Qumulo Getting Started Guide

Version 2.3

2020

Overview

Welcome to our Getting Started Guide! Here you'll find all the details you need to install your new nodes, configure your cluster, and hit the ground running as a new customer. While this guide serves as a great starting point, there's so much more you can do with Qumulo!

For a deeper dive into our features and administering your cluster, be sure to visit our Qumulo Care support portal where you can open a case, read articles and watch videos in our online content library, check out our product release notes, and get involved in the Qumulo community to make your voice heard.

If you do have any additional questions or want to provide some feedback, we would love to hear from you! Feel free to open a case, shoot an email over to care@qumulo.com, or ping us in your private Slack channel so that we can get you the answers you need.

Table of Contents

1. Qumulo Safety Instructions

Before racking and stacking your Qumulo-supported platform, check out the Qumulo Safety Instructions below.

Elevated Operating Ambient
If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, be sure to install the equipment in an environment where the maximum ambient temperature (Tma) does not exceed 40 degrees C.

Reduced Air Flow
Installation of the equipment in a rack or cabinet should be such that the amount of airflow required for safe operation of the equipment is not compromised.

Mechanical Loading
Mounting of the equipment in the rack or cabinet should be such that a hazardous condition is not achieved due to uneven mechanical loading.

Circuit Overloading
Consideration should be given to the connection between the equipment and the supply circuit. Appropriate consideration of equipment nameplate ratings should be used when addressing the effect that overloading the circuits might have on current protection and supply wiring.

Reliable Earthing
Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips).

Redundant Power Supplies
Where redundant power supplies are provided with the equipment, each power supply shall be connected to a separate circuit to optimize the equipment redundancy.

Servicing
Disconnect all power supplies prior to servicing the equipment.

Caution: Risk of explosion if battery is replaced by incorrect type. Dispose of used batteries according to the instructions provided.

2. Technical Specifications

2.1 QC Series 1U, 4U, and C-Series

Technical Specifications

Per Node	1U				4U			
	QC24	QC40	C-72T	C-168T	QC104	QC208	QC260	QC360
Connectivity Ports	2 x 10GbE (SFP+)		2 x 25GbE (SFP28)		4 x 40GbE (QSFP+)			
Management Ports	1GbE Base-T (RJ45)				1GbE Base-T (RJ45)			
Storage Media (all hot-swappable)	4 x 6TB HDD	4 x 10TB HDD	12 x 6TB HDD	12 x 14TB HDD	26 x 4TB HDD	26 x 8TB HDD	26 x 10TB HDD	36 x 10TB HDD
	2 x 800GB SSD		4 x 480GB SSD	4 x 960GB SSD	13 x 480GB SSD			4 x 1.6TB SSD
CPU	Intel® Xeon E3-1230 v6, 4 cores, 3.60GHz		Intel® Xeon-D D-1531 SOC, 6 cores, 2.2GHz		Intel® Xeon E5 2620v3, 6 cores, 2.40GHz			
Memory	64GB				128GB			256GB
Raw Storage Capacity	24TB	40TB	72TB	168TB	104TB	208TB	260TB	360TB
Power Supply	2 x 650W (fully redundant, hot-swappable)		2 x 400W Platinum PSU (fully redundant, hot swappable)		2 x 750W (fully redundant, hot-swappable)			
Dimensions (H x W x D)	1.75" (4.5cm) x 17.2" (43.7cm) x 27.9" (70.8cm)		1.7" (4.3 cm) x 17.2" (43.7cm) x 36.25" (92.1cm)		7" (17.8cm) x 17.2" (43.7cm) x 29" (73.7cm)			
Weight	55lbs (24.9kg)		63 lbs (28.6kg)		155lbs (70.3kg)			166lbs (75.3kg)
Power Requirements	100 – 240V, 50/60hz				100 – 240V, 50/60hz			
Typical Power Consumption	0.65A @ 240V, 1.41A @ 110V		0.59A @ 240V, 1.29A @ 110V		2.71A @ 240V, 5.91A @ 110V			
Typical Thermal Rating	155W (VA), 529 BTU/hr		142W (VA), 484 BTU/hr		650W (VA), 2,218 BTU/hr			
Maximum Power Consumption	1.04A @ 240V, 2.28A @ 110V		1.0A @ 240V, 2.18A @ 110V		3.55A @ 240V, 7.73A @ 110V			
Maximum Thermal Rating	250W (VA), 855 BTU/hr		240W (VA), 818 BTU/hr		850W (VA), 2,900 BTU/hr			
Operating Temperature	50° F – 95° F (10° C – 35° C)		41° F – 95° F (5° C – 35° C)		50° F - 95° F (10° C – 35° C)			
Non-operating Temperature	-40° F – 158° F (-40° C – 70° C)		-40° F – 149° F (-40° C – 65° C)		-40° F - 158° F (-40° C – 70° C)			
Operating Relative Humidity	8% to 90% (non-condensing)				8% to 90% (non-condensing)			
Non-operating Relative Humidity	5% to 95% (non-condensing)				5% to 95% (non-condensing)			

2.2 Qumulo P-Series 2U

Technical Specifications

Per Node	P-23T	P-92T	P-184T	P-368T
Raw Storage Capacity	23TB	92TB	184TB	368TB
NVMe Drives (hot swappable)	12 x 1.92TB NVMe	24 x 3.84TB NVMe	24 X 7.68TB NVMe	24 X 15.36TB NVMe
Connectivity Ports	4 x 100GbE (QSFP+)			
Management Ports	1GbE Base-T (RJ45)			
CPU	2 x Intel Gold 6126, 12 cores, 2.6Ghz			
Memory	192GB			
Power Supply	2 x 1100W (fully redundant, hot-swappable)			
Dimensions (HxWxD)	3.5" (8.9cm) x 17.2" (43.7cm) x 29" (73.7cm)			
Power Requirements	100 – 240V, 50/60hz			
Typical Power Consumption	450W			
Typical Thermal Rating	650W (VA), 2,218 BTU/hr			
Maximum Power Consumption	3.55A @ 240V, 7.73A @ 110V			
Maximum Thermal Rating	2,218W (VA), 2,900 BTU/hr			
Operating Temperature	50° F – 95° F (10° C – 35° C)			
Non-operating Temperature	-40° F – 158° F (-40° C – 70° C)			
Operating Relative Humidity	8% to 90% (non-condensing)			
Non-operating Relative Humidity	5% to 95% (non-condensing)			

2.3 Qumulo K-Series 1U

Technical Specifications

Per Node	K-144T	K-168T
Connectivity Ports	2 x dual 10GbE (SFP+)	
Management Ports	10GbE base-T (RJ45)	
Storage Media (all hot-swappable)	12 x 12TB HDD, 3 x 800GB SSD	12 x 14TB HDD, 3 x 960GB SSD
CPU	Intel® Xeon-D D-1531 SOC, 6 cores, 2.2GHz	
Memory	64GB	
Raw Storage Capacity	144TB	168TB
Power Supply	2 x 400W (fully redundant, hot-swappable)	
Dimensions (HxWxD)	1.7" (4.3cm) x 17.2" (43.7cm) x 36.25" (92.1cm)	
Weight	63lbs (28.6kg)	
Power Requirements	100 – 240V, 50/60hz	
Typical Power Consumption	0.59A @ 240V, 1.29A @ 110V	
Typical Thermal Rating	142W (VA), 484 BTU/h	
Maximum Power Consumption	1.0A @ 240V, 2.18A @ 110V	
Maximum Thermal Rating	240W (VA), 818 BTU/hr	
Operating Temperature	41°F to 95°F (5°C to 35°C)	
Non-operating Temperature	-40°F to 149°F (-40°C to 65°C)	
Operating Relative Humidity	8% to 90% (non-condensing)	
Non-operating Relative Humidity	5% to 95% (non-condensing)	

2.4 Qumulo for HPE

	HPE Apollo 36TB Hybrid SSD/Disk	HPE Apollo 90TB Hybrid SSD/Disk	HPE Apollo 192TB Hybrid SSD/Disk	HPE Apollo 336TB Active Archive
Raw Capacity	36TB	90TB	192TB	336TB
HDDs	9 x 4TB	9 x 10TB	24 x 8TB	24 x 14TB
Logical Flash Cache Capacity	1.44TB	2.88TB	5.76TB	7.68TB
Connectivity Ports	2 x 25GbE or 2 x 100GbE		2 x 100GbE (Min link speed is 25GbE)	2 x 25GbE
Management Ports	2 x IPMI 1GbE baseT (RJ45)			
CPU	1 x Intel Xeon-Silver 4210 2.2GHz 10-cores		2 x Intel Xeon-Silver 4210 2.2GHz 10-cores	1 x Intel Xeon-Silver 4210 2.2GHz 10-cores
Memory	64GB		128GB	128GB
Physical Dimensions (H x W x D)	3.44" (8.75cm) x 17.63" (44.8cm) x 32" (81.28cm)			

Additional technical specifications for these platforms are provided by HPE. Check out the links below for details.

- HPE Apollo 4200 Gen9 Server Specifications
- HPE Apollo 4200 Gen10 Server Document List

---

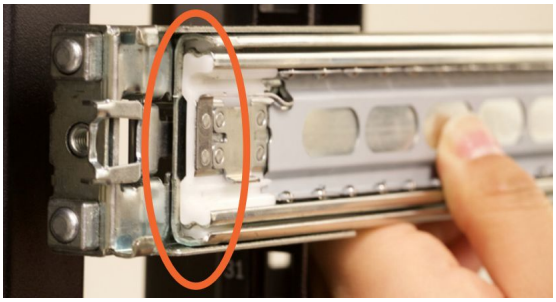
3. Rack & Roll

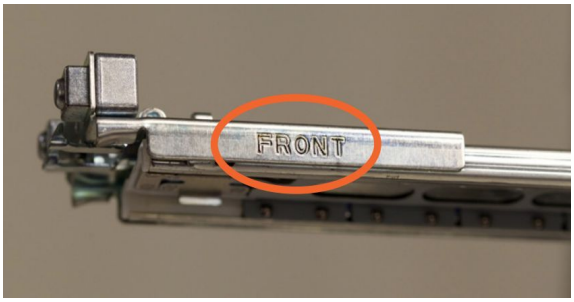
Now that you've reviewed Qumulo's safety instructions, it's time to rack and roll! Below you'll learn how to install and prepare your nodes before you create a cluster. Check out the appropriate section for your platform and then continue on to the Create a Cluster portion to start configuring your cluster.

- QC Series 1U
- QC Series 4U
- Qumulo C-Series 1U
- Qumulo P-Series 2U
- Qumulo K-Series 1U
- HPE Apollo 4200 Gen9
- HPE Apollo 4200 Gen10

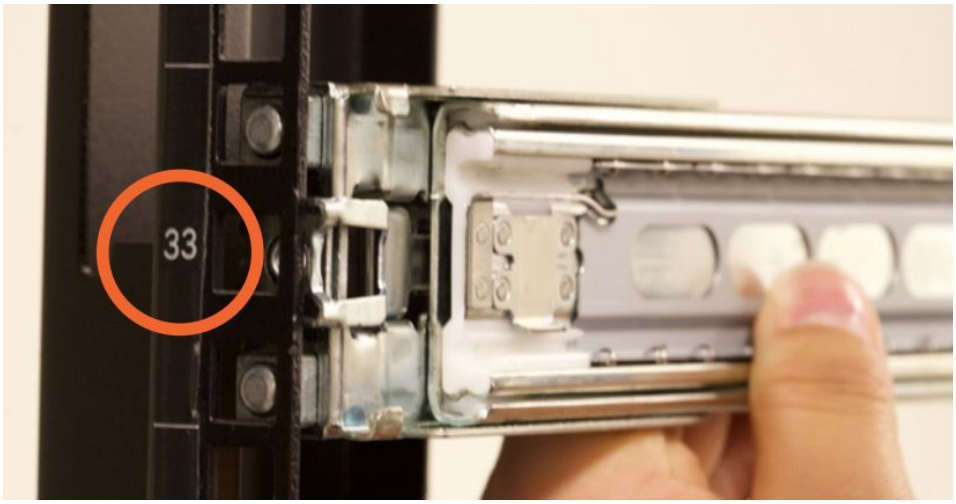
3.1 QC Series 1U

1. Slide the inner rail in place and verify the front end of the rail.

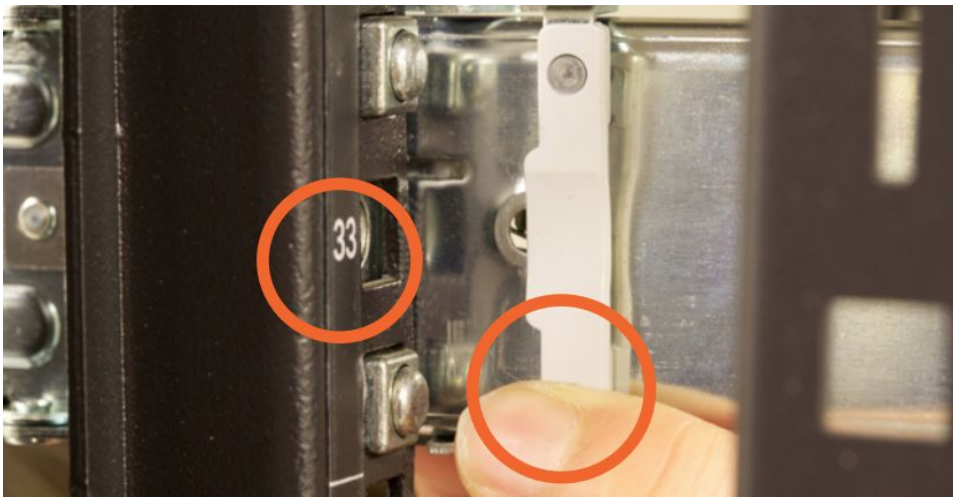




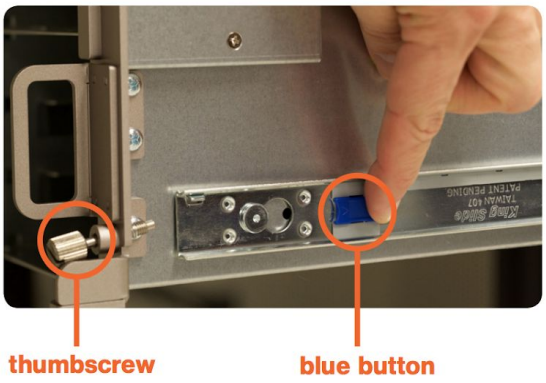
2. Place the front of the rail into the holes on the rack using the numbers as a guide.



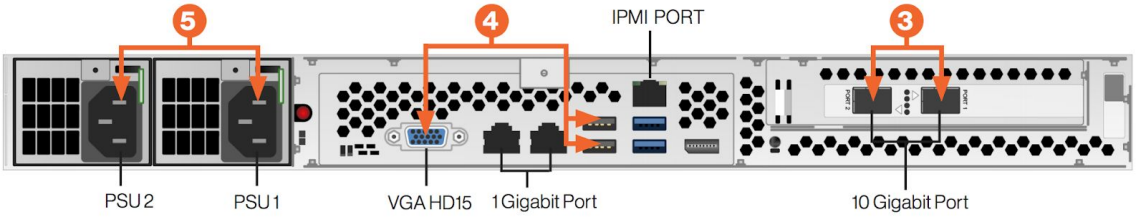
3. Hold the lock and place the rear of the rail into the holes using the same numerical placement as the front.
4. Release to lock the rail in place.



5. Place node into the rail system by aligning the rails between the node and the rack.
6. Release the blue button on the side of the node to slide the node and rails into the rack.
7. Tighten the thumbscrew to secure the node in place.



8. Attach the network cables (3) and plug in the power cables on the back of the node (5).



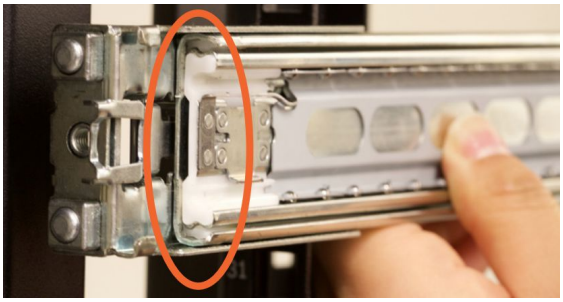
9. Connect any one of the nodes to a display, keyboard and mouse (4).

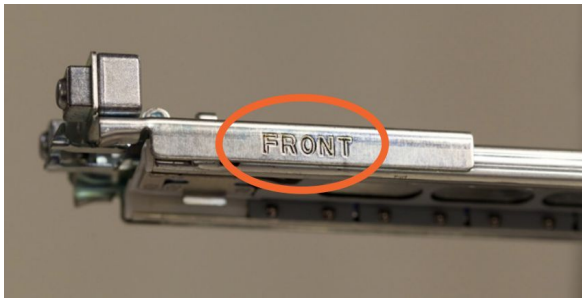
10. Turn on the nodes by pressing the power button on the front.

11. Check that all drive lights (red, blue, green) illuminate before proceeding to create a cluster.

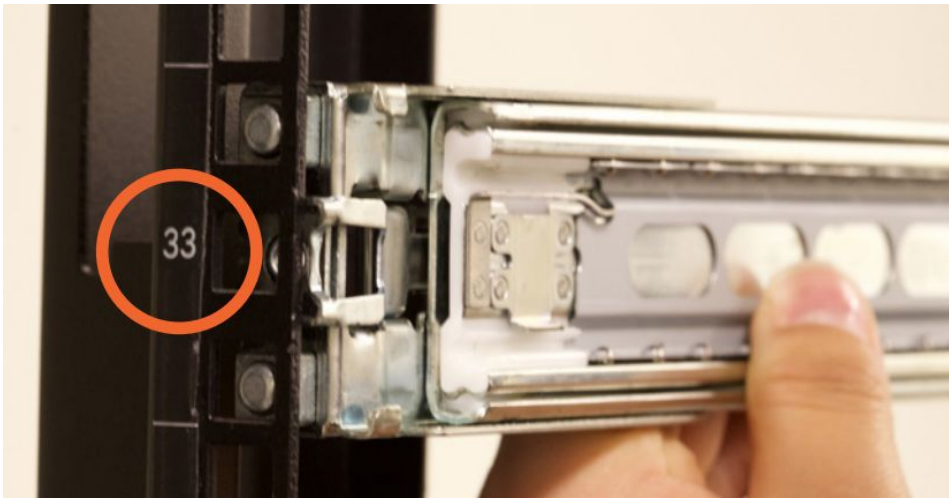
3.2 QC Series 4U

1. Slide the inner rail in place and verify the front end of the rail.

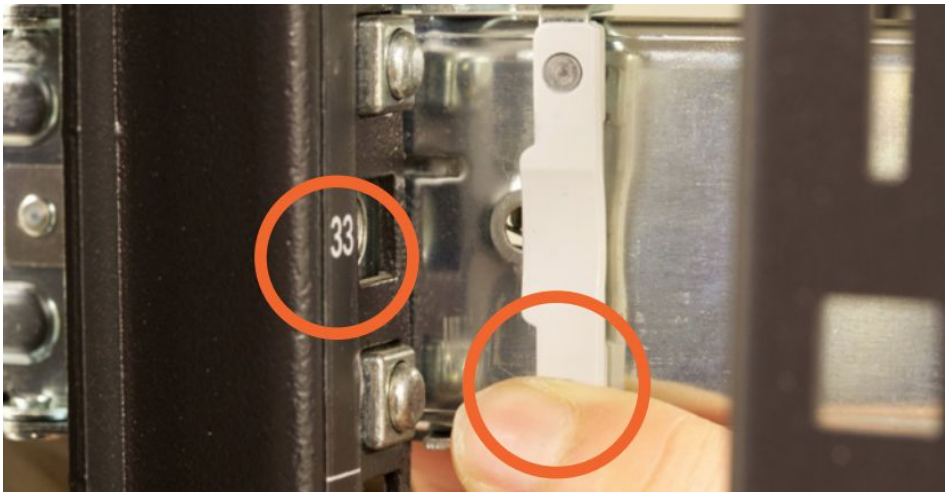




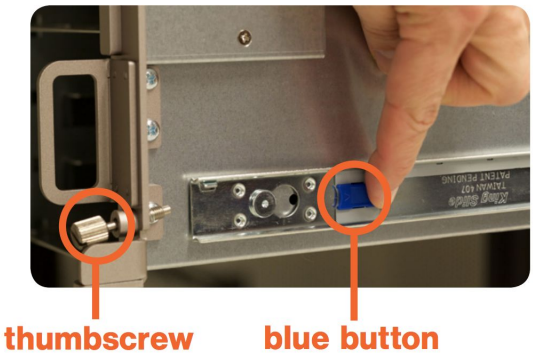
2. Place the front of the rail into the holes on the rack using the numbers as a guide.



3. Hold the lock and place the rear of the rail into the holes using the same numerical placement as the front.
4. Release to lock the rail in place.

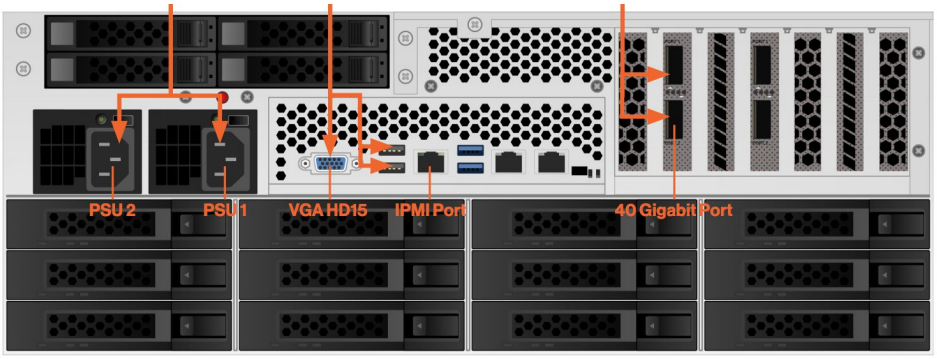


5. Place node into the rail system by aligning the rails between the node and the rack.
6. Release the blue button on the side of the node to slide the node and rails into the rack.
7. Tighten the thumbscrew to secure the node in place.



