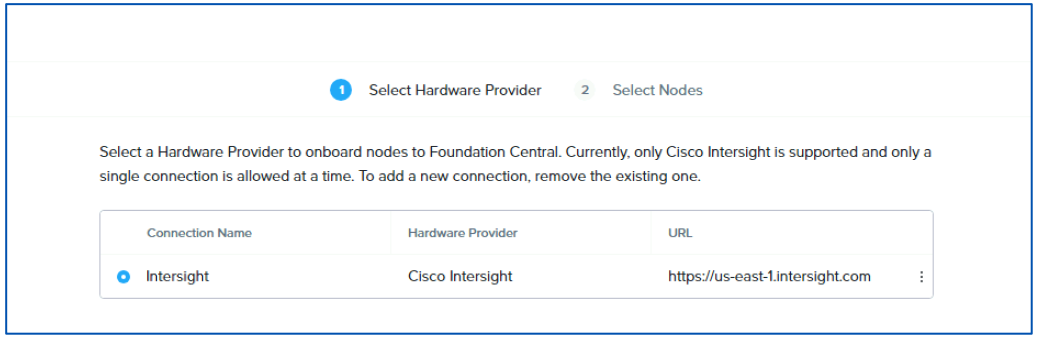
Onboard Servers in Foundation Central



Foundation Central now supports the onboarding of only Cisco nodes via Cisco Intersight. Connect Cisco Intersight to onboard nodes on Foundatio

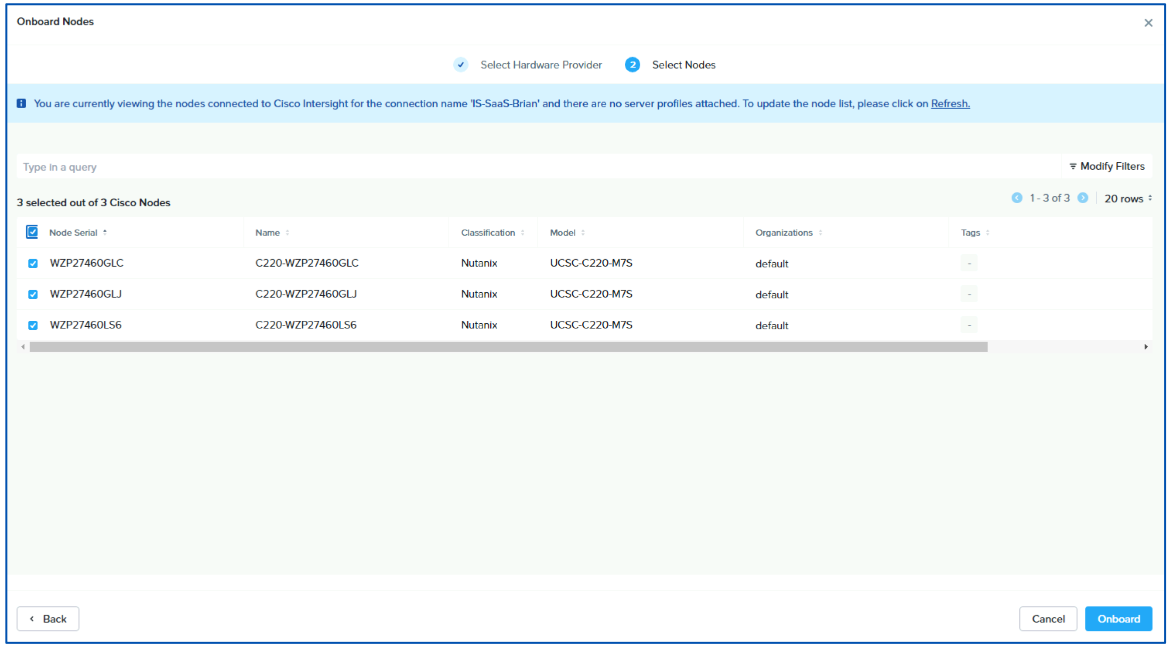
Onboard Nodes

Connect a Hardware Provider to Foundation Central, and you can directly onboard into Foundation Central.



Select a Hardware Provider to onboard nodes to Foundation Central. Currently, only Cisco Intersight is supported and only a single connection is allowed at a time. To add a new connection, remove the existing one.

	Connection Name	Hardware Provider	URL
●	Intersight	Cisco Intersight	https://us-east-1.intersight.com



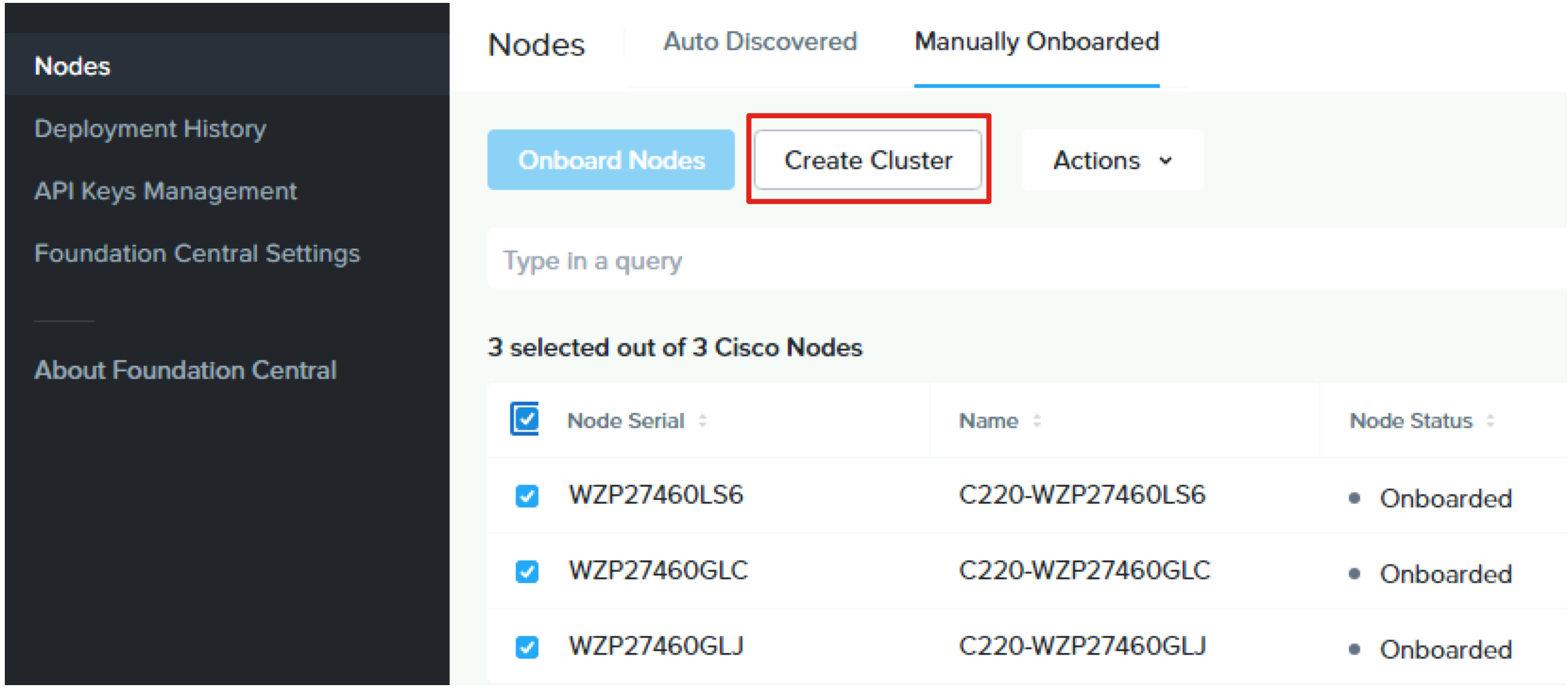
You are currently viewing the nodes connected to Cisco Intersight for the connection name 'IS-SaaS-Brian' and there are no server profiles attached. To update the node list, please click on Refresh.

3 selected out of 3 Cisco Nodes

☑	Node Serial	Name	Classification	Model	Organizations	Tags
☑	WZP27460GLC	C220-WZP27460GLC	Nutanix	UCSC-C220-M7S	default	-
☑	WZP27460GLJ	C220-WZP27460GLJ	Nutanix	UCSC-C220-M7S	default	-
☑	WZP27460LS6	C220-WZP27460LS6	Nutanix	UCSC-C220-M7S	default	-

Select only the nodes to be used to run Nutanix clusters to be installed by Foundation Central.

Begin Cluster Creation Wizard

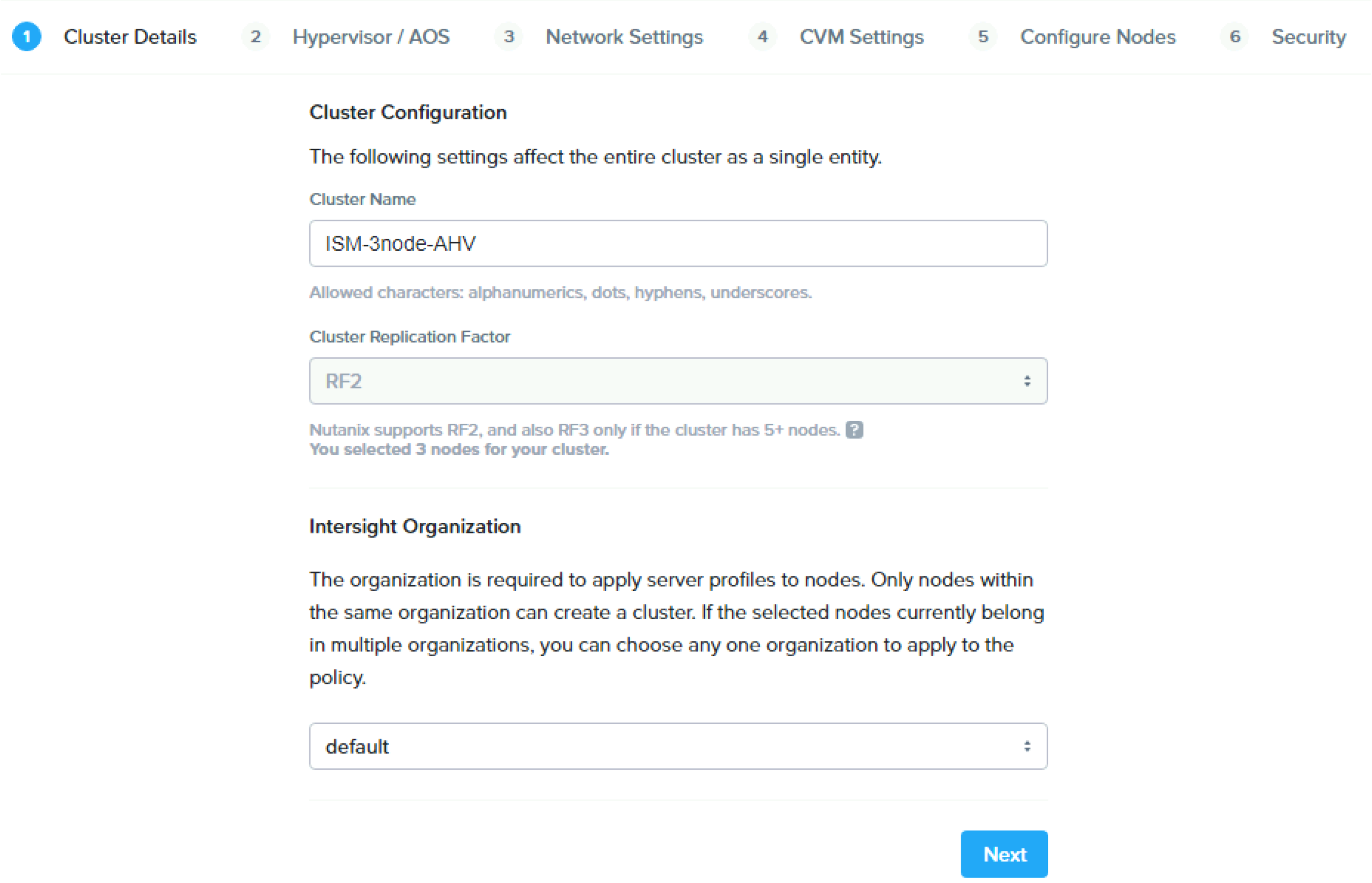


3 selected out of 3 Cisco Nodes

☑	Node Serial	Name	Node Status
☑	WZP27460LS6	C220-WZP27460LS6	● Onboarded
☑	WZP27460GLC	C220-WZP27460GLC	● Onboarded
☑	WZP27460GLJ	C220-WZP27460GLJ	● Onboarded

Select the onboarded nodes to be used in the new cluster, then click Create Cluster.

Cluster Creation Continued



Cluster Configuration

The following settings affect the entire cluster as a single entity.

Cluster Name

ISM-3node-AHV

Allowed characters: alphanumerics, dots, hyphens, underscores.

Cluster Replication Factor

RF2

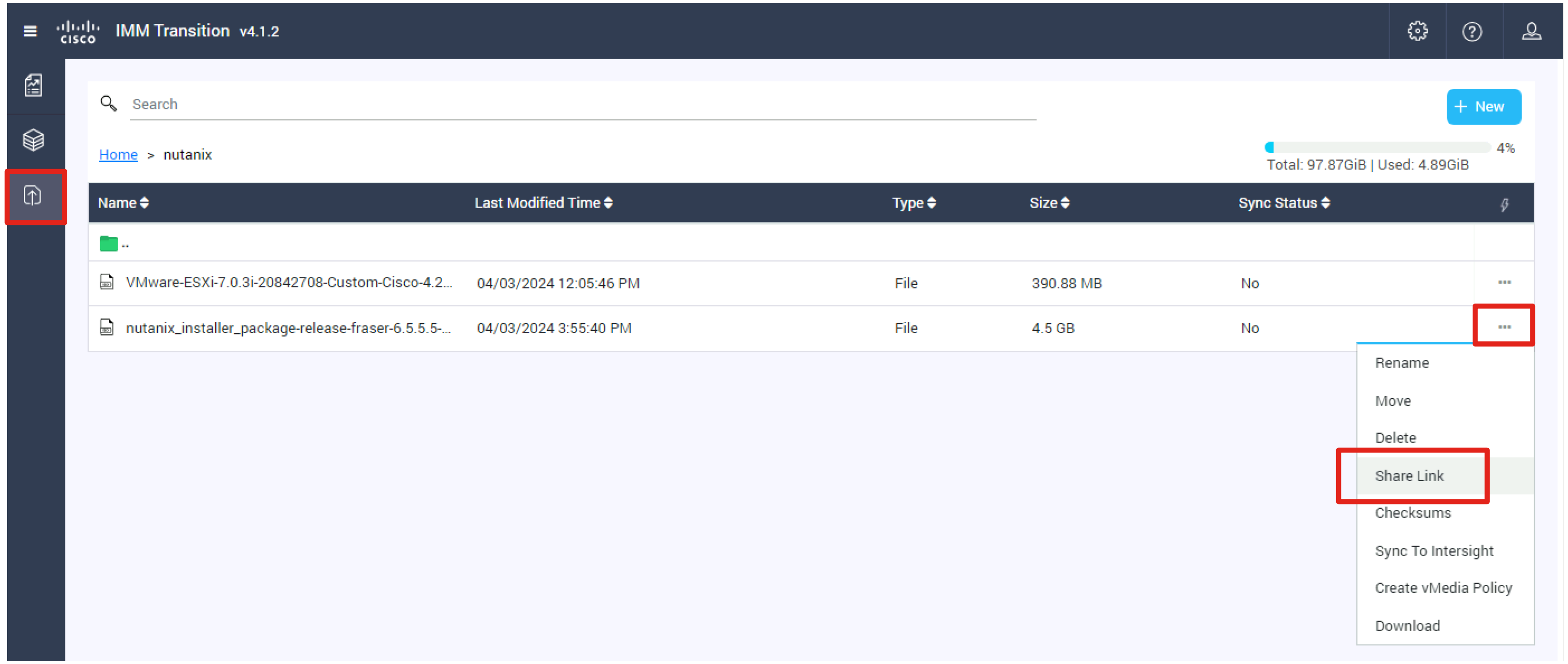
Nutanix supports RF2, and also RF3 only if the cluster has 5+ nodes. ?
You selected 3 nodes for your cluster.

Intersight Organization

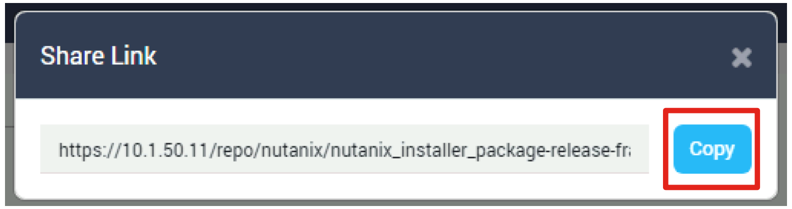
The organization is required to apply server profiles to nodes. Only nodes within the same organization can create a cluster. If the selected nodes currently belong in multiple organizations, you can choose any one organization to apply to the policy.

default

Retrieve AOS and Hypervisor file URLs (optional)

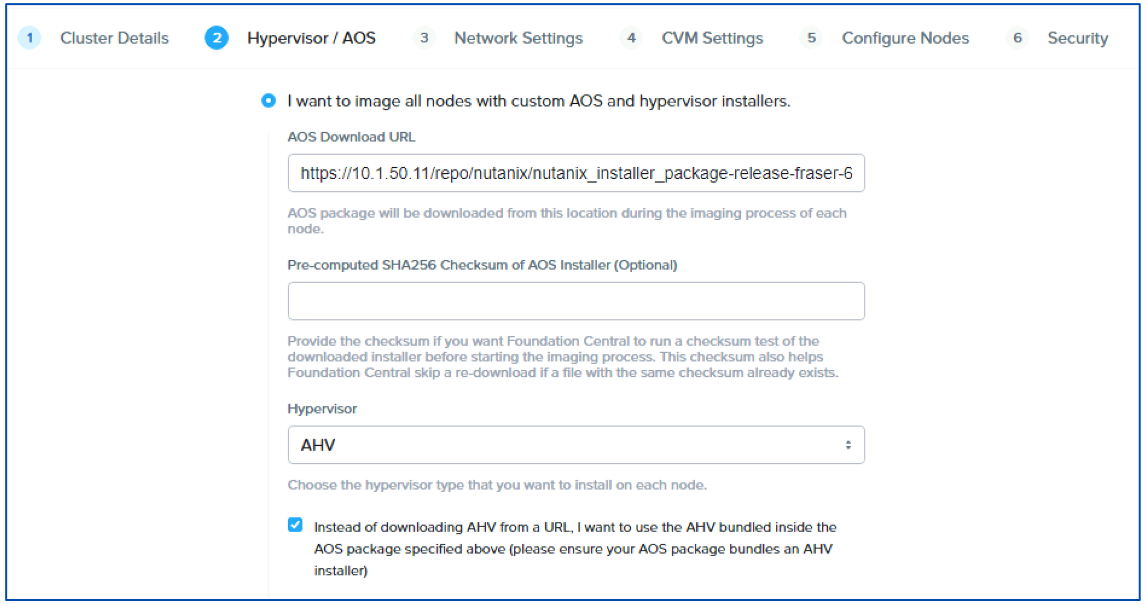


Name	Last Modified Time	Type	Size	Sync Status
..				
VMware-ESXi-7.0.3i-20842708-Custom-Cisco-4.2...	04/03/2024 12:05:46 PM	File	390.88 MB	No
nutanix_installer_package-release-fraser-6.5.5.5-...	04/03/2024 3:55:40 PM	File	4.5 GB	No



https://10.1.50.11/repo/nutanix/nutanix_installer_package-release-fr

Cluster Creation Continued



● I want to image all nodes with custom AOS and hypervisor installers.

AOS Download URL

https://10.1.50.11/repo/nutanix/nutanix_installer_package-release-fraser-6

AOS package will be downloaded from this location during the imaging process of each node.

Pre-computed SHA256 Checksum of AOS Installer (Optional)

Provide the checksum if you want Foundation Central to run a checksum test of the downloaded installer before starting the imaging process. This checksum also helps Foundation Central skip a re-download if a file with the same checksum already exists.

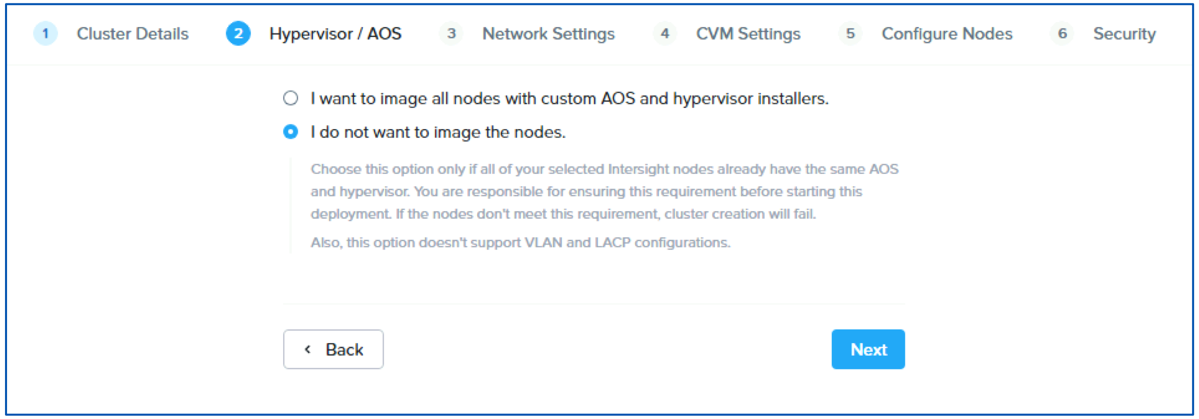
Hypervisor

AHV

Choose the hypervisor type that you want to install on each node.

☑ Instead of downloading AHV from a URL, I want to use the AHV bundled inside the AOS package specified above (please ensure your AOS package bundles an AHV installer)

or



○ I want to image all nodes with custom AOS and hypervisor installers.

● I do not want to image the nodes.

Choose this option only if all of your selected Intersight nodes already have the same AOS and hypervisor. You are responsible for ensuring this requirement before starting this deployment. If the nodes don't meet this requirement, cluster creation will fail.

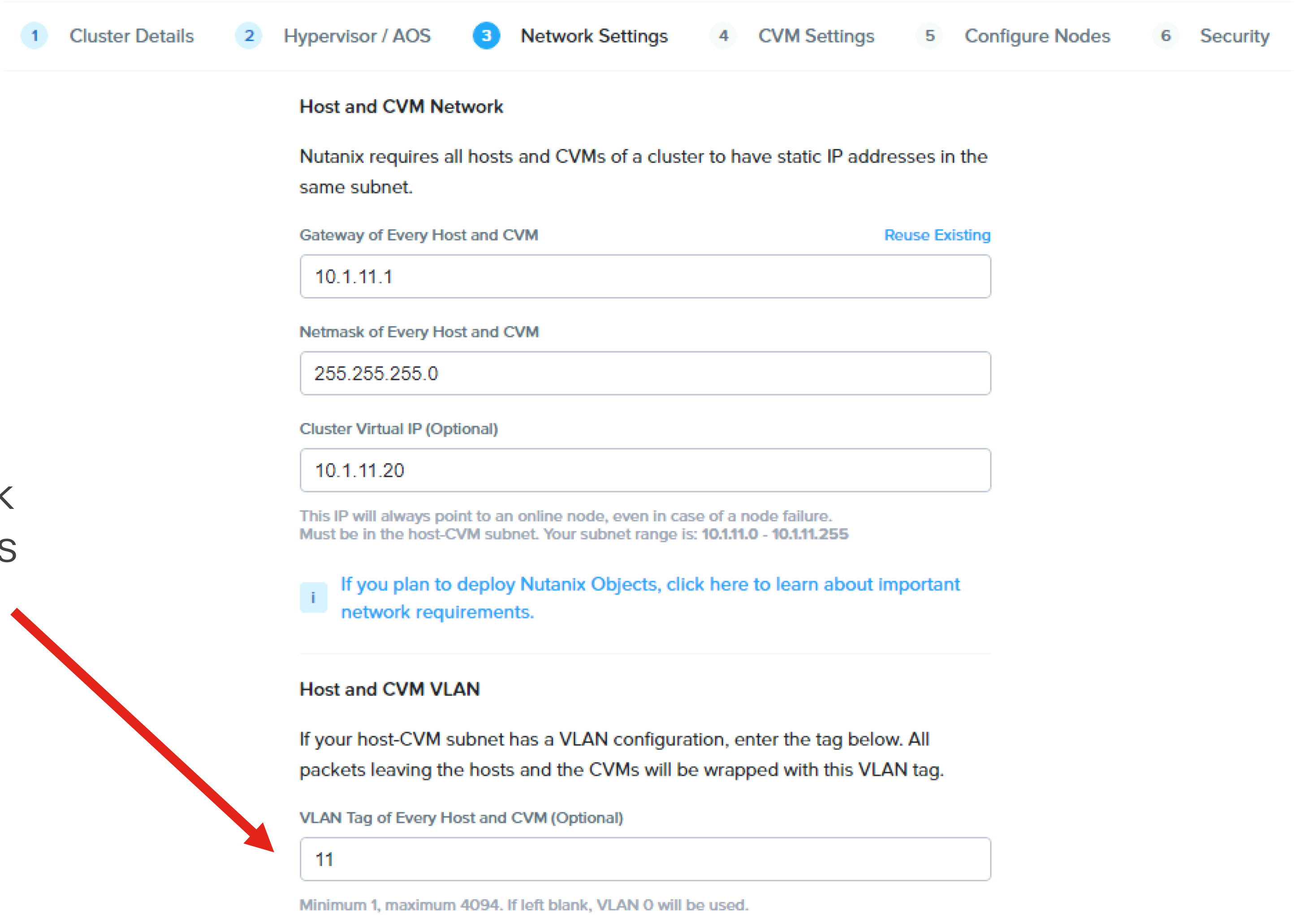
Also, this option doesn't support VLAN and LACP configurations.

Choose whether to use the factory installed AHV hypervisor and AOS software, or to re-image the servers. If deploying with ESXi as the hypervisor, provide the AOS Download URL, select ESX and provide the Download URL for the Cisco custom ESXi installation ISO. You can also provide a Download URL for AHV when the bundled version in AOS is not going to be used.

Note: AOS version 6.8 and later no longer include the AHV installation files in the AOS image, therefore you must download the AHV installation ISO file and supply its location when imaging the servers.

Cluster Creation Continued

Entering a VLAN ID tag will configure the servers’ vNICs as trunk ports, while leaving the field blank will configure them as access ports.



Host and CVM Network

Nutanix requires all hosts and CVMs of a cluster to have static IP addresses in the same subnet.

Gateway of Every Host and CVM — Reuse Existing

10.1.11.1

Netmask of Every Host and CVM

255.255.255.0

Cluster Virtual IP (Optional)

10.1.11.20

This IP will always point to an online node, even in case of a node failure.
Must be in the host-CVM subnet. Your subnet range is: **10.1.11.0 - 10.1.11.255**

i If you plan to deploy Nutanix Objects, click here to learn about important network requirements.

Host and CVM VLAN

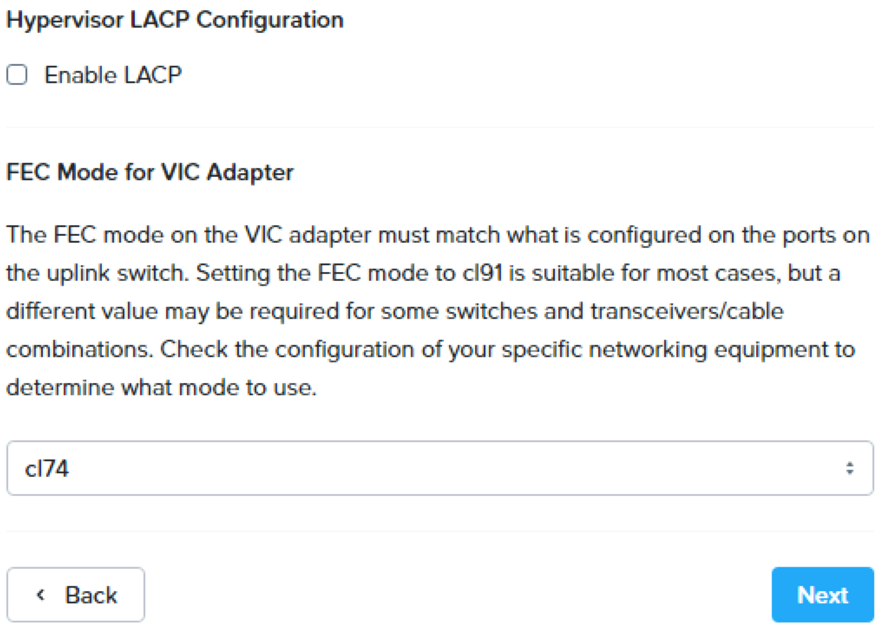
If your host-CVM subnet has a VLAN configuration, enter the tag below. All packets leaving the hosts and the CVMs will be wrapped with this VLAN tag.

