Unified Surveillance Platform (USP) 5.0

OS Installation and Cluster Setup Guide

6-069080-01, Rev B

Quantum

Table of Contents

Contents

Overview

This guide explains how to install USP 5.0 (Unified Surveillance Platform) software on a cluster of enterprise servers.

Hardware Requirements & Recommendations

Hardware Requirements

Component	Requirements
Server	• X86_64 Enterprise class server, updated with recent BIOS & firmware • Servers must be capable of having CentOS 8 stream installed, i.e., support by CentOS 8 Stream. ○ RHEL 8 (CentOS 8 & x86_64) Ecosystem Catalog • UEFI capable • VT/d enabled • Chassis Serial number is required
CPU	• X86_64 compatible • AMD or Intel • 14 cores minimum
Memory	Total CPU count needs to be taken into consideration for minimum memory requirements. Total CPU = (Threads per core * Cores per socket) * Physical Socket • 24 or less total CPU: **96 GB** • 28 – 40 total CPU: **128 GB** • 48 – 64 total CPU: **196 GB** • 68 and above total CPU: **256 GB**

Network	• 1 NIC port for iDRAC/KVM/IPMI
	• 4 10 GbE
	  ○ Management Network
	  ○ SAN 0 Network
	  ○ SAN 1 Network
	  ○ Application Network (Camera Network)

OS Boot Disk(s)	• Minimum size 120 GB • M.2, SSD, or HDD • For SSD or HDD recommend 2 disks per node for software RAID

Component	Requirements

Storage Disks	• Enterprise class SSDs and/or HDDs (512e)
	• Each node should have the same number of disks.
	• Disks across nodes should be the same size.
	• Sizes Requirements:
	  ○ SSD – 960 GB minimum, 8 TB maximum
	  ○ HDD – 1 TB minimum, 16 TB maximum

Cache Disks	• Required when using 16 or more HDDs for storage. • If used, then requires exactly 2. One cache disk is not supported. • 480 GB minimum, 2 TB maximum
Cluster	• Required 3 nodes of same hardware

Suggested Drive Configurations

This section describes three suggested drive configurations.

Drive Count	Configuration (per server)
Small (minimum)	• 4 SSDs (Storage Tier) **OR** • 4 HDDs (Storage Tier)
Medium	• 8 HDDs (Storage Tier) + 2 SSDs (Cache Tier) **OR** • 8 SSDs (Storage Tier)
Large (maximum)	• 12 HDDs (Storage Tier) + 2 SSDs (Cache Tier) **OR** • 16 HDDs (Storage Tier) + 2 SSDs (Cache Tier)

Hardware Limitations

- Lenovo SR655 with AMD 7452 Processor is not supported.
- Secure boot is not supported and must be disabled prior to installation.
- NVMe tiers are not supported.
- 16 HDDs per server is the maximum for this release.

Required Infrastructure Resources

This section outlines the resources used by the USP software.

Component	vCPU	RAM	Storage	Configuration (per server)
Acuity VM	10 vCPU	24 GB	14 GiB	1 per Host, manages storage.
Monitoring VM (historical)	8	12 GB	90.038 GiB	1 per Cluster
Monitoring VM (backend)	2	4 GB	36.035 GiB	1 per Cluster
Monitoring VM (zookeeper)	4	8 GB	36.035 GiB	1 per Cluster
Monitoring VM (broker)	4	8GB	36.035 GiB	1 per Cluster
Image Store	n/a	n/a	900.038 GiB	1 per Cluster
Nova	n/a	n/a	180.038 GiB	1 per Cluster

Example Configurations

The following table shows example configurations for large, medium, and small deployments.

Configuration	Server	RAM	CPU	OS Drive	Cache Tier	Storage Tier
Large	Dell R740 XD2	192 GB	2 x 24 cores	1 x 1TB M.2	2 x 2TB SSD	16 x 8TB HDD
Medium	Lenovo SR650	128 GB	2 x 12 cores	2 x 2TB SSD	N/A	8 x 4TB SSD
Small	Dell	96 GB	2 x 10 cores	2 x 1TB HDD	2 x 1TB SSD	4 x 4TB HDD

Network Overview

Network Types

- **MGMT** – This network is used for accessing the USP operating system that gets installed on each host. It is also used to connect to the instances running on the cluster.
- **VM Network / Application Network** – This network is used to host the application traffic inside each VM. For example, this is the network in which your cameras are connected.
- **SAN 0 / SAN 1** – These networks are used for SAN iSCSI traffic between the storage backend and the hosts in the cluster.
- **IPMI** – Out-of-band management network

NOTE: Jumbo frame support is required for the MGMT and VM Network. Performance may be impacted if jumbo frame support is not enabled.

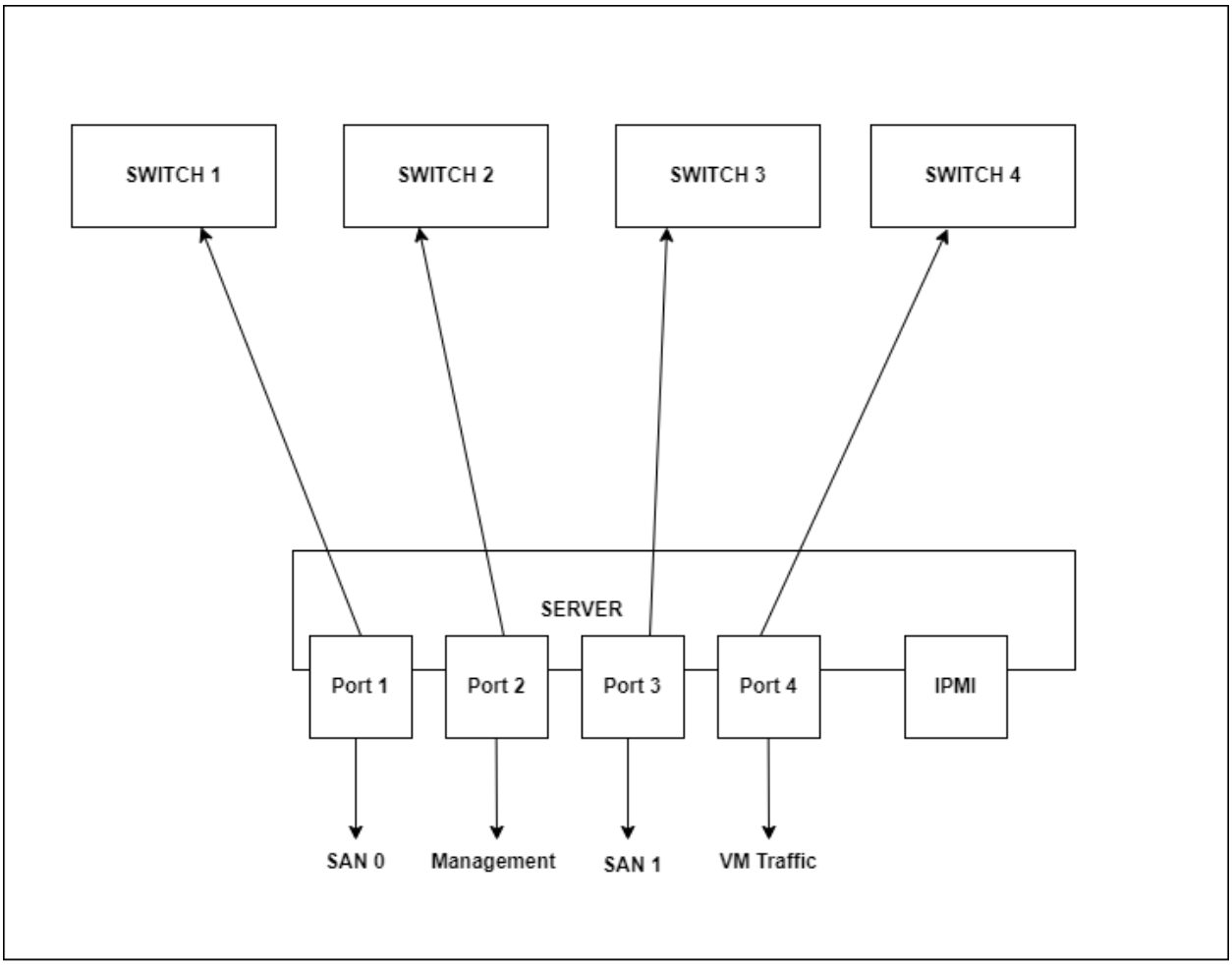
Recommended Network Configurations

Configuration	# Ports	Network	# Switches	Switch Redundancy	Port Redundancy
1	4	Flat	4	SAN Only	
2	4	4 VLAN	2	All Networks	
3	4	2 Flat (SAN 0/1) 2 VLAN (Management / VM Traffic)	4	All Networks	
4	6	Flat	4	SAN Only	All Networks
5	6	2 Flat (SAN 0/1) 2 VLAN (Management / VM Traffic)	4	All Networks	
6	6	Flat	6	All Networks	

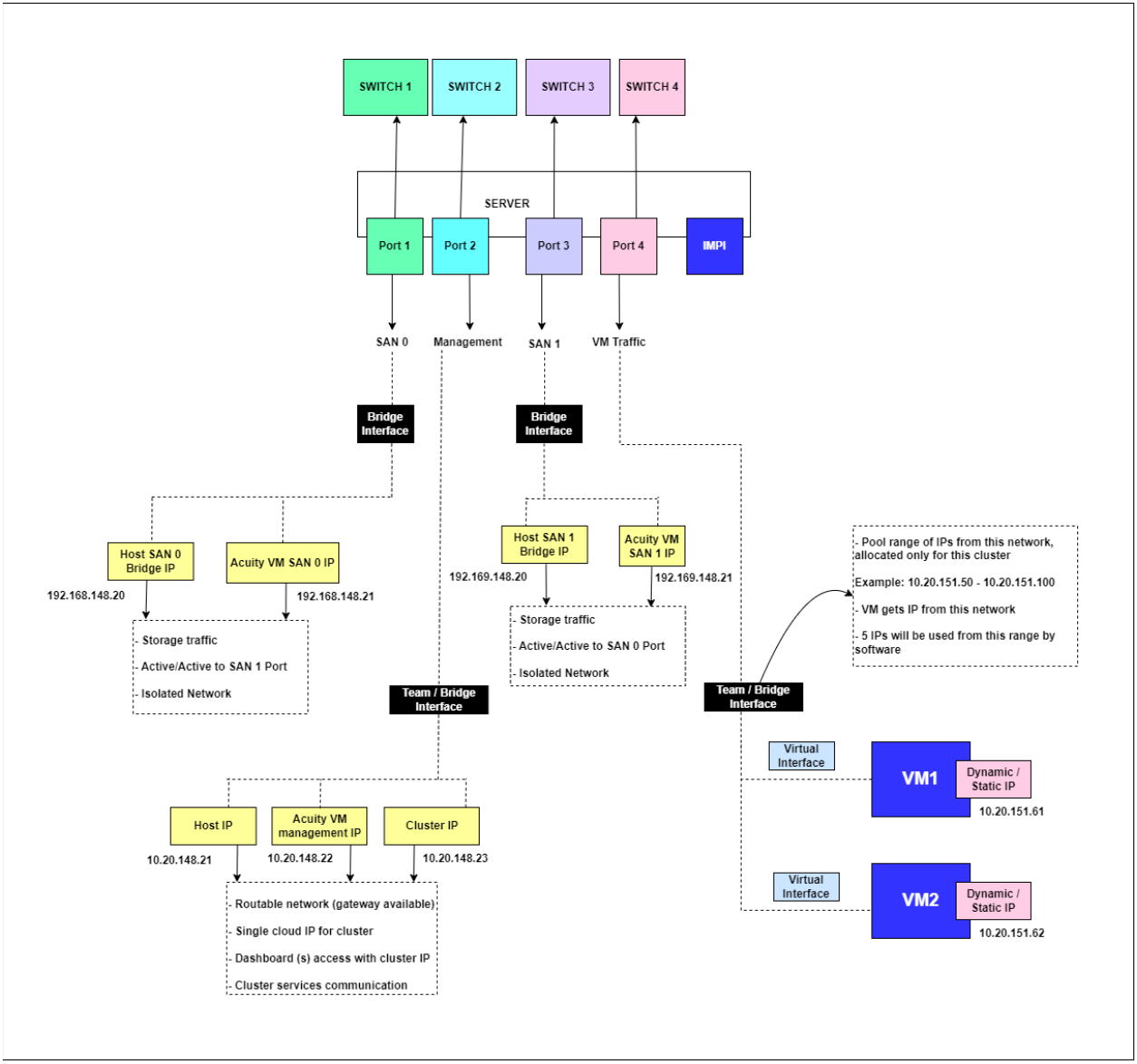
Configuration 1 – 4 Ports, Flat Network, 4 Switches

NOTE: The IPs illustrated in the diagrams are examples and will vary based on the customer's network environment.

Physical


SWITCH 1
SWITCH 2
SWITCH 3
SWITCH 4
SERVER
Port 1
Port 2
Port 3
Port 4
IPMI
SAN 0
Management
SAN 1
VM Traffic