8. Insert the included hard drives (HDD) into any open slot on the node.

9. Attach the network cables and plug in the power cables on the back of the node.

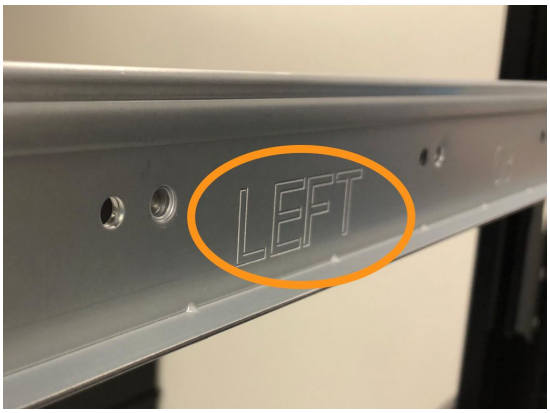


10. Connect any one of the nodes to a display, keyboard and mouse.
11. Turn on the nodes by pressing the power button on the front.

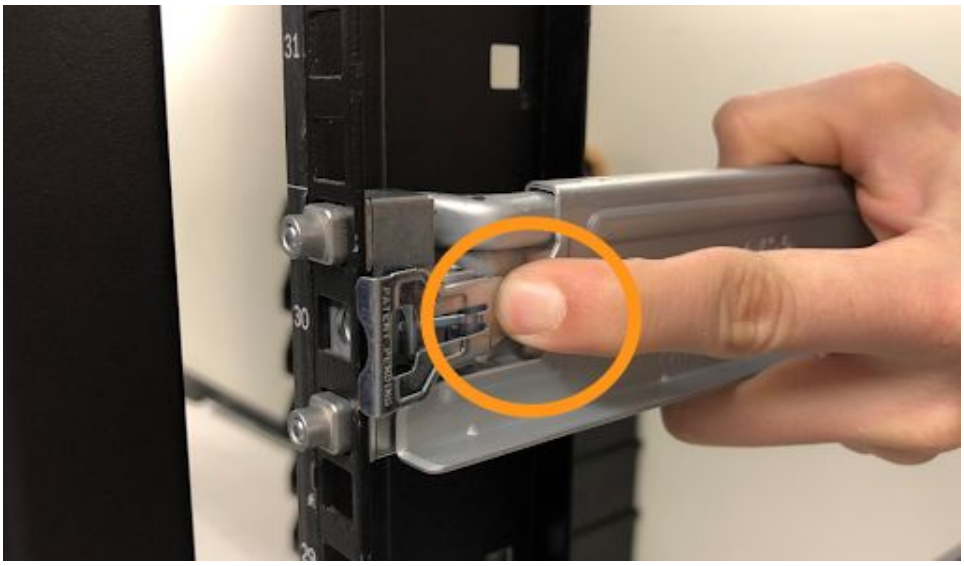
12. Check that all drive lights (red, blue, green) illuminate before proceeding to create a cluster.

3.3 Qumulo C-Series 1U

1. Verify the installation side of the rack and front end of the sled using the hardware labels.



2. Press the release lever on the front end while aligning the sled into the holes on the rack.



3. Release the lever to secure the sled.

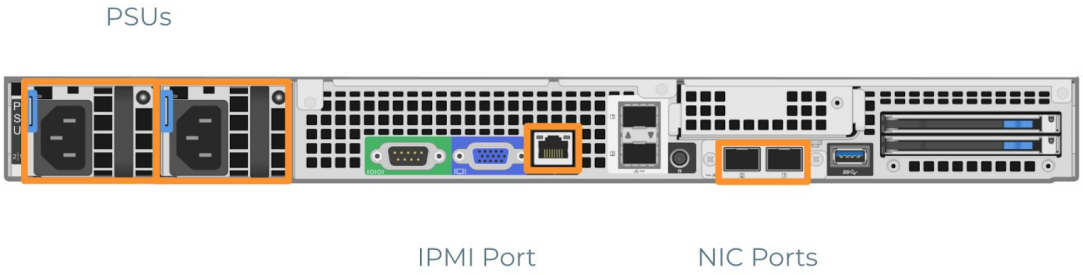
4. Repeat the steps above to install the rear of the sled using the same numerical placement as the front.

CAUTION! Sleds do not fully extend like other rail systems and are stationary in the racks. Use caution when installing or removing nodes.

5. Place the back of the node on the sleds and slide the node into the rack.

6. Tighten the two front thumbscrews to secure the node in place.
7. Press the drawer latch up on the front of the node and pull out the drawer using the handle.

8. Verify that all HDDs in the driver drawer are fully seated.
9. Push the drive drawer back into place until the drawer latch clicks.
10. Attach the network cables and plug in the power cables on the back of the node.



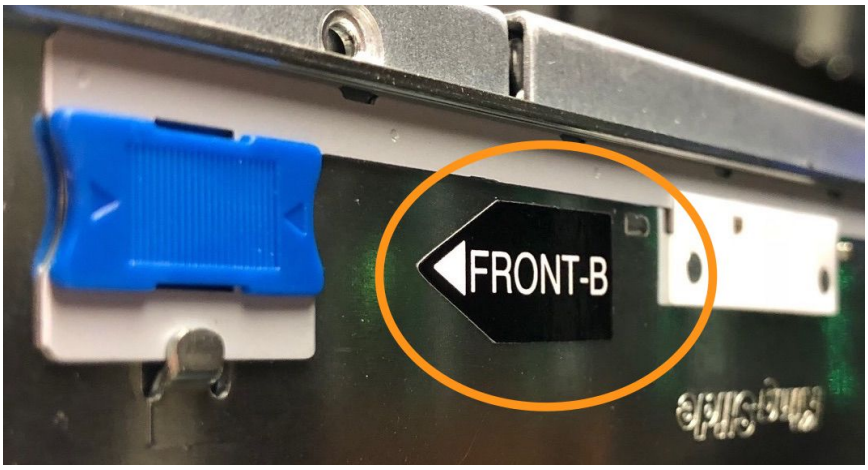
CAUTION: Do not use the LOM ports. Only use the external NIC ports for the 25Gb connections as highlighted above.

11. Connect any one of the nodes to a display, keyboard and mouse.

12. Turn on the nodes by pressing the power button on the front.

3.4 Qumulo P-Series 2U

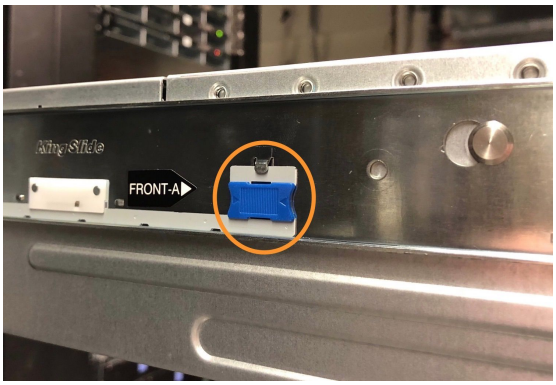
1. Slide the inner rail in place and verify the front end of the rail before installing on the rack.



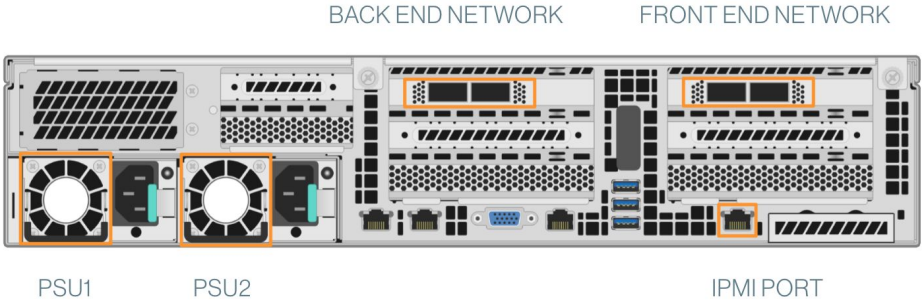
2. Place the front of the rail into the holes on the rack using the numbers as a guide.

3. Hold the lock and place the rear of the rail into the holes using the same numerical placement as the front; release to lock the rail in place.

4. Place node into the rail system by aligning the rails between the node and the rack.
5. Release the blue button on the side of the node to slide the node and rails into the rack.



6. Tighten the thumbscrews to secure the node in place.
7. Attach the network cables and plug in the power cables on the back of the node.



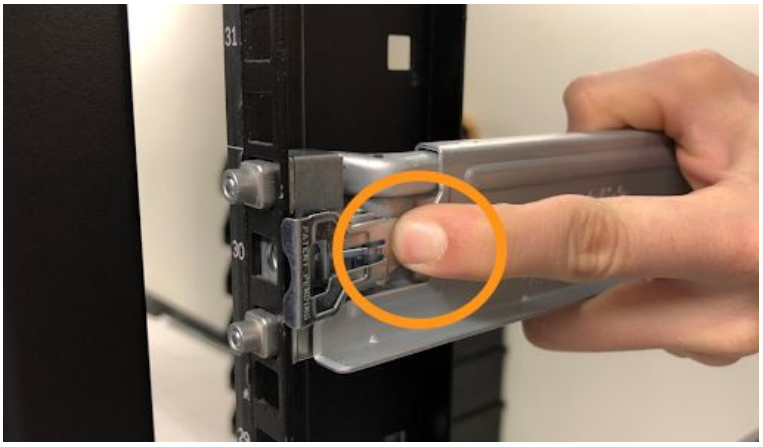
8. Connect any one of the nodes to a display, keyboard and mouse.
9. Turn on the nodes by pressing the power button on the front.

10. Check that all drive lights illuminate confirming that drives and nodes are ready for configuration.

3.5 Qumulo K-Series 1U

1. Verify the installation side of the rack and front end of the sled using the hardware labels.

2. Press the release lever on the front end while aligning the sled into the holes on the rack.



3. Release the lever to secure the sled.

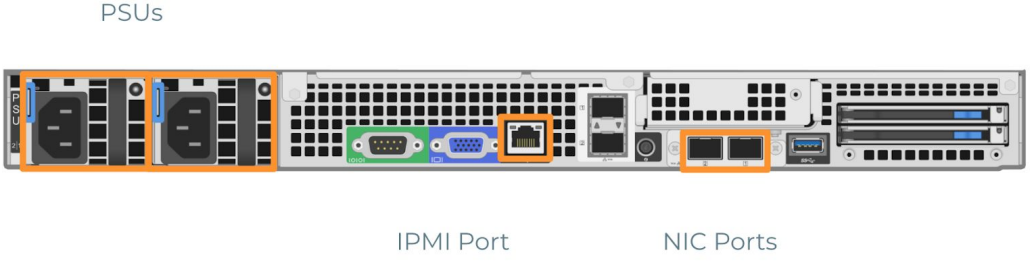
4. Repeat the steps above to install the rear of the sled using the same numerical placement as the front.

CAUTION! Sleds do not fully extend like other rail systems and are stationary in the racks. Use caution when installing or removing nodes.

11. Place the back of the node on the sleds and slide the node into the rack.

12. Tighten the two front thumbscrews to secure the node in place.
13. Press the drawer latch up on the front of the node and pull out the drawer using the handle.

14. Verify that all HDDs in the driver drawer are fully seated.
15. Push the drive drawer back into place until the drawer latch clicks.
16. Attach the network cables and plug in the power cables on the back of the node.



CAUTION: Do not use the LOM ports. Only use the external NIC ports for the 10Gb connections as highlighted above.

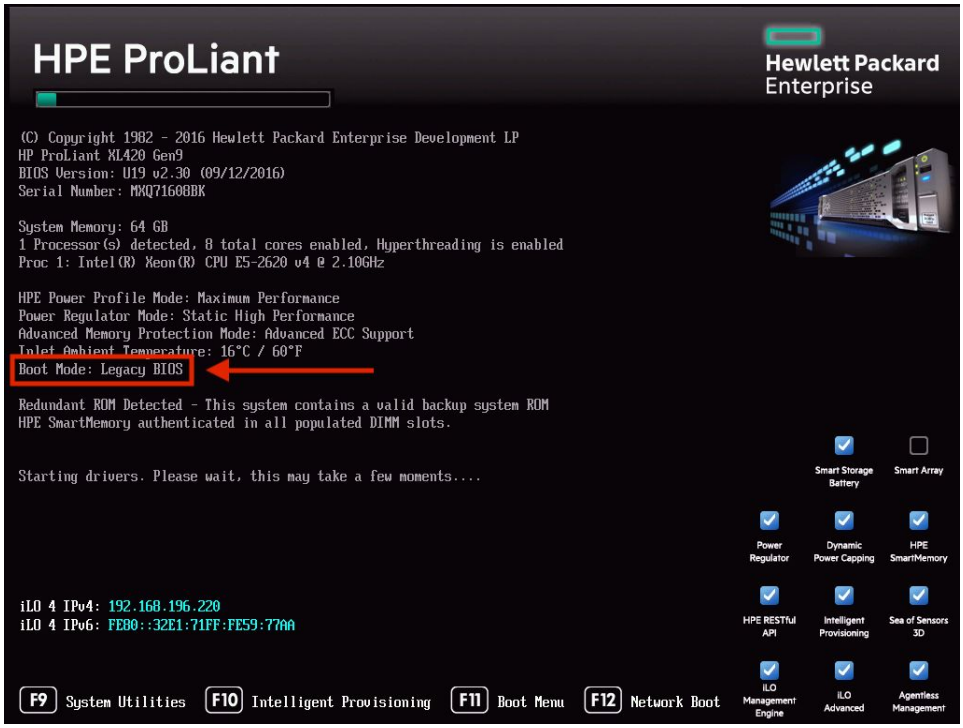
13. Connect any one of the nodes to a display, keyboard and mouse.
14. Turn on the nodes by pressing the power button on the front.

3.6 HPE Apollo 4200 Gen9

Once your Qumulo-supported hardware is installed, you will need to image the nodes using the instructions below.

1. Shut down the node and connect it to a display, keyboard, and mouse.
2. Plug in the **Qumulo Core Installer USB key** to an available USB port.
3. Press the **power button** highlighted below to power the node on and wait for the machine's boot screen to display.

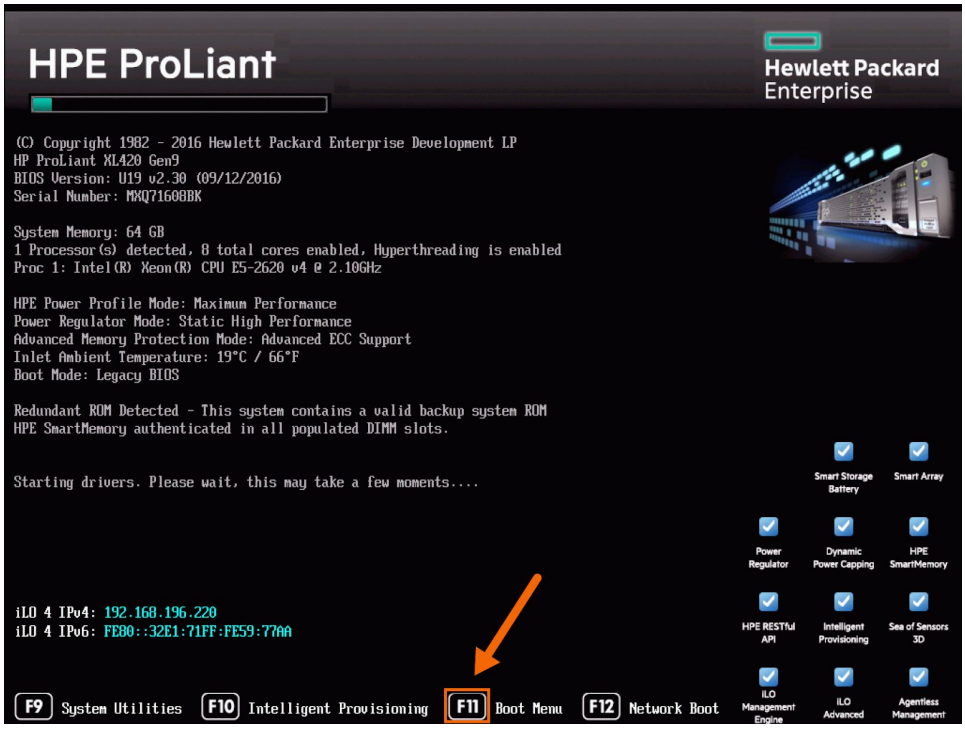
4. Verify that the **Boot Mode** is set to **Legacy BIOS**.
    - **If the Boot Mode is Legacy BIOS**, disregard the rest of the steps in this section and proceed to the **BOOT TO QUMULO CORE USB INSTALLER KEY** section.
    - **If the Boot Mode is not Legacy BIOS**, press **F9** to access the **System Utilities** menu and proceed with the subsequent steps.



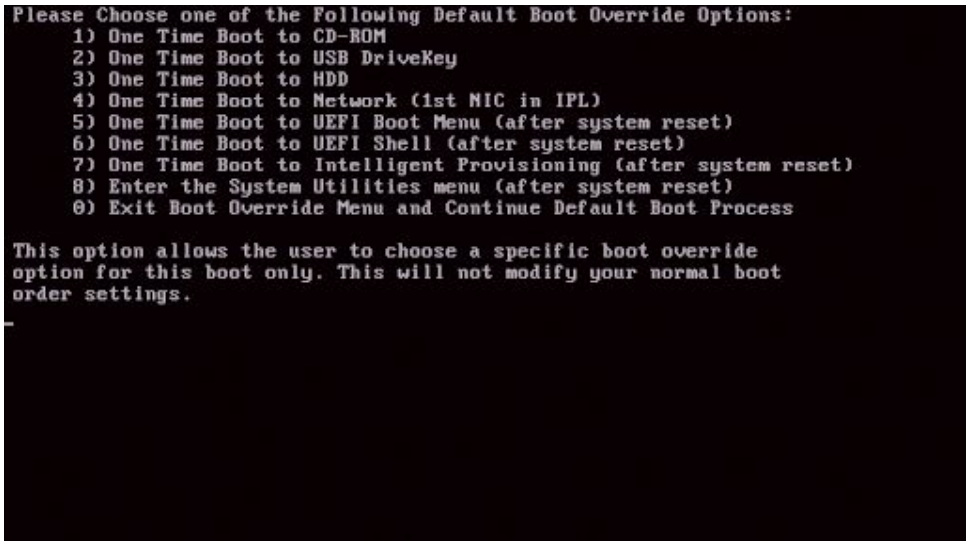
5. Click through the **System Configuration** page to the **BIOS/Platform Configuration** (RBSU) page to the **Boot Options** page.
6. Set **Boot Mode** to **Legacy BIOS Mode** on the **Boot Options** page.
7. Press **F10 to save** the change.
8. Press **Esc** until you return to the main page.
9. Select **Reboot the System**.

BOOT TO QUMULO CORE USB INSTALLER KEY

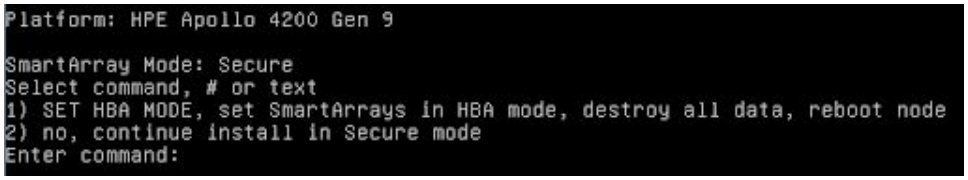
1. Press **F11** to access the **Boot Menu** when prompted at the HPE ProLiant screen. Note that this boot may take a few minutes.



2. Press **ENTER** to boot into the **Legacy Bios One-Time Boot** Menu.
3. Press **ENTER** again to confirm.
4. Select **Option 2** from the **Default Boot Override Options** to do a one-time boot to the Qumulo Core USB Installer key.



5. Select one of the following options to continue the install:

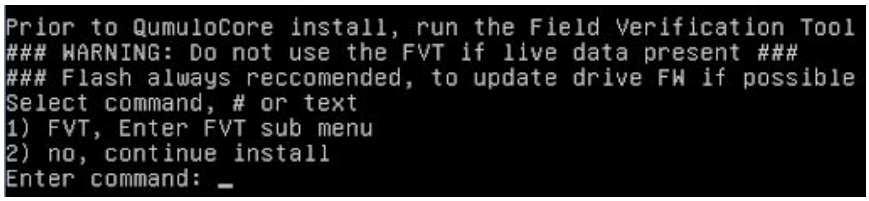


- For an **encrypted** install, select **option 2** and hit **ENTER**.
- For a **non-encrypted** install, select **option 1** and hit **ENTER**. Once the node automatically reboots, repeat the steps in this section to boot to the USB Installer key. Once you return to the SmartArray Mode prompt, select the **continue, install in NonSecure Mode option** for the following boot.

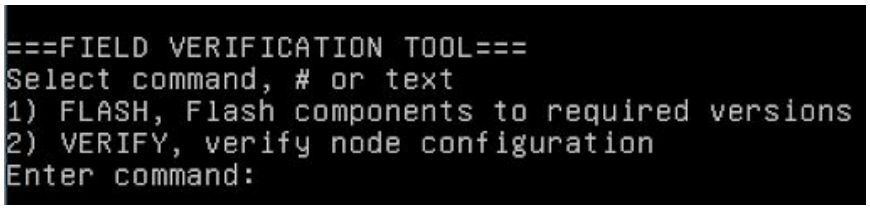
RUN FIELD VERIFICATION TOOL

IMPORTANT! DO NOT run the following Field Verification Tool if any live data is present on the node.

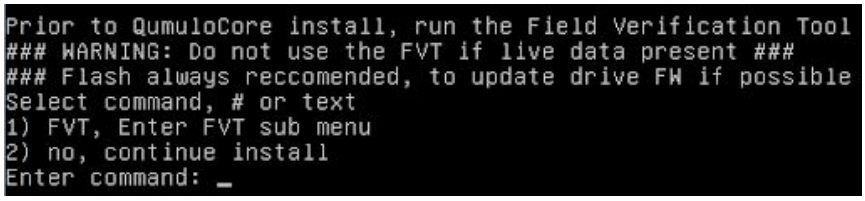
1. **Access the Field Verification Tool (FVT)** menu by typing **1** or **FVT** and hit **ENTER**.