VLAN Tag of Every Host and CVM (Optional)

11

Minimum 1, maximum 4094. If left blank, VLAN 0 will be used.

Cluster Creation Continued



Hypervisor LACP Configuration

☐ Enable LACP

FEC Mode for VIC Adapter

The FEC mode on the VIC adapter must match what is configured on the ports on the uplink switch. Setting the FEC mode to cl91 is suitable for most cases, but a different value may be required for some switches and transceivers/cable combinations. Check the configuration of your specific networking equipment to determine what mode to use.

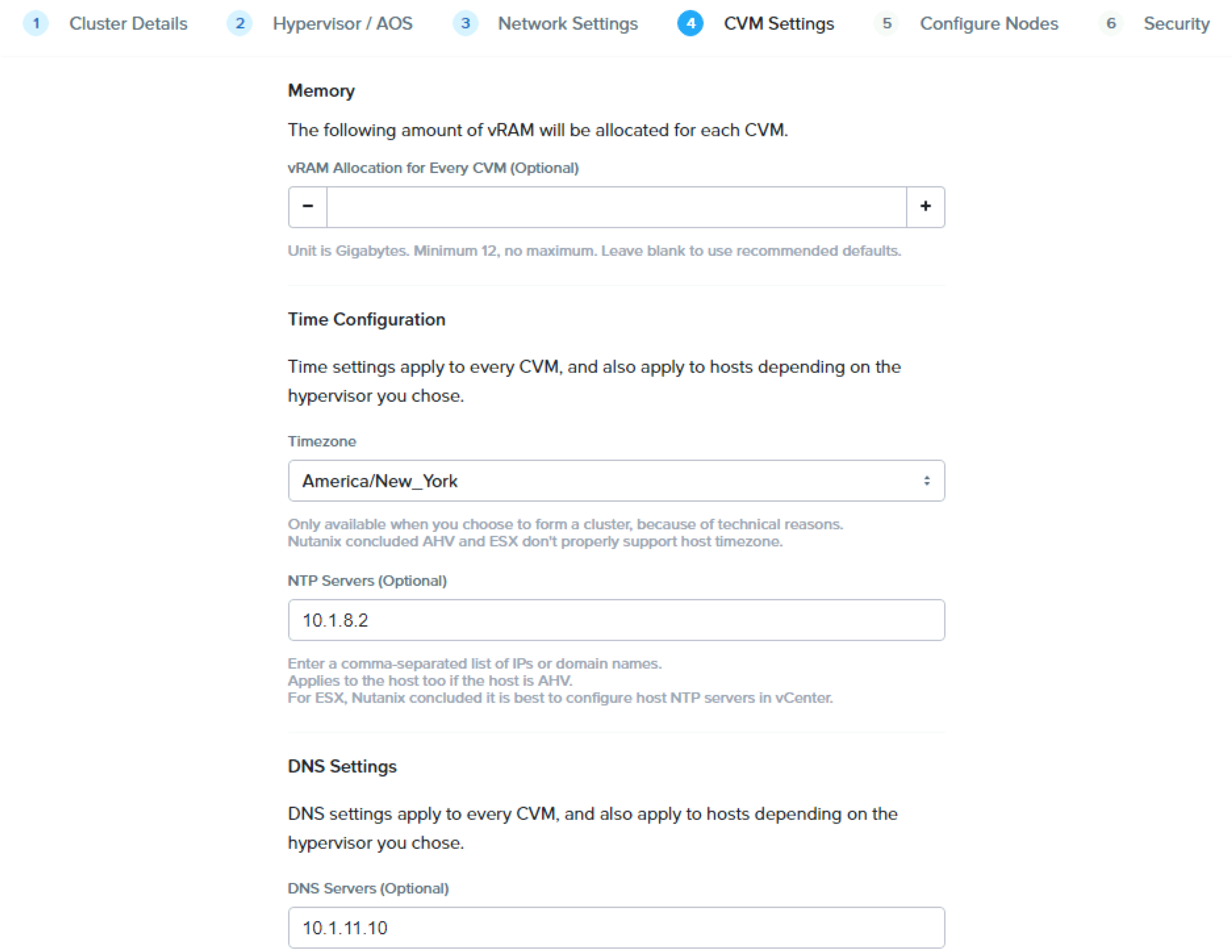
cl74

LACP is only supported when using AHV and the nodes are being re-imaged. The upstream switch ports should not be configured with LACP until after the install is completed. Please see Nutanix KB 16742 for more details.

Set the appropriate FEC mode for the cables, optics and switches in your environment. The default FEC setting is CL91 (RS-FEC), which is equivalent to auto, and is appropriate for all 10 GbE, 40 GbE, 50 GbE and 100 GbE cables and optics. Some models of 25 GbE cables and optics require CL74 (FC-FEC) in order for the links to be active.

Refer to the following documents to determine which FEC setting is appropriate for your hardware:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_Cisco_ACI_and_Forward_Error_Correction.html
and
https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736950.html

Cluster Creation Continued



Memory

The following amount of vRAM will be allocated for each CVM.

vRAM Allocation for Every CVM (Optional)

Unit is Gigabytes. Minimum 12, no maximum. Leave blank to use recommended defaults.

Time Configuration

Time settings apply to every CVM, and also apply to hosts depending on the hypervisor you chose.

Timezone: America/New_York

Only available when you choose to form a cluster, because of technical reasons.
Nutanix concluded AHV and ESX don't properly support host timezone.

NTP Servers (Optional): 10.1.8.2

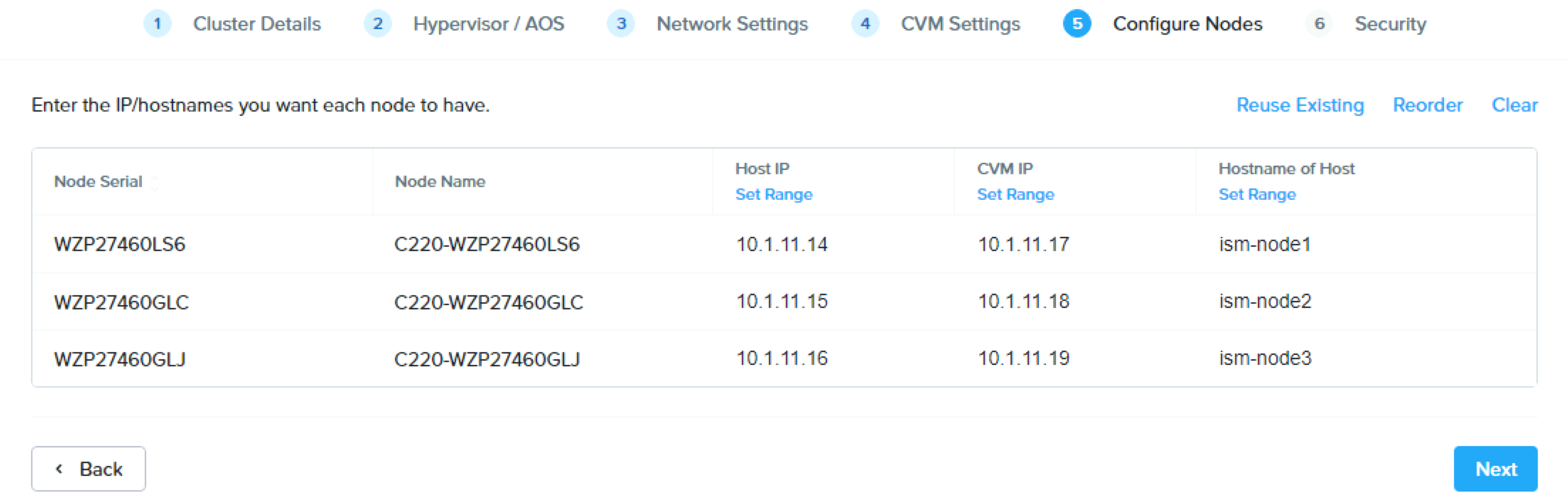
Enter a comma-separated list of IPs or domain names.
Applies to the host too if the host is AHV.
For ESX, Nutanix concluded it is best to configure host NTP servers in vCenter.

DNS Settings

DNS settings apply to every CVM, and also apply to hosts depending on the hypervisor you chose.

DNS Servers (Optional): 10.1.11.10

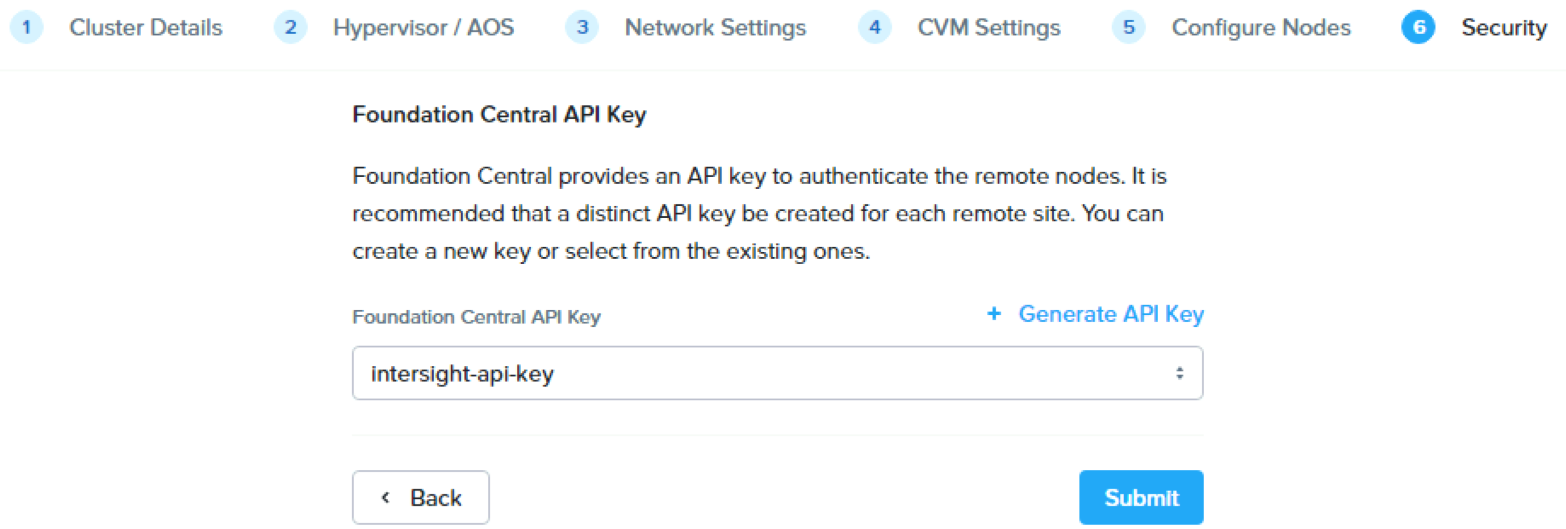
Cluster Creation Continued



Enter the IP/hostnames you want each node to have.

Node Serial	Node Name	Host IP Set Range	CVM IP Set Range	Hostname of Host Set Range
WZP27460LS6	C220-WZP27460LS6	10.1.11.14	10.1.11.17	ism-node1
WZP27460GLC	C220-WZP27460GLC	10.1.11.15	10.1.11.18	ism-node2
WZP27460GLJ	C220-WZP27460GLJ	10.1.11.16	10.1.11.19	ism-node3

Cluster Creation Continued

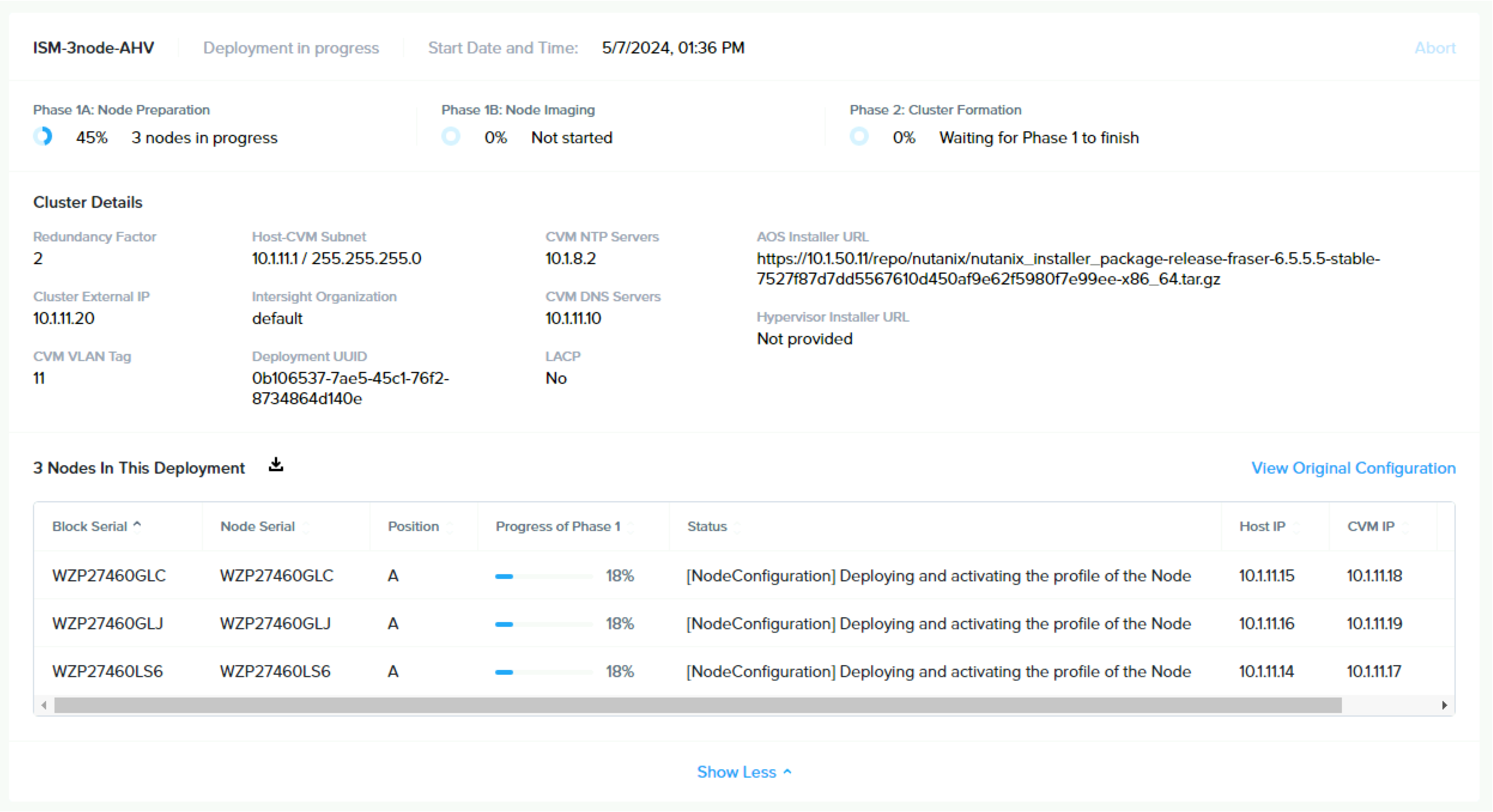


Foundation Central API Key

Foundation Central provides an API key to authenticate the remote nodes. It is recommended that a distinct API key be created for each remote site. You can create a new key or select from the existing ones.

Foundation Central API Key: intersight-api-key

Install Progress



ISM-3node-AHV | Deployment in progress | Start Date and Time: 5/7/2024, 01:36 PM

Phase 1A: Node Preparation
45% 3 nodes in progress

Phase 1B: Node Imaging
0% Not started

Phase 2: Cluster Formation
0% Waiting for Phase 1 to finish

Cluster Details

Redundancy Factor
2

Cluster External IP
10.1.11.20

CVM VLAN Tag
11

Host-CVM Subnet
10.1.11.1 / 255.255.255.0

Intersight Organization
default

Deployment UUID
0b106537-7ae5-45c1-76f2-8734864d140e

CVM NTP Servers
10.1.8.2

CVM DNS Servers
10.1.11.10

LACP
No

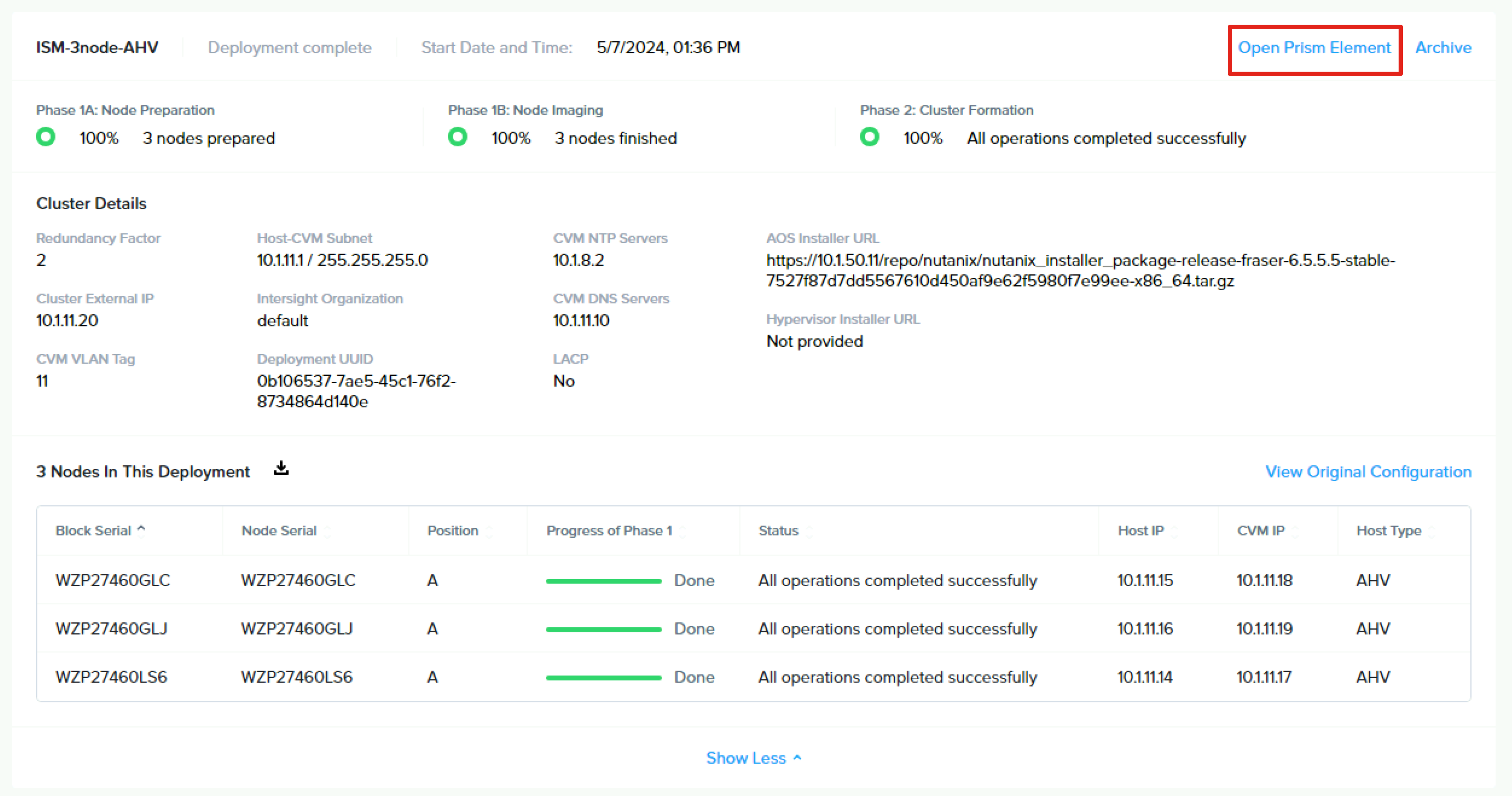
AOS Installer URL
https://10.1.50.11/repo/nutanix/nutanix_installer_package-release-fraser-6.5.5.5-stable-7527f87d7dd5567610d450af9e62f5980f7e99ee-x86_64.tar.gz

Hypervisor Installer URL
Not provided

3 Nodes In This Deployment

Block Serial	Node Serial	Position	Progress of Phase 1	Status	Host IP	CVM IP
WZP27460GLC	WZP27460GLC	A	18%	[NodeConfiguration] Deploying and activating the profile of the Node	10.1.11.15	10.1.11.18
WZP27460GLJ	WZP27460GLJ	A	18%	[NodeConfiguration] Deploying and activating the profile of the Node	10.1.11.16	10.1.11.19
WZP27460LS6	WZP27460LS6	A	18%	[NodeConfiguration] Deploying and activating the profile of the Node	10.1.11.14	10.1.11.17

Install Complete



ISM-3node-AHV | Deployment complete | Start Date and Time: 5/7/2024, 01:36 PM

Phase 1A: Node Preparation
100% 3 nodes prepared

Phase 1B: Node Imaging
100% 3 nodes finished

Phase 2: Cluster Formation
100% All operations completed successfully

Cluster Details

Redundancy Factor
2

Cluster External IP
10.1.11.20

CVM VLAN Tag
11

Host-CVM Subnet
10.1.11.1 / 255.255.255.0

Intersight Organization
default

Deployment UUID
0b106537-7ae5-45c1-76f2-8734864d140e

CVM NTP Servers
10.1.8.2

CVM DNS Servers
10.1.11.10

LACP
No

AOS Installer URL
https://10.1.50.11/repo/nutanix/nutanix_installer_package-release-fraser-6.5.5.5-stable-7527f87d7dd5567610d450af9e62f5980f7e99ee-x86_64.tar.gz

Hypervisor Installer URL
Not provided

3 Nodes In This Deployment

Block Serial	Node Serial	Position	Progress of Phase 1	Status	Host IP	CVM IP	Host Type
WZP27460GLC	WZP27460GLC	A	Done	All operations completed successfully	10.1.11.15	10.1.11.18	AHV
WZP27460GLJ	WZP27460GLJ	A	Done	All operations completed successfully	10.1.11.16	10.1.11.19	AHV
WZP27460LS6	WZP27460LS6	A	Done	All operations completed successfully	10.1.11.14	10.1.11.17	AHV

Click the link to open Prism Element when the installation is complete.

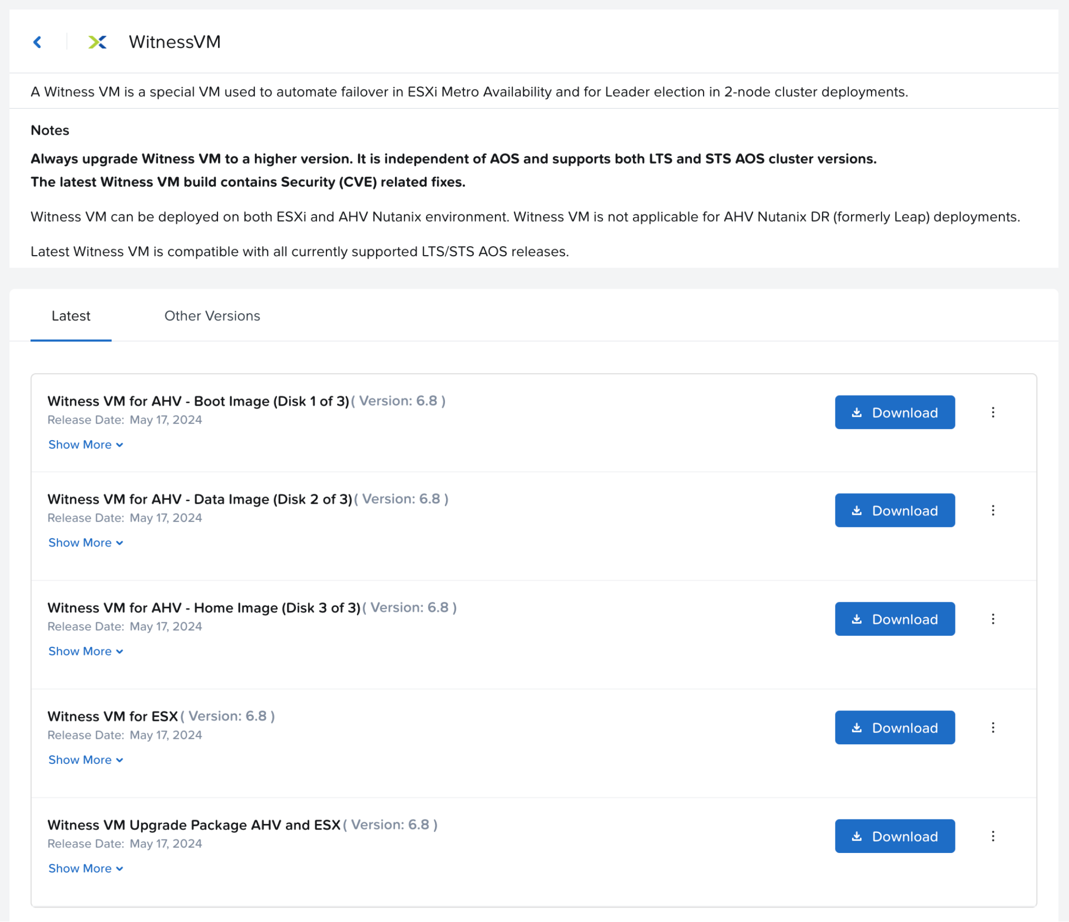
Witness VM Installation and Configuration

Witness VM Use Cases and Requirements

- A Witness VM is highly recommended for 2-node clusters or clusters configured for Metro Availability.
- The witness VM makes failover decisions during network outages or site availability interruptions to avoid split-brain scenarios.
- The witness VM must reside in a different failure domain from the clusters it is monitoring, meaning it has its own separate power and independent network communication to both monitored sites.
- The configuration of a witness VM is the same for 2-node clusters or metro availability clusters and can act as witness for up to 50 clusters.
- The witness VM only runs on AHV or ESXi clusters, it cannot be backed up or restored via snapshots, and cannot be migrated between vCenter servers.
- Network latency between the two sites and the witness VM must be less than 200ms.
- TCP port 9440 is used and must bypass any proxy servers in the network.
- For detailed information refer to the following Nutanix document: https://portal.nutanix.com/page/documents/details?targetId=Prism-Element-Data-Protection-Guide-v6_8:sto-cluster-witness-option-wc-c.html

Download Witness VM disk images

Download the witness VM disk images here:
https://portal.nutanix.com/page/downloads?product=witnessvm



WitnessVM

A Witness VM is a special VM used to automate failover in ESXi Metro Availability and for Leader election in 2-node cluster deployments.

Notes

Always upgrade Witness VM to a higher version. It is independent of AOS and supports both LTS and STS AOS cluster versions.
The latest Witness VM build contains Security (CVE) related fixes.

Witness VM can be deployed on both ESXi and AHV Nutanix environment. Witness VM is not applicable for AHV Nutanix DR (formerly Leap) deployments.

Latest Witness VM is compatible with all currently supported LTS/STS AOS releases.

