Cisco Compute Hyperconverged with Nutanix

Installation, Configuration, Expansion and Lifecycle Manager 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-field-guide/ta-p/4982563

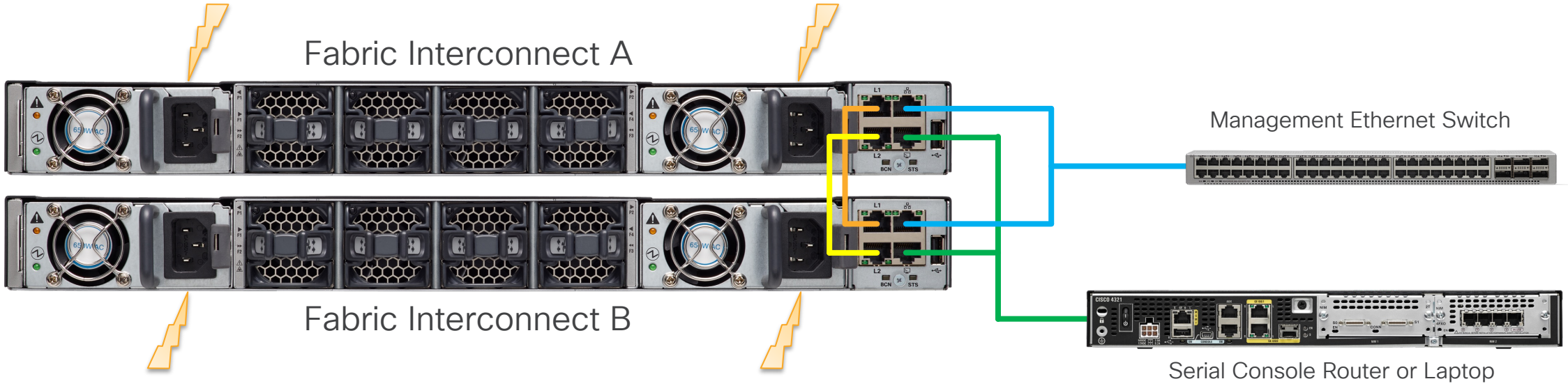
Revision History

Version	Date	Foundation VM version	Foundation Central version	AOS LTS version	AOS STS version	LCM Version	Notes
1.0	Dec 2023	5.5	N/A	6.5.4.5	6.7.1	2.7	Initial Release for FI based deployments with M6 generation servers.

Contents

Cisco UCS Configuration

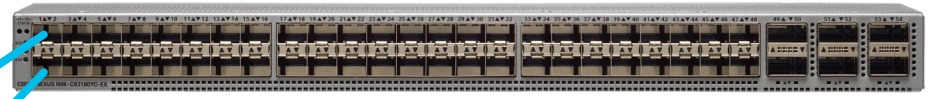
Cisco Fabric Interconnect Physical Installation



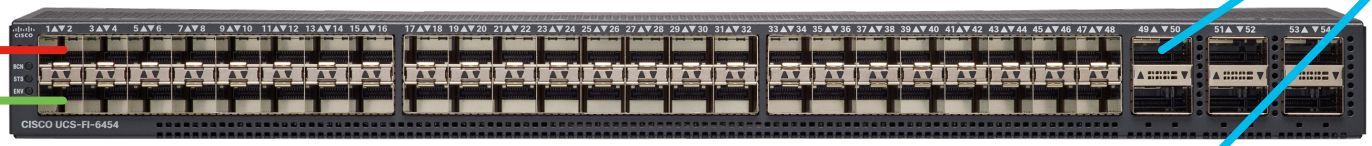
Note: L1 connects to L1, and L2 connects to L2

Cisco Fabric Interconnect and Server Cabling

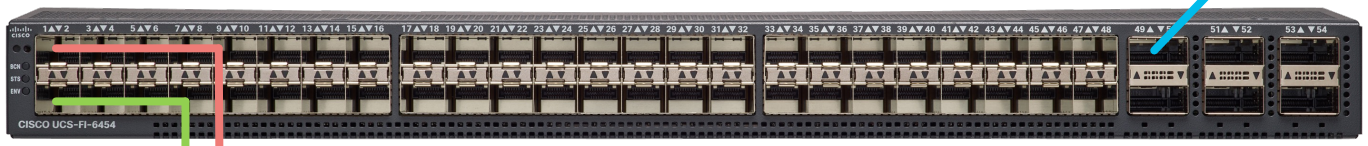
FI uplinks require 10Gb
ethernet minimum end-to-end



Uplink Switch(es)



Fabric Interconnect A



Fabric Interconnect B

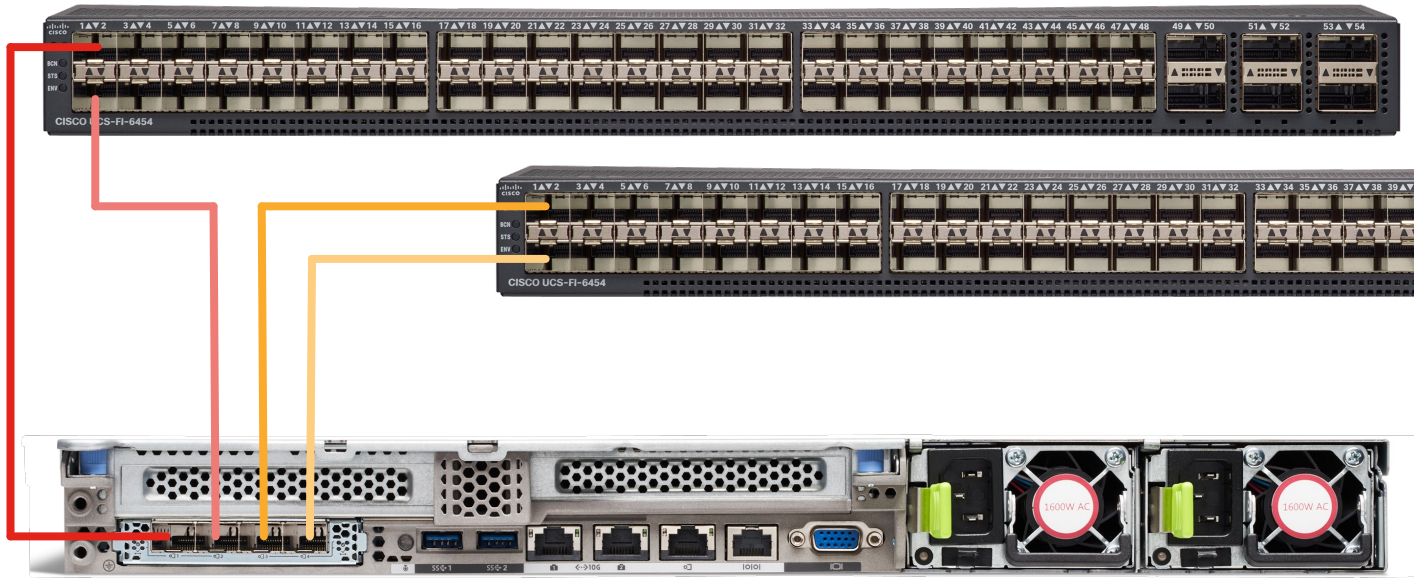
Server 1

Server 2

Continue

Note: When using 2 ports per server, use ports 1 and 3. Port 1 to FI-A, Port 3 to FI-B. Repeat this pattern for all servers.

Alternate Server Cabling - 4 cable method



Fabric Interconnect A

Fabric Interconnect B

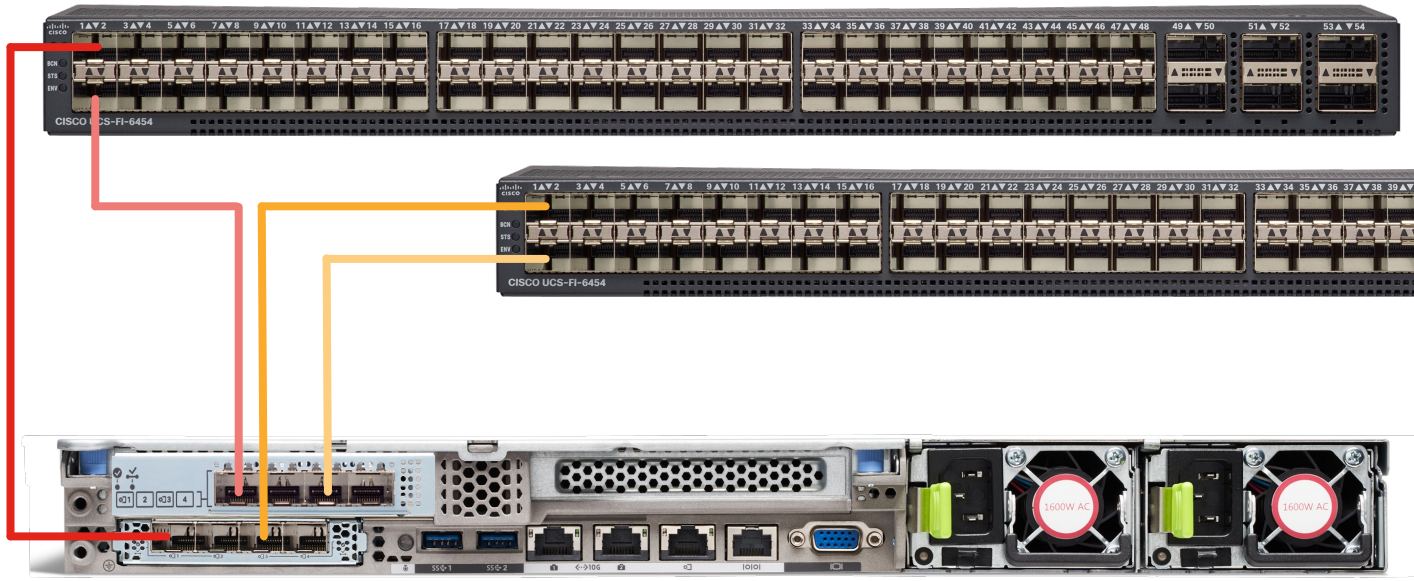
Server 1

Server 2

Continue

Note: When using 4 ports per server, use ports 1 and 2 to FI-A, ports 3 and 4 to FI-B. Repeat this pattern for all servers.

Alternate Server Cabling – Dual VIC



Fabric Interconnect A

Fabric Interconnect B

Server 1

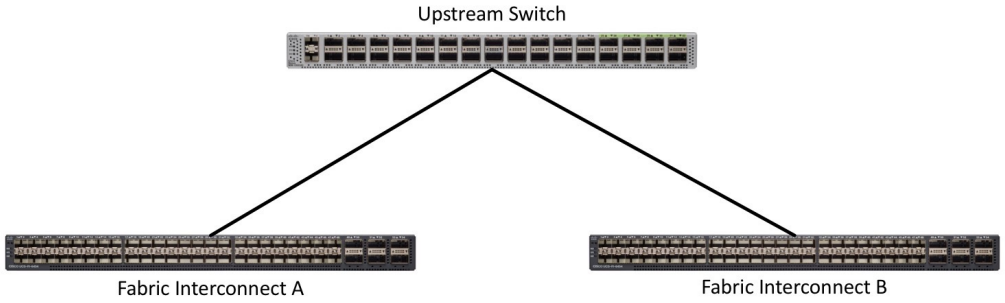
Server 2

Continue

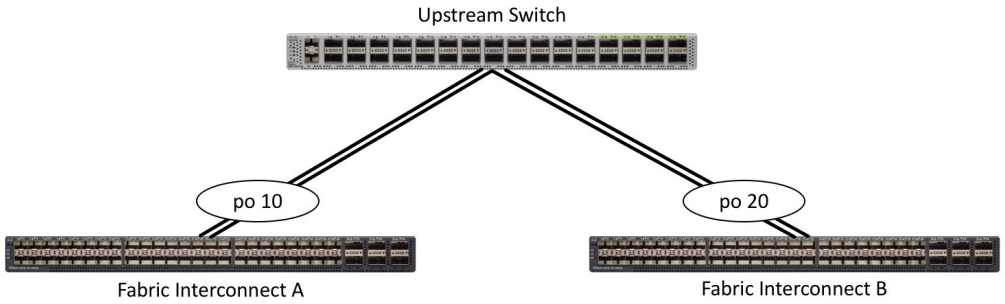
Note: When using 4 ports in a dual VIC config per server, use port 1 from each VIC to FI-A and port 3 from each VIC to FI-B. Repeat this pattern for all servers.

Fabric Interconnect Uplink Options

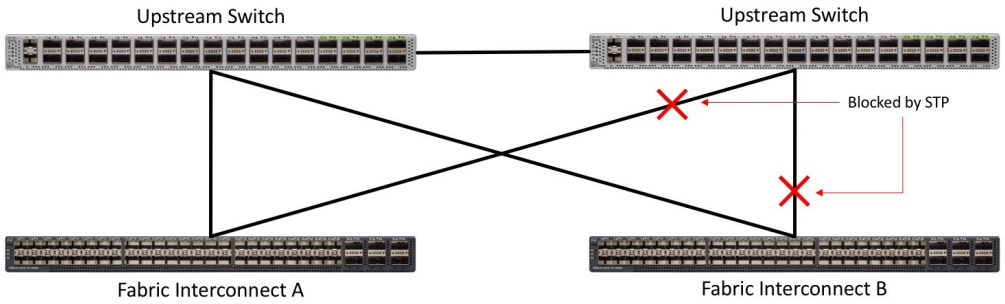
Single Switch



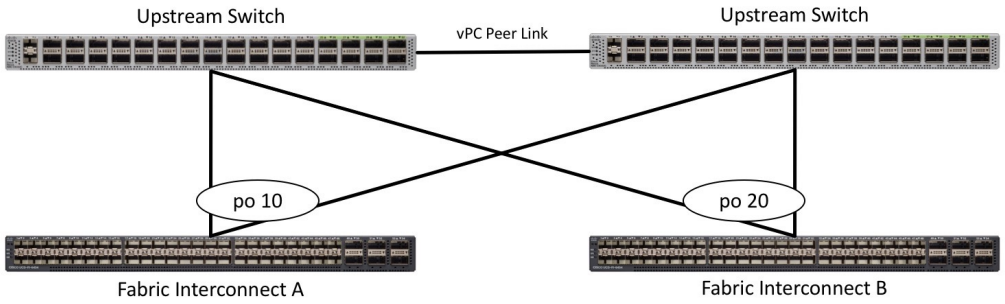
Single Switch with Port Channels



Dual Switch without Port Channels



Dual Switch with vPC



Note: For maximum flexibility, configure ports on the uplink switches for jumbo frames when possible

Initial UCS Configuration – Fabric Interconnect A

- Connect to FI-A via a serial console router or directly with a serial cable/adapter
- Configure FI-A via the CLI with the values for your UCS domain
- 3 IP addresses are required, one per FI and one for the cluster
- Choose UCSM management mode

```
---- Basic System Configuration Dialog ----

 This setup utility will guide you through the basic configuration of
 the system. Only minimal configuration including IP connectivity to
 the Fabric interconnect and its clustering mode is performed through these steps.

 Type Ctrl-C at any time to abort configuration and reboot system.
 To back track or make modifications to already entered values,
 complete input till end of section and answer no when prompted
 to apply configuration.


 Enter the configuration method. (console/gui) ? console

 Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup

 You have chosen to setup a new Fabric interconnect. Continue? (y/n): y

 Enter the management mode. (ucsm/intersight)? ucsm

 The Fabric interconnect will be configured in the ucsm managed mode. Choose (y/n)
 to proceed: y

 Enforce strong password? (y/n) [y]: y

 Enter the password for "admin":
 Confirm the password for "admin":
```

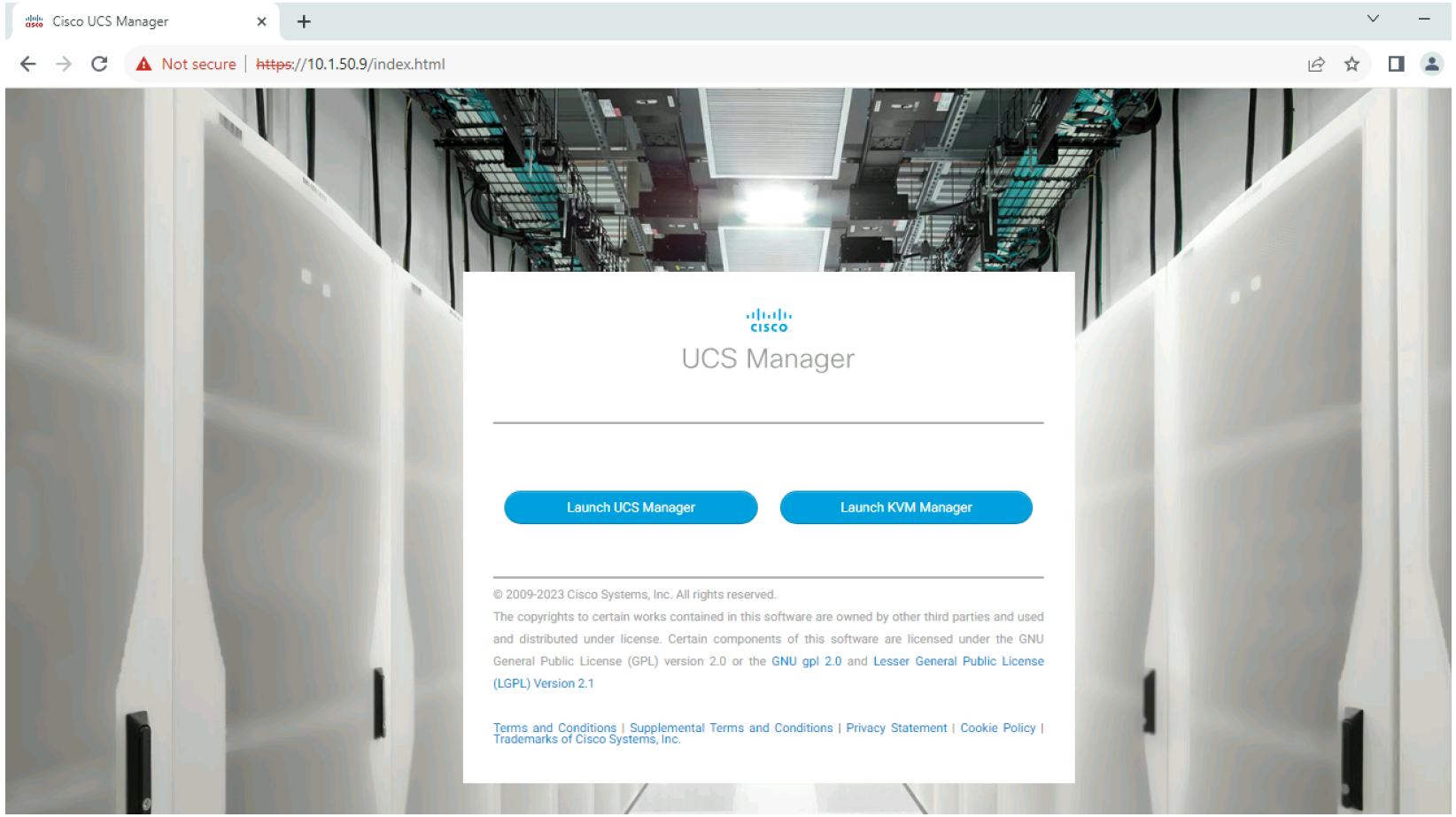
```
  Is this Fabric interconnect part of a cluster(select 'no' for standalone)? (yes/no) [n]: yes

    Enter the switch fabric (A/B) []: A

    Enter the system name:  Nutanix1-FI

    Physical Switch Mgmt0 IP address : 10.1.50.7

    Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0

    IPv4 address of the default gateway : 10.1.50.1

    Cluster IPv4 address : 10.1.50.9

    Configure the DNS Server IP address? (yes/no) [n]: yes

      DNS IP address : 10.1.50.10

  Configure the default domain name? (yes/no) [n]: yes

      Default domain name : punisher.local

    Join centralized management environment (UCS Central)? (yes/no) [n]: no

    Following configurations will be applied:

      Management Mode: ucsm
      Switch Fabric=A
      System Name=Nutanix1-FI
      Enforced Strong Password=no
      Physical Switch Mgmt0 IP Address=10.1.50.7
      Physical Switch Mgmt0 IP Netmask=255.255.255.0
      Default Gateway=10.1.50.1
      Ipv6 value=0
      DNS Server=10.1.50.10
      Domain Name=punisher.local

      Cluster Enabled=yes
      Cluster IP Address=10.29.133.106
      NOTE: Cluster IP will be configured only after both Fabric Interconnects are initialized

    Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
    Applying configuration. Please wait.

    Configuration file - Ok
```

Initial UCS Configuration – Fabric Interconnect B

- Connect to FI-B via a serial console router or directly with a serial cable/adapter
- Configure FI-B via the CLI with the values for your UCS domain
- Verify you can log into both FIs as admin using the password you provided

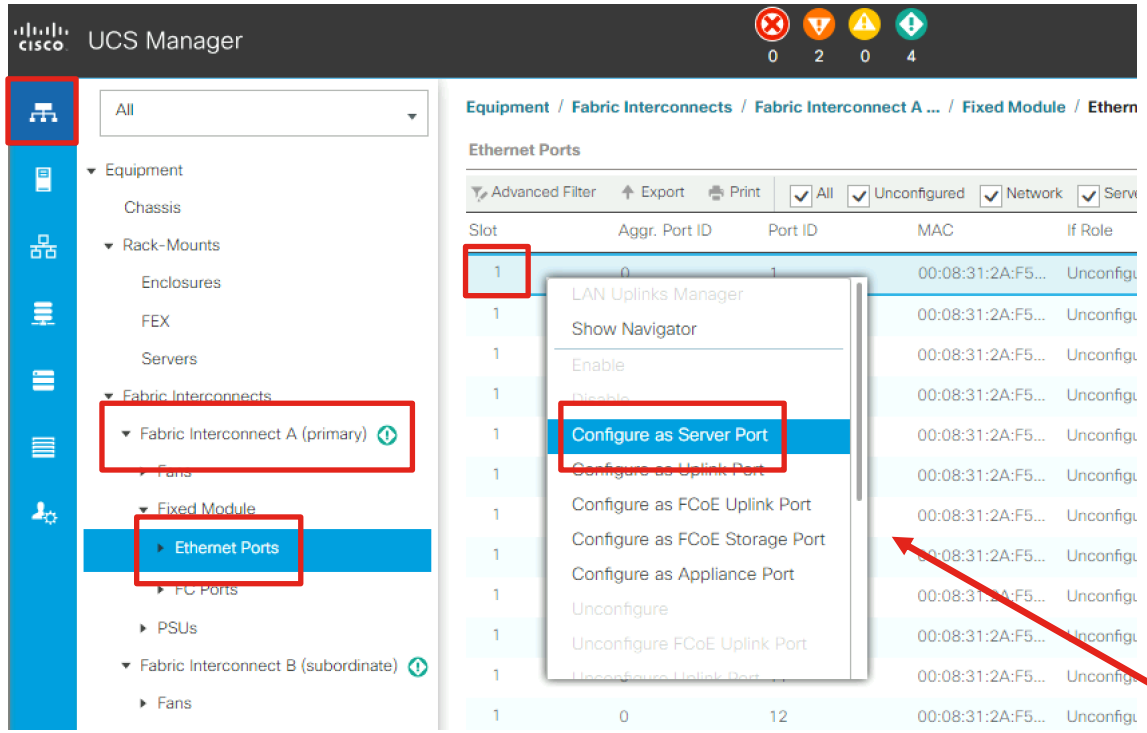
```
 ---- Basic System Configuration Dialog ----

  This setup utility will guide you through the basic configuration of
  the system. Only minimal configuration including IP connectivity to
  the Fabric interconnect and its clustering mode is performed through these steps.

  Type Ctrl-C at any time to abort configuration and reboot system.
  To back track or make modifications to already entered values,
  complete input till end of section and answer no when prompted
  to apply configuration.


  Enter the configuration method. (console/gui) ? console

  Installer has detected the presence of a peer Fabric interconnect. This Fabric
interconnect will be added to the cluster. Continue (y/n) ? y

  Enter the admin password of the peer Fabric interconnect:
    Connecting to peer Fabric interconnect... done
    Retrieving config from peer Fabric interconnect... done
    Peer Fabric interconnect Mgmt0 IPv4 Address: 10.1.50.7
    Peer Fabric interconnect Mgmt0 IPv4 Netmask: 255.255.255.0
    Cluster IPv4 address          : 10.1.50.9

    Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4
Address

  Physical Switch Mgmt0 IP address : 10.1.50.8


  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
  Applying configuration. Please wait.

Configuration file - Ok
```

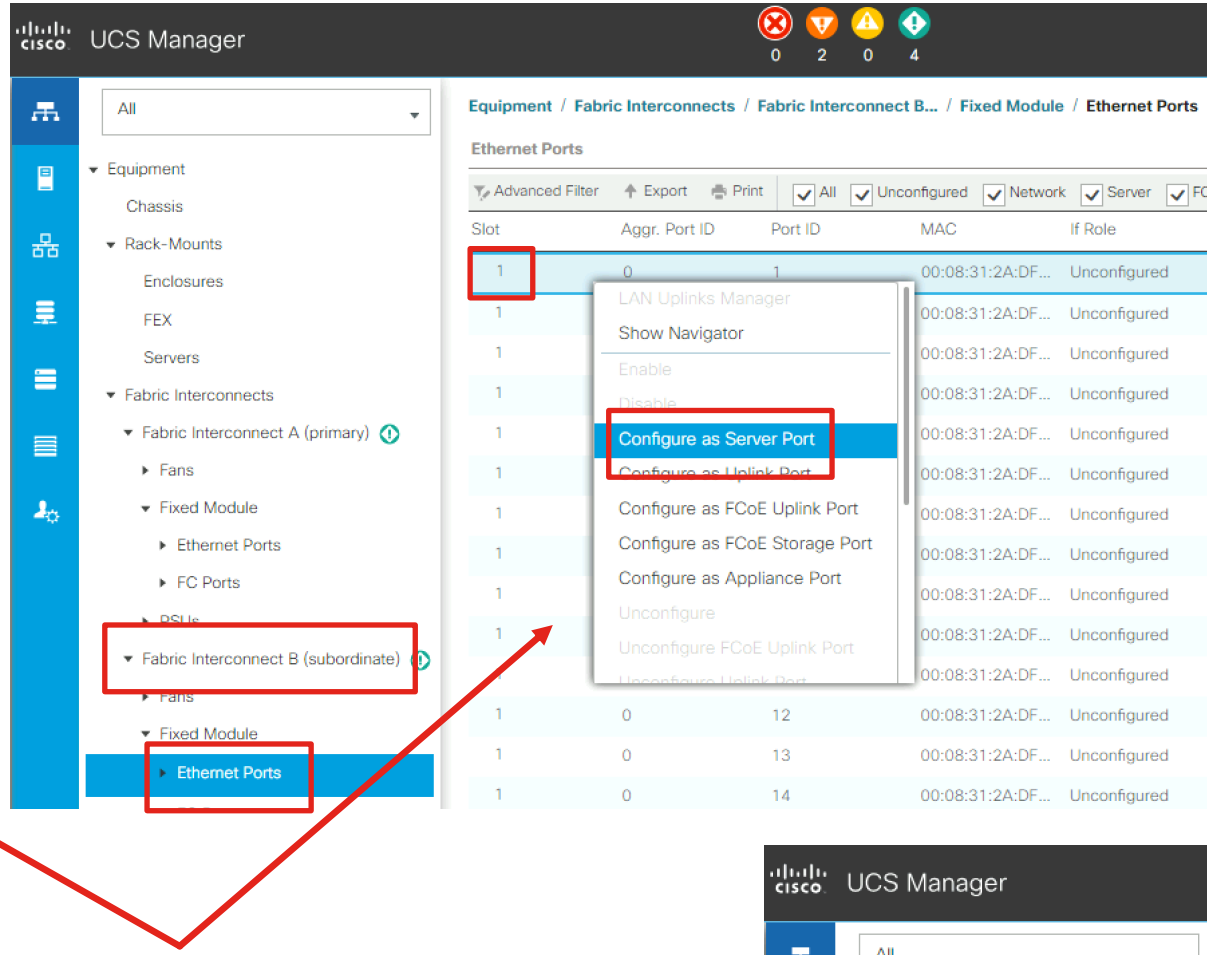
Log in to Cisco UCS Manager

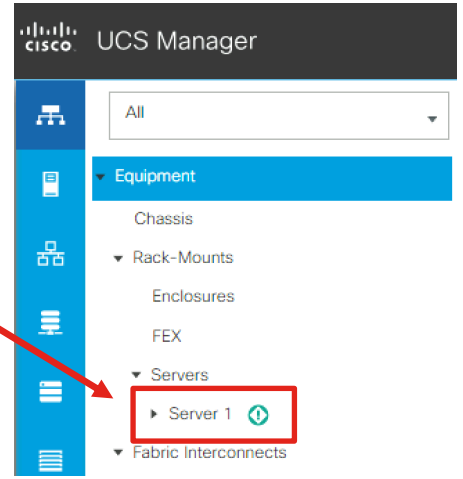


Connect to the roaming cluster IP address, not an individual FI's IP address

Enable Server Ports







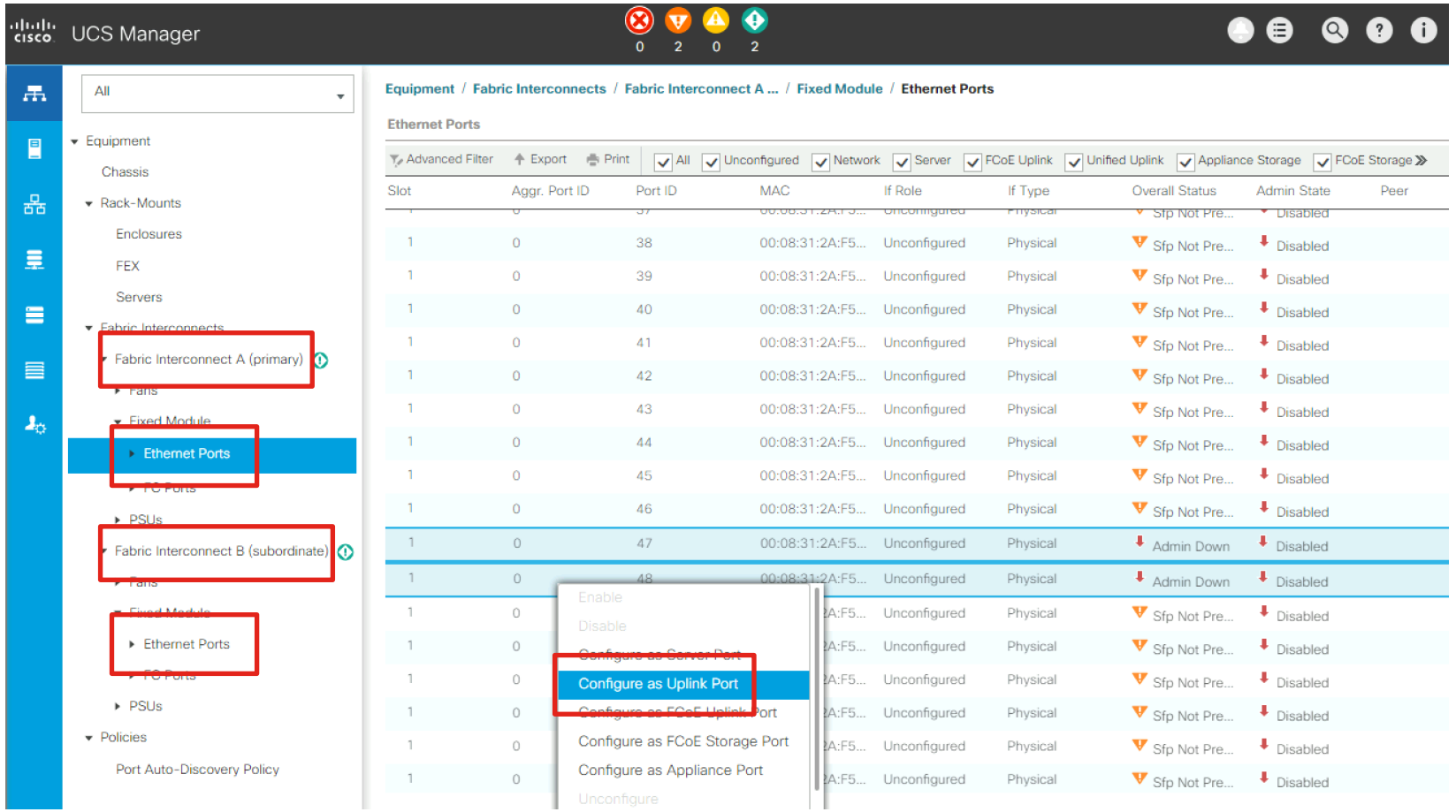
Configure the first ports on FI-A and FI-B which are connected to the first server as server ports.

Wait for the first server to appear in the inventory.

Configure the second Server ports on FI-A and FI-B and wait for it to appear.

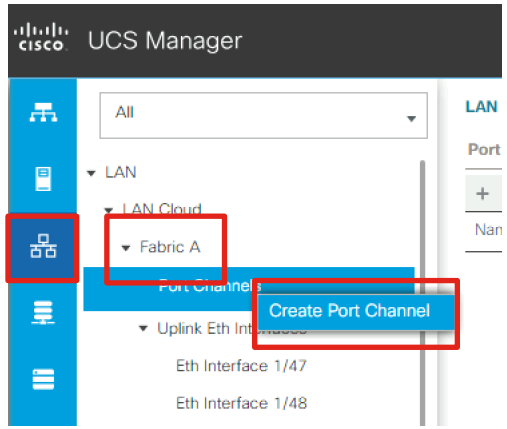
Repeat this pattern until all servers have appeared in the inventory.

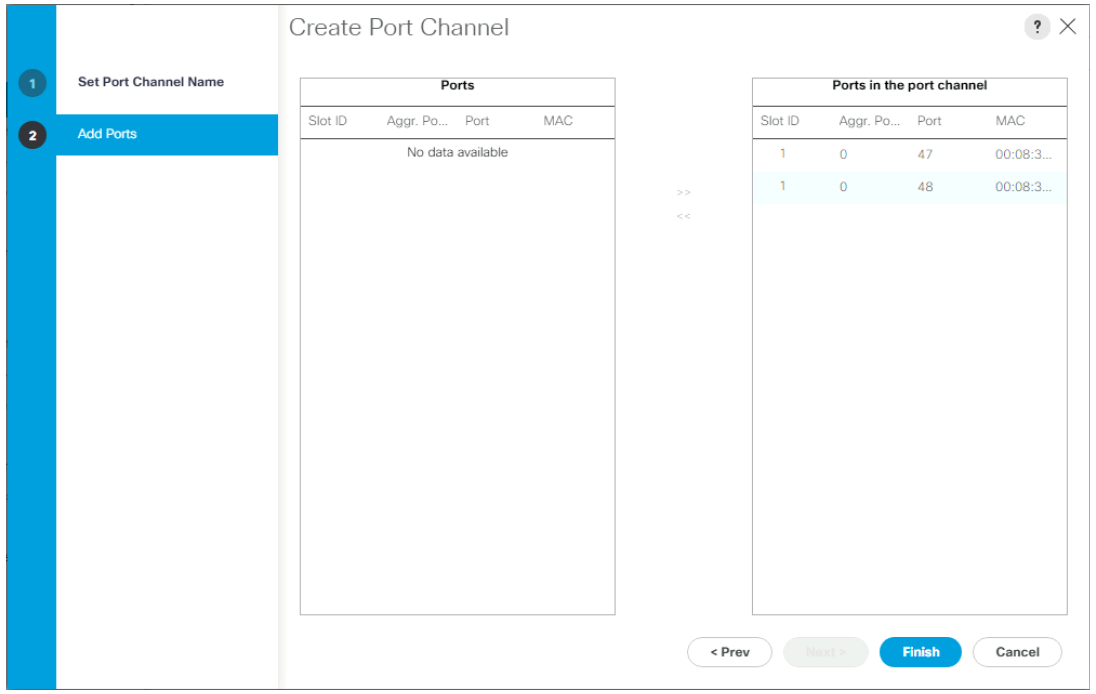
Enable Uplink Ports

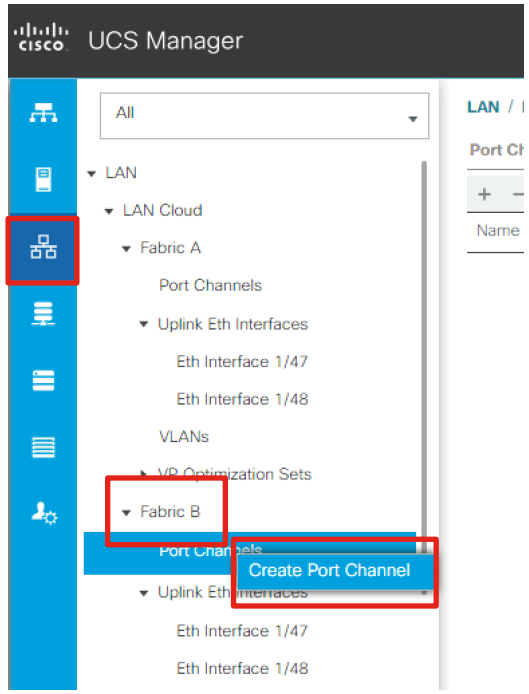


Configure the uplink ports for both FI-A and FI-B

Create Uplink Port Channels (optional)

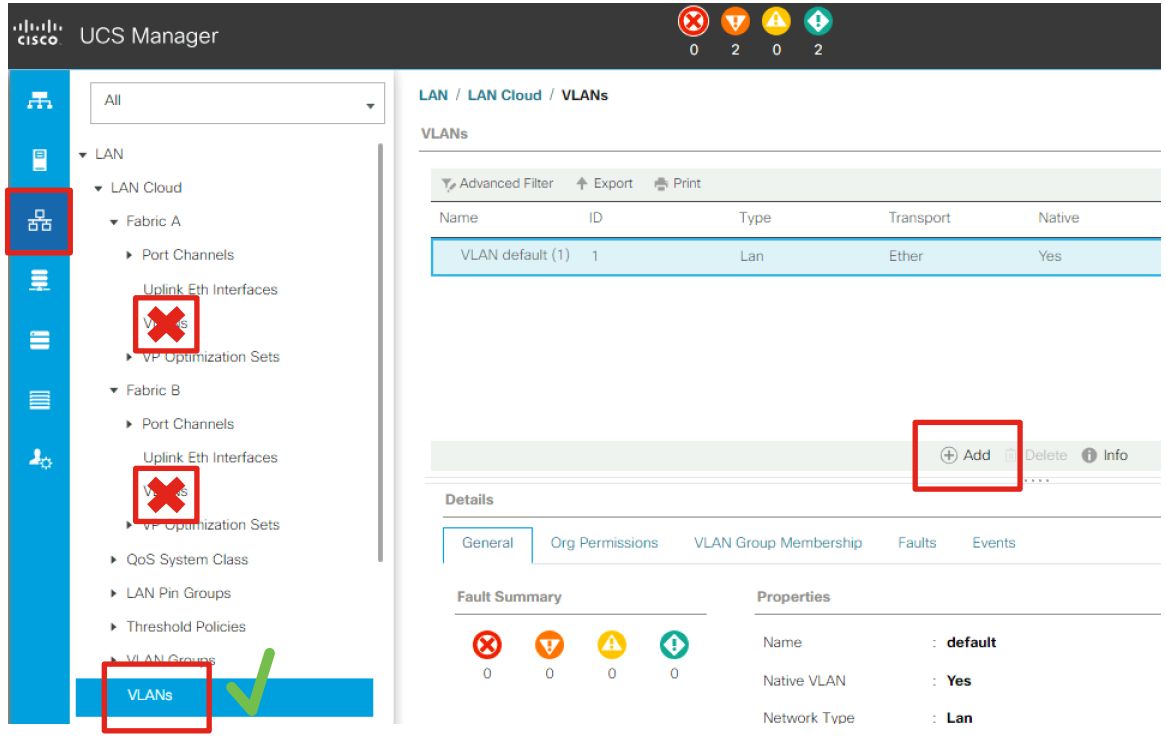


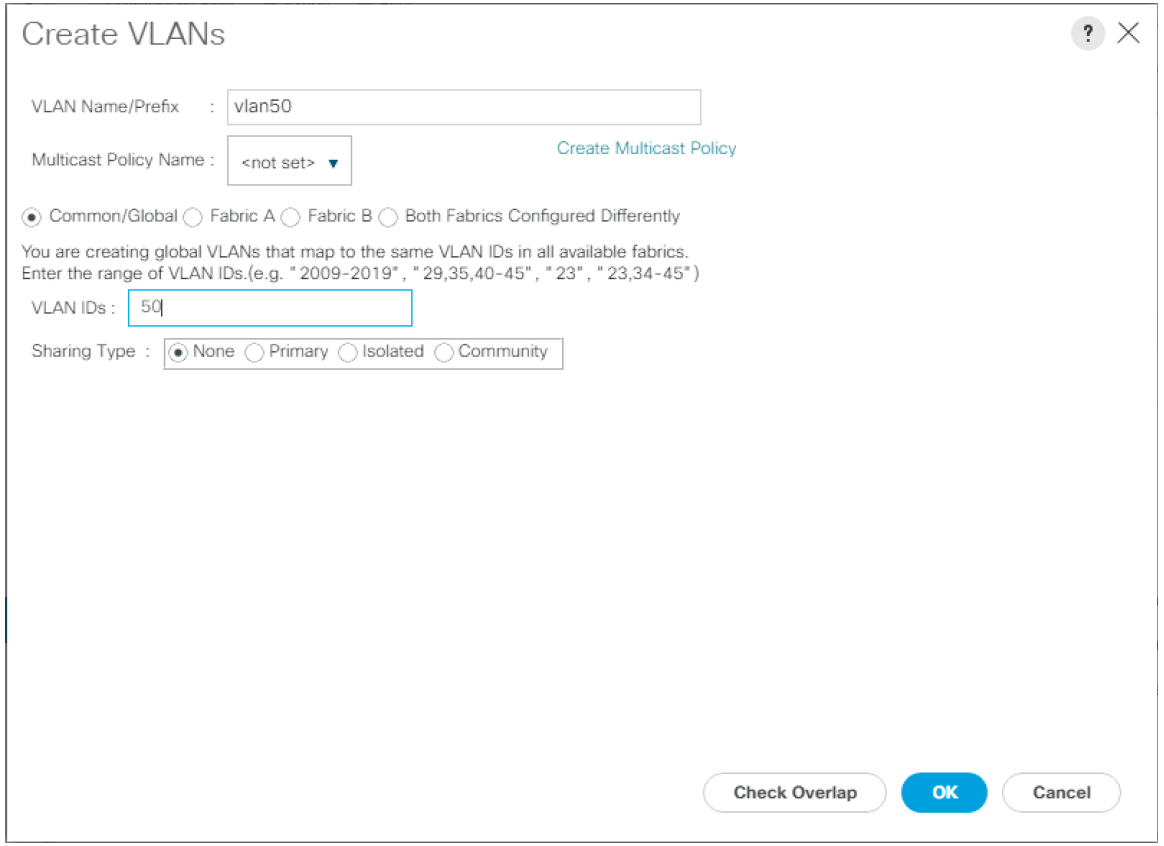




If using port-channels from the FIs to the uplink switches, create the port channels for FI-A and FI-B, adding the uplink ports that were enabled earlier.