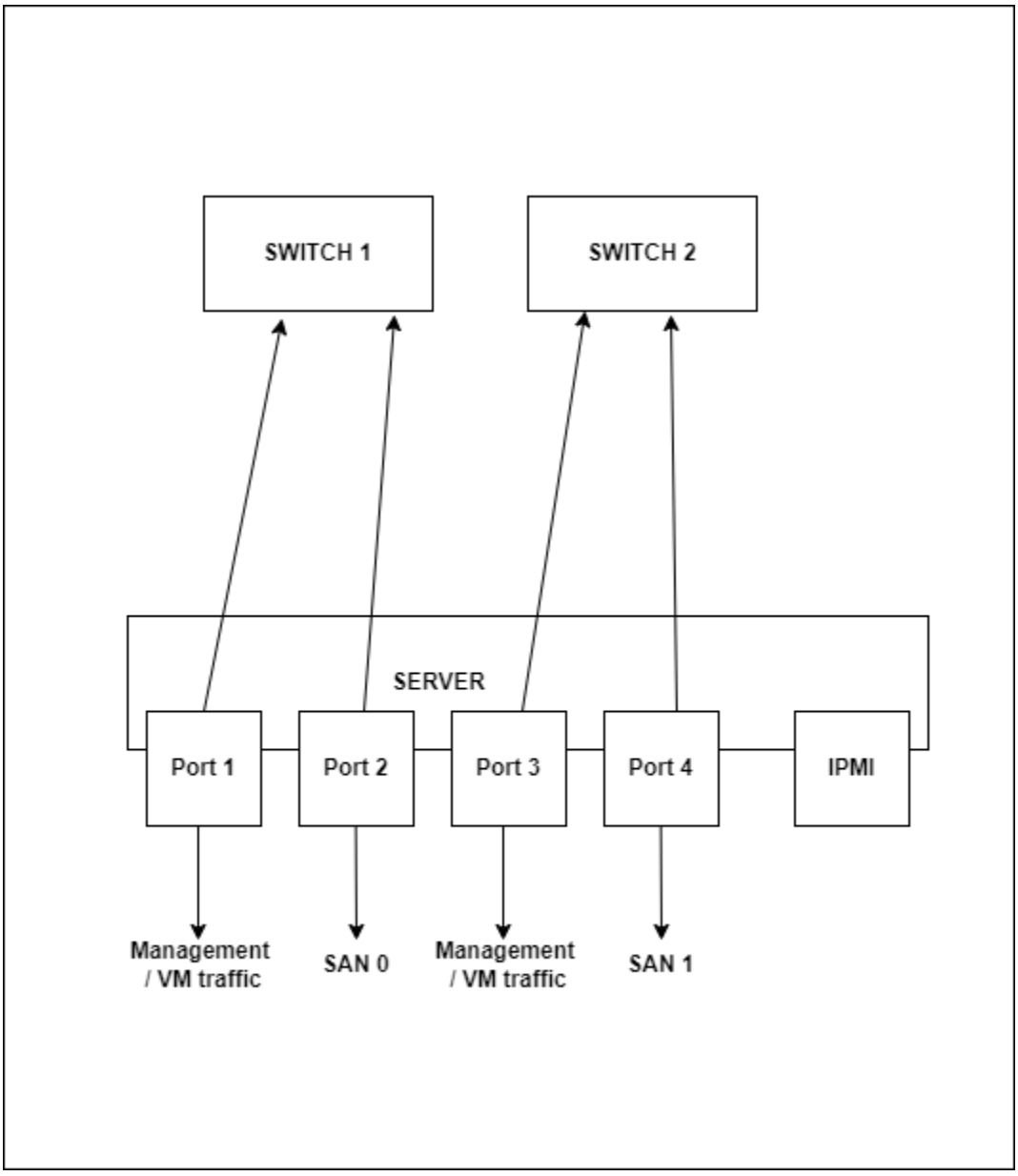
Logical



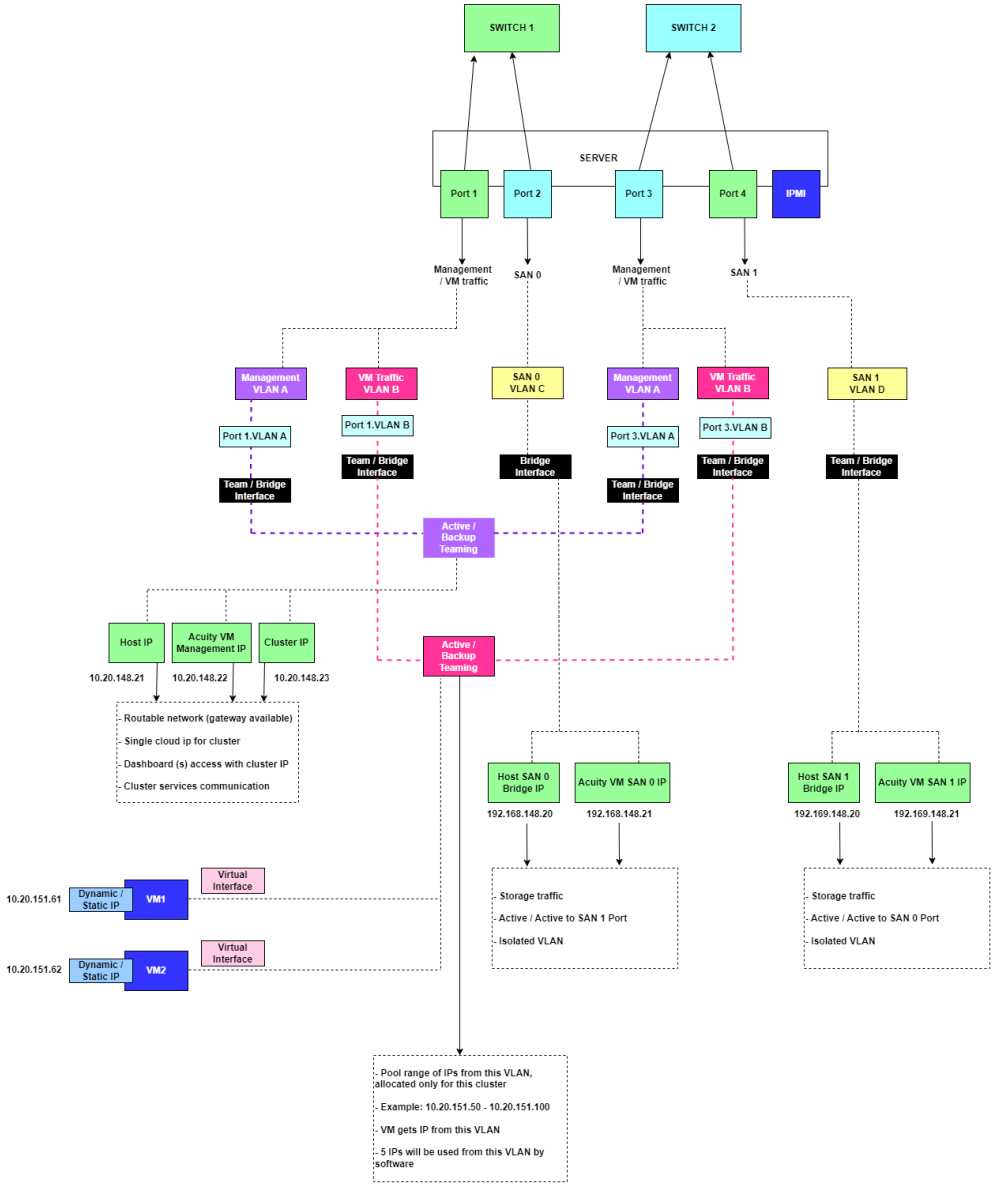
Configuration 2 – 4 Ports, 4 VLANs, 2 Switches

All VLANs should be trunk+tagged to switch ports.

Physical

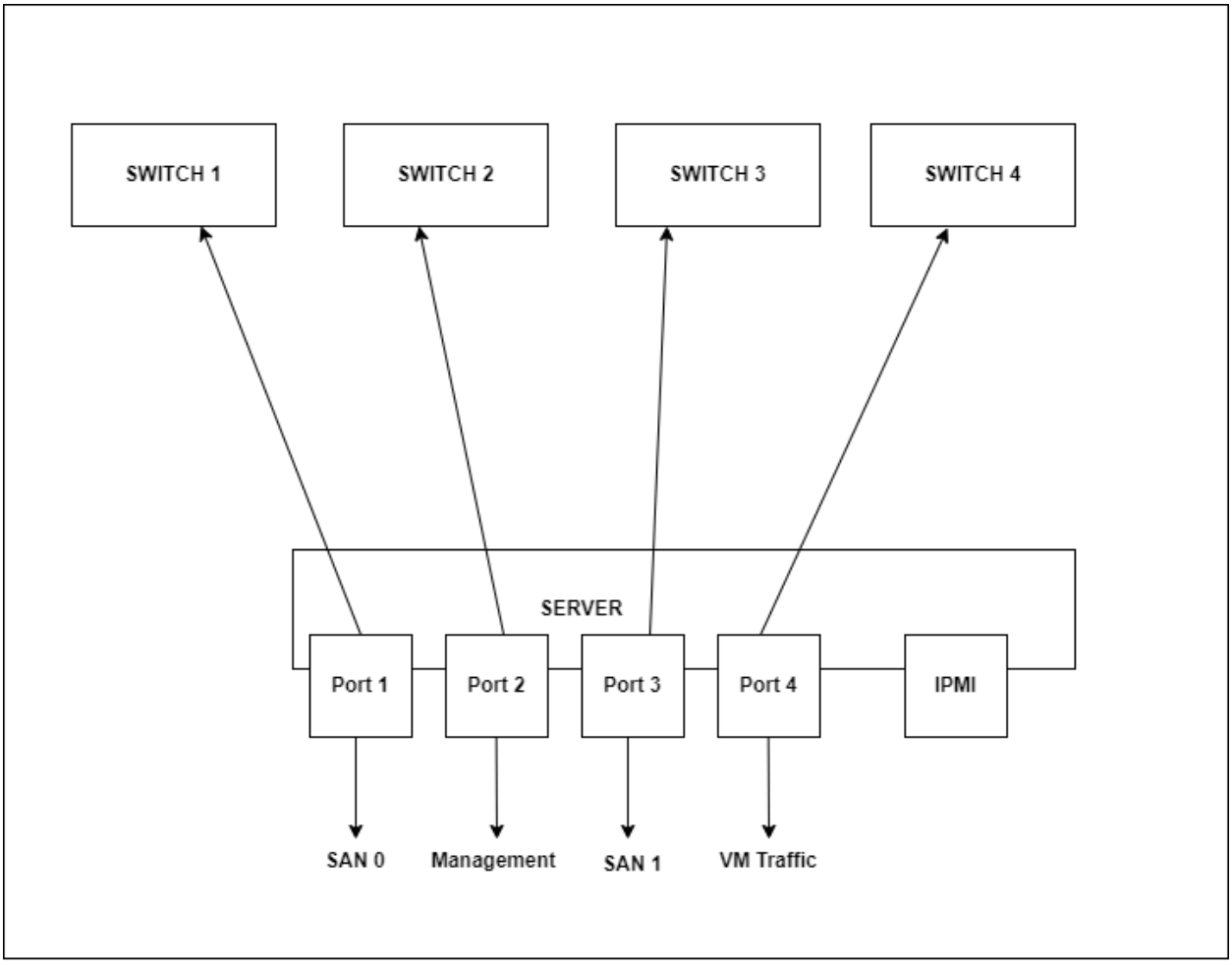

SWITCH 1
SWITCH 2
SERVER
Port 1
Port 2
Port 3
Port 4
IPMI
Management / VM traffic
SAN 0
Management / VM traffic
SAN 1

Logical

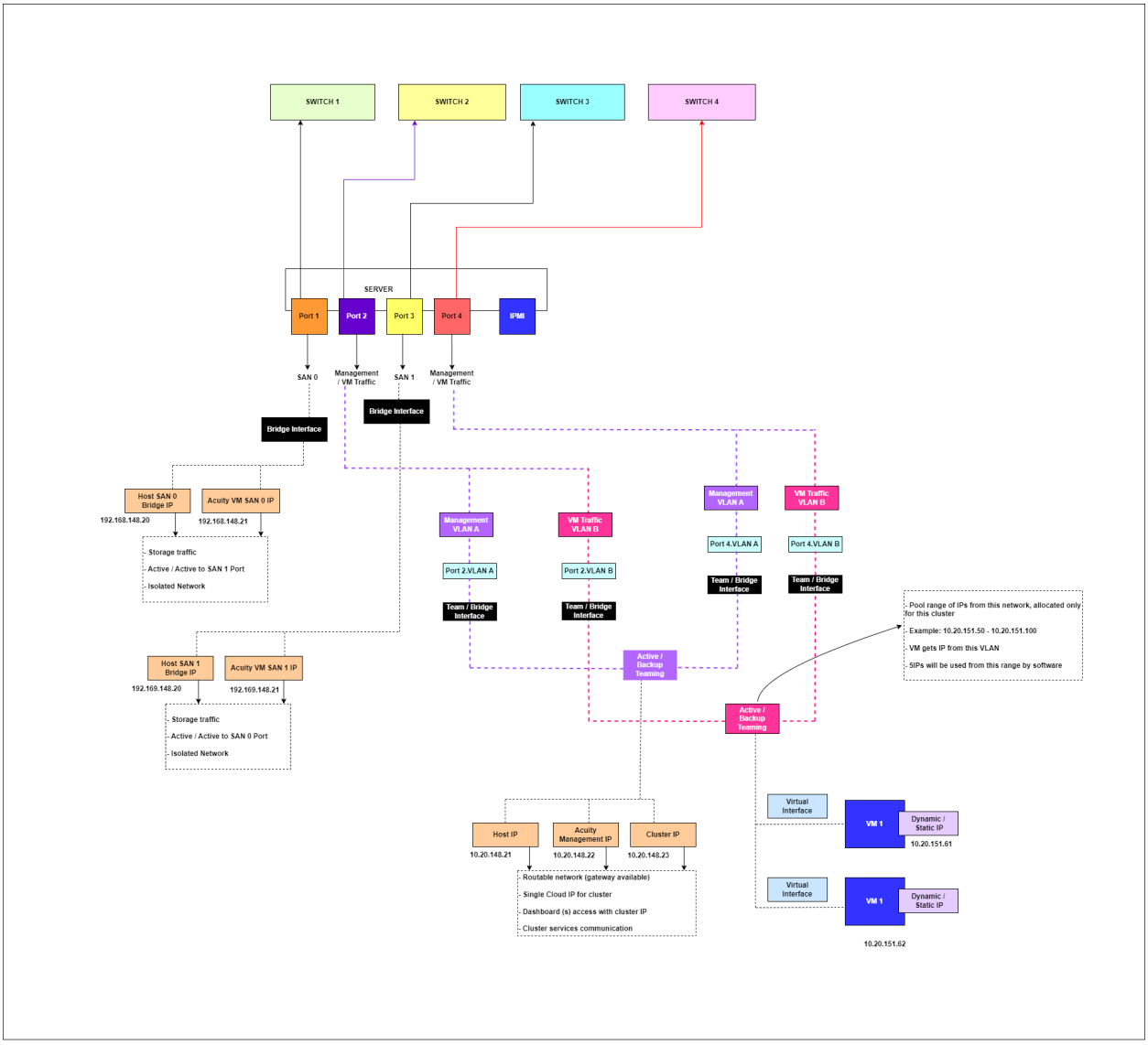

SWITCH 1
SWITCH 2
SERVER
Port 1
Port 2
Port 3
Port 4
IPMI
Management / VM traffic
SAN 0
Management / VM traffic
SAN 1
Management VLAN A
VM Traffic VLAN B
SAN 0 VLAN C
Management VLAN A
VM Traffic VLAN B
SAN 1 VLAN D
Port 1.VLAN A
Port 1.VLAN B
Port 3.VLAN A
Port 3.VLAN B
Team / Bridge Interface
Bridge Interface
Team / Bridge Interface
Team / Bridge Interface
Team / Bridge Interface
Team / Bridge Interface
Active / Backup Teaming
Host IP
Acuity VM Management IP
Cluster IP
10.20.148.21
10.20.148.22
10.20.148.23
Active / Backup Teaming
- Routable network (gateway available)
- Single cloud ip for cluster
- Dashboard (s) access with cluster IP
- Cluster services communication
Host SAN 0 Bridge IP
Acuity VM SAN 0 IP
192.168.148.20
192.168.148.21
Host SAN 1 Bridge IP
Acuity VM SAN 1 IP
192.169.148.20
192.169.148.21
- Storage traffic
- Active / Active to SAN 1 Port
- Isolated VLAN
- Storage traffic
- Active / Active to SAN 0 Port
- Isolated VLAN
10.20.151.61
Dynamic / Static IP
VM1
Virtual Interface
10.20.151.62
Dynamic / Static IP
VM2
Virtual Interface
- Pool range of IPs from this VLAN, allocated only for this cluster
- Example: 10.20.151.50 - 10.20.151.100
- VM gets IP from this VLAN
- 5 IPs will be used from this VLAN by software