Witness VM for AHV - Boot Image (Disk 1 of 3) (Version: 6.8)
Release Date: May 17, 2024
Show More

Witness VM for AHV - Data Image (Disk 2 of 3) (Version: 6.8)
Release Date: May 17, 2024
Show More

Witness VM for AHV - Home Image (Disk 3 of 3) (Version: 6.8)
Release Date: May 17, 2024
Show More

Witness VM for ESX (Version: 6.8)
Release Date: May 17, 2024
Show More

Witness VM Upgrade Package AHV and ESX (Version: 6.8)
Release Date: May 17, 2024
Show More

Download the 3 disk images for deployment on AHV, or the single OVA for deployment on ESXi

Upload Witness VM images to Prism

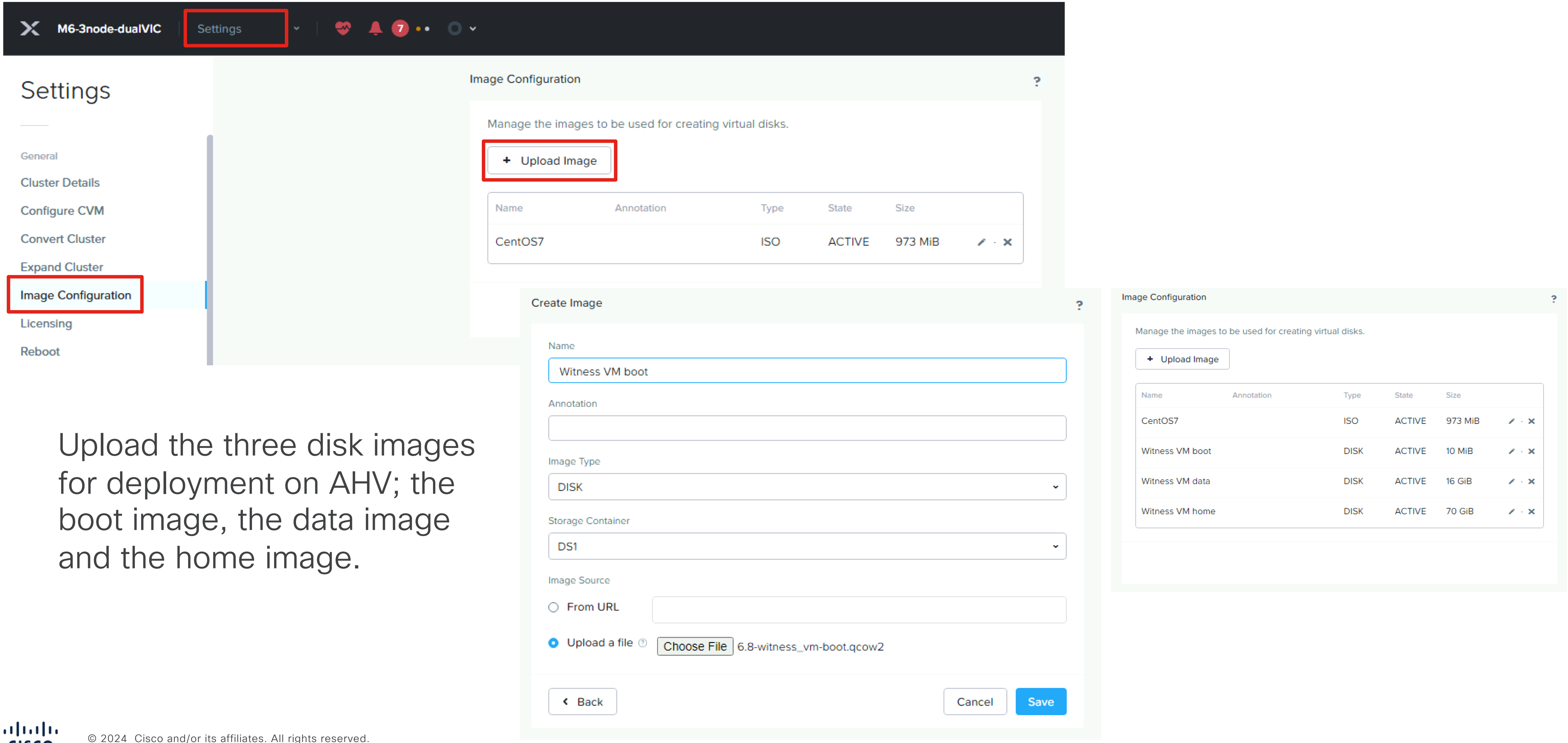


Image Configuration

Manage the images to be used for creating virtual disks.

+ Upload Image

Name	Annotation	Type	State	Size
CentOS7		ISO	ACTIVE	973 MiB

Create Image

Name: Witness VM boot

Annotation:

Image Type: DISK

Storage Container: DS1

Image Source

○ From URL

● Upload a file — Choose File 6.8-witness_vm-boot.qcow2

Image Configuration

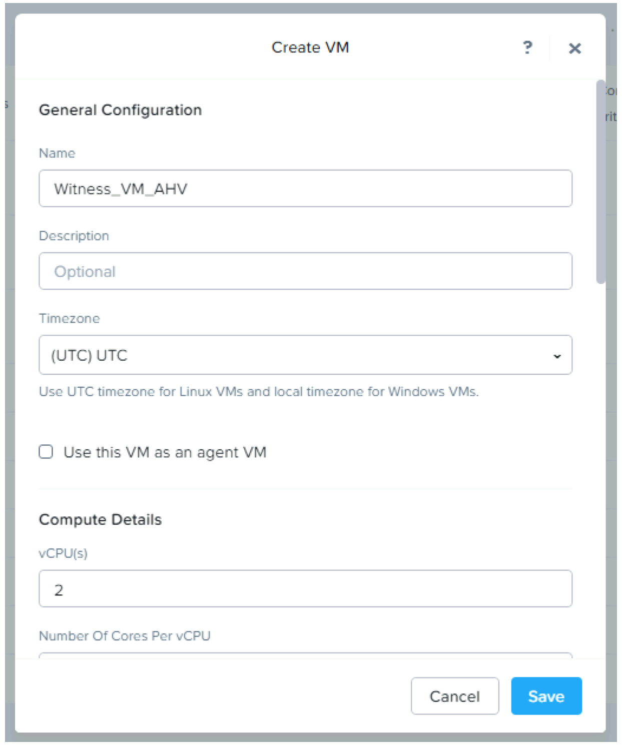
Manage the images to be used for creating virtual disks.

+ Upload Image

Name	Annotation	Type	State	Size
CentOS7		ISO	ACTIVE	973 MiB
Witness VM boot		DISK	ACTIVE	10 MiB
Witness VM data		DISK	ACTIVE	16 GiB
Witness VM home		DISK	ACTIVE	70 GiB

Upload the three disk images for deployment on AHV; the boot image, the data image and the home image.

Deploy Witness VM on Nutanix



Create VM

General Configuration

Name: Witness_VM_AHV

Description: Optional

Timezone: (UTC) UTC

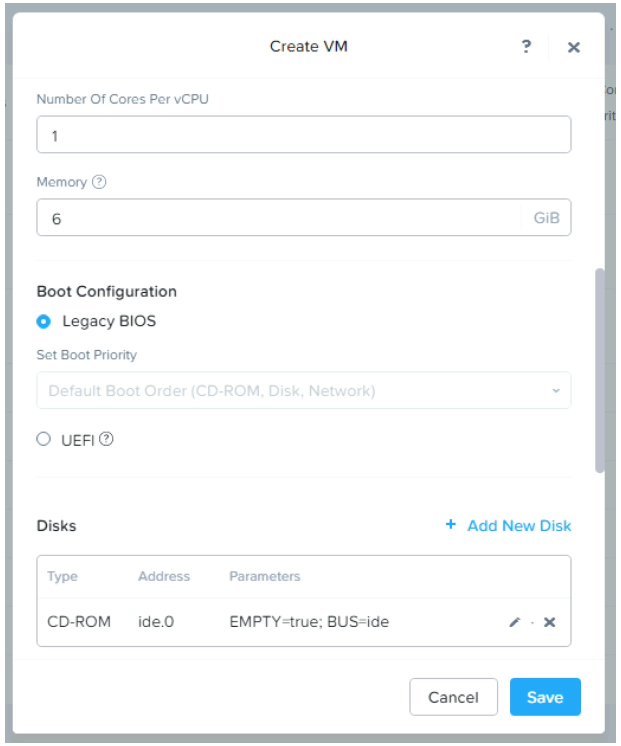
Use UTC timezone for Linux VMs and local timezone for Windows VMs.

□ Use this VM as an agent VM

Compute Details

vCPU(s): 2

Number Of Cores Per vCPU



Create VM

Number Of Cores Per vCPU: 1

Memory: 6 GiB

Boot Configuration

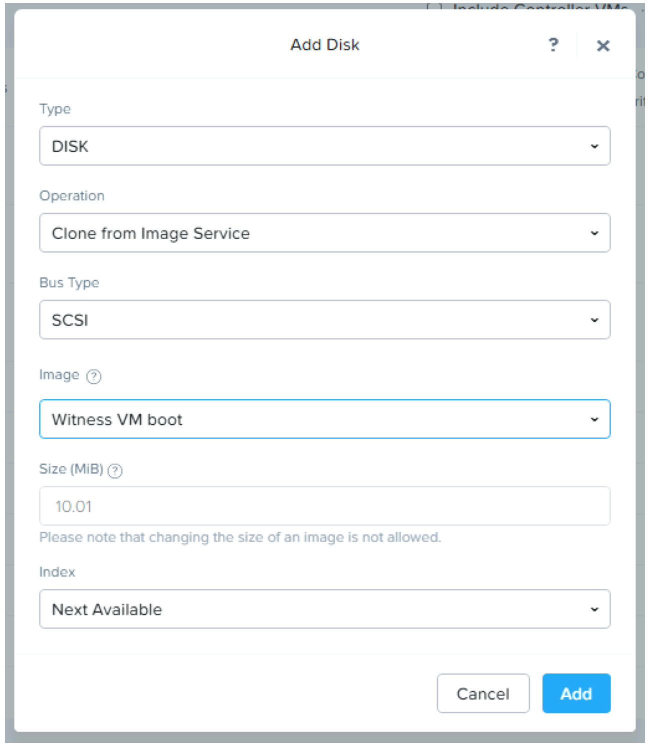
● Legacy BIOS

Set Boot Priority: Default Boot Order (CD-ROM, Disk, Network)

○ UEFI

Disks

Type	Address	Parameters
CD-ROM	ide.0	EMPTY=true; BUS=ide



Add Disk

Type: DISK

Operation: Clone from Image Service

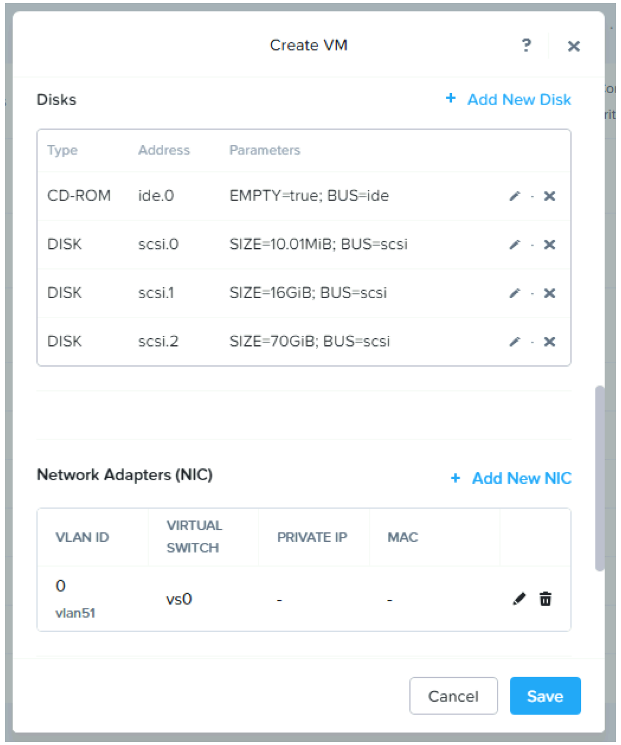
Bus Type: SCSI

Image: Witness VM boot

Size (MiB): 10.01

Please note that changing the size of an image is not allowed.

Index: Next Available



Create VM

Disks

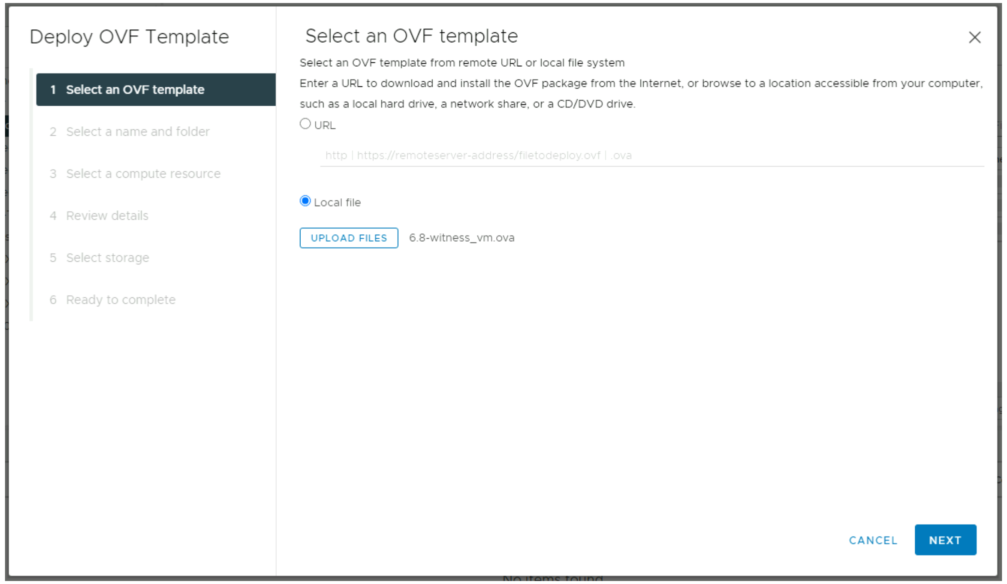
Type	Address	Parameters
CD-ROM	ide.0	EMPTY=true; BUS=ide
DISK	scsi.0	SIZE=10.01MiB; BUS=scsi
DISK	scsi.1	SIZE=16GiB; BUS=scsi
DISK	scsi.2	SIZE=70GiB; BUS=scsi

Network Adapters (NIC)

VLAN ID	VIRTUAL SWITCH	PRIVATE IP	MAC
0 vlan51	vs0	-	-

Create a new VM with minimum 2 vCPU and 6GB vRAM, add the three disk images as SCSI disks cloned from the image service, and add a NIC in the appropriate VLAN, then click Save and boot the VM.

Deploy Witness VM on ESXi



Select an OVF template

Select an OVF template from remote URL or local file system

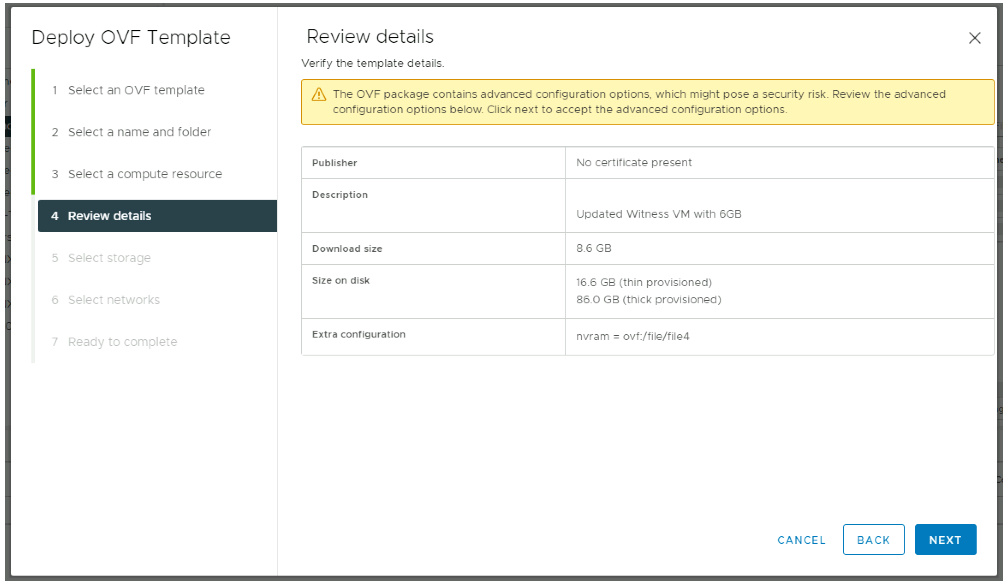
Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

UPLOAD FILES 6.8-witness_vm.ova

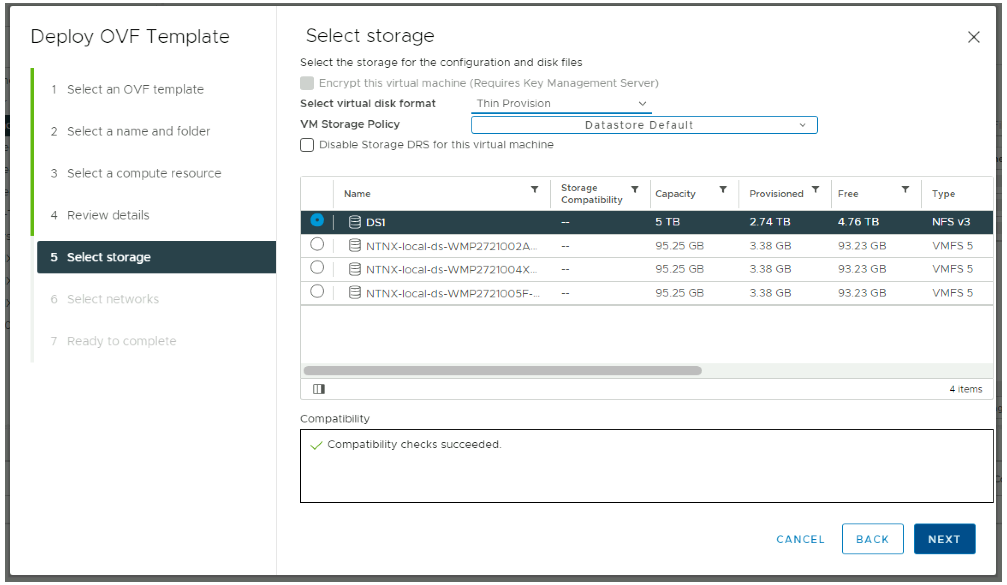


Review details

Verify the template details.

⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Publisher	No certificate present
Description	Updated Witness VM with 6GB
Download size	8.6 GB
Size on disk	16.6 GB (thin provisioned) 86.0 GB (thick provisioned)
Extra configuration	nvram = ovf:/file/file4



Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thin Provision

VM Storage Policy: Datastore Default

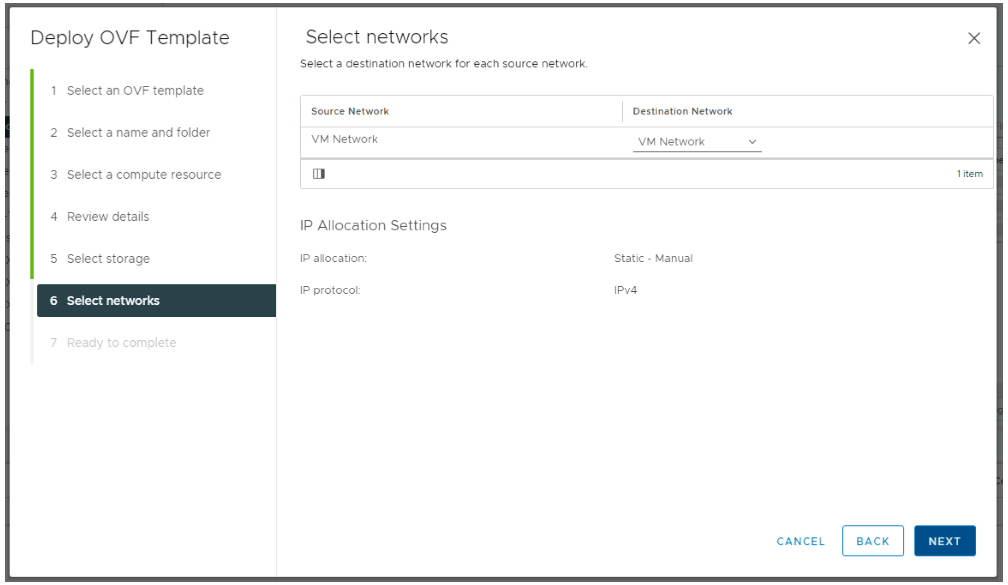
□ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	Type
●	DS1	--	5 TB	2.74 TB	4.76 TB	NFS v3
○	NTNX-local-ds-WMP2721002A...	--	95.25 GB	3.38 GB	93.23 GB	VMFS 5
○	NTNX-local-ds-WMP2721004X...	--	95.25 GB	3.38 GB	93.23 GB	VMFS 5
○	NTNX-local-ds-WMP2721005F-...	--	95.25 GB	3.38 GB	93.23 GB	VMFS 5

4 items

Compatibility

✓ Compatibility checks succeeded.



Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network

1 item

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

Configure Witness VM on Nutanix or ESXi

Open the console of the VM and log in as user admin, password Nutanix/4u, you will be prompted to change the password. Edit the network interface with a static IP address:

```
$ sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Add the NETMASK, IPADDR and GATEWAY lines, change BOOTPROTO to none, then save the changes and reboot:

```
NETMASK="xxx.xxx.xxx.xxx"
IPADDR="xxx.xxx.xxx.xxx"
BOOTPROTO="none"
GATEWAY="xxx.xxx.xxx.xxx”

$ sudo reboot
```

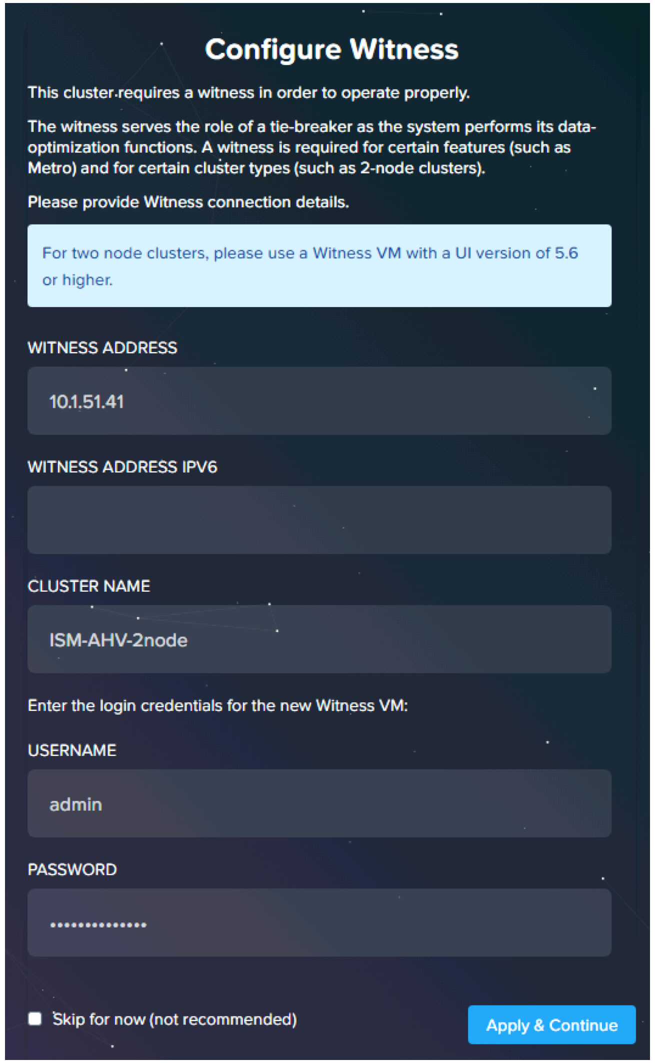
Create the witness VM cluster:

