Cisco Tetration (Secure Workload) M5 Cluster Hardware Deployment Guide

First Published: 2019-01-09

Last Modified: 2022-08-17

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
      800 553-NETS (6387)
Fax: 408 527-0883

Introduction

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE

CONTENTS

CHAPTER **1**

Overview

Overview

You can deploy the Tetration (Secure Workload) M5 cluster in either of the following ways:

- Large-form factor 39-rack unit (RU) platform (C1-Tetration single rack) for data centers with more than 5000 servers

Note You can deploy the large-form factor platform in either one or two racks depending on your requirements. See the following C1-Tetration single rack and dual rack figures for examples.

- Small-form factor 8-RU platform (C1-Tetration-M) for data centers with fewer than 5000 servers. See the C1-Tetration-M figure for the example.

The following figure shows the front and rear of the C1-Tetration single rack.

Figure 1: C1-Tetration Single Rack Front and Rear
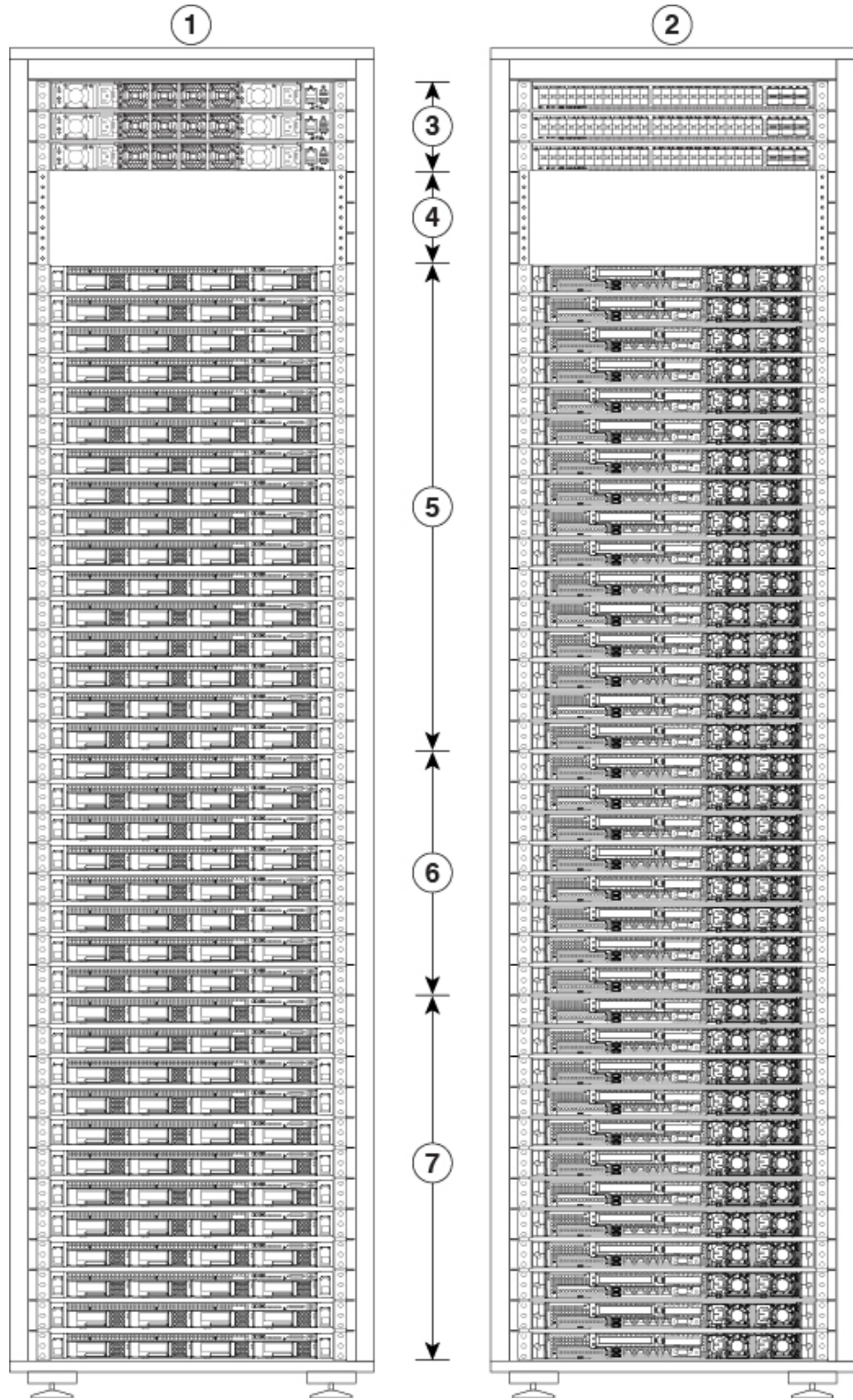
| **1** | Front (cold aisle view) | **2** | Rear (hot aisle view) |