Configuration 3 – 4 Ports, 2 Flat, 2 VLANs, 4 Switches

Physical

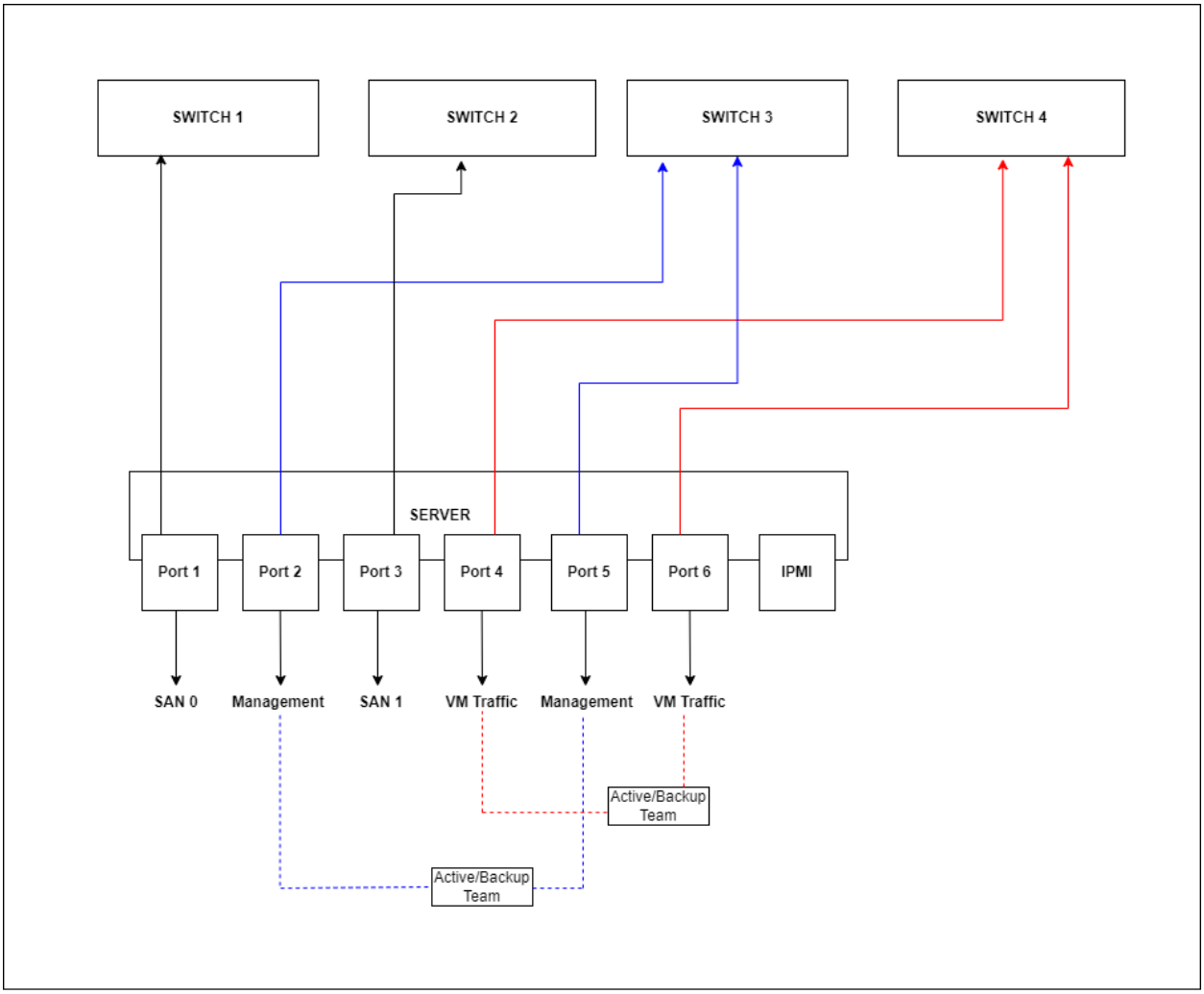


Logical

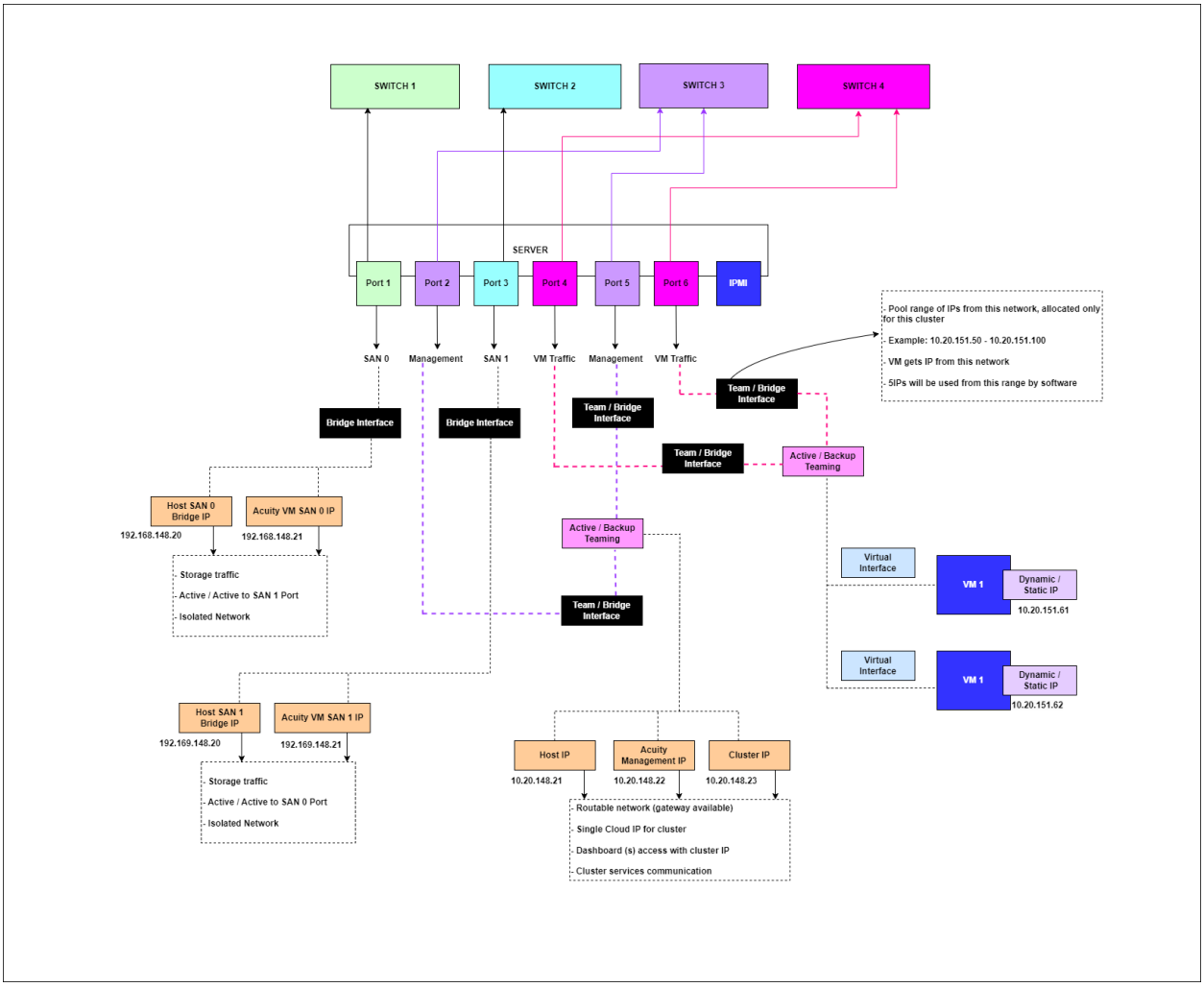

SWITCH 1
SWITCH 2
SWITCH 3
SWITCH 4
SERVER
Port 1
Port 2
Port 3
Port 4
IPMI
SAN 0
Management / VM Traffic
SAN 1
Management / VM Traffic
Bridge Interface
Bridge Interface
Host SAN 0 Bridge IP
192.168.148.20
Acuity VM SAN 0 IP
192.168.148.21
- Storage traffic
- Active / Active to SAN 1 Port
- Isolated Network
Management VLAN A
VM Traffic VLAN B
Port 2.VLAN A
Port 2.VLAN B
Team / Bridge Interface
Team / Bridge Interface
Management VLAN A
VM Traffic VLAN B
Port 4.VLAN A
Port 4.VLAN B
Team / Bridge Interface
Team / Bridge Interface
Host SAN 1 Bridge IP
192.169.148.20
Acuity VM SAN 1 IP
192.169.148.21
- Storage traffic
- Active / Active to SAN 0 Port
- Isolated Network
Active / Backup Teaming
Active / Backup Teaming
- Pool range of IPs from this network, allocated only for this cluster
- Example: 10.20.151.50 - 10.20.151.100
- VM gets IP from this VLAN
- SIPs will be used from this range by software
Host IP
10.20.148.21
Acuity Management IP
10.20.148.22
Cluster IP
10.20.148.23
- Routable network (gateway available)
- Single Cloud IP for cluster
- Dashboard (s) access with cluster IP
- Cluster services communication
Virtual Interface
VM 1
Dynamic / Static IP
10.20.151.61
Virtual Interface
VM 1
Dynamic / Static IP
10.20.151.62

Configuration 4 – 6 Ports, Flat, 4 Switches

Physical



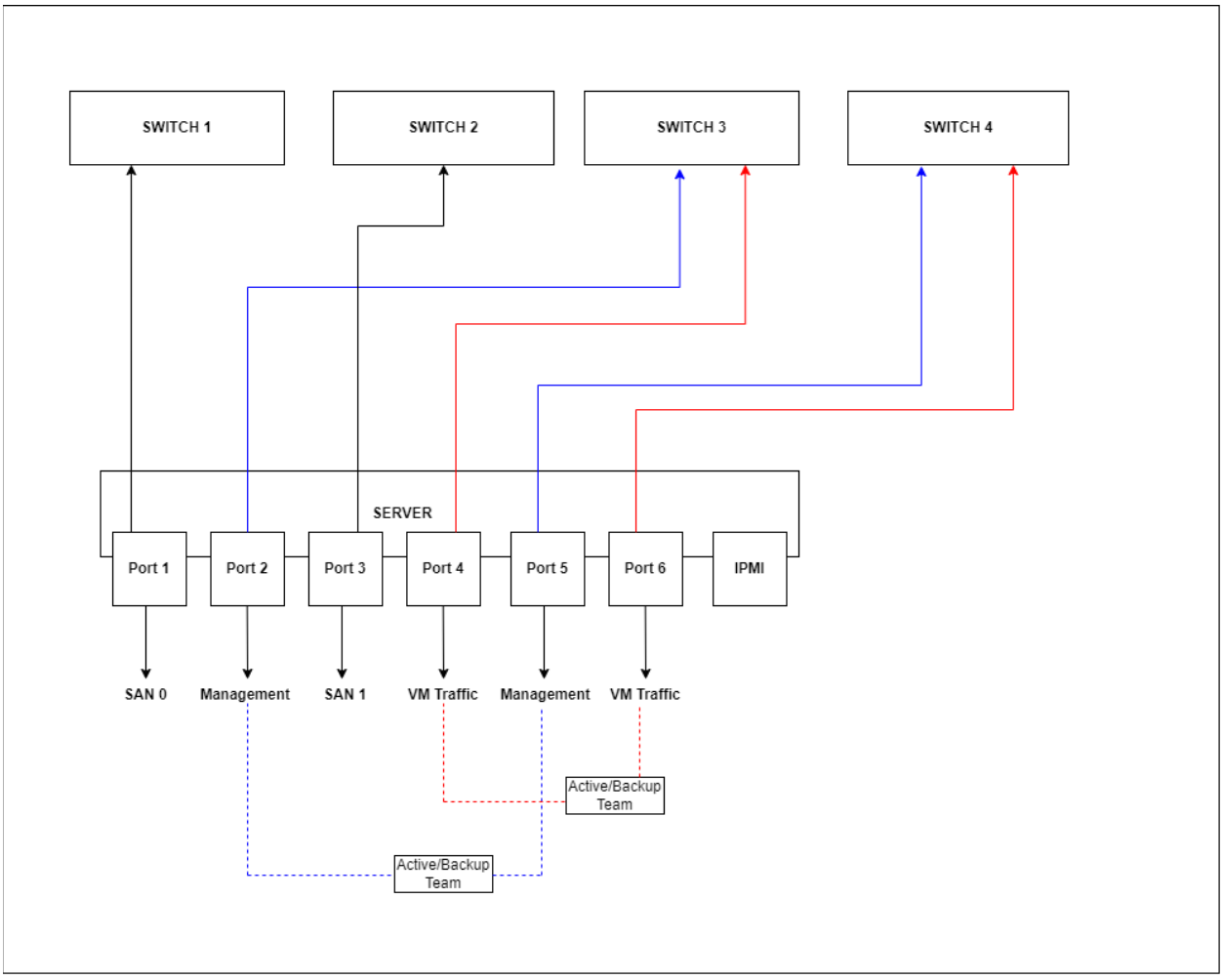
Logical



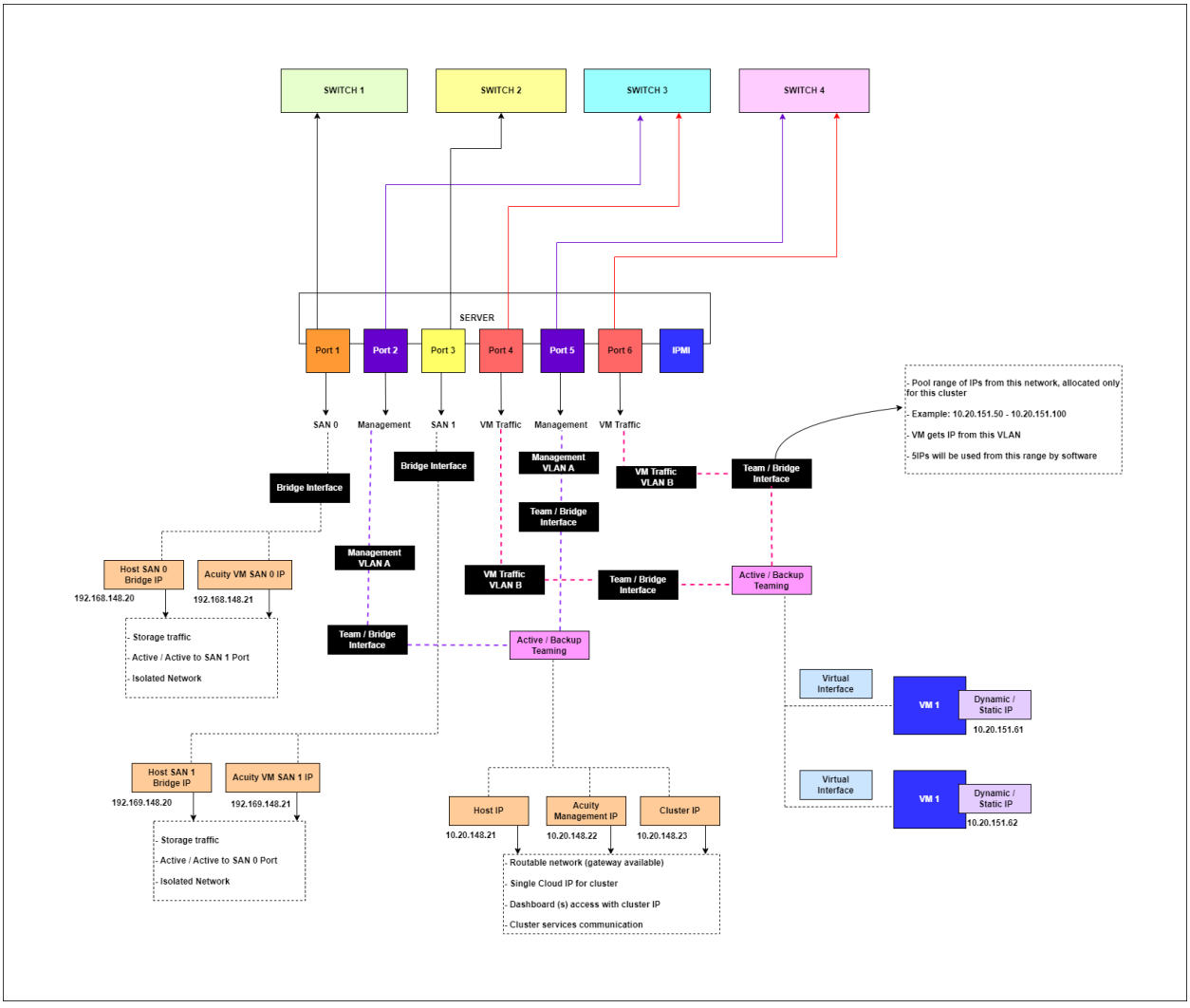
Configuration 5 – 6 Ports, 2 Flat, 2 VLAN, 4 Switches

VLANs should be trunk+tagged to switch ports.

Physical

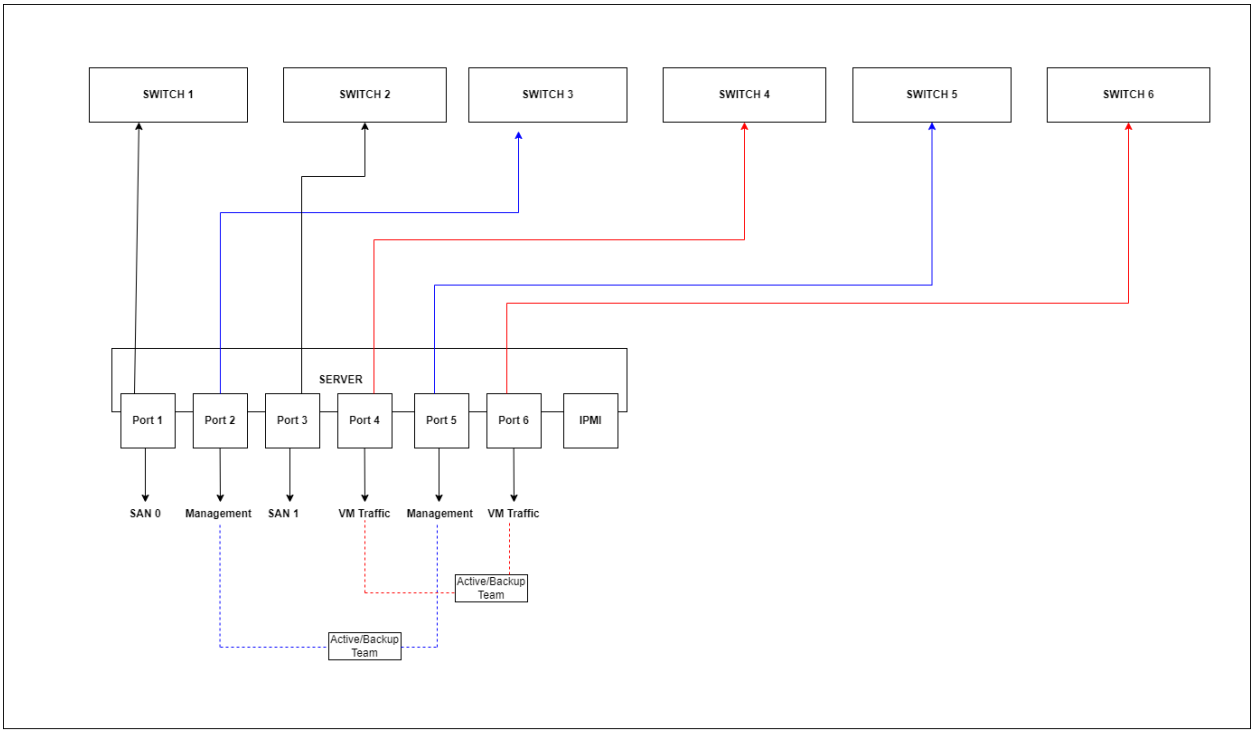

SWITCH 1
SWITCH 2
SWITCH 3
SWITCH 4
SERVER
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
IPMI
SAN 0
Management
SAN 1
VM Traffic
Management
VM Traffic
Active/Backup Team
Active/Backup Team

Logical

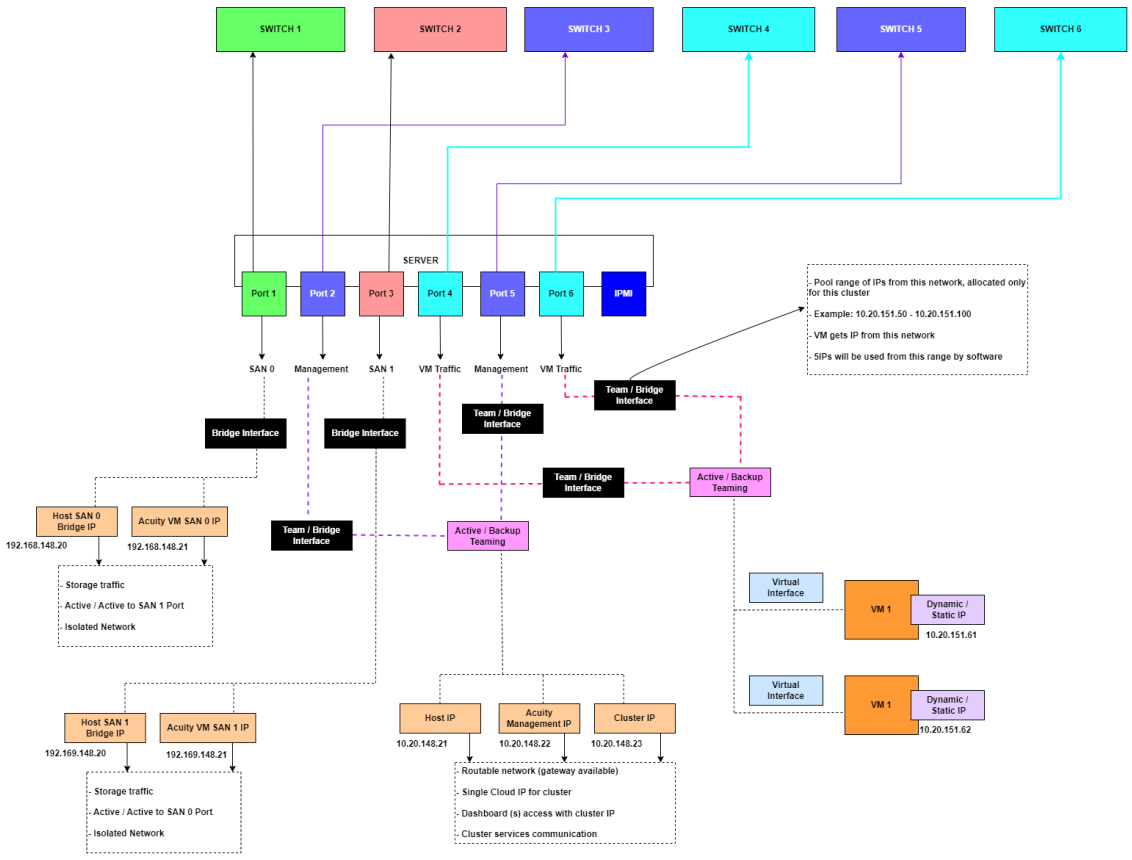

SWITCH 1
SWITCH 2
SWITCH 3
SWITCH 4
SERVER
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
IPMI
SAN 0
Management
SAN 1
VM Traffic
Management
VM Traffic
- Pool range of IPs from this network, allocated only for this cluster
- Example: 10.20.151.50 - 10.20.151.100
- VM gets IP from this VLAN
- 5IPs will be used from this range by software
Bridge Interface
Bridge Interface
Management VLAN A
VM Traffic VLAN B
Team / Bridge Interface
Team / Bridge Interface
Host SAN 0 Bridge IP
192.168.148.20
Acuity VM SAN 0 IP
192.168.148.21
Management VLAN A
VM Traffic VLAN B
Team / Bridge Interface
Active / Backup Teaming
- Storage traffic
- Active / Active to SAN 1 Port
- Isolated Network
Team / Bridge Interface
Active / Backup Teaming
Virtual Interface
VM 1
Dynamic / Static IP
10.20.151.61
Virtual Interface
VM 1
Dynamic / Static IP
10.20.151.62
Host SAN 1 Bridge IP
192.169.148.20
Acuity VM SAN 1 IP
192.169.148.21
Host IP
10.20.148.21
Acuity Management IP
10.20.148.22
Cluster IP
10.20.148.23
- Storage traffic
- Active / Active to SAN 0 Port
- Isolated Network
- Routable network (gateway available)
- Single Cloud IP for cluster
- Dashboard (s) access with cluster IP
- Cluster services communication

Configuration 6 – 6 Ports, All Flat Network, 6 Switches

Physical



Logical



USP 5.0 Beta supports the following port configuration:

- 1 x 10 Gbe – Management (OpenStack, Management UI/API, Guest VM)
- 1 x 10 Gbe – VM Traffic (Application / camera network)
- 1 x 10 Gbe – SAN 0 (Acuity storage traffic)

1 x 10 Gbe – SAN 1 (Acuity storage traffic)

***NOTE**: For failure redundancy it is highly recommended that the SAN 0 and SAN 1 networks be on separate switches.*

IP Address Requirements

The USP software will require a number of IP addresses in each of the different ranges.