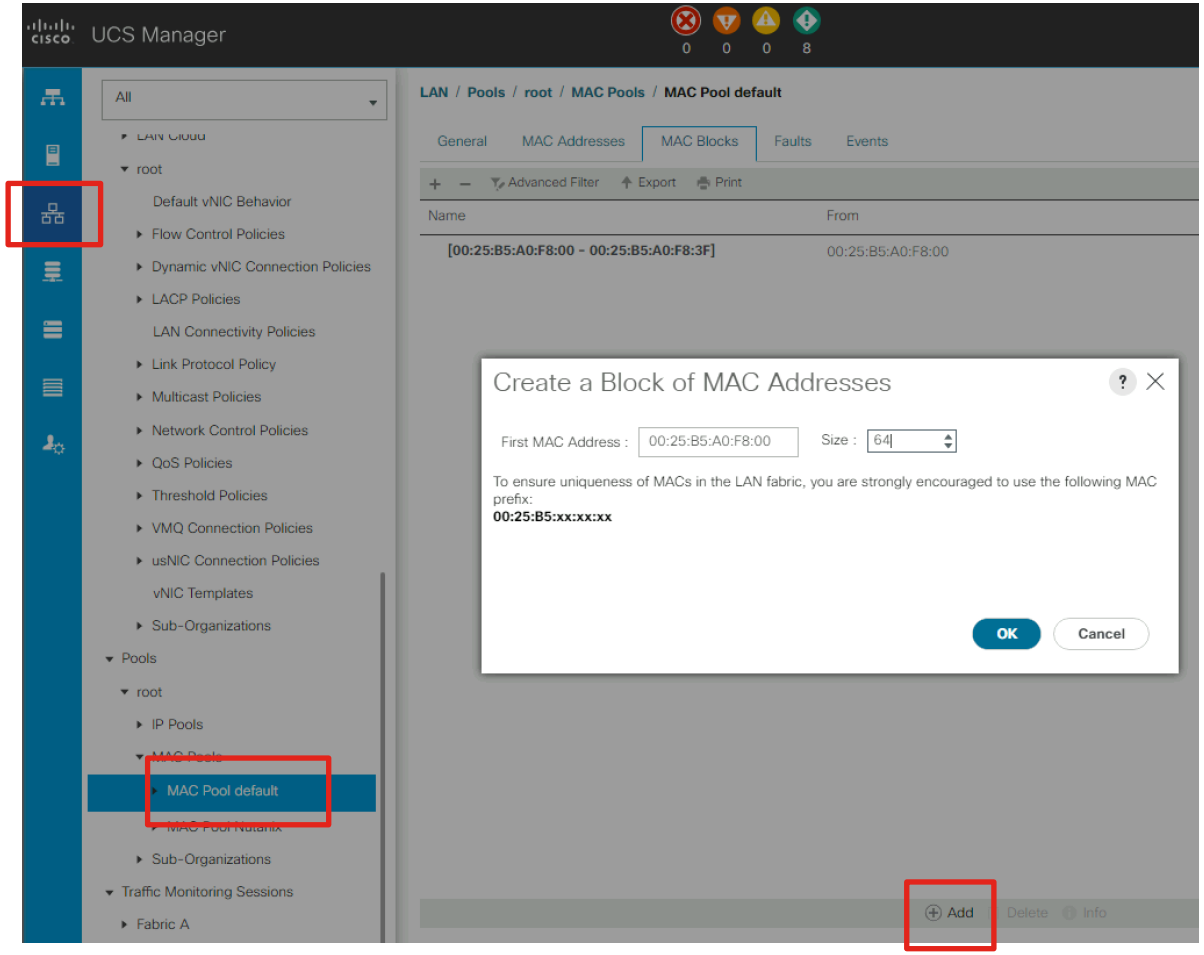
Create UCS VLANs





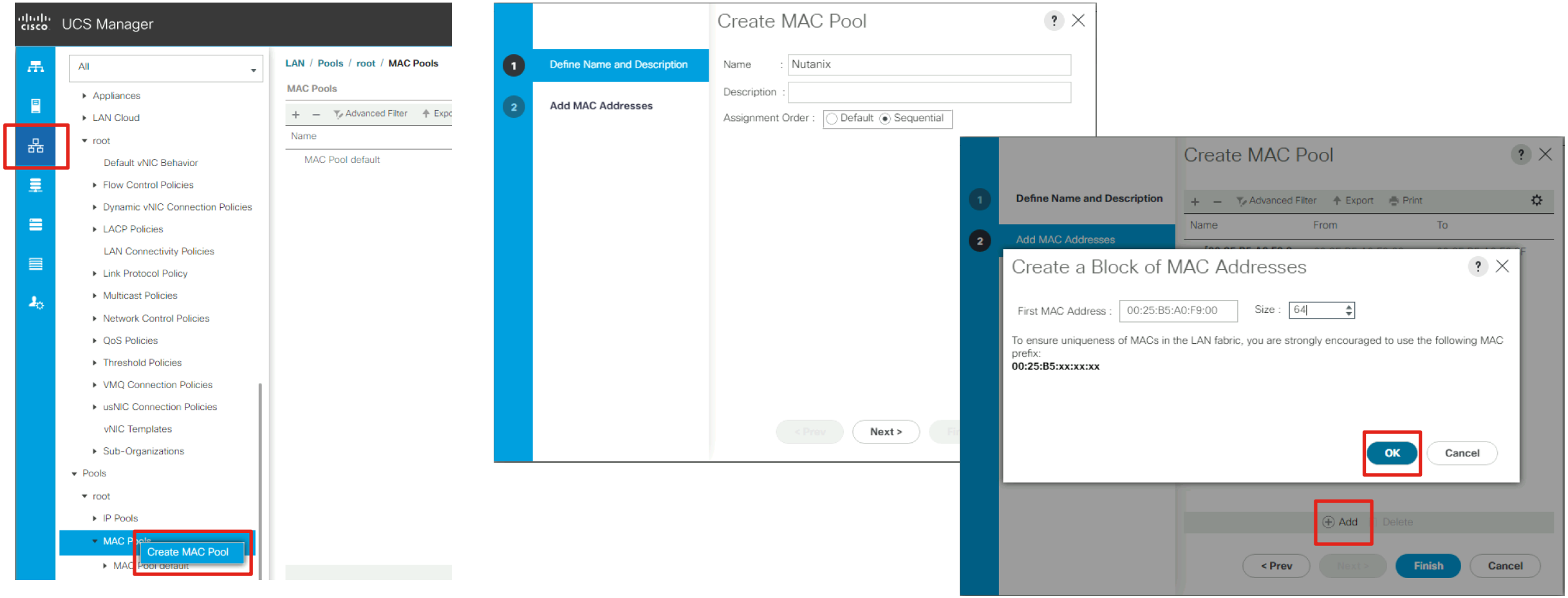
Create the VLANs needed in UCS Manager, for example the VLAN for Nutanix cluster CVMs and ESXi/AHV host management, and VLANs for the guest VMs.

Populate the Default MAC Address Pool



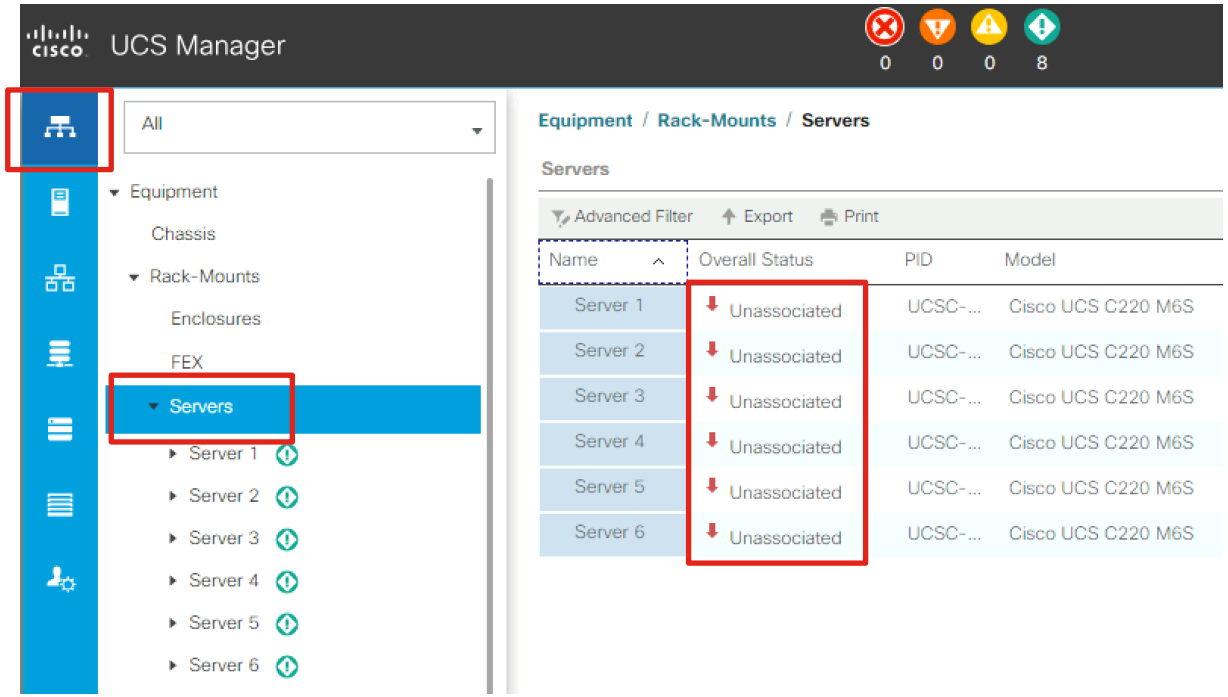
Create a block of MAC addresses in the default MAC Address Pool. This will be used during the installation only. Create a pool with at least 2 MAC addresses per node when using 2 cables per node, or 4 MAC addresses per node when using 4 cables. In the next screen we will create a unique pool which will be used long-term. Skipping this will lead to an installation failure.

Create MAC Address Pool



Recommend creating a unique MAC Address Pool rather than using the default pool in the long-term. Create at least 2 or 4 MAC addresses per node depending on if you are using 2 or 4 cables to the FIs, plus additional for growth. Remember the name of the pool created for use later.

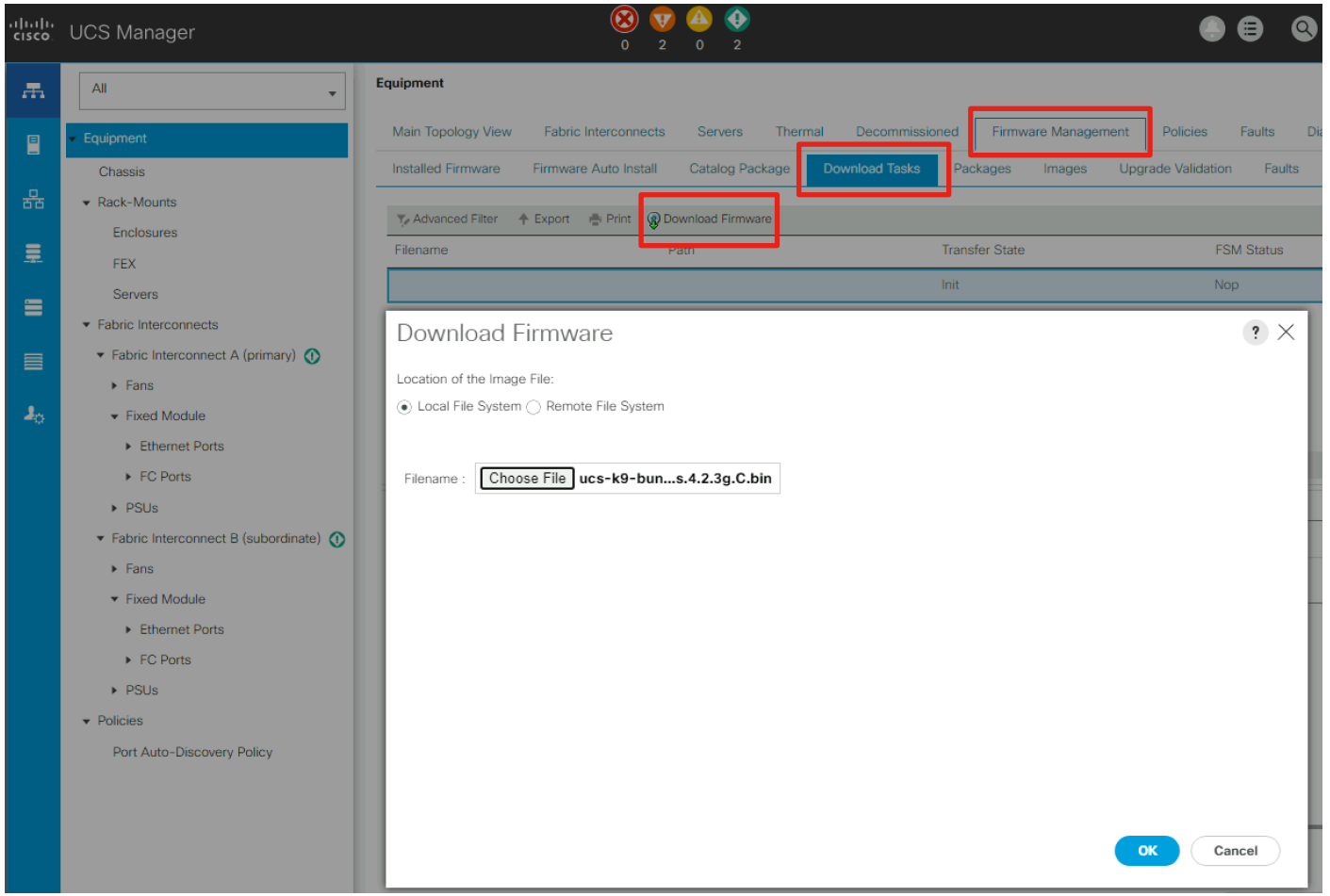
Verify All Servers Finish Discovery



Servers will start with a status of Discovery when they are first connected and reach a status of Unassociated when they have finished their inventory and are ready for use.

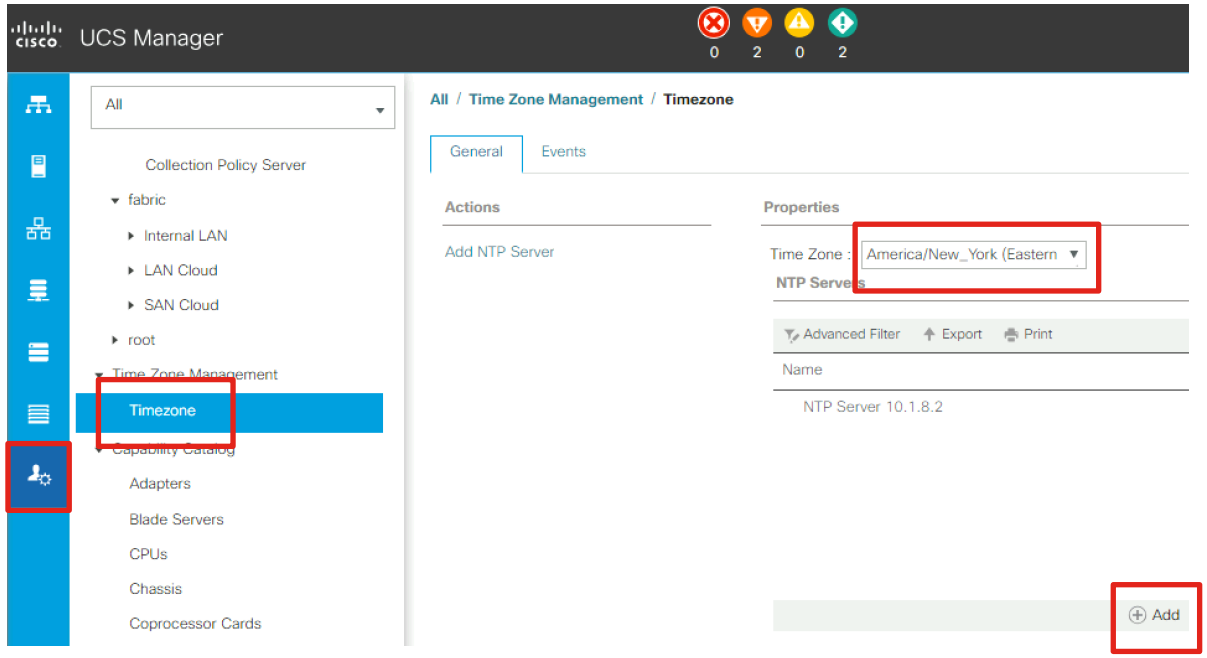
Upload Cisco UCS B-series and C-series bundles

- Consult the Cisco UCS HCL here: https://ucshcltool.cloudapps.cisco.com/public/#
- Search by operating system and select Nutanix to determine the required UCSM firmware version.
- Download the latest supported B-series and C-series bundles and release notes from here: https://software.cisco.com/download/home
- The A (infrastructure) bundle must be equal or newer than the required B and C bundles. Refer to tables 4 and 6 in the UCS Manager release notes to verify compatibility.
- If either required B or C bundle is missing the installation will fail.
- If the A (infrastructure) bundle requires upgrading, refer to the instructions found here: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Firmware-Mgmt/4-3/b_UCSM_GUI_Firmware_Management_Guide_4-3.html

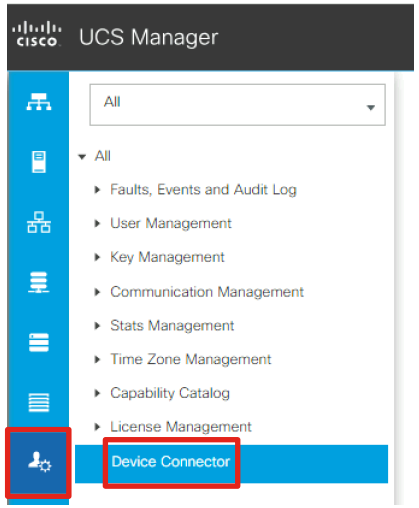


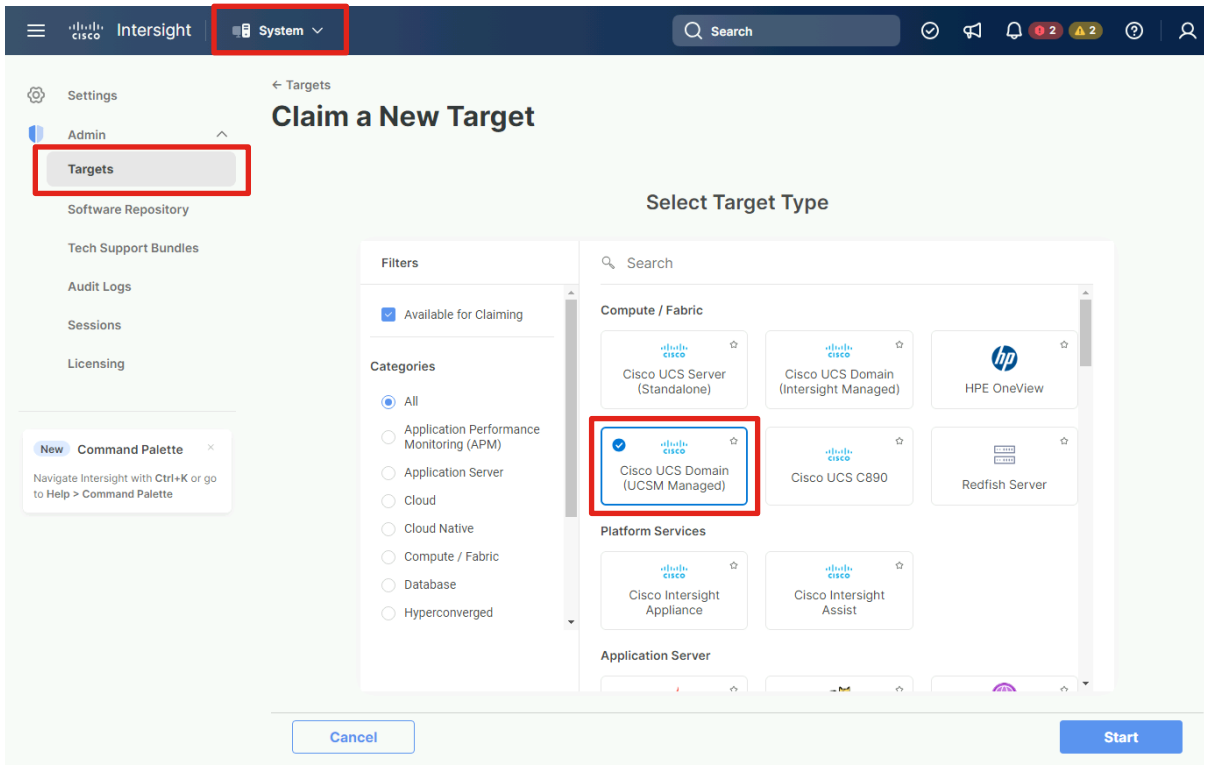
Other Optional UCSM Settings

Configure NTP servers and time zone



Claim UCS domain in Cisco Intersight

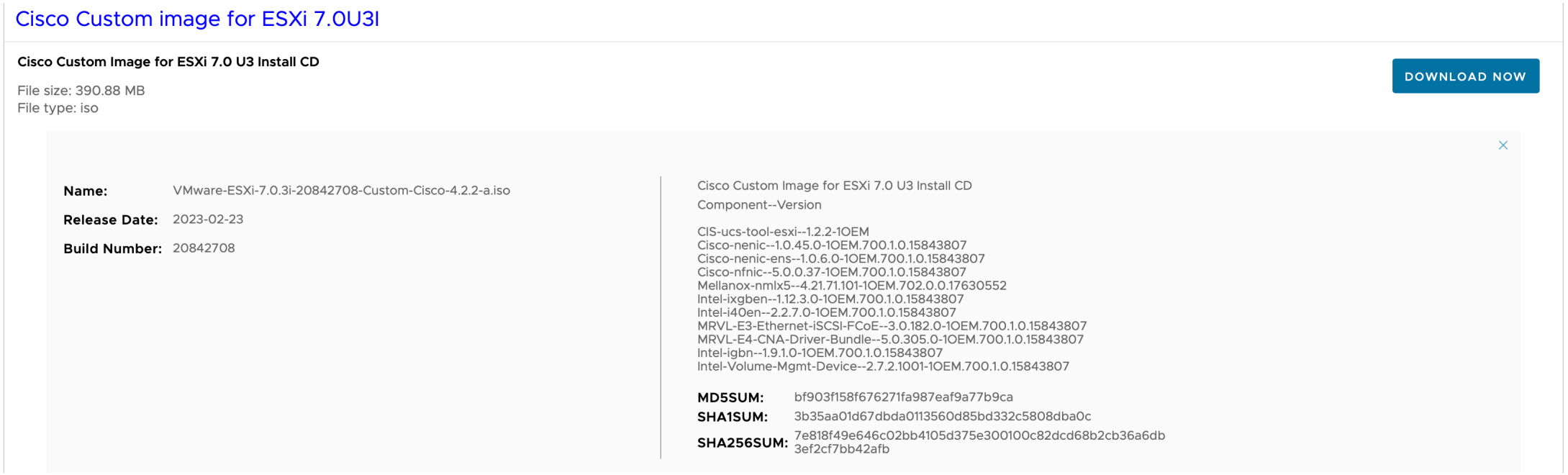




Nutanix Installation

Download Software

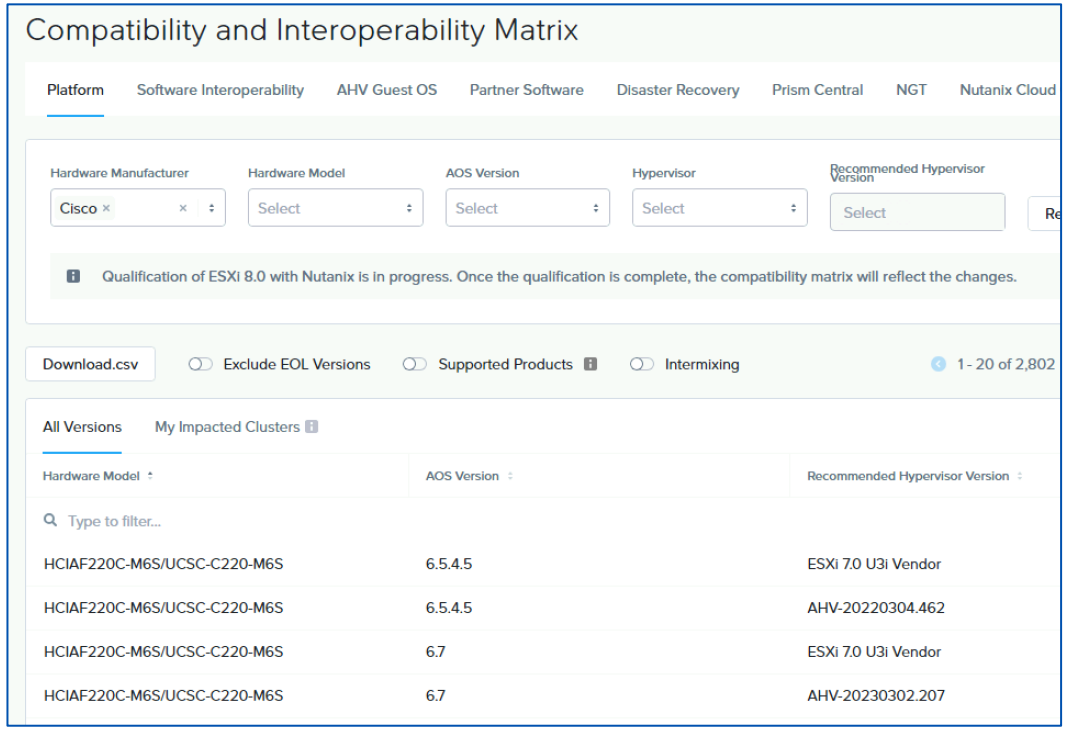
Download the latest Cisco custom ESXi ISO here:
https://customerconnect.vmware.com/downloads/details?downloadGroup=OEM-ESXI70U3-CISCO&productId=974
For example, the current ISO is version 7.0 Update 3i. Also copy the MD5SUM for the file to verify it later in Foundation if necessary.

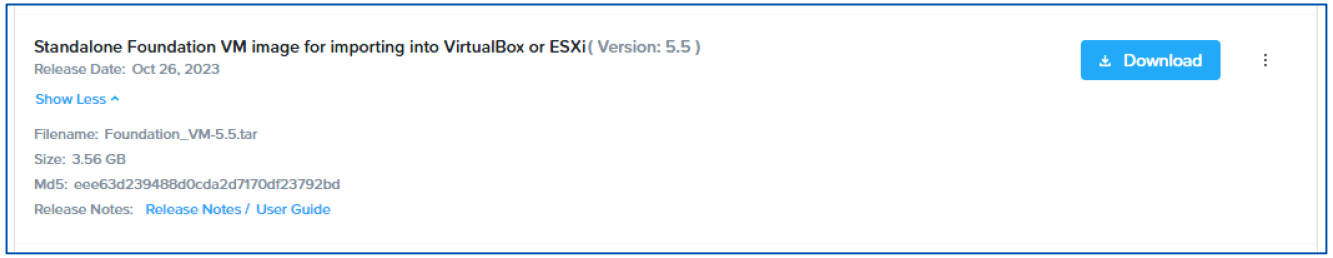


Download Software

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

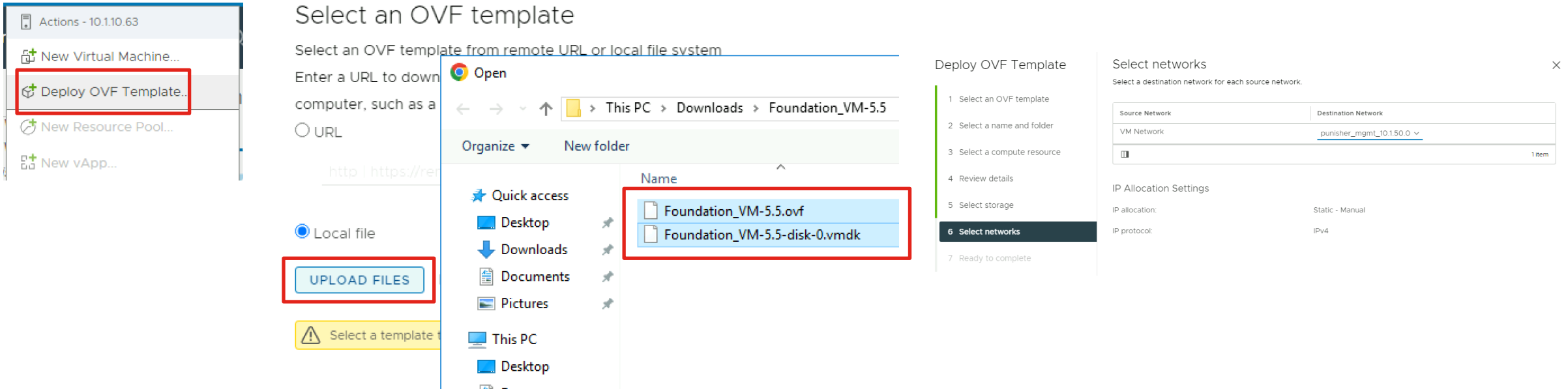
Download a supported Nutanix AOS STS or LTS image, the accompanying AOS metadata json file, plus the latest Foundation VM here: https://portal.nutanix.com/page/downloads/list





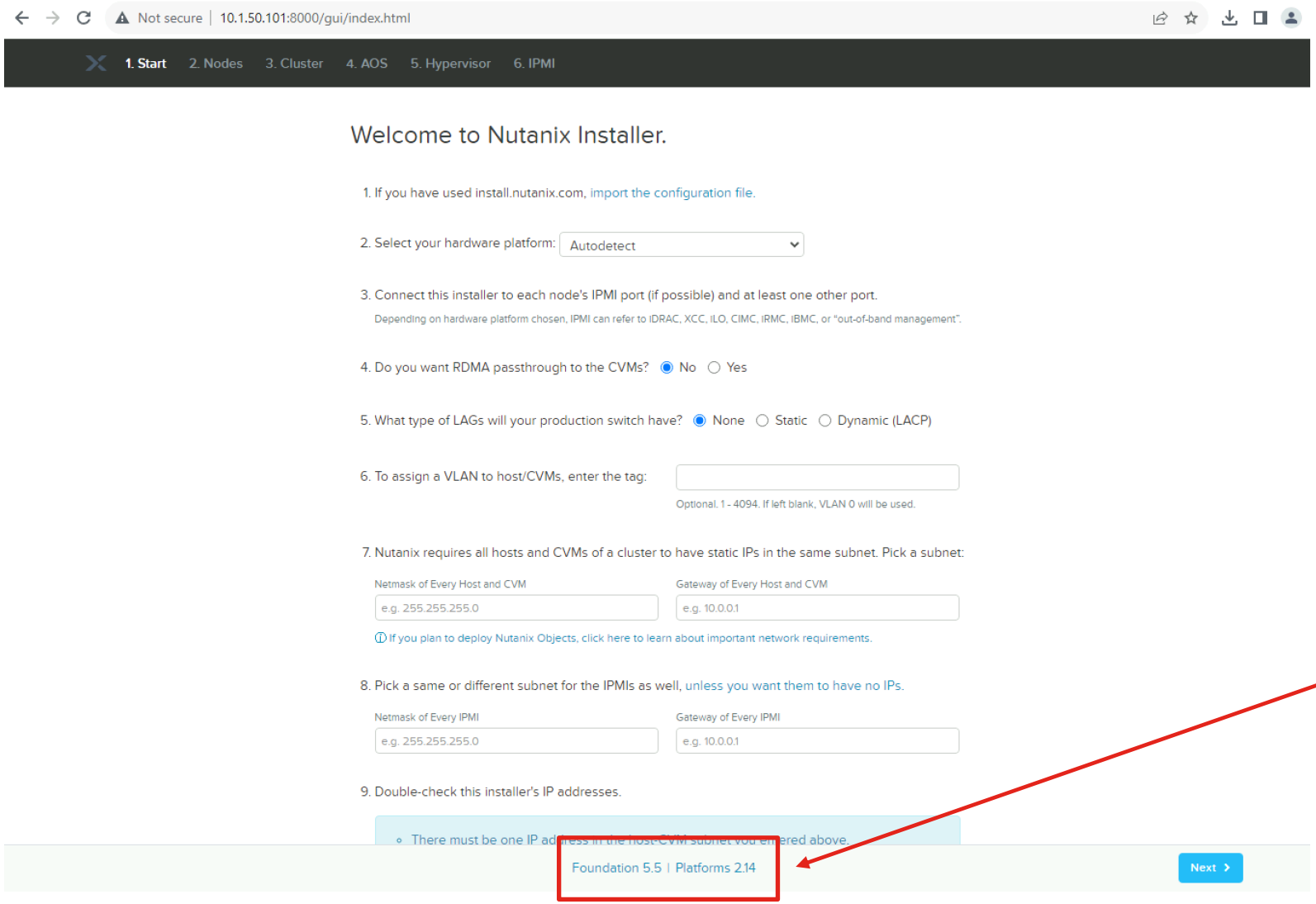
Deploy Foundation VM

First: Uncompress the downloaded .tar file



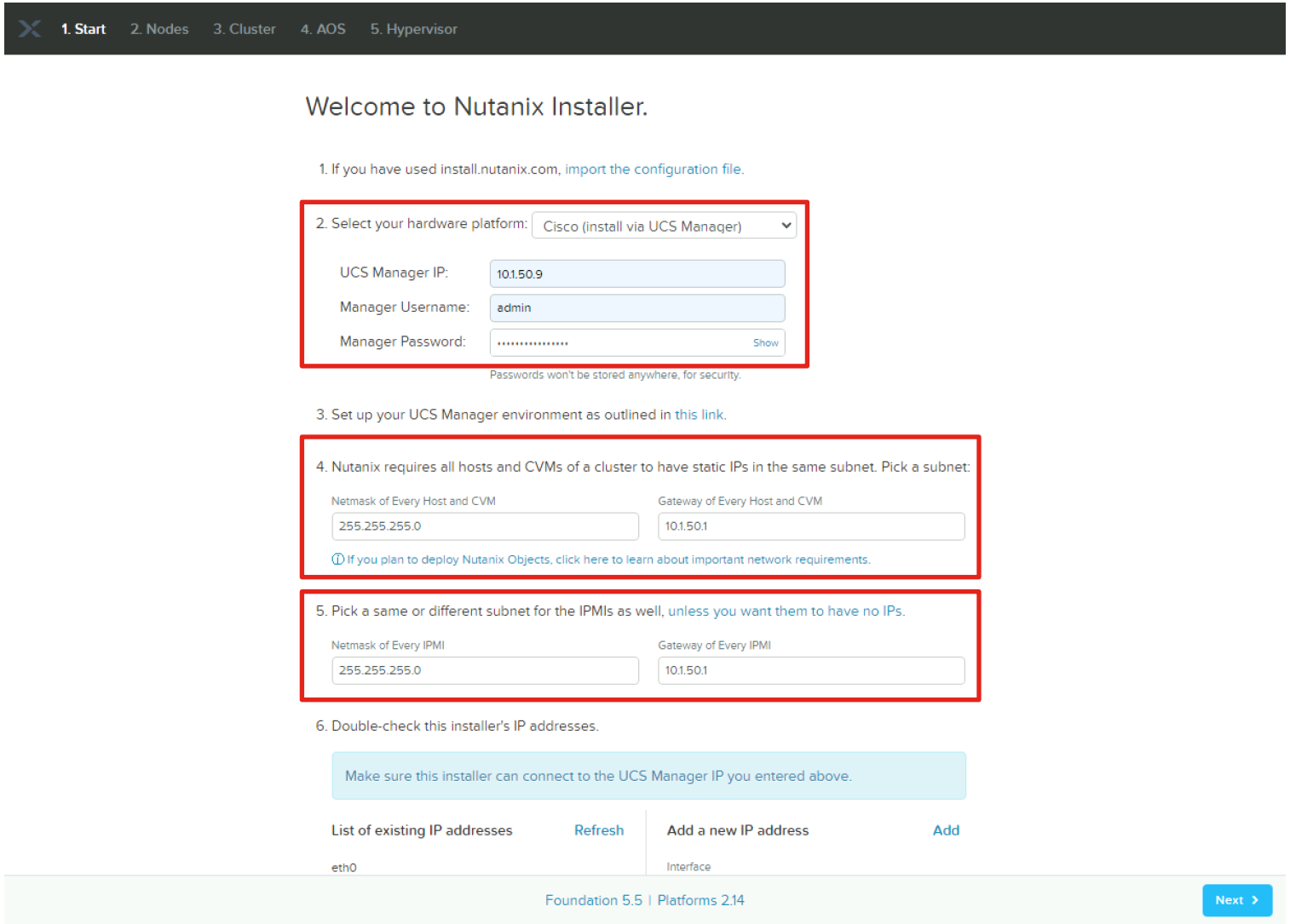
- Select a guest VM network with access to the UCS FIs, DNS, NTP, the ESXi or AHV hypervisor hosts, the storage controller VMs (which will be installed), and ideally internet access for updates.
- The Foundation VM will get an IP address via DHCP by default, despite the OVF saying it is static.
- To configure the Foundation VM for static IP, follow these steps: https://portal.nutanix.com/page/documents/details?targetId=Field-Installation-Guide-v5_5:fie-foundation-vm-install-on-workstation-t.html

Power on the VM and connect to the web interface



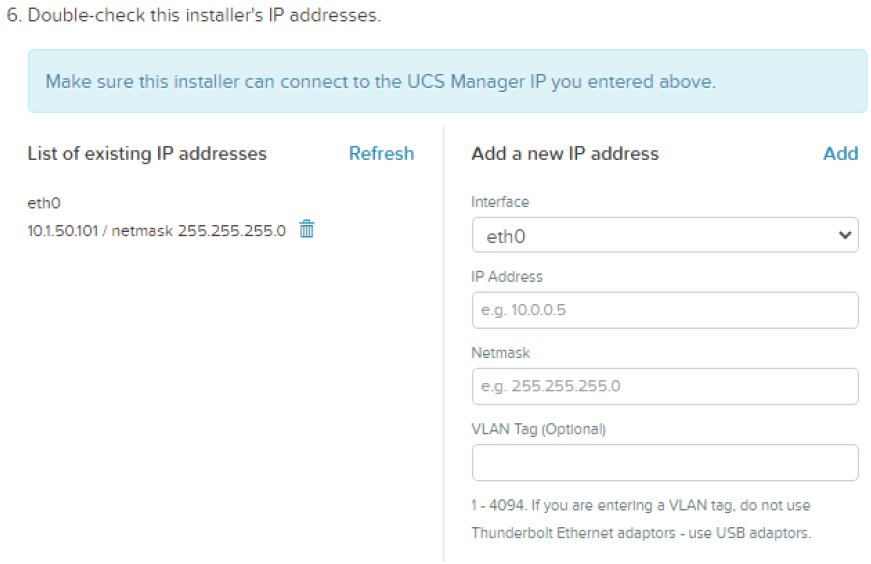
Click here to check for any updates online to Foundation or the Foundation Platforms data file

Enter values on the Start page



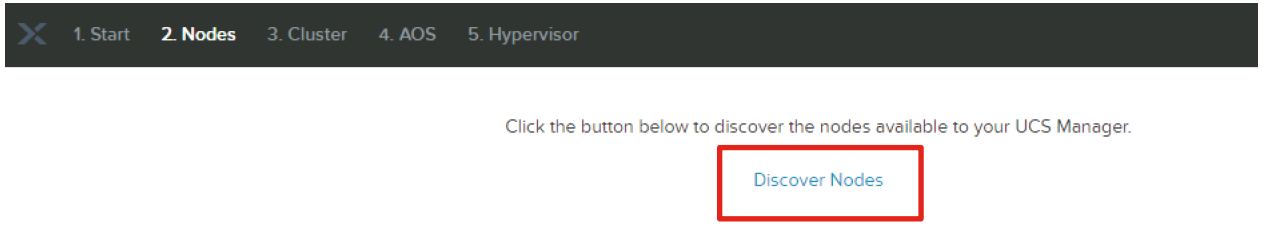
- Select Cisco (install via UCS Manager). Do not select the (install without UCS Manager) option, it is unsupported.
- Enter the UCS Manager details
- Enter the subnet mask and gateway for the hypervisor management interfaces and storage controller VMs. This can be a separate subnet from UCS Manager.
- Enter the subnet mask and gateway for the servers' CIMC (IPMI) addresses. This must be the same subnet as UCS Manager.

Enter values on the Start page continued



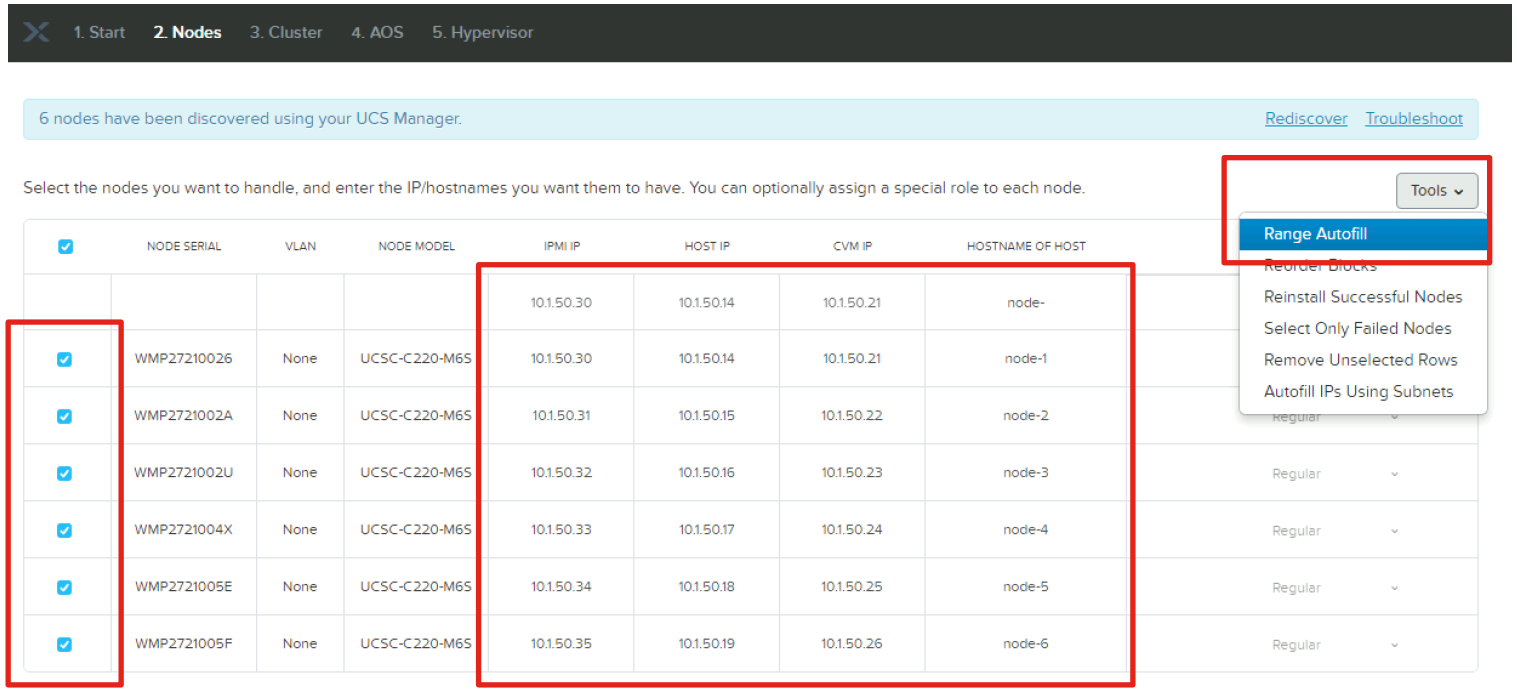
This is only necessary if the installer cannot reach both the hypervisor management and controller VM IP addresses, plus the UCSM and CIMC addresses via a single interface, for example if the networks were not routable. If this applies to you, add another interface in the appropriate subnet to the Foundation VM, so that it can reach all the required endpoints.

Enter values on the Nodes page



- You must click Discover Nodes to inventory the UCS domain. Do not continue and attempt to add nodes manually.
- Each node requires 3 IP addresses, one for the CIMC, one for the hypervisor host, and one for the storage controller VM.
- Add A records to your DNS server for the hypervisor hosts.