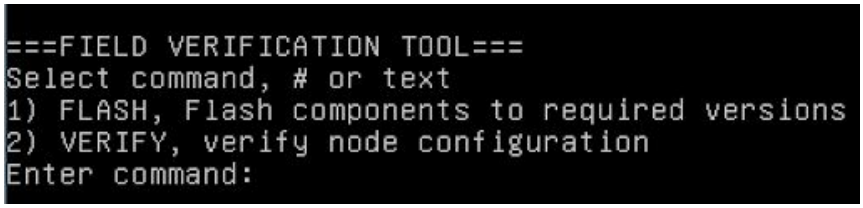
2. **Flash the node components** to the required versions by typing either **1** or **FLASH** and hit **ENTER**.



3. Type **1** or **FVT** on the main menu to continue with the test.



4. Type **2** or **VERIFY** and hit **ENTER** to check the node configuration.



5. Review the results and consider the following before proceeding with a clean install of Qumulo Core:
    - **FAIL messages** reported from **VERIFY** are not indicative of an unsuccessful **FLASH** command and can be resolved with a power-cycle to reflect recent firmware changes.
    - **FAIL messages** on the boot order when running **VERIFY** can be ignored at this time.

If all fields pass, you may skip the FLASHING OF HPE INTELLIGENT PROVISIONING FIRMWARE section and continue cluster configuration by following the steps outlined in the INSTALL QUMULO CORE VIA THE USB KEY section.

If the category for the Intelligent Provisioning Version returns FAILED, execute the steps in the FLASHING OF HPE INTELLIGENT PROVISIONING FIRMWARE section below. Once complete, return to step 3 in this section and run the VERIFY command for FVT. If all fields pass, you may continue to the INSTALL QUMULO CORE VIA THE USB KEY section.

FVT PASS EXAMPLE

FVT FAIL EXAMPLE

FLASHING OF HPE INTELLIGENT PROVISIONING FIRMWARE

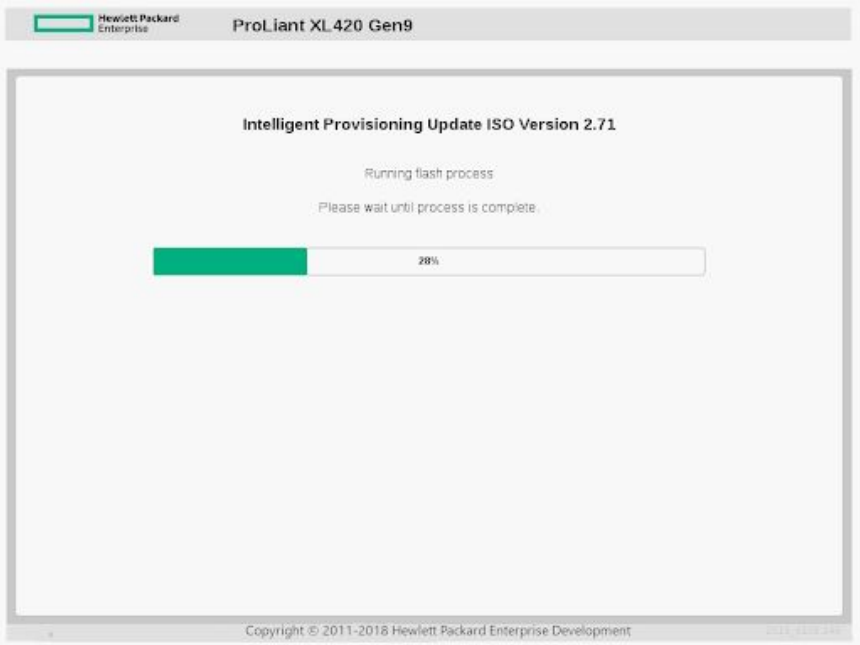
IMPORTANT! ONLY execute these instructions if the Intelligent Provisioning check in the FVT failed. The HPE Intelligent Provisioning firmware for the HPE Apollo 4200 has no method available to flash this component in the system. To acquire the firmware, download the binary file from HPE Support Center and follow the instructions below.

Update Firmware from System Utilities via a USB Drive

1. Convert the iso file to img format.
2. Apply the file to a USB drive or iLO virtual media. Reference the USB Key Utility for Windows article from HPE Support Center for more information.
3. Attach the media to the server.
4. Press **F11** to enter the **boot menu**.
5. Select **boot from USB stick**, and allow the Intelligent provisioning package to update the firmware.
6. Once the upgrade is complete, press **ESC** to return to the main menu and reboot the system.

Update Firmware from System Utilities via Virtual Media

1. Put the iso in an accessible location over the network for the node.
2. Select **Insert Media** and check the **boot on next reboot** option for the iso on the virtual media page.
3. Reset the node and allow the install to complete.



4. Reboot the node into the installer/FVT.
5. Once complete, return to **step 3** of the **RUN FIELD VERIFICATION TOOL** section to rerun FVT.
6. **Type 2** or **VERIFY** and hit **ENTER** to check the node configuration. If all fields pass, you may now proceed to install Qumulo Core.

INSTALL QUMULO CORE VIA THE USB KEY

1. Power on the node or perform a reboot.
2. Press the **F11** key to enter the **boot menu** on the BIOS splash screen.
3. **Type 2** to continue with the install and boot from the USB Installer key.
4. Select no when asked to change between RAID and HBA modes to proceed to the **DESTROY ALL DATA** page.
5. **Type DESTROY ALL DATA** (case-sensitive) to perform a clean install of Qumulo Core on your cluster.

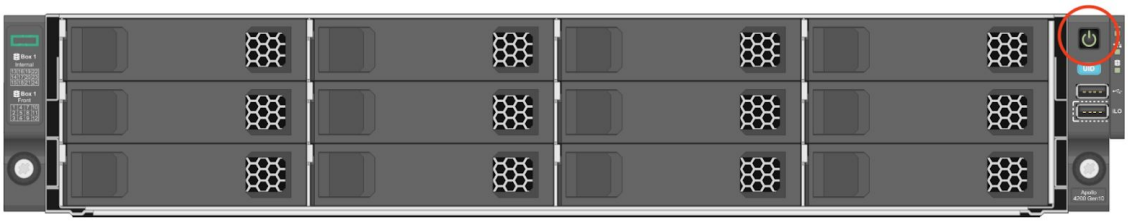
IMPORTANT! If you mistype **DESTROY ALL DATA** three times or type no, the installation will be aborted.

The node will automatically shut down once the installation of Qumulo Core is complete. At that time, remove the USB stick and press the power button to turn on the node. A successful install using the Qumulo Core USB Installer Key will boot the node to the End User Agreement page, the first step in creating a new cluster with Qumulo Core. Before you agree and continue, repeat the steps outlined above for each node that will be included in your Qumulo cluster. Leave the display, keyboard and mouse connected to the last imaged node and follow the instructions below to Create a Cluster.

3.7 HPE Apollo 4200 Gen10

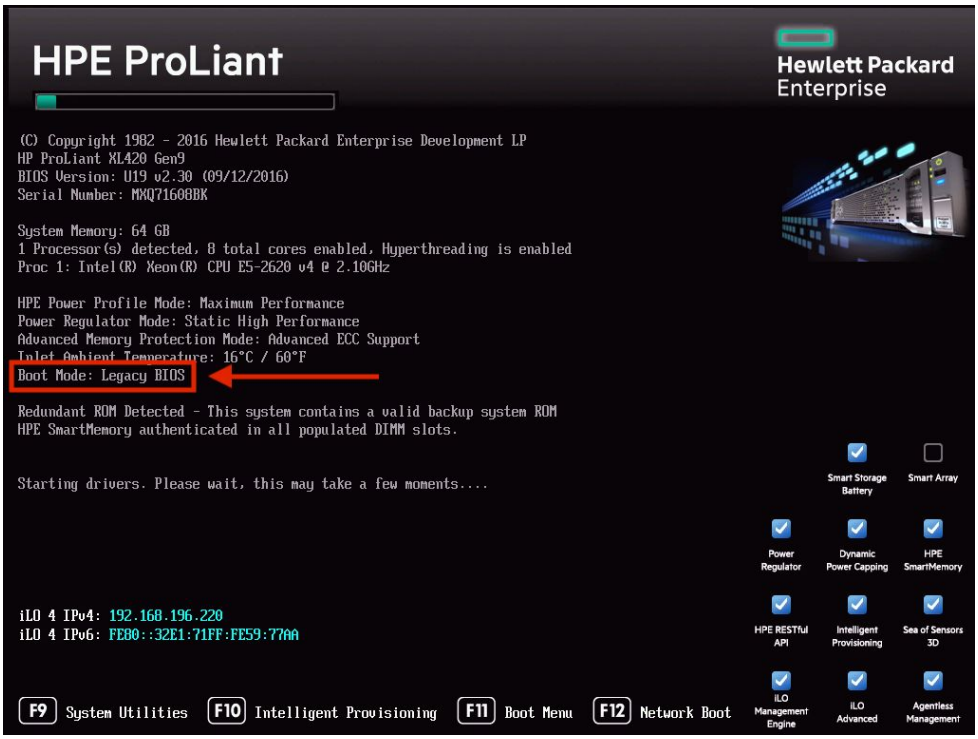
Once your Qumulo-supported hardware is installed, you will need to image the nodes using the instructions below.

1. Shut down the node and connect it to a display, keyboard, and mouse.
2. Plug in the Qumulo Core Installer USB key to an available USB port.
3. Press the **power button** highlighted below to power the node on and wait for the machine's boot screen to display.



4. Verify that the **Boot Mode** is set to **Legacy BIOS**.

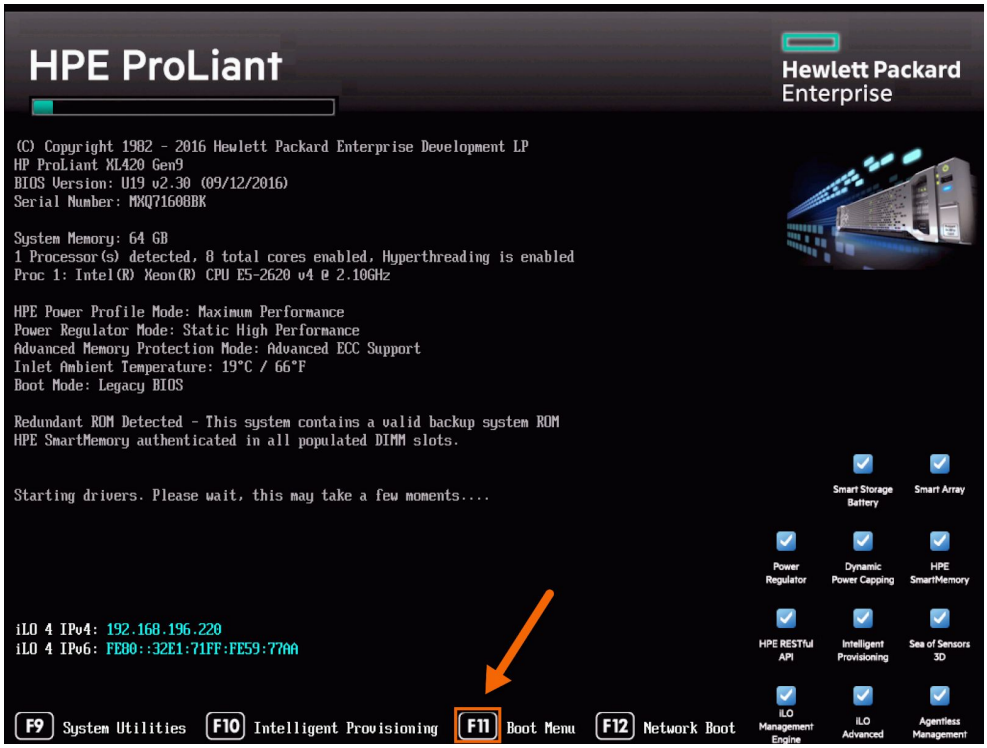
    - **If the Boot Mode is Legacy BIOS**, disregard the rest of the steps in this section and proceed to the **BOOT TO QUMULO CORE USB INSTALLER KEY** section.
    - **If the Boot Mode is not Legacy BIOS**, press **F9** to access the **System Utilities** menu and proceed with the subsequent steps.



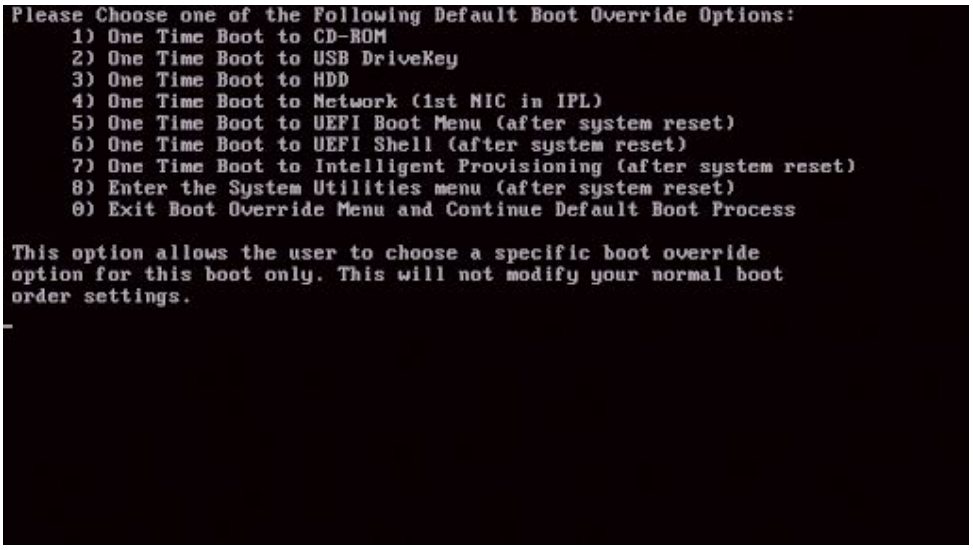
5. **If the Boot Mode is not Legacy BIOS**, press **F9** to access the **System Utilities** menu and proceed with the subsequent steps.
6. Click through the **System Configuration** page to the **BIOS/Platform Configuration** (RBSU) page to the **Boot Options** page.
7. Set **Boot Mode** to **Legacy BIOS Mode** on the **Boot Options** page.
8. Press **F10 to save** the change.
9. Press **Esc** until you return to the main page.
10. Select **Reboot the System**.

BOOT TO QUMULO CORE USB INSTALLER KEY

1. Press **F11** to access the **Boot Menu** when prompted at the HPE ProLiant screen. Note that this boot may take a few minutes.

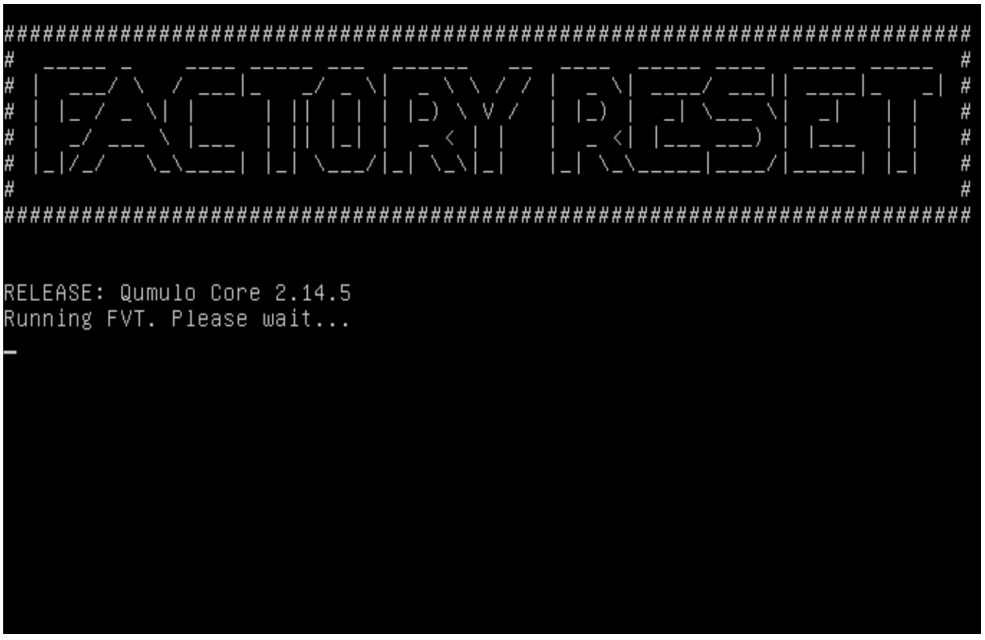


2. Press **ENTER** to boot into the **Legacy Bios One-Time Boot** Menu.
3. Press **ENTER** again to confirm.
4. Select **Option 2** from the **Default Boot Override Options** to do a one-time boot to the Qumulo Core USB Installer key.



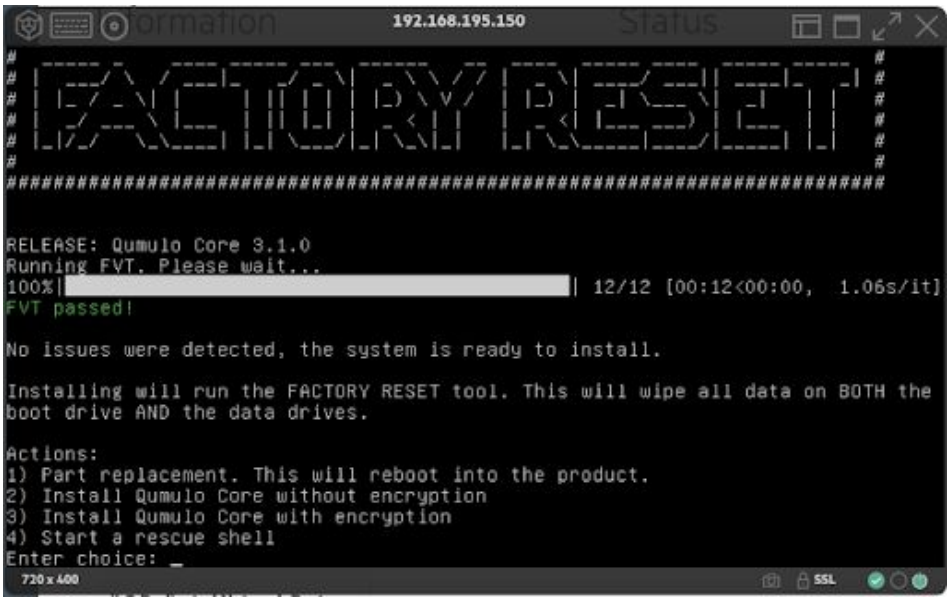
RUN FIELD VERIFICATION TOOL

IMPORTANT! DO NOT run the following Field Verification Tool if any live data is present on the node. The Field Verification Tool will automatically start after reboot.



The test results display once it has concluded. Refer to the following sections for details on Pass and Fail scenarios.

FVT PASS

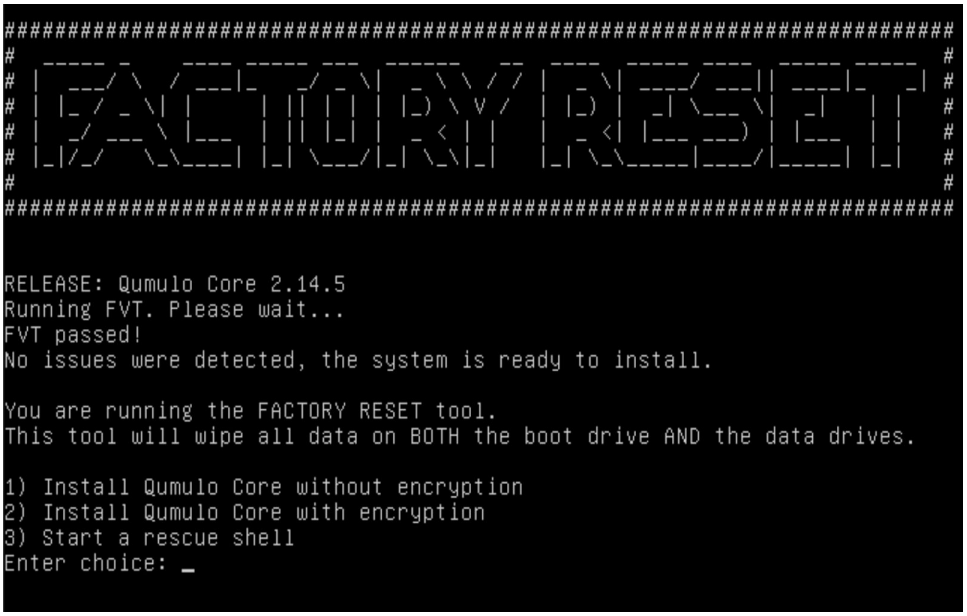


If you see an **FVT passed**! message, proceed to the Installing Qumulo Core section. If **FAIL** messages are present, review the example below to determine the appropriate course.

FVT FAIL CASES

Fixable Issues during Install

If the FVT fails and there are issues that are fixable, you will be prompted to select whether you wish to allow the FVT to auto-correct the detected issues depending on your install scenario.



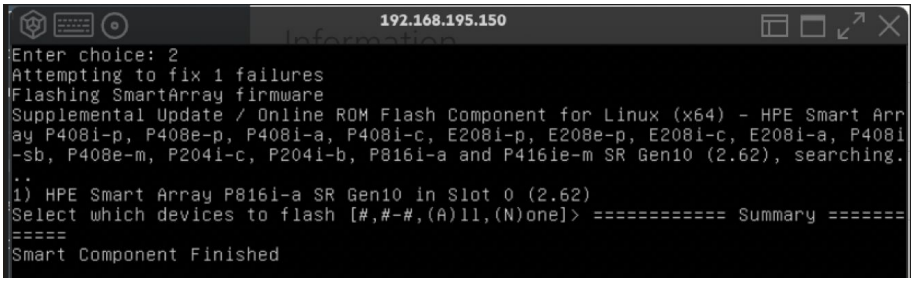
Issues that can be auto-corrected include:

- BIOS config
- Drive firmware
- Drive controller firmware
- NIC mode for CX5
- Boot order

When presented with this menu, **select option 1** to have the tool attempt to fix the issues. If the fixes are successful, the FVT will automatically reboot the node. Return to the **Boot To The Qumulo Core USB Installer Key section** to re-attempt verification and continue the install.

Fixable Issues during Part Replacement

In Qumulo Core 3.1.0 or above, the FVT offers an option to automatically correct issues (such as a firmware upgrade) after a part replacement has been performed. In this case, **select option 2** to run FVT Flash for a part replacement. This will fix the issue and reboot into the FVT menu once more to proceed with the installation.