Network	IP Address Requirements
Management	• Host IP (1 per server) • Acuity Management IP (1 per server) • Cluster IP (1)
SAN 0	• Host bridge IP (1 per server) • Acuity Storage VM (1 per server)
SAN 1	• Host bridge IP (1 per server) Acuity Storage VM (1 per server)
VM Network (Application)	• DHCP Agents (2) • Neutron Gateway (2) • Monitoring VMs (4) • Default department (1) • Guest VMs (1 * number NICs * number of VMs)
Out-of-band Management	1 IP per server

Ports Used

For ports used by the software, see the Appendix C – Ports Used section.

Install the USP OS

The following section describes how to install the USP Operating System (OS) on your servers. This process must be performed on every server that will become part of the USP cluster. The USP OS can be installed serially or in parallel on each node.

***NOTE**: If you purchased an appliance from Quantum that already has the USP OS installed, you can skip this step and go directly to the Configure the Management Network section below.*

Boot from ISO

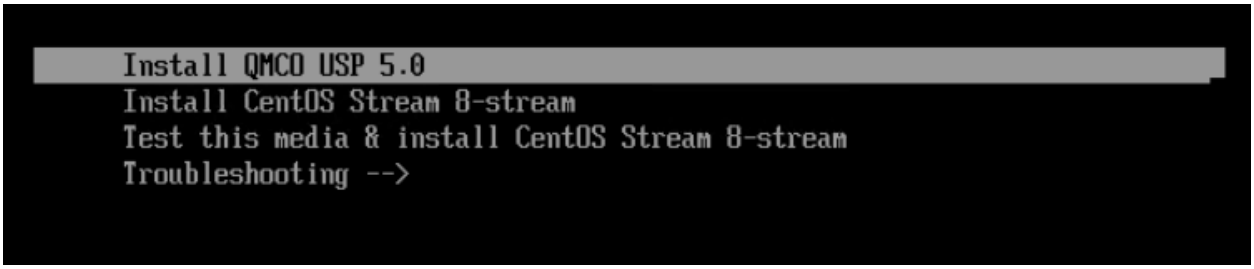
Each server must boot from the provided Quantum USP ISO file. This can be done by creating a bootable USB stick or by loading the ISO from a network share to the server's virtual media device.

To install the USP OS, you must boot each node member from the provided ISO file. See the following appendix sections to use either of the following methods:

- For instructions on creating a bootable USB, refer to Appendix A – Creating a Bootable USB Key
- For instructions on booting to the ISO using virtual media in the out-of-band management interface, refer to Appendix B - Booting from an ISO Through Out-Of-Band Management.

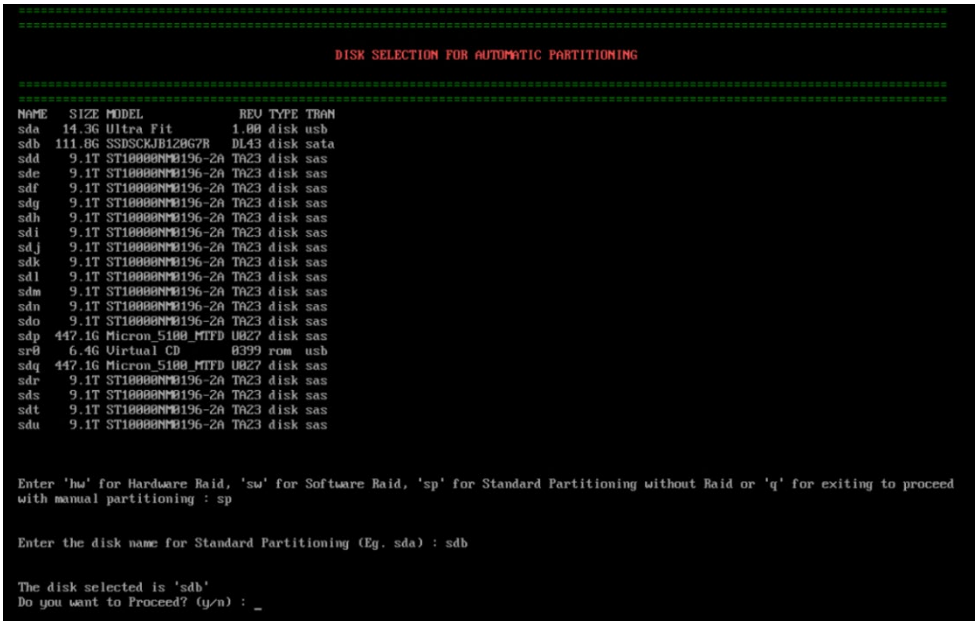
Install USP

Once the server is booted to the ISO, select **Install QMCO USP 5.0.**



Selecting the OS Disk Configuration

The next step is to choose your OS partition configuration. The installation screen will display the detected disks and prompt you to choose *Hardware Raid, Software Raid,* or *Standard Partitioning.*



Hardware Raid (hw)

Select the **Hardware Raid** option to install the USP Operating System on disks that are connected to a hardware RAID controller and have been previously configured using the server's out-of-band management interface or BIOS.

> ***NOTE**: If you select the **Hardware Raid** option and select a disk that is not configured for hardware raid, the installation will still proceed, and the disk will be partitioned using the **Standard Partitioning** method.*

Software Raid (sw)

Select the Software Raid option to configure software raid on 2 disks that are not connected to a hardware RAID controller. It is recommended to select two disks of the same type (HDD or SSD) and size.

Standard Partitioning (sp)

Select the Standard Partitioning option to install the USP Operating System on a single drive without hardware or software RAID. It is recommended to install the OS on an SSD drive, however either an SSD or HDD can be selected.

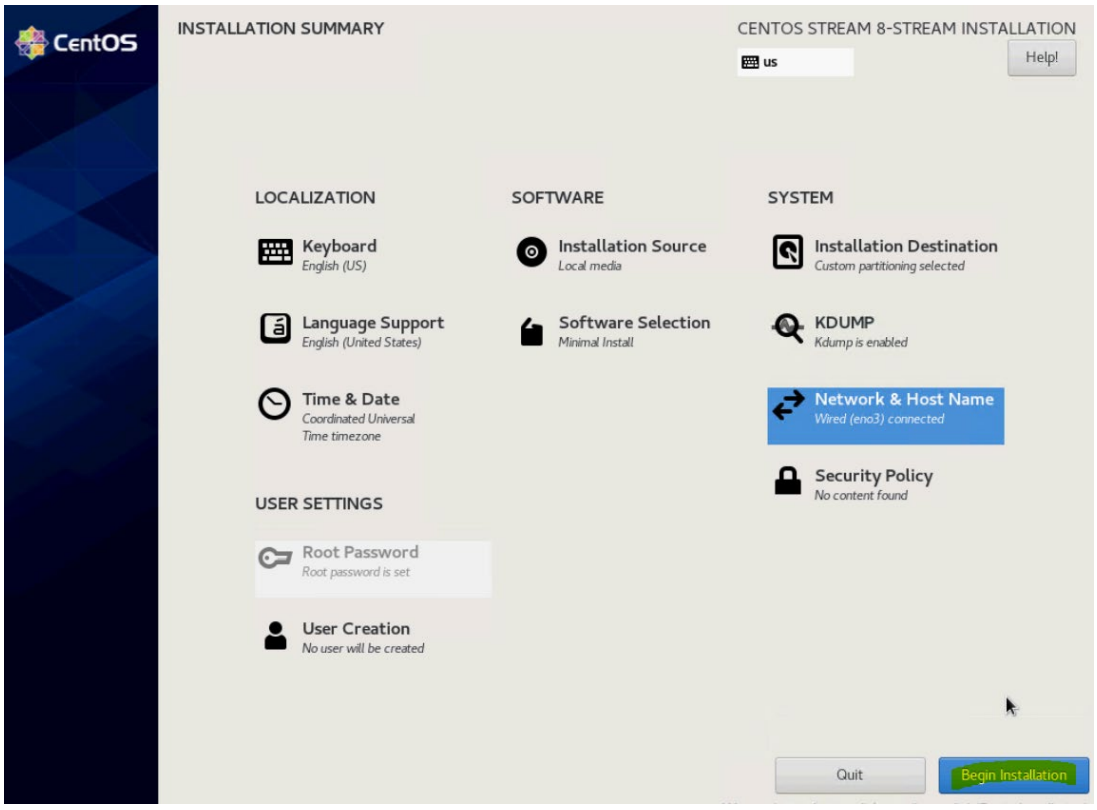
Manual Partitioning

CRITICAL: *Manual partitioning is not supported for this release. Only use the above options to install the USP OS.*

Running the Installation

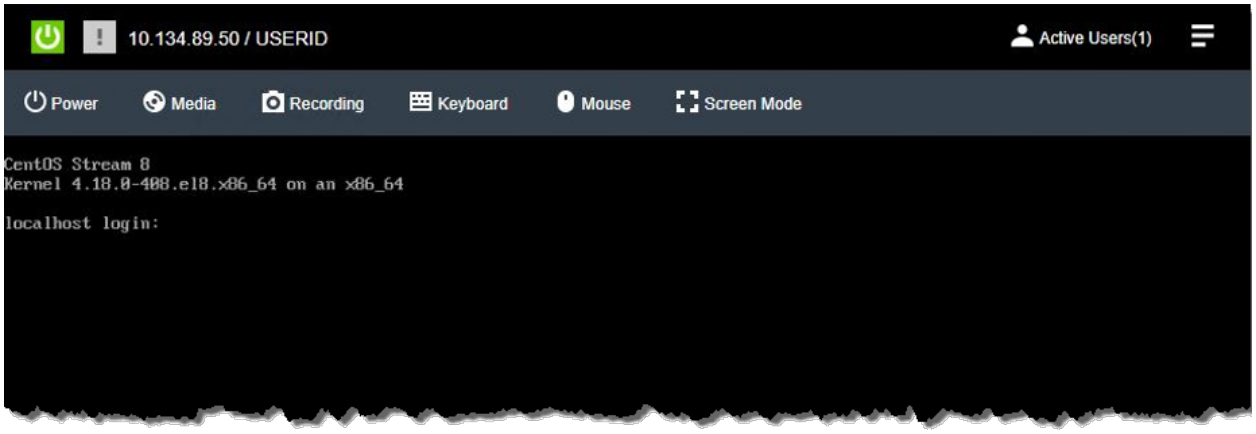
1. After choosing the installation disks and selecting **Y** to proceed, the CentOS Installation Summary screen is displayed. The screen will automatically advance to the Installation Progress screen.

NOTE: *If any buttons are selected on the CentOS installation screen, the install may not proceed automatically. If this happens, press the "Begin Installation" button to start the process.*



2. Once the installation is complete, click on **Reboot System** to reboot the system.

3. After rebooting the servers, they will boot to an intermediate state.

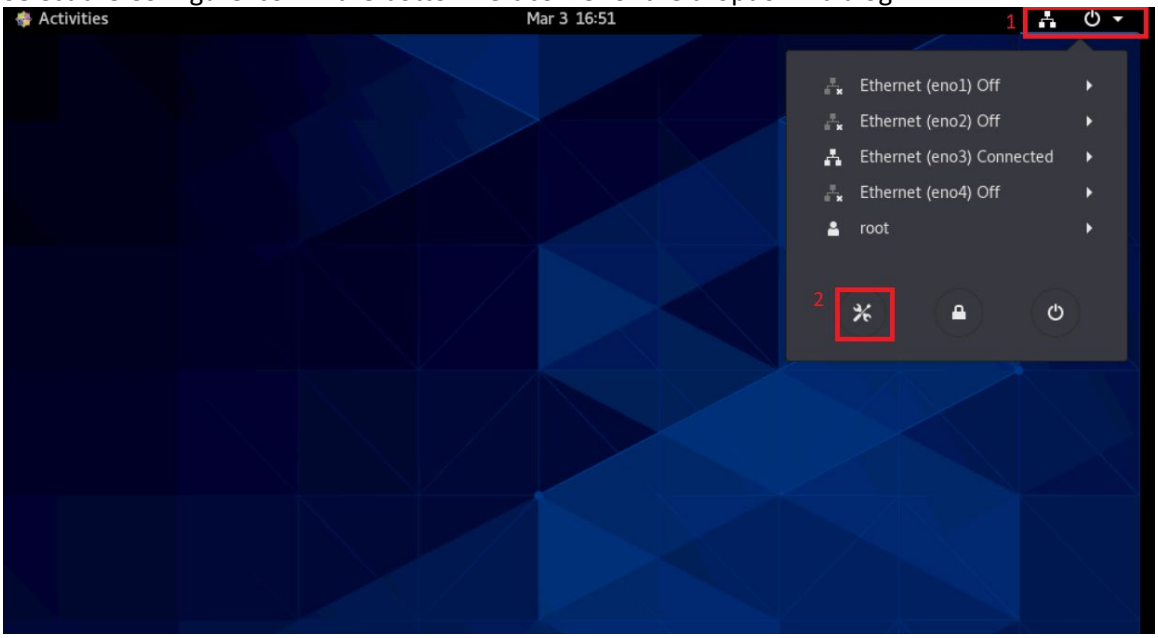


You can log in and watch the processing, but do not execute any keystrokes. The system will automatically boot to the console that is seen below.

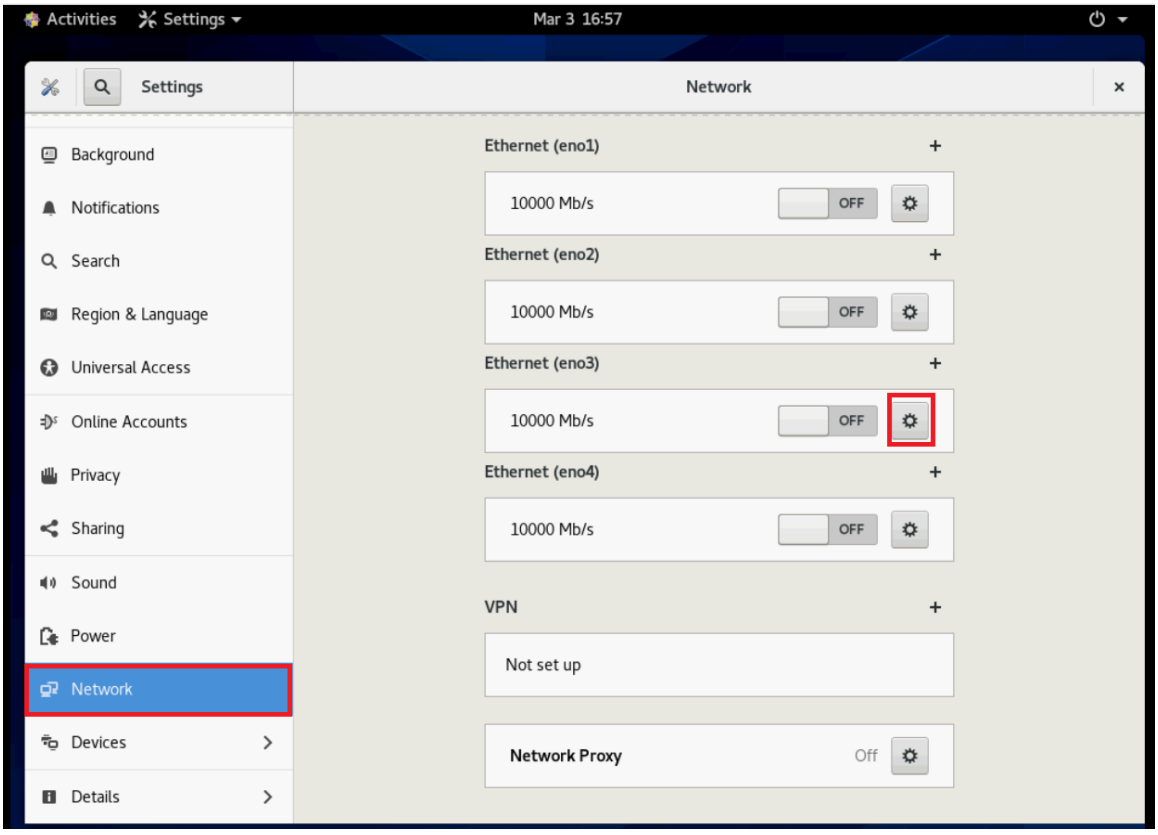
Configure the Management Network

After installing the USP OS, you must log on to the console of each server and manually configure the management network.