```
$ cluster -s vm_ip_address --cluster_function_list=witness_vm create
```

Note: the witness VM command prompt will say “-cvm” in the hostname, make sure you are in fact on the witness VM console and not an actual cluster controller VM

Configure Witness VM on 2-node cluster

Configure the witness during the first login to Prism Element



Configure Witness

This cluster requires a witness in order to operate properly.

The witness serves the role of a tie-breaker as the system performs its data-optimization functions. A witness is required for certain features (such as Metro) and for certain cluster types (such as 2-node clusters).

Please provide Witness connection details.

For two node clusters, please use a Witness VM with a UI version of 5.6 or higher.

WITNESS ADDRESS: 10.1.51.41

WITNESS ADDRESS IPV6:

CLUSTER NAME: ISM-AHV-2node

Enter the login credentials for the new Witness VM:

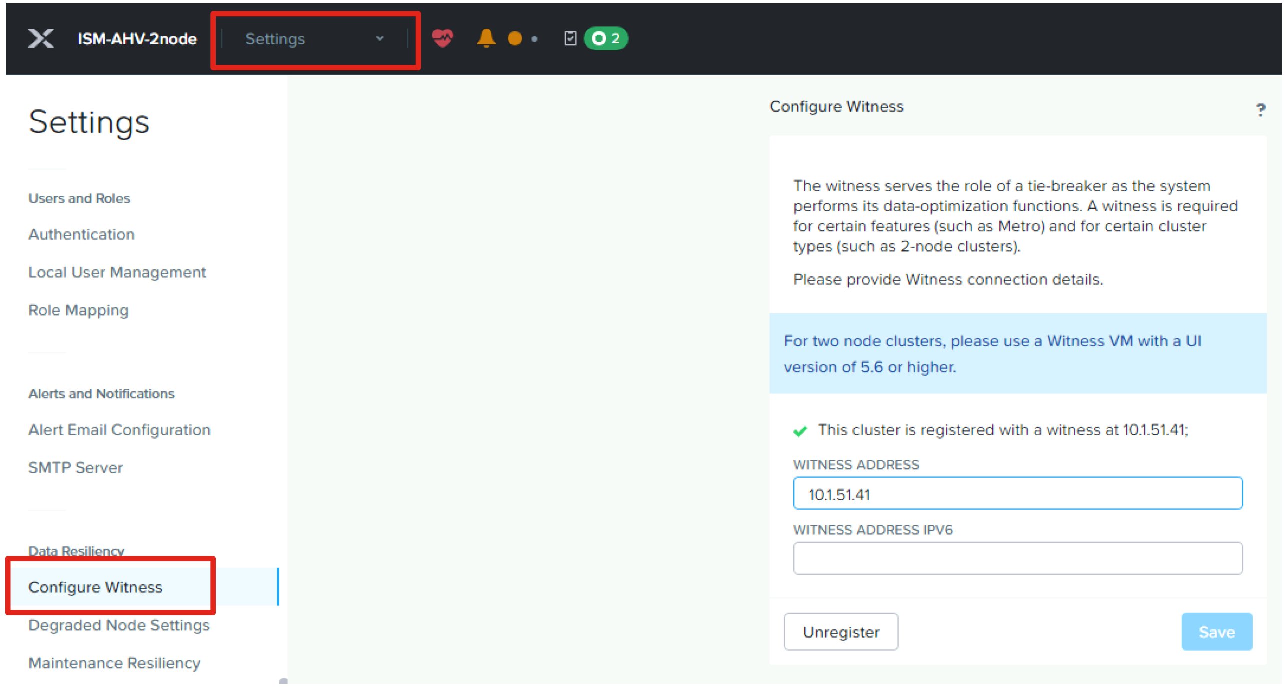
USERNAME: admin

PASSWORD: ••••••••••••••

□ Skip for now (not recommended)

Apply & Continue

Or configure later in Prism Element Settings



Configure Witness

The witness serves the role of a tie-breaker as the system performs its data-optimization functions. A witness is required for certain features (such as Metro) and for certain cluster types (such as 2-node clusters).

Please provide Witness connection details.

For two node clusters, please use a Witness VM with a UI version of 5.6 or higher.

✓ This cluster is registered with a witness at 10.1.51.41;

WITNESS ADDRESS: 10.1.51.41

WITNESS ADDRESS IPV6:

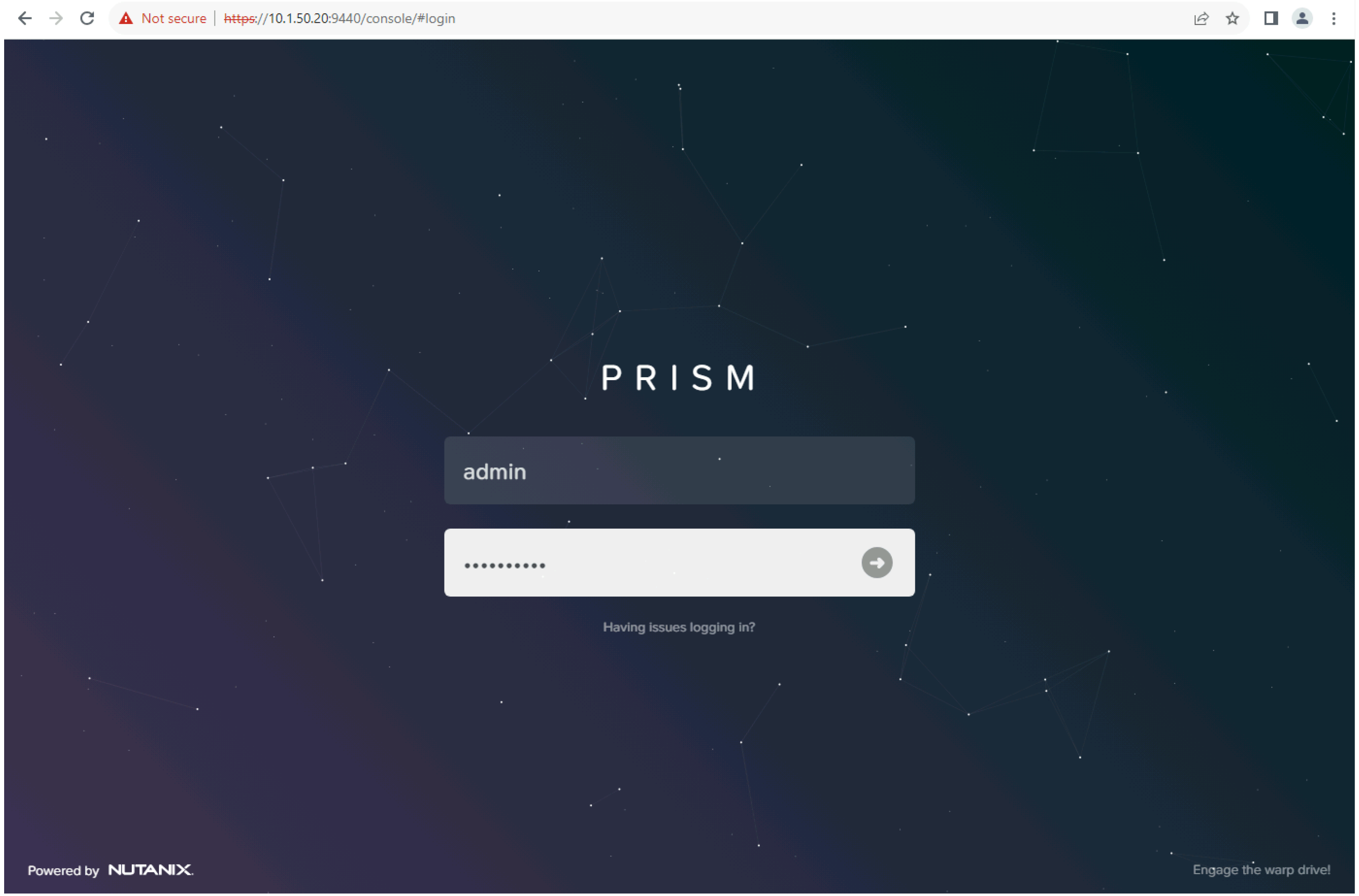
Unregister   Save

Initial Cluster Configurations

- Initial Configuration for ESXi
- Initial Configuration for AHV

Initial Nutanix Cluster Config for ESXi

Access Prism Element



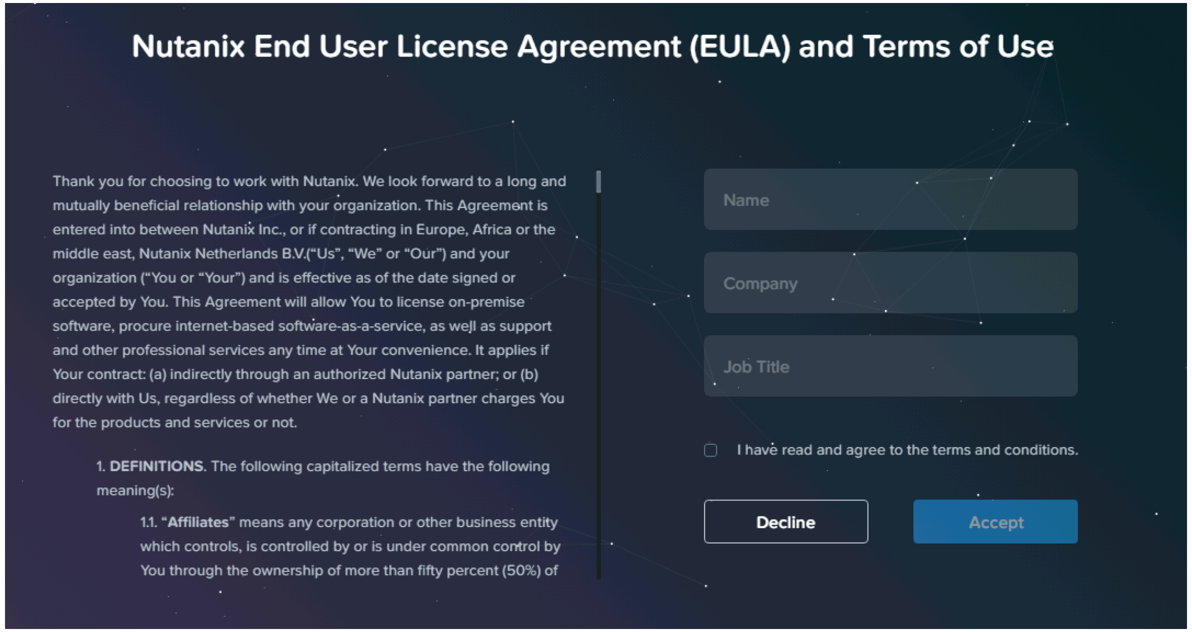
Not secure | ~~https~~://10.1.50.20:9440/console/#login

admin

••••••••••

- Access Prism Element (the built-in version of Prism) at the cluster IP address or an individual controller VM IP address, using HTTPS at port 9440
- Default username: admin
- Default password (case sensitive): Nutanix/4u
- Password must be changed on first login

Accept EULA and Enable Pulse



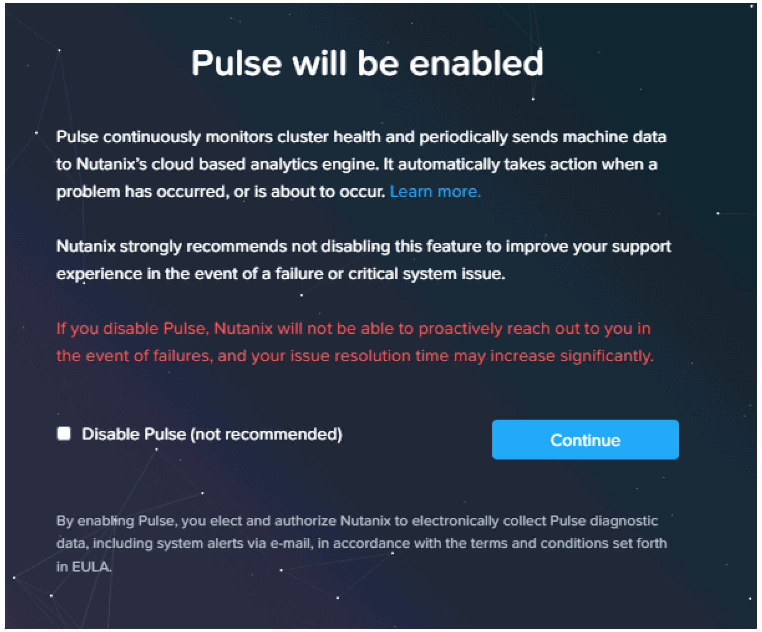
Nutanix End User License Agreement (EULA) and Terms of Use

Thank you for choosing to work with Nutanix. We look forward to a long and mutually beneficial relationship with your organization. This Agreement is entered into between Nutanix Inc., or if contracting in Europe, Africa or the middle east, Nutanix Netherlands B.V.("Us", "We" or "Our") and your organization ("You or "Your") and is effective as of the date signed or accepted by You. This Agreement will allow You to license on-premise software, procure internet-based software-as-a-service, as well as support and other professional services any time at Your convenience. It applies if Your contract: (a) indirectly through an authorized Nutanix partner; or (b) directly with Us, regardless of whether We or a Nutanix partner charges You for the products and services or not.

1. **DEFINITIONS**. The following capitalized terms have the following meaning(s):

1.1. "**Affiliates**" means any corporation or other business entity which controls, is controlled by or is under common control by You through the ownership of more than fifty percent (50%) of

□ I have read and agree to the terms and conditions.



Pulse will be enabled

Pulse continuously monitors cluster health and periodically sends machine data to Nutanix's cloud based analytics engine. It automatically takes action when a problem has occurred, or is about to occur. Learn more.

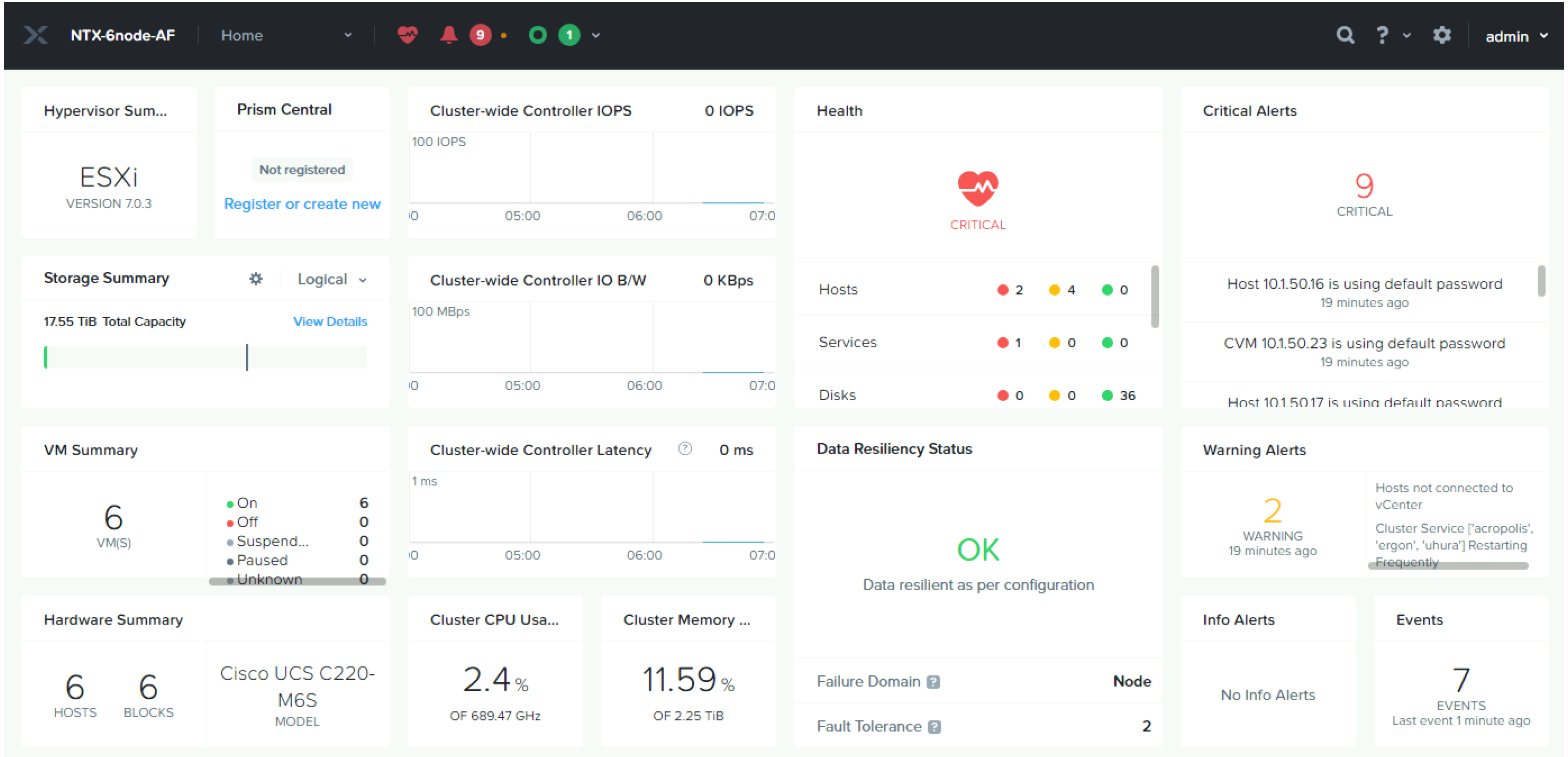
Nutanix strongly recommends not disabling this feature to improve your support experience in the event of a failure or critical system issue.

If you disable Pulse, Nutanix will not be able to proactively reach out to you in the event of failures, and your issue resolution time may increase significantly.

□ Disable Pulse (not recommended)

By enabling Pulse, you elect and authorize Nutanix to electronically collect Pulse diagnostic data, including system alerts via e-mail, in accordance with the terms and conditions set forth in EULA.

Prism Element Home



Hypervisor Sum...

ESXi
VERSION 7.0.3

Prism Central

Not registered
Register or create new

Cluster-wide Controller IOPS 0 IOPS

Health

CRITICAL

Hosts	🟥 2	🟨 4	🟩 0
Services	🟥 1	🟨 0	🟩 0
Disks	🟥 0	🟨 0	🟩 36

Critical Alerts

9
CRITICAL

Host 10.1.50.16 is using default password
19 minutes ago

CVM 10.1.50.23 is using default password
19 minutes ago

Host 10.1.50.17 is using default password

Storage Summary Logical

17.55 TiB Total Capacity View Details

Cluster-wide Controller IO B/W 0 KBps

VM Summary

6
VM(S)

● On	6
● Off	0
● Suspend...	0
● Paused	0
● Unknown	0

Cluster-wide Controller Latency 0 ms

Data Resiliency Status

OK
Data resilient as per configuration

Failure Domain	Node
Fault Tolerance	2

Warning Alerts

2
WARNING
19 minutes ago

Hosts not connected to vCenter

Cluster Service ['acropolis', 'ergon', 'uhura'] Restarting Frequently

Hardware Summary

6 HOSTS 6 BLOCKS

Cisco UCS C220-M6S
MODEL

Cluster CPU Usa...

2.4 %
OF 689.47 GHz

Cluster Memory ...

11.59 %
OF 2.25 TiB

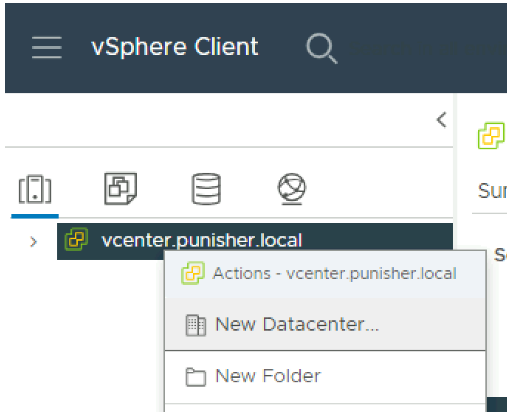
Info Alerts

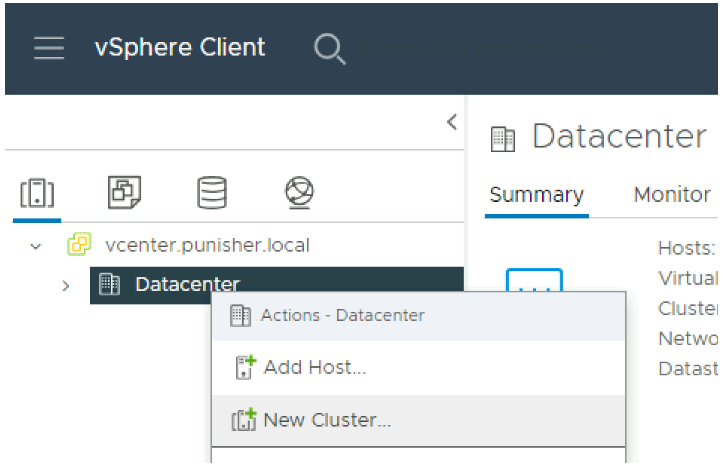
No Info Alerts

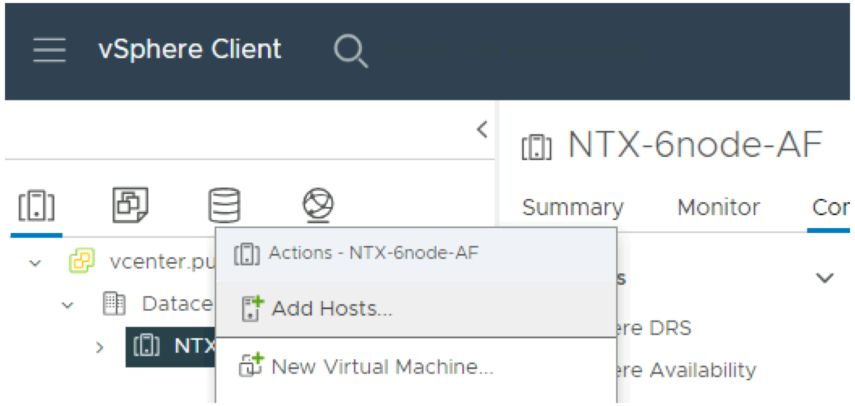
Events

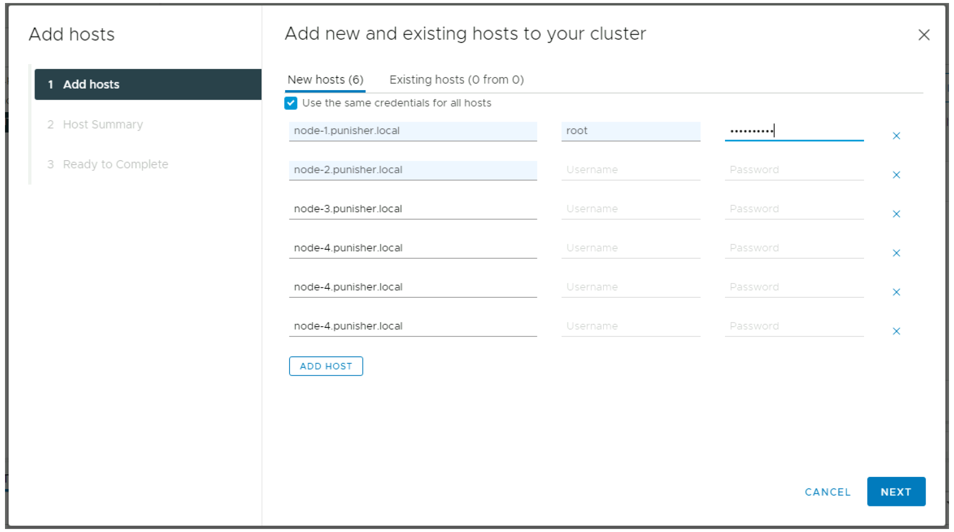
7
EVENTS
Last event 1 minute ago

Add Hosts to vCenter Server









Add hosts

1 Add hosts
2 Host Summary
3 Ready to Complete

Add new and existing hosts to your cluster

New hosts (6) Existing hosts (0 from 0)

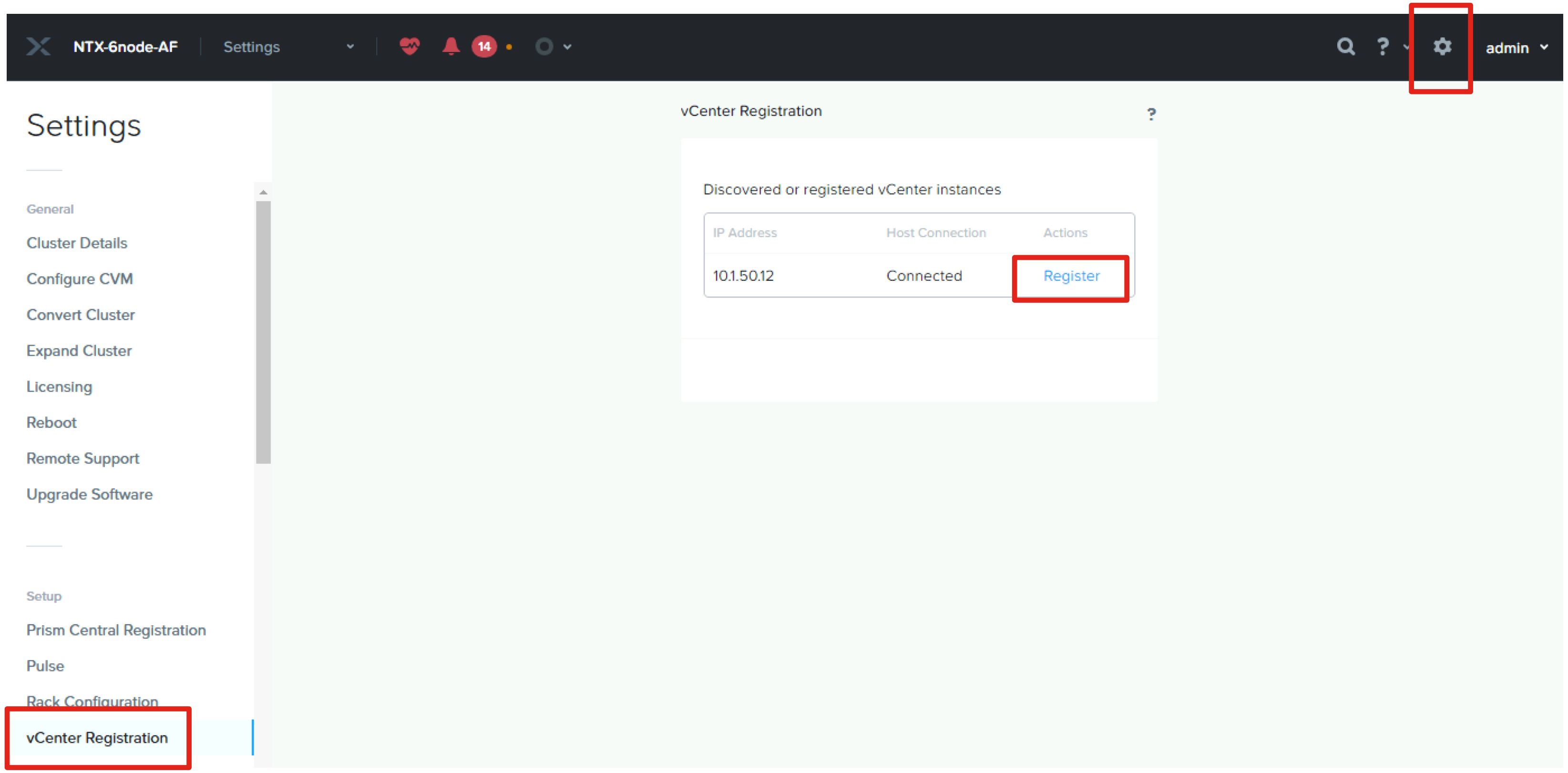
☑ Use the same credentials for all hosts

node-1.punisher.local	root	··········
node-2.punisher.local	Username	Password
node-3.punisher.local	Username	Password
node-4.punisher.local	Username	Password
node-4.punisher.local	Username	Password
node-4.punisher.local	Username	Password

In the vSphere Web Client, create a Datacenter, a Cluster and add the hosts. You will have to move the hosts into the cluster after adding them.

Refer here for the recommended vSphere, DRS and HA settings: https://portal.nutanix.com/page/documents/details?targetId=vSphere-Admin6-AOS-v6_5:vsp-cluster-settings-vcenter-vsphere-c.html

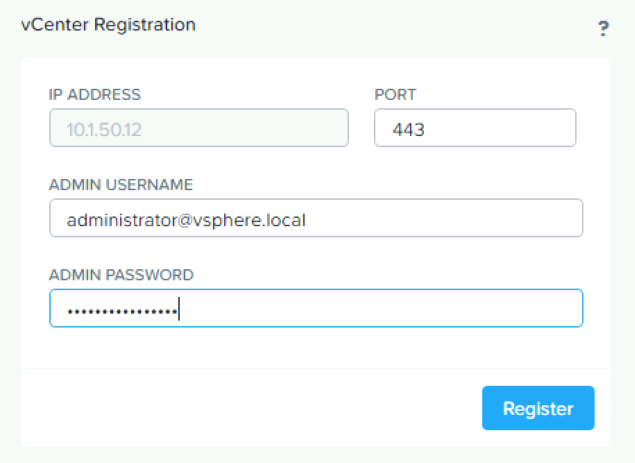
Prism Element to vCenter Server Registration



vCenter Registration ?

Discovered or registered vCenter instances

IP Address	Host Connection	Actions
10.1.50.12	Connected	Register



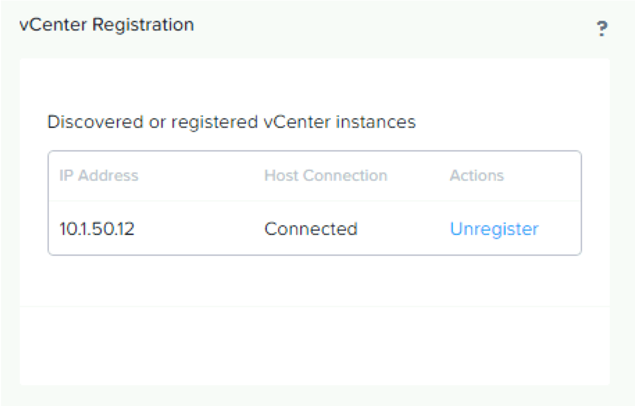
vCenter Registration ?

IP ADDRESS: 10.1.50.12

PORT: 443

ADMIN USERNAME: administrator@vsphere.local

ADMIN PASSWORD: ••••••••••••••••



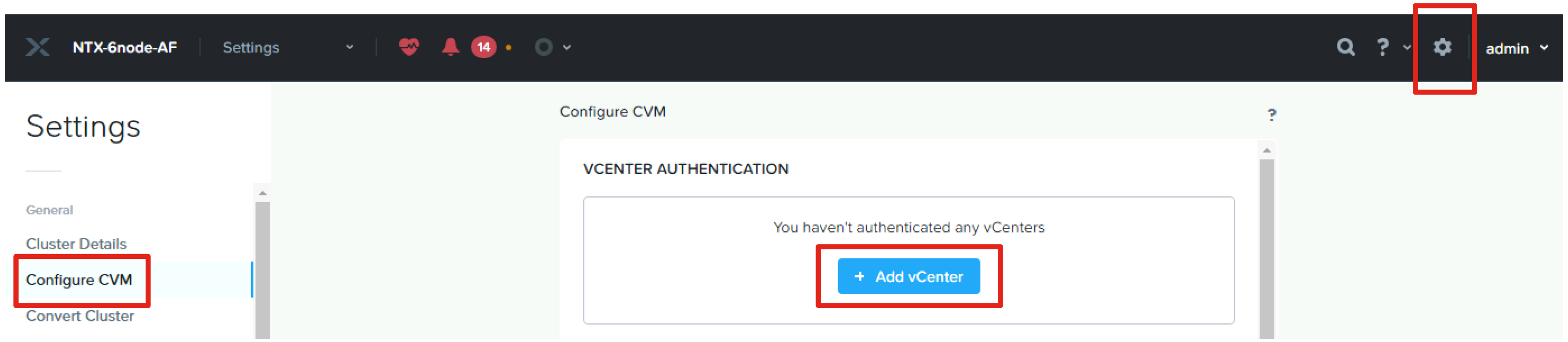
vCenter Registration ?

Discovered or registered vCenter instances

IP Address	Host Connection	Actions
10.1.50.12	Connected	Unregister

Note: It may take a few minutes after adding the nodes for the vCenter to be discovered and allow you to register it.

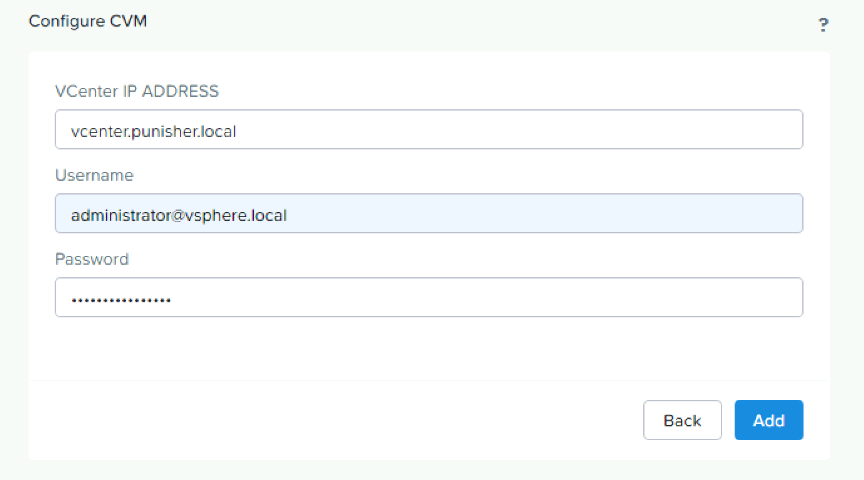
Configure vCenter Server Authentication



Configure CVM

VCENTER AUTHENTICATION

You haven't authenticated any vCenters



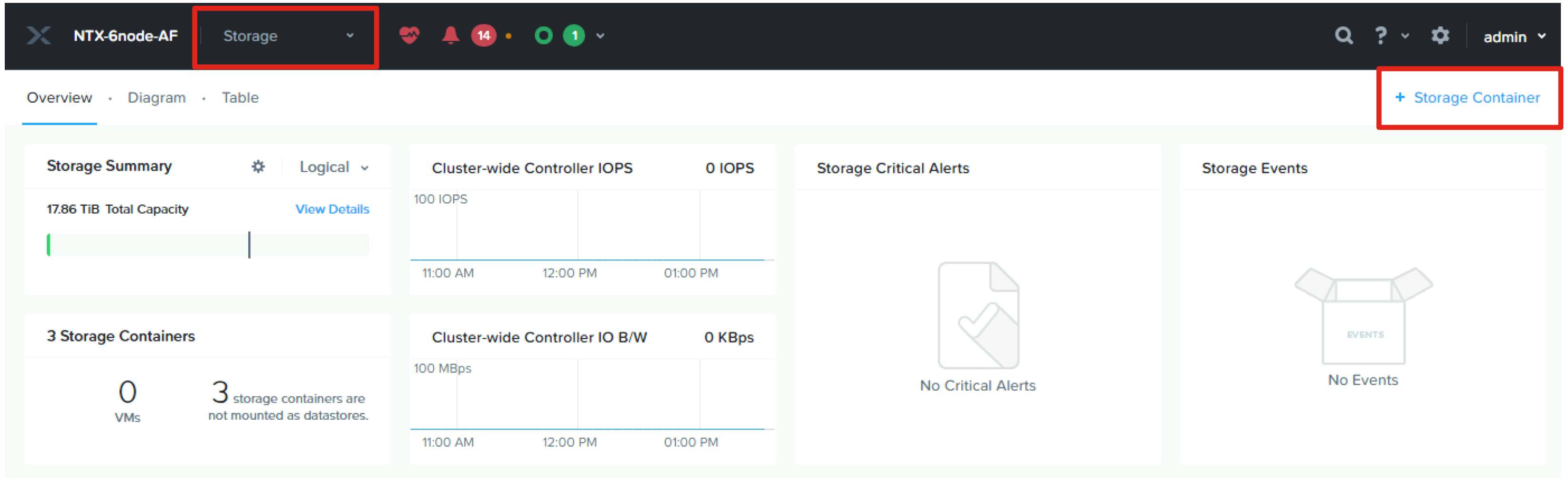
Configure CVM

VCenter IP ADDRESS: vcenter.punisher.local

Username: administrator@vsphere.local

Password: ••••••••••••••••

Create Storage Containers (Datastores)


NTX-6node-AF · Storage · 14 · 1 · admin

Overview · Diagram · Table · + Storage Container

Storage Summary · Logical
17.86 TiB Total Capacity · View Details

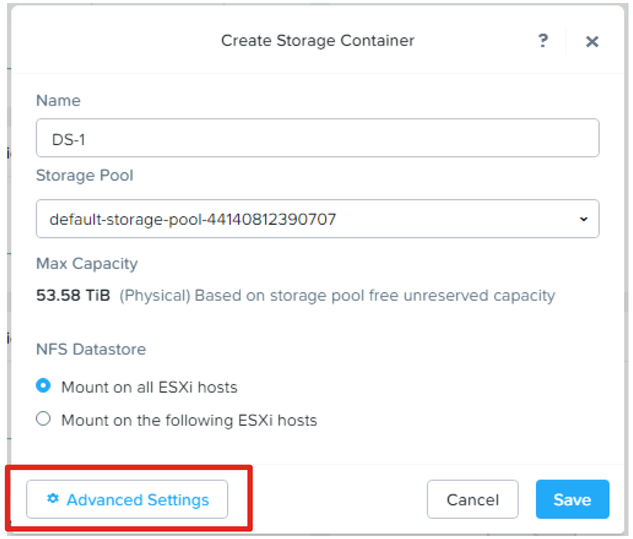
Cluster-wide Controller IOPS: 0 IOPS
100 IOPS · 11:00 AM · 12:00 PM · 01:00 PM

Storage Critical Alerts: No Critical Alerts

Storage Events: No Events

3 Storage Containers
0 VMs
3 storage containers are not mounted as datastores.

Cluster-wide Controller IO B/W: 0 KBps
100 MBps · 11:00 AM · 12:00 PM · 01:00 PM

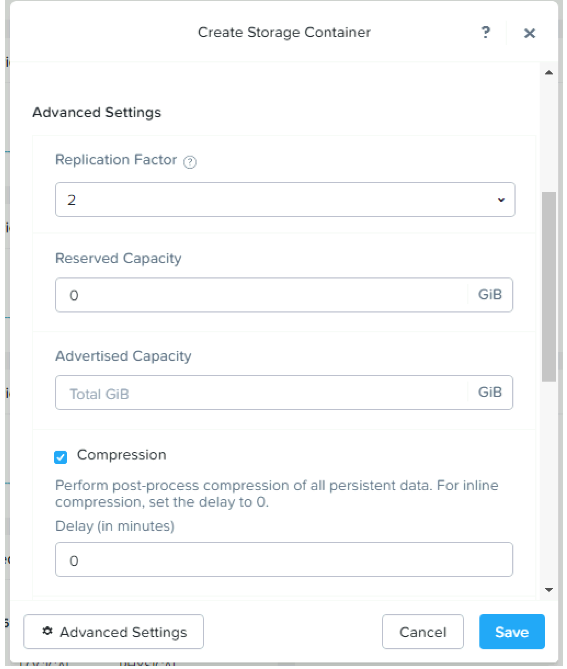

Create Storage Container

Name: DS-1

Storage Pool: default-storage-pool-44140812390707

Max Capacity: 53.58 TiB (Physical) Based on storage pool free unreserved capacity

NFS Datastore
● Mount on all ESXi hosts
○ Mount on the following ESXi hosts


Create Storage Container

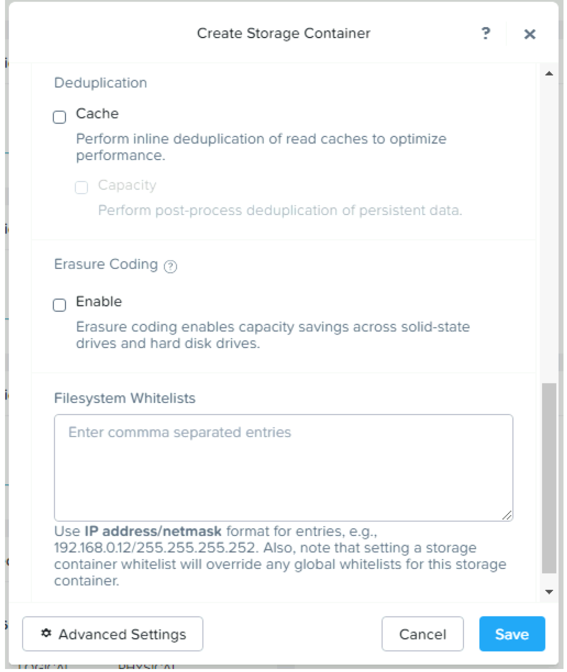
Advanced Settings

Replication Factor: 2

Reserved Capacity: 0 GiB

Advertised Capacity: Total GiB

☑ Compression
Perform post-process compression of all persistent data. For inline compression, set the delay to 0.
Delay (in minutes): 0


Create Storage Container

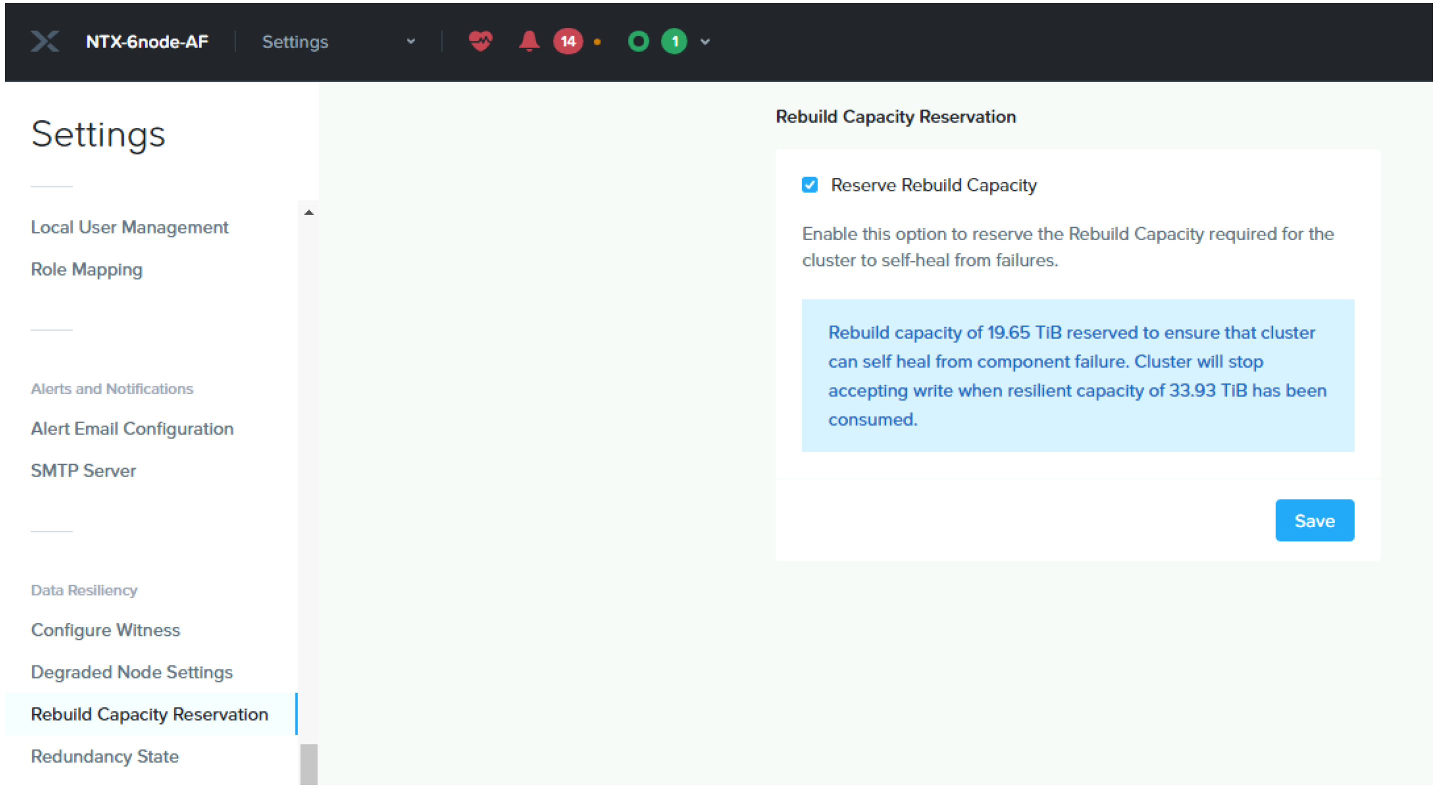
Deduplication
□ Cache
Perform inline deduplication of read caches to optimize performance.
□ Capacity
Perform post-process deduplication of persistent data.

Erasure Coding
□ Enable
Erasure coding enables capacity savings across solid-state drives and hard disk drives.

Filesystem Whitelists
Enter commma separated entries
Use IP address/netmask format for entries, e.g., 192.168.0.12/255.255.255.252. Also, note that setting a storage container whitelist will override any global whitelists for this storage container.

Note: After creating the containers, you should manually select them as the HA datastores in the vCenter Cluster Availability settings, when using ESXi.

Set Rebuild Capacity Reservation



Settings

Local User Management
Role Mapping

Alerts and Notifications
Alert Email Configuration
SMTP Server

Data Resiliency
Configure Witness
Degraded Node Settings
Rebuild Capacity Reservation
Redundancy State

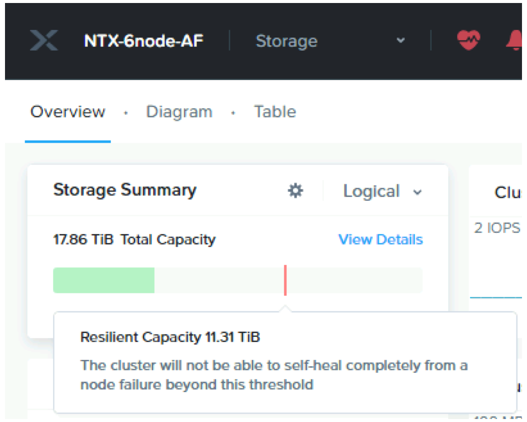
Rebuild Capacity Reservation

☑ Reserve Rebuild Capacity

Enable this option to reserve the Rebuild Capacity required for the cluster to self-heal from failures.

Rebuild capacity of 19.65 TiB reserved to ensure that cluster can self heal from component failure. Cluster will stop accepting write when resilient capacity of 33.93 TiB has been consumed.

Save



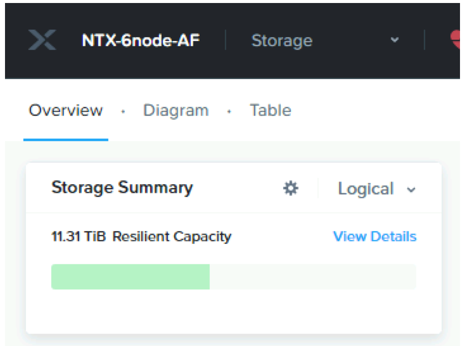
Storage Summary Logical

17.86 TiB Total Capacity View Details

Resilient Capacity 11.31 TiB

The cluster will not be able to self-heal completely from a node failure beyond this threshold

Without this setting enabled, cluster will accept incoming writes even if all blocks cannot completely heal during failures

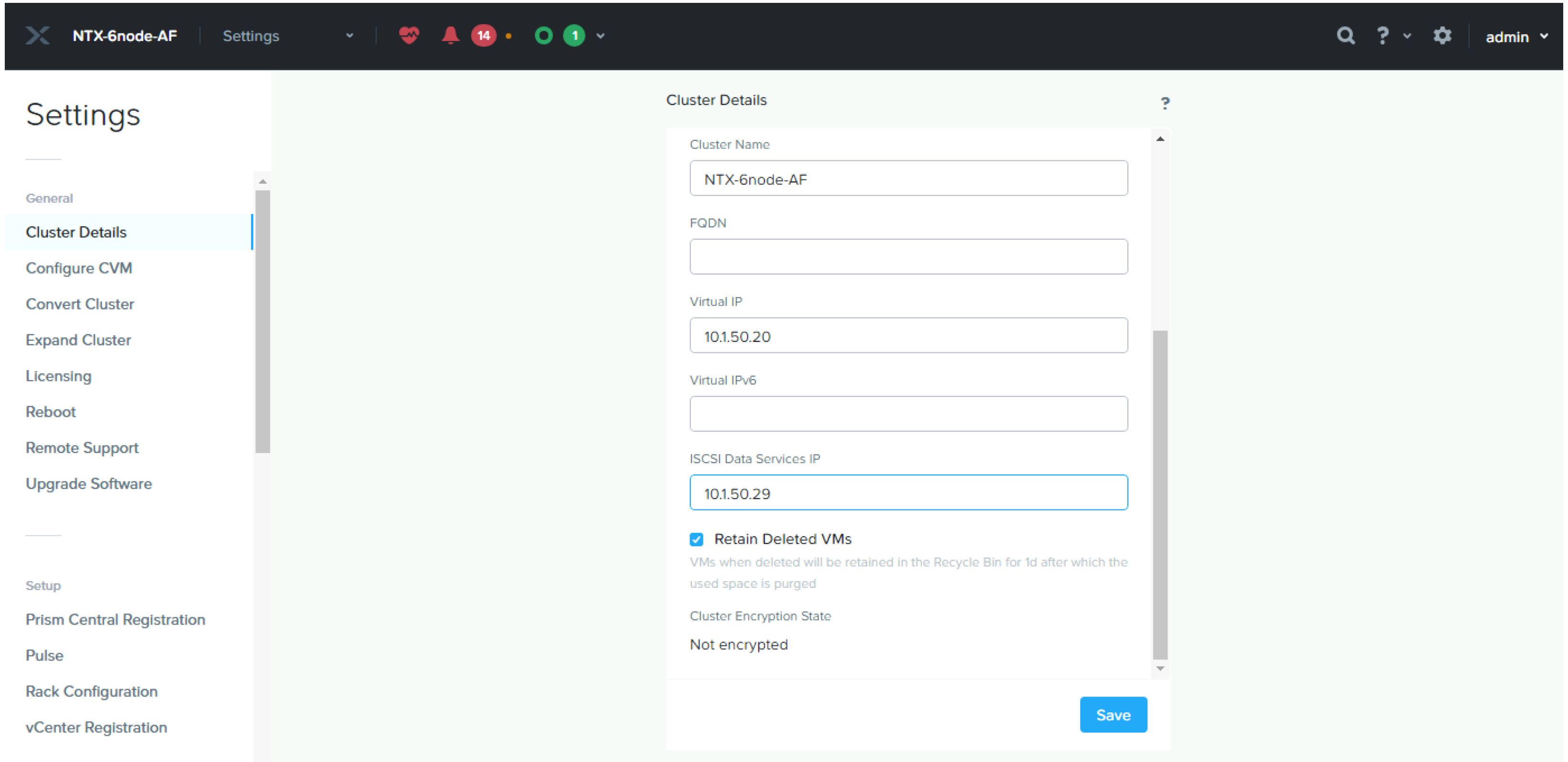


Storage Summary Logical

11.31 TiB Resilient Capacity View Details

After enabling, cluster will refuse new writes if they cannot be fully protected during failures

Set iSCSI Data Services IP Address



Cluster Details

Cluster Name: NTX-6node-AF

FQDN:

Virtual IP: 10.1.50.20

Virtual IPv6:

ISCSI Data Services IP: 10.1.50.29

☑ Retain Deleted VMs

VMs when deleted will be retained in the Recycle Bin for 1d after which the used space is purged

Cluster Encryption State: Not encrypted

This is an additional clustered IP address for enabling iSCSI Data Services, which is required to install Prism Central.

Modify Default Passwords on ESXi and CVMs

Follow the instructions here to reset the default administrative passwords on the ESXi hypervisors and the Nutanix controller VMs: https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e000000LKXcCAO

Log on to a CVM via SSH, username: nutanix password: nutanix/4u

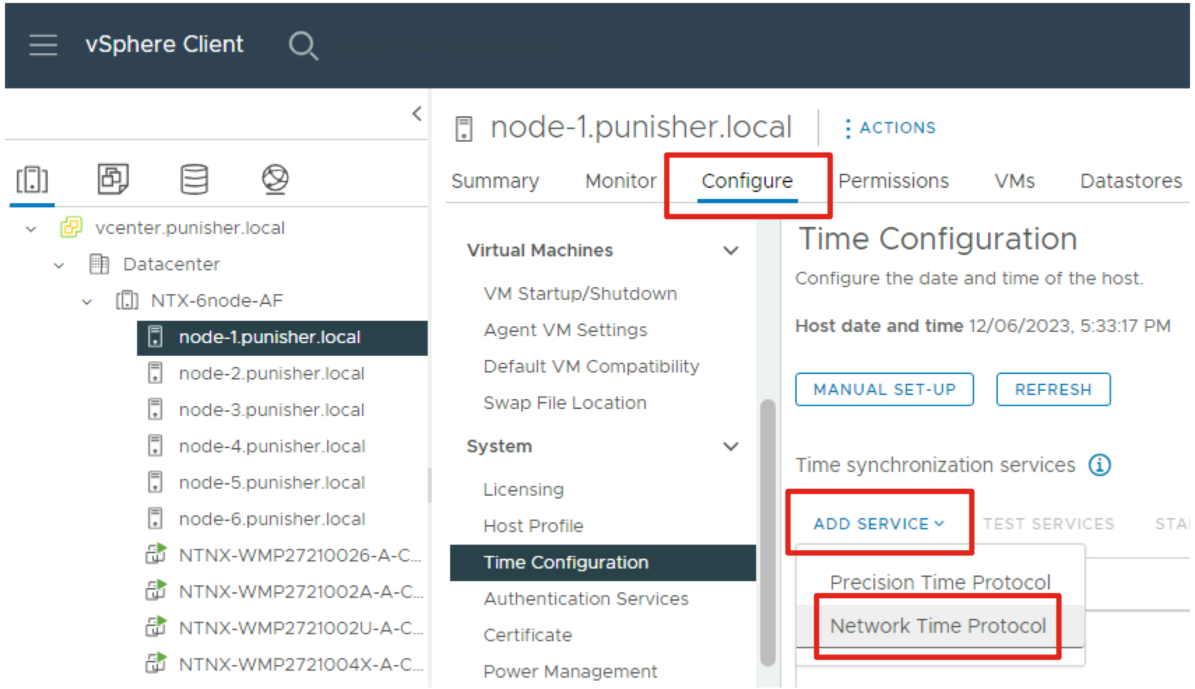
```
nutanix@NTNX-WMP27210026-A-CVM:10.1.50.21:~$ sudo passwd nutanix
Changing password for user nutanix.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Re-run NCC password health check after changing the passwords

```
nutanix@NTNX-WMP27210026-A-CVM:10.1.50.21:~$ ncc health_checks
system_checks default_password_check
```

```
nutanix@NTNX-WMP27210026-A-CVM:10.1.50.21:~$ echo -e "CHANGING ALL
ESXi HOST PASSWORDS. Note - This script cannot be used for passwords
that contain special characters ( $ \ { }  ^ &)\nPlease input new
password: "; read -s password1; echo "Confirm new password: "; read -s
password2; if [ "$password1" == "$password2" ] && [[ ! "$password1" =~
[\\\{\$\^\}\&] ]]; then hostssh "echo -e \"${password1}\" | passwd
root --stdin"; else echo "The passwords do not match or contain
invalid characters (\ $ { } ^ &)"; fi
CHANGING ALL ESXi HOST PASSWORDS. Note - This script cannot be used
for passwords that contain special characters ( $ \ { }  ^ &)
Please input new password:
Confirm new password:
============= 10.1.50.14 ============
Changing password for root
passwd: password updated successfully
============= 10.1.50.18 ============
Changing password for root
passwd: password updated successfully
============= 10.1.50.16 ============
Changing password for root
passwd: password updated successfully
============= 10.1.50.15 ============
Changing password for root
passwd: password updated successfully
============= 10.1.50.19 ============
Changing password for root
passwd: password updated successfully
============= 10.1.50.17 ============
Changing password for root
passwd: password updated successfully
```