Non-Fixable Issues

If the FVT is unable to automatically fix any failures detected, the message “Not fixable issues were detected” will display after providing failure reasons.

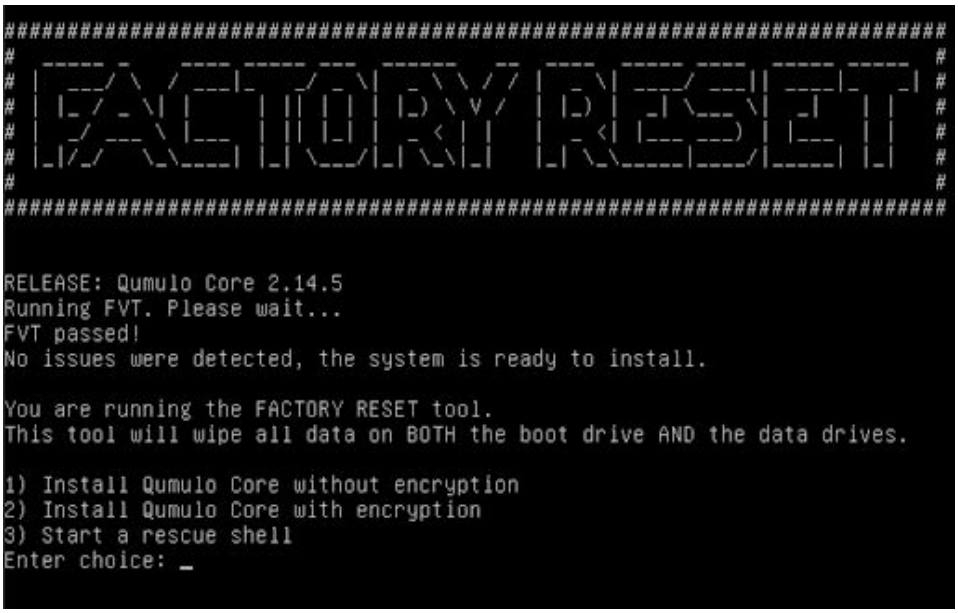
Examples of non-fixable issues:

- BIOS version
- ILO version
- NIC FW

Please reach out to Qumulo Care for additional troubleshooting options.

INSTALL QUMULO CORE

Now that the server has verified it is ready to be configured, you can start to install Qumulo Core.



NOTE: If only performing a part replacement on your system, **select option 1** to reboot and skip the remaining steps.

1. Select whether you wish to install with or without encryption.
2. When prompted, type **DESTROY ALL DATA** to confirm that all data will be destroyed on the server.
3. If you selected Install Qumulo Core with encryption in Step 1, enter your crypto login password and master encryption key following the guidelines displayed. See the requirements below:

Encryption Master Key Requirements

- 10 to 32 characters in length
- ASCII only
- Uppercase letters, lowercase letters, numbers, and symbols are allowed
- <space>, <semicolon>, and <double quote> are NOT allowed

IMPORTANT! Be sure to store the key in a secure location for the lifetime of the cluster.

Crypto Login Password Requirements

- 8 to 16 characters in length
- Must contain at least one upper-case character
- Must contain at least one lower-case character
- Must contain at least one numeric character
- Must contain at least one symbol such as # or $
- ASCII only
- Uppercase letters, lowercase letters, numbers, and symbols are allowed
- <space>, <semicolon>, and <double quote> are NOT allowed

The node will automatically shut down once the installation of Qumulo Core is complete. At that time, remove the USB stick and press the power button to turn on the node. A successful install using the Qumulo Core USB Installer Key will boot the node to the End User Agreement page, the first step in creating a new cluster with Qumulo Core. Before you agree and continue, repeat the steps outlined above for each node that will be included in your Qumulo cluster. Leave the display, keyboard and mouse connected to the last imaged node and follow the instructions below to Create a Cluster.

For additional guidance on cluster configuration and getting started, reference the Qumulo Installation FAQ article in the Getting Started section of Qumulo Care for more details.

---

4. Networking

Your cluster is racked so on to networking! Before beginning, verify that you have compatible network cables, enough ports to connect all the nodes to the same switch fabric, and have configured one static IP per node per defined VLAN. Lastly, ensure that your network switch meets the following criteria:

- 10Gbps, 40Gbps or 100Gbps ethernet, depending on platform
- Fully non-blocking architecture
- IPv6 capable

For additional details on configuring your network, check out the Networking section available on Qumulo Care.

4.1 Recommendations for QC Series

- Two redundant switches
- One physical connection per node to each redundant switch
- One LACP port-channel per node
    - Active mode
    - Slow transmit rate
    - Trunk port with a native VLAN
- N-1 (N=number of nodes) floating IPs per node per client-facing VLAN
- DNS servers
- Time server (NTP)
- Firewall protocol/ports allowed for Proactive Monitoring

Networking is required for front-end and intra-node communication on Qumulo clusters.

- Front-end networking supports IPv4 and IPv6 for client connectivity and also offers support for multiple networks.
- Intra-node communication requires no dedicated backend infrastructure and shares interfaces with front-end connections.
- Clusters use IPv6 link-local and Neighbor Discovery protocols for node discovery and intra-node communication.

TIP! For IPMI configuration details, check out the IPMI Quick Reference Guide on Qumulo Care for information on port location and setup.

Layer 1 Connectivity for QC24/QC40

- Supports 10GbE Only
- SFP+optics with LC/LC Fiber
- SFP+Passive Twinax Copper (Max length 5M)

NIC Ports

Layer 1 Connectivity for QC104/QC208/QC260/QC360

- Supports 40GbE
- QSFP+ transceivers
- Bidirectional (BiDi) transceivers are supported with Mellanox Connect-X 4/5 NICs
- QSFP+Passive Twinax Copper (Max length 5M)

NOTE: Currently only the left-most network card is utilized on the 4U platforms. The card on the right is reserved for future expansion and is not available for use.

NIC Ports

Layer 2 Connectivity & Interface Bonding

Interface Bonding combines multiple physical interfaces into a single logical interface. Bonding enables built-in redundancy so that a logical interface can survive a physical interface failure. In the case of LACP, additional bond members increase the aggregate throughput. Note that LACP is Qumulo's default network bonding and preferred configuration.

Below are the different types of supported bonding for active port communication:

- Link aggregation control protocol (LACP)
    - Active-active functionality
    - Requires switch-side configuration
    - May span multiple switches when utilizing multi-chassis link aggregation
- Active-backup NIC bonding
    - Automatic fail-back
    - Does not require switch-side configuration
    - All active ports must reside on the same switch

4.2 Recommendations for Qumulo K-Series

The Qumulo K-series platform uses a networking configuration where both back end and front end traffic are handled by the same NIC. For reliability, the recommended configuration is fully-cabled, where both ports on each node should be connected. Connecting a single port on the NIC is not recommended, because if the single connection fails, the node will be unavailable.

CAUTION: Do not use the LOM ports. Only use the external NIC ports for the 10Gb connections as highlighted below.

Recommendations:

- One set of redundant switches
  - Jumbo Frame support with a minimum of 9000 MTU
- One physical connection per node to each redundant switch
- One LACP port-channel on each node
  - Active mode
  - Slow transmit rate
  - Trunk port with a native VLAN
- N-1 (N=number of nodes) floating IPs per node per client-facing VLAN
- DNS servers
- Time server (NTP)
- Firewall protocol/ports allowed to Enable Proactive Monitoring

TIP! For IPMI configuration details, check out the IPMI Quick Reference Guide for Qumulo K-Series on Qumulo Care for information on port location and setup.

Connect to Redundant Switches

The details below outline how to connect a 4 node Qumulo K-series cluster to dual switches for redundancy. This is the recommended configuration for Qumulo K-series hardware. If either switch goes down, the cluster will still be accessible from the remaining switch.

- The two NIC ports (2x10Gb) on the nodes are connected to separate switches
- Uplinks to the client network should equal the bandwidth from the cluster to the switch
- The two ports form an LACP port channel via multi-chassis link aggregation group

Connect to a Single Switch

The details below outline how to connect a 4 node Qumulo K-series cluster to a single switch. Note if this switch goes down, the cluster will not be accessible.

- Each node contains two ports (2x10Gb) that are connected to the switch
- Uplinks to the client network should equal the bandwidth from the cluster to the switch
- The two ports form an LACP port channel

4.3 Recommendations for Qumulo P-Series

The all-flash platform uses a networking configuration where back end and front end traffic is handled by different NICs. The front end and back end NICs in a cluster may all be connected to the same switch, or the back end NICs may be connected to a different switch from the front end NICs. For reliability, the recommended configuration is fully-cabled where all four ports on every node should be connected. Both ports on the front end NIC should be connected to the front end switch, and both ports on the back end NIC should be connected to the back end switch. Connecting a single port on the back end NIC is not recommended. If the single back end connection fails, the node will be unavailable.

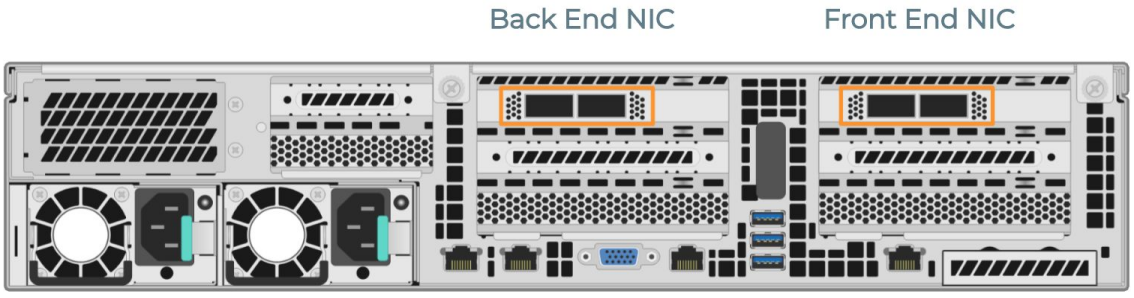
Recommendations:

- One set of redundant switches for the front end network with minimum 9000 MTU configured
- One set of redundant switches for the back end network with minimum 9000 MTU configured
- One physical connection per node to each redundant switch
- One LACP port-channel per network (front end and back end) on each node with the following:
    - Active mode
    - Slow transmit rate
    - Trunk port with a native VLAN
- N-1 (N=number of nodes) floating IPs per node per client-facing VLAN
- DNS servers
- Time server (NTP)
- Firewall protocol/ports allowed to Enable Proactive Monitoring

TIP! For IPMI configuration details, check out the IPMI Quick Reference Guide for information on port location and setup.

Connect to Redundant Switches

The details below outline how to connect a 4 node Qumulo P-series cluster to dual switches for redundancy. This is the recommended configuration for Qumulo P-series hardware. If either switch goes down, the cluster will still be accessible from the remaining switch.



Front End

- The two front end NIC ports (2x40Gb or 2x100Gb) on the nodes are connected to separate switches
- Uplinks to the client network should equal the bandwidth from the cluster to the switch
- The two ports form an LACP port channel via multi-chassis link aggregation group

Back End

- The two back end NIC ports (2x40Gb or 2x100Gb) on the nodes are connected to separate switches with an appropriate inter-switch link or virtual port channel
- For all connection speeds, the default behavior is LACP with a 9000 MTU. This Qumulo configuration, in conjunction with a Multi-Chassis Link-Aggregation configuration on the switch side and associated 9216 network MTU, benefits from both link redundancy and increased bandwidth capacity.
- For all connection speeds, the default behavior is LACP with 9000 MTU. The switch should be running in a Link-Aggregation configuration with 9216 network MTU. You can optionally configure these ports in Active-Backup through the qq command-line interface. Please see the section below for those instructions.

Connect to a Single Switch

The details below outline how to connect a 4 node Qumulo P-series cluster to a single switch. Note if this switch goes down, the cluster will not be accessible.

Front End

- Each node contains two front end ports (2x40Gb or 2x100Gb) that are connected to the switch
- Uplinks to the client network should equal the bandwidth from the cluster to the switch
- The two ports form an LACP port channel

Back End

- Each node contains two back end ports (2x40Gb or 2x100Gb) that are connected to the switch
- For all connection speeds, the default behavior is LACP with a 9000 MTU. This Qumulo configuration, in conjunction with a Link-Aggregation configuration on the switch side and associated 9216 network MTU, benefits from both link redundancy and increased bandwidth capacity.
- For all connection speeds, the default behavior is LACP with 9000 MTU. The switch should be running in a Link-Aggregation configuration with 9216 network MTU. You can optionally configure these ports in Active-Backup through the qq command-line interface. Please see the section below for those instructions.

Set the Back End MTU and Bonding Mode via QQ CLI

The bonding mode and MTU for the back end network can be configured via the qq command-line with the following qq commands.

Use the command below to show the current configuration:

```
qq network_get_interface --interface-id 2
```

To set the MTU, use the following command:

```
qq network_mod_interface --interface-id 2 --mtu 9000
```

Run the following command to set the bonding mode to **Active/Backup:**

```
qq network_mod_interface --interface-id 2 --bonding-mode ACTIVE_BACKUP
```

IMPORTANT! If Active_Backup is set, please ensure all configurations related to LACP or other redundancy methodologies are removed from the switch configurations on the affected ports. Failure to do so may result in unpredictable behaviors.

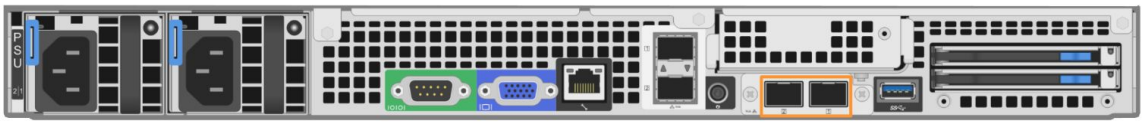
To list both interfaces on the back end network, run the following command:

```
qq network_list_interfaces
```

4.4 Recommendations for Qumulo C-Series

The Qumulo C-series platform uses a networking configuration where both back end and front end traffic are handled by the same NIC. For reliability, the recommended configuration is fully-cabled, where both ports on each node should be connected. Connecting a single port on the NIC is not recommended, because if the single connection fails, the node will be unavailable.

CAUTION: Do not use the LOM ports. Only use the external NIC ports for the 25Gb connections as highlighted below.



NIC Ports

Recommendations:

- One set of redundant switches
    - Jumbo Frame support with a minimum of 9000 MTU
- One physical connection per node to each redundant switch
- One LACP port-channel on each node
    - Active mode
    - Slow transmit rate
    - Trunk port with a native VLAN
- N-1 (N=number of nodes) floating IPs per node per client-facing VLAN
- DNS servers
- Time server (NTP)
- Firewall protocol/ports allowed to Enable Proactive Monitoring

TIP! For IPMI configuration details, check out the IPMI Quick Reference Guide for Qumulo C-Series on Qumulo Care for information on port location and setup.

Connect to Redundant Switches
The details below outline how to connect a 4 node Qumulo C-series cluster to dual switches for redundancy. This is the recommended configuration for Qumulo C-series hardware. If either switch goes down, the cluster will still be accessible from the remaining switch.

- The two NIC ports (2x25Gb) on the nodes are connected to separate switches
- Uplinks to the client network should equal the bandwidth from the cluster to the switch
- The two ports form an LACP port channel via multi-chassis link aggregation group

Connect to a Single Switch
The details below outline how to connect a 4 node Qumulo C-series cluster to a single switch. Note that if this switch goes down, the cluster will not be accessible.

- Each node contains two ports (2x25Gb) that are connected to the switch
- Uplinks to the client network should equal the bandwidth from the cluster to the switch
- The two ports form an LACP port channel

4.5 Configure LACP

LACP is enabled by default for new clusters. If your switch ports are not configured for LACP, the interface will automatically downgrade to active-backup mode. The active-backup mode that's automatically enabled has one consideration: if a failover happens, the backup port will take over as expected. When the active port comes back up, the active port will not resume as expected. Traffic will instead be pinned to the backup port until another failure event happens.

To avoid this behavior, you can explicitly set the ports to active-backup with the following command:

```
qq network_conf_mod --bonding-mode ACTIVE_BACKUP
```

NOTE: Be aware that making these changes will trigger a cluster event while the new network bond is negotiated per node and will result in a small outage.

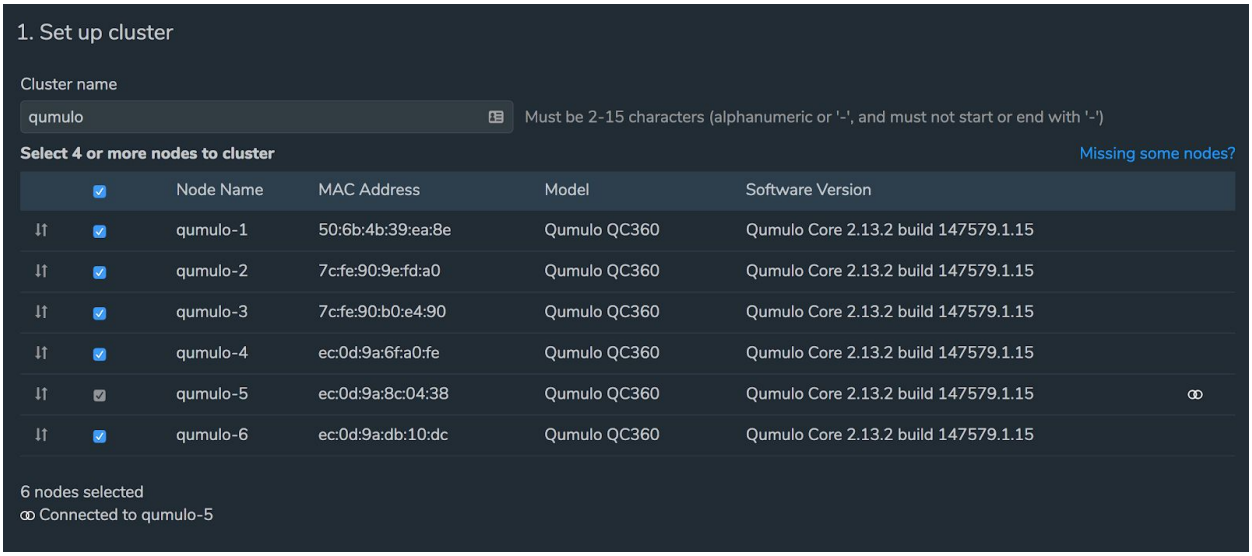
---

5. Create a Cluster

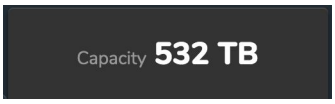
- Power on the node(s) that will be used to form the cluster
- Review the End User License Agreement, check the box to agree and click **Submit**

5.1 Set up cluster

- Name the cluster
- Select the nodes for the cluster
  - If any nodes are missing, verify that the node is currently running and on the same network



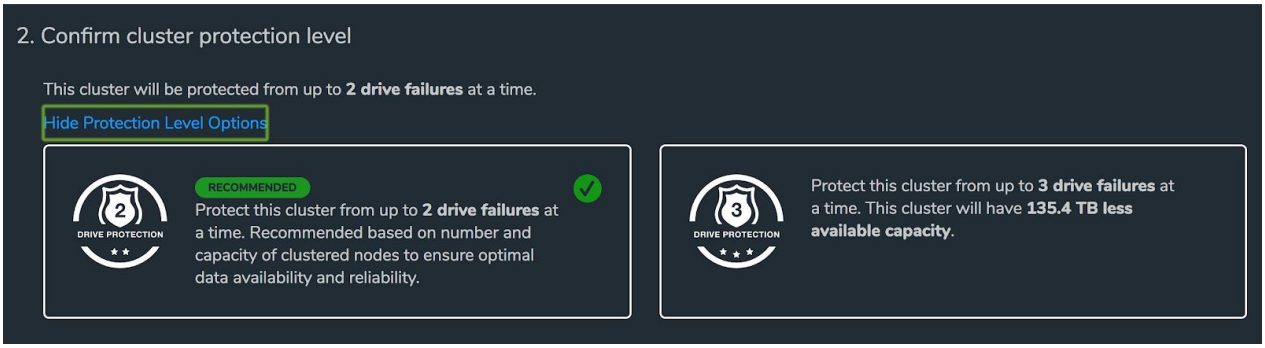
NOTE: The total capacity for the cluster is dynamically updated at the bottom of the page when selecting nodes.



5.2 Confirm cluster protection level

The recommended 2- or 3-drive protection level will be selected by default

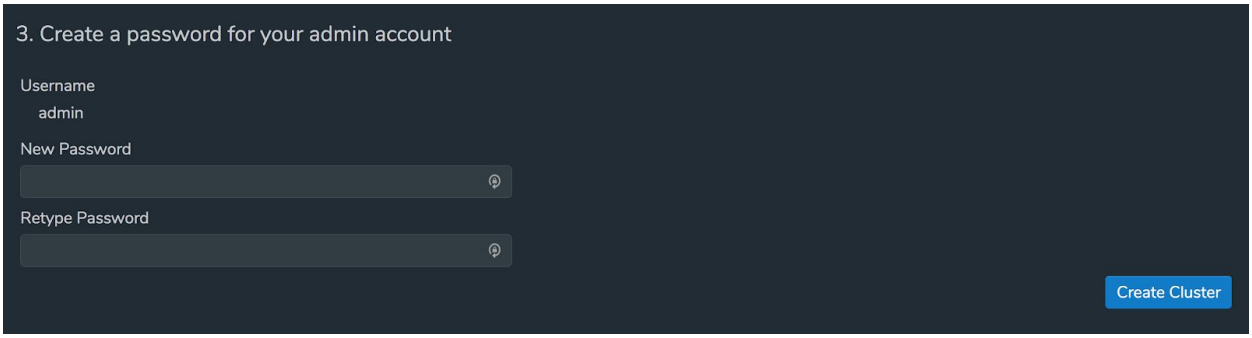
If **Customize Protection Level** is displayed, the option is available to increase the resilience of the system by selecting 3 drive protection. Keep in mind that selecting 3 drive protection will result in less capacity for the cluster.



NOTE: The option for selecting the drive protection level is only available at cluster creation and cannot be changed after the fact.