1. Log on to the CentOS operating system using the default credentials.
   - **Username:** *root*
   - **Password:** *server1011q2w*
2. Select the Network dropdown in the upper-right corner.
3. Select the Configure icon in the bottom-left corner of the dropdown dialog

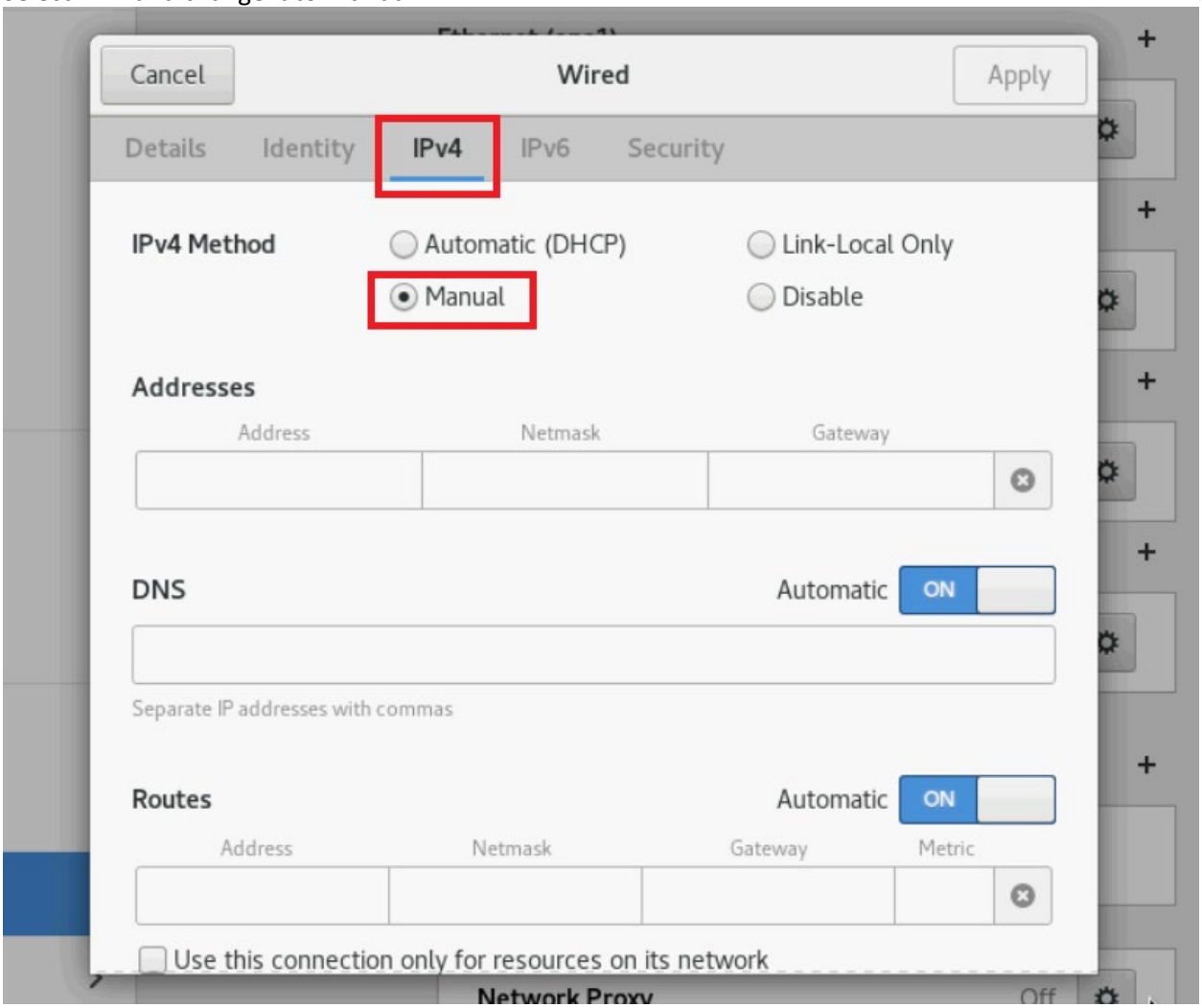


4. Select **Network** on the left side of the configuration dialog and press the **Configure** button for the correct network

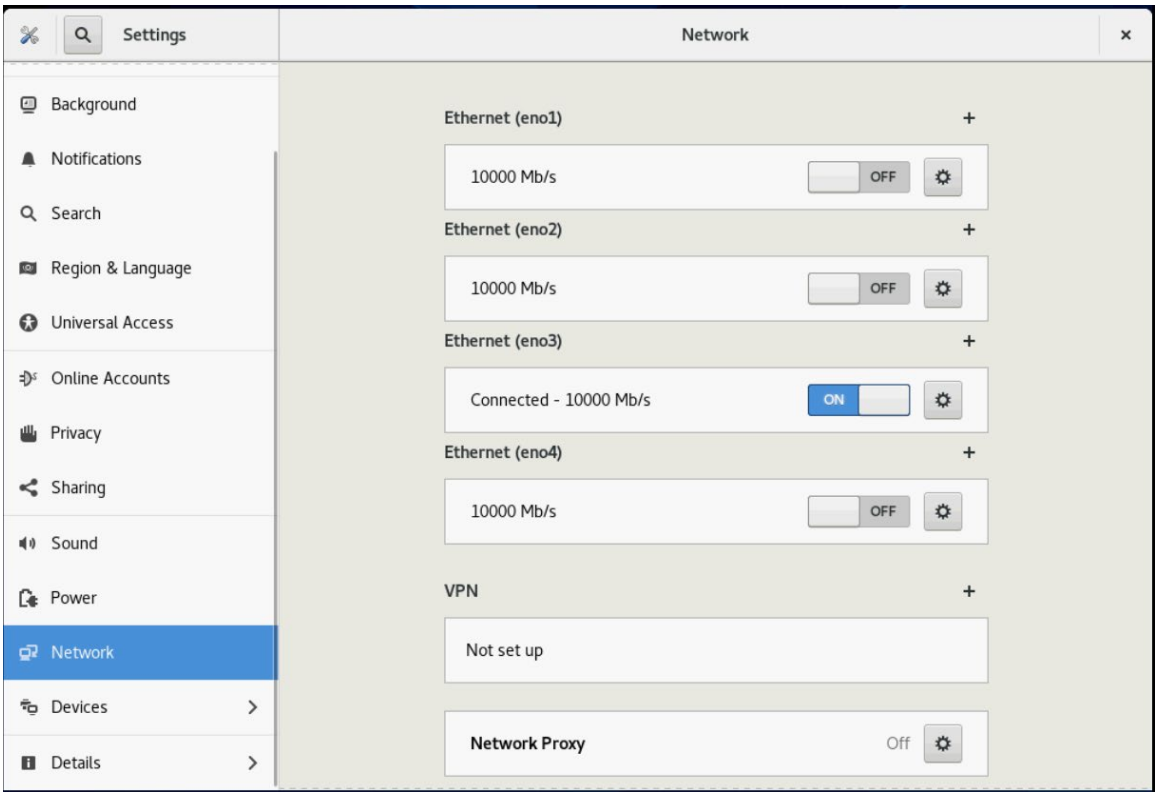


CRITICAL: *Physical ports are not always enumerated in the same order on each server. Ensure that you choose the correct Ethernet port on each host. Use the ping utility to confirm that all hosts can ping each other once the IP addresses are configured.*

5. Select **IPv4** and change it to **Manual**.



6. Enter the values for **IP Address**, **Netmask**, **Gateway,** and **DNS**. If you have multiple DNS addresses, enter them as comma-separated values.
7. Click on **Apply.**
8. To load the new configuration, restart the network by toggling the **Off/On** button.



Configure VLAN

If you configured the management networks using VLAN in the installation template, then you need to follow these steps on each node to finish configuring your network.

1. Navigate to the out-of-band management web page and log in to the server console.
2. Open the **Terminal** application from the **Application** menu in the top-left corner.
3. Execute the following command to change directories: cd /etc/sysconfig/network-scripts
4. Edit the management network configuration file. The file will be named after the interface name. For example, if your management port is **eno1**, the network file will be called **ifcfg-eno1**.
5. Edit the network configuration file by typing the following command in the terminal:
   vim ifcfg-eno1
6. Type the following to enter Insert mode: i
7. Add/modify the content to look like this:

   TYPE=Ethernet
   BOOTPROTO=none
   DEVICE=eno1
   ONBOOT=yes

8. To save the file, press the Escape key and type **:wq**
9. Press Enter to save.
10. Create a new file using the VLAN tag you specified for this network during installation. For this example, we will use '3' as our VLAN tag.
    a. Type the following to open a new file: vim ifcfg-eno1.3
    b. Type the following to change to Insert mode: i

c. Add the following content to the file.

```
DEVICE=eno1.3
BOOTPROTO=none
ONBOOT=yes
IPADDR=10.20.3.231
PREFIX=24
GATEWAY=10.20.3.1
VLAN=yes
```

d. Save the file by pressing the Escape key and typing **:wq**
e. Press Enter to save the new file.

11. Restart service by typing this command: systemctl restart NetworkManager

---

NOTE:

eno1 is example interface, it can change based on the hardware.

3 is example VLAN for management, it will depend on your network environment.

DEVICE=interface-name.vlanid

PREFIX is CIDR for subnet

IPADDR and GATEWAY as per subnet

Configure the USP Cluster

Once the USP OS been installed on all nodes, the next step is to configure the cluster.

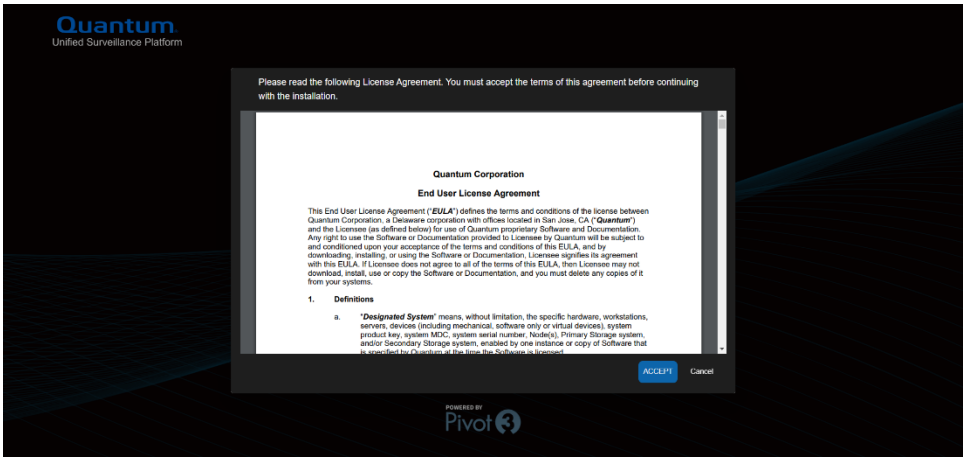
NOTE: *The USP Cluster setup process only needs to be executed on one of the nodes. You can choose any of the nodes to run this workflow.*

CRITICAL: *IPMI over LAN must be enabled on each server in the cluster. If this setting is disabled, the configuration process will fail.*

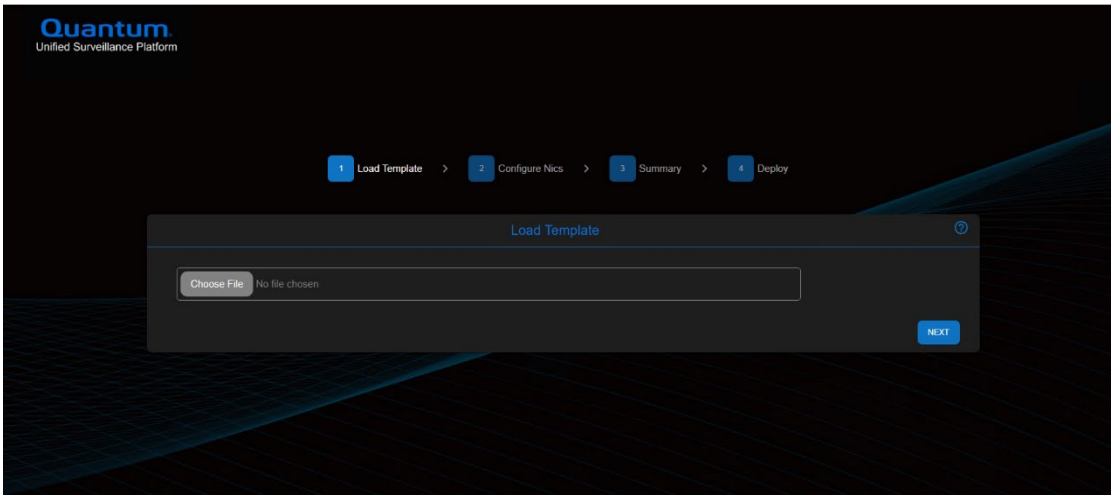
---

1. The template upload UI can be accessed from a web browser by pointing to the management address of the first host.

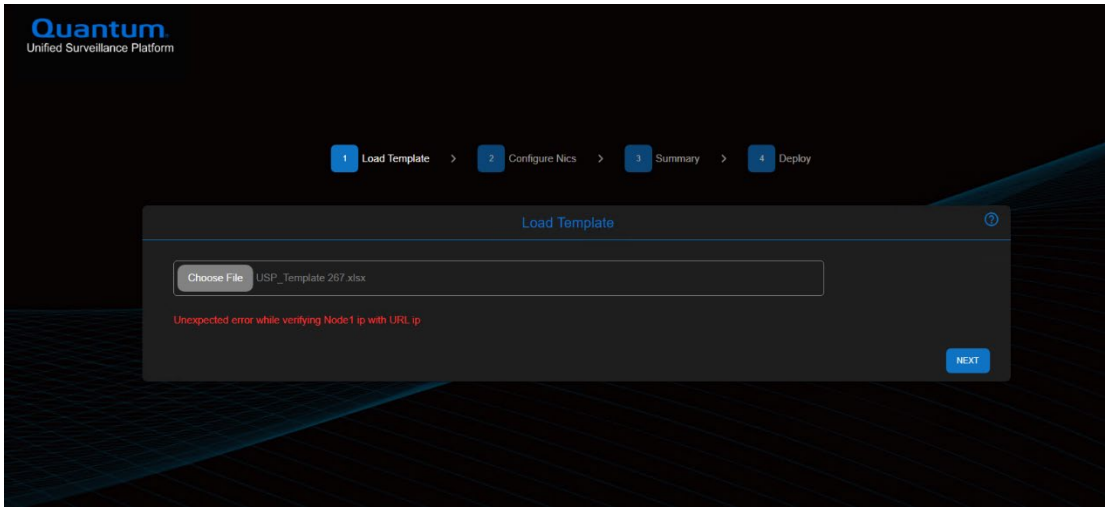
NOTE: You must accept terms and conditions of EULA to move forward with installation.



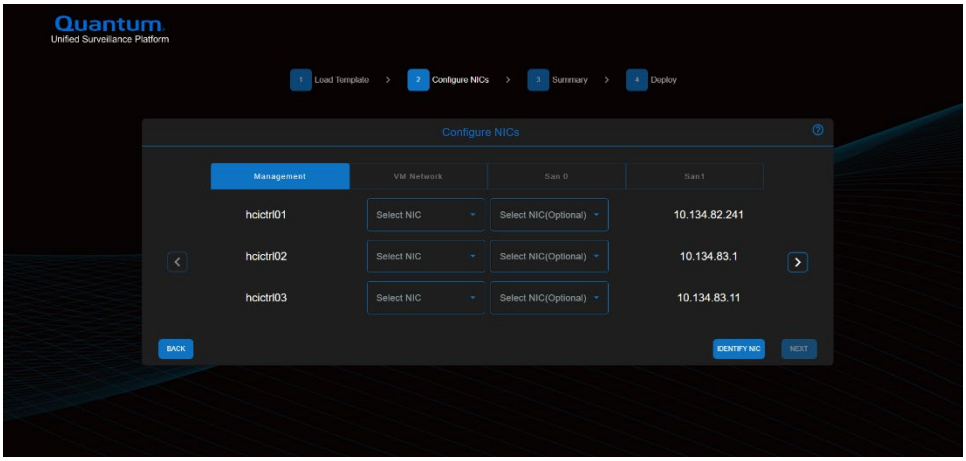
2. Click the “Choose file” button and browse to the pre-configured template file you want to upload. Click the “Next” button to continue.



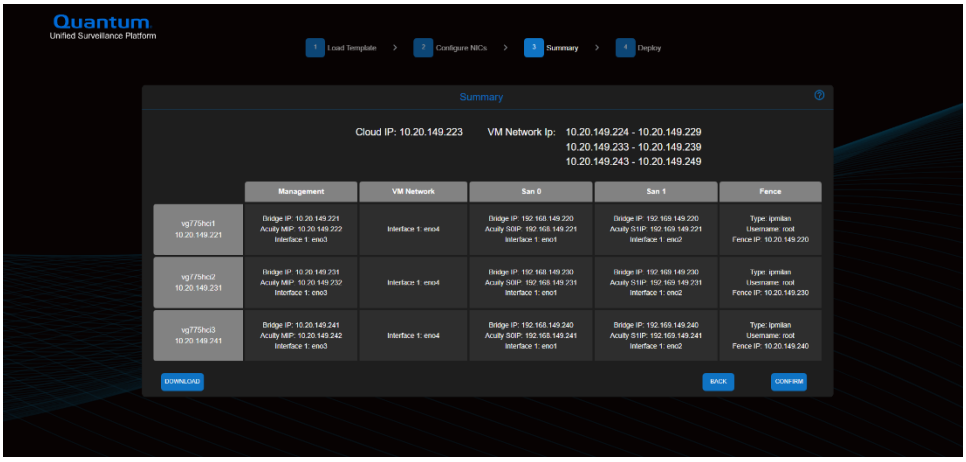
NOTE: If there is a validation issue with the template, you will get an error message on the UI. You can update the template as needed and upload again.