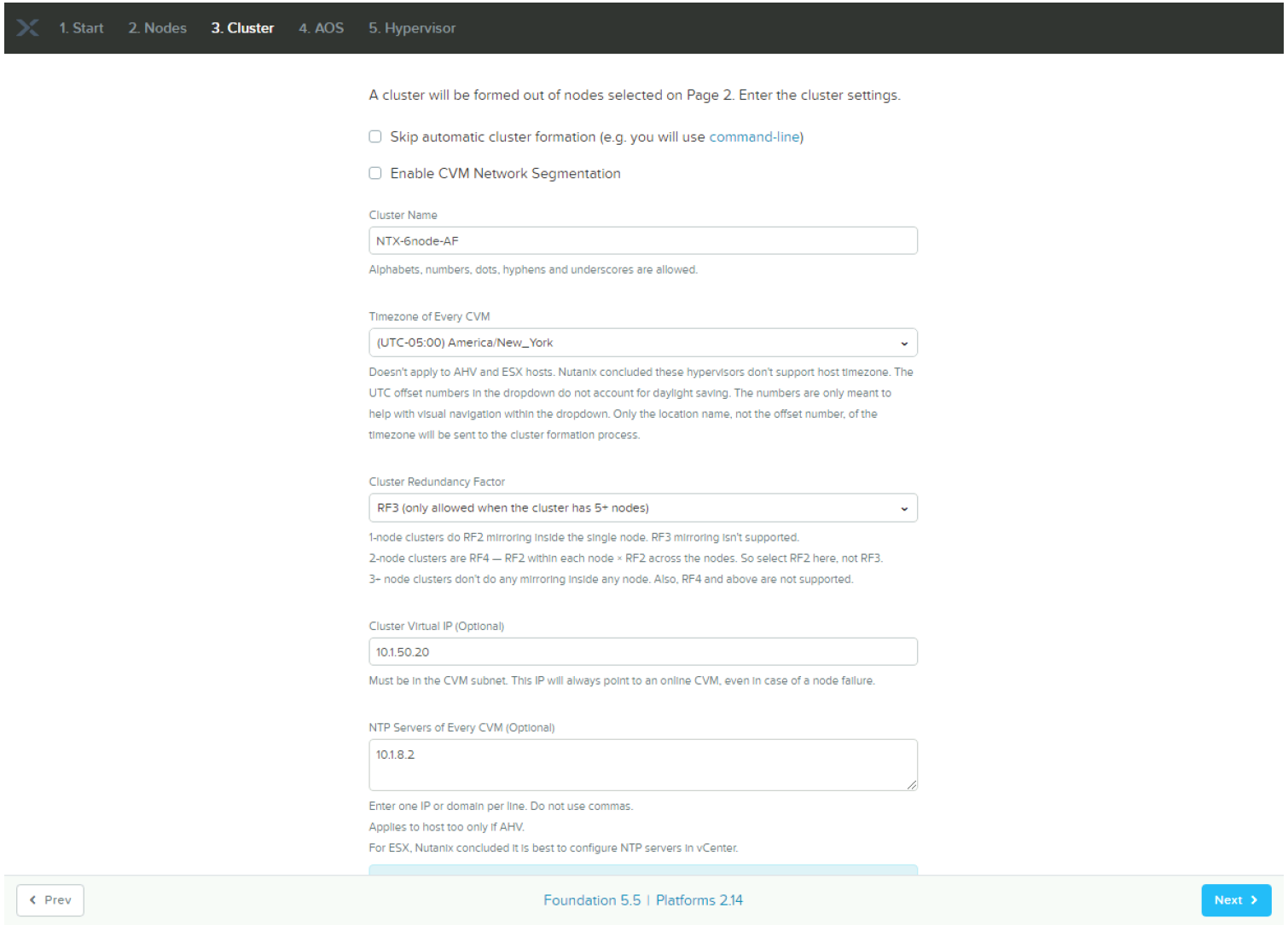
Enter values on the Nodes page continued



- Select the nodes for the cluster
- Select Range Autofill to enter starting IPs and hostnames and auto fill the values
- IPMI IP will be the CIMC IP address, Host IP is the hypervisor, and CVM IP is the controller VM.
- Verify all values are correct before continuing

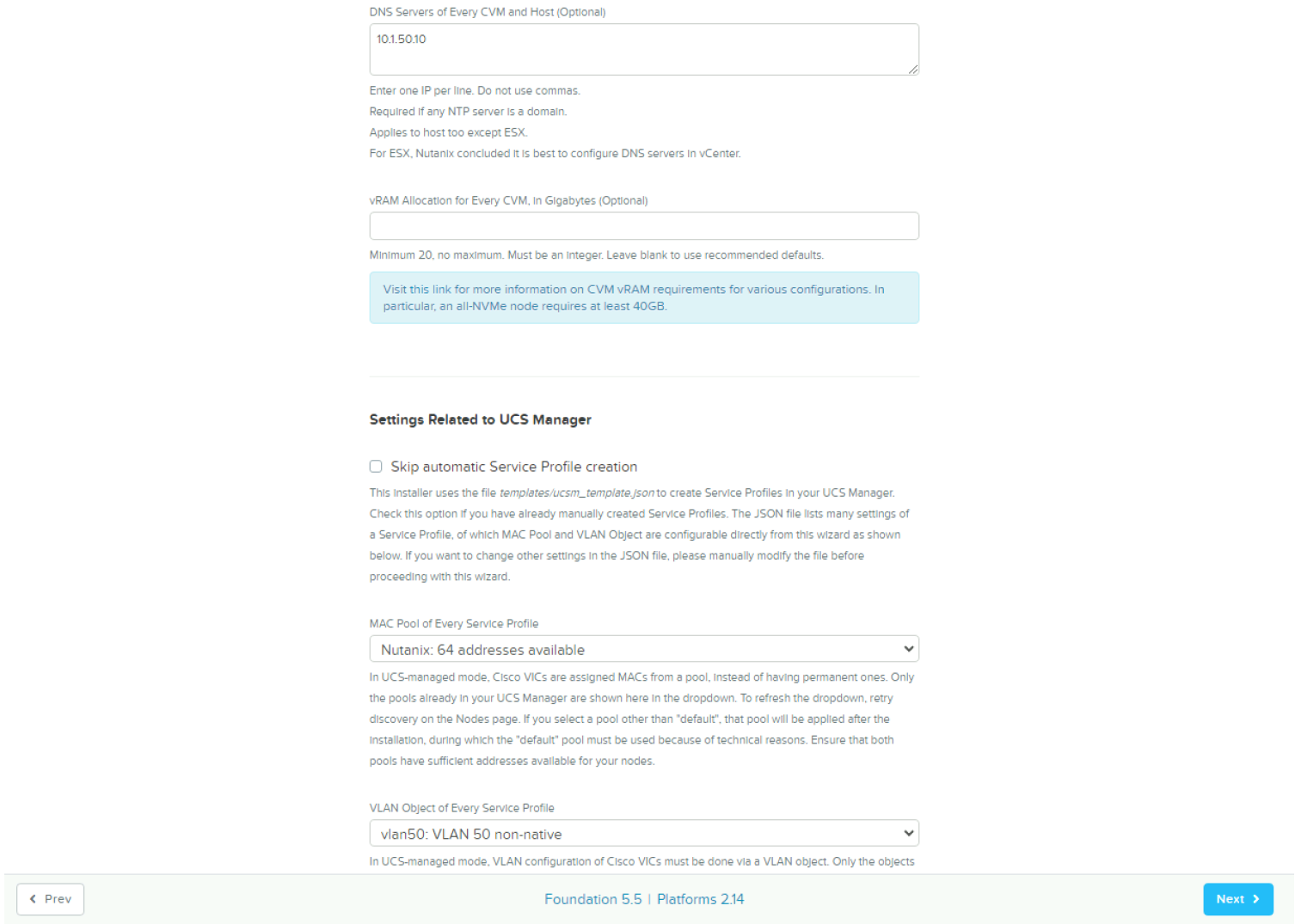
Note: Be cautious not to pick a server already in use, it will be immediately shut down and re-imaged, causing data loss.

Enter values on the Cluster page



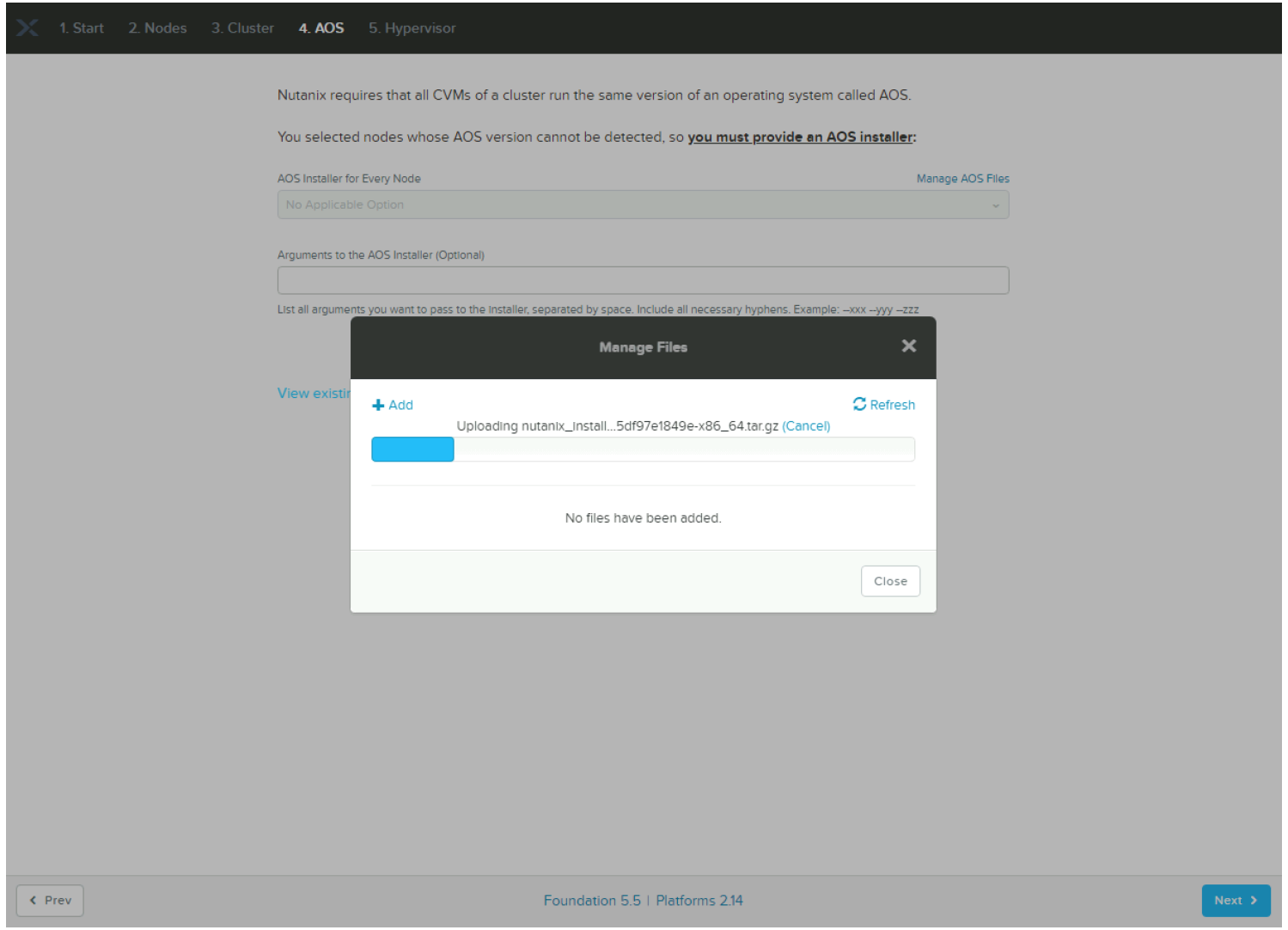
- Leave the checkbox unchecked to create the cluster.
- Do not enable CVM network segmentation, this will cause an installation failure.
- Enter the cluster name, time zone and redundancy factor.
- Nutanix generally recommends RF2, and only using RF3 when business rules or policies require it.
- It is highly recommended to enter the cluster virtual IP and NTP server address(es).

Enter values on the Cluster page continued



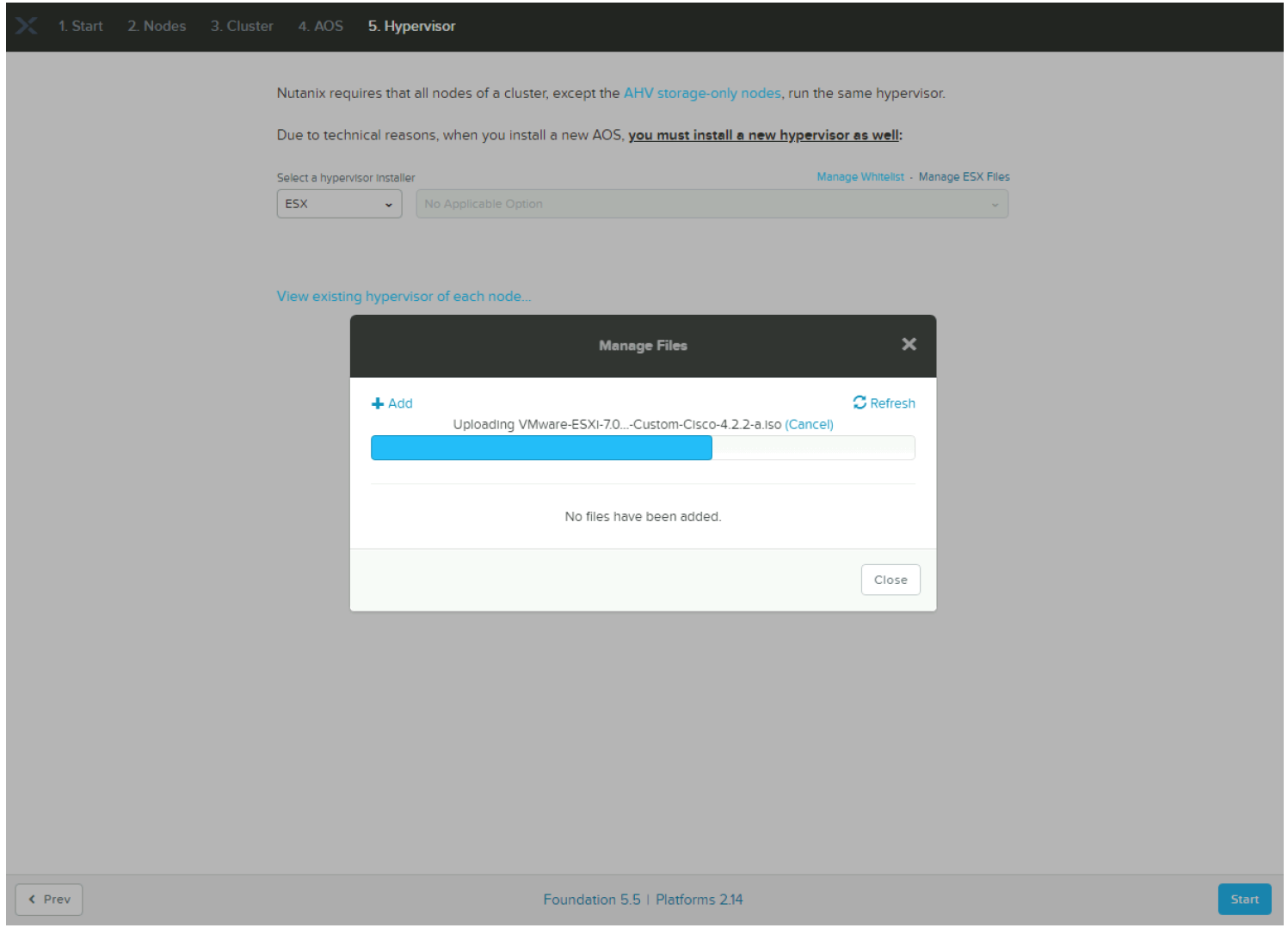
- Enter DNS server IP address(es).
- Leave CVM vRAM allocation blank for automatic config unless you know for sure what value to enter.
- Do not skip Service Profile creation!
- Select the MAC address pool created earlier, and the VLAN created earlier, this will be the VLAN used by the controller VMs and the hypervisor hosts.

Upload files on the AOS page



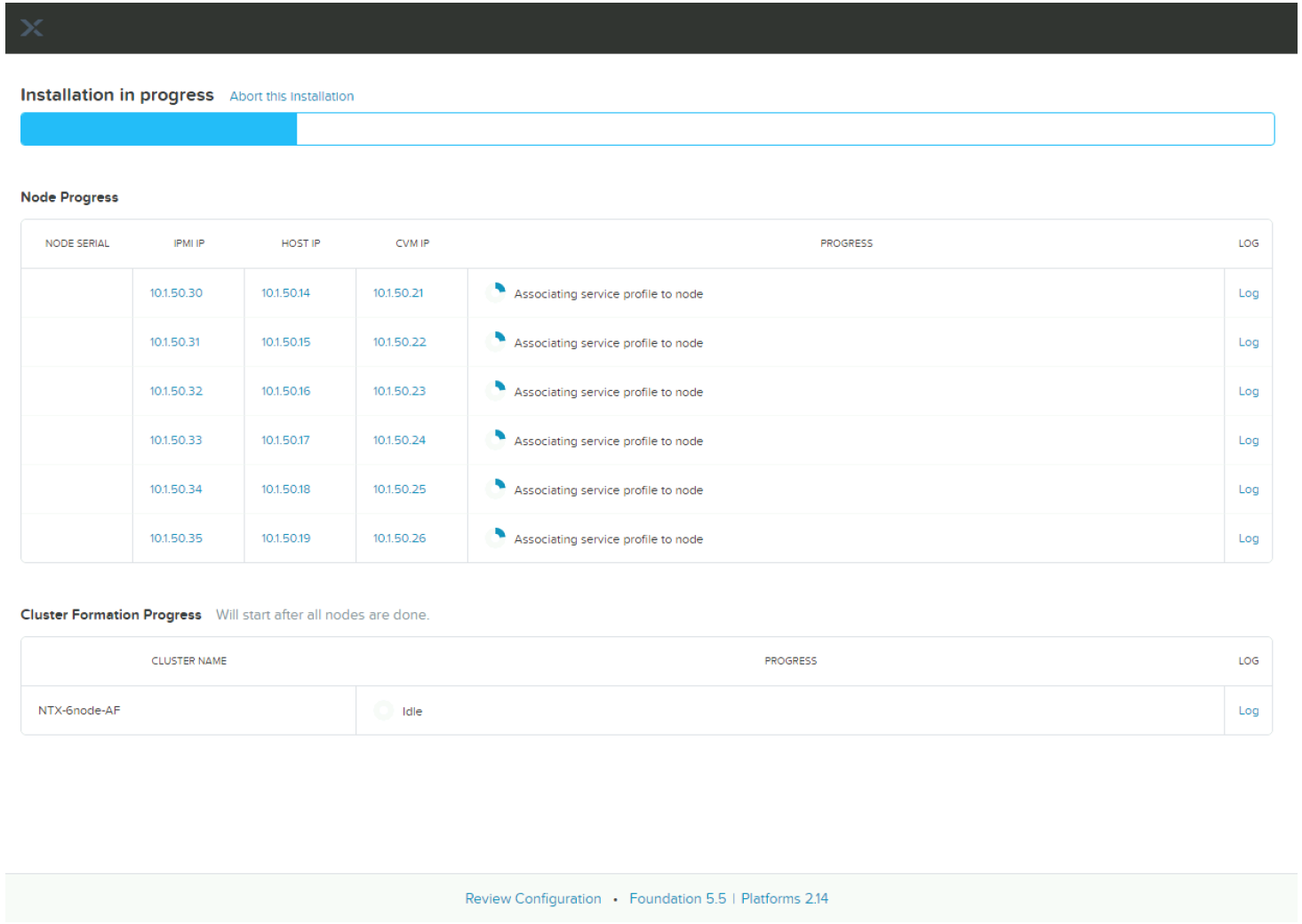
- Upload the AOS version file downloaded earlier.
- Select the uploaded file from the dropdown list.
- Do not enter custom installer values.

Upload files on the Hypervisor page

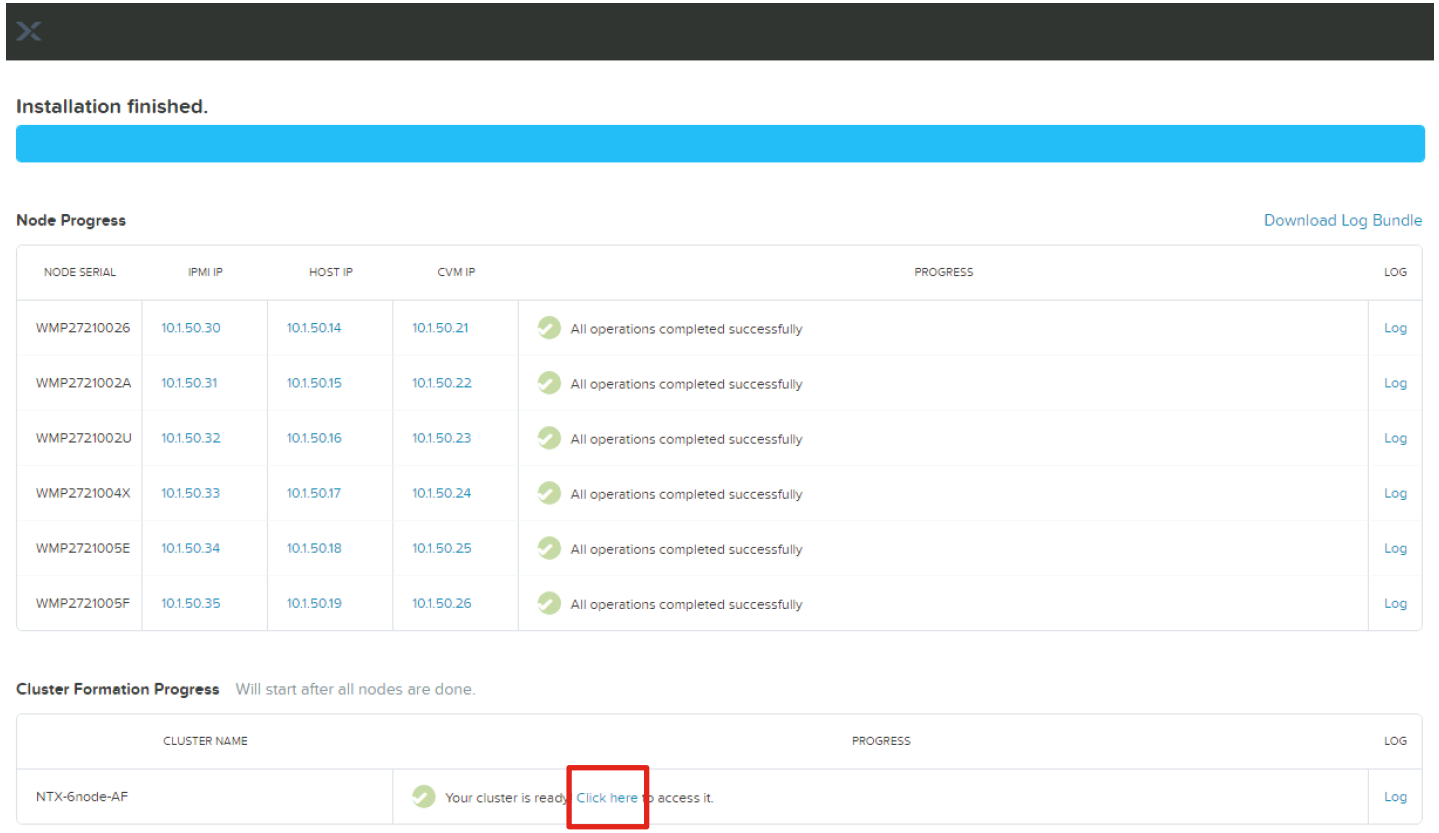


- Select AHV or ESXi
- If using AHV, use the version bundled with AOS from the dropdown list.
- If using ESXi, upload the Cisco custom ESXi ISO file downloaded earlier. Do not use a generic ESXi ISO image.
- Select the uploaded file from the dropdown list.
- The Cisco custom ESXi ISO should be auto whitelisted.
- Click Start.
- Ensure the installer is being run from a machine that will not go to sleep during the install.

Install Progress



Install Complete



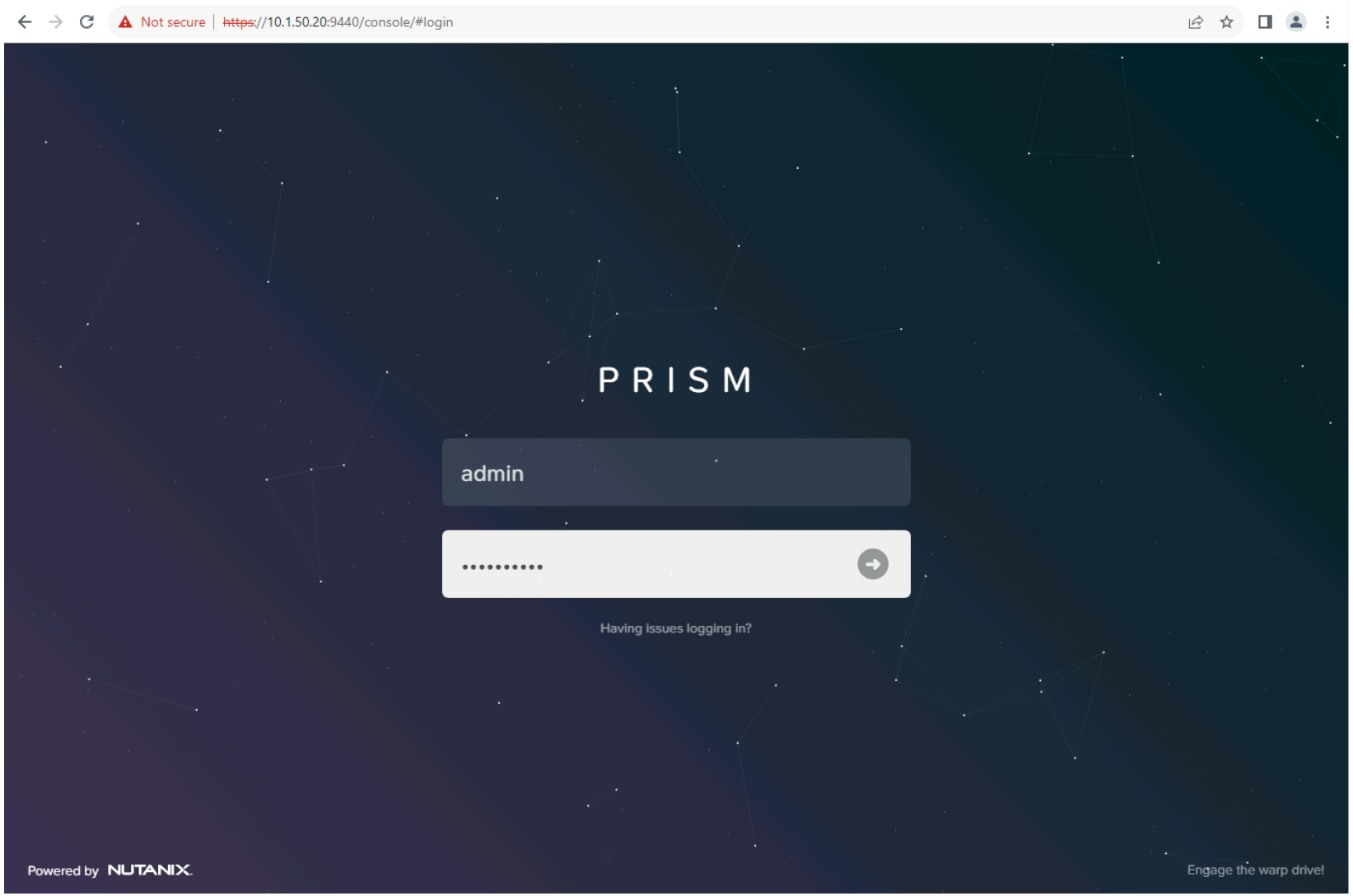
Click the link to open Prism Element when the installation is complete.

Initial Cluster Configurations

- Initial Configuration for ESXi
- Initial Configuration for AHV

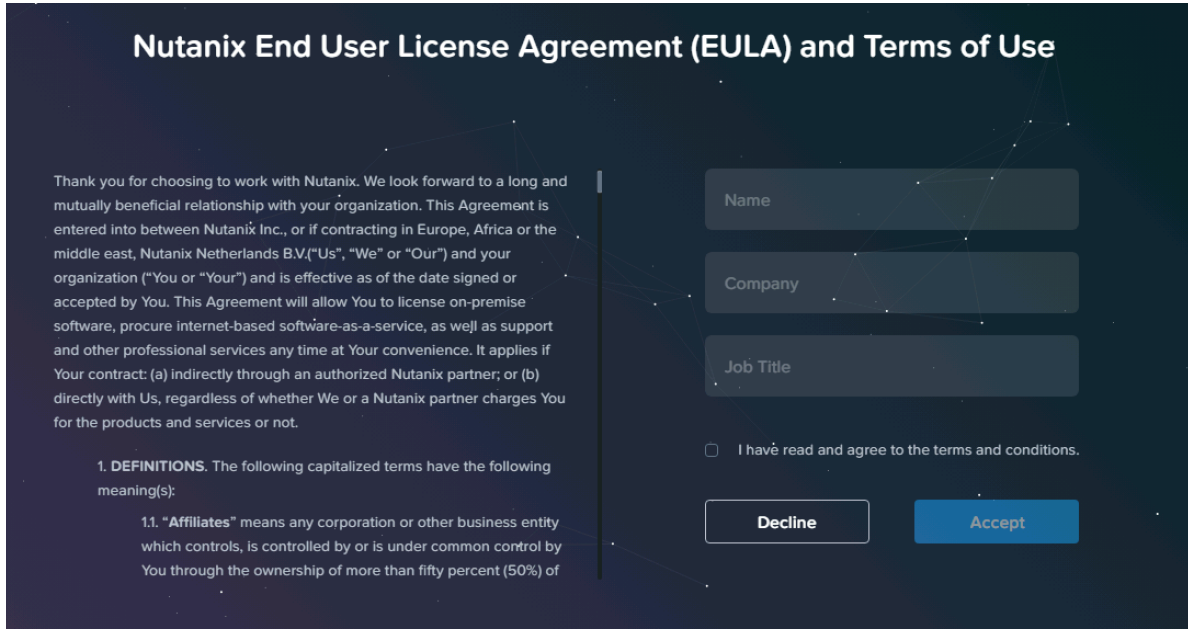
Initial Nutanix Cluster Config for ESXi

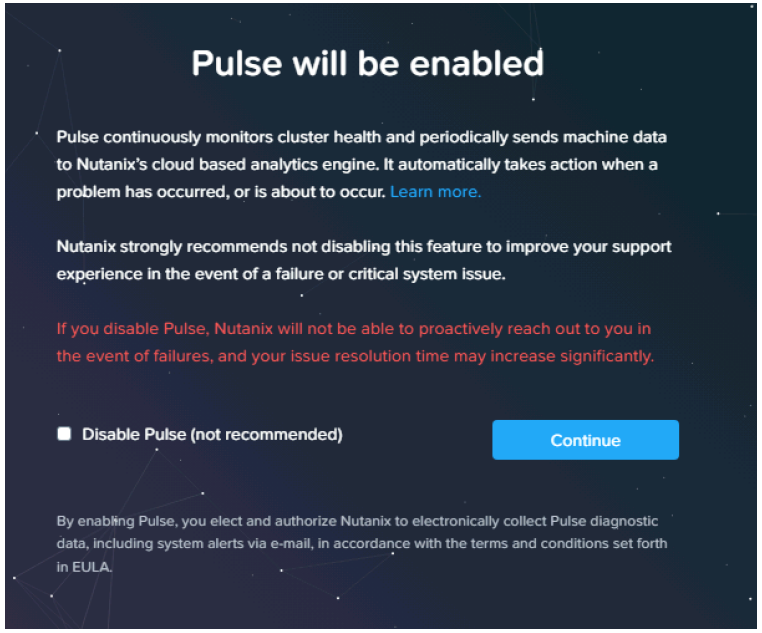
Access Prism Element



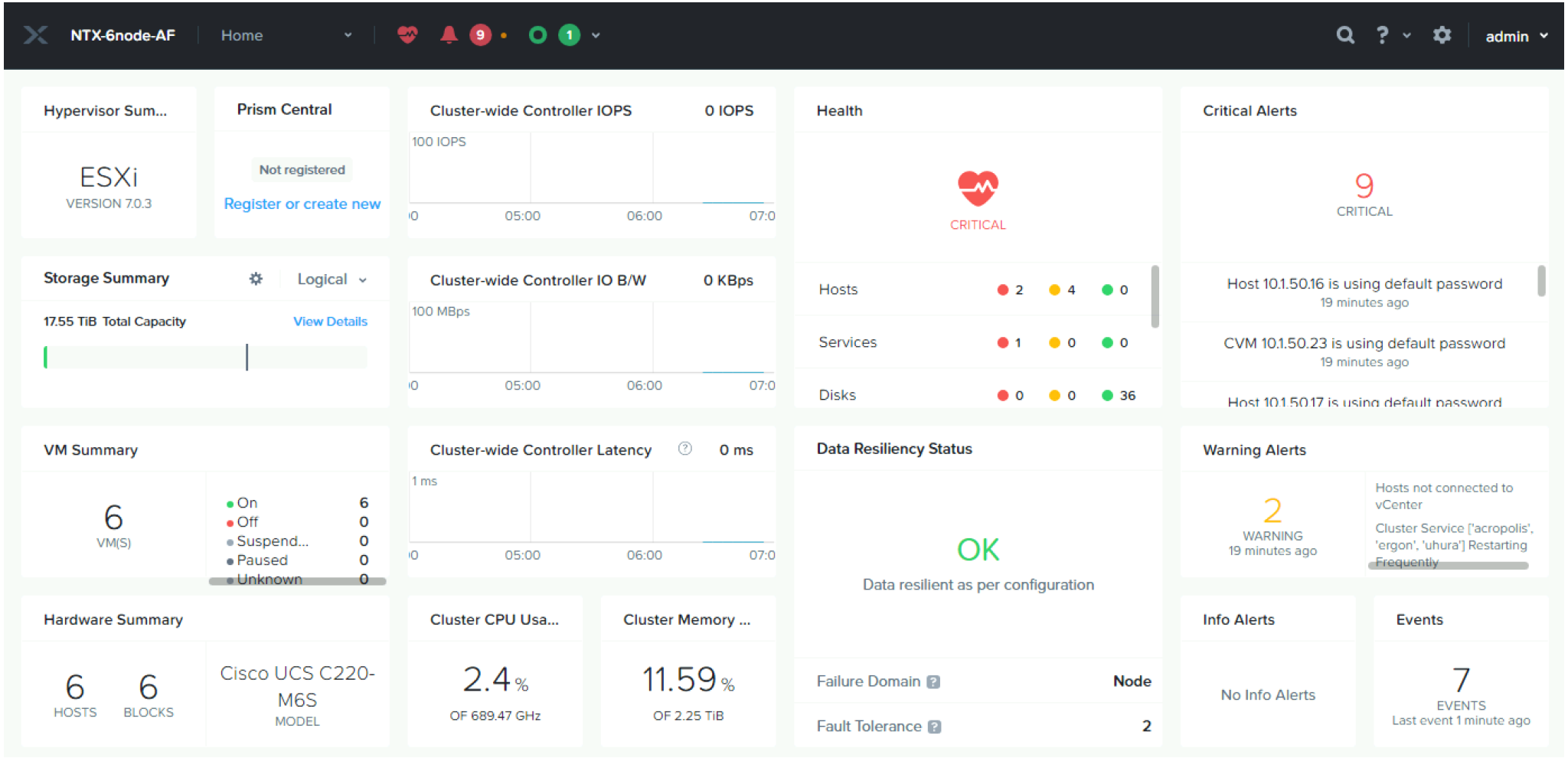
- Access Prism Element (the built-in version of Prism) at the cluster IP address or an individual controller VM IP address, using HTTPS at port 9440
- Default username: admin
- Default password (case sensitive): Nutanix/4u
- Password must be changed on first login

Accept EULA and Enable Pulse

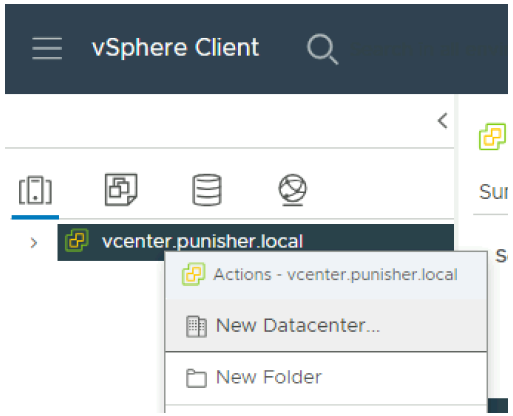


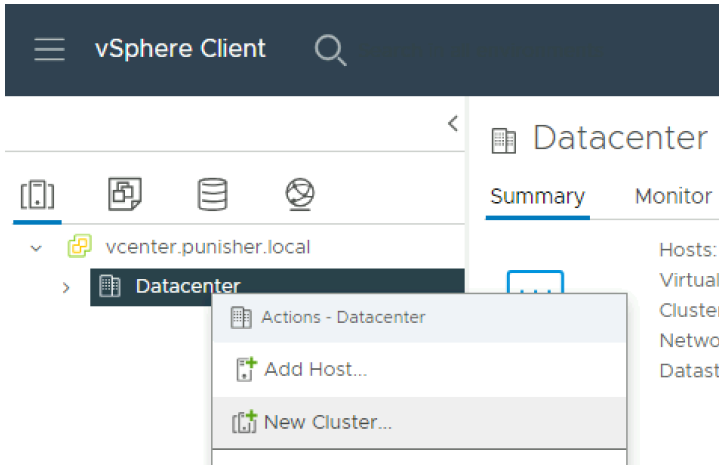


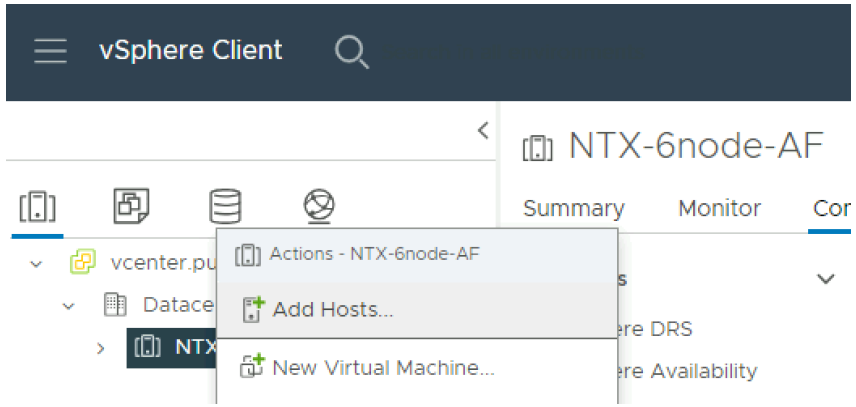
Prism Element Home

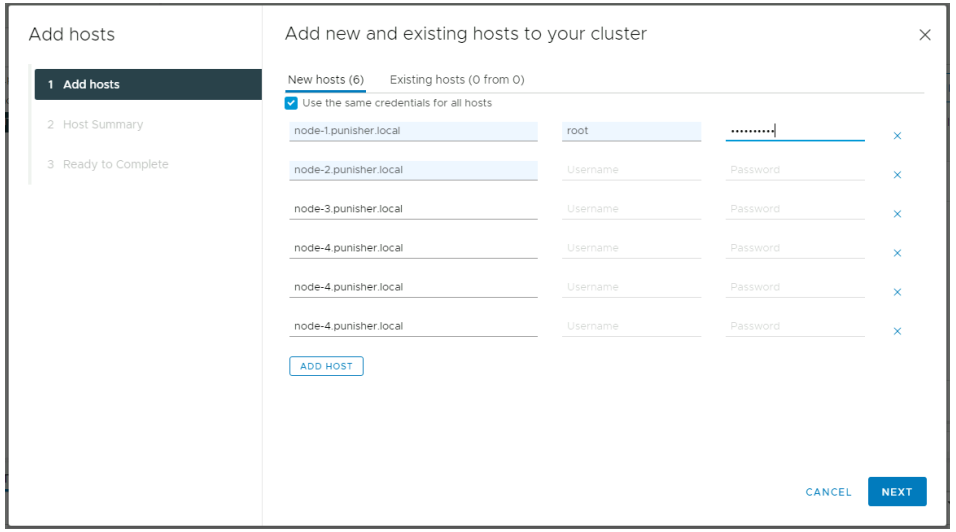


Add Hosts to vCenter Server





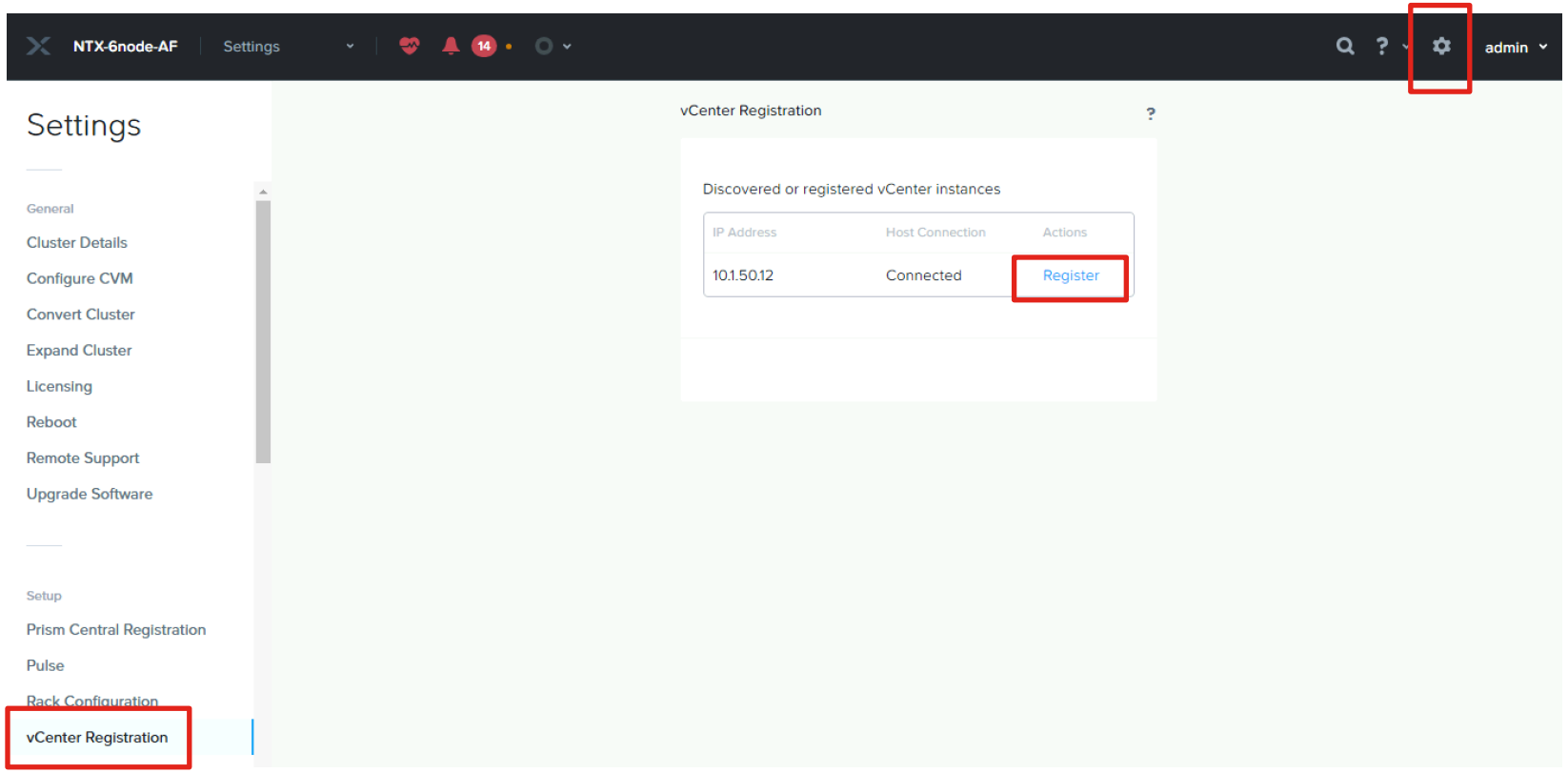


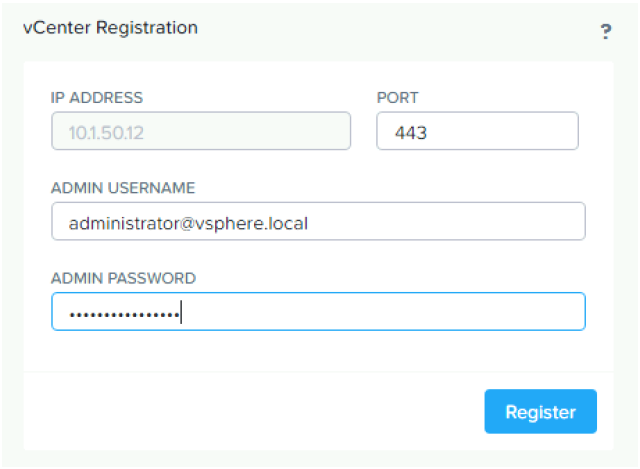


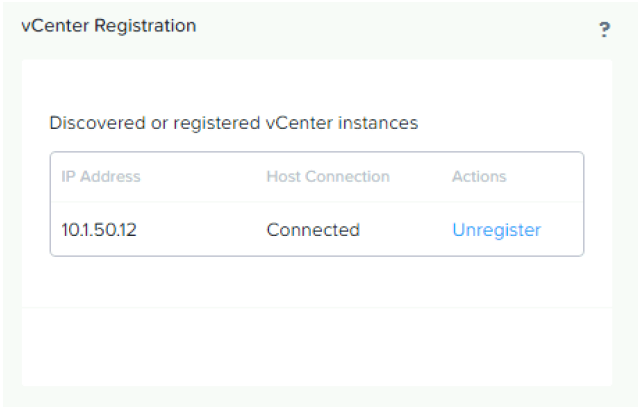
In the vSphere Web Client, create a Datacenter, a Cluster and add the hosts. You will have to move the hosts into the cluster after adding them.