5.3 Create a password for your admin account

- Type in the password for your admin account
- Retype the password to confirm
- Click **Create Cluster**

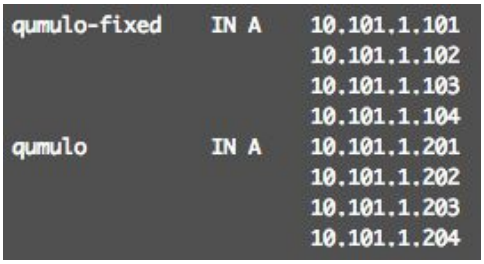


To access the dashboard in the Qumulo Core UI remotely, use any node's IP address to connect via web browser.

6. Configure IP Failover

IP Failover is a high-availability feature that allows a node's virtual IP address(es) to be reassigned to other nodes in the cluster should a node go offline for any reason. In addition to the fixed IP range assigned to a cluster, an administrator can set a floating range of addresses that can be reshuffled amongst online nodes as necessary. When using IP Failover, it is recommended that the cluster's client-facing DNS record be pointed at these floating IPs as opposed to the fixed range.

For example, in a BIND zone, your records may look something like this where 10.101.1.201-204 is the floating range:



```
qumulo-fixed    IN A    10.101.1.101
                        10.101.1.102
                        10.101.1.103
                        10.101.1.104
qumulo          IN A    10.101.1.201
                        10.101.1.202
                        10.101.1.203
                        10.101.1.204
```

Clients mount the cluster using the Qumulo hostname:

Mac Client

```
mount -t nfs -o rsize=65536,wsize=65536,intr,hard,tcp,rdirplus,readahead=128
your.qumulo.ip:/share /path/to/mountpoint
```

Mac Client with Local Locking Enforced

```
mount -t nfs -o
rsize=65536,wsize=65536,intr,hard,tcp,locallocks,rdirplus,readahead=128
your.qumulo.ip:/share /path/to/mountpoint
```

Linux Client

- Please note that modern Linux distributions auto negotiate a 1MB read/write block size (rsize/wsize of rsize=1048576).

```
mount -t nfs -o intr,hard,tcp your.qumulo.ip:/share /path/to/mountpoint
```

Linux Client with Local Locks Enforced

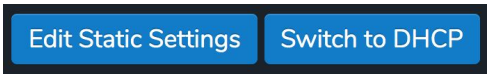
```
mount -t nfs -o intr,hard,tcp,local_lock=all your.qumulo.ip:/share
/path/to/mountpoint
```

In a node outage scenario, any IP in the floating range that was assigned to the offline node would move to another available node ensuring that connected clients can continue writing and reading to/from the cluster. Typically the time it takes to fail an IP over to another node will cause only a momentary blip in any running workloads. Please note that certain connections like SMB will have to re-connect, as they require a new TCP connection. However, the failover is fast enough that most operating systems' retry mechanism can handle it.

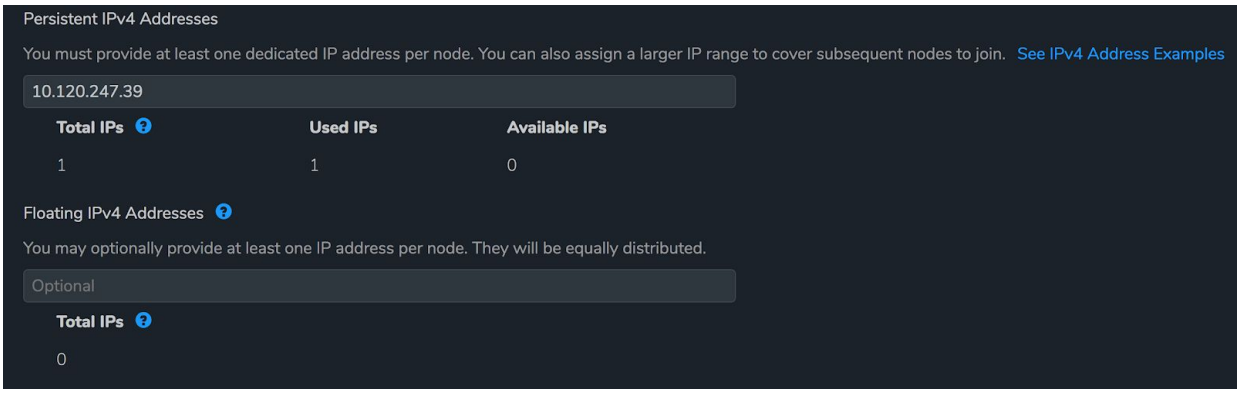
You can use the Qumulo Core Web UI or the CLI to set up IP Failover on your Qumulo cluster as detailed below.

6.1 Web UI

1. Log in to your cluster's Web UI as 'admin'.
2. Hover over the **Cluster** menu and select **Network Configuration**.
3. On the Network Configuration page, click on **Edit Static Settings**.



4. In the fields for Persistent IPv4 Addresses and Floating IPv4 Addresses, enter your fixed and floating ranges.



5. Click **Save**.

6.2 QQ CLI

1. Using a node's IP address, ssh to the cluster as admin.

```
ssh admin@10.101.1.101
```

2. Login as root:

```
sudo -s
```

3. Run the following qq command replacing the IP range with your preferred floating range:

```
qq network_conf_mod --floating-ip-ranges 10.100.1.201-204
```

Note: We recommend assigning enough floating IP addresses so that each node will have the total number of nodes minus one for the number of floating IP addresses (up to 10 per node). The math to use is N-1*N where N is the total number of nodes in the cluster. Assuming many client connections, this best practice could help evenly distribute the connections from the lost node onto the remaining nodes as needed. For example, in a 4 node cluster when 1 node goes offline, its 3 virtual IPs would then float to each of the remaining 3 nodes.

---

7. Install VPN Keys

You can install Qumulo VPN keys over the network on a MAC or Windows machine by following the steps outlined below. Before you begin, ensure that you have the VPN keys on hand from our friendly Qumulo Care team and check that firewall rules have been modified to allow the following ports:

- Whitelist *missionq.qumulo.com*, *ep1.qumulo.com*, and *monitor.qumulo.com* and permit outbound HTTPS traffic over port 443

NOTE: If the firewall performs Stateful Packet Inspection (sometimes called SPI or Deep Packet Inspection), the firewall admin must explicitly Allow OpenVPN (SSL VPN) rather than simply opening port 443.

7.1 Mac

1. Download and unzip the zip file that your Customer Success Manager provided onto a computer running Mac OS X on the same network as the cluster.
2. Bring up a terminal and copy the 3 files onto one of the nodes.

```
scp /<VPN Key file path>/* admin@<node ip address>:~/
```

3. SSH to the same node where you've copied the VPN key files.

```
ssh admin@<node ip address>
```

4. Install VPN Keys to all the nodes on the cluster.

```
sudo qq install_vpn_keys /home/admin/
```

5. Proceed to Final Steps below.

7.2 Windows

1. Download the latest version of putty.exe and pscp.exe from here onto a Windows machine.
2. Download and unzip the zip file that your Customer Success Manager provided onto the same Windows machine on the same network as the cluster.
3. Bring up a command line window, browse to the folder that contains putty.exe and pscp.exe and copy the three files onto one of the nodes.

```
cd \Users\<username>\Downloads\
pscp \<VPN Key file path>\* admin@<node ip address>:/home/admin
```

4. Execute putty.exe and enter in the Host Name field of the same node where you've copied the VPN key files.

```
admin@<node ip address>
```

5. Install VPN Keys to all the nodes on the cluster.

```
sudo qq install_vpn_keys /home/admin/
```

7.3 Final Steps

1. Verify that the keys are installed.

```
sudo qq get_vpn_keys
```

2. Clean up by removing VPN Key files from */home/admin*:

```
rm /home/admin/*.key
rm /home/admin/*.crt
```

3. Identify cluster ID using the following command:

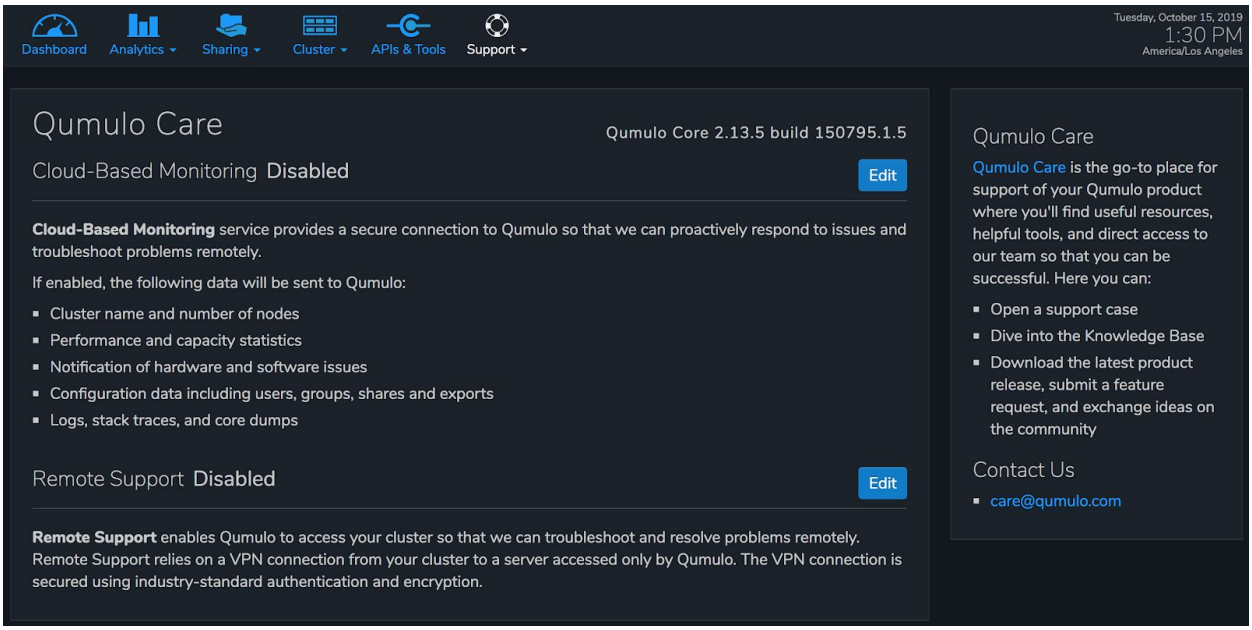
```
sudo qq node_state_get
```

4. Send the Customer Success team the output and provide the name of the cluster.
5. Enable the Qumulo Care Remote Support option via the Web UI.
6. Notify Customer Success Team when this is complete so that VPN connectivity can be tested and the cluster can be added to Qumulo's Cloud-Based Monitoring service.

---

8. Enable Proactive Monitoring

Qumulo Care offers you the ability to enable two support features on your Qumulo cluster: Qumulo's Cloud-Based Monitoring, which enables our team to proactively detect potential problems; and Qumulo's Remote Support, which allows access to your cluster via VPN to troubleshoot and resolve problems remotely.



To use Qumulo's proactive monitoring, make sure that you have done the following:

- Installed VPN Keys as instructed above
- Protocols/ports allowed to the following destination hostnames as outlined in the table below:

Feature	Protocol	Ports	Destination
Cloud-Based Monitoring	tcp	443	missionq.qumulo.com
Remote Support	tcp	443	ep1.qumulo.com
Log Uploads	tcp	443	monitor.qumulo.com
Proxy Forwarding [if applicable]	tcp	443	missionq-dumps.s3.amazonaws.com

8.1 Cloud-Based Monitoring

Cloud-Based Monitoring is an internal monitoring tool that allows Qumulo's Customer Success team to proactively monitor your cluster. Enabling this feature in the UI or via the qq CLI allows the cluster to send detailed diagnostic data over an encrypted connection to a Qumulo cloud instance. Qumulo has developed a proprietary application that aggregates cluster diagnostic data and sends alerts to our Customer Success team should an issue arise.

Once enabled, the following data will be collected by Qumulo so that our team can proactively reach out if an incident occurs.

- Cluster name and number of nodes
- Performance and capacity statistics
- Notification of hardware and software issues
- Configuration data including users, groups, shares and exports
- Logs, stack traces, and core dumps

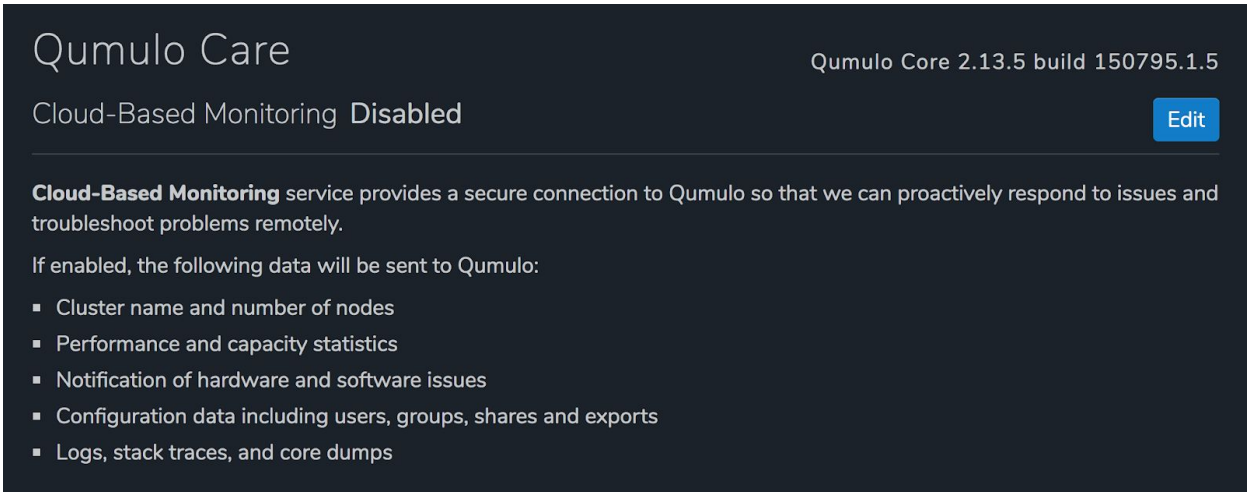
Information that is **not** collected by our Cloud-Based Monitoring service includes:

- File and path names
- Client IP addresses
- Login information (such as usernames and passwords)

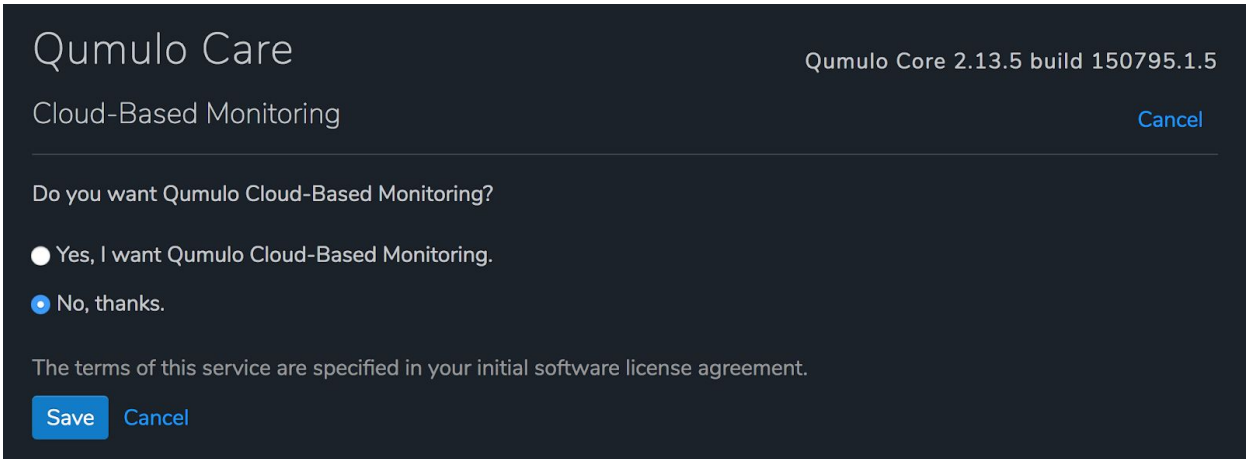
NOTE: Qumulo's Cloud-Based Monitoring service does **not** collect file & path names, client IP addresses, and login information (such as usernames & passwords).

To enable Cloud-Based Monitoring via the UI:

1. In the Web UI, hover over the **Support menu** and click **Qumulo Care.**
2. Click the **Edit** button for Cloud-Based Monitoring.

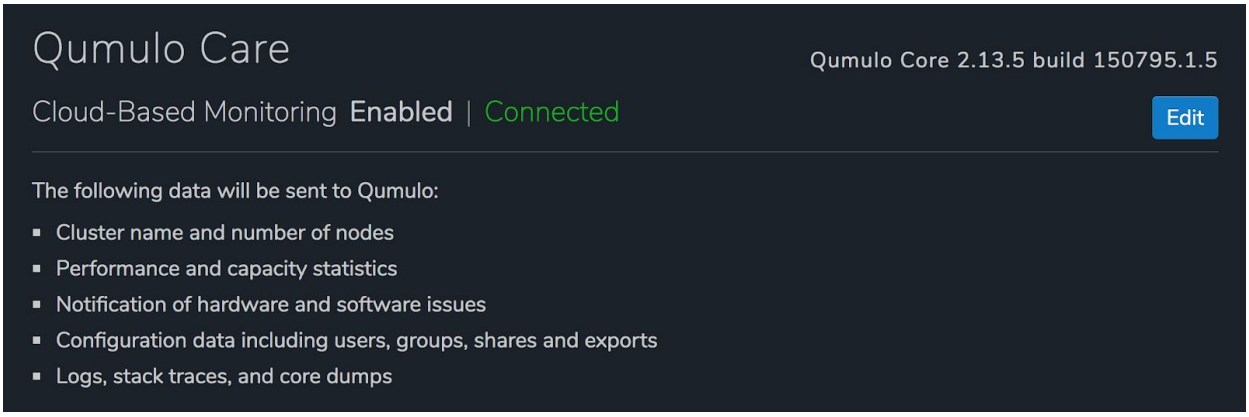


3. Enable Cloud-based Monitoring by selecting **Yes** or disable by selecting **No**.



4. Click **Save**.

Once enabled, Cloud-Based Monitoring will display as **Enabled | Connected** on the Qumulo Care page.



To enable Cloud-Based Monitoring via QQ CLI:

Run the following command from a node to enable:

```
qq set_monitoring_conf --enabled
```

Run the command below to disable:

```
qq set_monitoring_conf --disabled
```

Verify the cluster's monitoring configuration by using the following command:

```
qq monitoring_conf
```

Our team receives alerts 24/7 for the following incidents via Cloud-based Monitoring so that we can be available for help when you need it the most:

- Drive CRC errors & SMART status alerts
- Drive Failures (SSD & HDD)
- Capacity Triggers
- Power Supply Failure
- Fan failure
- New Process Core Dump
- Recused Node
- Node Offline
- Lost Communication with Cluster

Depending on the severity of the issue and the current state of the cluster, a member from our team will reach out in the following ways. Primarily your team will be notified via Slack or email for most incidents listed above. For critical alerts, our team will call the phone number provided for the technical contact to resolve the issue. Reference the table below for additional details.

Severity	Description	Response Times
0	Outage, data loss or corruption. Example: Cluster is down or not enough up nodes to form quorum.	2 hours; 24×7
1	High business impact, but the cluster is still functional. Example: A node is down but the cluster is still in quorum.	2 hours; 24×5
2	Bad bug, but a workaround is available. Example: Poor performance if you ls and dd from the same client. The workaround could be to mount to two different nodes and run ls against node 1 and dd against node 2.	2 hours; 24×5
3	Poor user experience or annoyance. Example: A hover dialog lingers for ~5s after changing.	6 hours; 24×5
4	Cosmetic, other. Example: Change in the background color of a dialog box.	6 hours; 24×5

Hardware replacement: Advance replacement, next business day FRUs: HDD, SSD, power supply, fans, optics and cables

8.2 Remote Support

Remote Support allows access to your cluster so that Qumulo Care can troubleshoot and resolve problems remotely. Using a secure VPN connection accessed only by Qumulo, the following information is available to an authorized Qumulo Care team member to provide help when you need it the most.

- Cluster name and number of nodes
- Performance and capacity statistics
- Notification of hardware and software issues
- Configuration data including users, groups, shares and exports
- Logs, stack traces, and core dumps

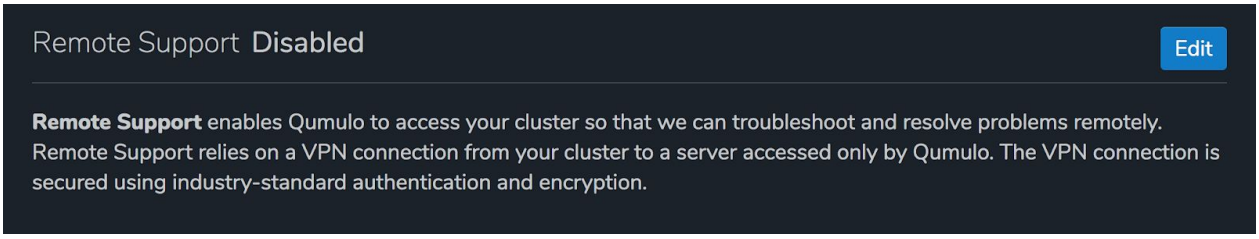
Remote Support relies on a VPN connection (IPv6 configurations not supported) from your cluster to a server accessed only by Qumulo using industry standard authentication and encryption. To secure this connection, VPN Keys are installed on each Qumulo node in /etc/openvpn at initial installation. Once Remote Support is enabled on your cluster, an authorized member of the Qumulo Care team can open a connection to your cluster via the openvpn tunnel that is closed by default. This connection will remain established for a fixed period of four hours or can be modified per customer security requirements if necessary.