Enable NTP on ESXi hosts

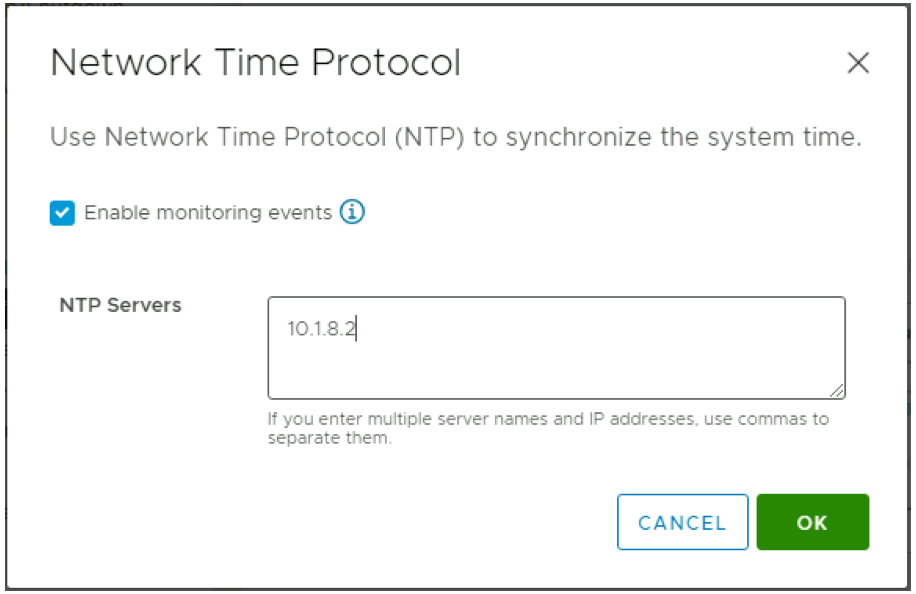


Time Configuration

Configure the date and time of the host.

Host date and time 12/06/2023, 5:33:17 PM

Time synchronization services



Network Time Protocol

Use Network Time Protocol (NTP) to synchronize the system time.

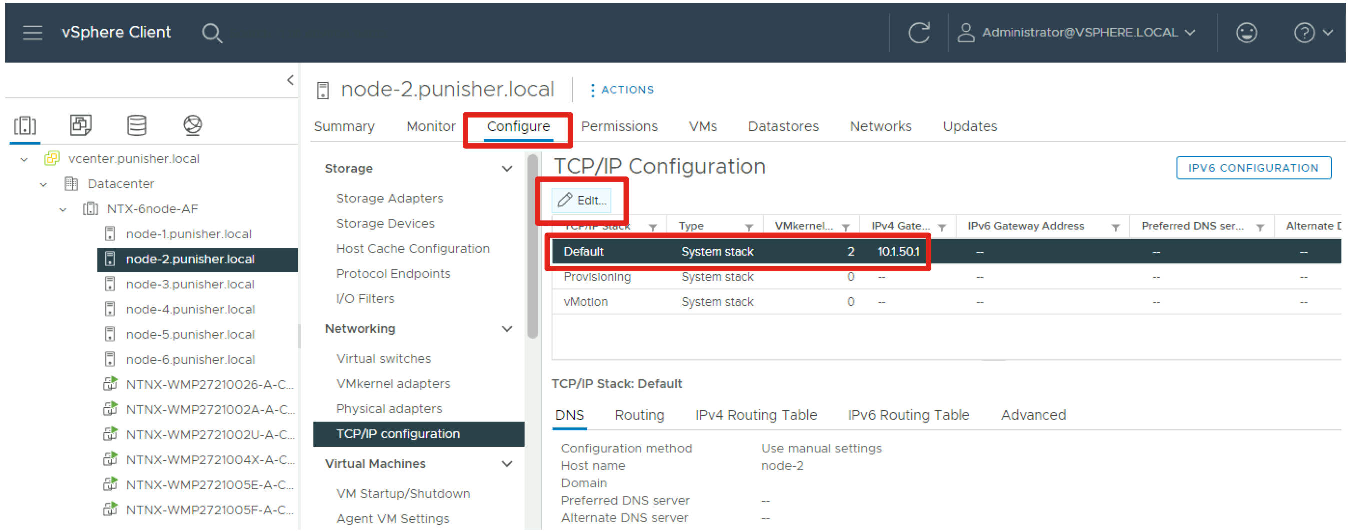
☑ Enable monitoring events

NTP Servers 10.1.8.2

If you enter multiple server names and IP addresses, use commas to separate them.