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

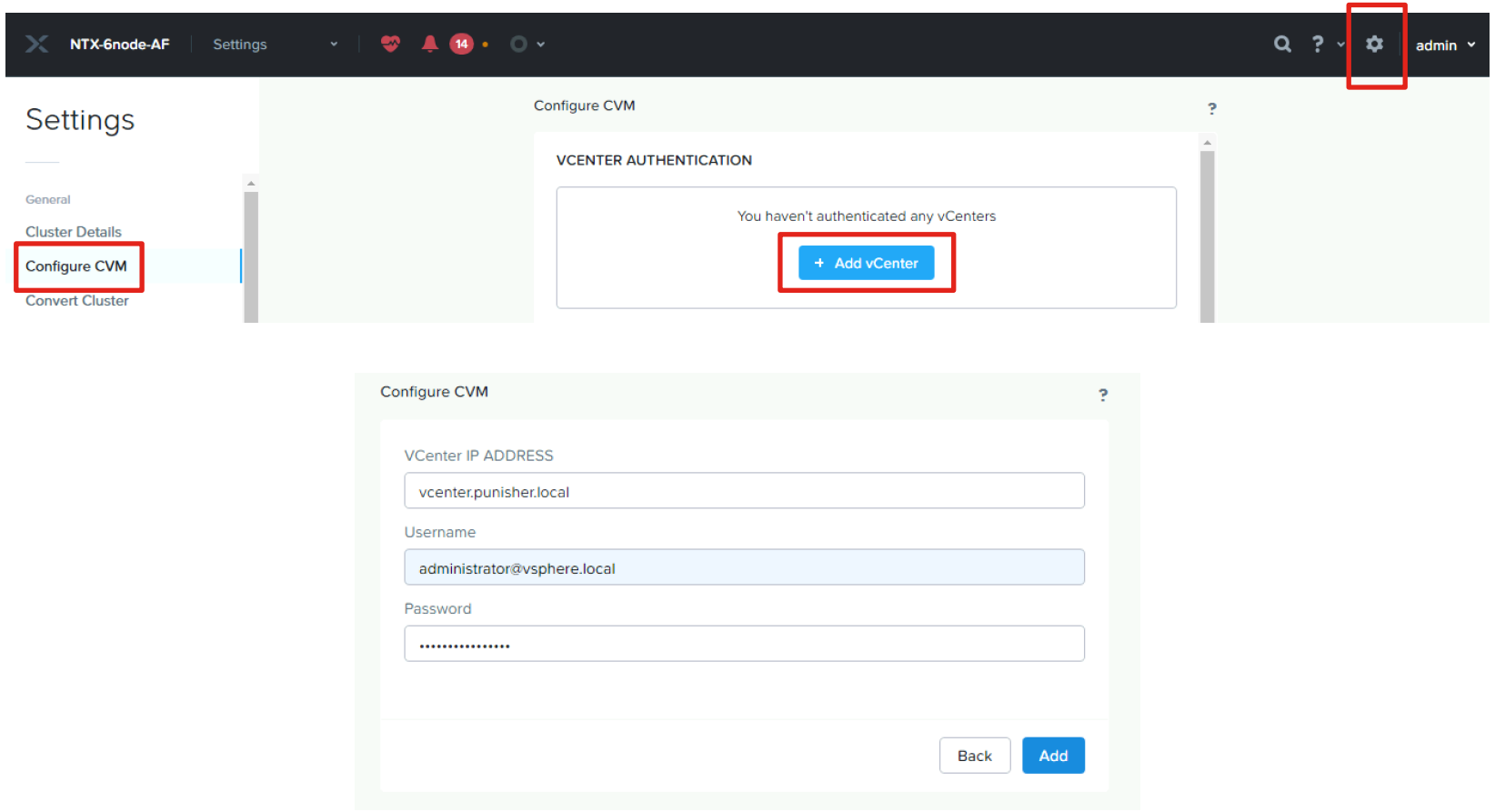




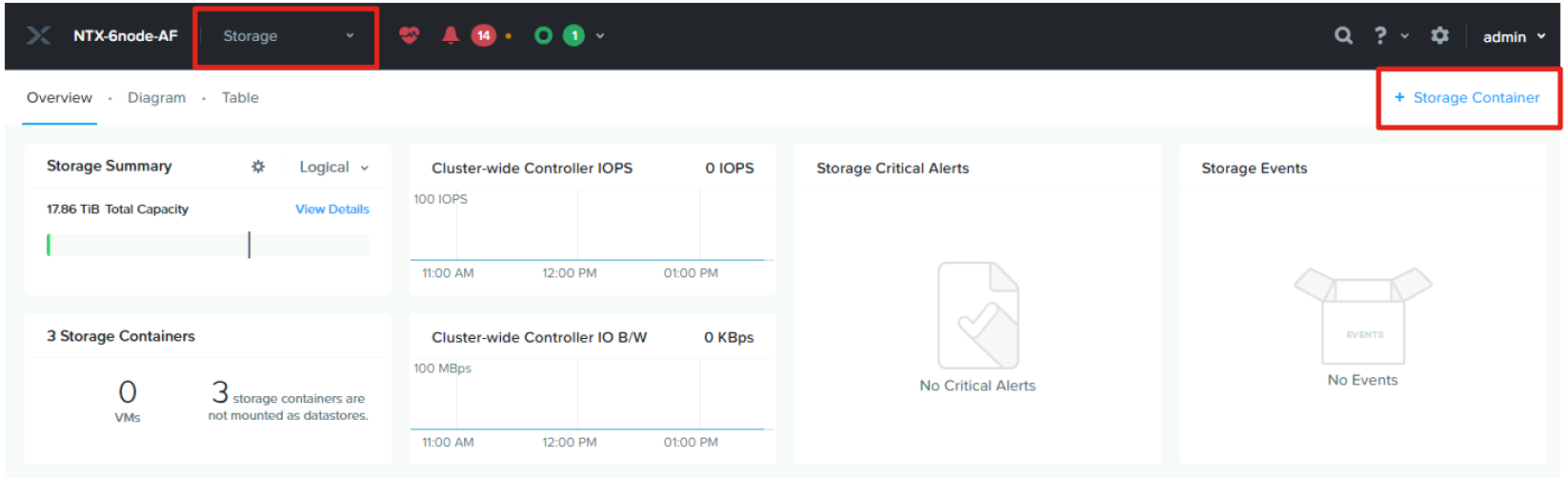


Note: It may take a few minutes after adding the nodes for the vCenter to be discovered and allow you to register it.

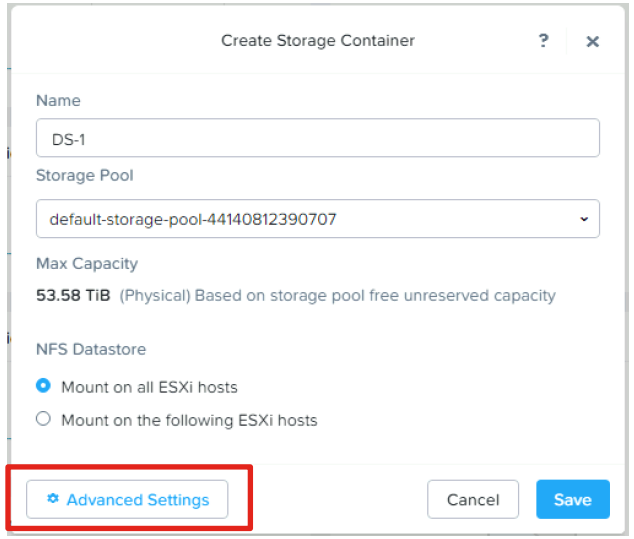
Configure vCenter Server Authentication

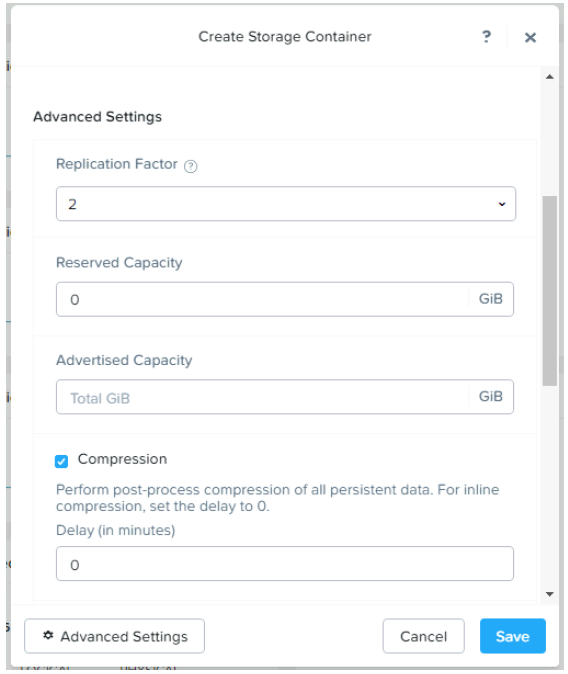


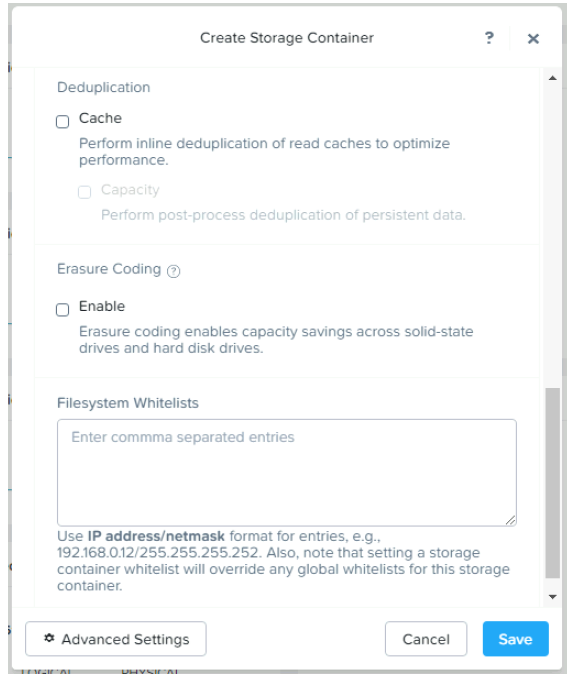
Create Storage Containers (Datastores)



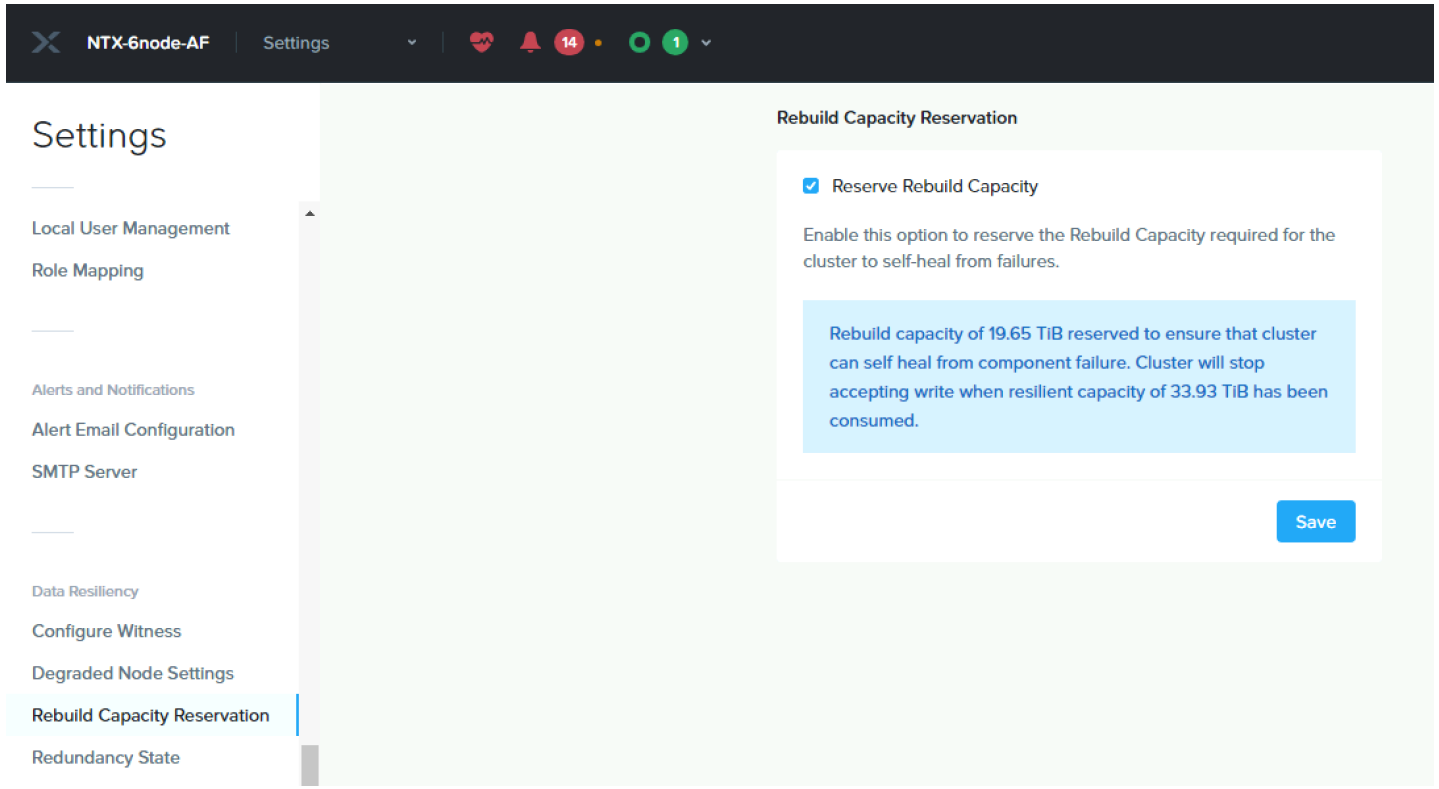
Note: After creating the containers, you should manually select them as the HA datastores in the vCenter Cluster Availability settings, when using ESXi.

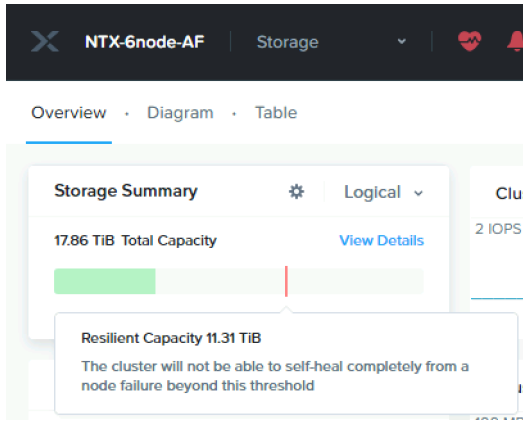




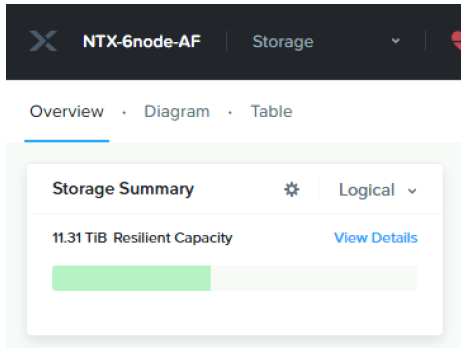


Set Rebuild Capacity Reservation



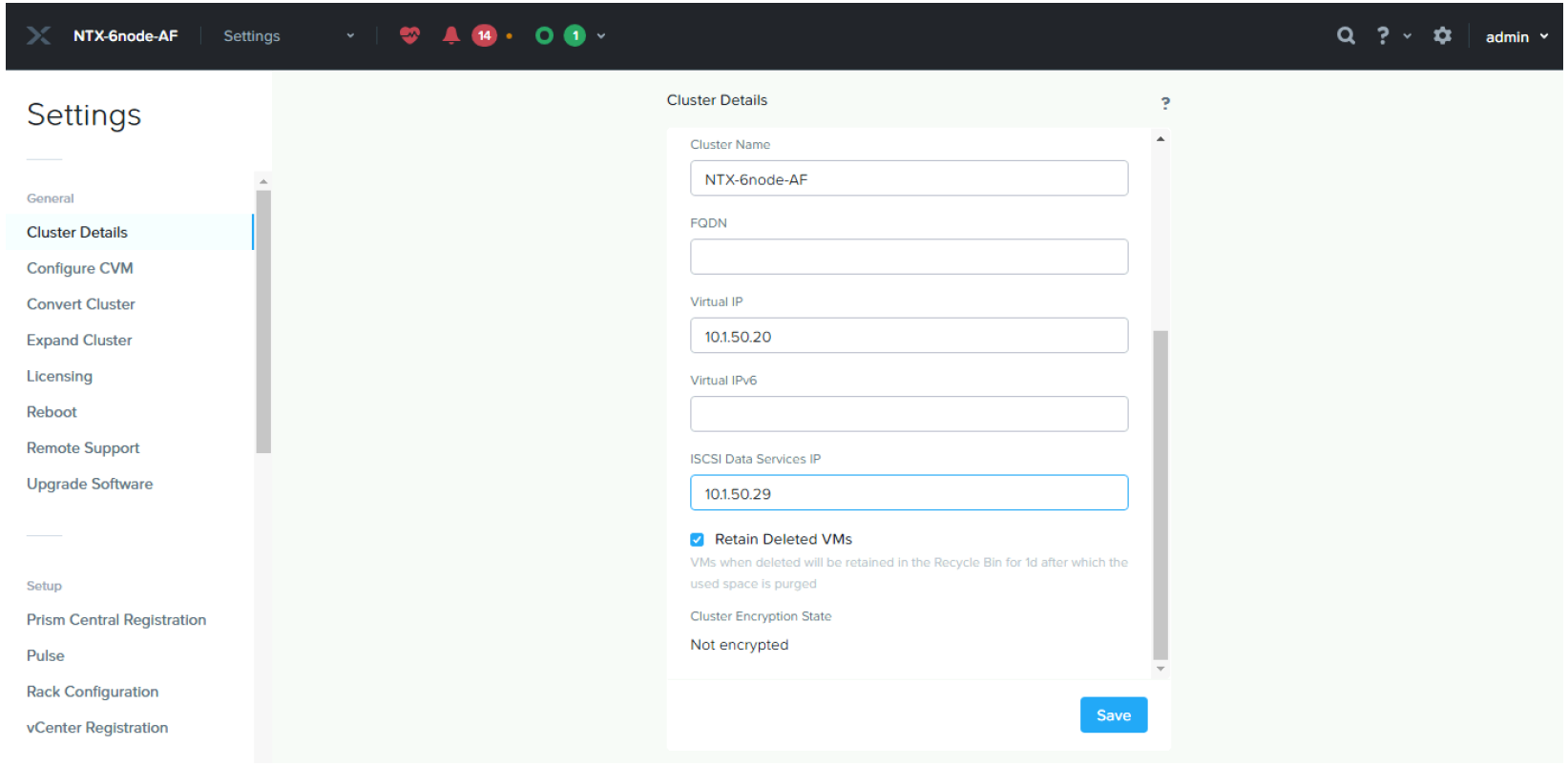


Without this setting enabled, cluster will accept incoming writes even if all blocks cannot completely heal during failures



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

Set ISCSI Data Services IP Address



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

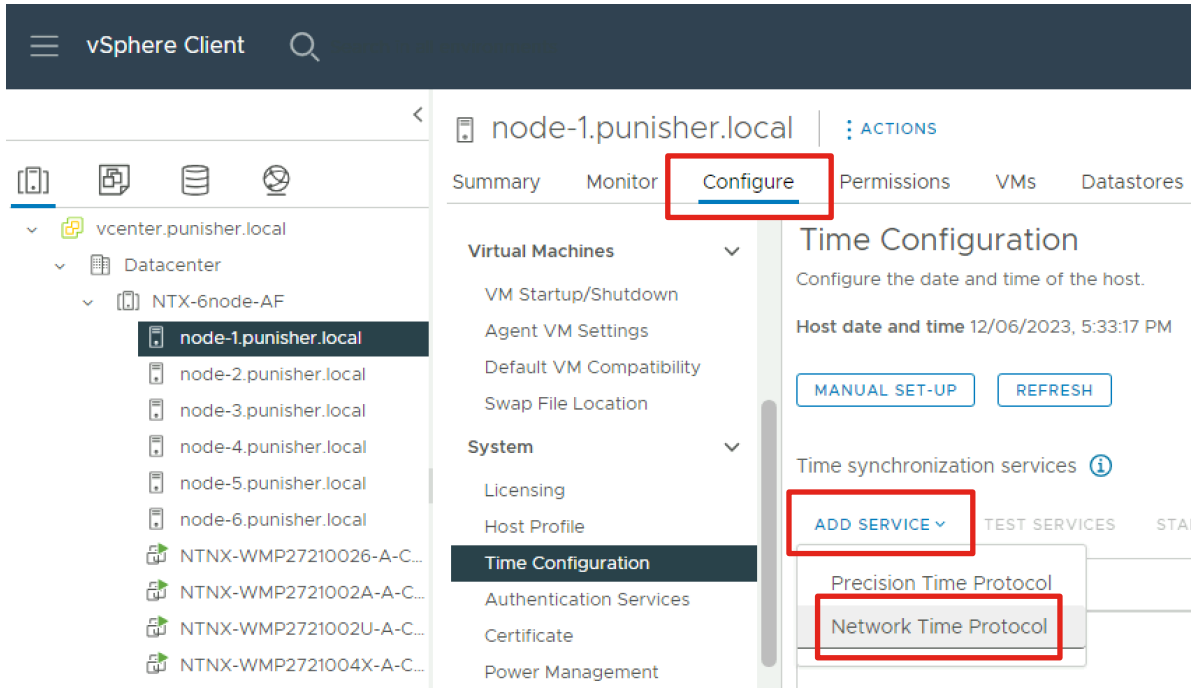
```
nutanix@NTNX-WMP27210026-A-CVM:10.1.50.21:~$ sudo passwd nutanix
Changing password for user nutanix.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

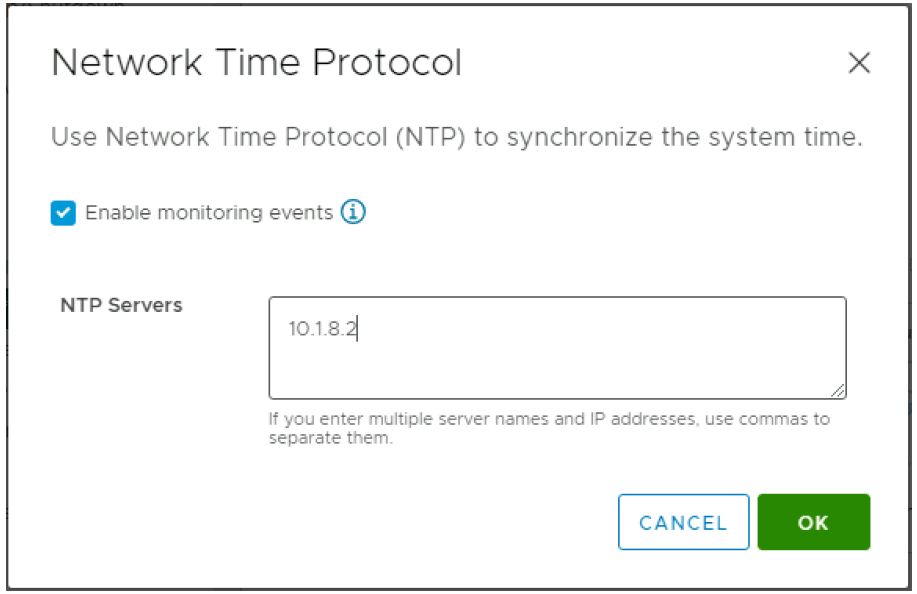
Re-run NCC password health check after changing the passwords

```
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
```

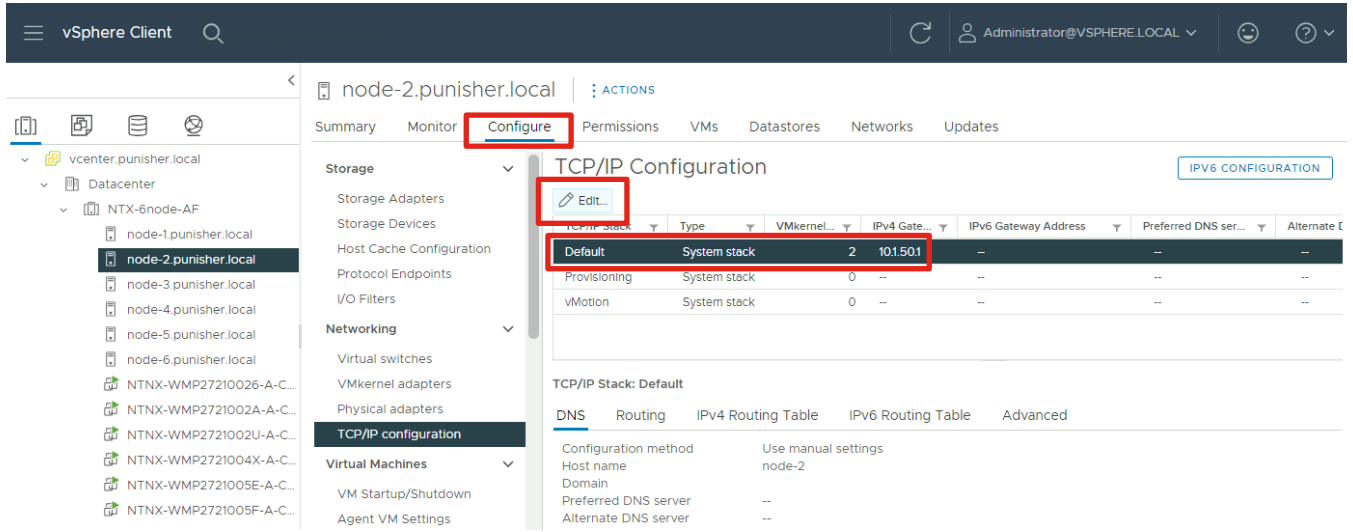
Enable NTP on ESXi hosts

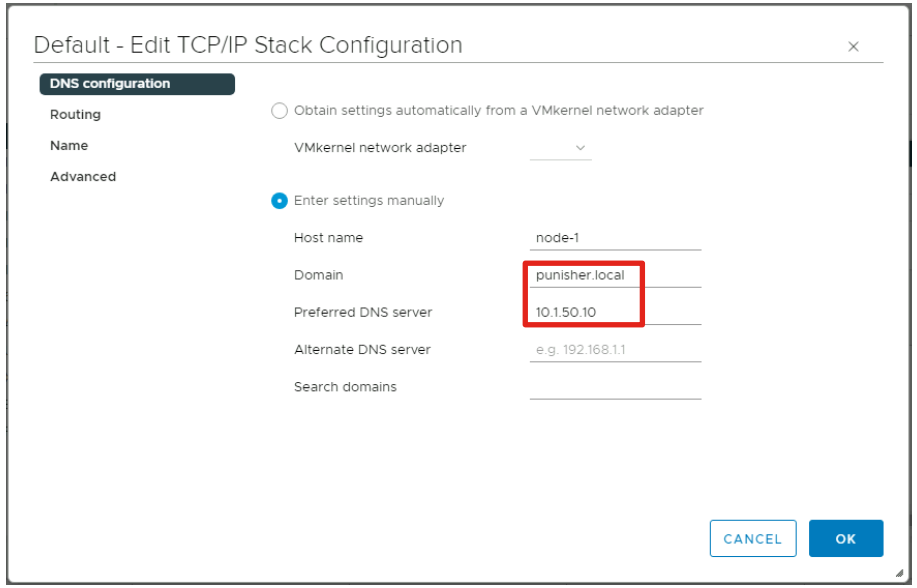




Repeat for each ESXi hypervisor host

Configure DNS on ESXi hosts

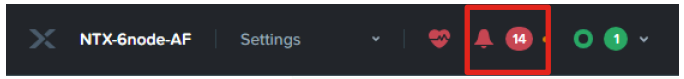




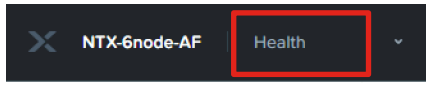
Repeat for each ESXi hypervisor host

Remediate all NCC Failures and Warnings

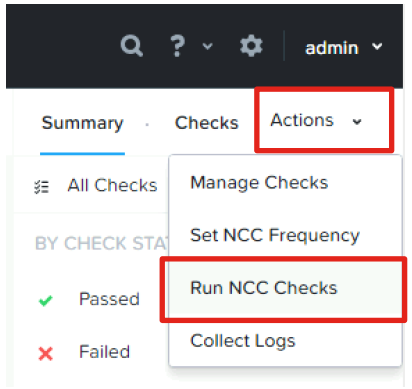
Resolve all active alerts



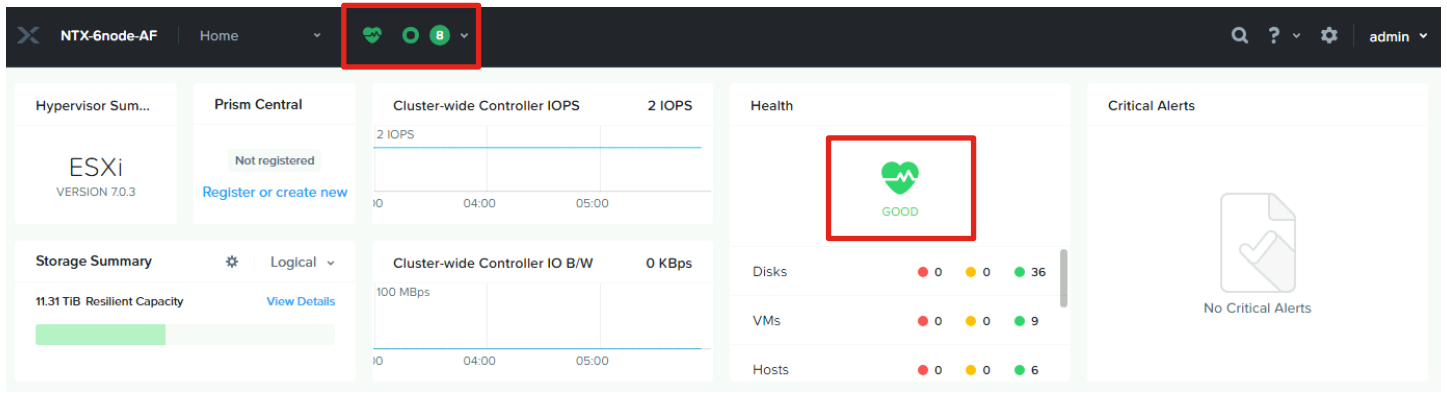
Go to Health

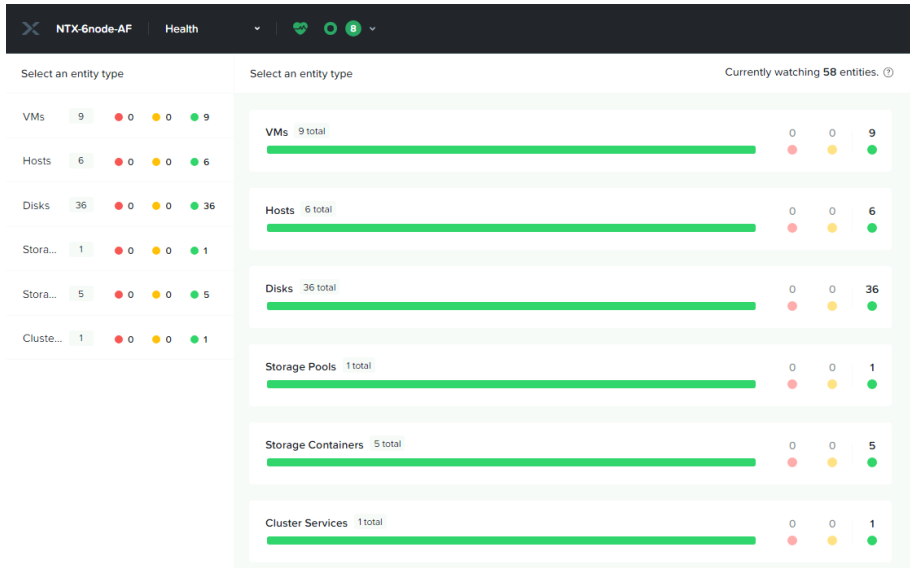


Run NCC checks



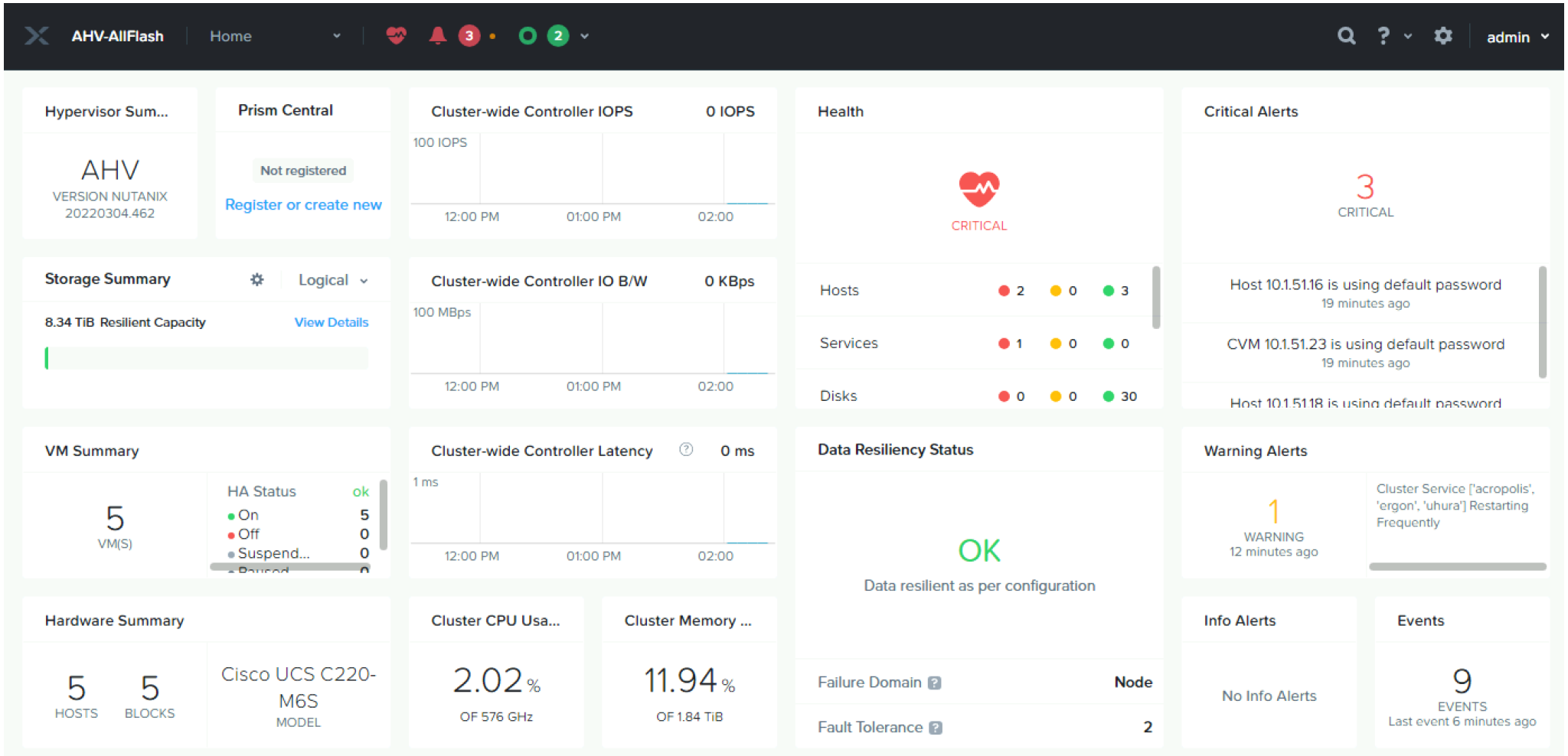
Remediate until all Alerts, Failures and Warnings are gone



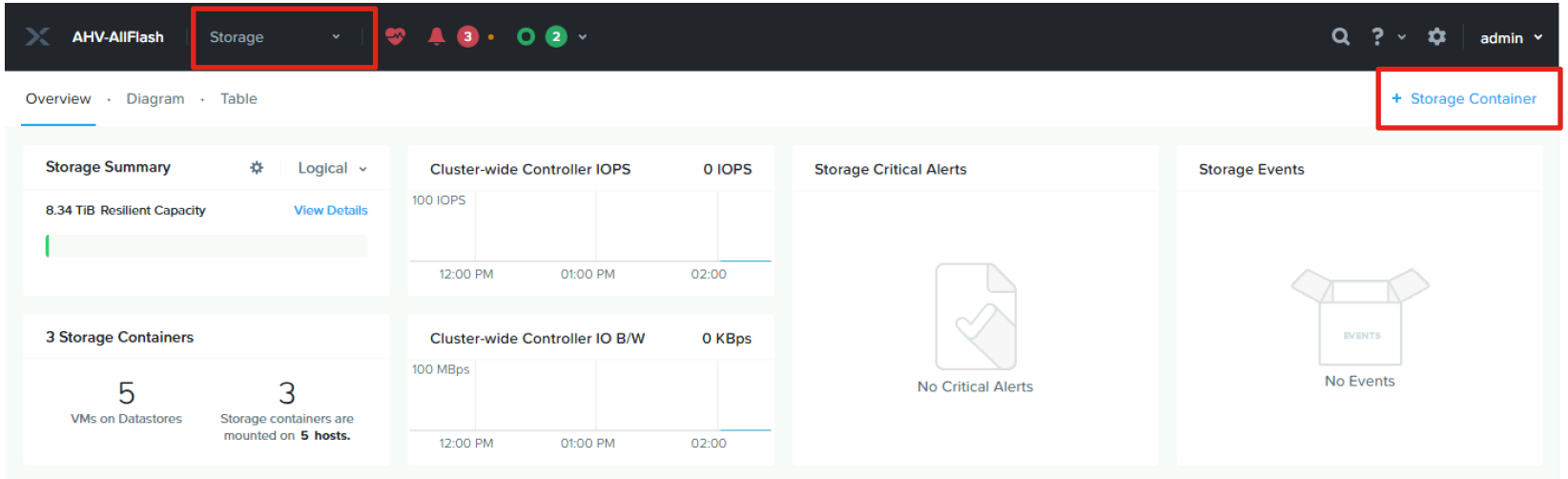


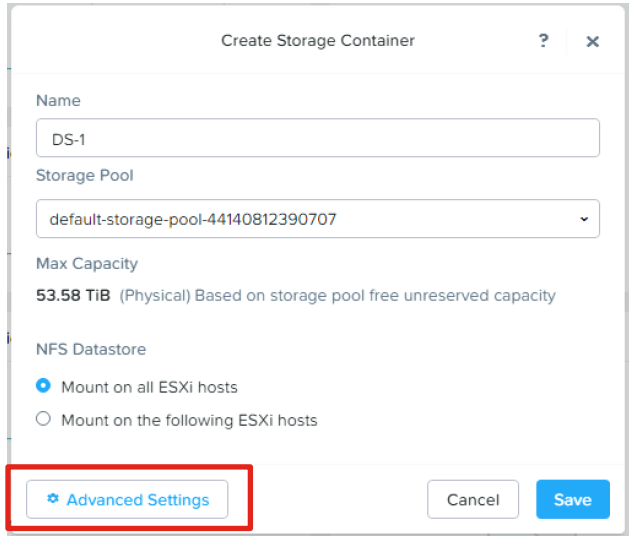
Initial Nutanix Cluster Config for AHV

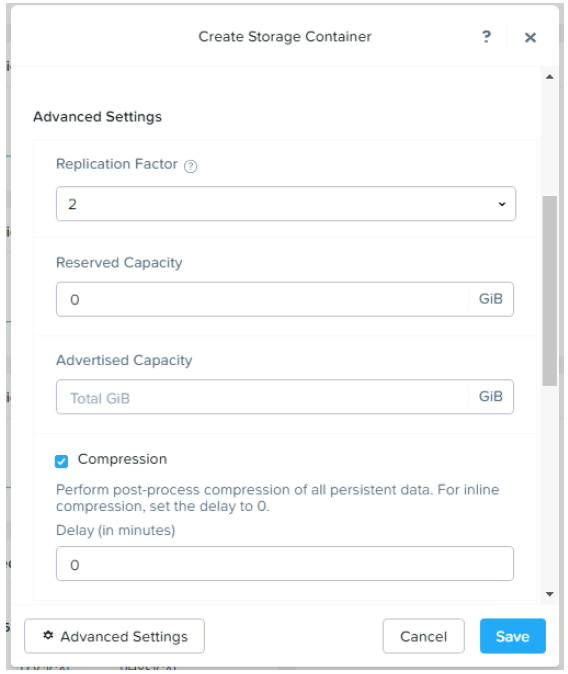
Prism Element Home

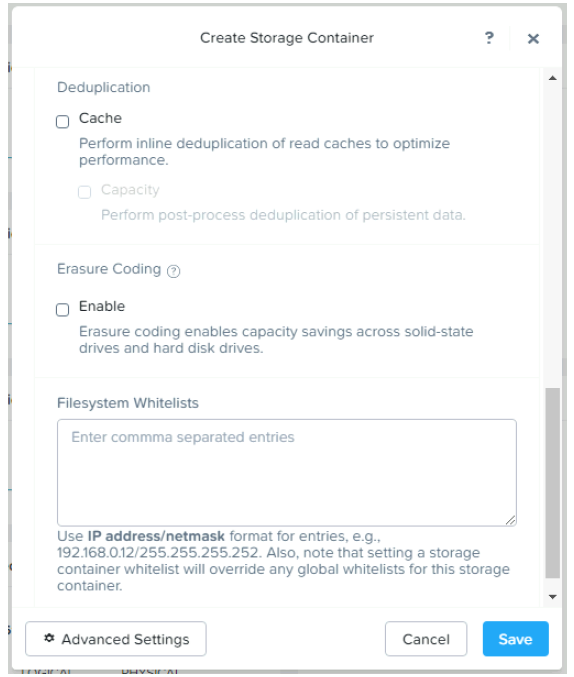


Create Storage Containers (Datastores)

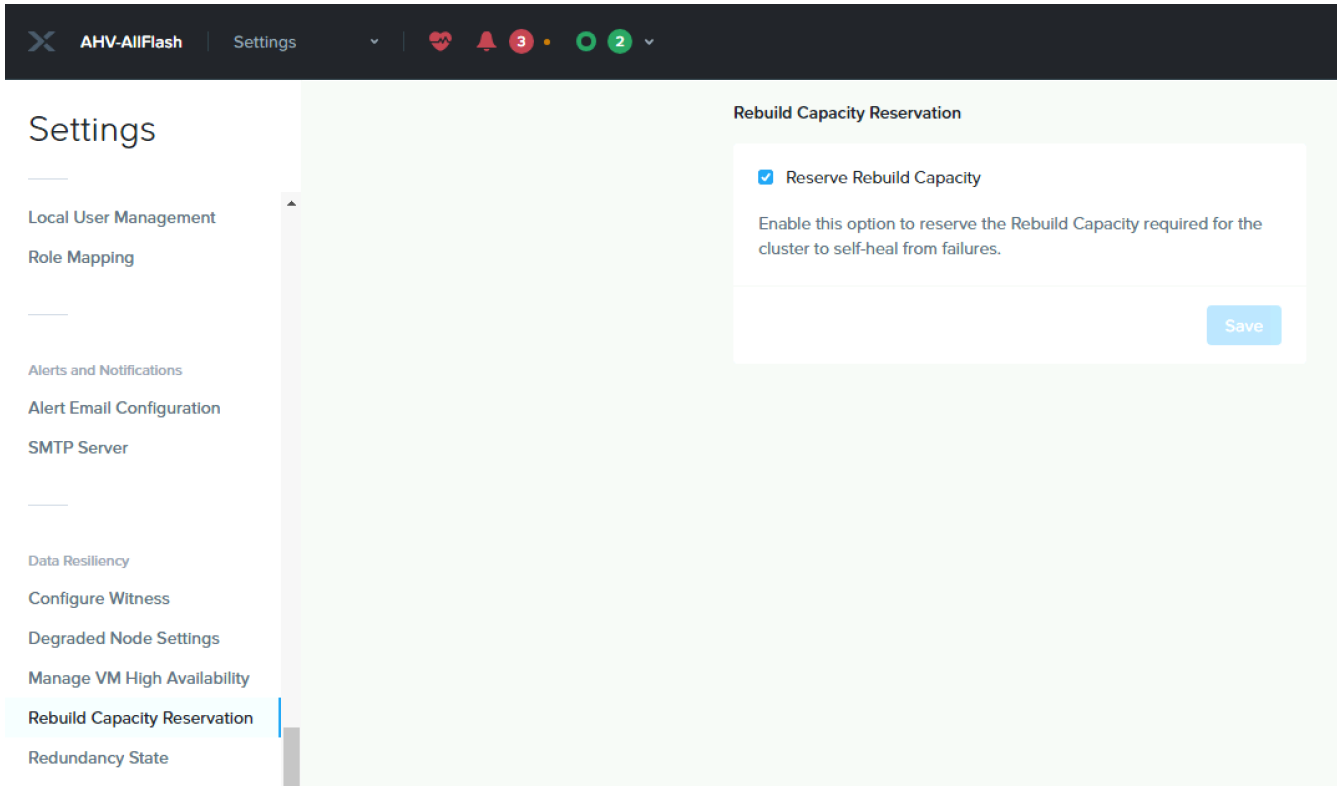


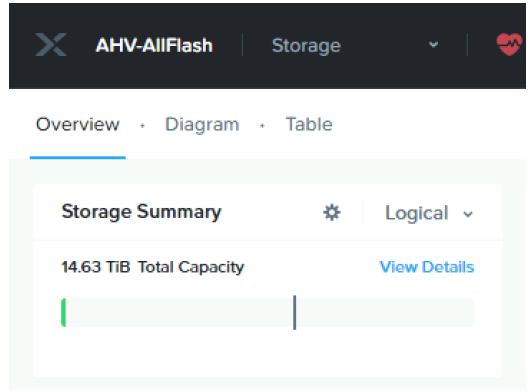




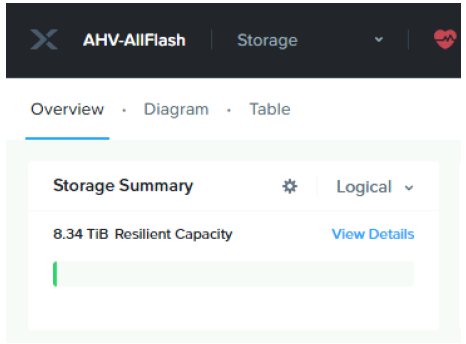


Set Rebuild Capacity Reservation



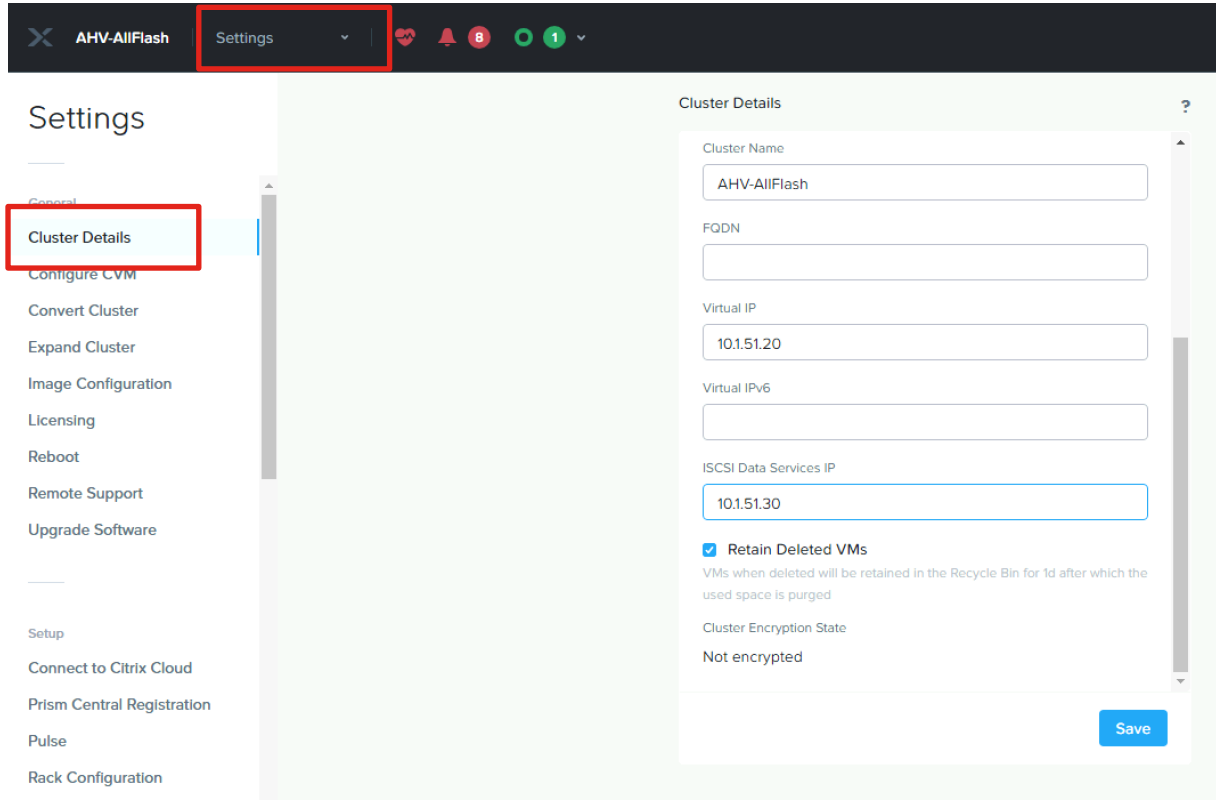


Without this setting enabled, cluster will accept incoming writes even if all blocks cannot completely heal during failures



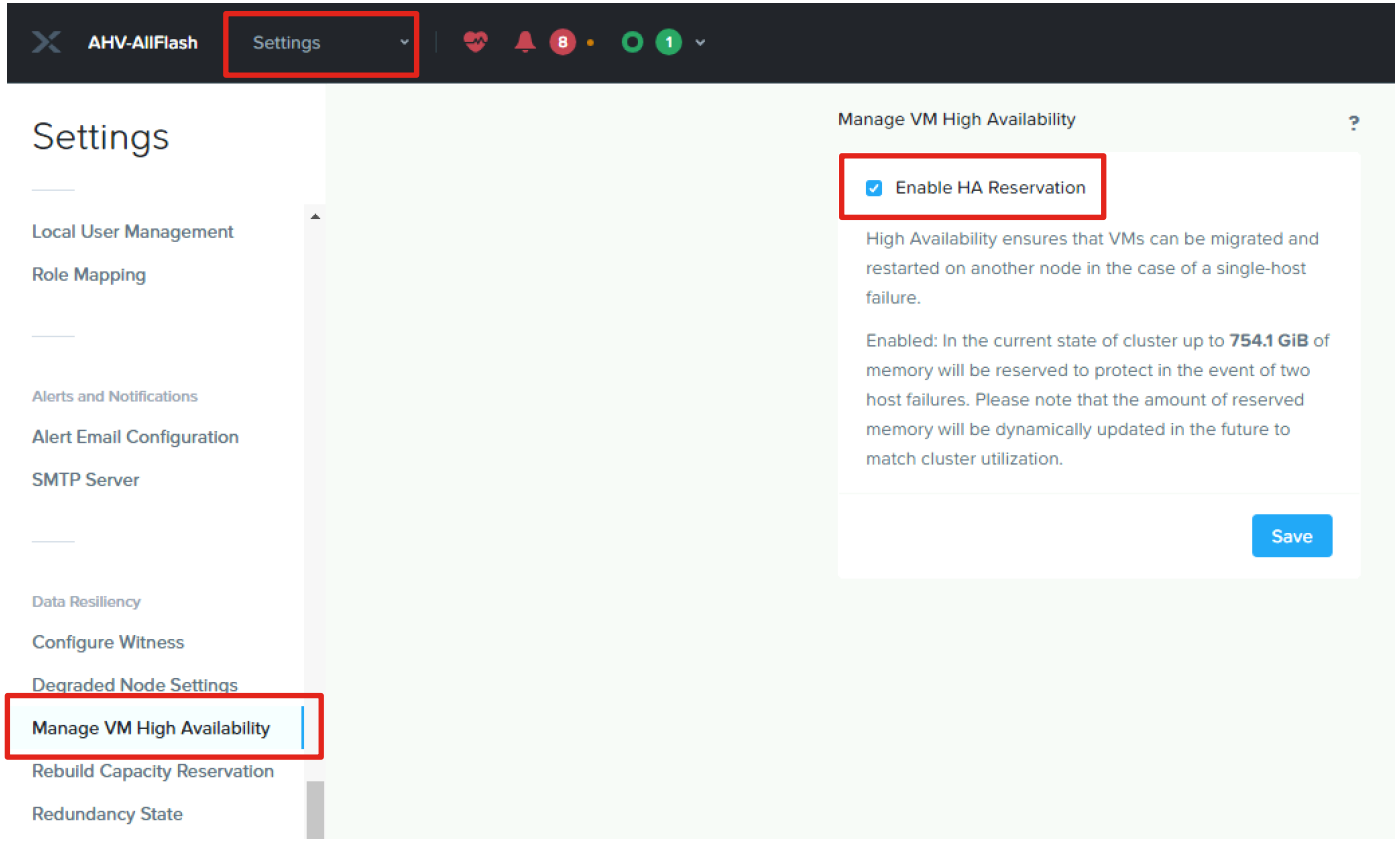
After enabling, cluster will refuse new writes if they cannot be fully protected during failures

Set ISCSI Data Services IP Address



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

Enable VM High Availability Reservation



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

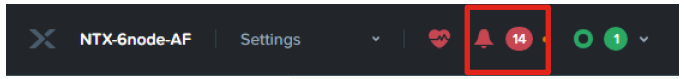
```
nutanix@NTNX-WMP27210026-A-CVM:10.1.50.21:~$ sudo passwd nutanix
Changing password for user nutanix.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Re-run NCC password health check after changing the passwords