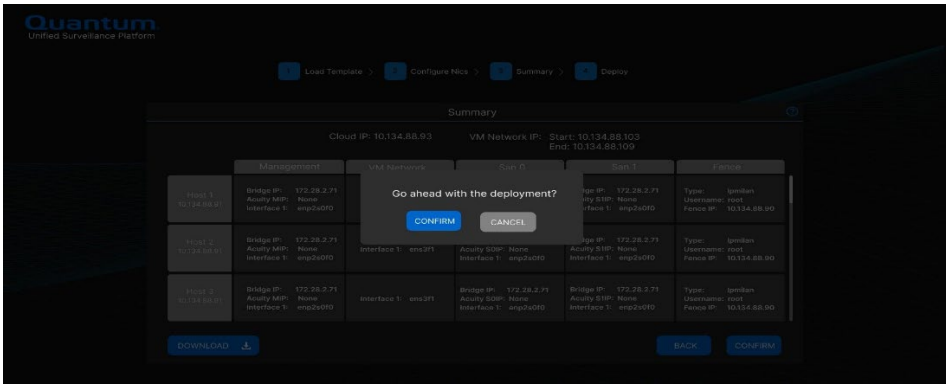


3. For each network, select the correct physical NIC on each host. You can use the "Identify NIC" button to blink the light on the physical NIC to ensure the correct ones are chosen. Click the "Next" button after completing the NIC details of all tabs.

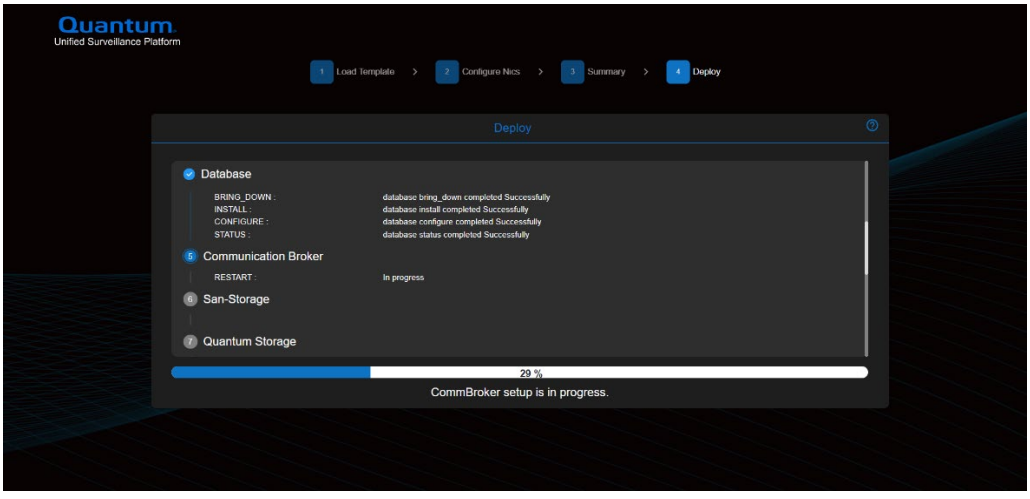


4. View the summary and confirm all the information is correct.

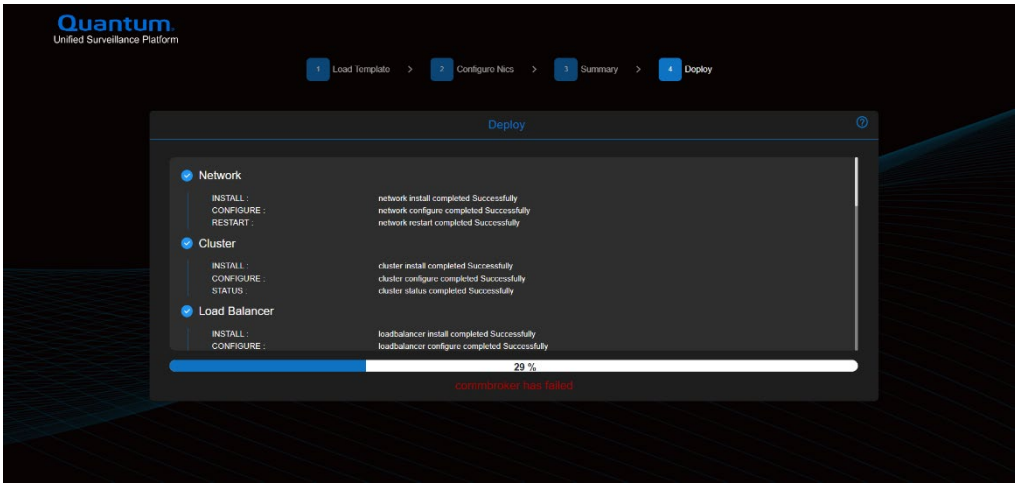




5. A log of the steps and a progress bar will be displayed.



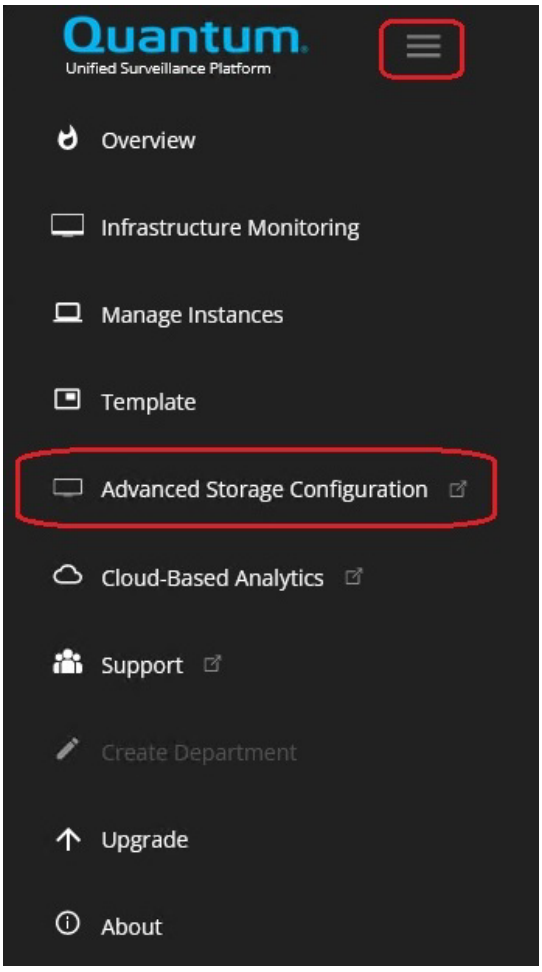
NOTE: If the deployment fails, you will get a high-level detail of the failure as shown below.



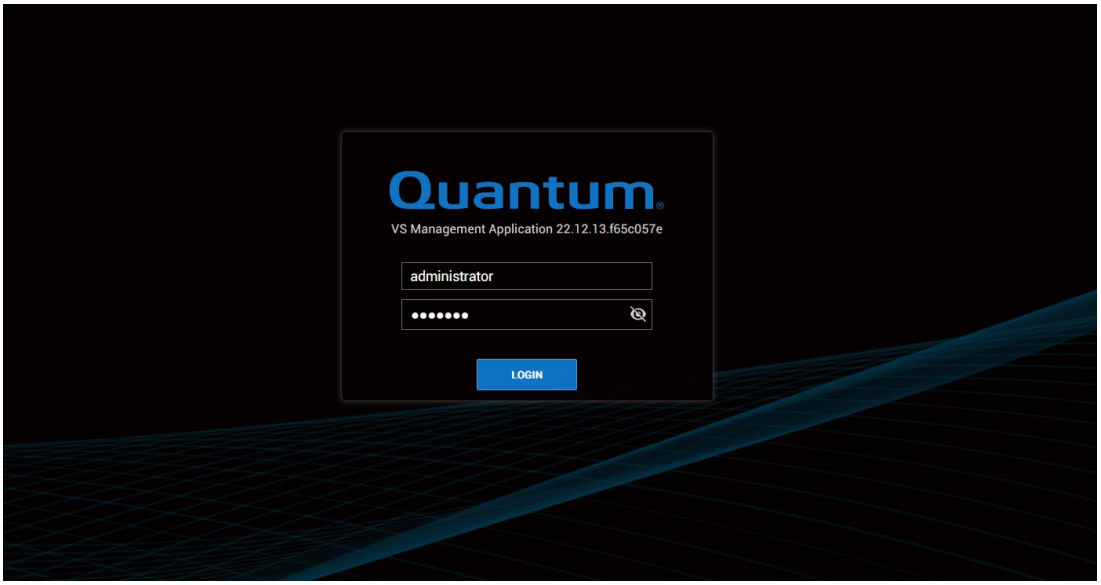
6. A confirmation page will display that the deployment was successful. There will be a link attached to visit the USP Management Application.

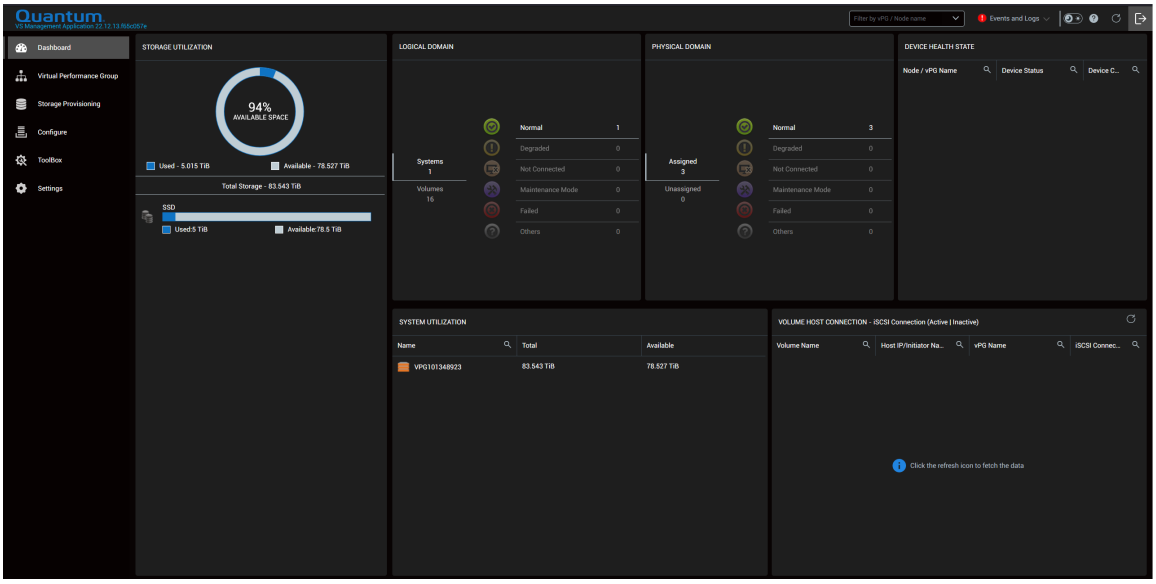
7. Once the installation is complete, launch the USP Management Application in the browser.

   https://<cluster_ip>/quantum/usp/dashboard



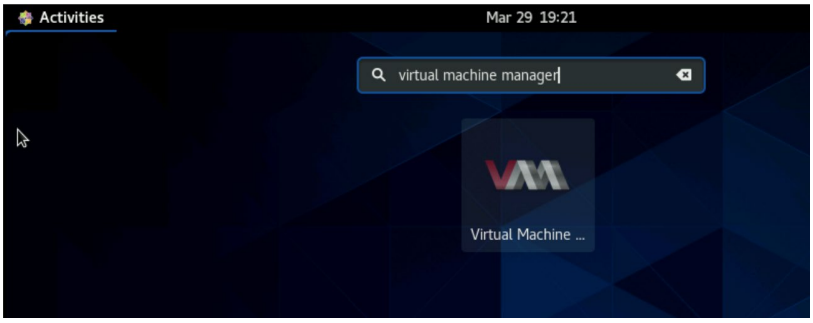
8. Log on to the Advanced Storage Configuration Utility using the same credentials you used to access the Quantum USP Management Application.



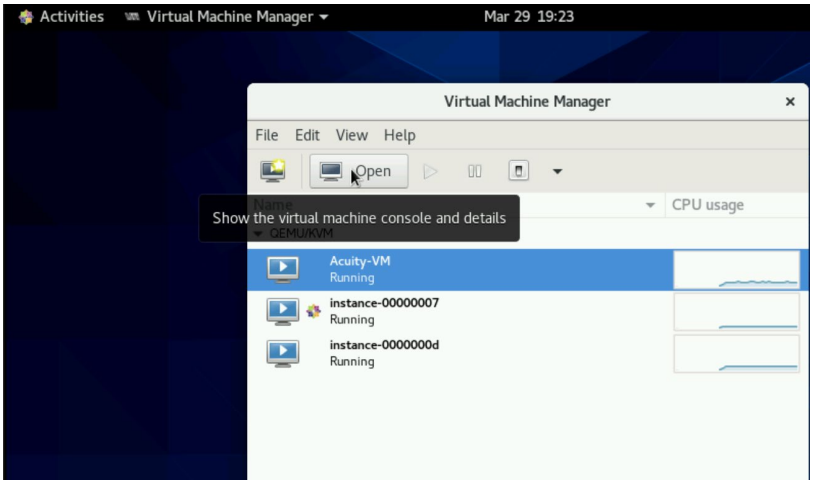


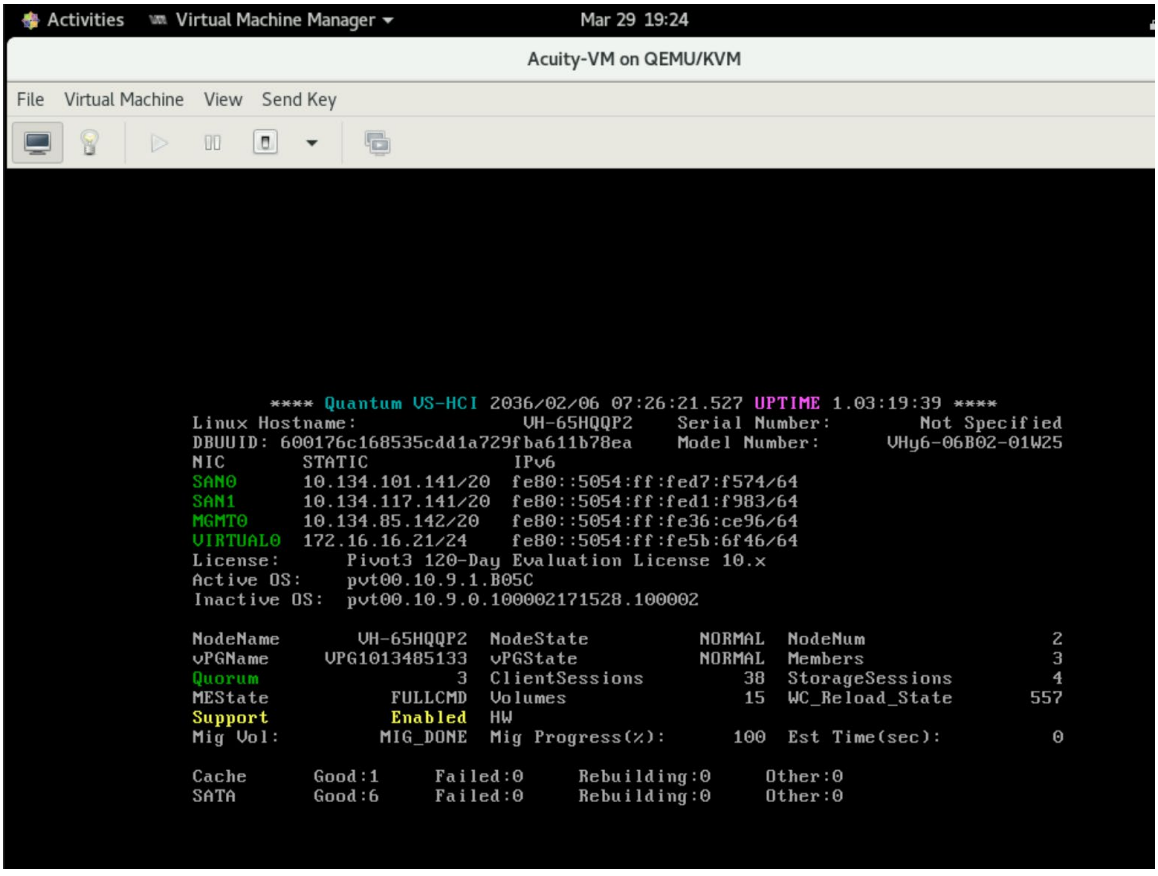
Viewing the Acuity VM Console

1. Log on to the USP CentOS console.
2. Click the **Activities** button at top-left.
3. Search for **Virtual Machine Manager** and click on the icon to launch.



4. Select the **Acuity-VM** instance and click on **Open** to launch the console.





Network Adapter Physical-to-Logical Mapping

While installing the USP software, you will be prompted to select the adapter within the Linux operating system to use for each network. It is important to ensure that the physical-to-logical port mapping for each host is correct, especially if there are isolated switches for the different networks. The logical adapter you choose on each host should be cabled to the same switch as the logical adapters for the others hosts for the same network.

During installation, the USP Configuration Utility will attempt to blink the physical ports on the server so that you can ensure that the ports are cabled correctly (the same as the other servers).

If for some reason the blinking functionality does not work, or it is impossible to physically see the back of the server, it may be necessary to log in to each server using SSH and confirm that you can ping between all the adapters in the cluster for the given network.

Cluster Status Failed Popup During Cluster Setup

This popup message can be displayed for several different reasons. See the below sections to help debug the issue further.

iDRAC Password Reset Issue

Identify Error: On the system running the USP Cluster Setup utility, look at the contents of the <todo> /var/log/enclouden/orchestrator_run_history.log file and check for the existence of this message:

If you run the following command using ipmitool you will see the error message “RAKP 2 HMAC is invalidError: Unable to establish IPMI v2 / RMCP+ session”.

ipmitool -I lanplus -H [iDRAC_IP_ADRESS] -U [USERNAME] -P [PASSWORD] -v chassis power status

Cause: If there were hardware replacements in this server, for example a motherboard replacement, the iDRAC password will not work for the IPMI interface even though you can still log in to the Web Interface.