IMPORTANT! If your company has an intrusion detection device or firewall that performs SSL/HTTPS Deep Packet Inspection, you will need to add an exception for the ep1.qumulo.com IP address. Run the command below on your cluster to identify the IP address for ep1.qumulo.com:

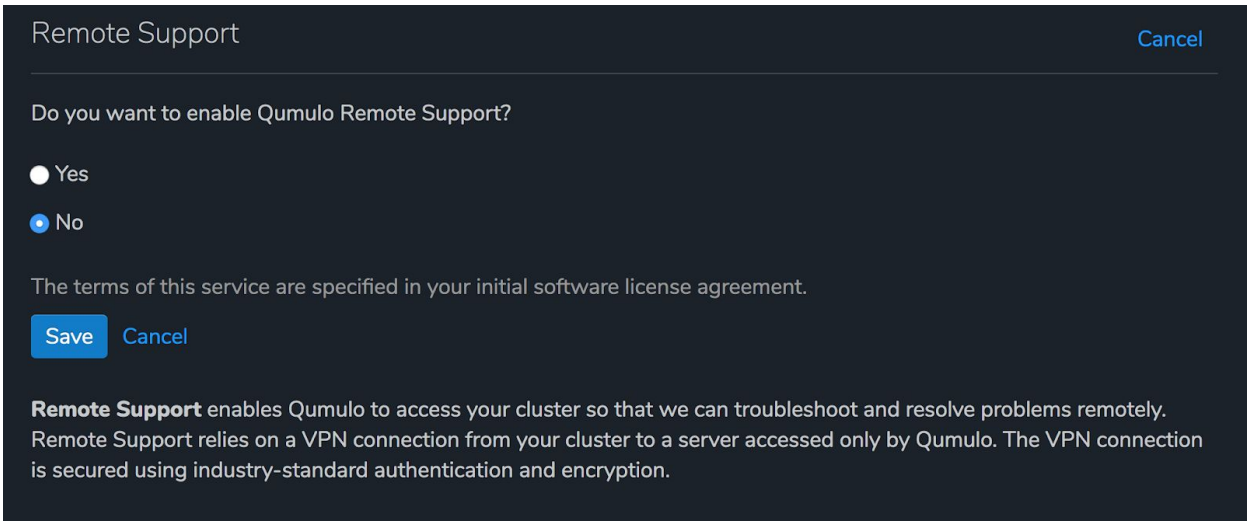
```
nslookup ep1.qumulo.com
```

To enable Remote Support via the UI:

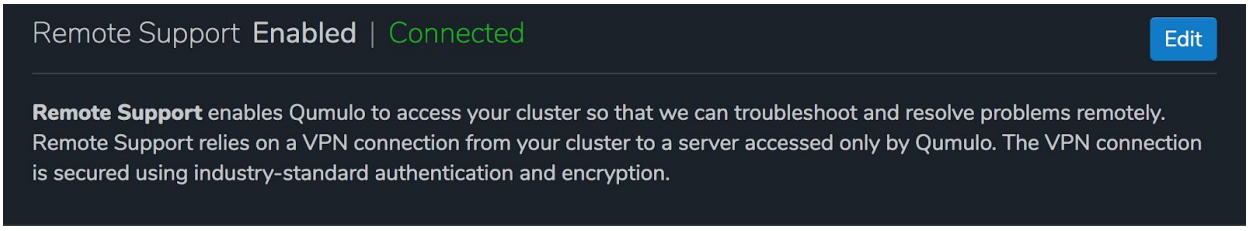
1. In the Web UI, hover over the **Support** menu and click **Qumulo Care.**
2. Click the **Edit** button for Remote Support.



3. Enable Remote Support by selecting **Yes** or disable Remote Support by selecting **No** and click **Save.**



Once enabled, Remote Support will display as **Enabled | Connected**.



To enable Remote Support via the QQ CLI:

Run the following command from a node:

```
qq set_monitoring_conf --vpn-enabled
```

Run the command below to disable Remote Support:

```
qq set_monitoring_conf --vpn-disabled
```

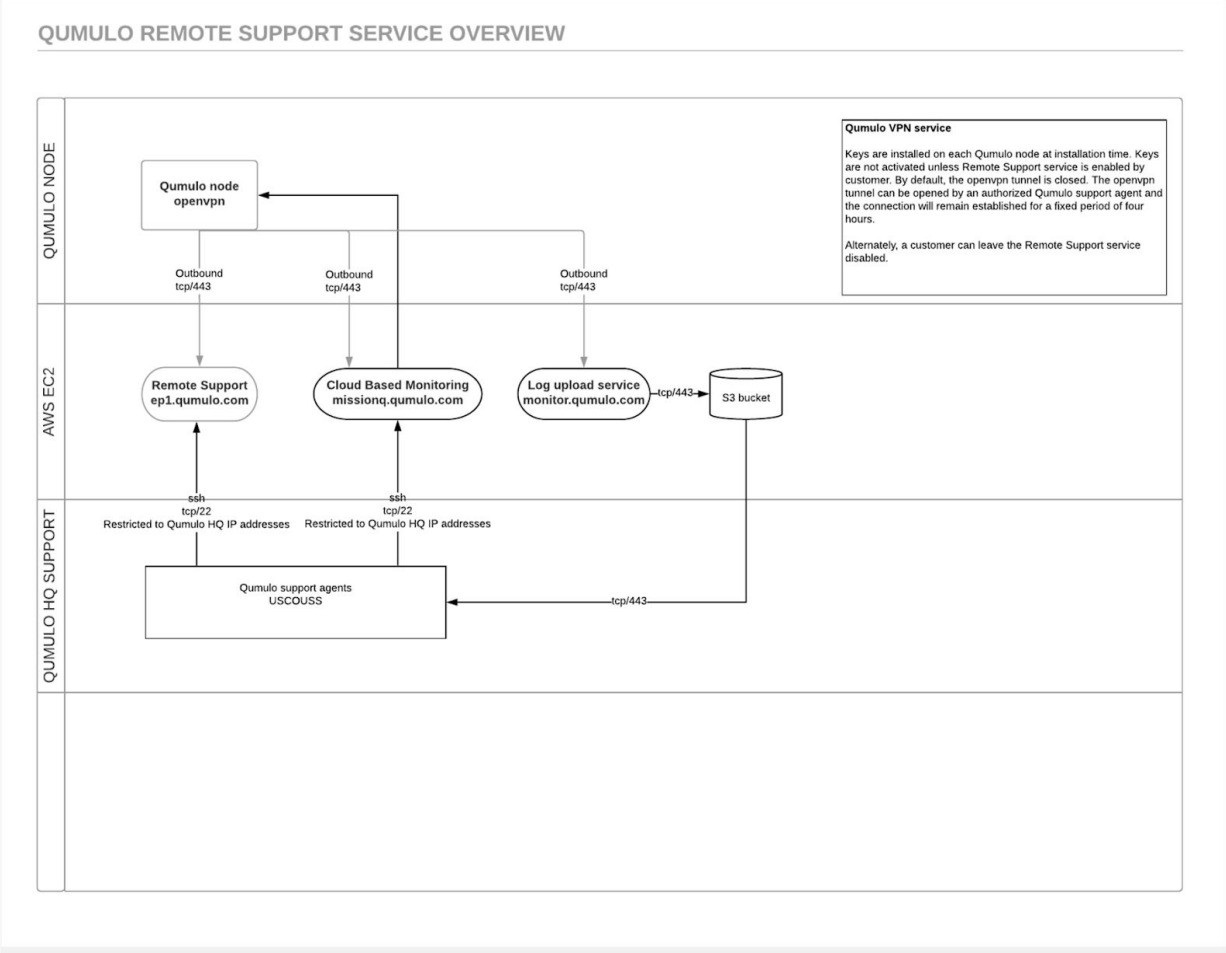
Lastly, verify the cluster's support configuration by using the following command:

```
qq monitoring_conf
```

Remote Support Process

1. The customer initiates a VPN connection by enabling the Remote Support option in the UI on the Qumulo Care page.
2. The customer notifies the Qumulo Customer Success team that Remote Support is enabled.

3. A Qumulo Support Engineer will activate an openvpn connection, creating a tunnel from the customer's Qumulo cluster to *ep1.qumulo.com* server.
4. The Support Engineer will initiate ssh from Qumulo HQ to the *ep1.qumulo.com* server.
5. The Support Engineer will initiate ssh via the established openvpn tunnel from *ep1.qumulo.com* to customer cluster.
6. Qumulo will now have access to troubleshoot and upload logs first to *monitor.qumulo.com*, then to S3 bucket.
    - Log uploads, while not shown in the UI, can be initiated manually by a member of the Customer Success team. Logs and other pertinent diagnostic data are sent to a private Amazon EC2 instance for analysis by our support team.
7. Once completed, Qumulo will notify the customer to deactivate Remote Support.
8. The customer disables Remote Support via Web UI, CLI or API.



We highly recommend that you enable Cloud-Based Monitoring with Remote Support so that our team can proactively provide fast support when you need it the most.

9. Default File Permissions

9.1 NFS

- The default permissions for the NFS root directory are **rwxrwxrwx (0777)**
- The NFS root directory is owned by root (UID 0) and group “nfsnobody”
- All users will be able to create files and directories in the current directory.
- All users will be able to delete files and directories in the current directory, including those owned by root.
- Users other than root will not be able to chmod or chown files and directories not owned by their UID. (This assumes that root is not being mapped to another user in the Qumulo NFS share settings)
- Files and Directories will have POSIX mode bits set according to the user’s system umask settings - Refer to your system’s documentation on how to modify your file system’s creation umask.

9.2 SMB (NTFS)

Qumulo* denotes the local Domain name (Cluster Name) of your Qumulo cluster and **Admin** refers to the built-in Qumulo Admin account, not the Active Directory Domain Admin or Machine-local Admin account.

A newly-created Qumulo Cluster uses the following directory path:
\\yournewqumulo.yourcompany.com\Files

These are the permissions of the root directory of a newly-created Qumulo Cluster. One User Account and two groups are given rights to the root share by default:

- **Qumulo\admin (User)**: All ACEs except Full Control and Delete for “This folder only”
- **Qumulo\users (Group)**: “Modify” ACL for “This folder only”
- **Everyone (Group)**: “Modify” ACL for “This folder only”

9.3 SMB Root Share

SMB user logged in as Qumulo\admin:

- User will be able to create files and directories in the current and all future directories.
- User will be able to read all files and file attributes and list all directories in the current and all future directories.
- User will be able to delete or rename all files and directories in the current and all future directories
- User will be able to change ownership and permissions for all files and directories in the current and all future directories.

SMB user logged in as a non-admin member for the Qumulo\users group:

- This is the default group that all non-Guest accounts belong to at time of account creation.
- User will be able to read all files and file attributes and list all directories in the root directory and any future directories created by other members of the Qumulo\users group in the root directory.
- User will be able to rename, delete and modify permissions on any files or directories created by this user in the current directory and in any subsequent sub-directories created in this directory.
- User will be able to create or append new files and directories in the root directory and in any subsequently created sub-directories. The new files and directories created will be owned by this user and will receive the following permissions:
    - **File/Folder Creator** - “Modify” ACL
    - **Everyone (Group**) - “Read” ACL
    - **Qumulo\Users (Group)** - “Read” ACL

9.4 Default “Modify” ACL

- Traverse folder / execute file
- List folder / read data
- Read attributes
- Read extended attributes
- Read permissions
- Create files / write data
- Create folders / append data
- Write attributes
- Write extended attributes
- Delete subfolders and files

9.5 Default “Read” ACL

- Traverse folder / execute file
- List folder / read data
- Read attributes
- Read extended attributes
- Read permissions

NOTE: This means that the files and directories inside the Qumulo root share cannot be modified by anyone other than Qumulo admin users and users that are implicitly granted permission to do so. This includes all other non-admin members of the Qumulo\users group.

9.6 SMB User Logged in as Guest

Guest access has to be enabled in the **Sharing > SMB Shares** panel by clicking on the pencil Edit icon next to the share name in the SMB Shares list.

- The Guest account belongs to the “Guests” Qumulo user group and is not a member of the Qumulo\users group
- The Guest account falls under the “Everyone” NTFS permissions group of the Qumulo root share

Guest will be able to create files and directories in the Qumulo share root directory as inherited by the root directories Everyone permissions ACL.

Files created by Guest will have the owner Qumulo\guest and receive the following permissions:

- **Guest** - “Modify” ACL
- **Everyone (Group)** - “Read” ACL
- **Qumulo\Guests (Group)** - “Read” ACL

Non-Qumulo admin members of other user groups will be able to read files and list directories created by Guest but will not be able to write to, append or modify those files or directories. Guest will be able modify permissions and change ownership of files and directories created by this account.

---

10. Create an NFS Export

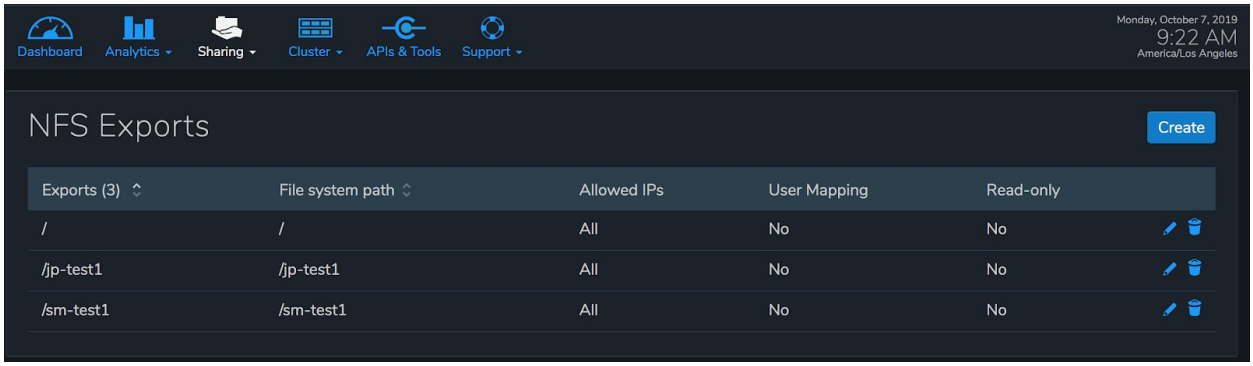
10.1 NFS Export Page Overview

In the Web UI, hover over **Sharing** and click **NFS Exports** from the dropdown. A list of NFS Exports displays the following details:

- **Exports:** Name of the NFS Export
- **File system path:** The directory path of the NFS Export
- **Allowed IPs:** Details whether all or some of the IPs are allowed access
- **User Mapping:** Displays whether User Mapping is enabled
- **Read-only:** Displays whether Read-only access is configured

10.2 Create an NFS Export

1. Click **Create** on the NFS Exports page.



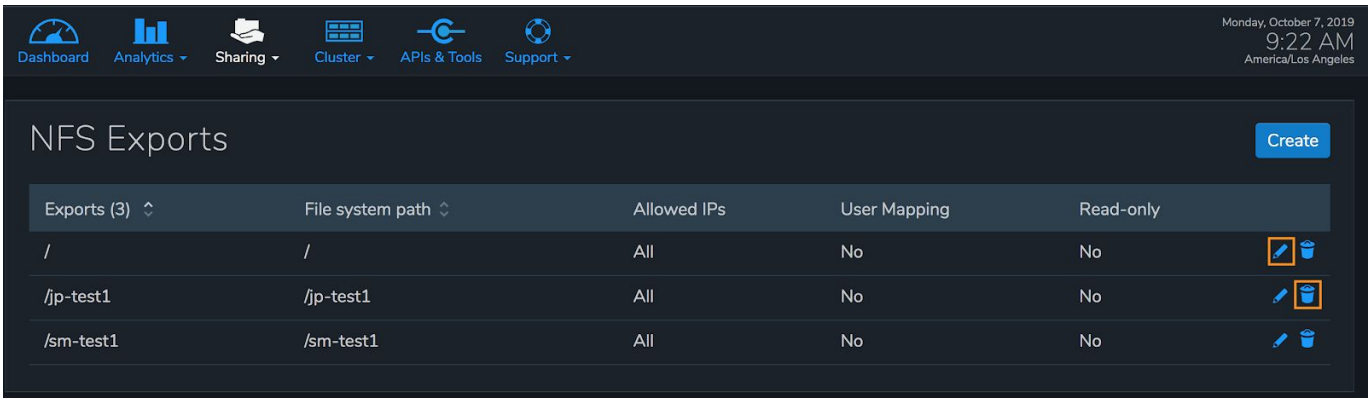
2. Fill in the following fields:

    - **File system path:** The directory path of the NFS Export.
    - **Create new directory with inherited permissions:** Creates a new directory if the file system path does not exist.
    - **Export path:** The NFS Export name that the client will mount to.
    - **Description:** A description of the export (optional).
    - **User Mapping:** Forces user IDs to be mapped to a specific ID. Note that the No Mapping option is selected by default.
    - **Allowed IPs:** A list of IP addresses that the export can be restricted to. Note that all IPs are allowed by default if the allowed IP field is left blank.
    - **Read-only:** Enables the Export to have read-only access.

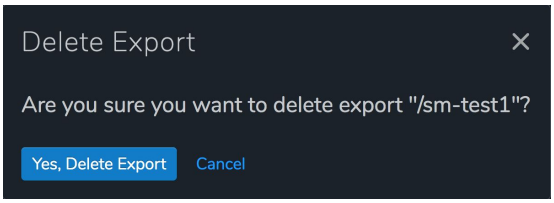
3. Click **Save** to create the new export and add it to the NFS Exports page.

10.3 Edit or Delete an NFS Export

- To **Edit** an existing NFS Export, click the pencil icon next to the listing on the NFS Exports page
- **Delete an NFS Export** by clicking the trashcan icon



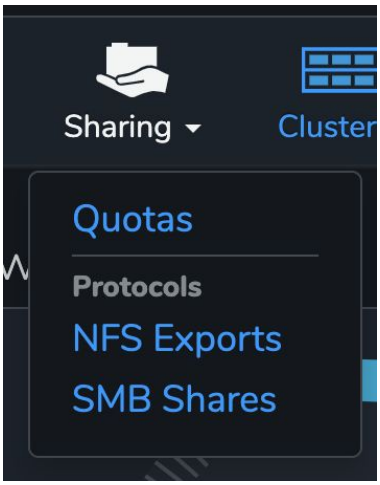
- Confirm the delete of an NFS export by selecting **Yes, Delete Export** when prompted or click Cancel



11. Create an SMB Share

11.1 SMB Share Page Overview

In the Web UI, hover over **Sharing** and click **SMB Shares** from the dropdown.



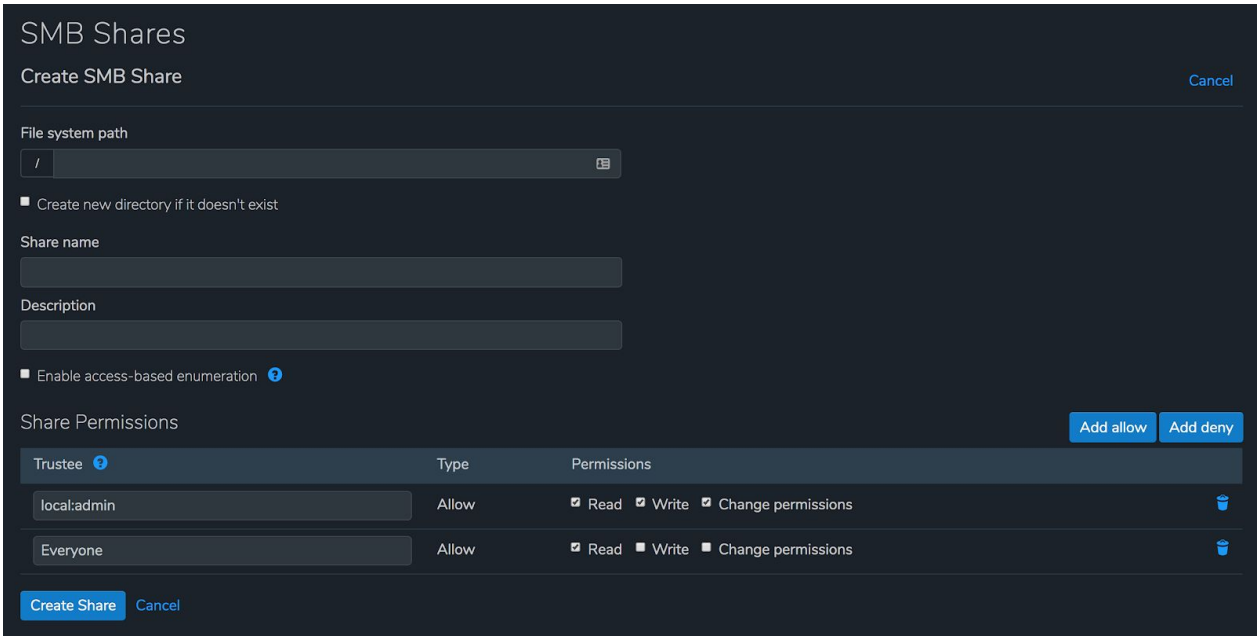
A list of SMB shares displays, including the name of each SMB share and corresponding file system path.

11.2 Create an SMB Share

1. Click **Create Share** on the SMB Shares page.

2. Fill in the following fields:
    - **File system path:** The directory path to the share from the root of the Qumulo file system. Check Create new directory if it doesn't exist to create it.
    - **Share name:** The SMB Share name the client will mount to.
        - Include "$" at the end of the name to hide the share from root.
    - **Description:** A brief description of the share (optional).
    - **Enable access-based enumeration:** Displays only the files and folders that a user has permissions to access. If a user does not have Read or equivalent permissions for a folder, the folder is hidden from the user's view.

- **Add allow/deny:** Click the option for the share permissions entry type you wish to create (allow or deny).
- **Trustee:** The trustee for the share permissions entry. This can be as simple as Everyone or a specific domain user. Click the '?' icon for examples.
- **Permissions:** Specify the explicit access permissions for each entry in the share permissions.



3. Click **Create Share** to create the new share and add it to the SMB Shares page.

NOTE: When you add a Deny entry, it is added to the top of the listing, while Allow entries are added to the bottom. This ensures that users who are explicitly denied access are processed prior to granting access to any.

11.3 Edit an SMB Share

1. From the SMB Shares page, click the Edit ( ) button next to the share you wish to change on the SMB Shares page.
2. Make the desired changes and click **Save** to finish.