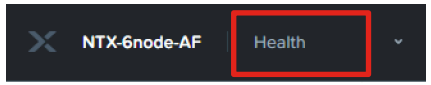
```
nutanix@NTNX-WMP27210026-A-CVM:10.1.50.21:~$ ncc health_checks
system_checks default_password_check
```

Remediate all NCC Failures and Warnings

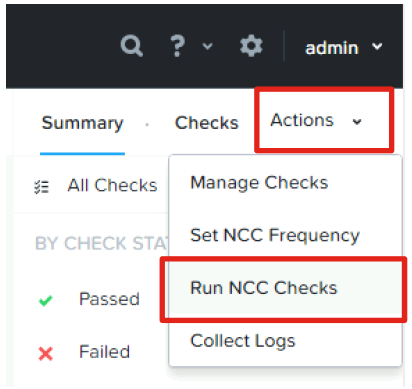
Resolve all active alerts



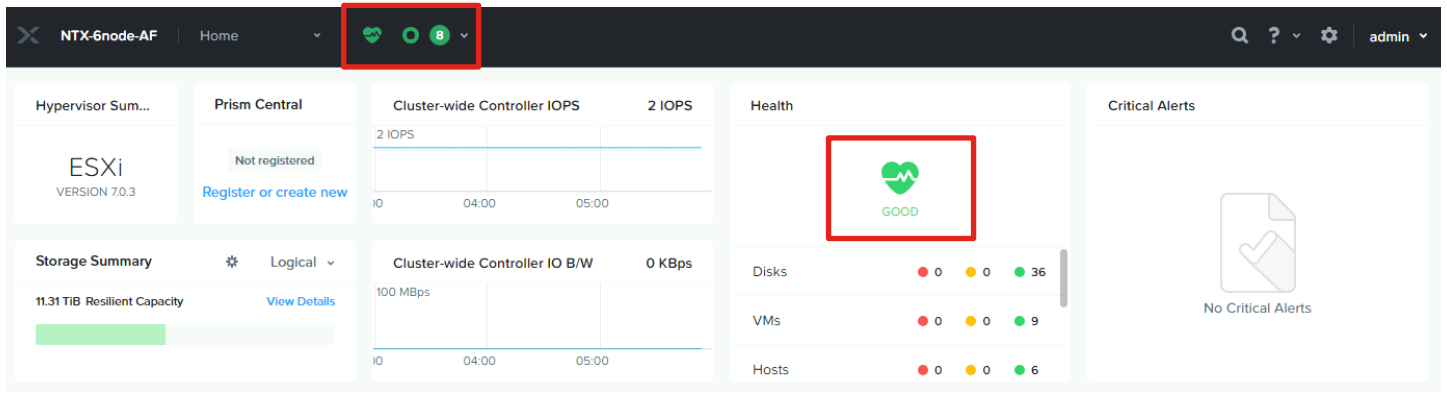
Go to Health

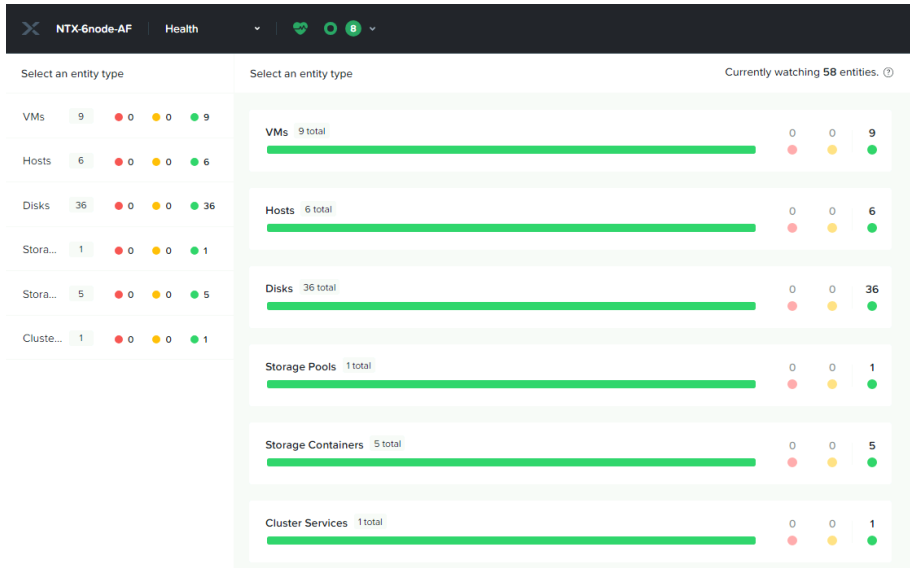


Run NCC checks



Remediate until all Alerts, Failures and Warnings are gone



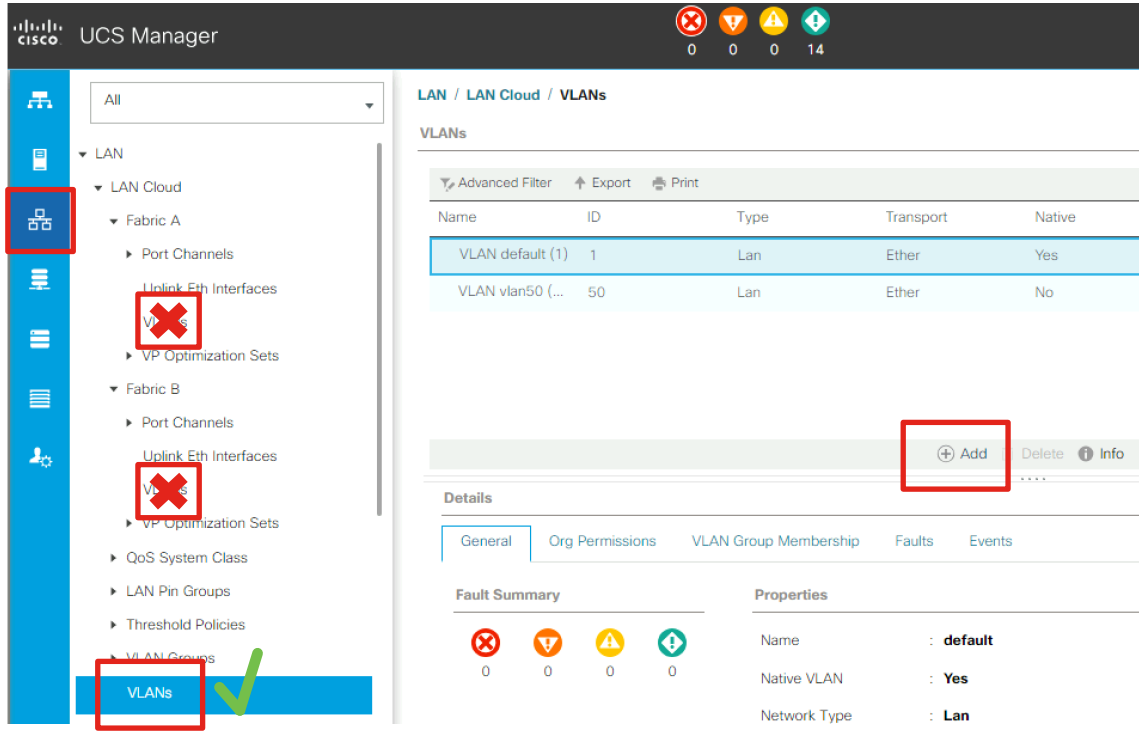


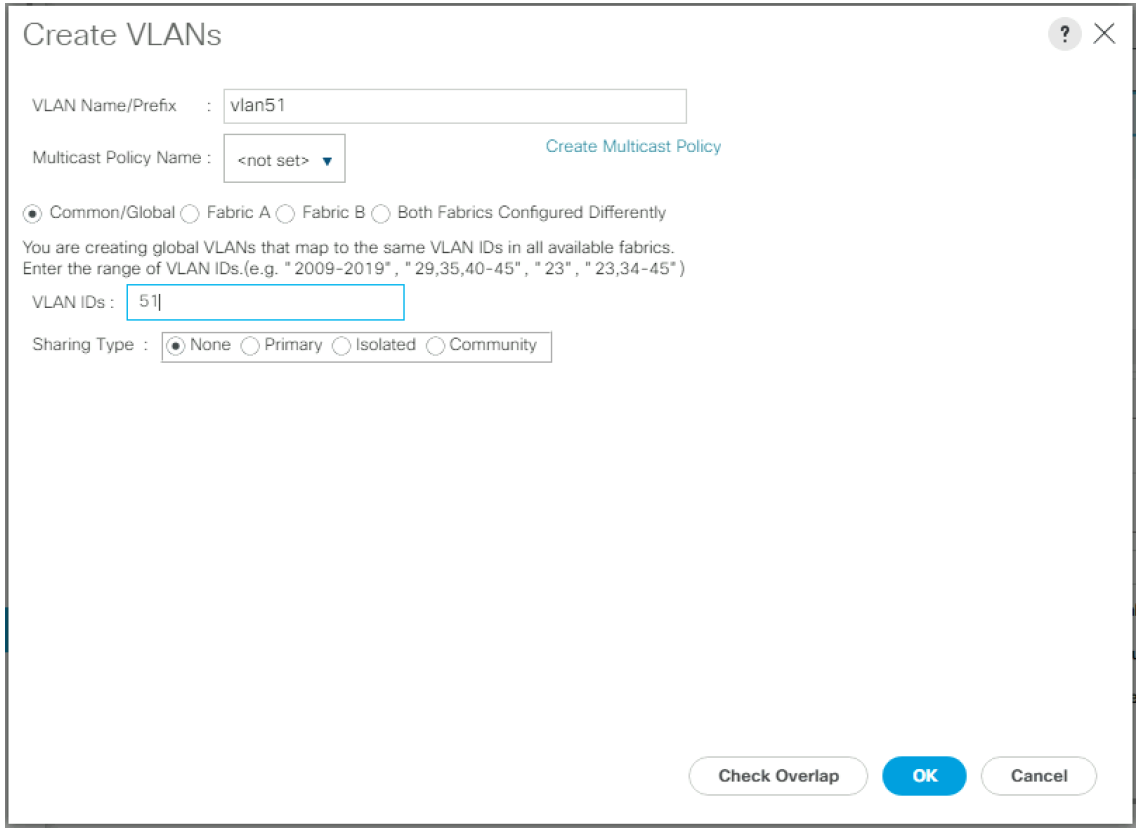
Guest VM Networking

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

Configure Guest VM Networking for ESXi

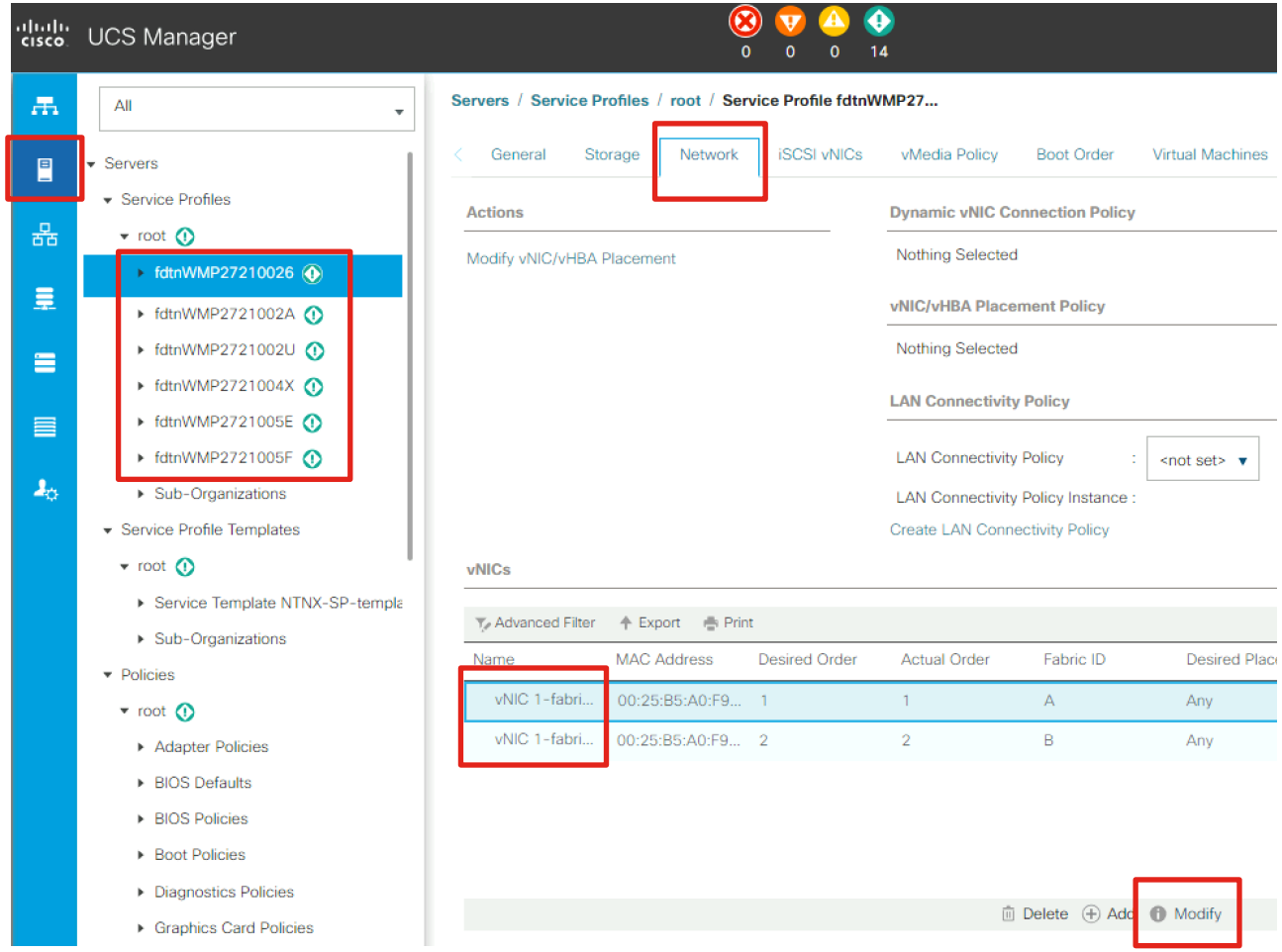
Add VLANs in UCS Manager

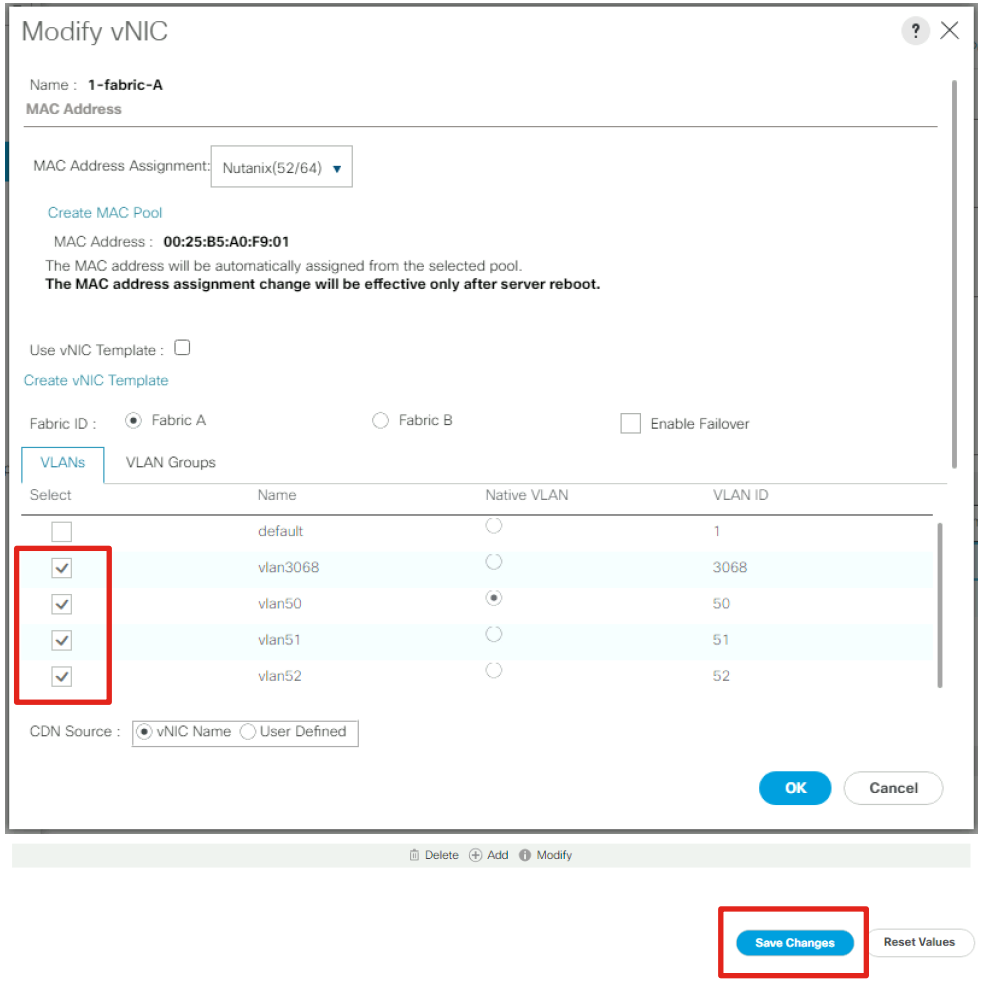




Create additional VLANs in UCS Manager for guest VMs, if not already created earlier

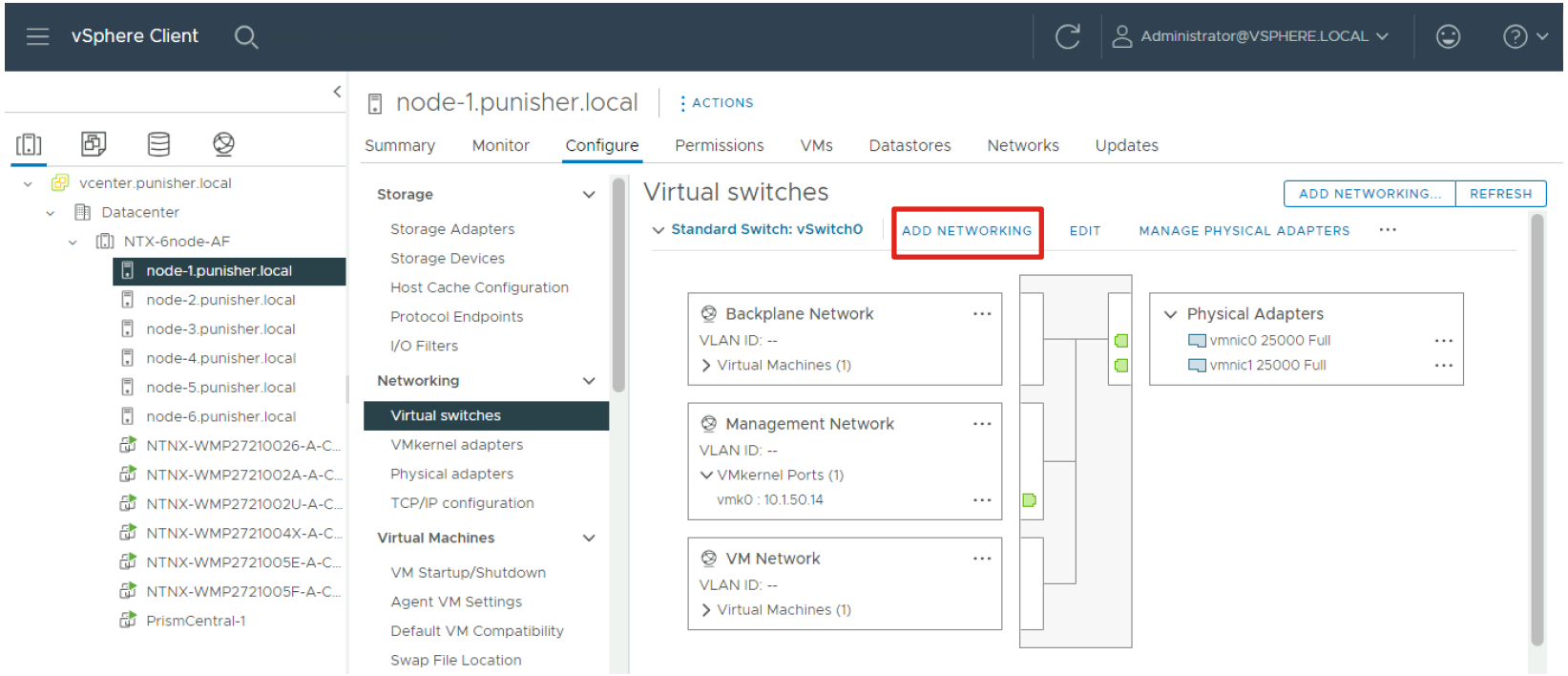
Add VLAN(s) to Nutanix Host vNICs

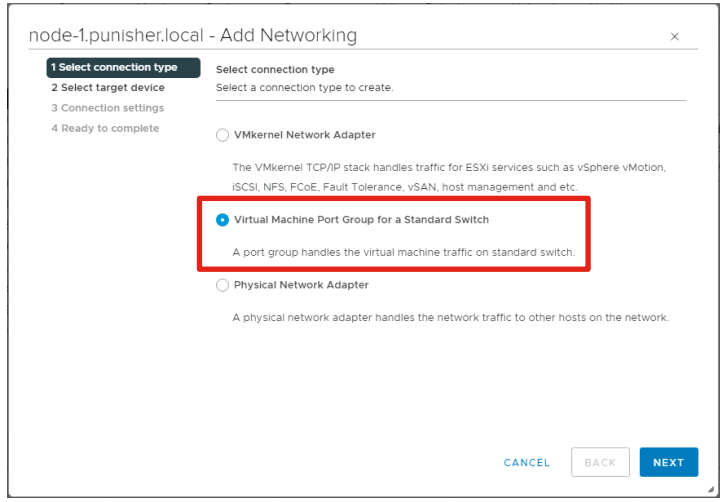


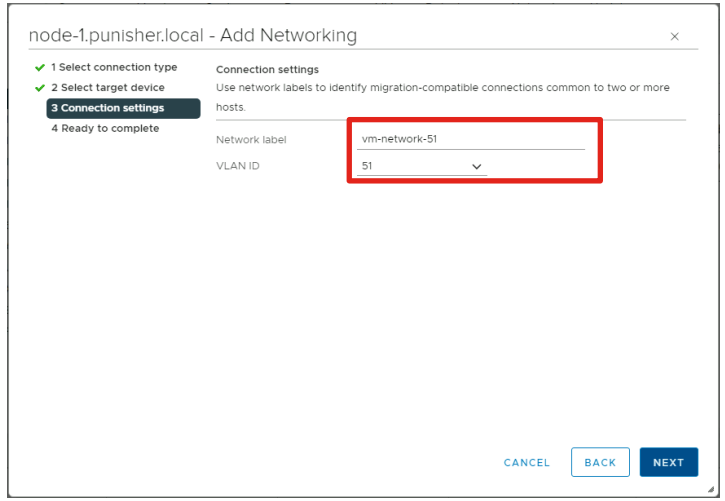


Add VLANs to the vNICs of the Nutanix service profiles. New VLANs must be non-native (i.e. tagged), while the original VLAN used during installation is native. Modify both vNICs in the service profile and save changes. Repeat for all vNICs in all the service profiles.

Create New Port Groups in vCenter



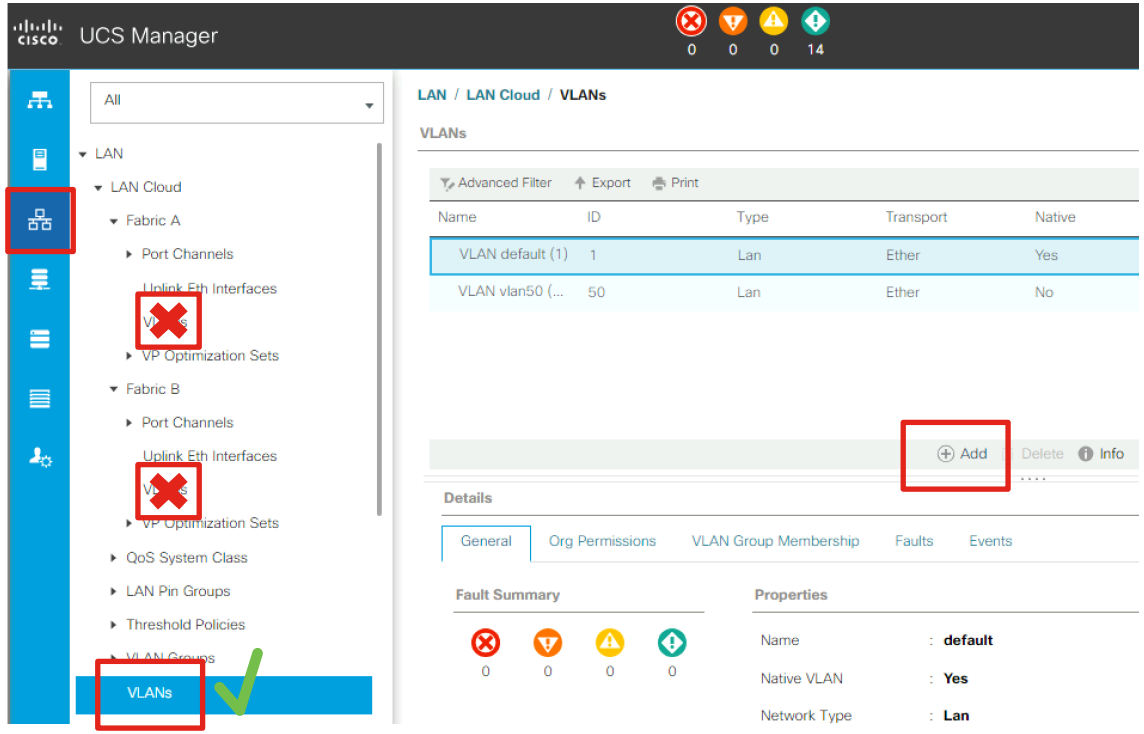


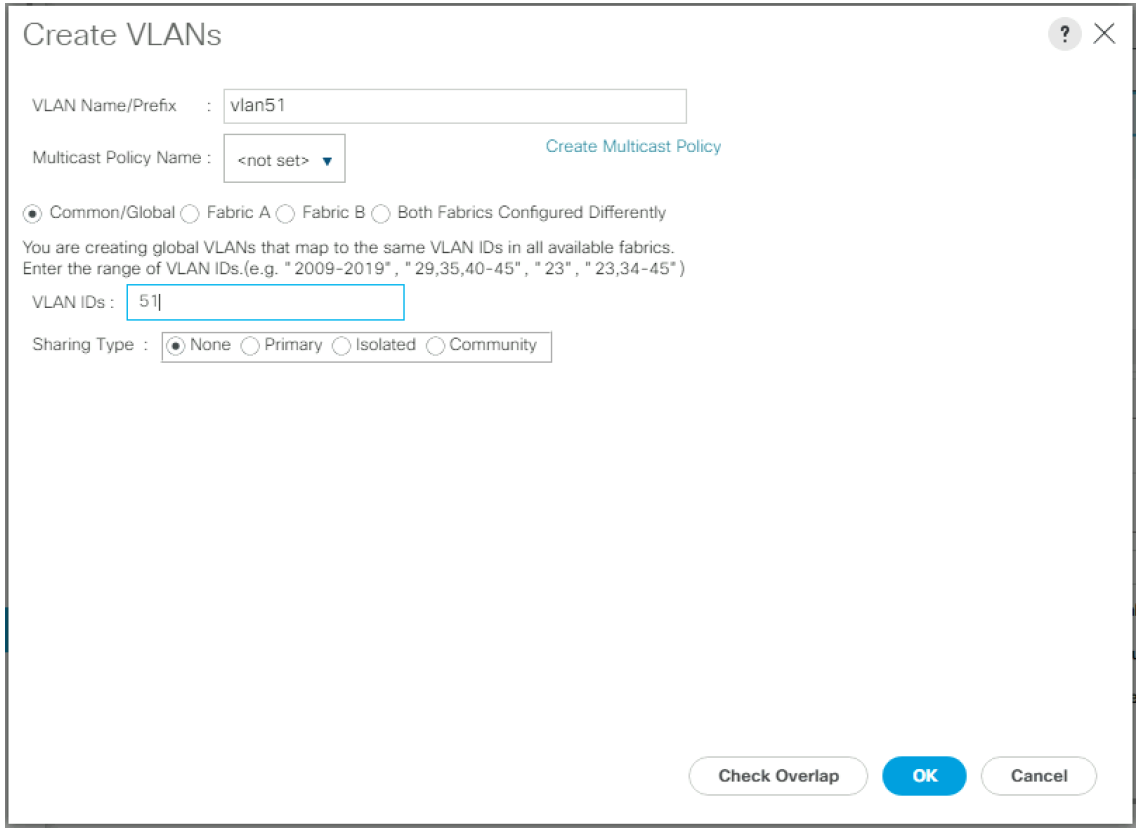


Add a new port group to the default vSwitch0 for the guest VMs, using VLAN ID tags. Repeat for each VLAN required and repeat for all the hosts in the vCenter cluster so their configuration matches.