Solution: To fix this issue you will need to reset the iDRAC password and then restart the USP cluster setup.

Validation: Once the iDRAC password has been reset, you can verify by running the following ipmitool command and observing a success message.

ipmitool -I lanplus -H [iDRAC_IP_ADRESS] -U [USERNAME] -P [PASSWORD] -v chassis power status

Troubleshooting

Launching the Acuity Advanced Storage Configuration Utility

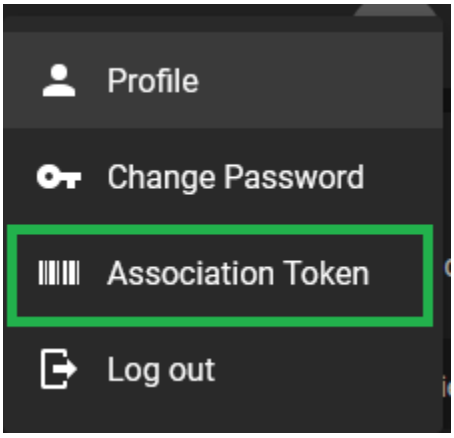
To launch the Acuity Advanced Storage Configuration Utility, navigate to the USP Menu and select Advances Storage Configuration.

Associating USP Cluster with Your Cloud-Based Analytics Account

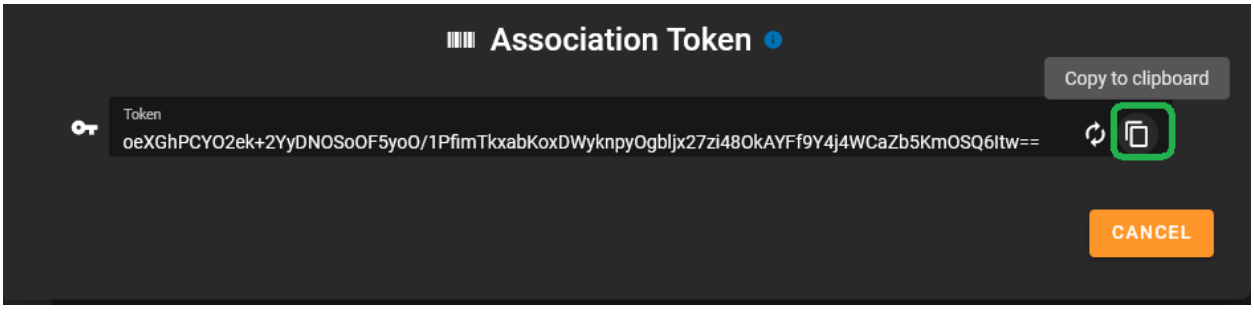
If you would like to automatically associate your USP cluster with your Cloud-Based Analytics account, you must retrieve your association token. This token can be entered into the installation template in the next section.

1. If you do not have an account with the Quantum CBA Portal UI, you can request access by clicking the **Request Site Access** link.
2. To find your Association token, log in to the Quantum CBA Portal UI and click the ***user*** icon, as highlighted in the following image.

1. When you click the ***user*** icon, the following menu displays with the appropriate options. Click **Association Token** for the Association token for your account.



Your unique Association token displays in a pop-up dialog box. Click **Copy to Clipboard** to copy the Association token to your clipboard.



Appendix A – Creating a Bootable USB Key

Creating a Bootable USB Key from a Linux Operating System

1. Use PXE to install any Linux ext4 filesystem on the target OS disk.
2. Copy the ISO file and the md5 checksum file to any location on a Linux server with an ext4 filesystem. Make sure both the md5 checksum and the ISO file are in the same directory.
3. Run the md5sum command to verify the ISO has been properly copied:
   ```
   # md5sum -c USP-5.0.0.iso.md5
   ```
4. Detect the USB from the command:
   ```
   # lsblk -d -o name,size,tran | grep usb
   Example Output: sdt   14.3G usb
   ```

NOTE: For the remaining examples we will use "sdt" as the location returned from the lsblk command.

For the remaining examples, we will use "sdt" as the USB location.

5. Use fdisk or any other tool to remove partitions/re-format from the USB:
   ```
   # fdisk /dev/sdt
   ```
   - Use "p" option to print the existing partitions.
   - Use "d" option to delete a partition and specify the partition numbers, if any.
6. After deleting, use "w" option to save the config.
7. Use the "dd" command to wipe the first few Bytes of the USB:
   ```
   # dd if=/dev/zero of=/dev/sdt bs=1M count=1 status=progress
   ```

NOTE: This is done to guarantee that there is nothing left on the USB. You can increase the bs size to 10M or any other size you require.

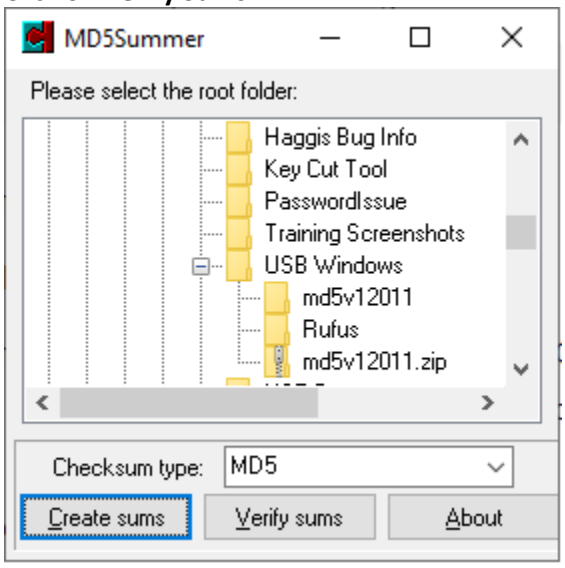
8. Now that the USB drive is formatted, use any of the following commands to copy the ISO to the USB:
   - using dd: (recommended method)
     ```
     # dd bs=4M if=path/to/USP-5.0.0.iso of=/dev/sdt conv=fsync
     oflag=direct status=progress
     ```
   - using cat:
     ```
     # cat path/to/USP-5.0.0.iso > /dev/sdt
     ```
   - using cp:
     ```
     # cp path/to/USP-5.0.0.iso /dev/sdt
     ```
   - using tee:
     ```
     # tee < path/to/USP-5.0.0.iso > /dev/sdt
     ```
9. Use fdisk to verify that the USB has been copied with the right content:
   ```
   # fdisk /dev/sdt
   ```
10. Use the "p" option to print the partitions.
    You will see 2 partitions. Part 1 will be the size of the ISO file. Part 2 will be an EFI partition.

11. Once verified, complete these steps to USB drive as a bootable option:
    a. Attach the USB to the server for installation.
    b. Reboot the server.
    c. Navigate to the One-Time-Boot Option of the server to see the USB drive as a bootable option.
    It will usually be named with the USB drive's manufacturer. For example: SanDisk, Samsung, etc.

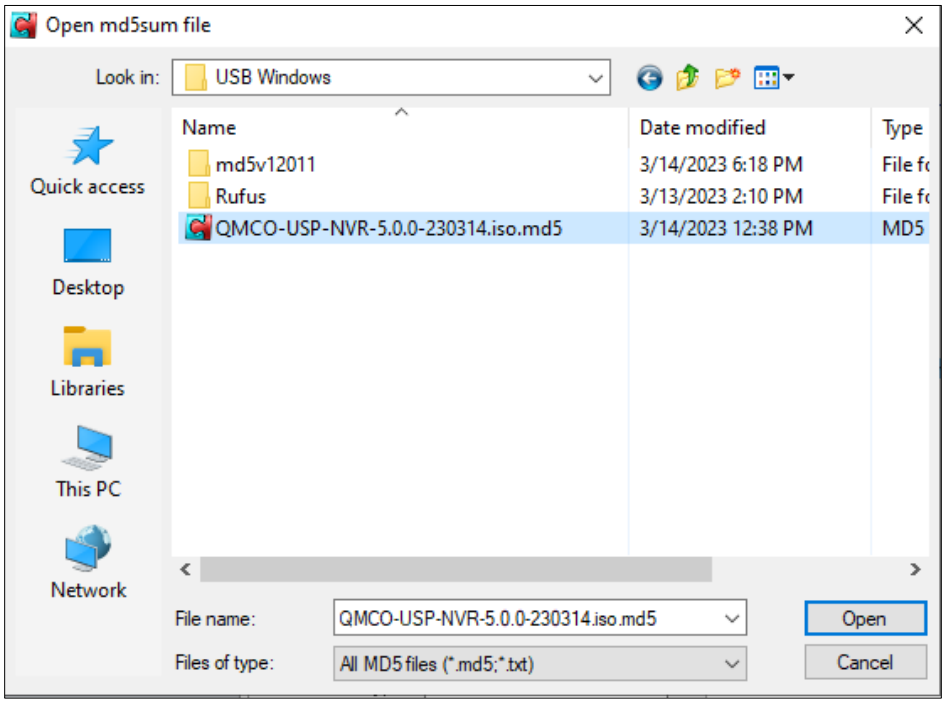
The rest of the process is similar to other OS installations.

Creating a Bootable USB Key from a Windows Operating System

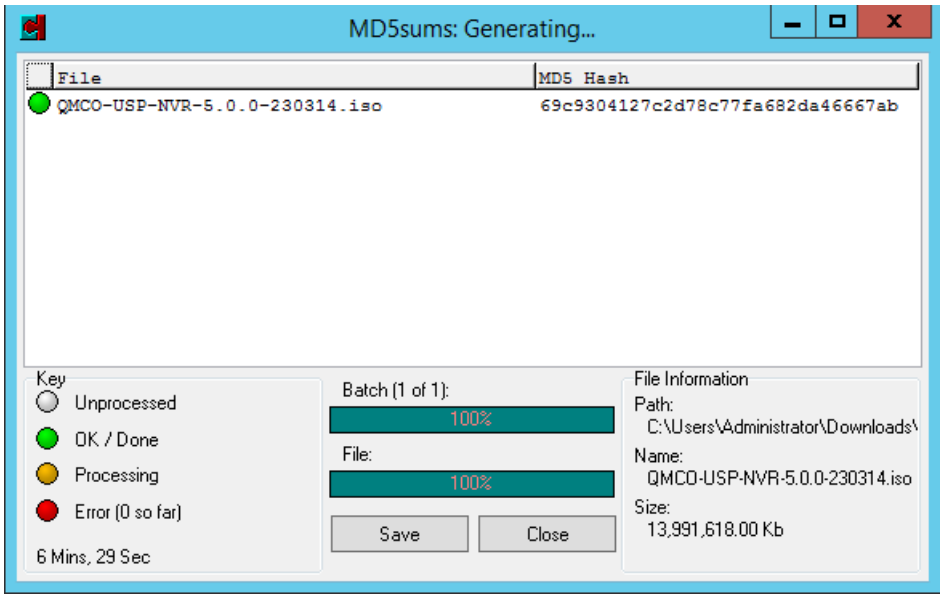
1. Copy the ISO file and the md5 checksum file to the server at any location. Make sure both the md5 checksum and the ISO file are in the same directory.
2. Use a program to verify that the ISO's md5 checksum has been properly copied.
    - Using md5summer:
        a. Click on **Verify Sums.**



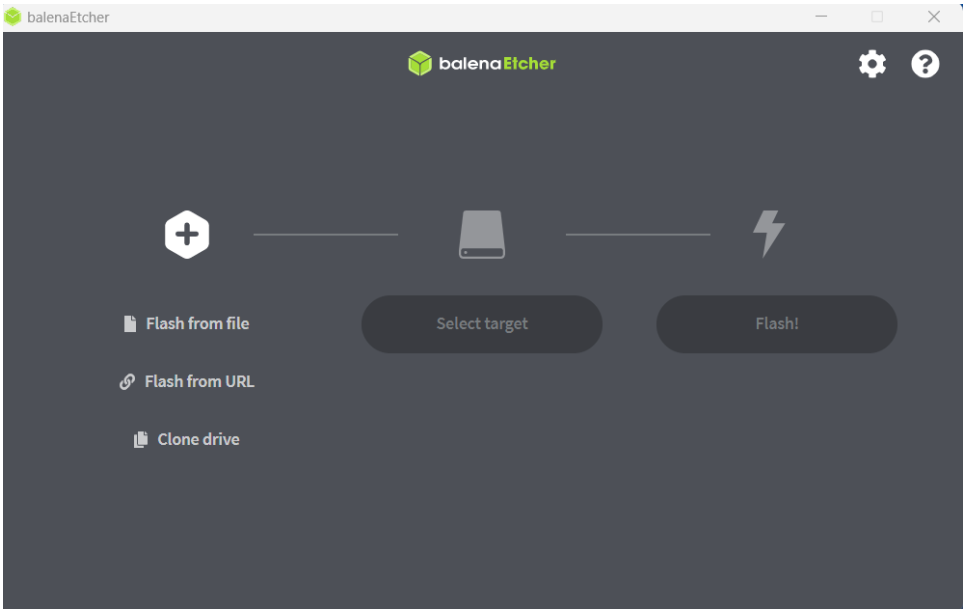
b. From the **Open** dialog, select the .md5 file.



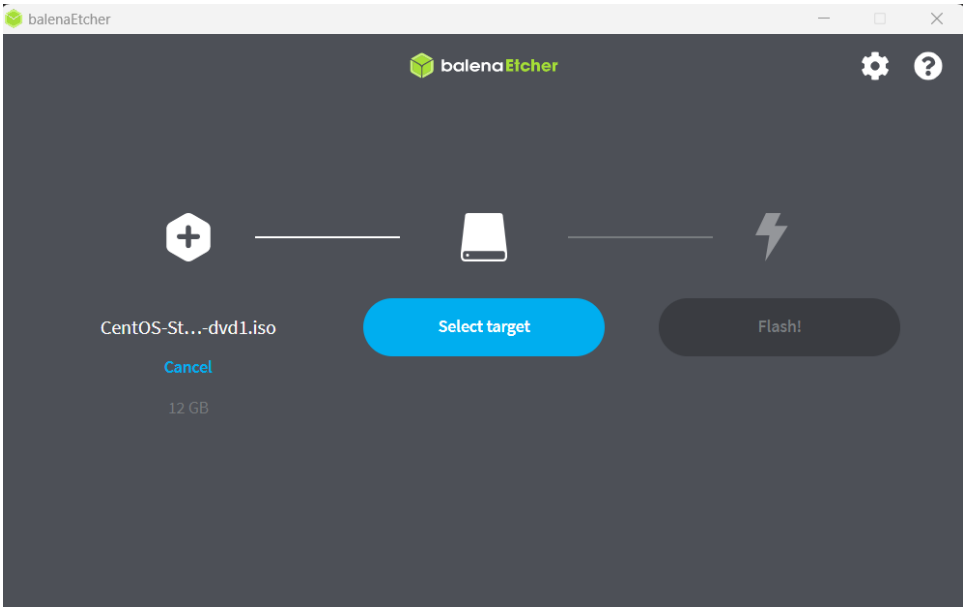
Opening the file may take a few minutes to complete.



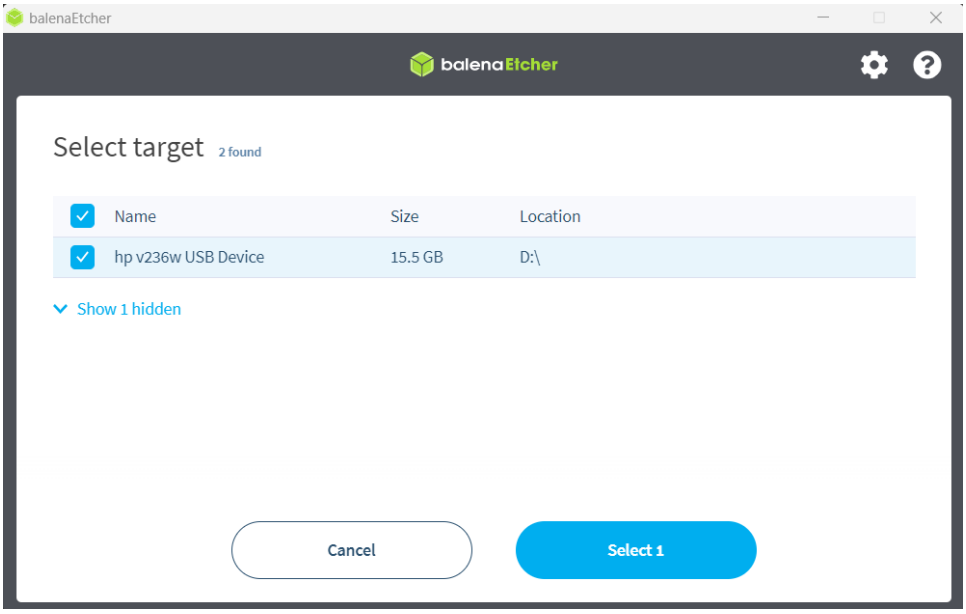
c. Plug in the USB drive to use for creating the installation file.
d. Using balenaEtcher select the ISO file from your local system.