Repeat for each ESXi hypervisor host

Configure DNS on ESXi hosts

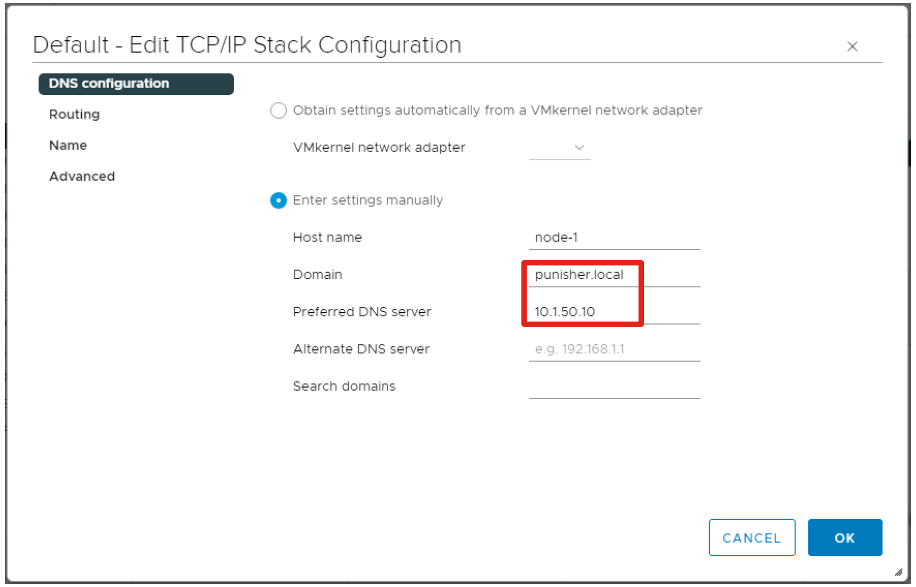


TCP/IP Configuration

TCP/IP Stack	Type	VMkernel...	IPv4 Gate...	IPv6 Gateway Address	Preferred DNS ser...	Alternate D
Default	System stack	2	10.1.50.1	--	--	--
Provisioning	System stack	0	--	--	--	--
vMotion	System stack	0	--	--	--	--

TCP/IP Stack: Default

Configuration method	Use manual settings
Host name	node-2
Domain	
Preferred DNS server	--
Alternate DNS server	--



Default - Edit TCP/IP Stack Configuration

○ Obtain settings automatically from a VMkernel network adapter

VMkernel network adapter

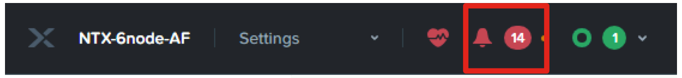
● Enter settings manually

Host name	node-1
Domain	punisher.local
Preferred DNS server	10.1.50.10
Alternate DNS server	e.g. 192.168.1.1
Search domains	

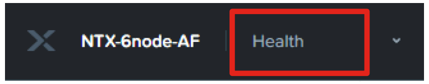
Repeat for each ESXi hypervisor host

Remediate all NCC Failures and Warnings

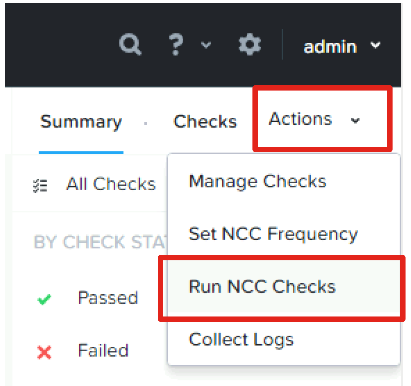
Resolve all active alerts



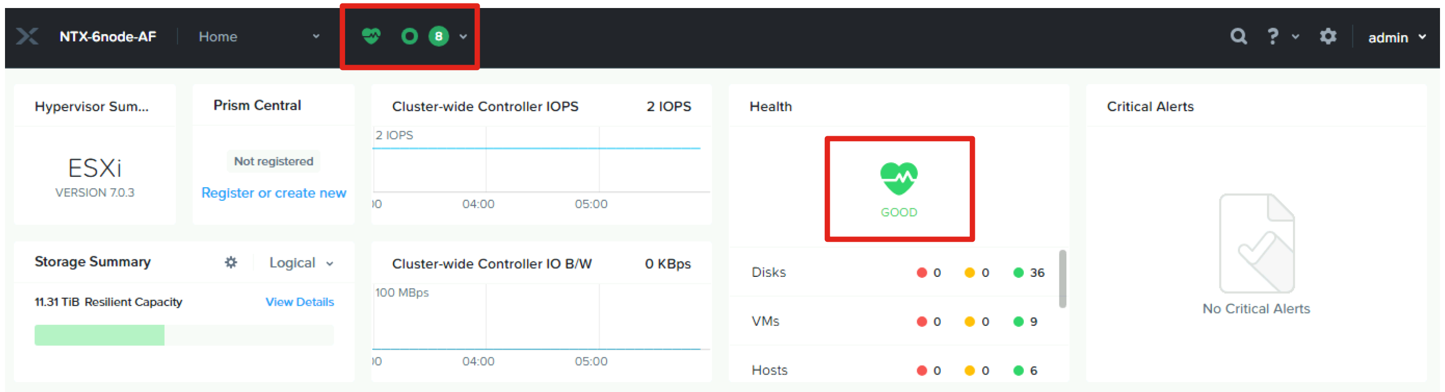
Go to Health



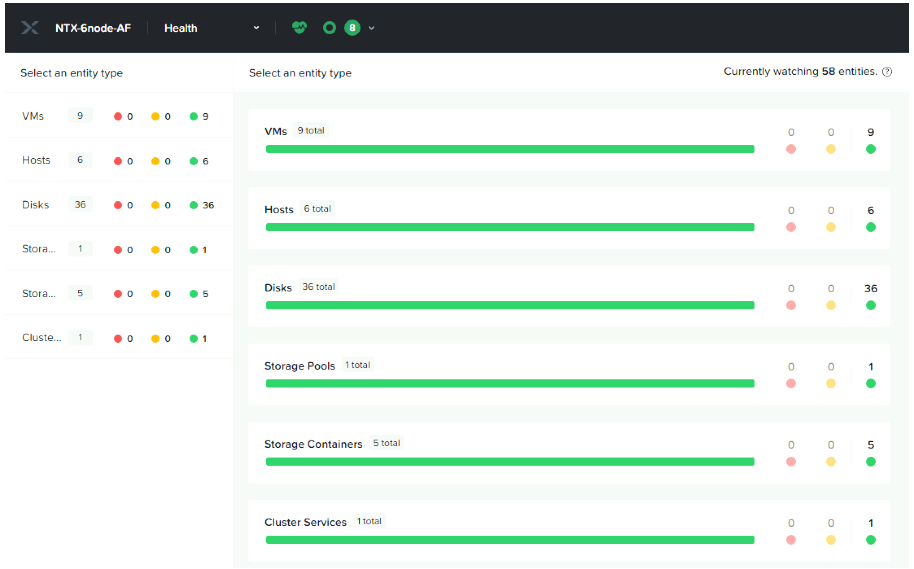
Run NCC checks



Remediate until all Alerts, Failures and Warnings are gone



Health			
Disks	0	0	36
VMs	0	0	9
Hosts	0	0	6

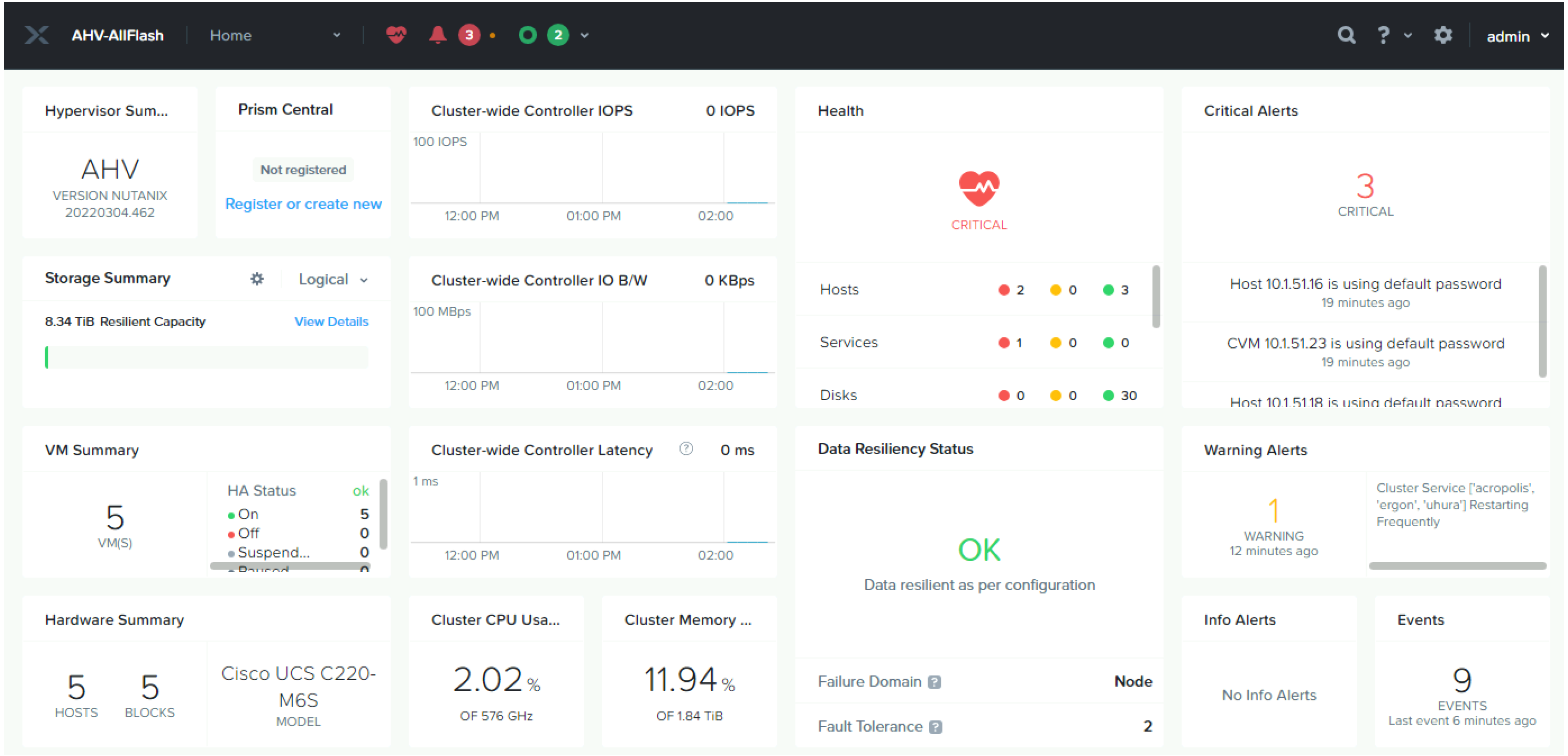


VMs	9	0	0	9
Hosts	6	0	0	6
Disks	36	0	0	36
Stora...	1	0	0	1
Stora...	5	0	0	5
Cluste...	1	0	0	1

VMs 9 total	0	0	9
Hosts 6 total	0	0	6
Disks 36 total	0	0	36
Storage Pools 1 total	0	0	1
Storage Containers 5 total	0	0	5
Cluster Services 1 total	0	0	1

Initial Nutanix Cluster Config for AHV

Prism Element Home



Hypervisor Sum...

AHV
VERSION NUTANIX 20220304.462

Prism Central

Not registered

Register or create new

Cluster-wide Controller IOPS 0 IOPS

Health

CRITICAL

Hosts	● 2	● 0	● 3
Services	● 1	● 0	● 0
Disks	● 0	● 0	● 30

Critical Alerts

3
CRITICAL

Host 10.1.51.16 is using default password
19 minutes ago

CVM 10.1.51.23 is using default password
19 minutes ago

Host 10.1.51.18 is using default password

Storage Summary — Logical

8.34 TiB Resilient Capacity — View Details

Cluster-wide Controller IO B/W 0 KBps

VM Summary

5
VM(S)

HA Status	ok
● On	5
● Off	0
● Suspend...	0
● Paused	0

Cluster-wide Controller Latency 0 ms

Data Resiliency Status

OK
Data resilient as per configuration

Failure Domain	Node
Fault Tolerance	2

Warning Alerts

1
WARNING
12 minutes ago

Cluster Service ['acropolis', 'ergon', 'uhura'] Restarting Frequently

Hardware Summary

5 HOSTS — 5 BLOCKS

Cisco UCS C220-M6S
MODEL

Cluster CPU Usa...

2.02 %
OF 576 GHz

Cluster Memory ...

11.94 %
OF 1.84 TiB

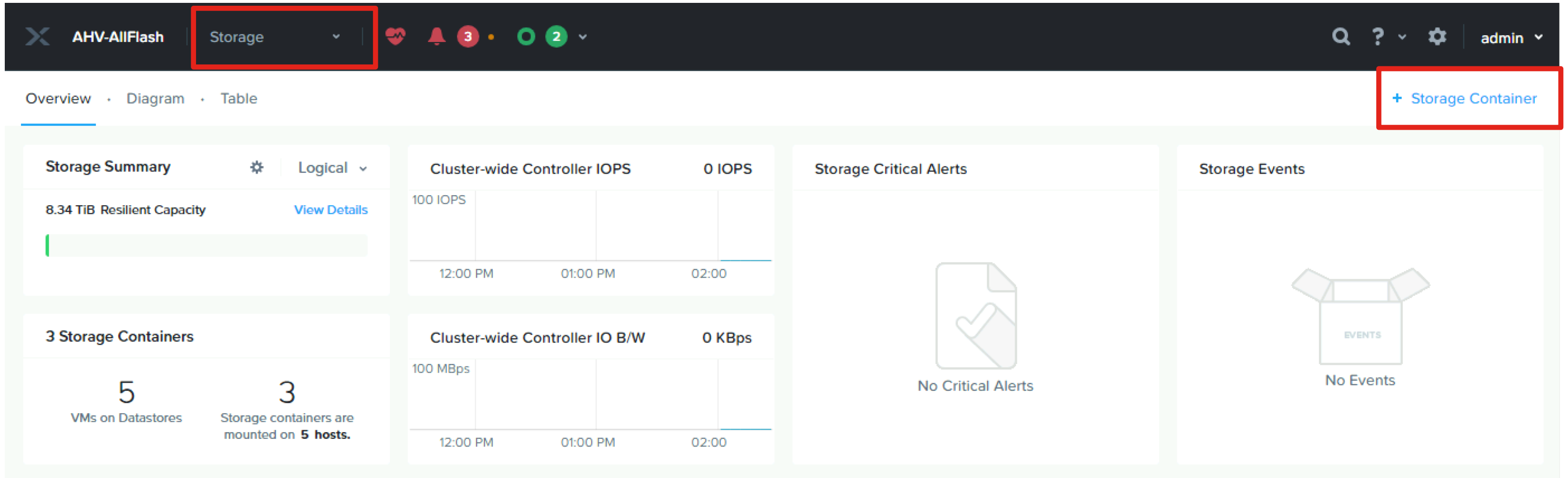
Info Alerts

No Info Alerts

Events

9
EVENTS
Last event 6 minutes ago

Create Storage Containers (Datastores)



Storage Summary · Logical

8.34 TiB Resilient Capacity · View Details

3 Storage Containers

5 VMs on Datastores

3 Storage containers are mounted on 5 hosts.

Cluster-wide Controller IOPS · 0 IOPS

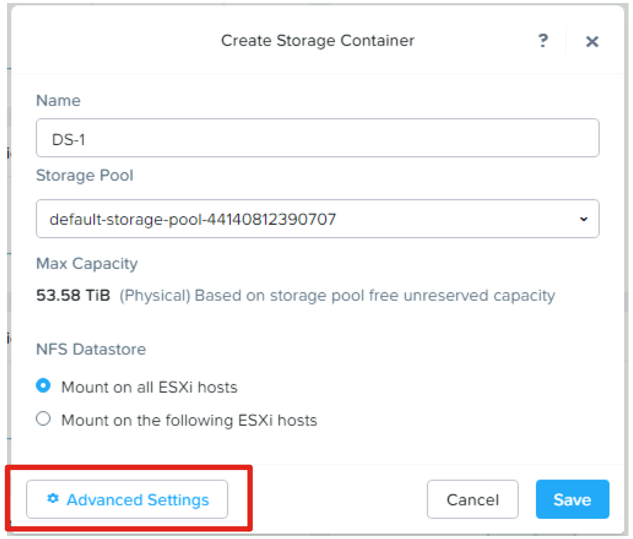
Cluster-wide Controller IO B/W · 0 KBps

Storage Critical Alerts

No Critical Alerts

Storage Events

No Events



Create Storage Container

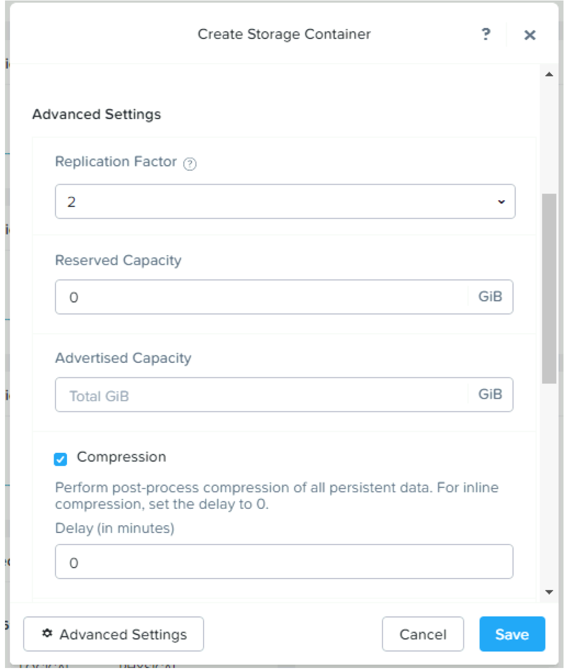
Name: DS-1

Storage Pool: default-storage-pool-44140812390707

Max Capacity: 53.58 TiB (Physical) Based on storage pool free unreserved capacity

NFS Datastore

- ● Mount on all ESXi hosts
- ○ Mount on the following ESXi hosts



Create Storage Container

Advanced Settings

Replication Factor: 2

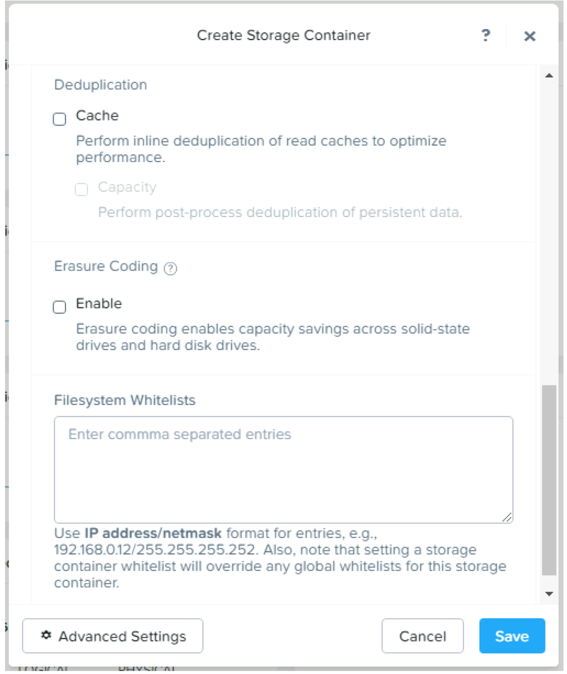
Reserved Capacity: 0 GiB

Advertised Capacity: Total GiB

☑ Compression

Perform post-process compression of all persistent data. For inline compression, set the delay to 0.

Delay (in minutes): 0



Create Storage Container

Deduplication

□ Cache

Perform inline deduplication of read caches to optimize performance.

□ Capacity

Perform post-process deduplication of persistent data.

Erasure Coding

□ Enable

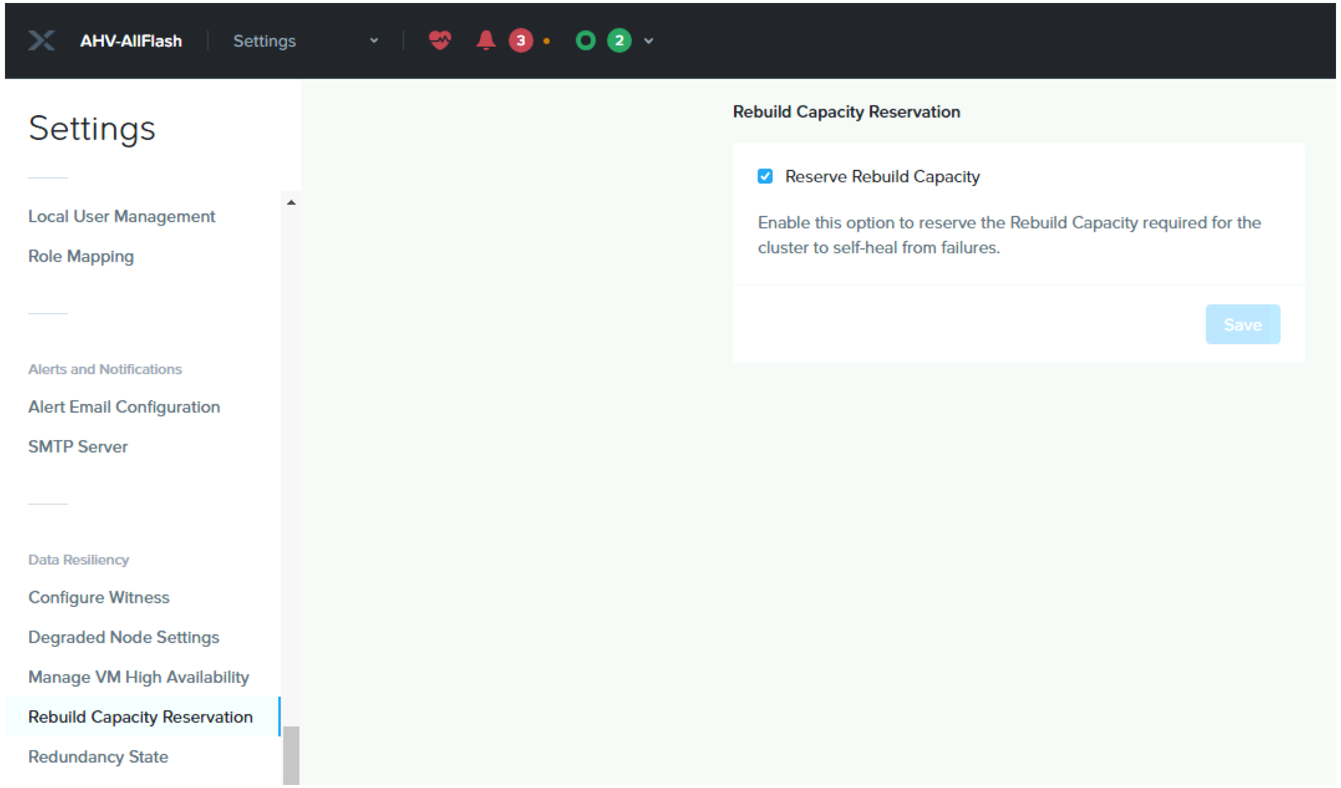
Erasure coding enables capacity savings across solid-state drives and hard disk drives.

Filesystem Whitelists

Enter commma separated entries

Use **IP address/netmask** format for entries, e.g., 192.168.0.12/255.255.255.252. Also, note that setting a storage container whitelist will override any global whitelists for this storage container.

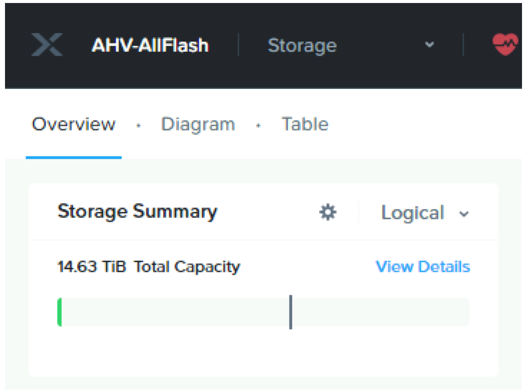
Set Rebuild Capacity Reservation



Rebuild Capacity Reservation

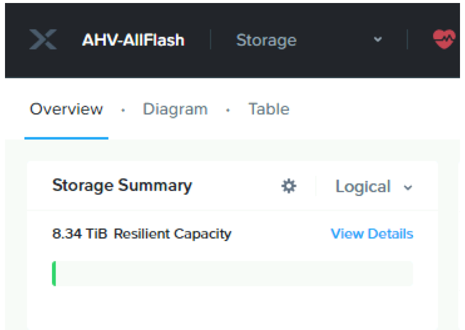
☑ Reserve Rebuild Capacity

Enable this option to reserve the Rebuild Capacity required for the cluster to self-heal from failures.



14.63 TiB Total Capacity

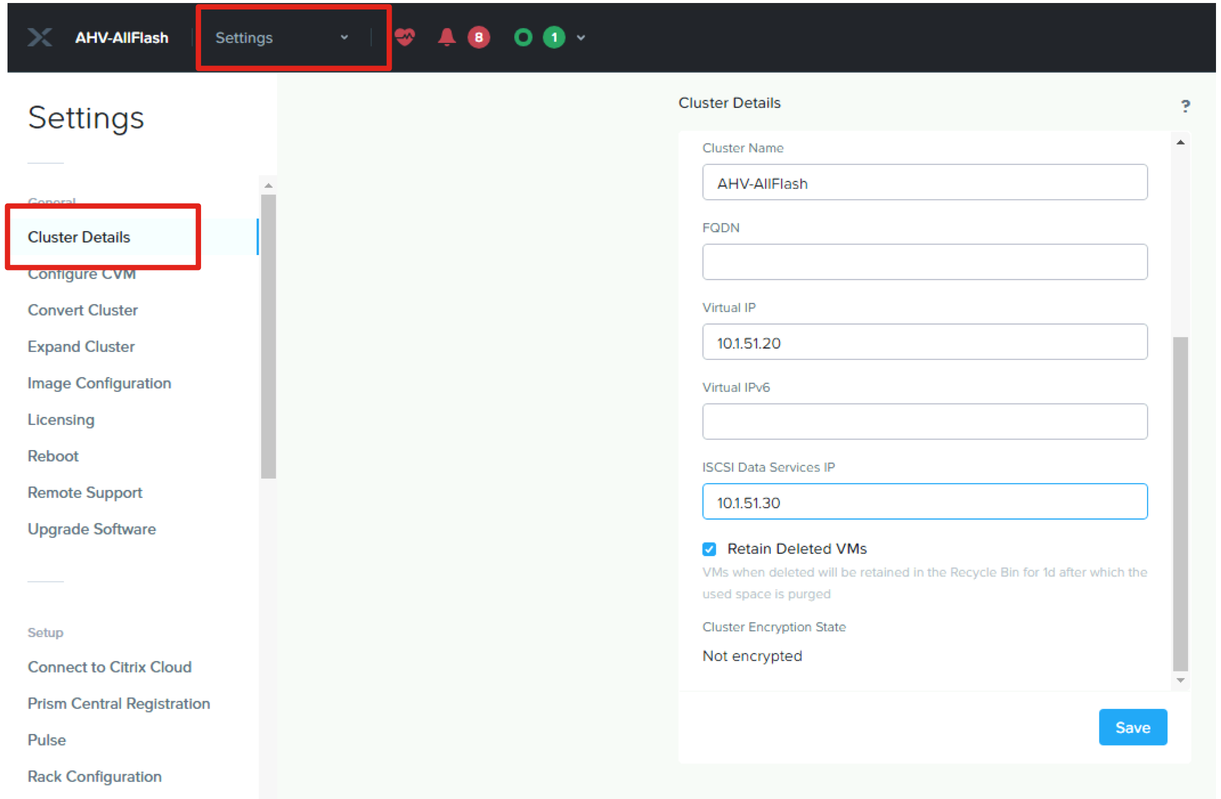
Without this setting enabled, cluster will accept incoming writes even if all blocks cannot completely heal during failures



8.34 TiB Resilient Capacity

After enabling, cluster will refuse new writes if they cannot be fully protected during failures

Set iSCSI Data Services IP Address



Settings

General

Cluster Details

Configure CVM

Convert Cluster

Expand Cluster

Image Configuration

Licensing

Reboot

Remote Support

Upgrade Software

Setup

Connect to Citrix Cloud

Prism Central Registration

Pulse

Rack Configuration

Cluster Details

Cluster Name: AHV-AllFlash

FQDN:

Virtual IP: 10.1.51.20

Virtual IPv6:

ISCSI Data Services IP: 10.1.51.30

☑ Retain Deleted VMs

VMs when deleted will be retained in the Recycle Bin for 1d after which the used space is purged

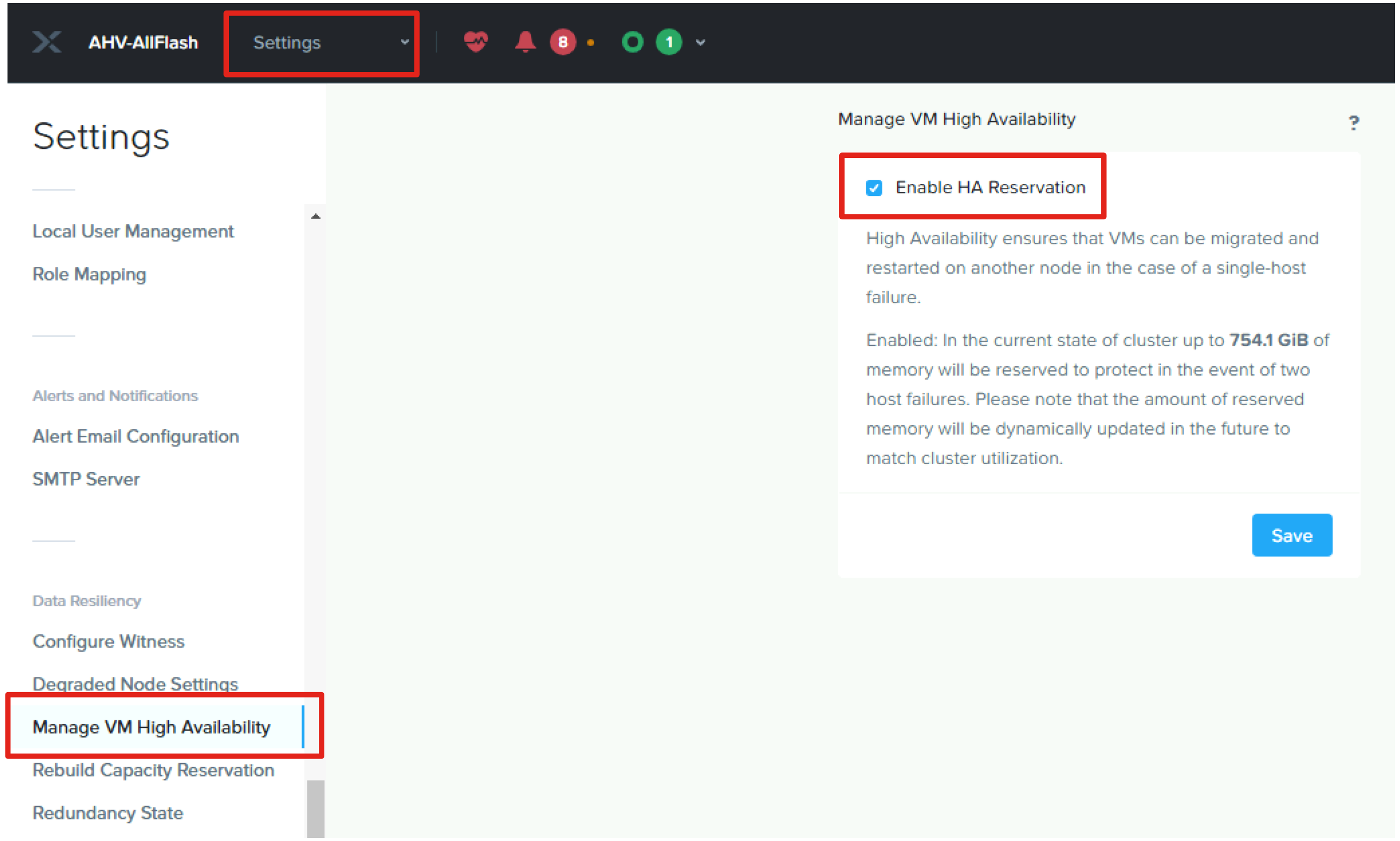
Cluster Encryption State

Not encrypted

Save

This is an additional clustered IP address for enabling iSCSI Data Services, which is required to install Prism Central.