Configure Guest VM Networking for AHV

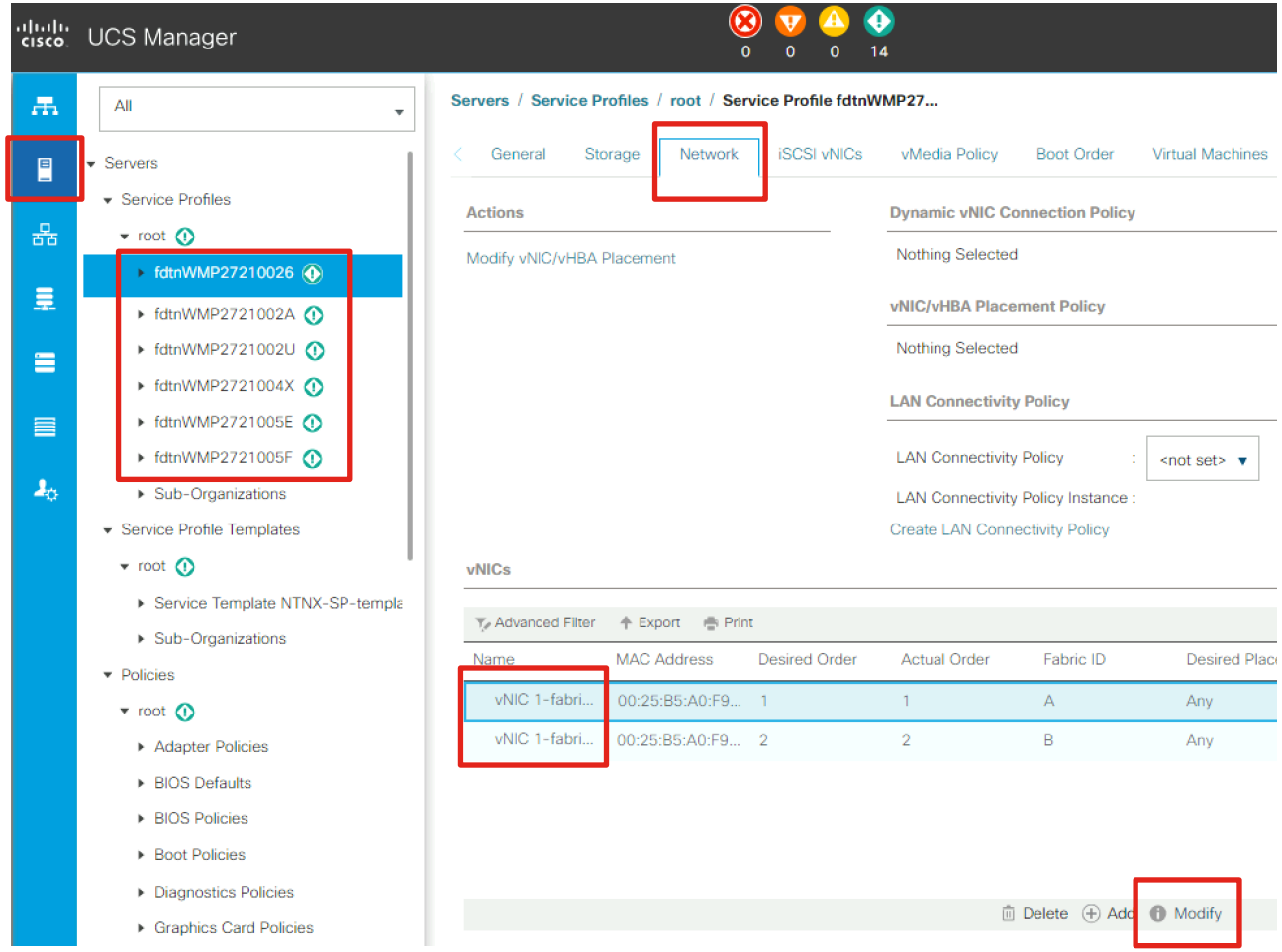
Add VLANs in UCS Manager

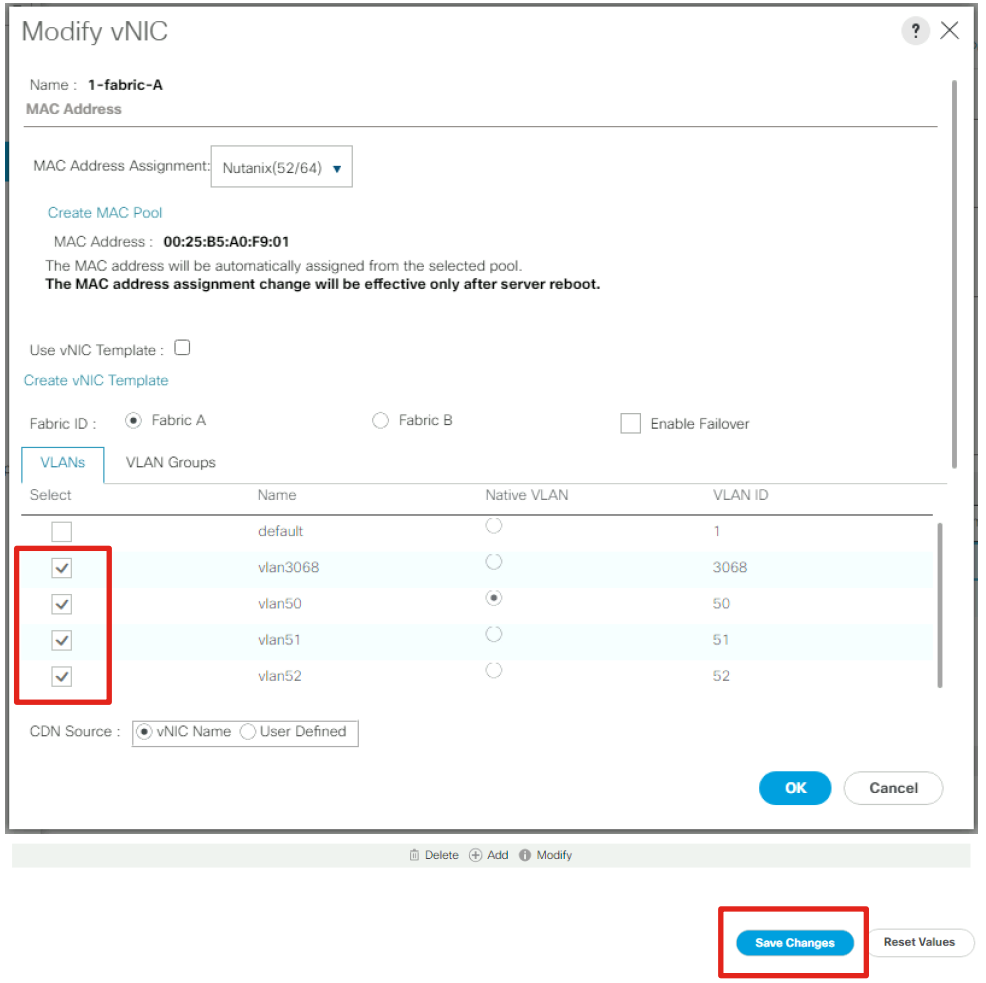




Create additional VLANs in UCS Manager for guest VMs, if not already created earlier

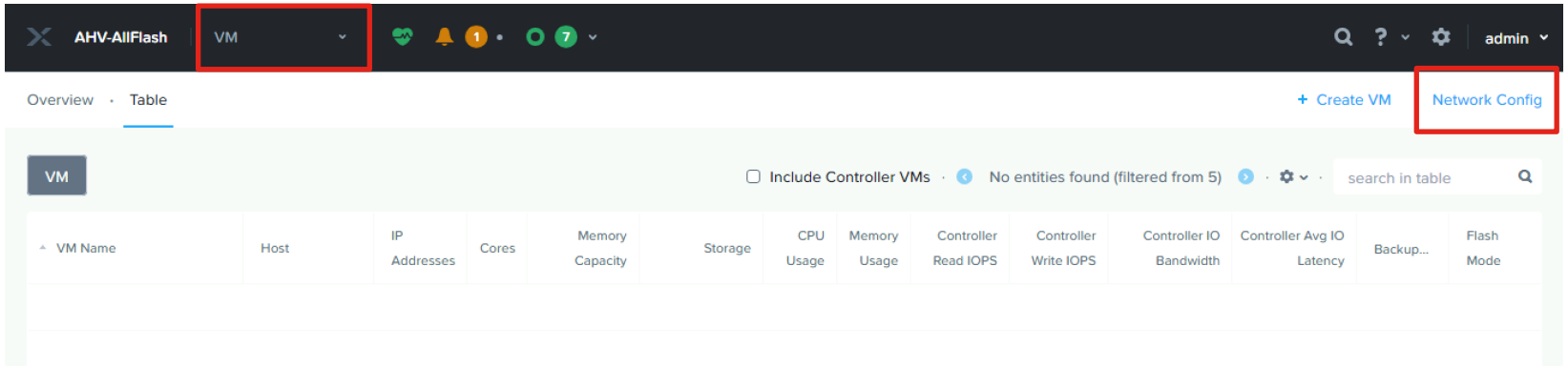
Add VLAN(s) to Nutanix Host vNICs

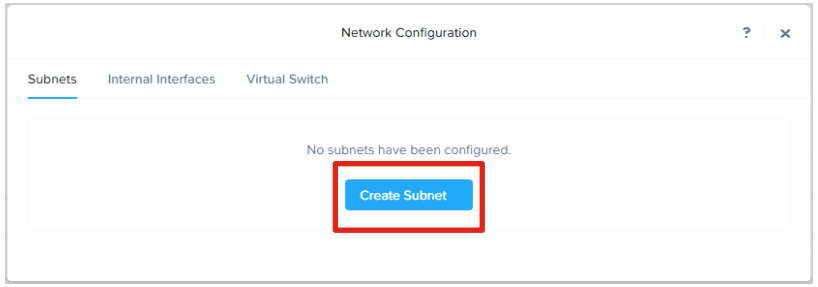


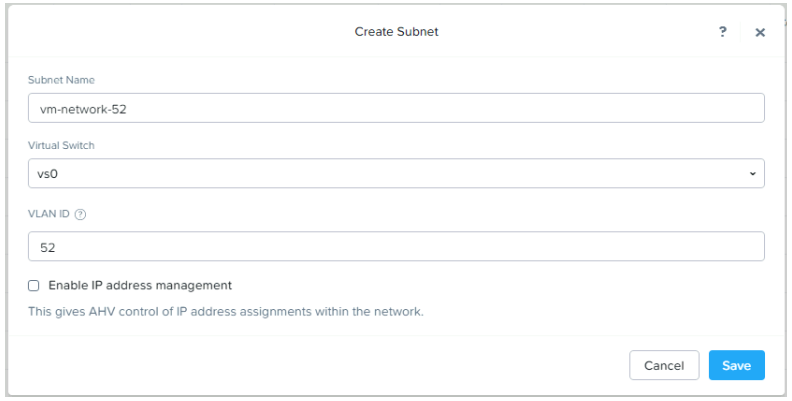


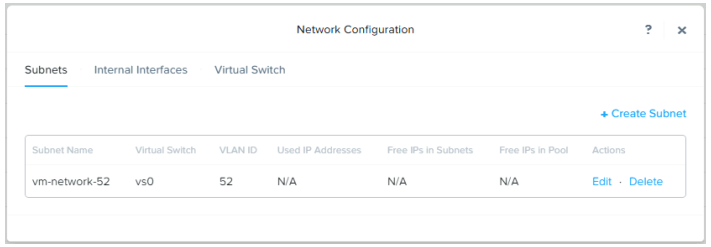
Add VLANs to the vNICs of the Nutanix service profiles. New VLANs must be non-native (i.e. tagged), while the original VLAN used during installation is native. Modify both vNICs in the service profile and save changes. Repeat for all vNICs in all the service profiles.

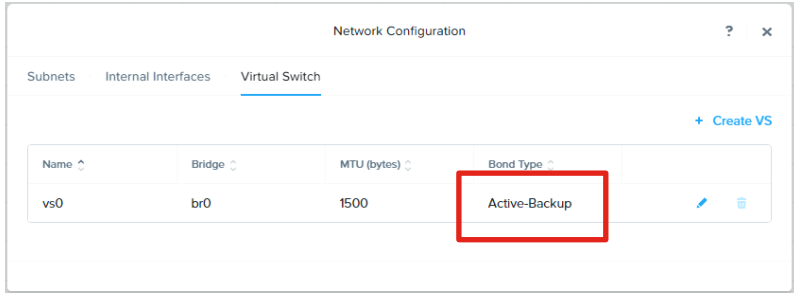
Create VM Subnet(s)







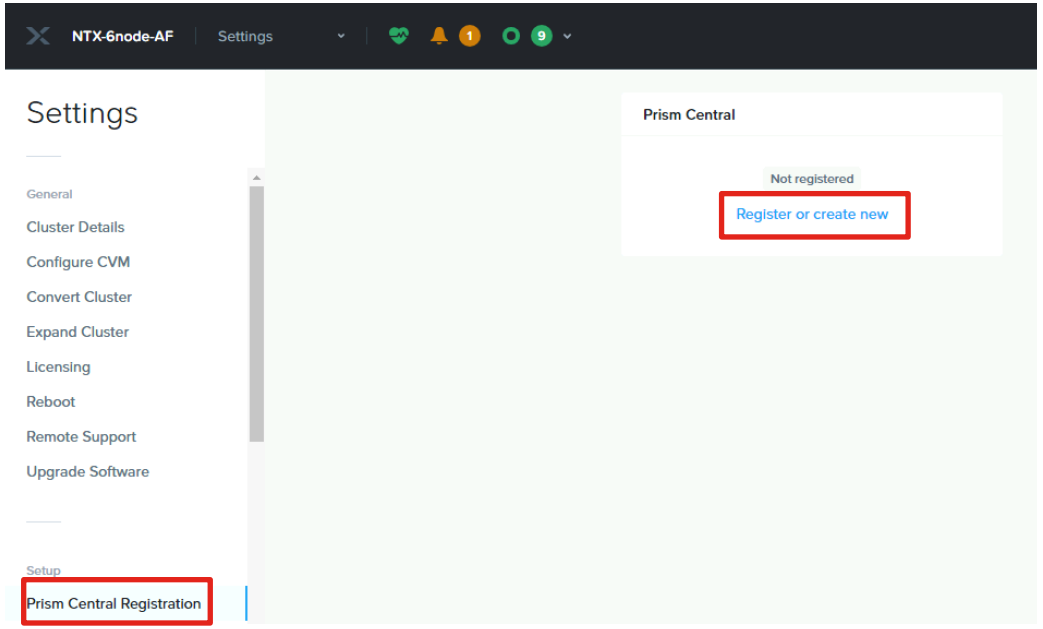


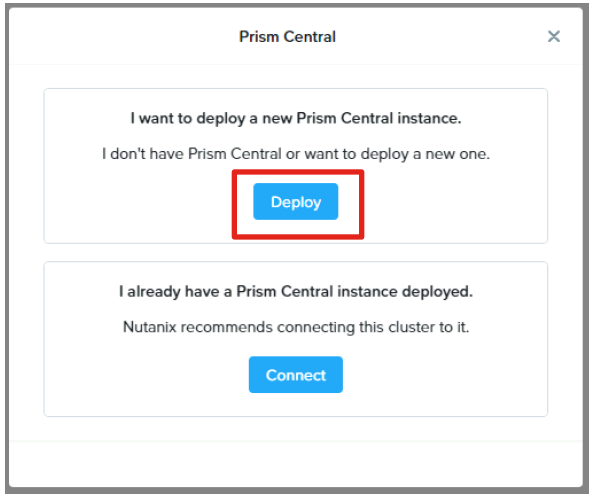


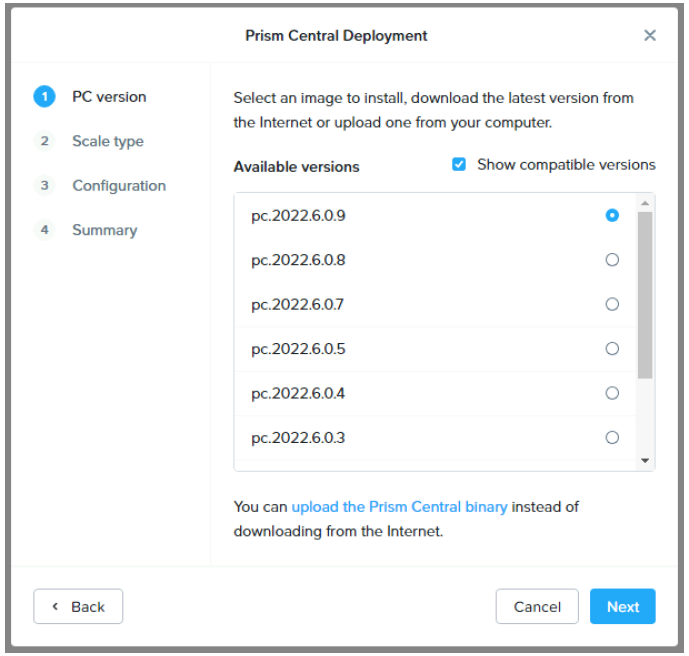
Note: Do not modify the default virtual switch bond type to Active-Active. This requires LACP and will not work within Cisco UCS domains.

Prism Central Installation

Start Prism Central Installation

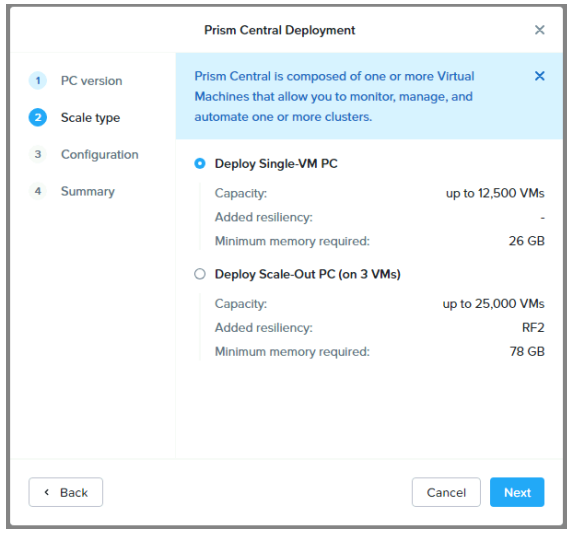


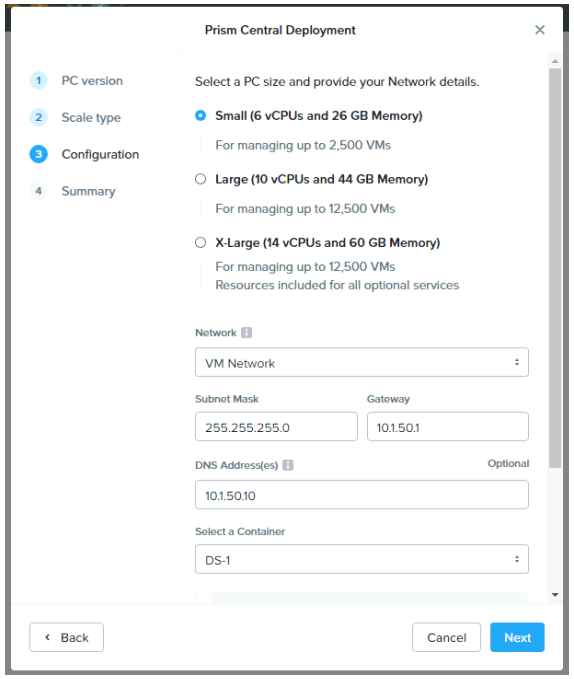


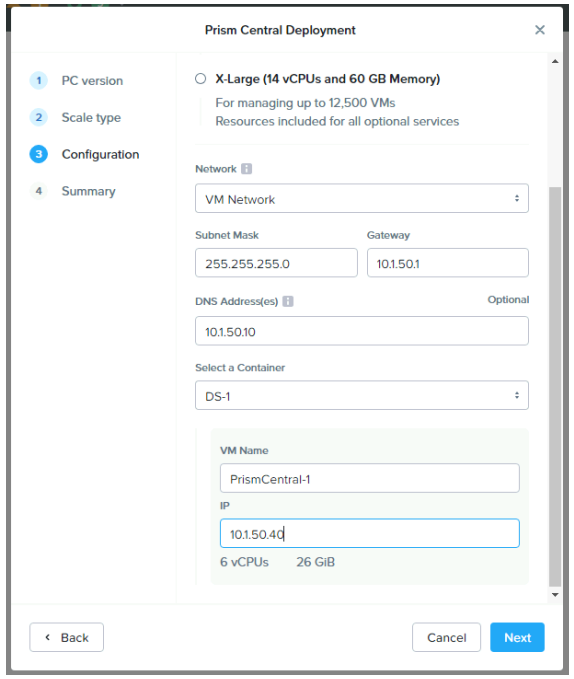


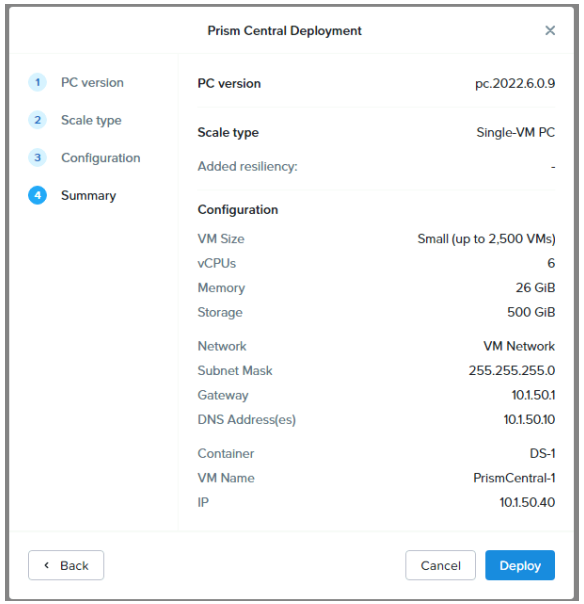
Take extra care when deploying a new Prism Central VM or cluster. Prism Central binaries can be downloaded here: https://portal.nutanix.com/page/downloads?product=prism This page also lists some compatibility information, for example, version 2022.9 or later can only be newly deployed on AOS 6.6 or later. If you were to attempt to upload this Prism Central binary for a new deployment on AOS 6.5 LTS, the install will fail. 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

Start Prism Central Installation continued

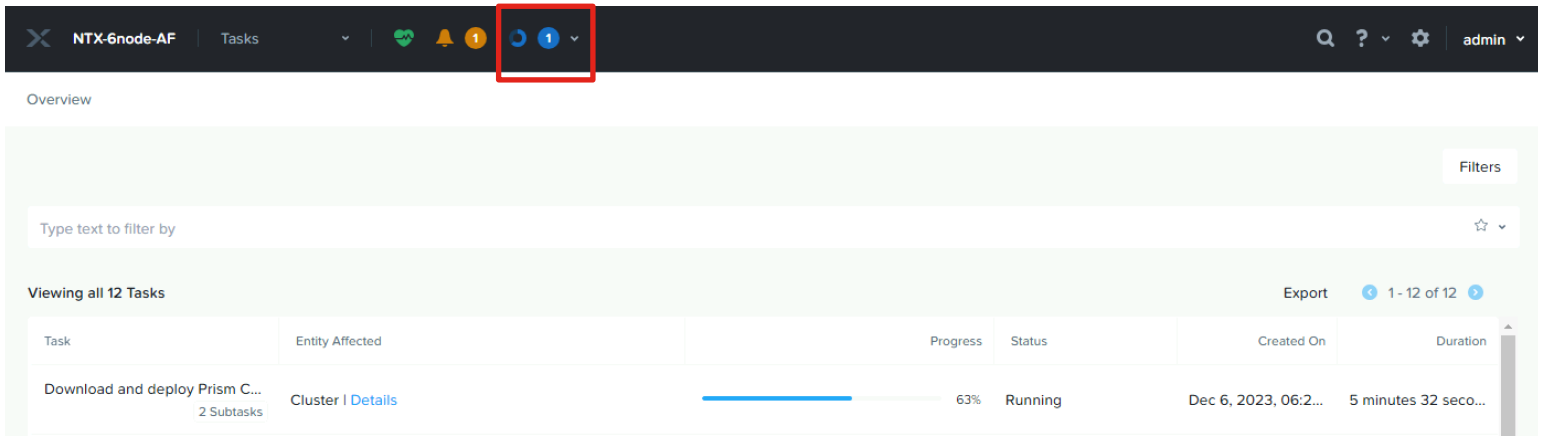




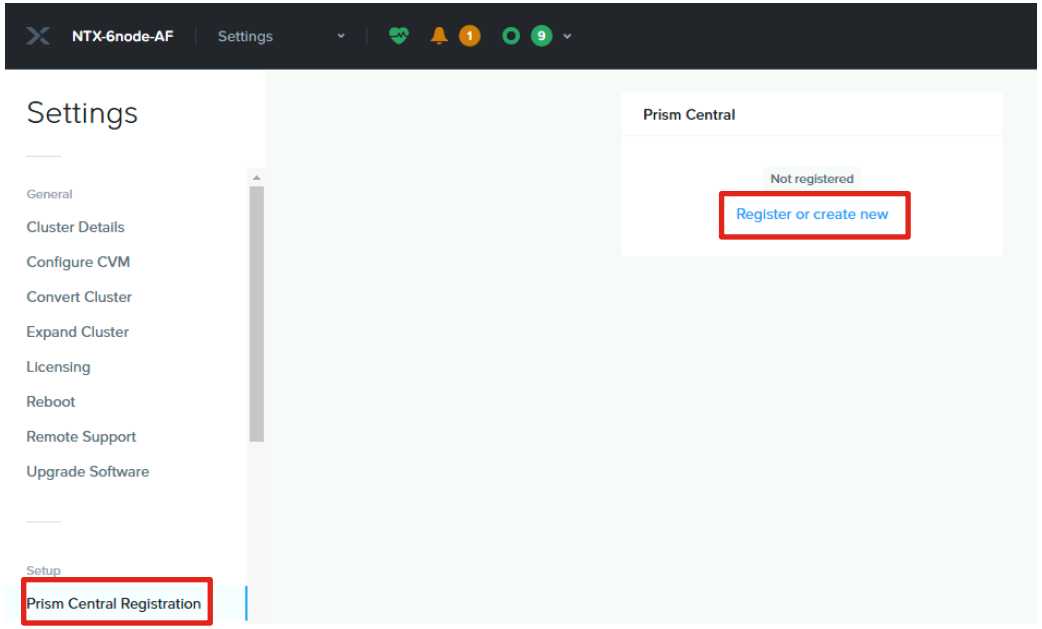


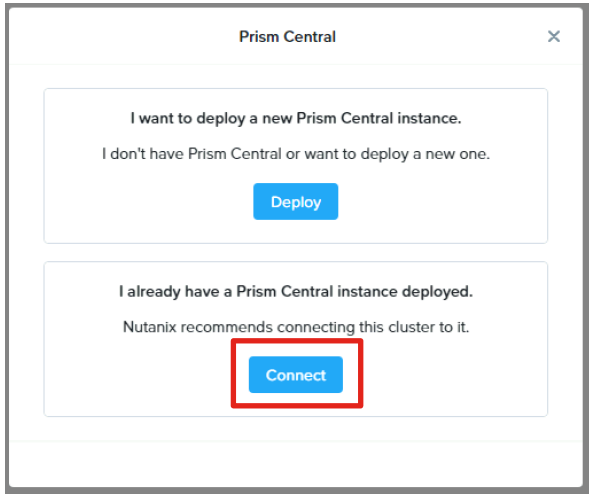


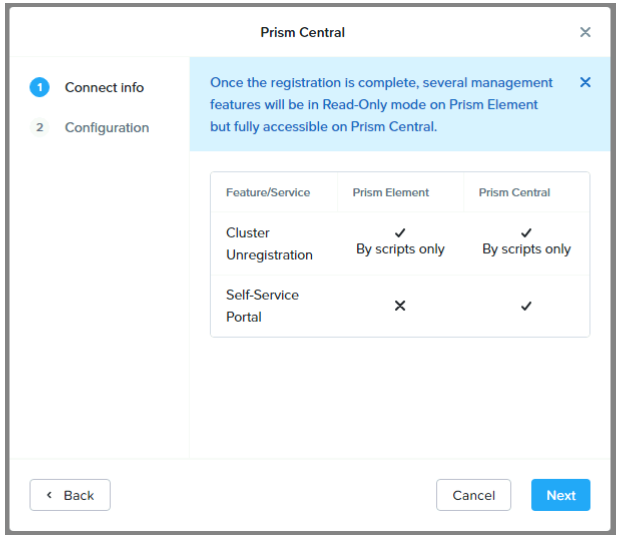
Note:
Deployment can take 30+ minutes

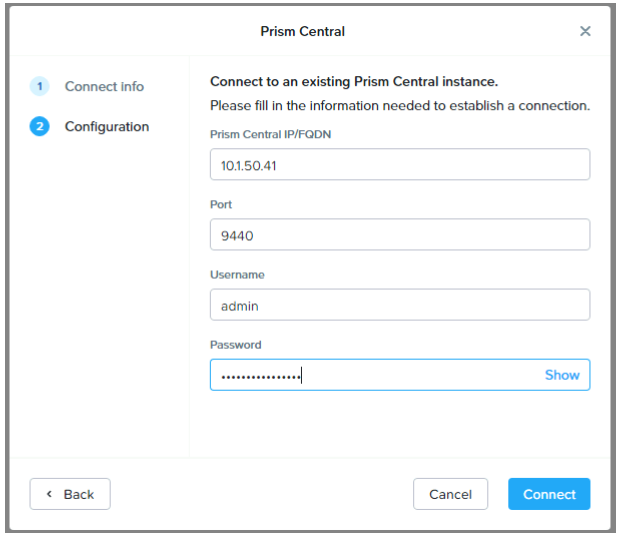


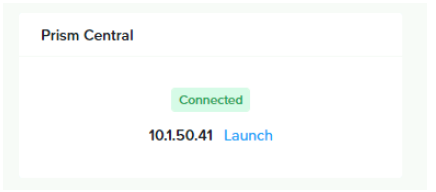
Register Cluster with Prism Central



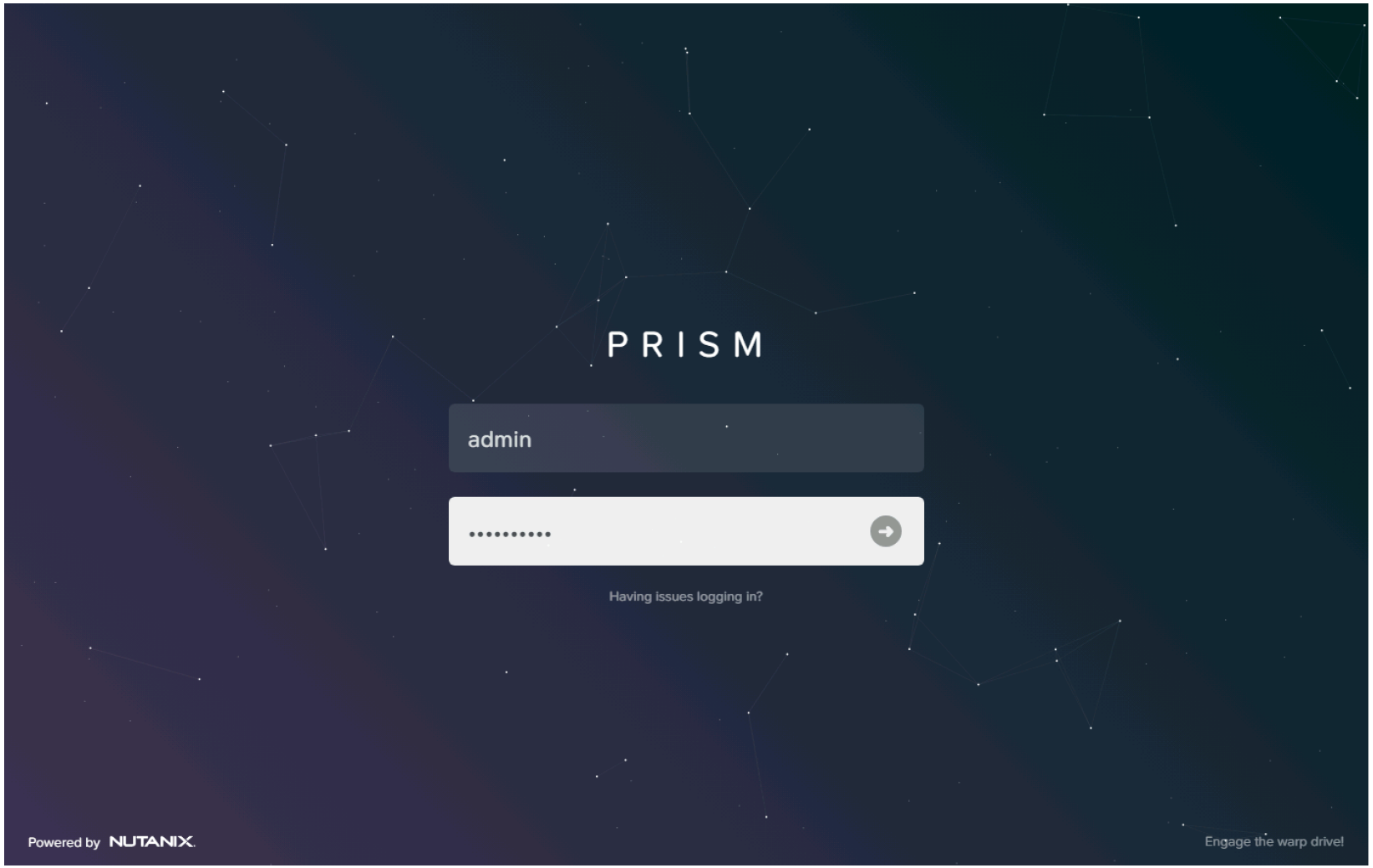






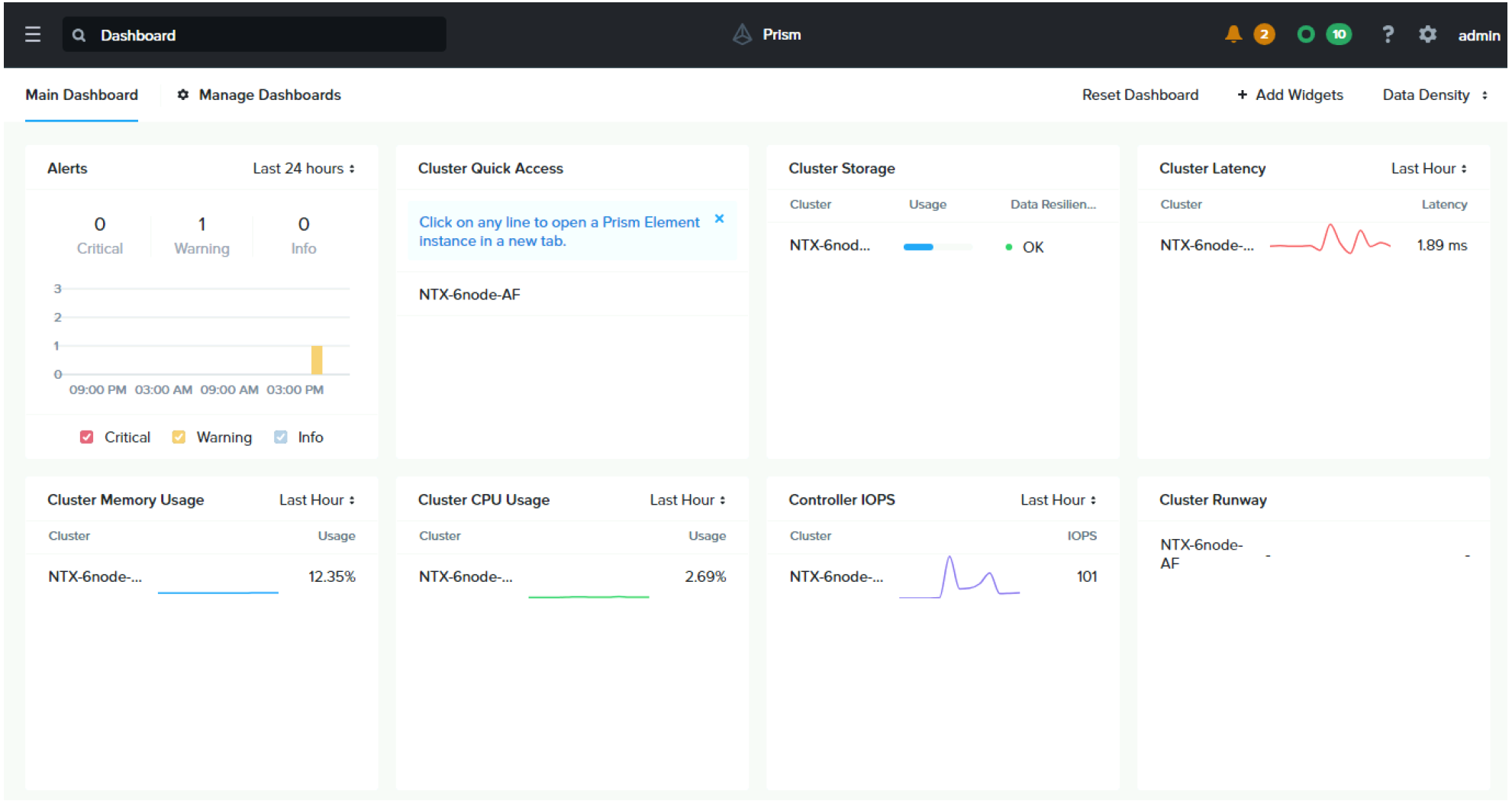


Access Prism Central

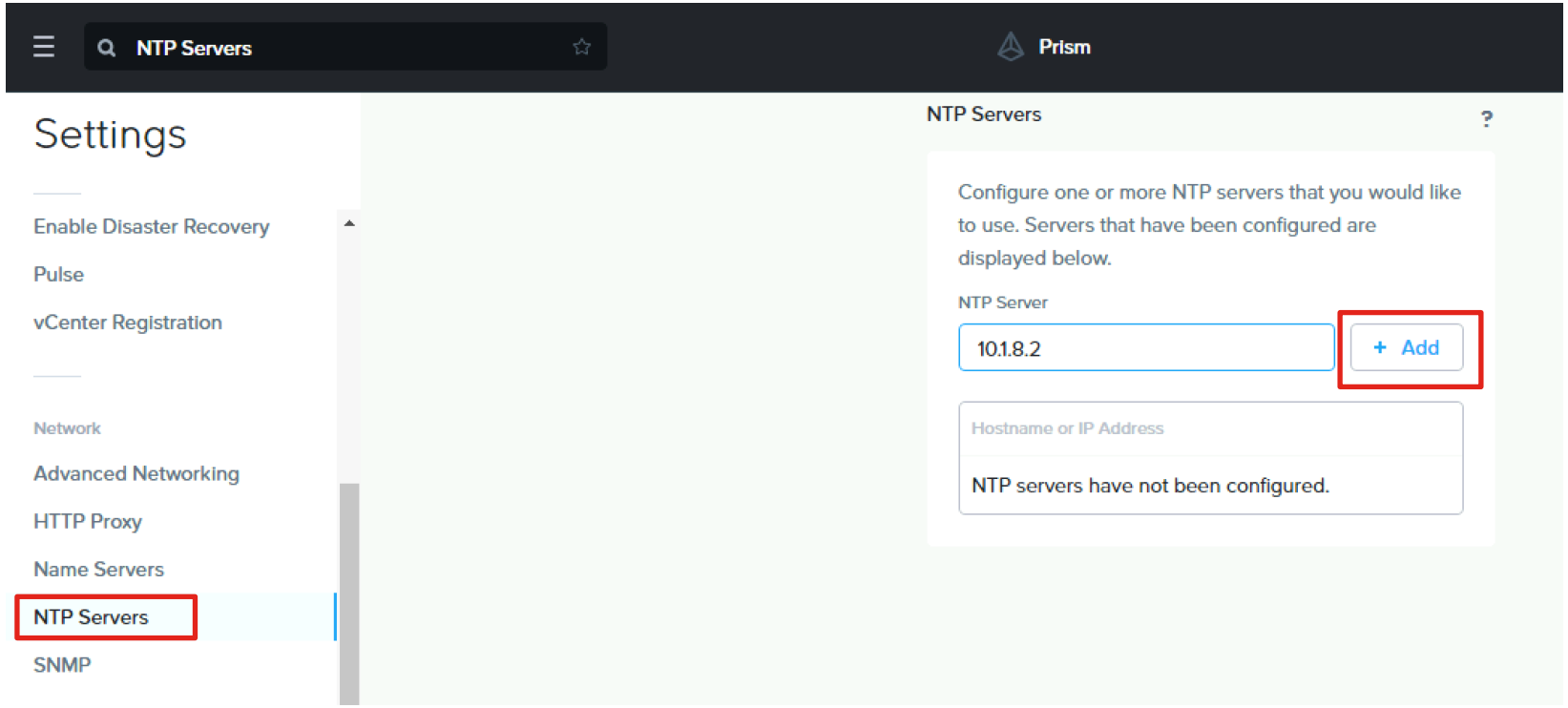


- Access Prism Central at the VM or cluster IP address, using HTTPS at port 9440
- Default username: admin
- Default password: Nutanix/4u
- Password must be changed on first login

Prism Central Dashboard

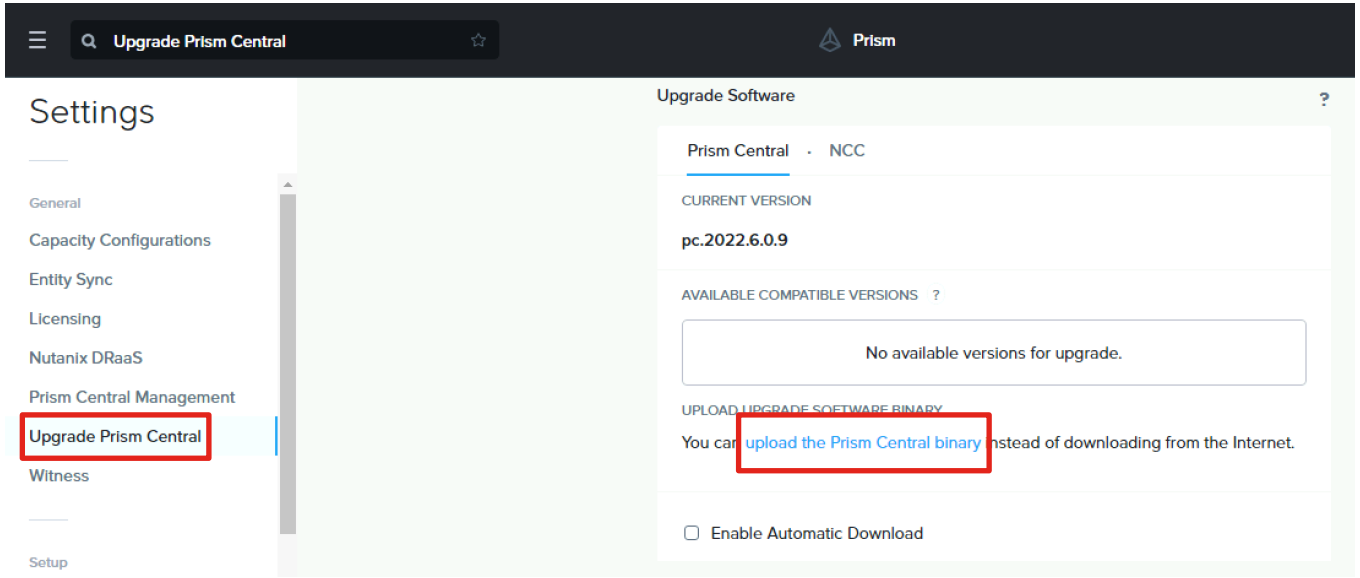


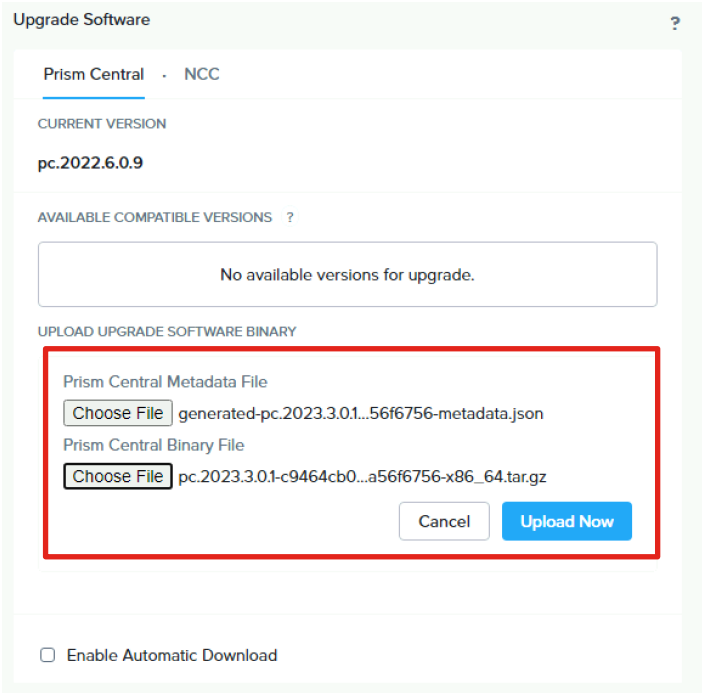
Configure NTP in Prism Central



Prism Central cannot be upgraded without DNS and NTP configured

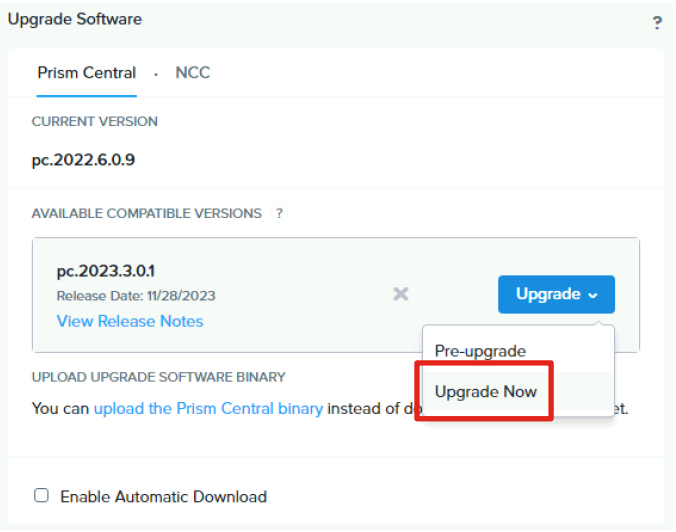
Prism Central Upgrade



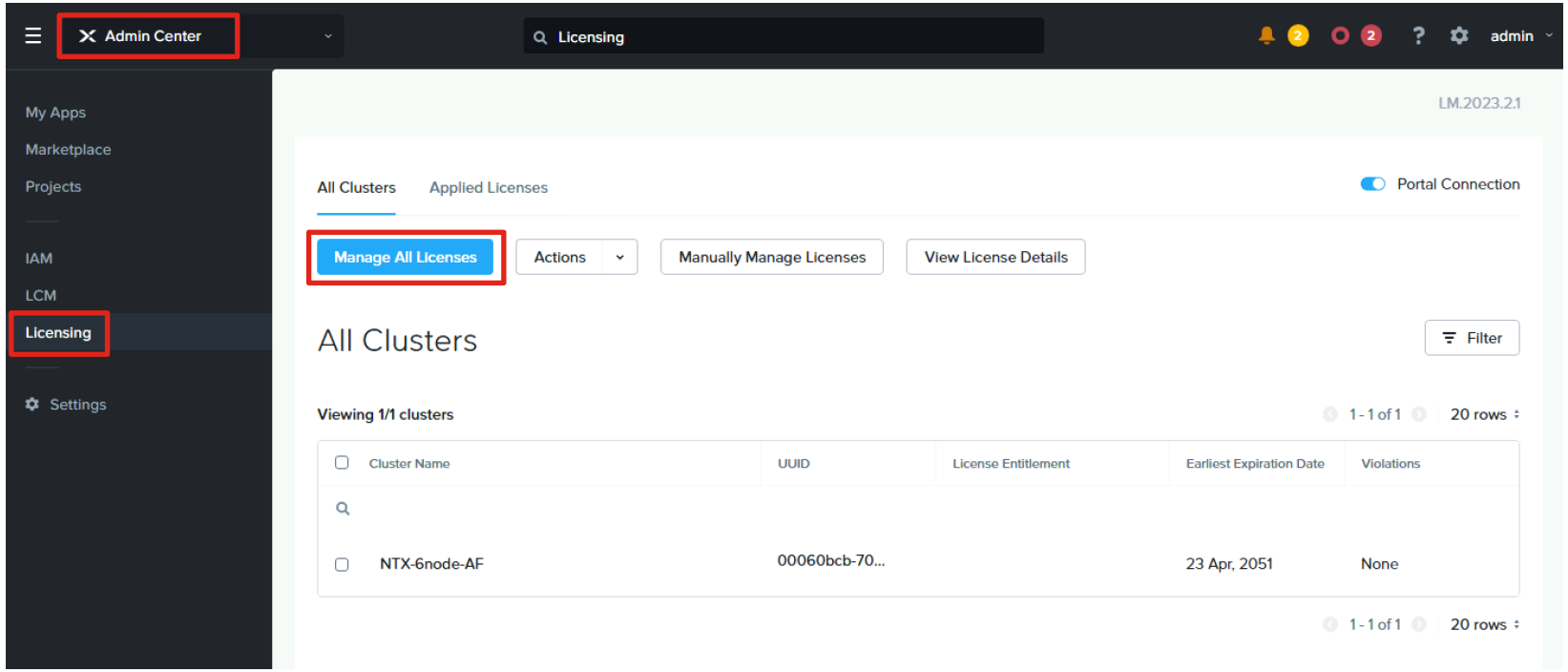


Manually upload after verifying compatibility

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.