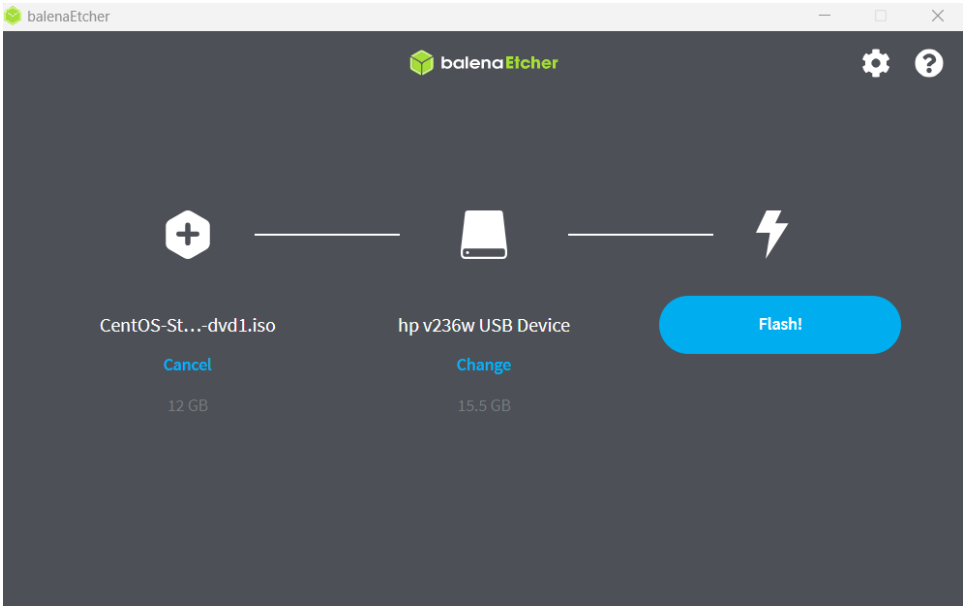


e. Select the Target device (USB drive).

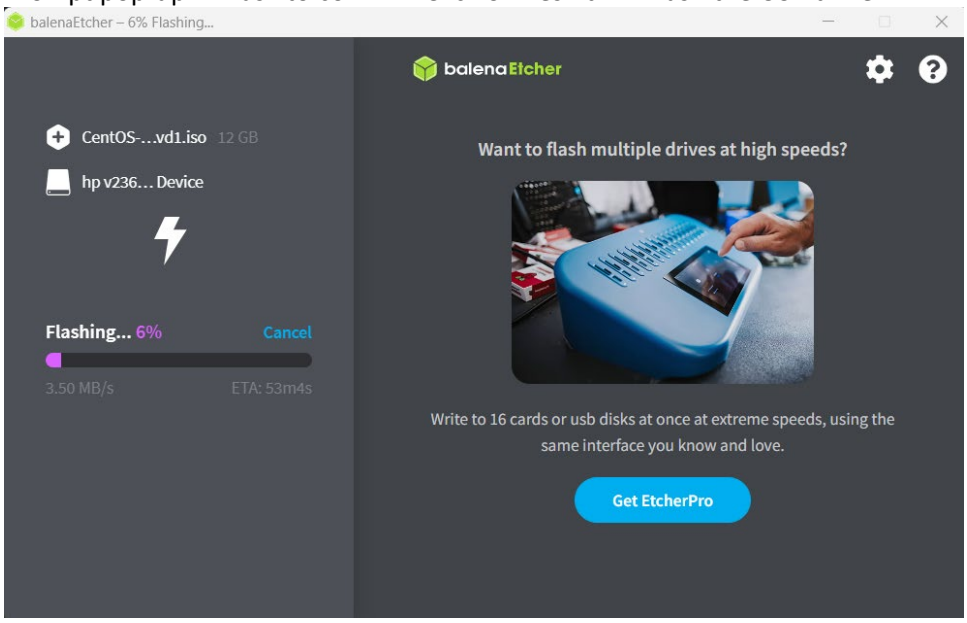


f. Note that current data on the device will be destroyed. It will start writing the ISO to USB key, which will take a few minutes.


balenaEtcher
balenaEtcher
Select target
2 found
Name
Size
Location
hp v236w USB Device
15.5 GB
D:\
Show 1 hidden
Cancel
Select 1


balenaEtcher
balenaEtcher
CentOS-St…-dvd1.iso
Cancel
12 GB
hp v236w USB Device
Change
15.5 GB
Flash!

g. Once the "Flash!" button displays, click on it to start the USB drive flashing. A Command Prompt pop-up will ask to confirm. Click on Yes. It will flash the USB drive.



h. Confirming that the flash has completed, exit the program, safely eject the USB key, and then insert it in the server to install USP 5.0.

i. Boot the server and go to the One-Time-Boot Option of the server to select the USB drive as a bootable option. The drive will usually be named with the manufacturer of the USB drive. For example: SanDisk, Samsung, etc.

Appendix B - Booting from an ISO Through Out-Of-Band Management

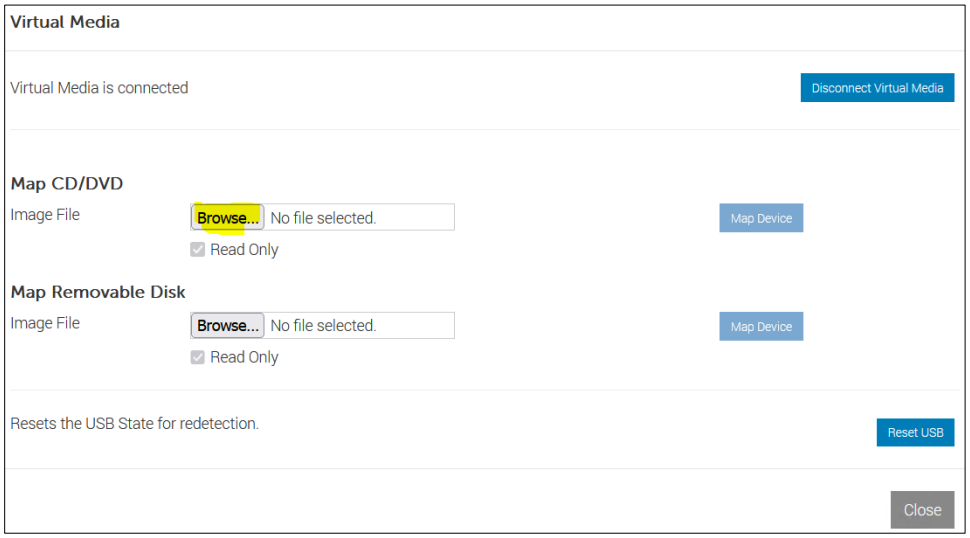
NOTE: The example below is for a Dell server. Your server out-of-band management interface may differ from the example below. See the vendor specific instructions for booting from virtual media.

1. Place the Quantum .ISO file on a network share that is accessible to all of your nodes.
2. Connect to the out-of-band interface and log in.

3. Click on the Virtual Console.

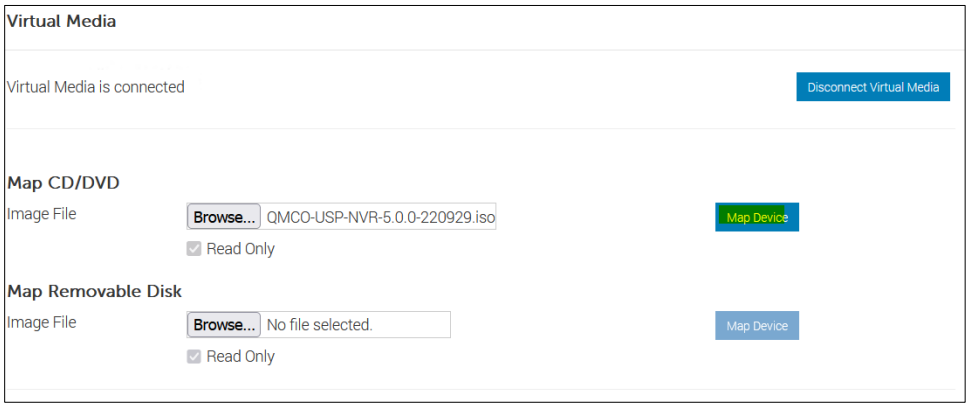
4. Select the “Connect “Virtual Media” button.

5. In the “Map CD/DVD” section, select **Browse.**

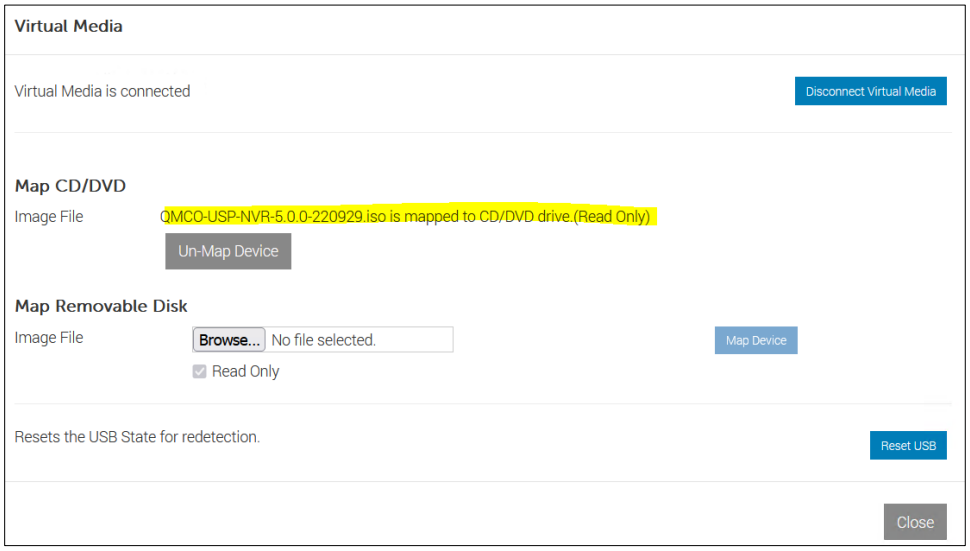


6. Browse to the Quantum ISO file and press Open.

7. Select “Map Device”



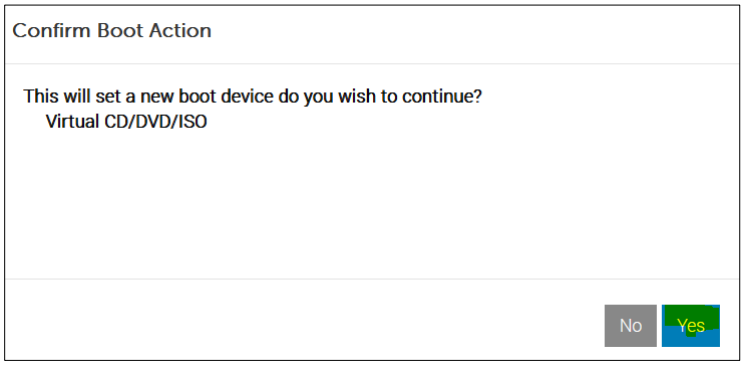
8. The ISO will appear as mapped. Press “Close”



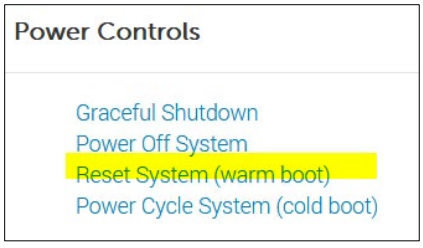
9. Configure the server to boot from the virtual ISO by pressing the “Boot” button and selecting “Virtual CD/DVD/ISO.”

10. Select **Virtual CD/DVD/ISO.**

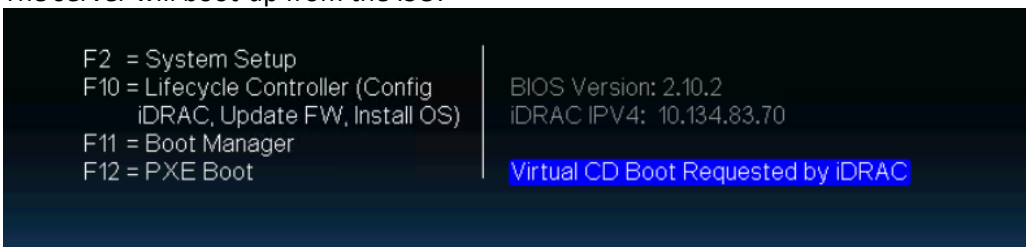
11. Click on **Yes.**



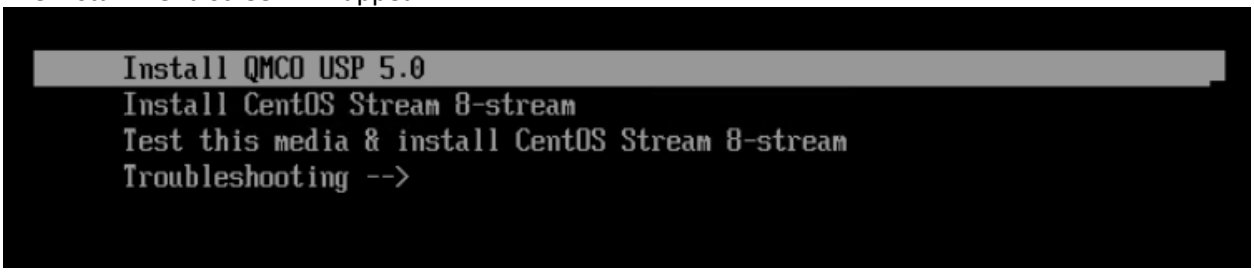
12. Select **Power.**
13. Select **Reset System (Warm boot).**



14. Confirm Power action, select “Yes.”
15. On the next boot, your server will boot from the Quantum USP ISO.
    The server will boot-up from the ISO.



The Install Menu screen will appear.



16. Select Install QMCO USP 5.0 and click on **Enter.**
    The next screen will allow you to select disks for the OS partition.

Appendix C – Ports Used

The following ports are used by the USP software.

Service	Port	Protocol	Description
haproxy_stats	1984	TCP	haproxy statistics port
galera_dbclient_haproxy	3305	TCP	Galera Cluster database client connections
galera_dbclient	3306	TCP	Galera Cluster database client connections
galera_replication	4567	TCP	Galera Cluster database replication traffic
galera_inc_state_transfer	4568	TCP	Galera Cluster database Incremental State Transfers
galera_state_snapshot_transfer	4444	TCP	Galera Cluster other database State Snapshot Transfer methods
nova_metadata	8785	TCP	nova metadata service bind port
nova_osapi_compute	8784	TCP	nova compute osapi service bind port
nova_novncproxy	8881	TCP	nova novncproxy service bind port
nova_metadata_haproxy	8775	TCP	nova metadata service loadbalancer virtual port
nova_osapi_compute_haproxy	8774	TCP	nova compute osapi service loadbalancer virtual port
nova_novncproxy_haproxy	8880	TCP	nova novncproxy service loadbalancer virtual port
placement	8778	TCP	placement api service bind port
placement_haproxy	8788	TCP	placement api service loadbalancer virtual port
squid	8883	TCP	squid proxy bind port
squid_icp	8884	TCP	squid proxy ICP (cache synchronization) bind port

Service	Port	Protocol	Description
squid_haproxy	8882	TCP	loadbalancer virtual port
heat_api	8005	TCP	heat api service bind port
heat_api_haproxy	8004	TCP	heat api service loadbalancer virtual port
heat_api_cfn	8001	TCP	heat cloudformation api service bind port
heat_api_cfn_haproxy	8000	TCP	heat cloudformation api service loadbalancer virtual port
glance_api	9293	TCP	glance api serivice bind port
glance_api_haproxy	9292	TCP	glance api serivice loadbalancer virtual port
barbican_api	9312	TCP	barbican api service bind port
barbican_api_haproxy	9311	TCP	barbican api service loadbalancer virtual port
iscsi	3260	TCP	iscsi initiator port
cinder_api	8777	TCP	cinder api service bind port
cinder_api_haproxy	8776	TCP	cinder api service loadbalancer virtual port
keystone_public	5001	TCP	keystone public api service bind port
keystone_public_haproxy	5000	TCP	keystone public api service loadbalancer virtual port
keystone_admin	35358	TCP	keystone admin api service bind port
keystone_admin_haproxy	35357	TCP	keystone admin api service loadbalancer virtual port
neutron_api	9596	TCP	neutron api service bind port
neutron_api_haproxy	9696	TCP	neutron api service loadbalancer virtual port
vxlan	4789,8472	UDP	IANA and Linux VXLAN connection ports
neutron_dhcp_in	67	UDP	Neutron dhcp input
neutron_dhcp_out	68	UDP	Neutron dhcp output
libvirtd	16514	TCP	libvirtd tls remote connection port
kvm	49152-49261	TCP	kvm livemigration ephemeral connection ports
vncspice	5900-6700	TCP	virtual machine VNC and SPICE connectin ports
memcached	11211	TCP	memcached connection port
rabbitmq	5672	TCP	rabbitmq connection port
epmd	4369	TCP	erlang epmd connection port

Service	Port	Protocol	Description
rabbitmq_dist	44001-44010	TCP	rabbitmq distrubution connection ports
rabbitmq_haproxy	5671	TCP	rabbitmq service loadbalancer virtual port
ntp	123	UDP	ntp connection port
http	80	TCP	apache http unsecure bind port
https_haproxy	443	TCP	apache httpd SSL haproxy loadbalancer virtual port
pcsd	2224,3121, 21064	TCP	pcsd and pacemaker ports
corosync	5404,5405	UDP	corosync ports
ceph_mon	3300,6789	TCP	ceph monitor ports
ceph	6800-7300	TCP	ceph OSD and MSD ports
ceph_rgw	7480	TCP	Ceph RADOS Gateway port
ceph_dashboard	8443	TCP	ceph dashboard port
ceph_container_registry	5009	TCP	ceph container local registry port
acuity_mgmt_api	8080	TCP	port for acuity management api
acuity_mgmt_ui	8443	TCP	port for acuity management UI
acuity_mgmt_ui_websocket	8887	TCP	port for acuity management websocket
acuity_mgmt_ui_haproxy	8442	TCP	mngmnt SSL haproxy loadbalancer virtual port
cba	5050	TCP	server port for cba

Quantum

Quantum technology, software, and services provide the solutions that today's organizations need to make video and other unstructured data smarter – so their data works for them and not the other way around. With over 40 years of innovation, Quantum's end-to-end platform is uniquely equipped to orchestrate, protect, and enrich data across its lifecycle, providing enhanced intelligence and actionable insights. Leading organizations in cloud services, entertainment, government, research, education, transportation, and enterprise IT trust Quantum to bring their data to life, because data makes life better, safer, and smarter. Quantum is listed on Nasdaq (QMCO) and the Russell 2000® Index. For more information visit www.quantum.com.

www.quantum.com | 800-677-6268