Enable VM High Availability Reservation



Manage VM High Availability

☑ Enable HA Reservation

High Availability ensures that VMs can be migrated and restarted on another node in the case of a single-host failure.

Enabled: In the current state of cluster up to **754.1 GiB** of memory will be reserved to protect in the event of two host failures. Please note that the amount of reserved memory will be dynamically updated in the future to match cluster utilization.

Modify Default Passwords on AHV and CVMs

Follow the instructions here to reset the default administrative passwords on the AHV hypervisors, and the Nutanix controller VMs:
https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e000000LKXcCAO
Three accounts on AHV must have their passwords reset: root, admin and nutanix

Log on to a CVM via SSH, username: nutanix
password: nutanix/4u

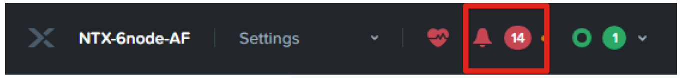
```
nutanix@NTNX-WMP27210026-A-CVM:10.1.50.21:~$ sudo passwd nutanix
Changing password for user nutanix.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Re-run NCC password health check after changing the passwords

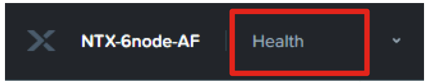
```
nutanix@NTNX-WMP27210026-A-CVM:10.1.50.21:~$ ncc health_checks
system_checks default_password_check
```

Remediate all NCC Failures and Warnings

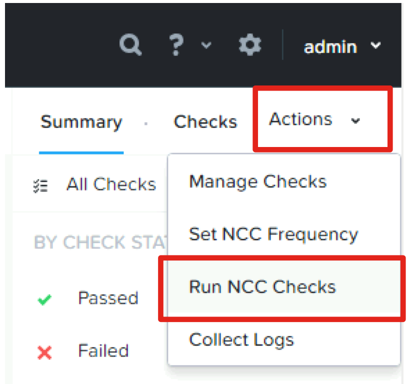
Resolve all active alerts



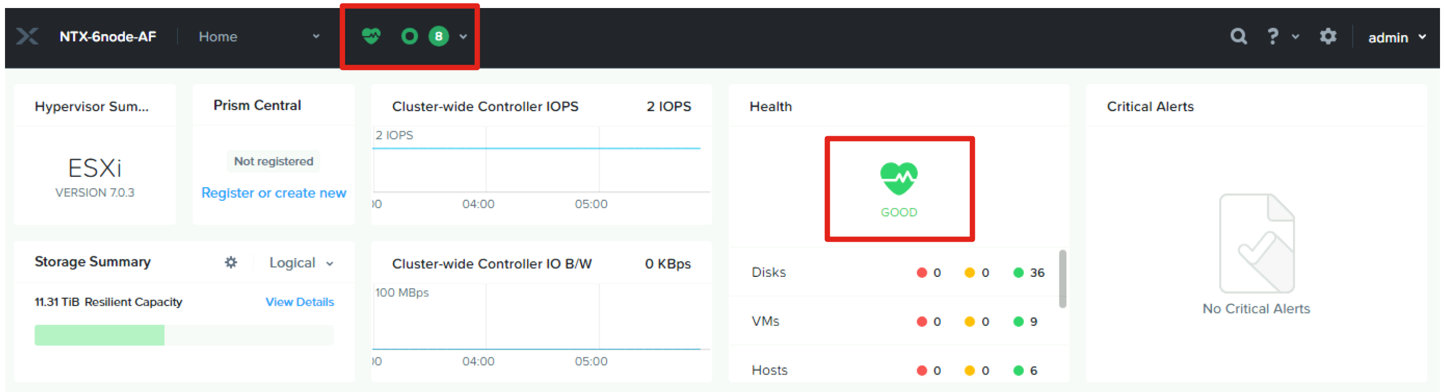
Go to Health



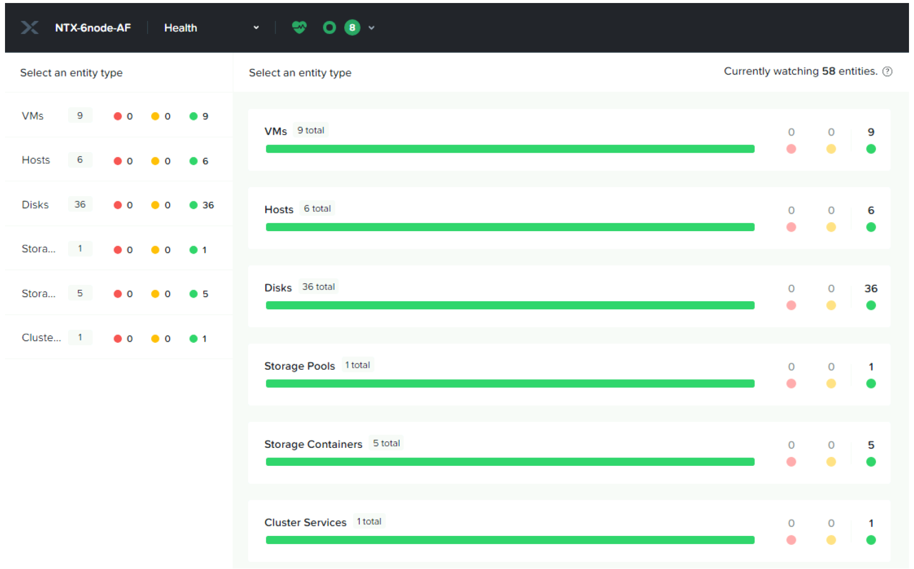
Run NCC checks



Remediate until all Alerts, Failures and Warnings are gone



Health			
Disks	0	0	36
VMs	0	0	9
Hosts	0	0	6



VMs	9	0	0	9
Hosts	6	0	0	6
Disks	36	0	0	36
Stora...	1	0	0	1
Stora...	5	0	0	5
Cluste...	1	0	0	1

VMs 9 total	0	0	9
Hosts 6 total	0	0	6
Disks 36 total	0	0	36
Storage Pools 1 total	0	0	1
Storage Containers 5 total	0	0	5
Cluster Services 1 total	0	0	1

Guest VM Networking

- Guest VM Networking for ESXi
- Guest VM Networking for AHV

Configure Guest VM Networking for ESXi

Verify or Modify Top-of-Rack Switch Configuration

Trunk ports

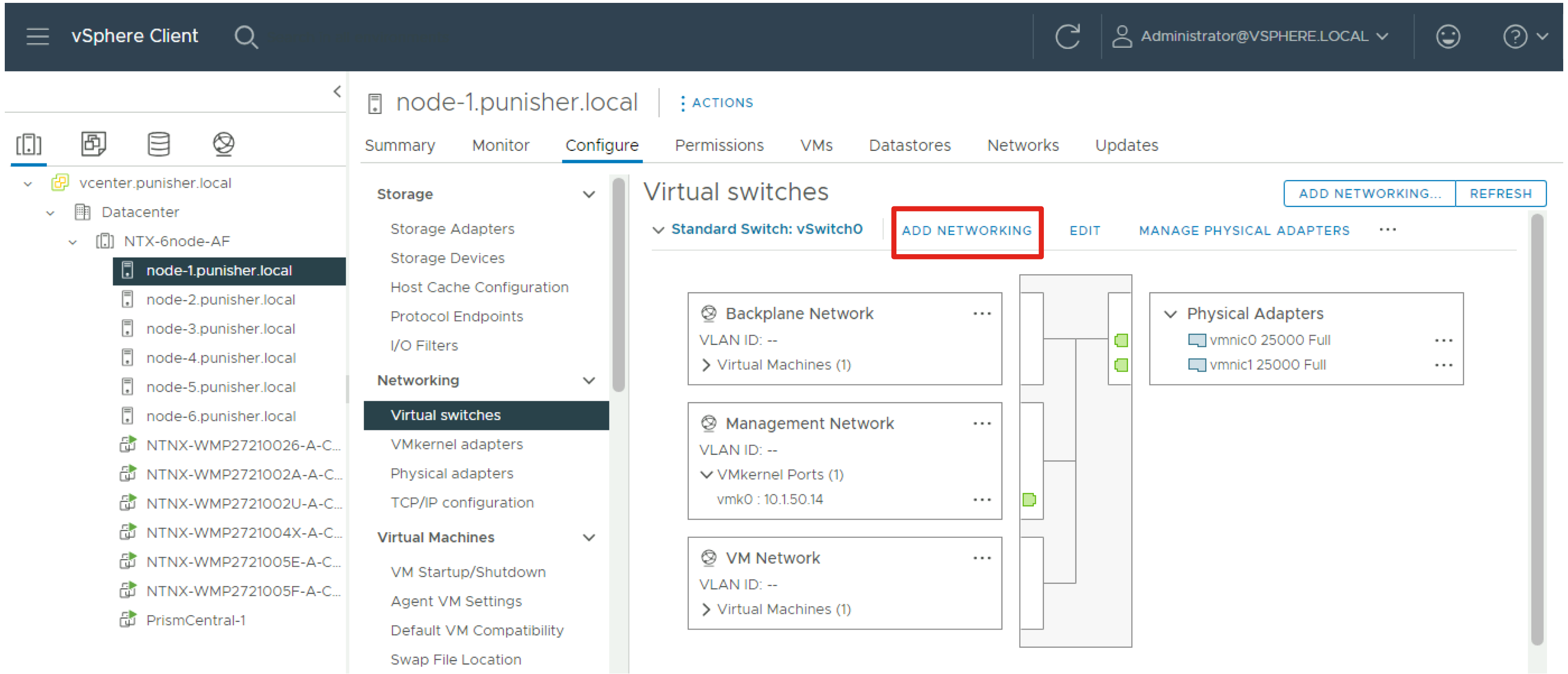
```
interface Ethernet1/6
  switchport mode trunk
  switchport trunk allowed vlan 11-13
  spanning-tree port type edge trunk
  mtu 9216
```

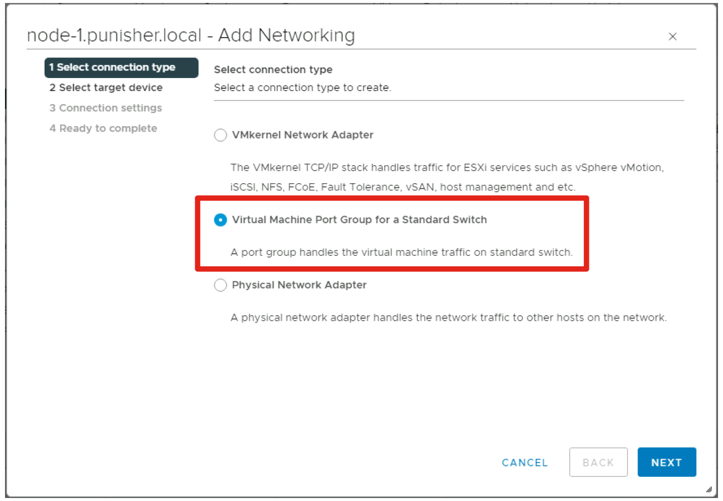
Modify trunk ports

```
NEX-93180YC-EX-1-B10# configure
Enter configuration commands, one per line. End with CNTL/Z.
NEX-93180YC-EX-1-B10(config)# interface e1/6
NEX-93180YC-EX-1-B10(config-if)# switchport trunk allowed vlan add 13
```

Verify trunk port configurations already carry the required VLAN IDs or modify them if necessary. Jumbo frames are optional and not required.

Create New Port Groups in vCenter





node-1.punisher.local - Add Networking

1 Select connection type
2 Select target device
3 Connection settings
4 Ready to complete

Select connection type

Select a connection type to create.

○ VMkernel Network Adapter

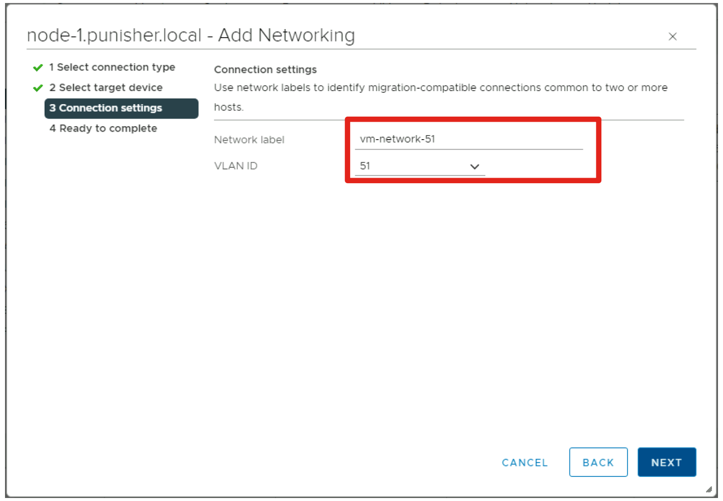
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.

● Virtual Machine Port Group for a Standard Switch

A port group handles the virtual machine traffic on standard switch.

○ Physical Network Adapter

A physical network adapter handles the network traffic to other hosts on the network.



node-1.punisher.local - Add Networking

✓ 1 Select connection type
✓ 2 Select target device
3 Connection settings
4 Ready to complete

Connection settings

Use network labels to identify migration-compatible connections common to two or more hosts.

Network label: vm-network-51

VLAN ID: 51

Add a new port group to the default vSwitch0 for the guest VMs, using VLAN ID tags. Repeat for each VLAN required and repeat for all the hosts in the vCenter cluster so their configuration matches.

Configure Guest VM Networking for AHV

Verify or Modify Top-of-Rack Switch Configuration

Trunk ports

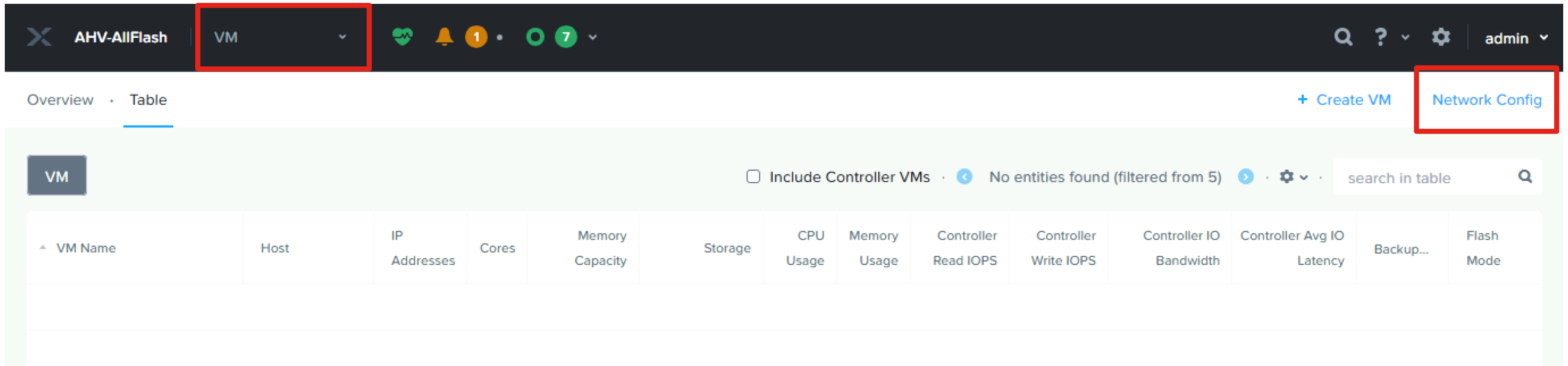
```
interface Ethernet1/6
  switchport mode trunk
  switchport trunk allowed vlan 11-13
  spanning-tree port type edge trunk
  mtu 9216
```

Modify trunk ports