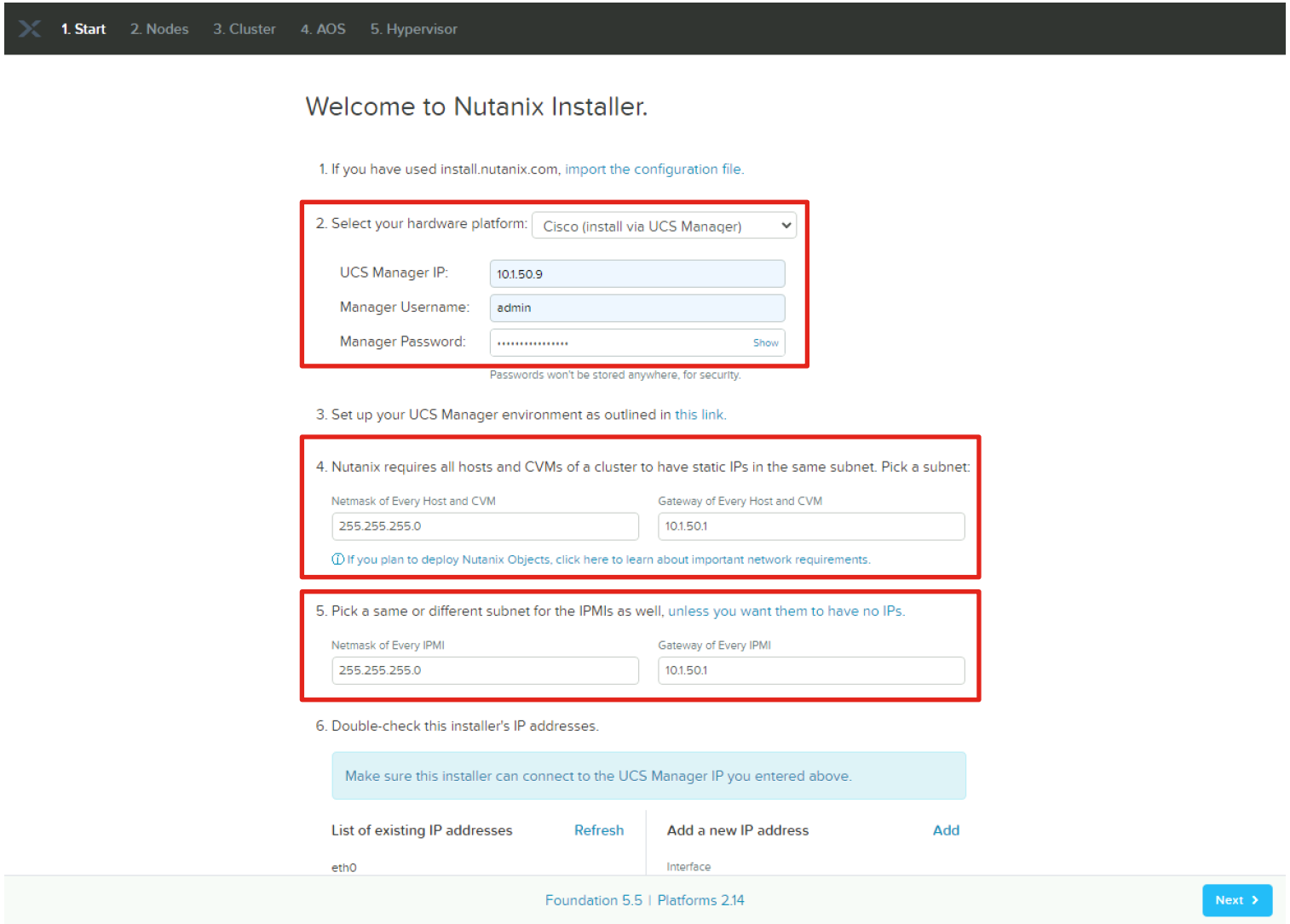
Configure Licensing



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

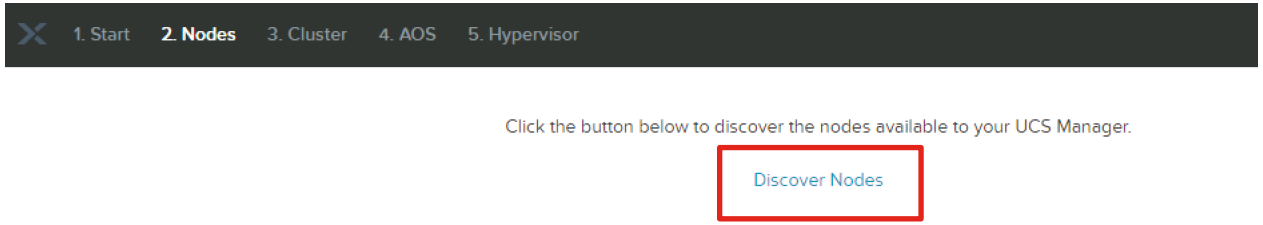
Cluster Expansion

Enter values on the Start page



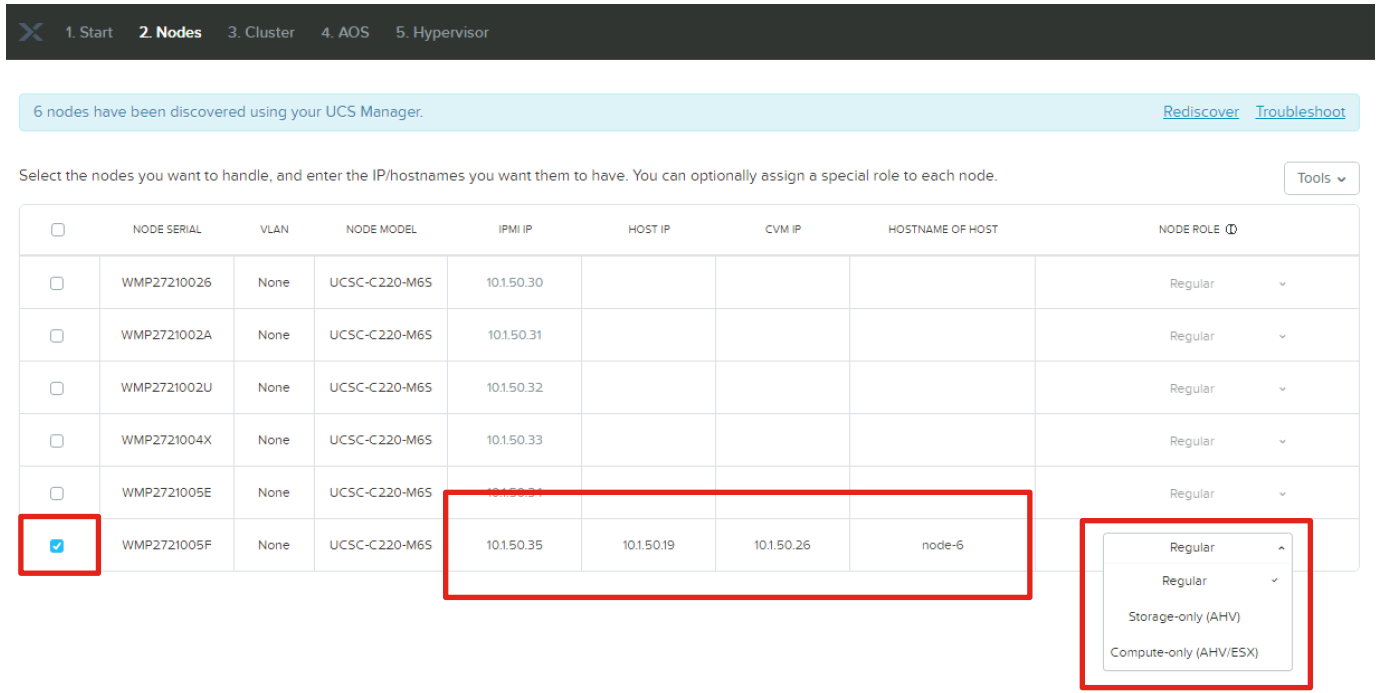
- A new node being added to the cluster must be prepared using Foundation first
- Use the Foundation VM deployed earlier
- Click the Reset link at the bottom of the page to clear the information from a previous installation
- Enter the UCS Manager details
- Enter the storage controller VM subnet mask and gateway matching the existing nodes
- Enter the subnet mask and gateway for the servers' CIMC addresses matching the existing nodes

Enter values on the Nodes page



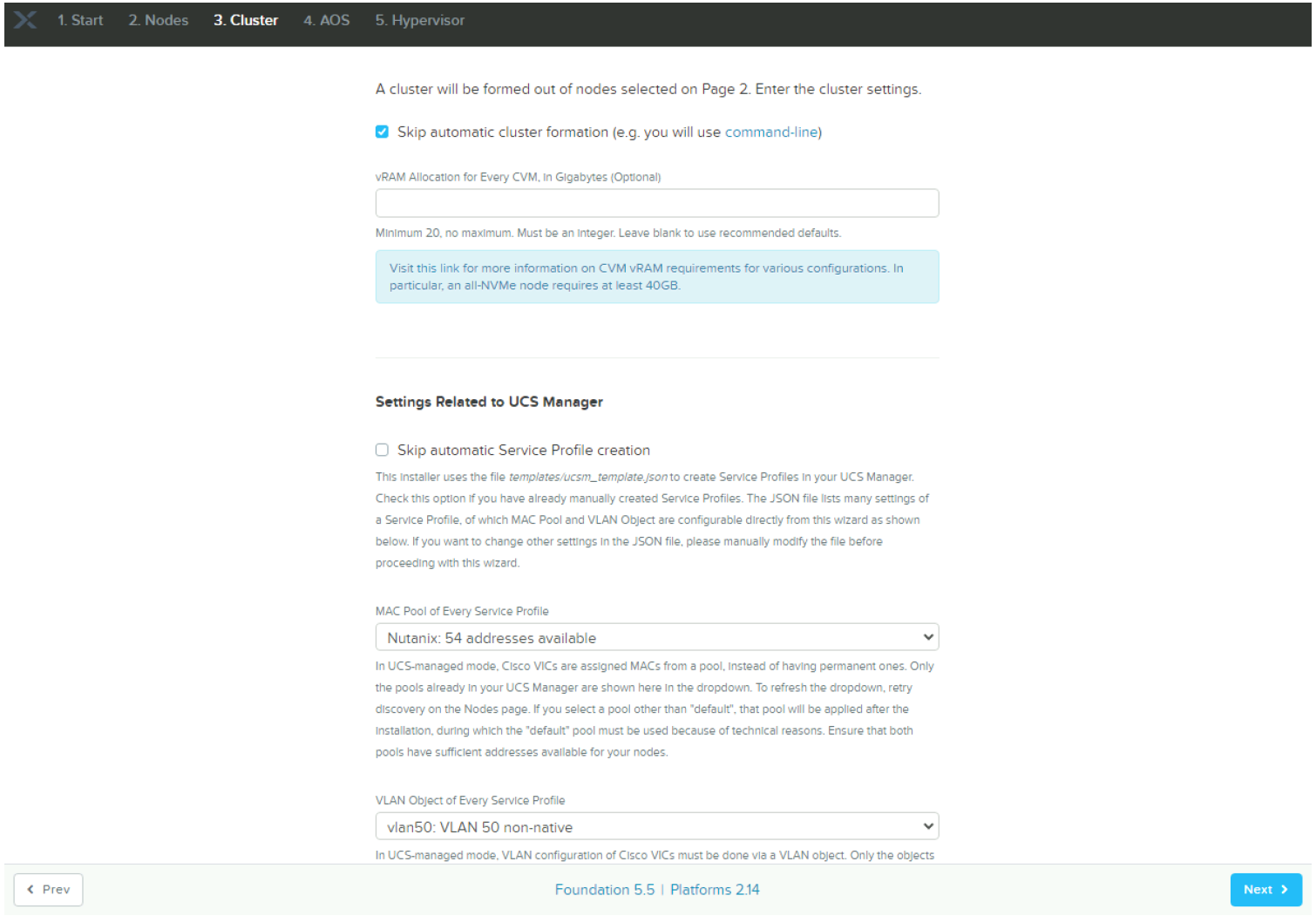
- You must click Discover Nodes to inventory the UCS domain. Do not continue and attempt to add nodes manually.
- Each node requires 3 IP addresses, one for the CIMC, one for the hypervisor host, and one for the storage controller VM.
- Add A records to your DNS server for the hypervisor hosts.

Enter values on the Nodes page continued



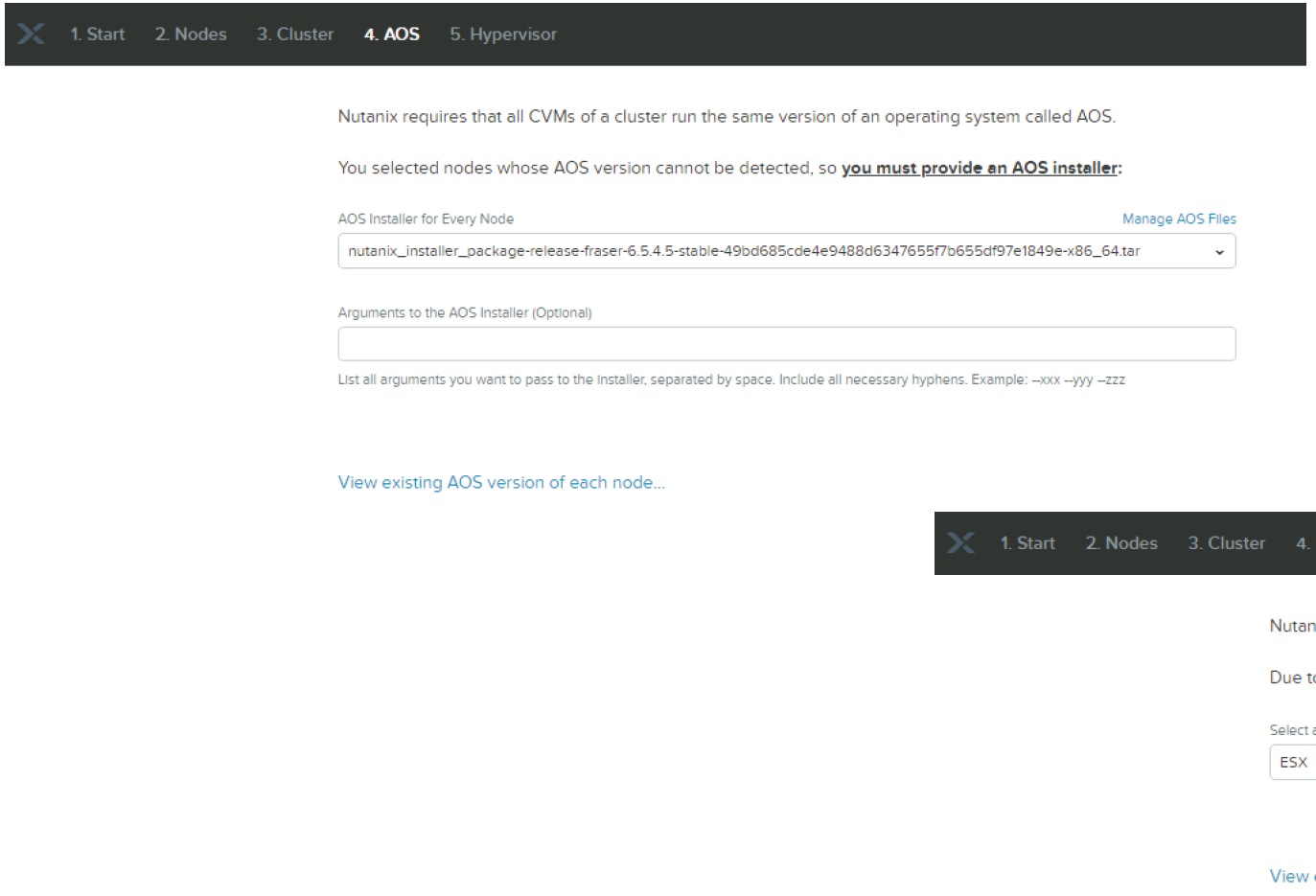
- Select only the node(s) to be added the cluster
- Enter the IPs and hostnames for the new nodes
- Select to add a Regular (i.e. HCI) node, a Storage-only node or a Compute-only node.

Enter values on the Cluster page

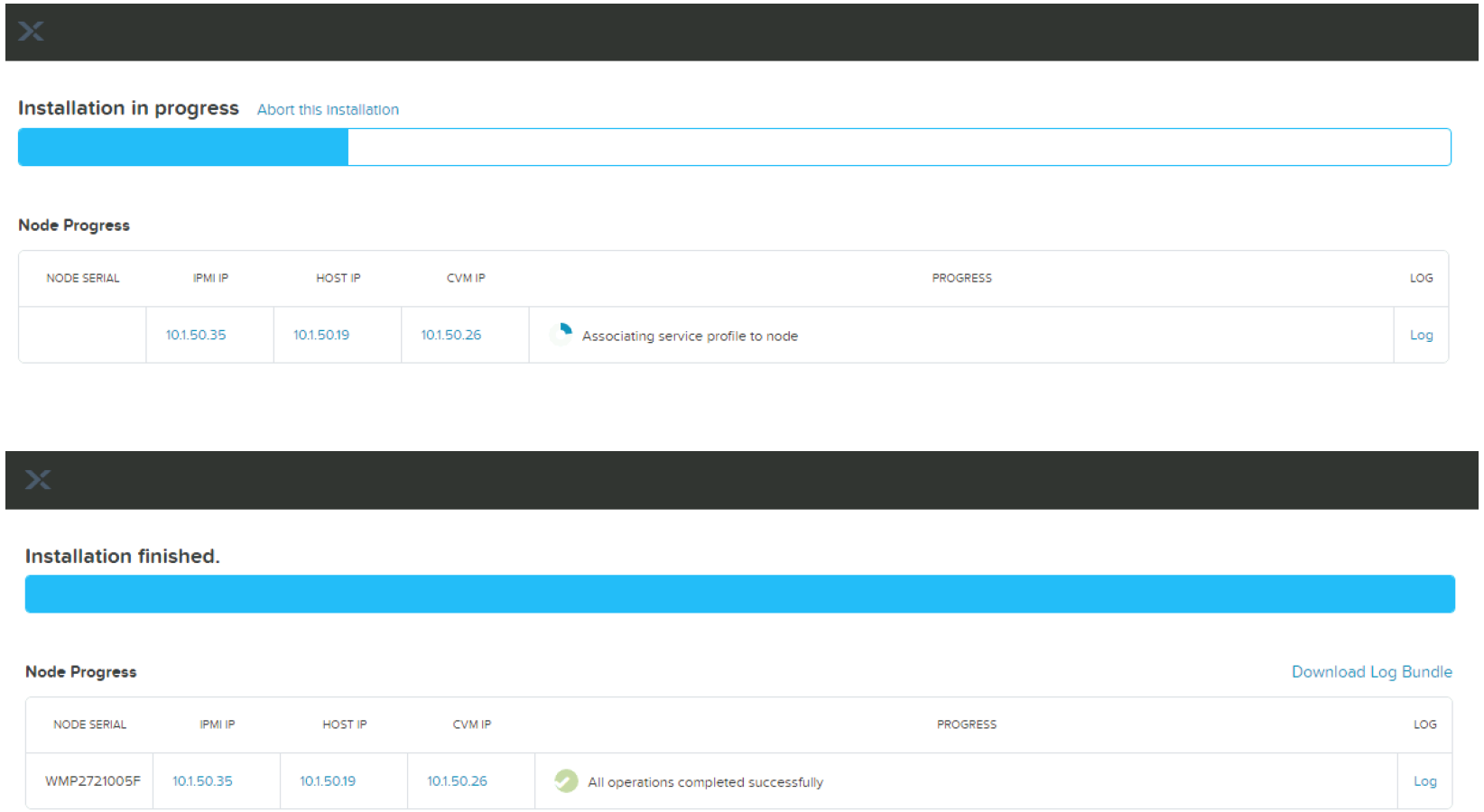


- Check the box to skip creating a cluster.
- Select the appropriate existing MAC address pool and subnet.

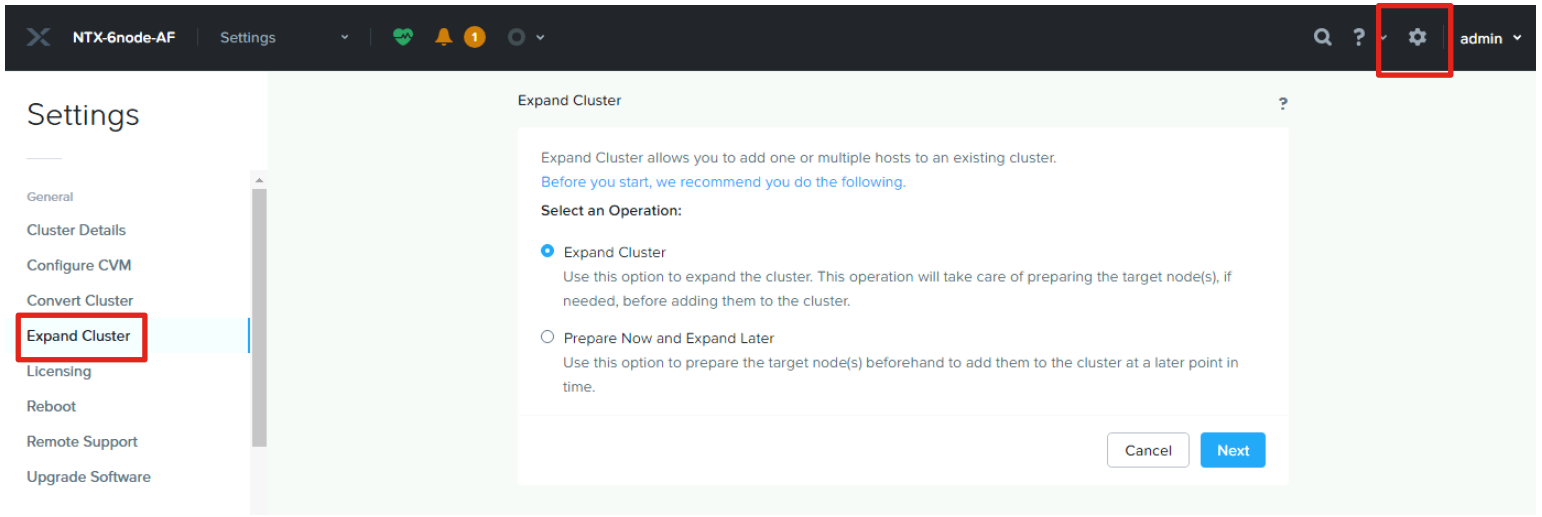
Select the AOS and hypervisor versions

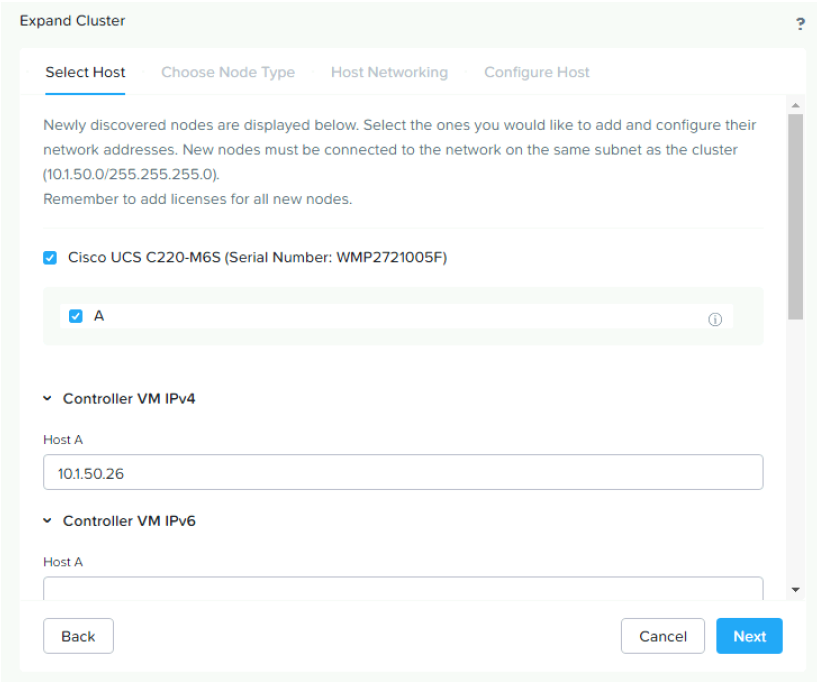


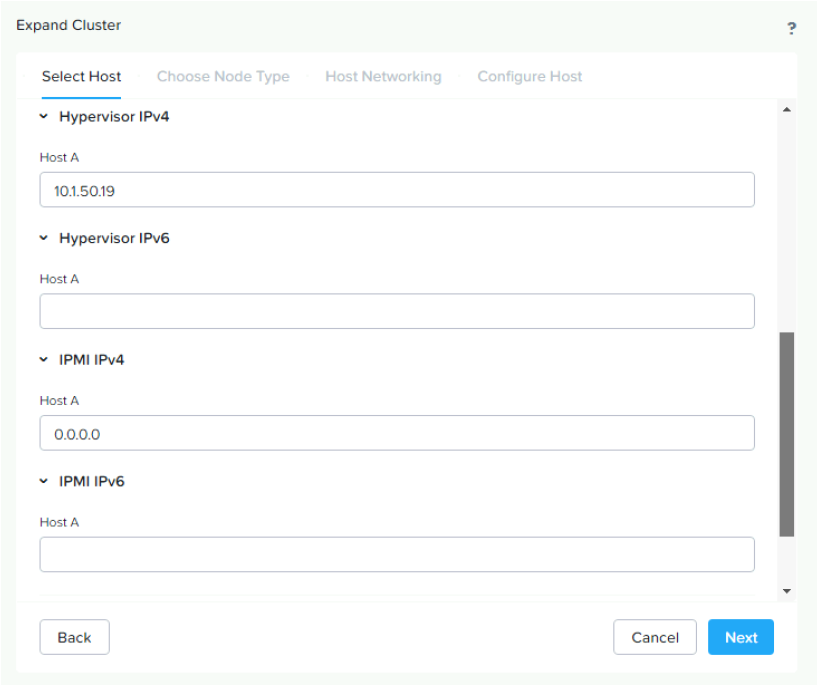
Observe the node preparation progress until complete



Expand the cluster from Prism Element

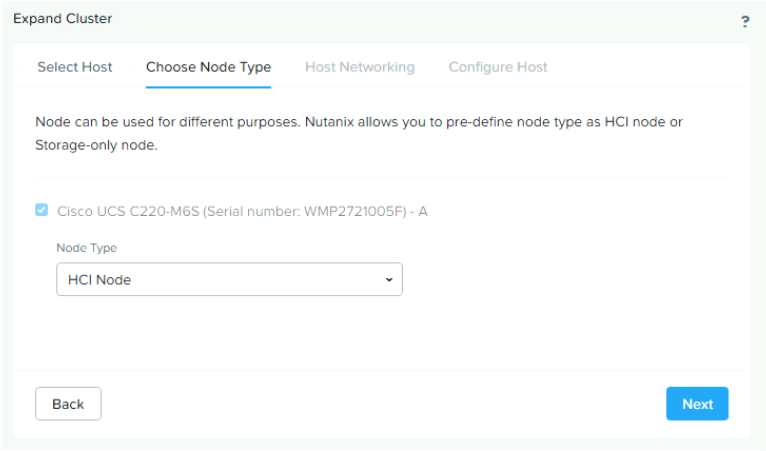


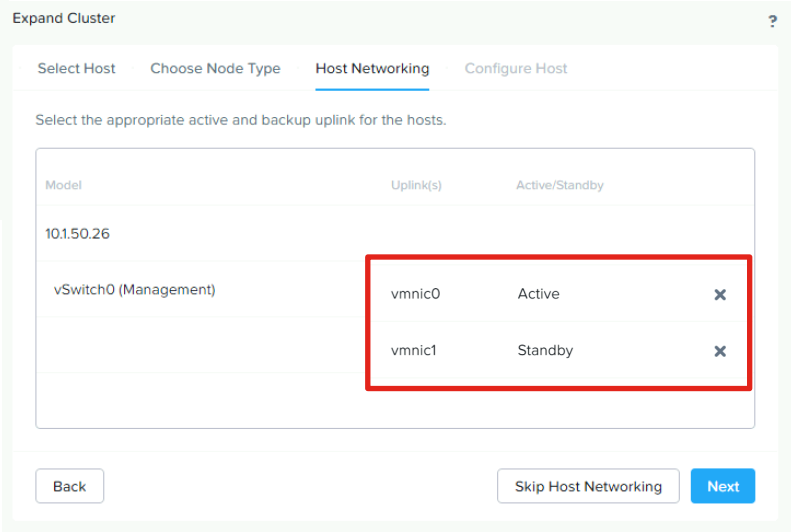




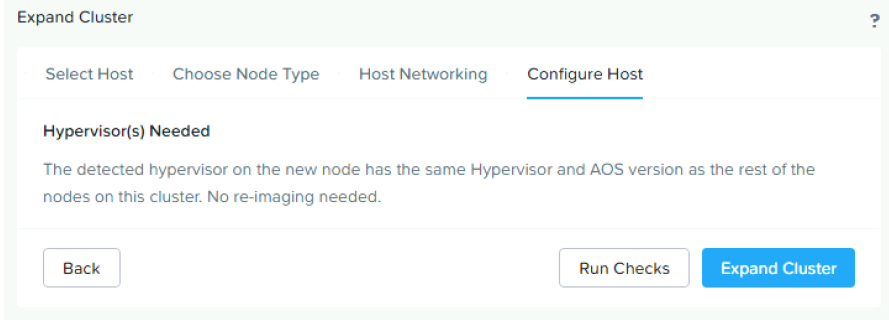
The newly prepared node should be discovered automatically with its preset IP addresses configured in Foundation. A compute-only node will likely not be discovered, and the IP address of the hypervisor host will need to be manually entered.

Expand the cluster from Prism Element continued

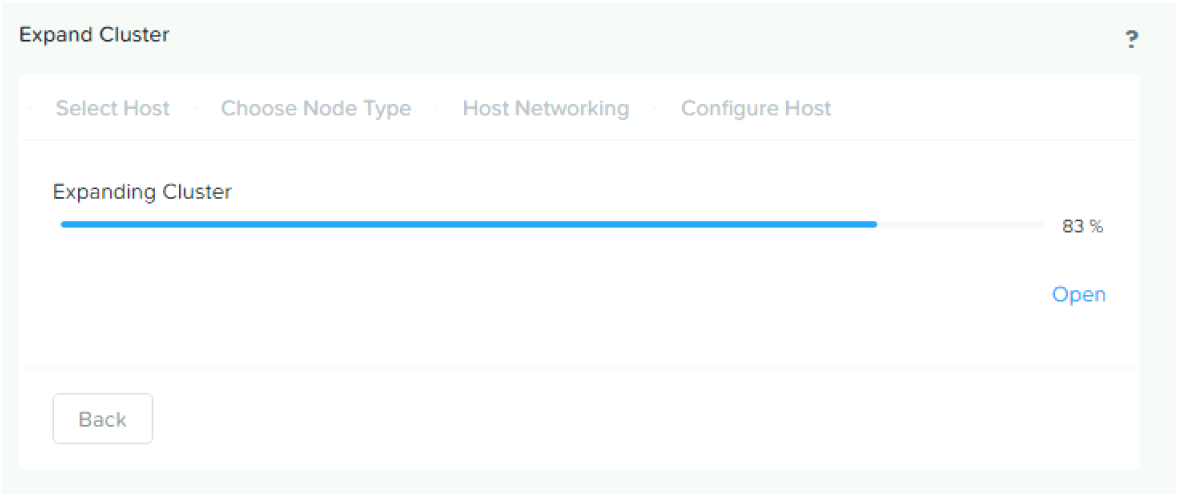


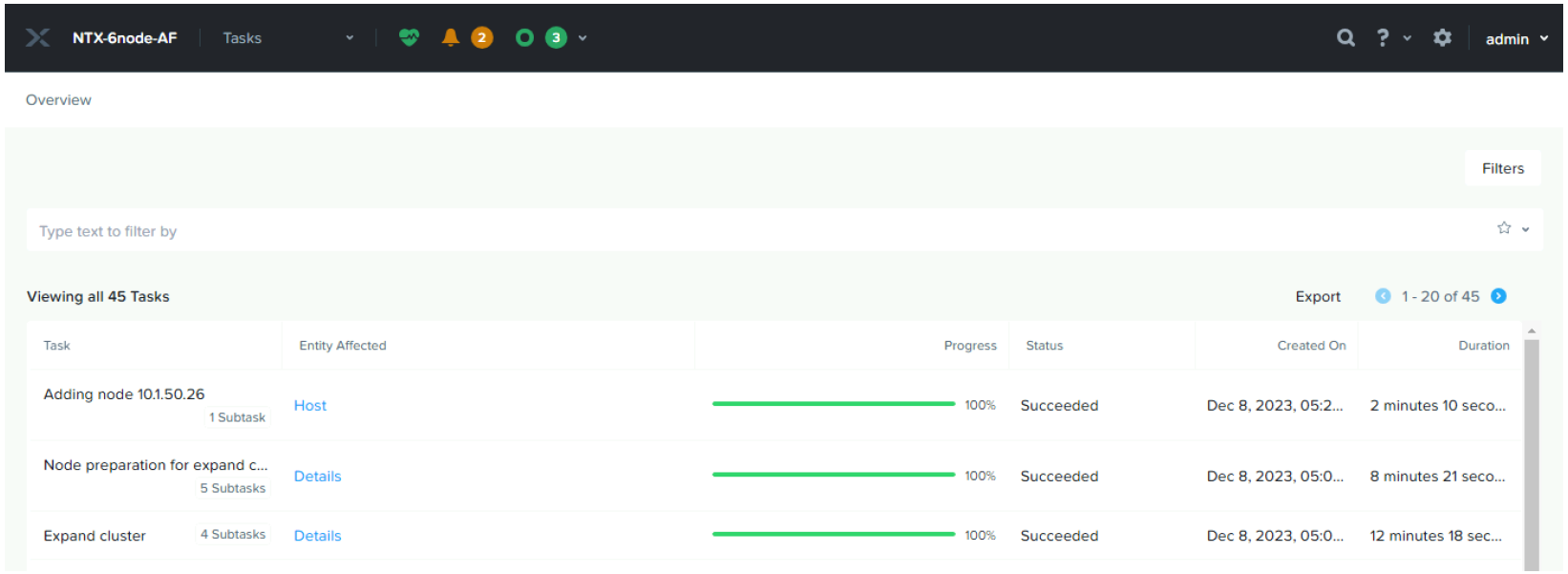


Add the vNICs as uplinks in this screen before continuing. For ESXi and AHV the default config is vmnic0 is Active and vmnic1 is Standby. AHV based compute-only and storage-only nodes may not show any uplinks.



Observe cluster expansion until completed



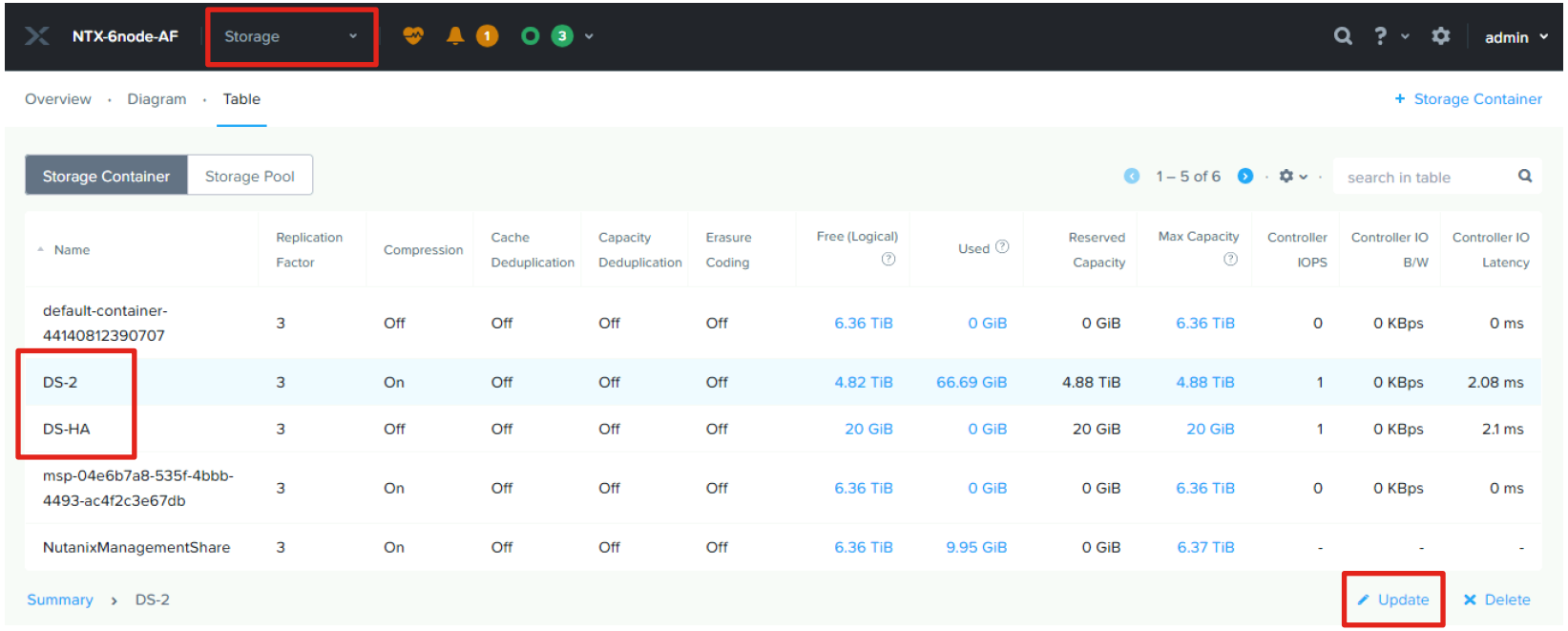


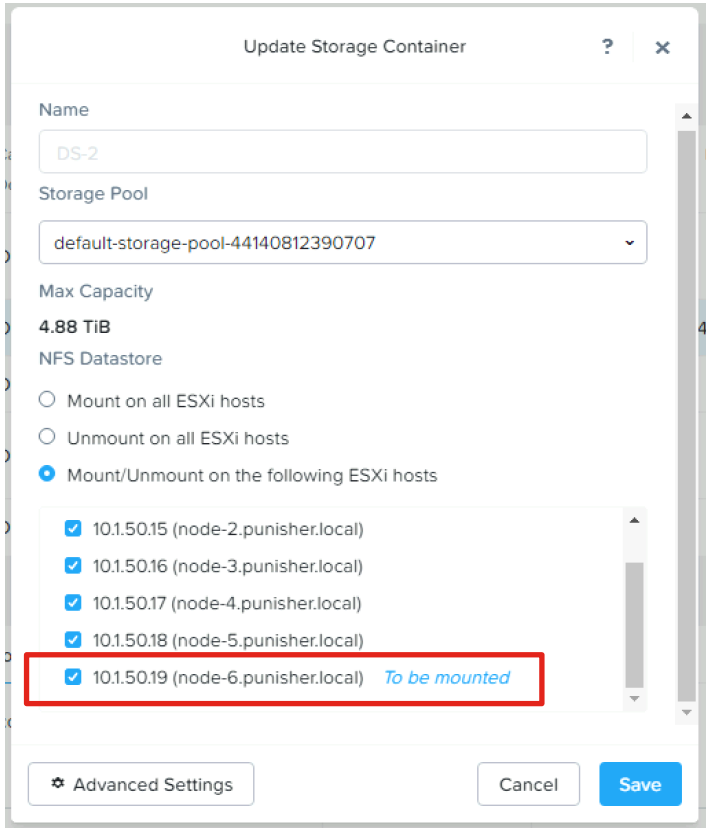
Perform post-expansion configuration

Perform the following tasks, as documented earlier, for the post-expansion configuration:

- Change the ESXi hypervisor root password, where applicable
- Change the AHV root, admin and nutanix account passwords, where applicable
- Change the CVM Nutanix account password (ESXi and AHV)
- Add the new host to the vCenter Datacenter (ESXi only)
- Configure NTP on the new host (ESXi only)
- Configure DNS on the new host (ESXi only)
- Move the new host into the vCenter cluster (ESXi only)
- Add any additional VLANs as tagged VLANs to the vNICs in UCS Manager (ESXi and AHV)
- Add the additional port groups to the default vSwitch0 (ESXi only)

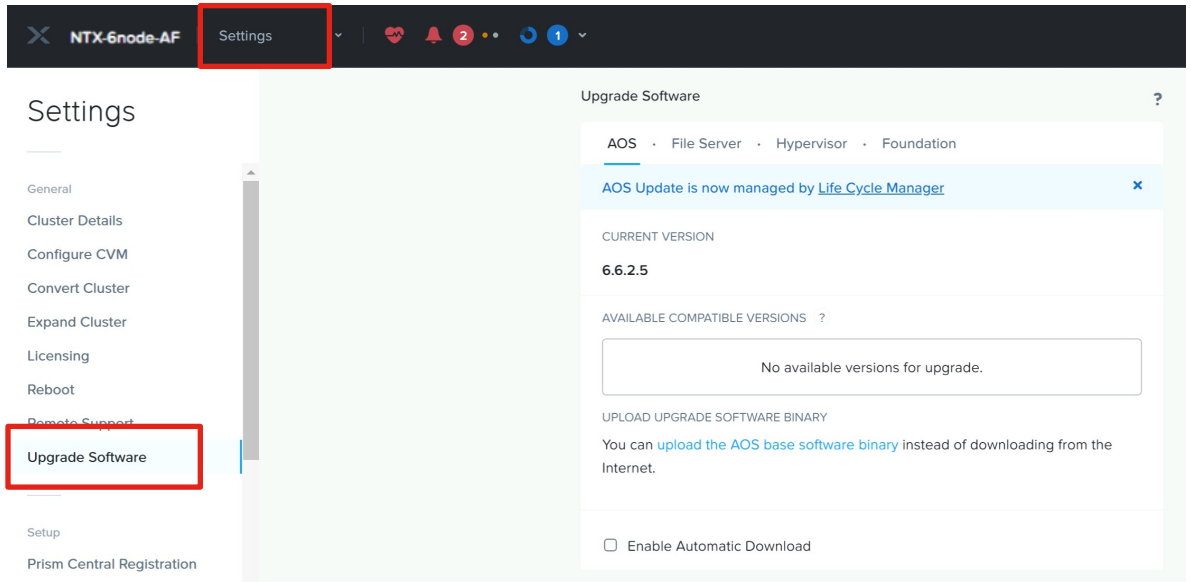
Mount user created storage containers to the new node(s)