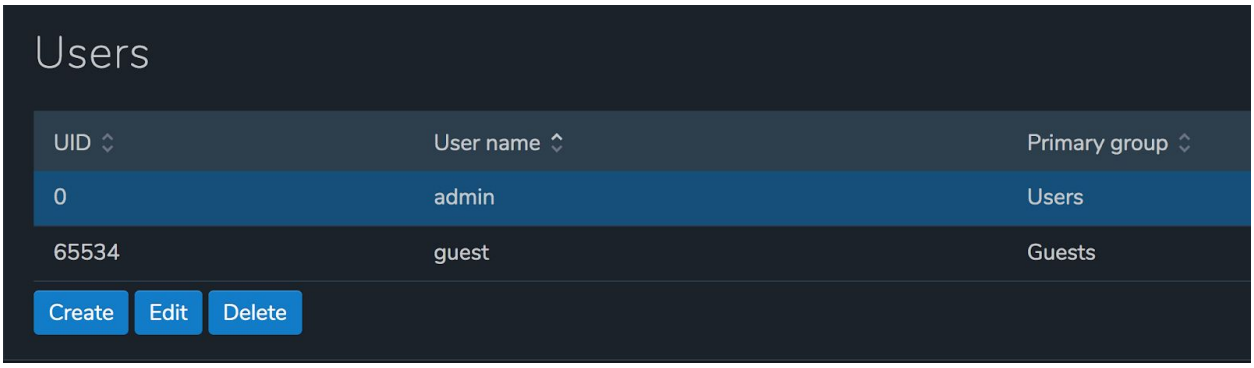
11.4 Remove an SMB Share

1. On the SMB Shares page, click the Delete ( ) button next to the share you wish to remove.
2. Confirm the removal of the share by selecting **Yes, Delete Share** when prompted or click Cancel to keep the share.

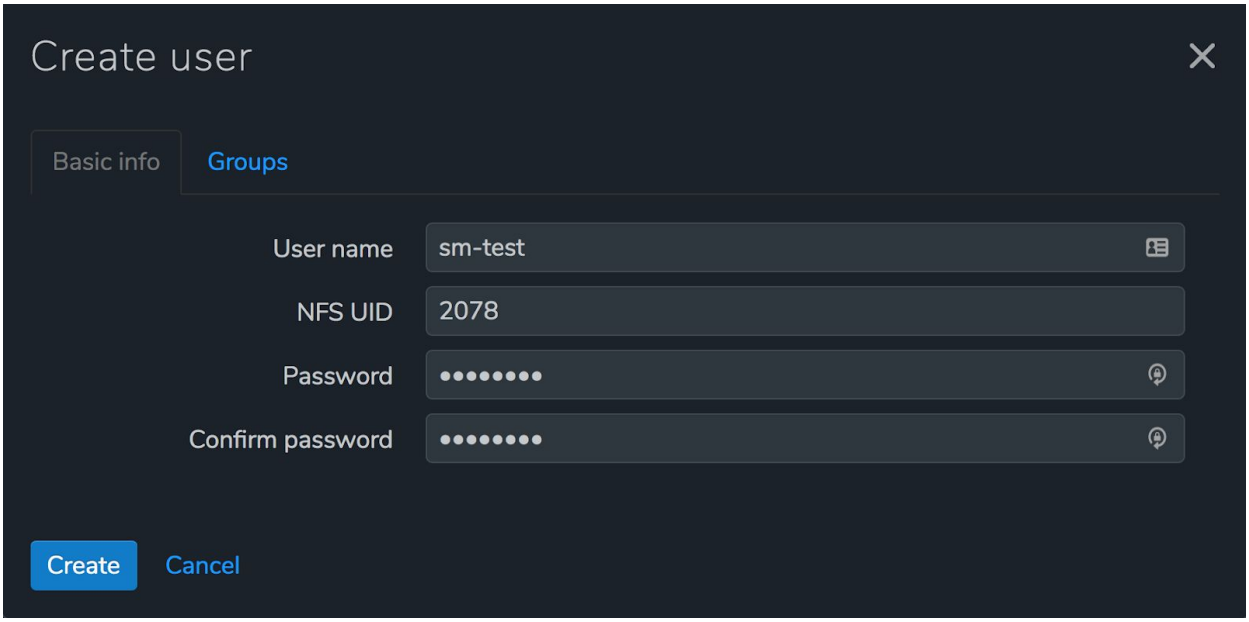
12. Create Users & Groups

12.1 Create a new User

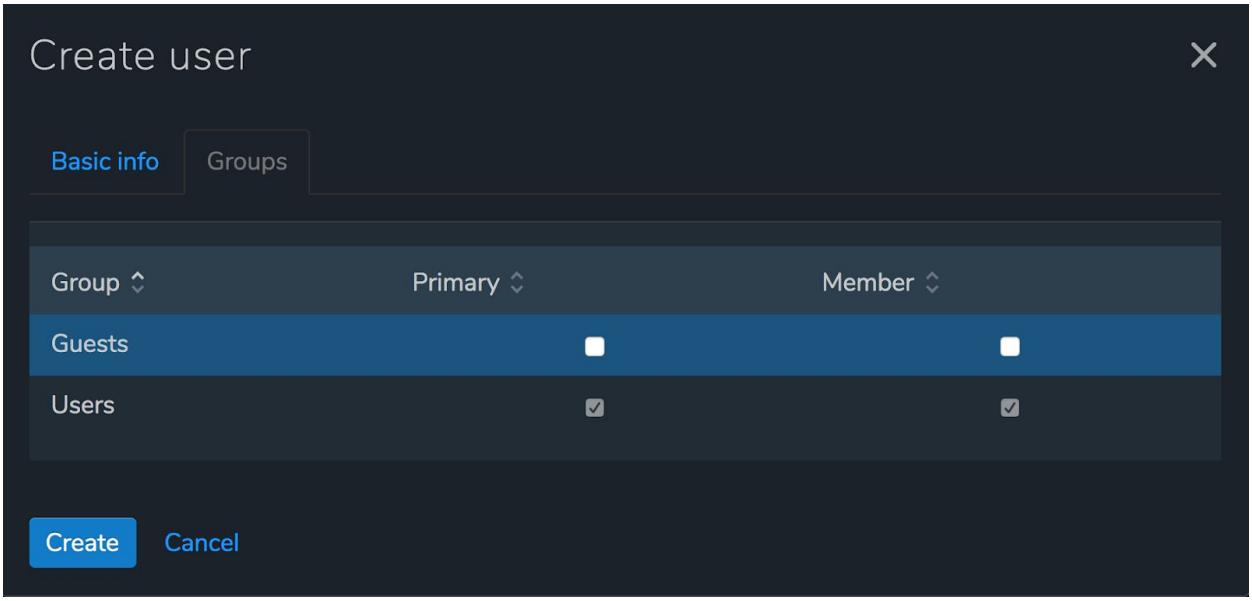
1. In the Qumulo Core Web UI, hover over **Cluster** and click **Local Users & Groups.**
2. Click **Create** under the **Users List** to create a new User.



3. Enter the desired username and password.



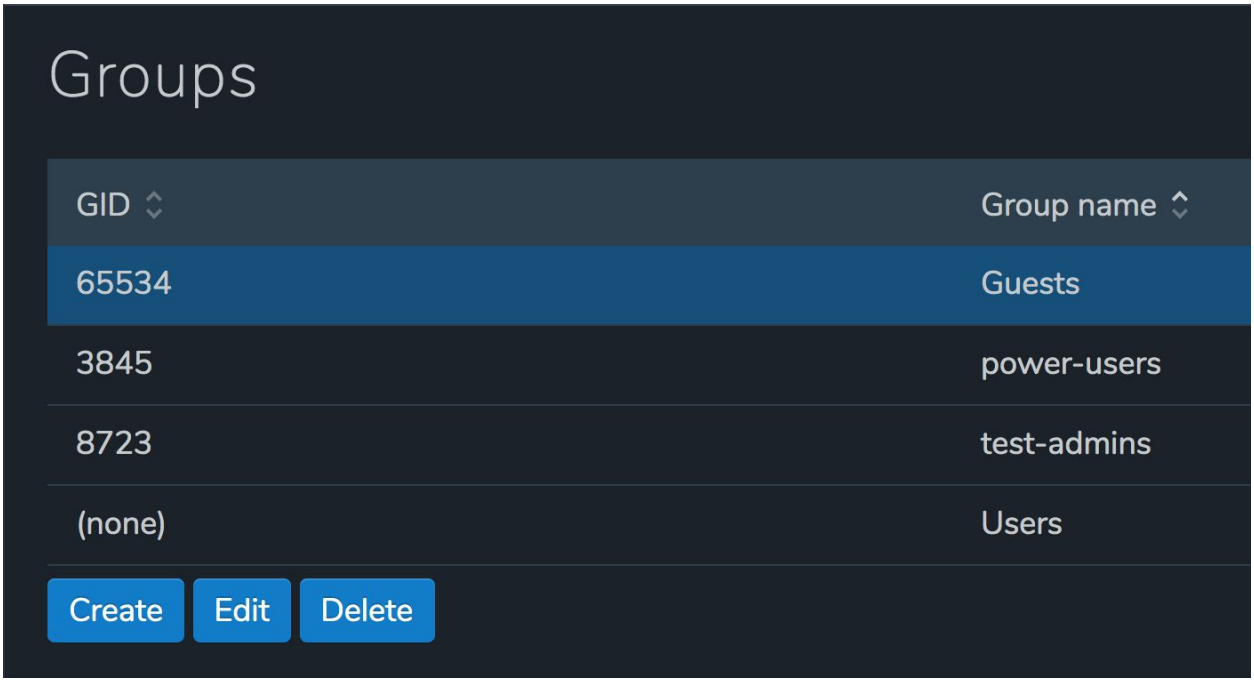
- If you have both SMB and NFS users, input an NFS UID that matches the user's POSIX UID on their client machine.
- Optionally, click the Groups tab and select the user's primary group, and any other groups they should belong to. Note that while a user can be a member of multiple groups, there can only be one primary group per user.



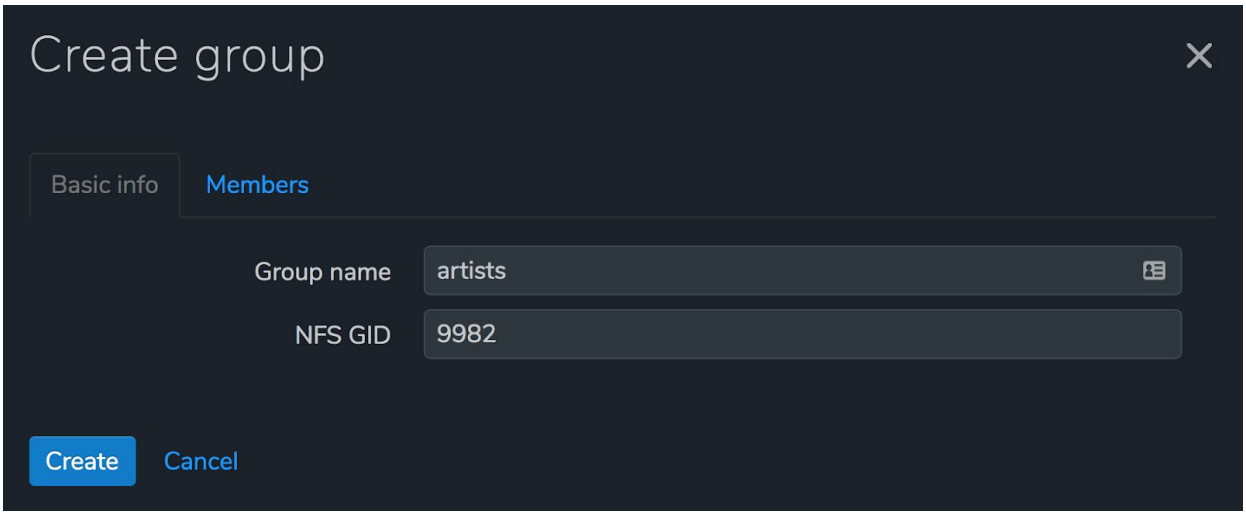
4. Click the **Create** button when finished.

12.2 Create a new Group

1. On the Users and Groups page, click the **Create** button under the Groups list.



2. Enter the desired group name:
    - If you will have both SMB and NFS users, input an NFS GID that matches a corresponding POSIX GID used on your client machines.
    - Optionally, click the Members tab and add any members you wish to be a part of the new group.



3. Click the **Create** button when finished.

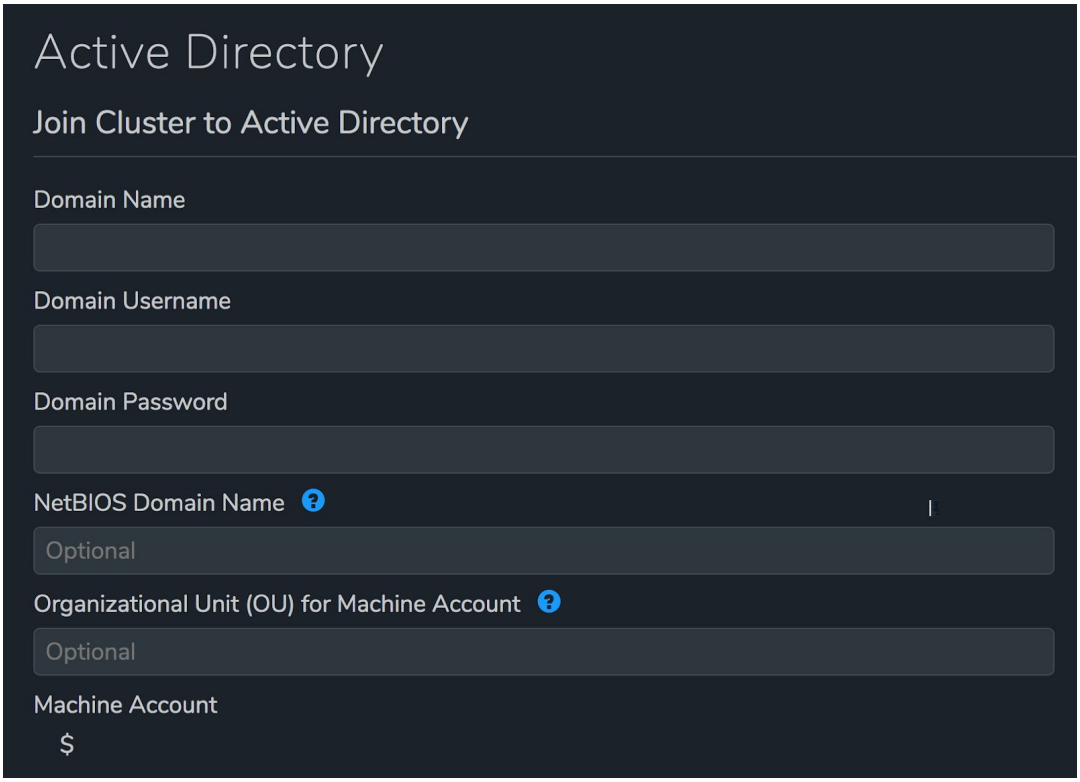
You will now be able to connect to an SMB share or mount an NFS export as a Qumulo user. Keep in mind that for NFS users, the UID/GIDs of users in their Linux/Unix/Mac environment need to match the UID/GIDs used when creating users above.

---

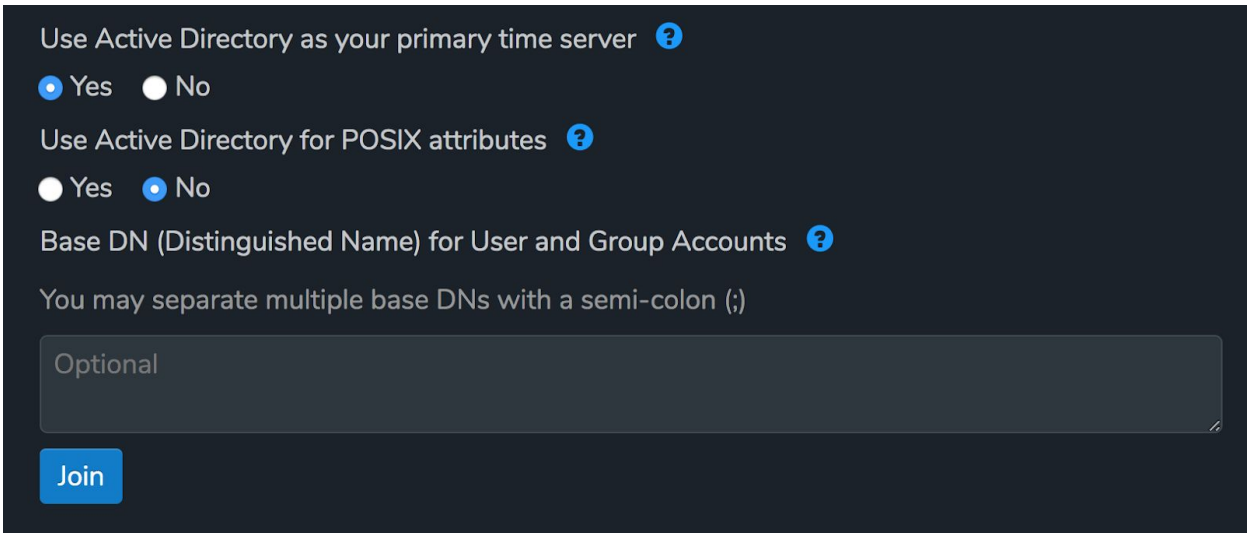
13. Join your cluster to Active Directory

Before beginning, make sure you have the details for your Active Directory domain including **Domain name**, **Domain username**, and **Domain password**. Keep in mind that Qumulo Core only supports joining a cluster to one Active Directory Domain.

1. In the Web UI, hover over the **Cluster** menu and click **Active Directory** under Authentication and Authorization.
2. Fill in the following mandatory fields:
    - **Domain Name**: name of your domain. Example: *ad.example.com*
    - **Domain Username**: the user account or service account you will use to authenticate against the domain
    - **Domain Password**: the password for the user account or service account
3. Fill in the following two optional fields:
    - **NetBIOS name**: This is the first portion of the fully-qualified domain name. If your Qumulo cluster name is Qumulo and you are joined to the *ad.example.com* domain, then your NetBIOS name will be Qumulo.
    - **Organizational Unit (OU)**: If known, this information can be entered and can normally be obtained from your Systems Administrator. If unknown, leave it blank and Qumulo will attempt to join the domain without an OU specified.



4. Click the **Yes** button to use your AD as your primary time server.
5. Select the option to use Active Directory for POSIX attributes.
    - Use in environments where 'user objects' in Active Directory are assigned UNIX UID and GID attributes to allow the cluster to properly enforce permissions regardless of the protocol used to access the data.
    - For additional details, see the article Using Active Directory for POSIX attributes in the Permissions section on Qumulo Care.



6. Optionally, enter your Base DN for User and Group Accounts in the text field.
7. Click **Join.**

NOTE: DNS entries will be automatically created from the node used to add the cluster to Active Directory and can be removed without issue.

14. REST API

Qumulo's scale-out data storage solution is enhanced with our RESTful API built right into the file system. It's the foundation used behind the Qumulo web application and is used internally by our engineering team for testing, automation, and more. As a storage admin or storage user, you can:

- Automate tasks like creating shares, quotas, or snapshots
- Streamline your workflow with scripted automation
- Dive deeper into analytics to understand how your storage is being used

In the Qumulo Core UI, you'll find an **API and Tools** menu that provides direct, navigable "live" documentation where you can read about the different APIs and experiment by trying things out directly in one place.

14.1 Authentication

Qumulo API endpoints can be divided into three categories:

- APIs that don't require any authentication like */v1/version*
- A login API at */v1/session/login* which takes a username and password
- APIs that take a bearer token returned from the */v1/session/login* API

When using Qumulo's API, you need to start an authentication session by logging in. Calling the login API gives you a temporary credential called a bearer token, which is sent along with subsequent API calls as proof that you have been authenticated.

NOTE: Non-admin users can login but may not have access to certain endpoints.

ACQUIRE A BEARER TOKEN
You start an authentication session by calling the */v1/session/login* API with a valid username and password as outlined in the example below using curl.

```
curl -k -X POST https://clusterIPorDNSname:8000/v1/session/login -H "Content-Type:
application/json" -d '{"username":"user", "password":"SECRET"}'
```

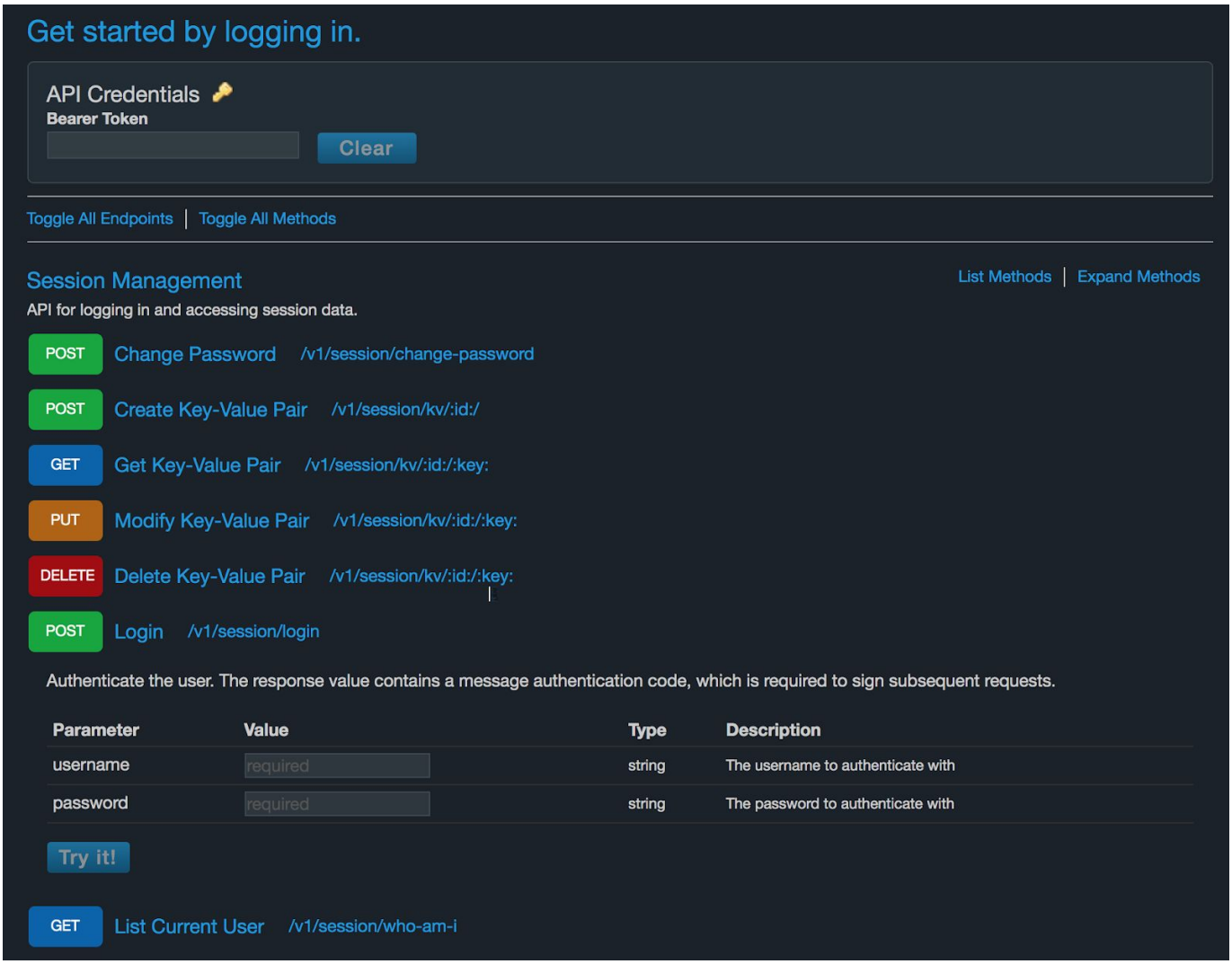
Output:

```
{ "bearer_token": "1:ATwAAABlSnp6MVZvUXhRQUViN2RCYUFVZy9zTElBQWFNVEZBYWljME94R3hBSEp
PWWtwdVpad2RrQVFBNEtnZmIgAAAAXU/JXGz/syigeb+FQ5zEzmNtk8L8GtaQ0M3UejImW4k=" }
```

Bearer tokens can also be obtained from using the interactive API available in Qumulo Core.