```
NEX-93180YC-EX-1-B10# configure
Enter configuration commands, one per line. End with CNTL/Z.
NEX-93180YC-EX-1-B10(config)# interface e1/6
NEX-93180YC-EX-1-B10(config-if)# switchport trunk allowed vlan add 13
```

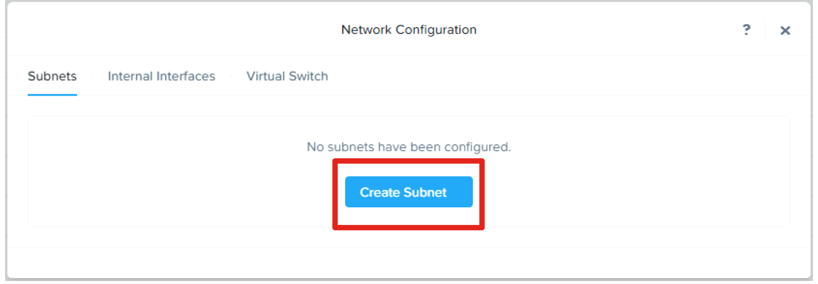
Verify trunk port configurations already carry the required VLAN IDs or modify them if necessary. Jumbo frames are optional and not required.

Create VM Subnet(s)

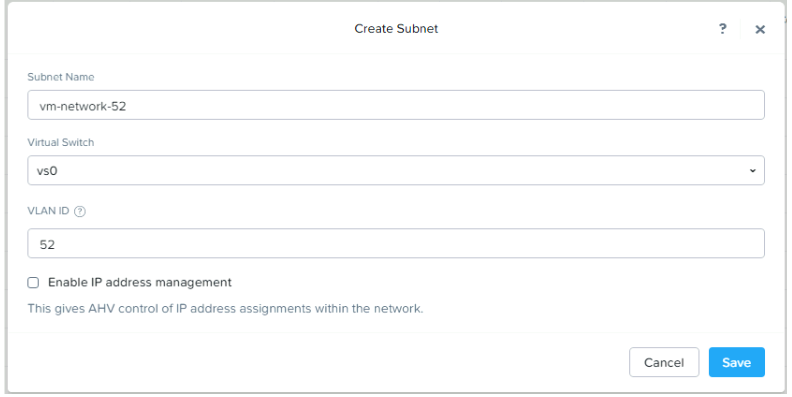


□ Include Controller VMs · No entities found (filtered from 5)

VM Name	Host	IP Addresses	Cores	Memory Capacity	Storage	CPU Usage	Memory Usage	Controller Read IOPS	Controller Write IOPS	Controller IO Bandwidth	Controller Avg IO Latency	Backup...	Flash Mode



No subnets have been configured.



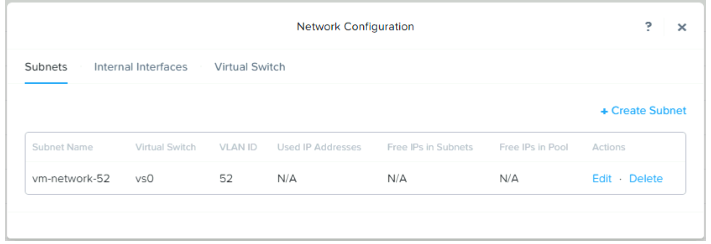
Subnet Name: vm-network-52

Virtual Switch: vs0

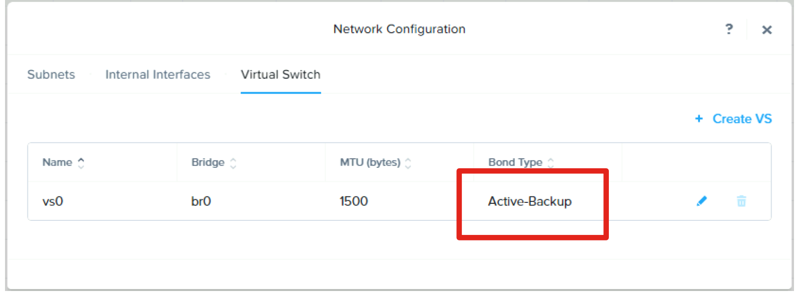
VLAN ID: 52

□ Enable IP address management

This gives AHV control of IP address assignments within the network.



Subnet Name	Virtual Switch	VLAN ID	Used IP Addresses	Free IPs in Subnets	Free IPs in Pool	Actions
vm-network-52	vs0	52	N/A	N/A	N/A	Edit · Delete

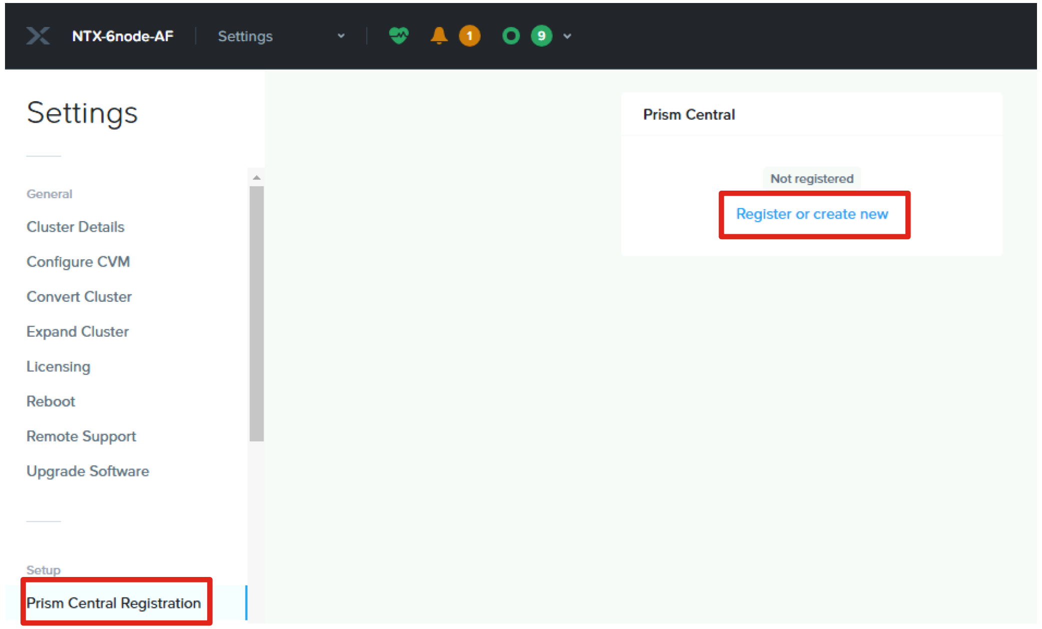


Name	Bridge	MTU (bytes)	Bond Type
vs0	br0	1500	Active-Backup

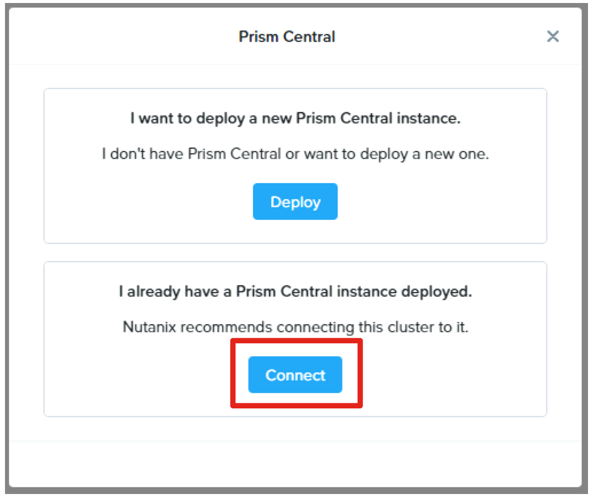
Note: Do not modify the default virtual switch bond type to Active-Active. This requires LACP and will not work within Cisco UCS domains.

Prism Central Configuration

Register Cluster with Prism Central



These instructions assume the Prism Central instance or cluster used to deploy the Nutanix cluster in standalone mode will also be the one registered for management, therefore the installation instructions from the beginning of this document will suffice.

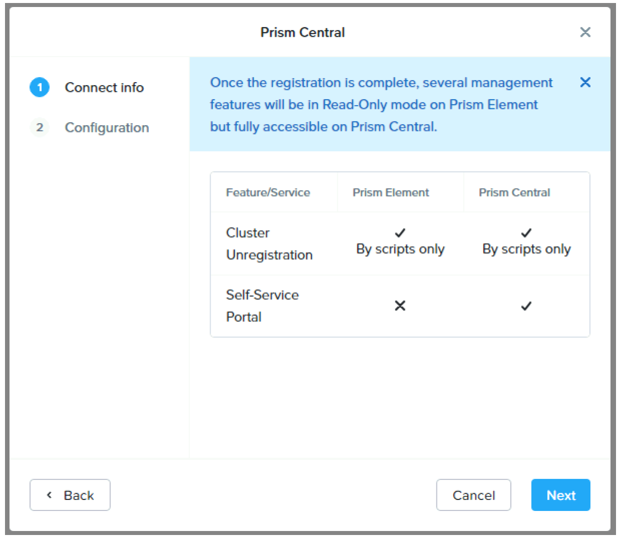


I want to deploy a new Prism Central instance.

I don't have Prism Central or want to deploy a new one.

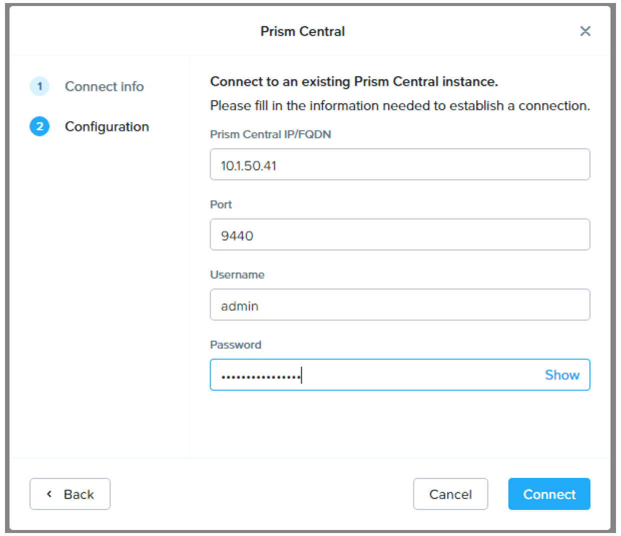
I already have a Prism Central instance deployed.

Nutanix recommends connecting this cluster to it.



Once the registration is complete, several management features will be in Read-Only mode on Prism Element but fully accessible on Prism Central.

Feature/Service	Prism Element	Prism Central
Cluster Unregistration	✓ By scripts only	✓ By scripts only
Self-Service Portal	✕	✓



Connect to an existing Prism Central instance.

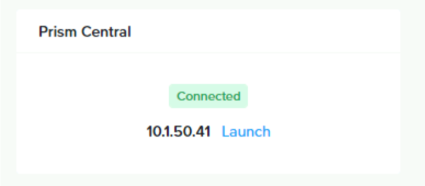
Please fill in the information needed to establish a connection.

Prism Central IP/FQDN: 10.1.50.41

Port: 9440

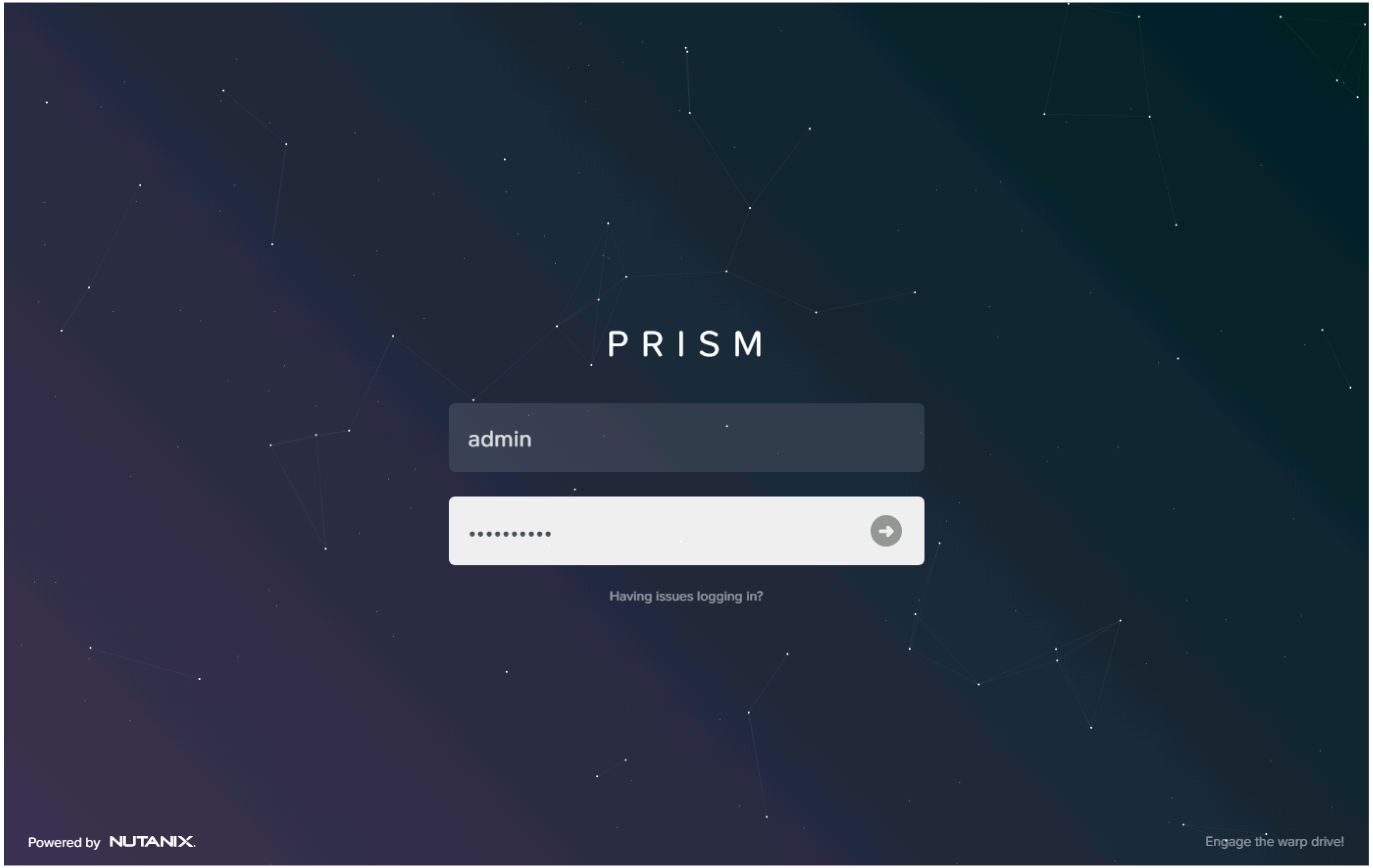
Username: admin

Password: .... Show



10.1.50.41 Launch

Access Prism Central



PRISM

admin

••••••••••

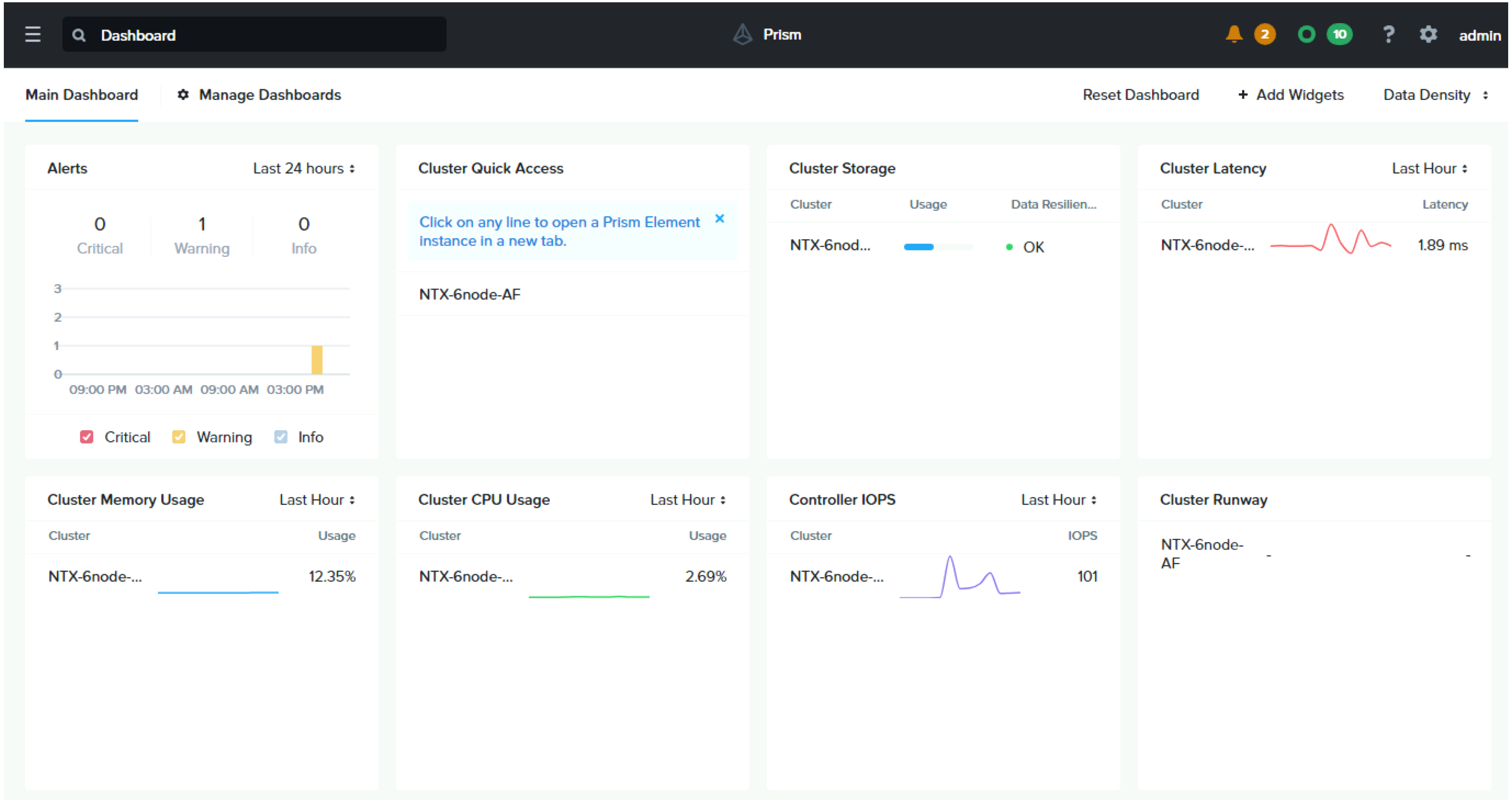
Having issues logging in?

Powered by NUTANIX

Engage the warp drive!

- Access Prism Central at the VM or cluster IP address, using HTTPS at port 9440
- Default username: admin
- Default password: Nutanix/4u
- Password must be changed on first login

Prism Central Dashboard



Dashboard

Prism

2 10 ? admin

Main Dashboard Manage Dashboards Reset Dashboard + Add Widgets Data Density

Alerts Last 24 hours

0	1	0
Critical	Warning	Info

☑ Critical ☑ Warning ☑ Info

Cluster Quick Access

Click on any line to open a Prism Element instance in a new tab. ×

NTX-6node-AF

Cluster Storage

Cluster	Usage	Data Resilien...
NTX-6nod...		● OK

Cluster Latency Last Hour

Cluster	Latency
NTX-6node-...	1.89 ms

Cluster Memory Usage Last Hour

Cluster	Usage
NTX-6node-...	12.35%

Cluster CPU Usage Last Hour

Cluster	Usage
NTX-6node-...	2.69%

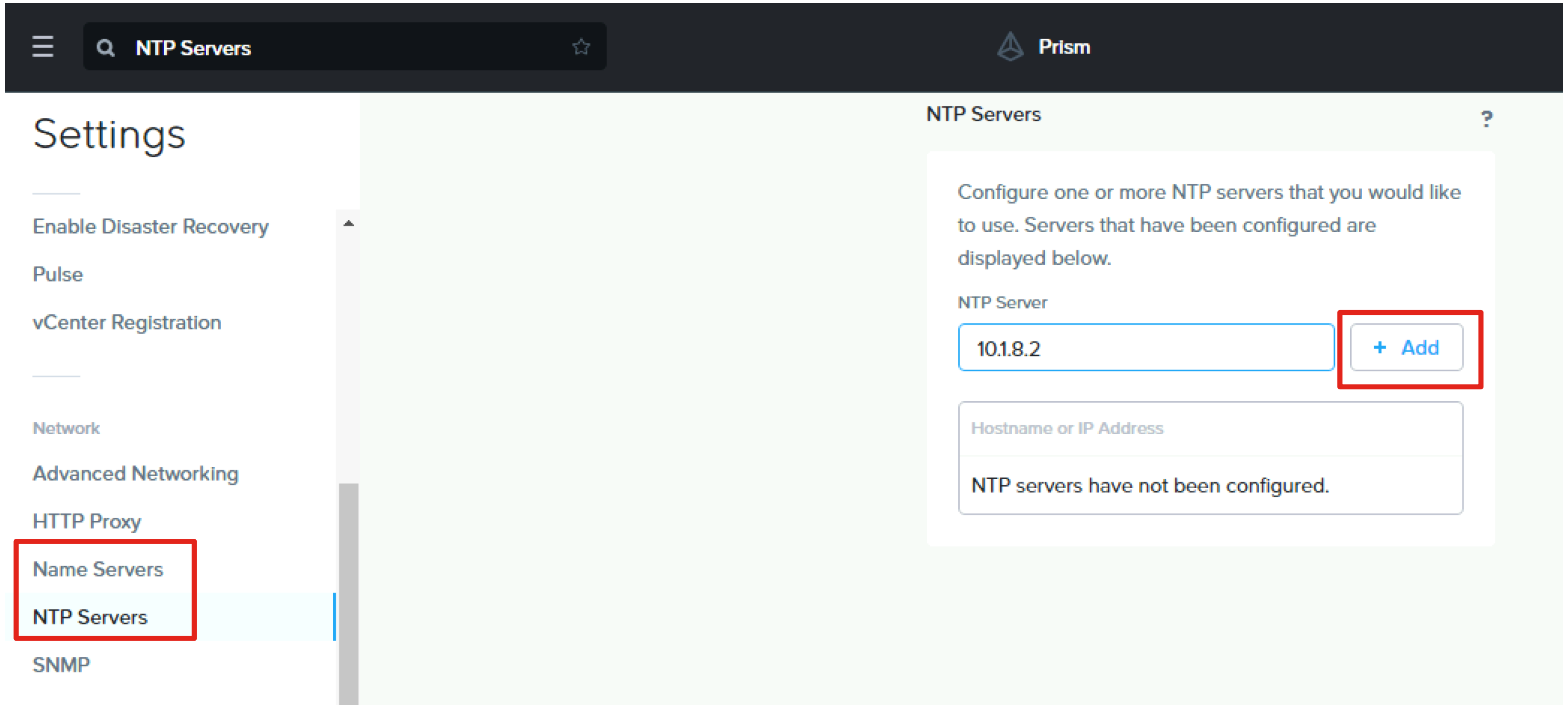
Controller IOPS Last Hour

Cluster	IOPS
NTX-6node-...	101

Cluster Runway

NTX-6node-AF - -

Verify DNS and NTP in Prism Central



Configure one or more NTP servers that you would like to use. Servers that have been configured are displayed below.

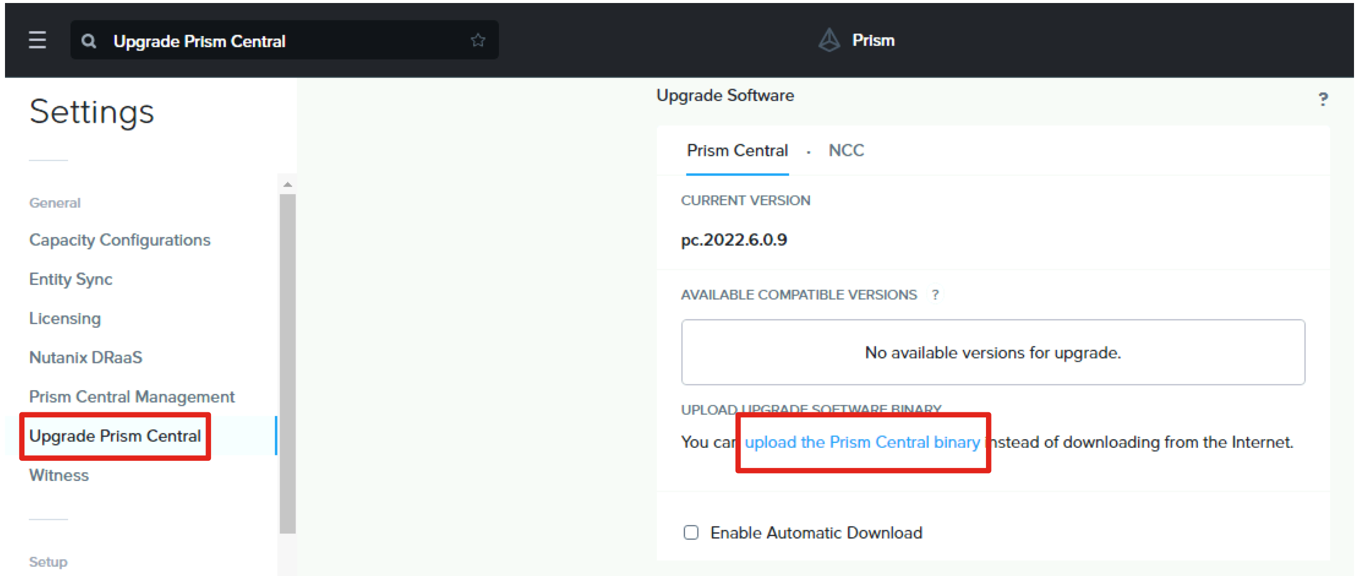
NTP Server: 10.1.8.2

+ Add

Hostname or IP Address
NTP servers have not been configured.

Prism Central cannot be upgraded without DNS and NTP configured

Prism Central Upgrade



CURRENT VERSION

pc.2022.6.0.9

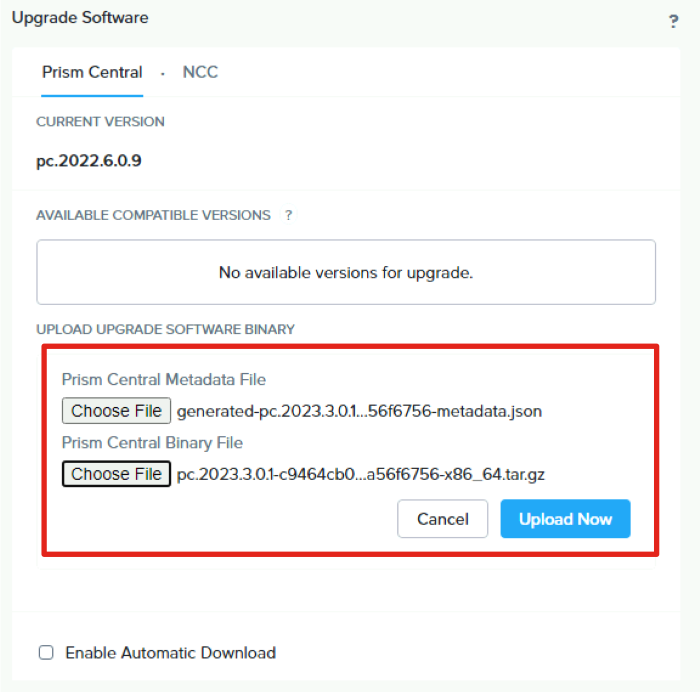
AVAILABLE COMPATIBLE VERSIONS ?

No available versions for upgrade.

UPLOAD UPGRADE SOFTWARE BINARY

You can upload the Prism Central binary instead of downloading from the Internet.

☐ Enable Automatic Download



CURRENT VERSION

pc.2022.6.0.9

AVAILABLE COMPATIBLE VERSIONS ?

No available versions for upgrade.

UPLOAD UPGRADE SOFTWARE BINARY

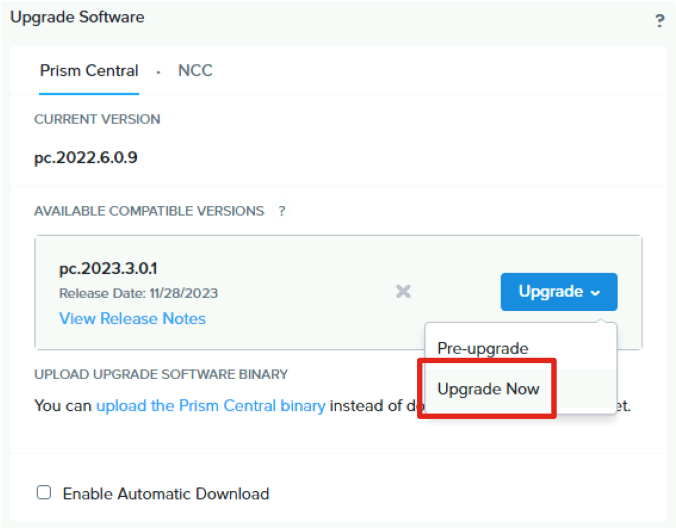
Prism Central Metadata File: generated-pc.2023.3.0.1...56f6756-metadata.json

Prism Central Binary File: pc.2023.3.0.1-c9464cb0...a56f6756-x86_64.tar.gz

☐ Enable Automatic Download

Manually upload after verifying compatibility

Verify upgrade path and compatibility here:
https://portal.nutanix.com/page/documents/upgrade-paths
and here:
https://portal.nutanix.com/page/documents/compatibility-interoperability-matrix/interoperability
Prism Central must be upgraded first to a compatible version before upgrading AOS.



CURRENT VERSION

pc.2022.6.0.9

AVAILABLE COMPATIBLE VERSIONS ?

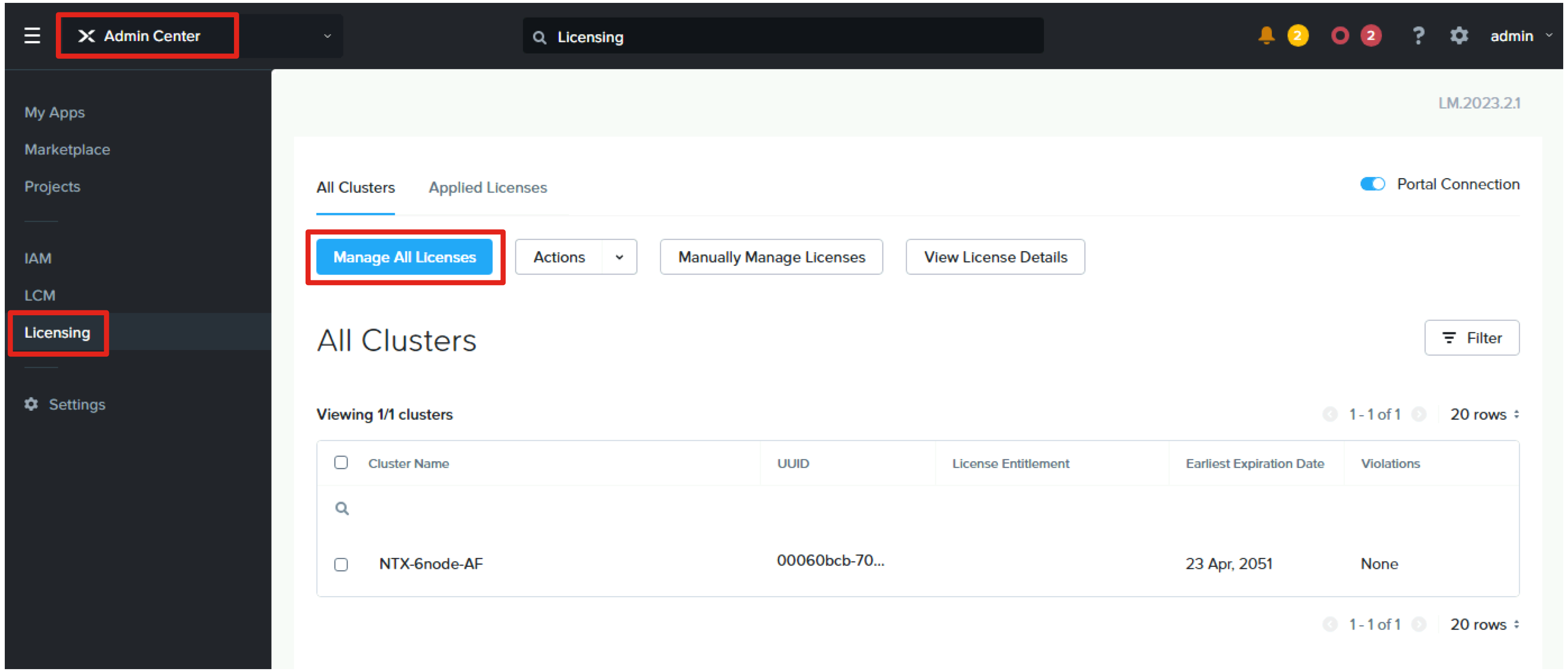
pc.2023.3.0.1
Release Date: 11/28/2023
View Release Notes

UPLOAD UPGRADE SOFTWARE BINARY

You can upload the Prism Central binary instead of d… …et.

☐ Enable Automatic Download

Configure Licensing



Viewing 1/1 clusters

□	Cluster Name	UUID	License Entitlement	Earliest Expiration Date	Violations
□	NTX-6node-AF	00060bcb-70...		23 Apr, 2051	None

Recommended method for licensing is to use Seamless Licensing via Prism Central, which requires internet access. Clicking on “Manage All Licenses” will prompt you to log in to the Nutanix support portal. Ensure you log in with a valid My Nutanix account with administrative rights and is entitled with valid licenses. Licenses can be selected and applied to the clusters in the subsequent screens. For more information on licensing, refer to this page: https://portal.nutanix.com/page/documents/details?targetId=License-Manager:License-Manager

Cluster Expansion

Cluster Expansion Status

As of the initial publication of this guide, standalone clusters cannot be expanded using Nutanix Foundation Central. The ability to expand will be added in roughly 3 months time. This guide will be updated at that time to document the expansion process.

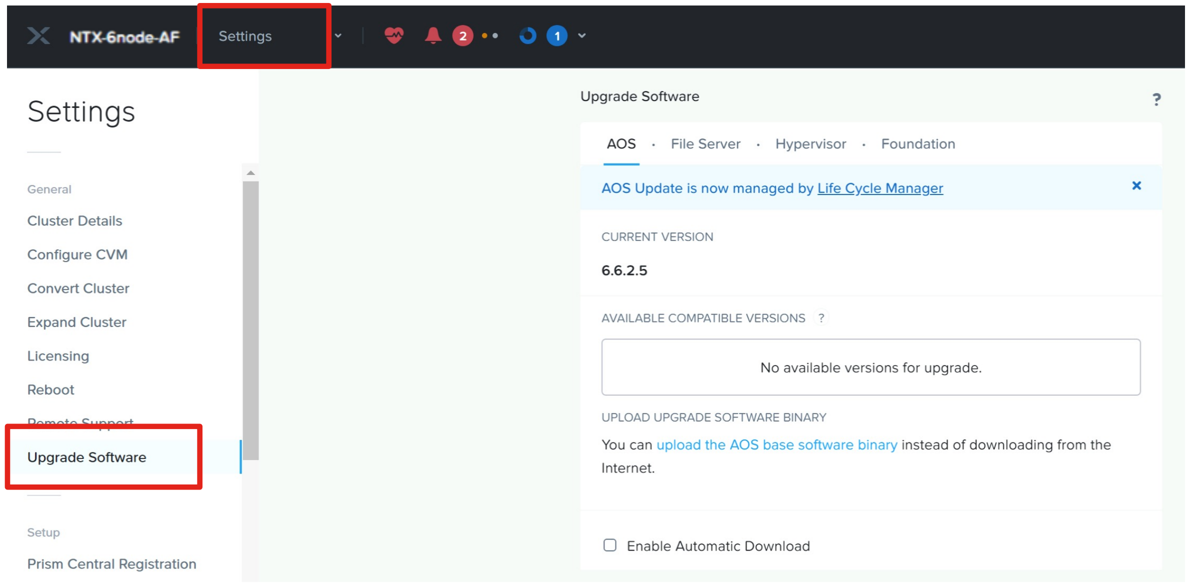
Nutanix Lifecycle Manager

Nutanix Lifecycle Manager Status

As of the initial publication of this guide, standalone clusters cannot be upgraded using Nutanix Lifecycle Manager. Nutanix Lifecycle Manager will be upgraded in roughly 2 months time to support standalone clusters managed by Cisco Intersight, including firmware upgrades. This feature will require the cluster to run AOS 6.8+. This guide will be updated at that time to document the upgrade process. In the meantime, if an upgrade to AOS is required the "Upgrade Software" feature in Prism Element can be used to perform an upgrade.

Warning: Do not run an LCM inventory job, which will attempt to upgrade LCM to the latest version. LCM version 3.0.1 will support Cisco clusters and will also require the cluster to run AOS 6.8+. If LCM is upgraded to version 3.0.1 prior to AOS being upgraded to 6.8, LCM will not be able to upgrade Cisco server firmware. In this scenario, LCM will need to be used to upgrade AOS to version 6.8, before the ability to upgrade Cisco server firmware can be used.

Do Not Use LCM, Only Use Upgrade Software For Now



Settings

General

- Cluster Details
- Configure CVM
- Convert Cluster
- Expand Cluster
- Licensing
- Reboot
- Remote Support
- Upgrade Software

Setup

- Prism Central Registration

Upgrade Software ?

AOS · File Server · Hypervisor · Foundation

AOS Update is now managed by Life Cycle Manager ×

CURRENT VERSION

6.6.2.5

AVAILABLE COMPATIBLE VERSIONS ?

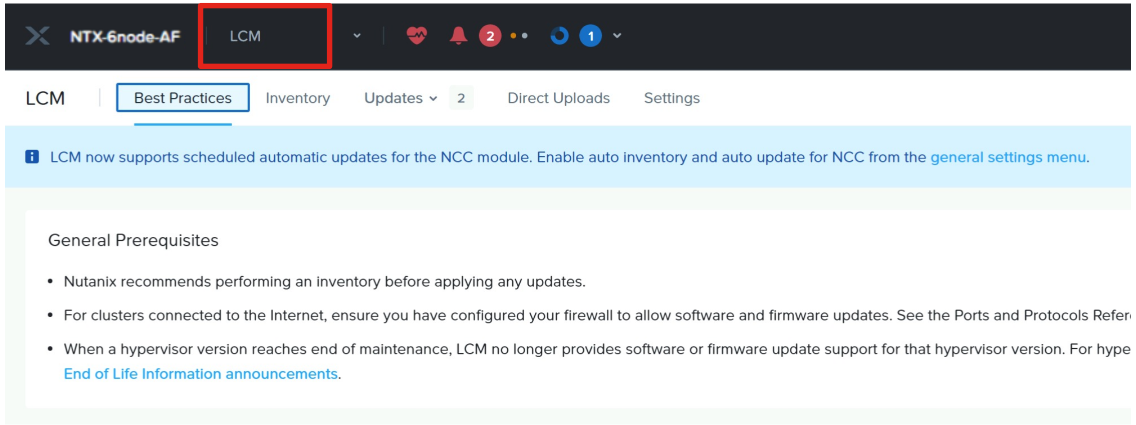
No available versions for upgrade.

UPLOAD UPGRADE SOFTWARE BINARY

You can upload the AOS base software binary instead of downloading from the Internet.

☐ Enable Automatic Download

✓



LCM | Best Practices | Inventory | Updates 2 | Direct Uploads | Settings

LCM now supports scheduled automatic updates for the NCC module. Enable auto inventory and auto update for NCC from the general settings menu.

General Prerequisites

- Nutanix recommends performing an inventory before applying any updates.
- For clusters connected to the Internet, ensure you have configured your firewall to allow software and firmware updates. See the Ports and Protocols Refer
- When a hypervisor version reaches end of maintenance, LCM no longer provides software or firmware update support for that hypervisor version. For hype End of Life Information announcements.

✗

CISCO

The bridge to possible