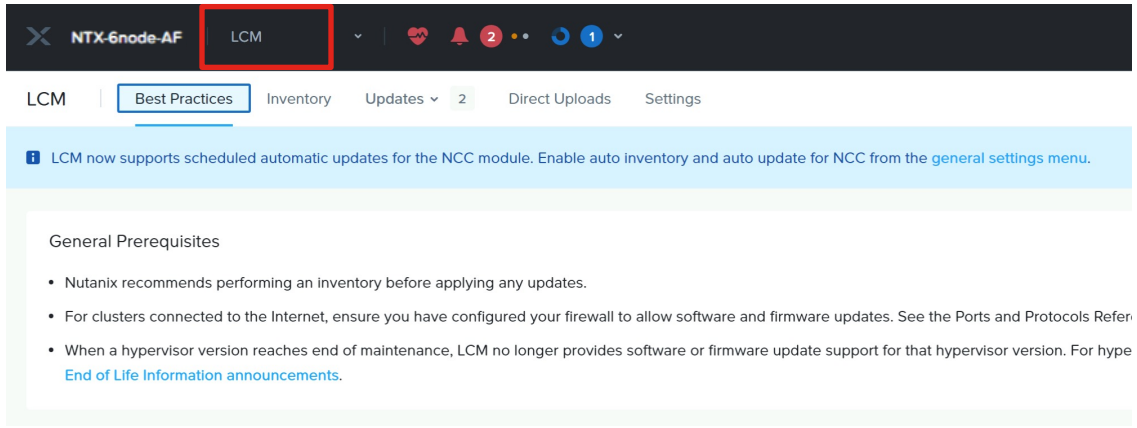


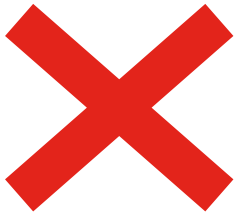


Nutanix Lifecycle Manager

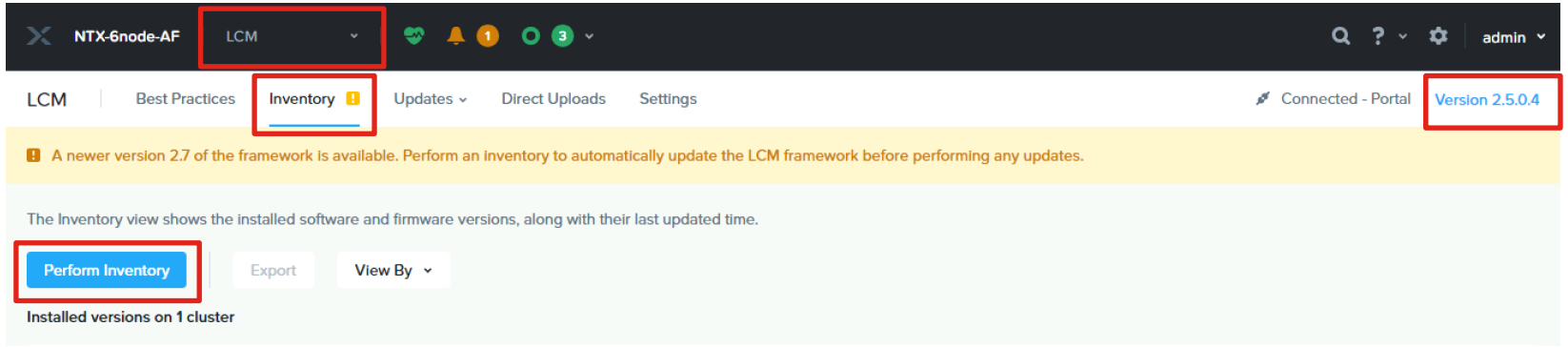
Do Not Use Upgrade Software, Only Use LCM

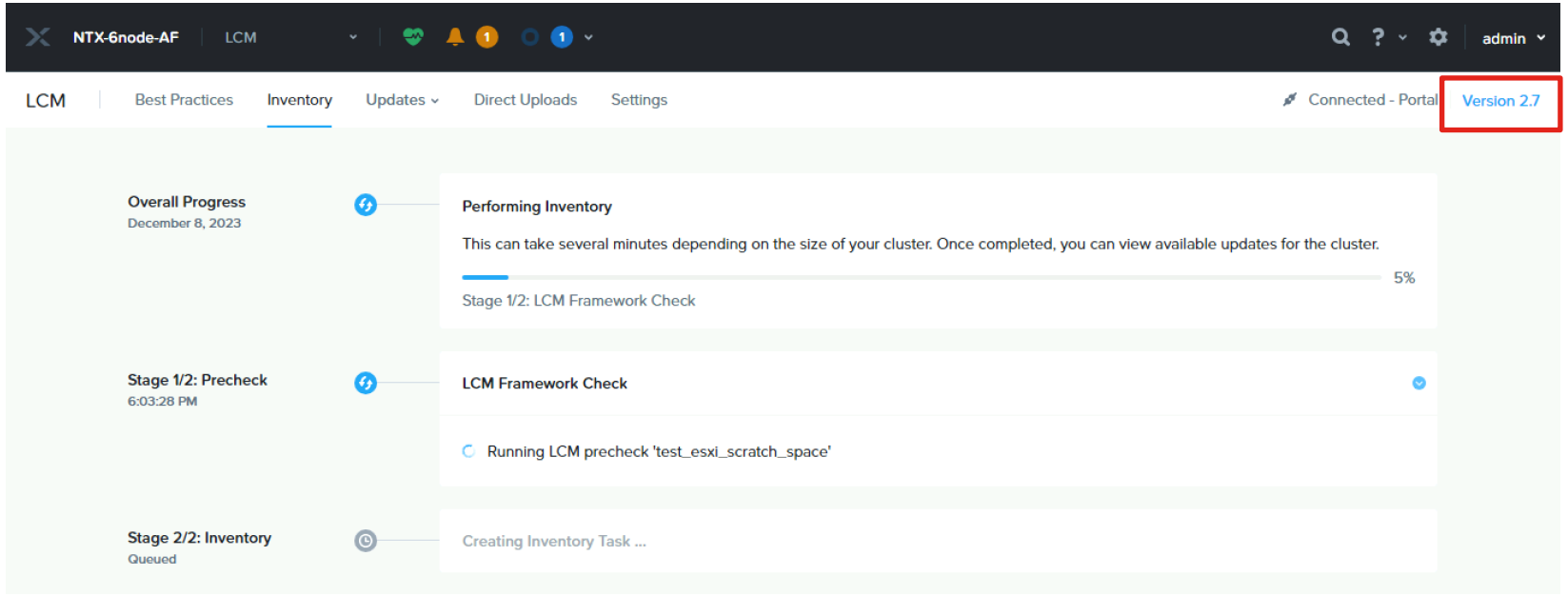






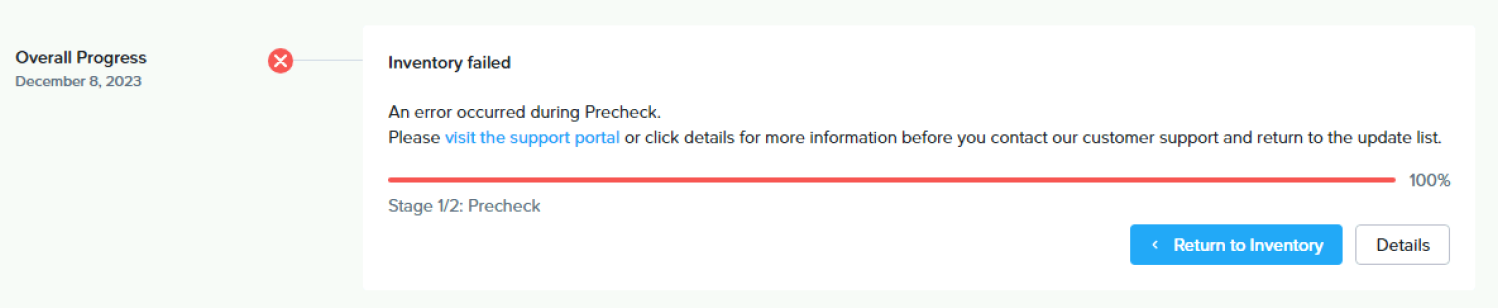
Perform initial inventory to update LCM



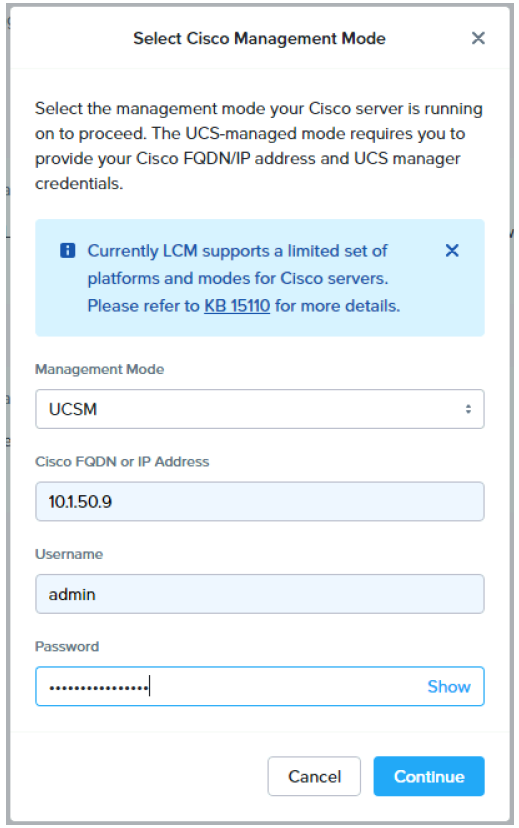


Perform second inventory after the upgrade

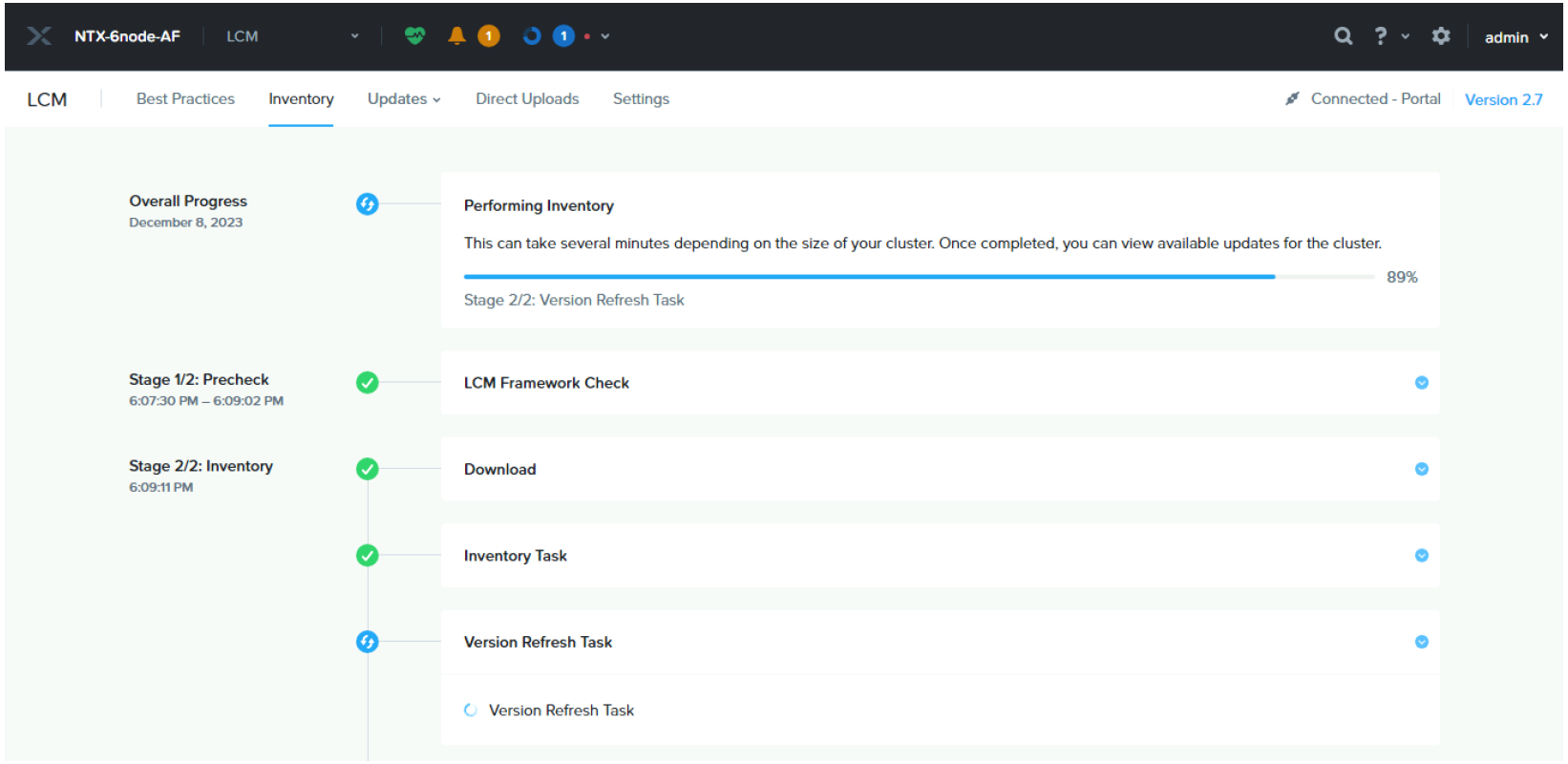
The initial inventory will fail because LCM had not been upgraded yet.



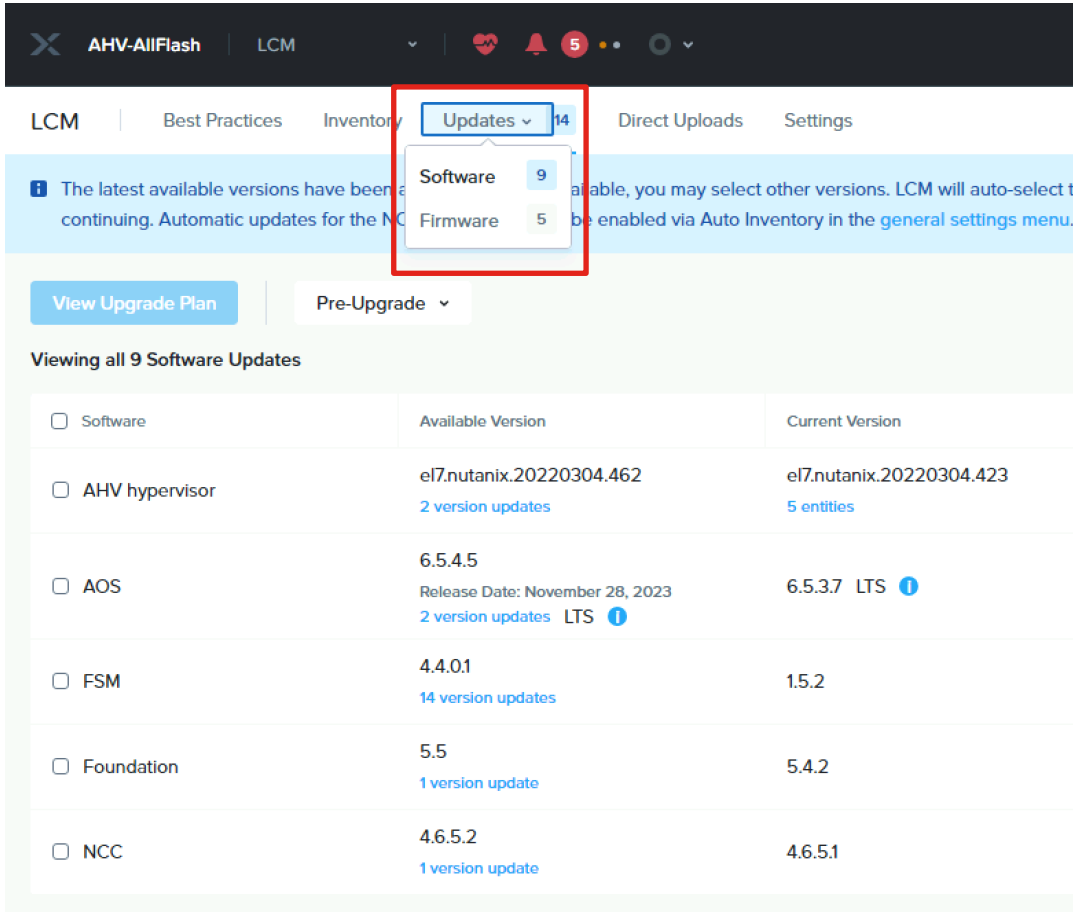
Return to inventory, then perform inventory a second time once LCM is upgraded to version 2.7+. You will be prompted for the Cisco Management Mode, and the IP address and credentials to log in to UCS Manager.

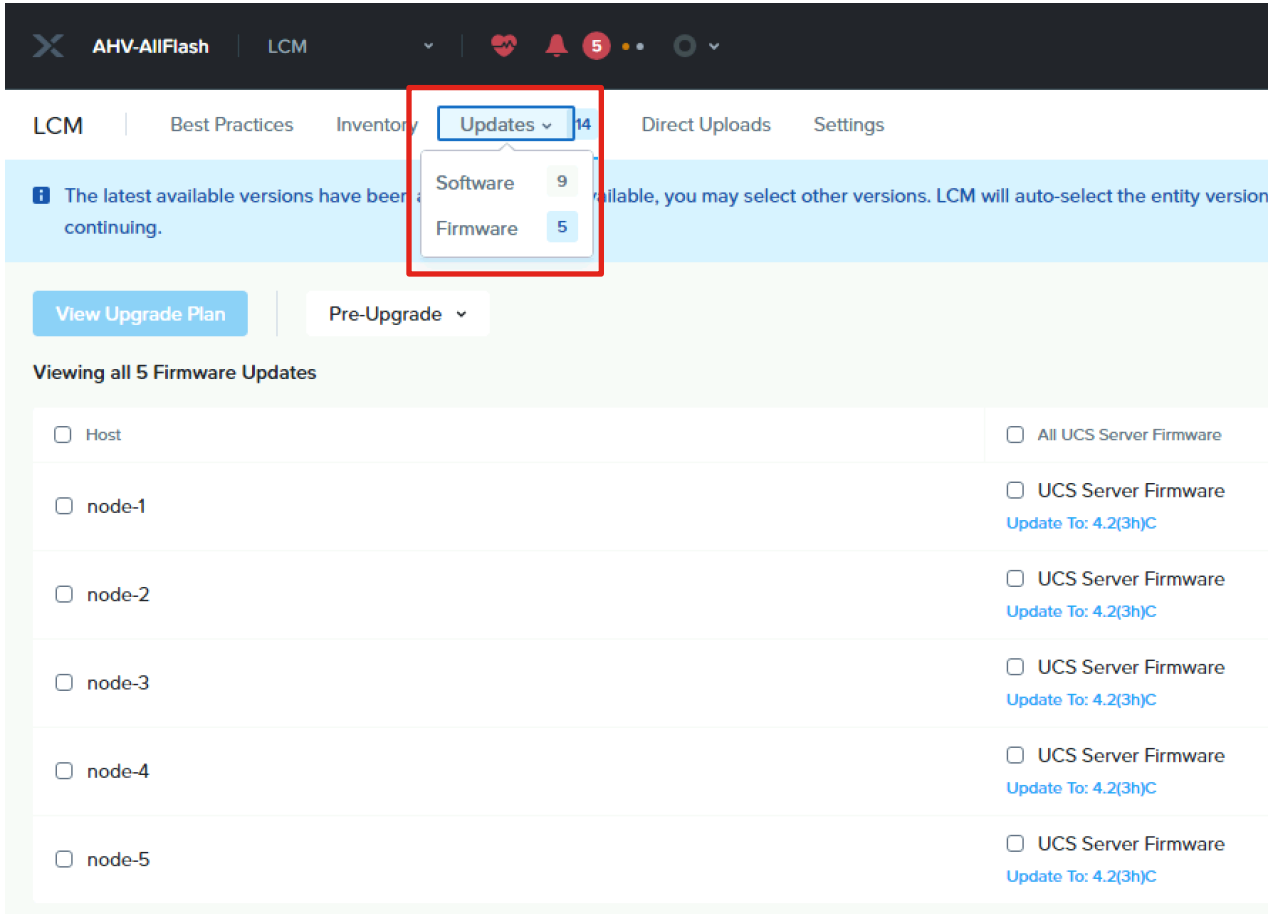


Inventory Progress



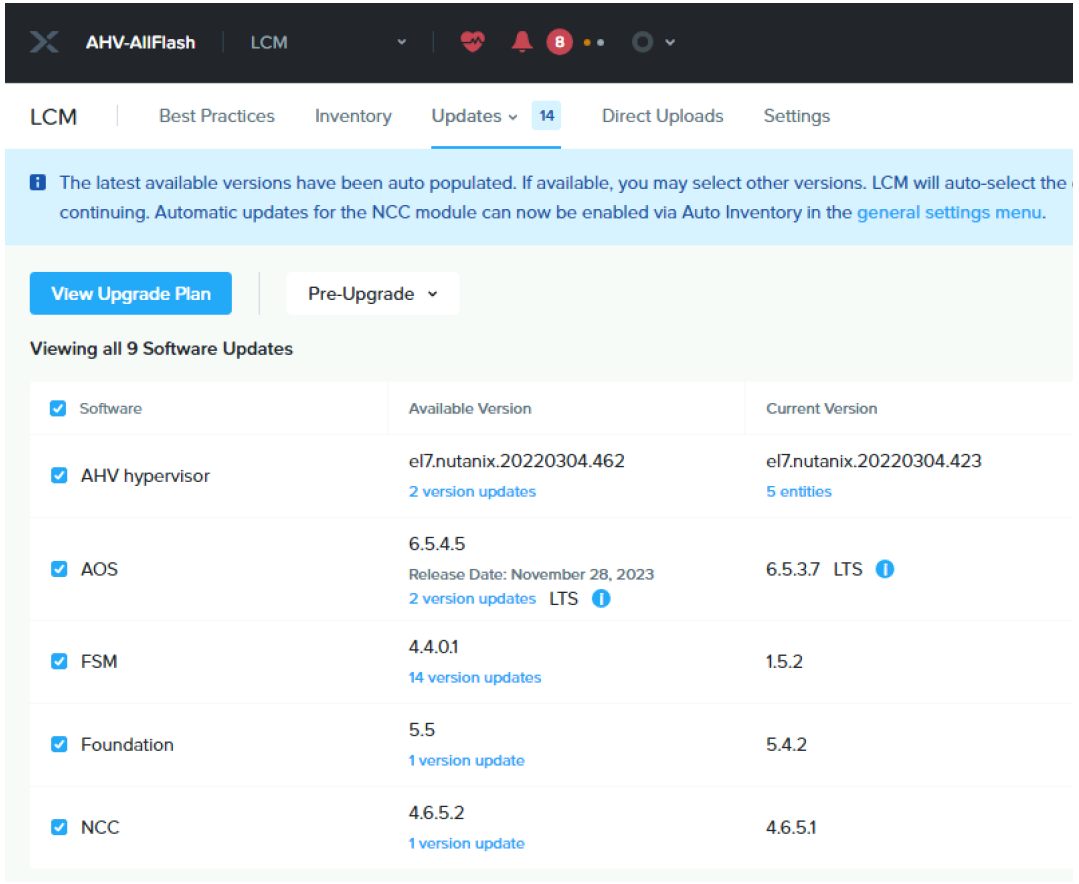
Available Updates

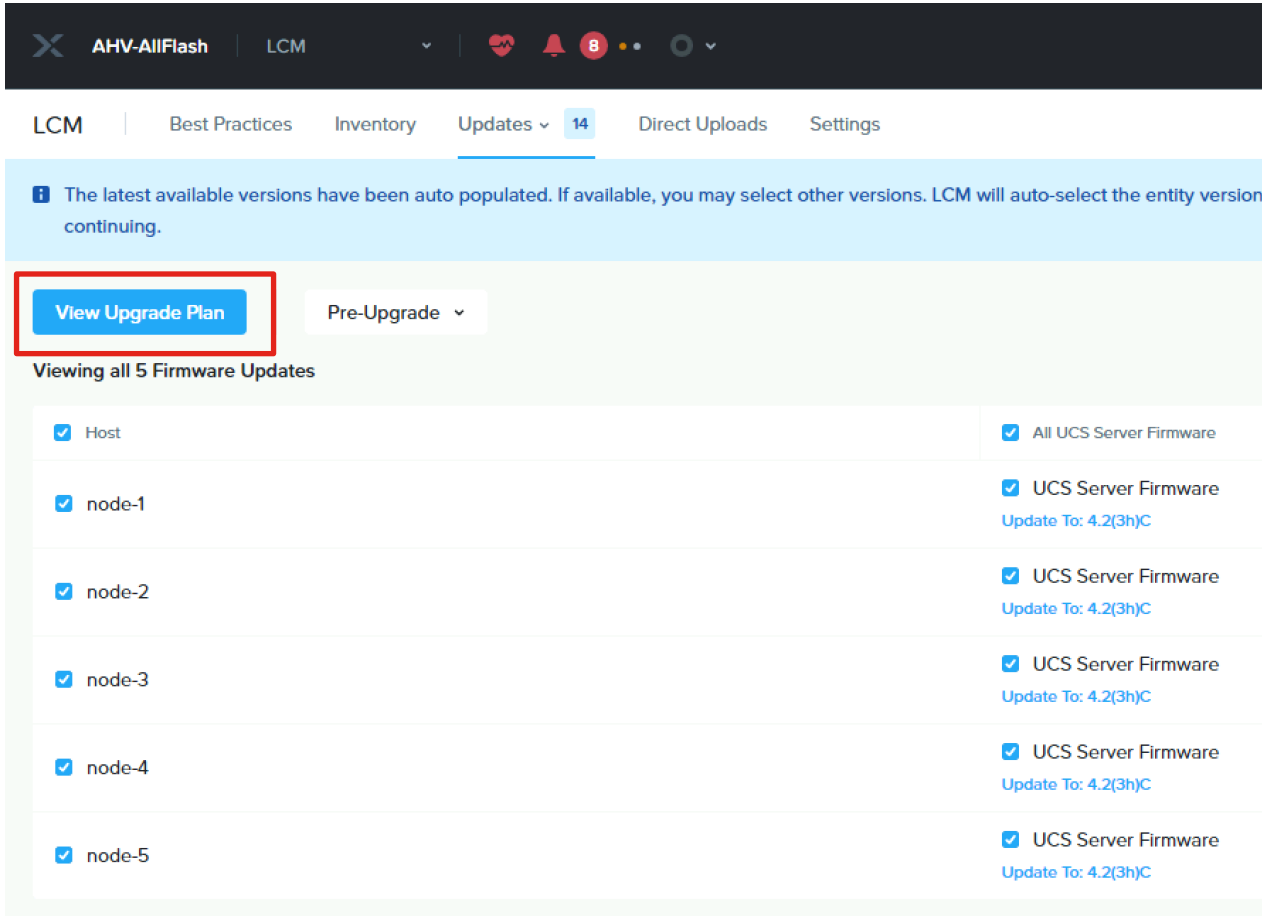




Nutanix generally recommends doing all software updates and firmware updates at once and letting LCM handle the proper order and dependencies. For manual upgrade order, refer to this page: https://portal.nutanix.com/page/documents/details?targetId=Acropolis-Upgrade-Guide-v6_7:upg-upgrade-recommended-order-t.html

Select All Available Updates

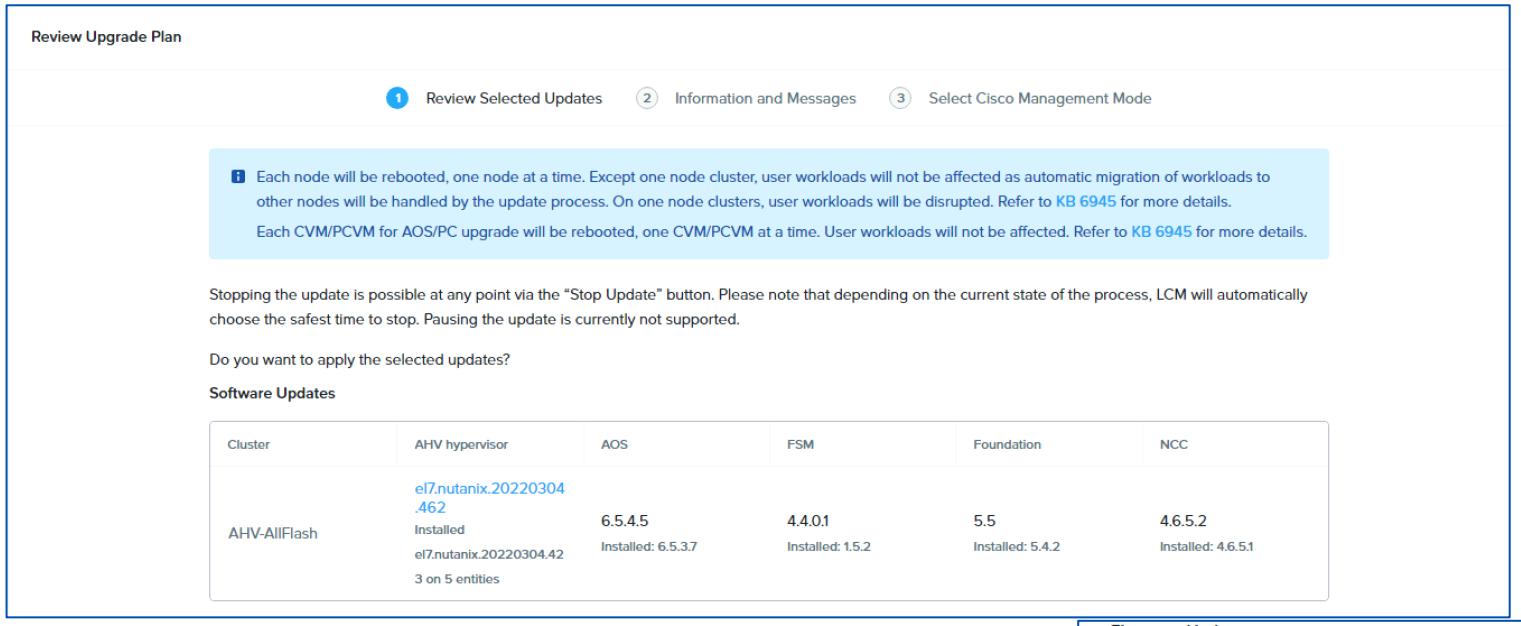


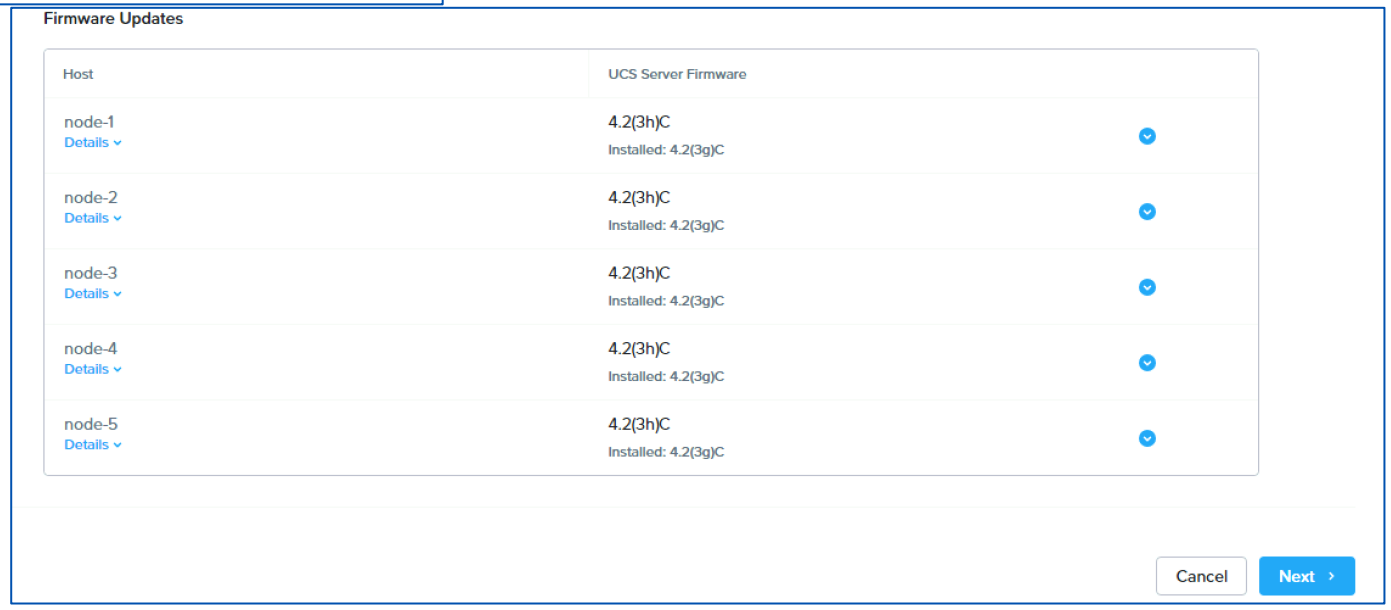


Select all the available updates from the two pages then click View Upgrade Plan.

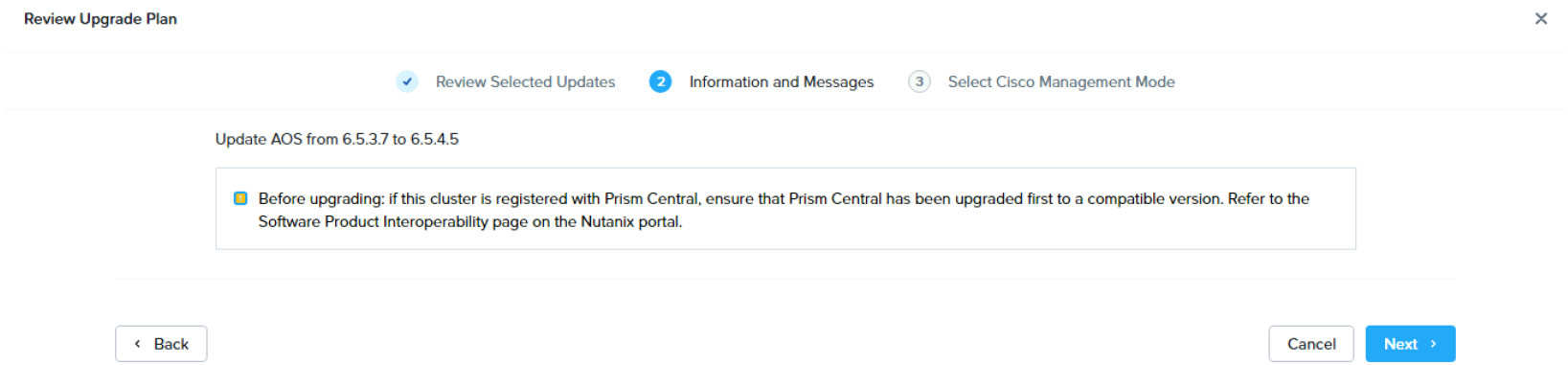
Note: Performing all available updates at once assumes your cluster is configured with DRS in fully automated mode for ESXi, or the VM High Availability Reservation is enabled for AHV. This allows for the VMs to automatically migrate, and the nodes to automatically reboot without service interruptions.

Review Upgrade Plan

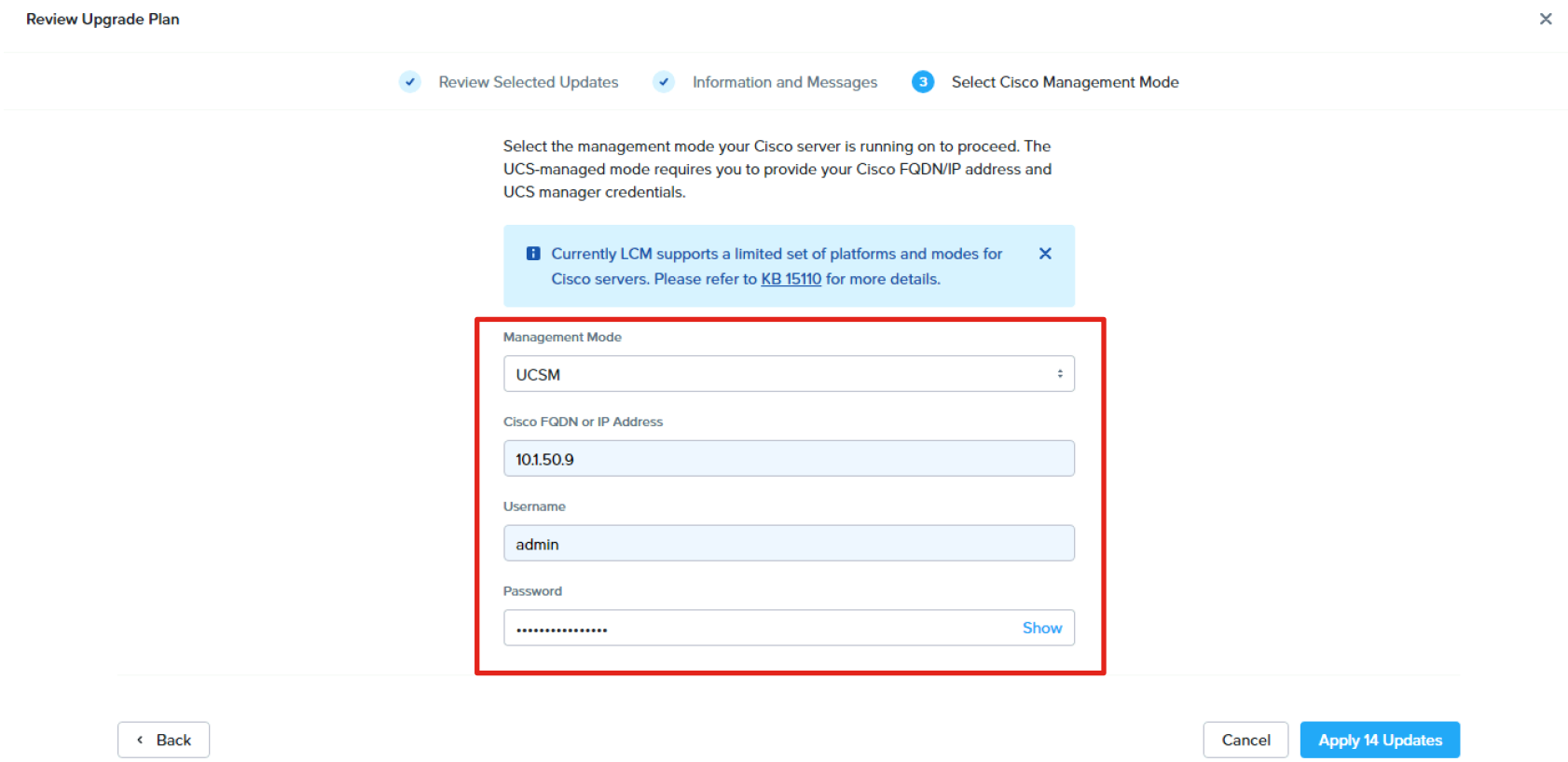




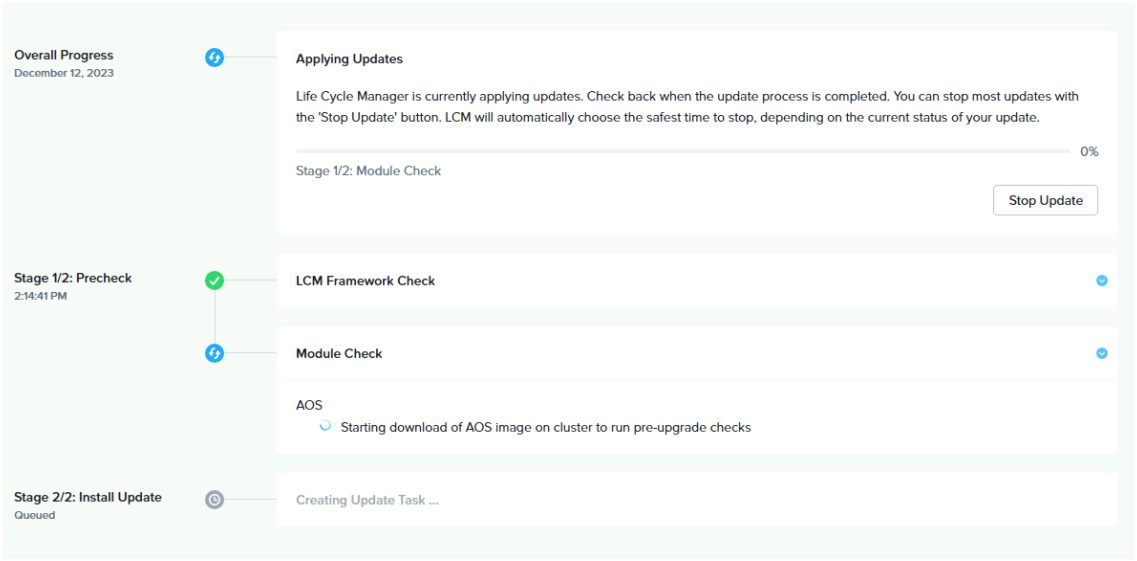
Review Upgrade Plan continued

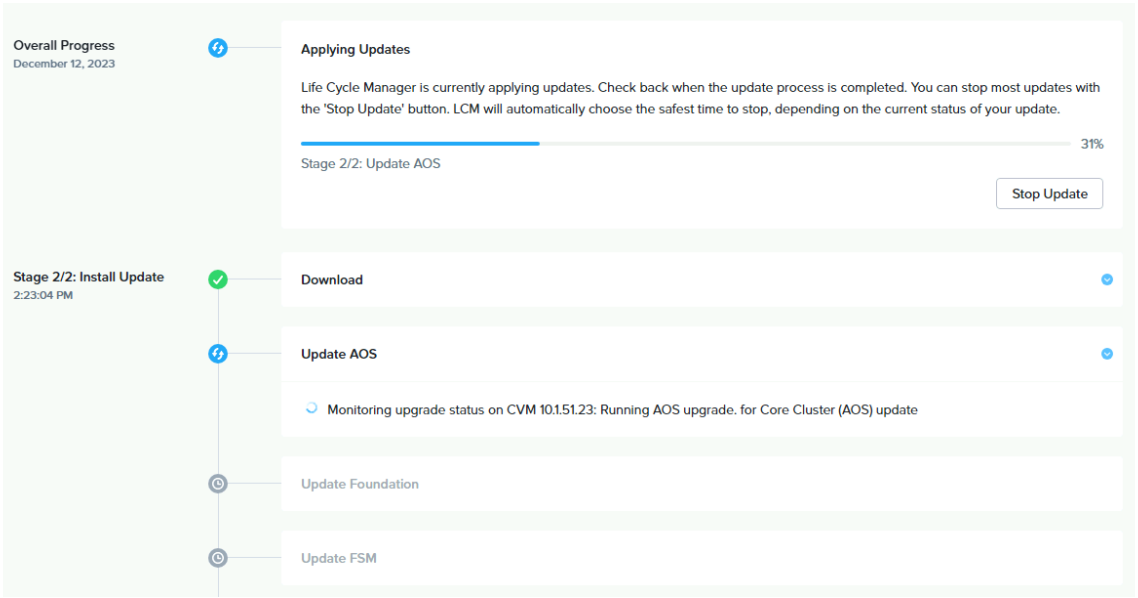


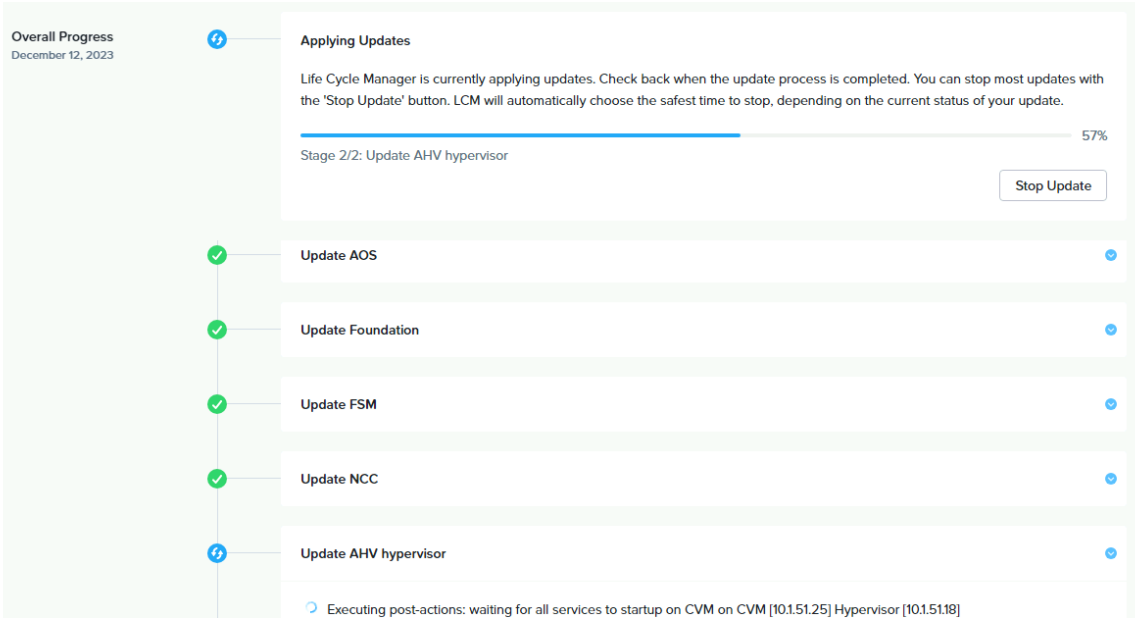
Review Upgrade Plan continued



Monitor LCM Upgrade Progress







The bridge to possible