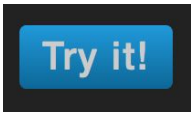
1. In the Web UI, click on **API & Tools.**

2. Select **Get started by logging in** beneath the page introduction to expand the Login section under Session Management.

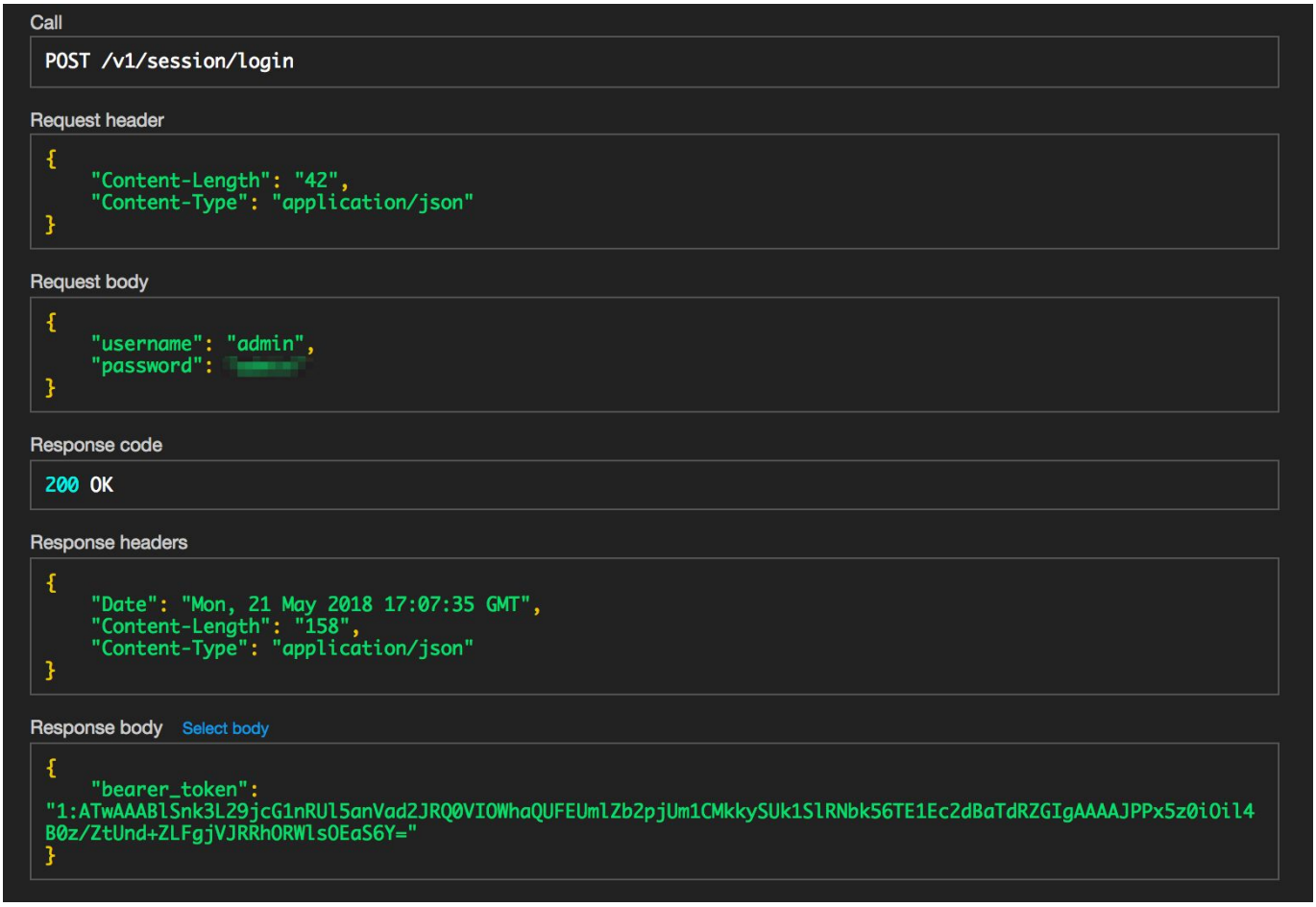


3. Type in **admin** for the username value and the assigned password.

4. Click **Try it!**



5. Confirm successful authentication with a 200 OK response code.



6. Copy the **"bearer_token"** value from the response body.
7. To ensure another user cannot use your login credentials, click the **Clear** button in the API Credentials box or reload the page.

IMPORTANT! The bearer token is valid for 10 hours and can be used to make API requests. To continue using the API after 10 hours, you must re-authenticate with your username and password to start a new authentication session.

USE THE BEARER TOKEN

Now that you have a bearer token, calls to API endpoints that require authentication can be requested using the token in the request header. Reference the example below to see how a bearer token is used to list the nodes in a single node cluster.

```
curl -k GET https://clusterIPorDNSname:8000/v1/cluster/nodes/ -H
"Authorization: Bearer 1:ATwAAABlSnp6MVZvUXhRQUViN2RCYUFVZy9z
TElBQWFNVEZBYWljME94R3hBSEpPWWtwdVpad2RrQVFBNEtnZmIgAAAAXU/JXGz/syigeb+FQ5zEzmNtk8L8GtaQ0M3UejIm
W4k="
```

Output:

```
{"id": 1, "node_status": "online", "node_name": "music-1",
"uuid": "becee591-23bc-4fec-91de-e4c78fab642e", "label": "f4:52:14:2b:40:30",
"model_number": "Q0626", "capacity_in_bytes": "25605032656896",
"serial_number": "XXX", "mac_address": "XX:XX:XX"}
```

TIP! In a UNIX shell like bash, assign the bearer token to a variable so that authentication does not require the full token value from the original login request. See the example below where our bearer token is assigned to the q_prod variable.

```
$ q_prod="1:ATwAAABlSnp6MVZvUXhRQUViN2RCYUFVZy9z
TElBQWFNVEZBYWljME94R3hBSEpPWWtwdVpad2RrQVFBNEtnZmIgAAAAXU/JXGz/syigeb+FQ5zEzmNtk8L8GtaQ0M3UejIm
W4k="
```

```
curl -k GET https://clusterIPorDNSname:8000/v1/cluster/nodes/ -H
"Authorization: Bearer $q_prod"
```

14.2 Conflict Detection

Many of our configuration endpoints have straightforward behavior. You can use GET to retrieve a document (e.g. GET */v1/users/123*) and use PATCH to update the document. The requests take effect immediately so that when you receive a 200 OK response, you know the change has been made. But REST is not transactional when it comes to making changes, which can impact the user experience if not considered properly. With our conflict detection scheme, clients are able to query resources to find out if they've changed since the last access time. Resources have a unique tag describing their current value, which is represented in HTTP 1.1 by an entity tag (ETag).

The API leverages the HTTP ETag mechanism to handle concurrent resource modifications. We return an ETag containing a version string for each versioned resource. If conflict detection is desired, the caller should provide an If-Match header containing the ETag associated with the expected resource version.

The flow for modifying a resource is as follows:

- Client requests the current representation of a resource with a GET request. Response includes an ETag header.
- Client sends an update for that resource with a PATCH, PUT or DELETE request. The request includes an If-Match header with the previously received ETag value.
- If the resource's current ETag is the same as the If-Match value, the request succeeds with a 2xx response. Otherwise, the request fails with a 412 Precondition Failed response.
- Upon receiving a 412, the client can GET the resource again and automatically retry the operation, or inform the user of the underlying change and confirm that they want to proceed.

Let's say an administrator is editing a file share on the cluster using the Interactive API in API & Tools. Between the time the UI retrieves the file share details and when the administrator saves their changes, another user or process could change that file share. By default in our API, the last writer wins so the administrator would unwittingly clobber these changes. That's not the user experience we want, so we use ETag and If-Match HTTP headers for all of our documents to prevent accidental overwrites.

When the UI retrieves a document, it reads the ETag response header (entity tag or essentially a hashcode) and stores that. Later, when updating that same document, the UI sends an If-Match request header which tells the cluster to only perform the action if the document is the same as we expect. If the document changed, we'll get back a 412 Precondition Failed response which allows us to build a better experience for the user.

14.3 GitHub

Qumulo culture values openness and transparency, with an emphasis on sharing. We want to extend this culture to customers that use the Qumulo REST APIs by sharing samples using our APIs via GitHub. Our goals in sharing samples on GitHub include:

- Make it easy for our customers new to the Qumulo REST API to understand how it works
- Provide a good, representative cross-section of samples for common tasks including disk utilities, creating shares and storage statistics
- Provide reference implementations for common customer sample requests such as monitoring agents and working with time series data from our clusters
- Provide a central clearinghouse for customers who want to share their own Qumulo REST API samples with others
- Provide guidance to customers to help ensure code quality through good coding standards and tests

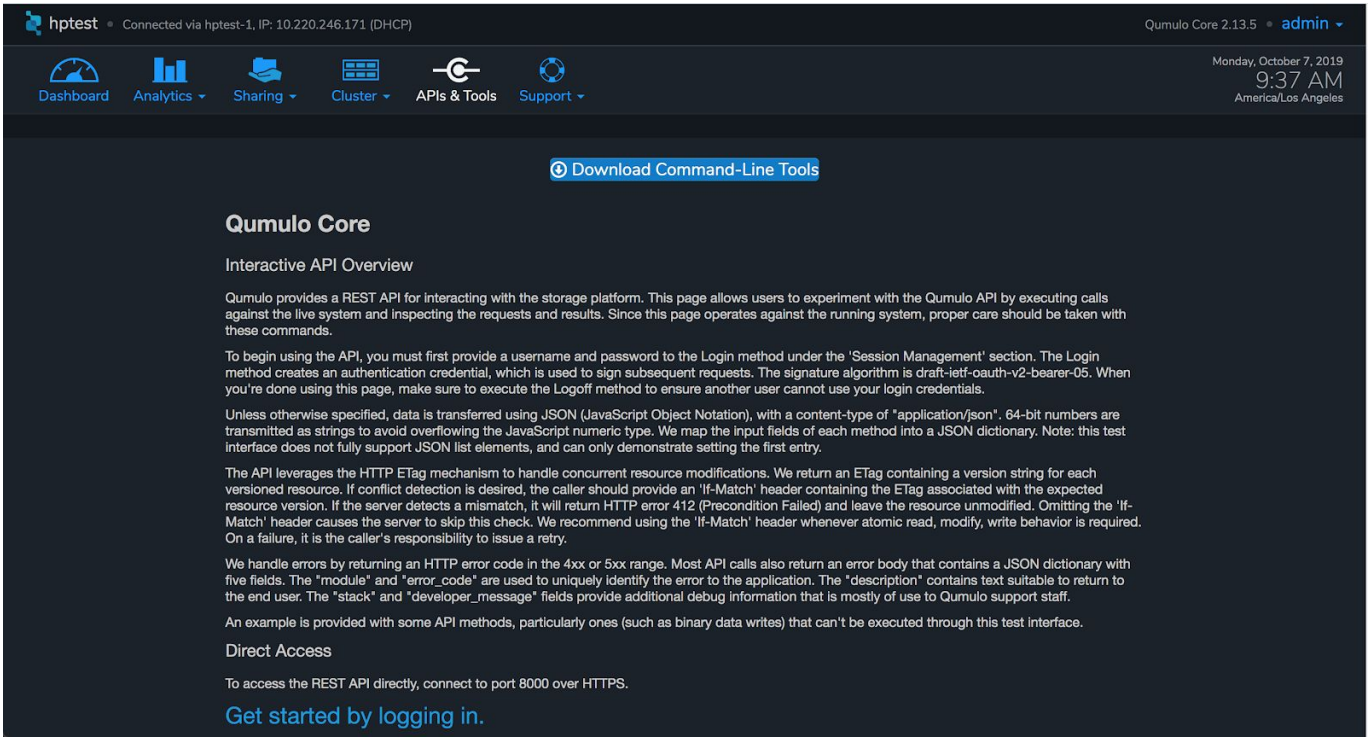
Check out our Github page by heading on over to https://github.com/Qumulo to see our REST API samples.

14.4 QQ Command-Line Tools

The Qumulo-provided qq command line (CLI) tool is the way to harness the power of Qumulo's REST API from the CLI and in shell scripts. The entirety of Qumulo's REST API is exposed via qq and can be run on a remote machine or directly on a node.

Install Command Line Tools on a Remote Machine

1. In the Qumulo Core Web UI, select **API & Tools.**
2. Click the **Download Command-Line Tools** button.



3. Copy the qumulo_api directory to your home directory to ensure that only you are able to run the qq command on the computer where you are installing. If others need access, copy the qumulo_api directory to one of the following:
    - Apple and Linux computers - copy to /opt/
    - Windows - copy to C:\Program Files (x86)\

Windows

On Windows, the qq file must be run with the python.exe 2.7 interpreter:

```
$ python.exe /Users/qumulo_user/qq
```

NOTE: You can also install the Qumulo API tools via the Python SDK by running the command below. The qq file (qq.exe for Qumulo Core 3.1.4 and higher) is installed in the Scripts directory next to your Python installation (e.g., C:\Python27\Scripts). Add that directory to your PATH to allow qq.exe to be executed from anywhere.

```
$ pip install qumulo_api
```

Mac/Linux
On Mac and Linux, the qq file can be run with the python 2.7 interpreter:

```
$ python ~/qq
```

Alternatively, you can configure the file's executable bit and run it directly:

```
$ chmod +x ~/qq
$ ~/qq
```

Use Command Line Tools
To use the qq CLI from one your nodes, simply ssh to the node and run as root. Note that you can run as admin, but you will need to authenticate via the login command.

Once you've accessed a node via ssh, you can see the full list of qq commands by heading on over to the QQ CLI section of Qumulo Care or by running the following command:

```
qq -h
```

---

15. Qumulo Core Upgrades

Qumulo offers simple and fast upgrades that customers rely on to stay up to date with Qumulo's continuous delivery of new features and enhancements. With this model, we aim to quickly adapt to your needs so that improvements and changes can be made in weeks instead of years. Our upgrade process is incredibly simple and only takes a few clicks. Depending on the protocol used, upgrades will not stop applications from running and will complete in under five minutes.

15.1 Qumulo Core Upgrades

With the release of Qumulo Core 2.13.0, all subsequent releases will be a quarterly upgrade source so that you can easily upgrade directly from any incremental version to a later (2.13.X) release, up to and including the next quarterly X.X.0 build. No matter what version past 2.13.0 your cluster is running, you will need to install every quarterly release before proceeding to upgrade to a later version of Qumulo Core.

To help demonstrate what is and is not supported for upgrades with Qumulo Core 2.13.0 and above, we've provided some specific examples below:

- **You CAN upgrade from 2.13.3 to 2.14.0 –** this path is supported since all versions of Qumulo Core now act as a quarterly release source.
- **You CAN upgrade from 2.13.1 to 2.13.5** – this path is supported since you can now skip versions within as long as the jump does not include a quarterly release.
- **You CANNOT upgrade from 2.13.5 to 2.14.1** – this path is not supported since you cannot skip a quarterly release (X.X.0). You need to install 2.14.0 before you can upgrade to the 2.14.1 release.
- **You CANNOT upgrade from 2.12.4 to 2.13.0** – this path is not supported since the new relaxed upgrade restrictions are only available starting with the 2.13.0 version of Qumulo Core. You need to install 2.12.5 and 2.12.6 before upgrading to the 2.13.0 release.

Recommended upgrade paths when moving from a past version of Qumulo Core to a recent release are outlined below:

Upgrade Path from 2.13.0 to 3.0.4

2.13.0 -> 2.14.0 -> 3.0.0 -> 3.0.4

Upgrade Path from 2.12.1 to 3.0.4

2.12.1 -> 2.12.2 -> 2.12.3 -> 2.12.4 -> 2.12.5 -> 2.12.6 -> 2.13.0 -> 2.14.0 -> 3.0.0 -> 3.0.4

Upgrade Path from 2.14.2 to 3.0.4

2.14.2 -> 3.0.0 -> 3.0.4

IMPORTANT! Back to back upgrades of Qumulo Core may require a wait period between specific releases to allow background processes to run. Before attempting to install multiple releases of Qumulo Core in an extended maintenance window, reach out to the Qumulo Care team for guidance on your upgrade path.

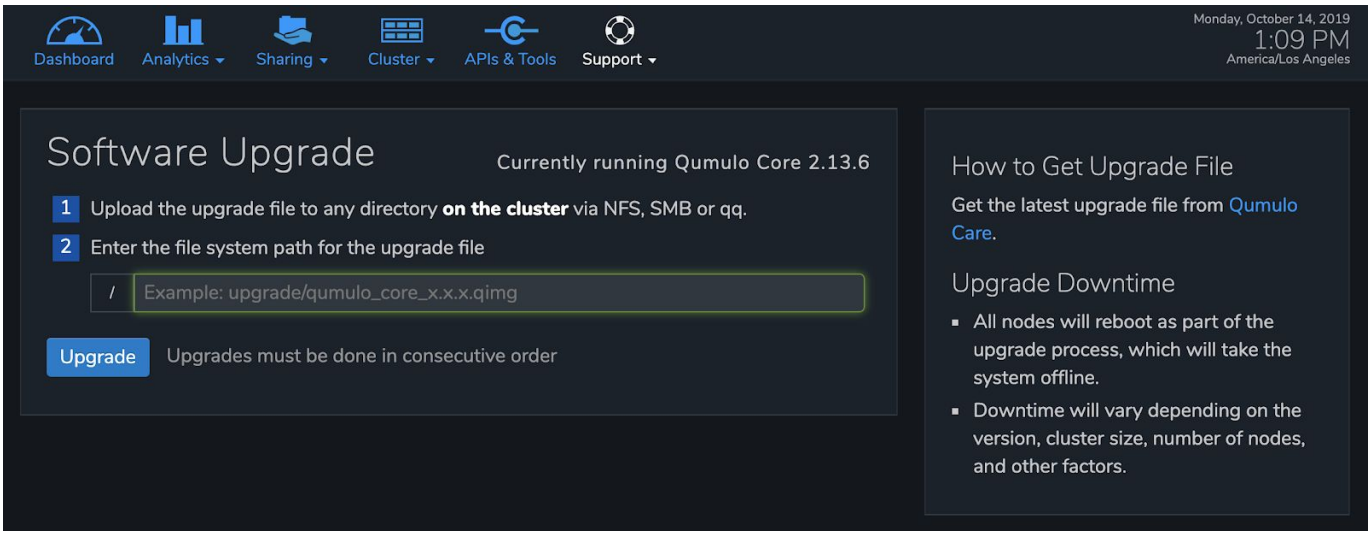
TIP! Click the **Follow** button on the Product Releases & Announcements section of the Qumulo Community to be notified when a new Qumulo Core version is released.

15.2 Upgrades via the UI

Before you install the latest version of Qumulo Core, ensure that your cluster is in a healthy state with no current hardware failures and that you have downloaded the latest upgrade image for your cloud or on-prem cluster.

1. Upload the upgrade file **qumulo_core_x.x.x.qimg** to any directory on the cluster via a client protocol like NFS or SMB.
    - Note that cloud clusters and on-prem clusters require different upgrade images. Verify the compatibility before installing.
2. Login to the Qumulo Core Web UI.
3. Hover over the **Support** menu and click **Software Upgrade.**
4. Enter the file system path for the upgrade file without the leading slash.

Example: If the share/export that contains the upgrade file is /upgrade/ your file system path should be **upgrade/qumulo_core_2.8.7.qimg**



5. Click the **Upgrade** button.

15.3 Upgrades via the CLI

1. Upload the upgrade file **qumulo_core_x.x.x.qimg** to any directory on the cluster via a client protocol like NFS or SMB.
2. Connect to a node via ssh using your IP address:

```
ssh admin@your_IP_address
```

3. Become root by running the following command:

```
sudo -s
```

4. Confirm that the upgrade status is “IDLE” using the command below:

```
qq upgrade_status
```

5. The output should reflect the following:

```
"details": "",
"install_path": "",
"state": "UPGRADE_IDLE"
```

6. Prepare the upgrade by running the following command using the path to the .qimg file you uploaded:

```
qq upgrade_config_set --path /qumulo_core_x.x.x.qimg --target prepare
```

7. Issue the following command to monitor the ‘prepare’ status:

```
qq upgrade_status --monitor
```

8. Proceed once you see the following output:

```
UPGRADE_PREPARED
```

9. Arm the upgrade to begin the installation using the command below:

```
qq upgrade_config_set --path /qumulo_core_x.x.x.qimg --target arm
```

10. Re-login after the upgrade completes and the Qumulo process is restarted.
11. Check that the upgrade was successful by running the following command and verifying the new version number:

```
qq version
```

16. Additional Resources

- Qumulo Care Knowledge Base
- Open a Case
- Product Release Announcements