3	One spine (RU 42) and two leaf switches: leaf 2 (RU 40) and leaf 1 (RU 41)	4	Open rack units (RU 37 to 39)
5	16 compute servers (RU 21 to 36)	6	Eight serving servers (RU 13 to 20)
7	12 base servers (RU 1 to 12)		—

The following figure shows the front and rear of rack one of the C1-Tetration dual rack.

Figure 2: C1-Tetration Dual Rack—Rack 1 Front and Rear
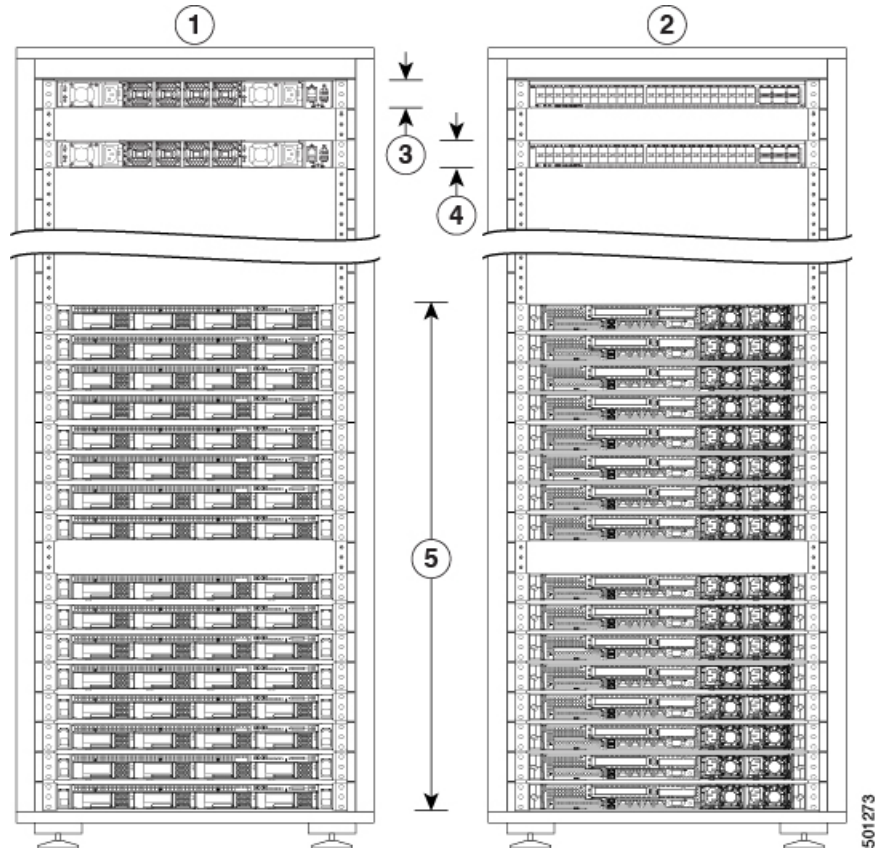
1	Front (cold aisle view)	2	Rear (hot aisle view)
3	One spine switch (RU 42)	4	Leaf 1 switch (RU 40)
5	16 compute servers (RU 1 to 4 and 6 to 9)	6	—

The following figure shows the front and rear of rack 2 of the C1-Tetration dual rack.

Figure 3: C1-Tetration Dual Rack— Rack 2 Front and Rear
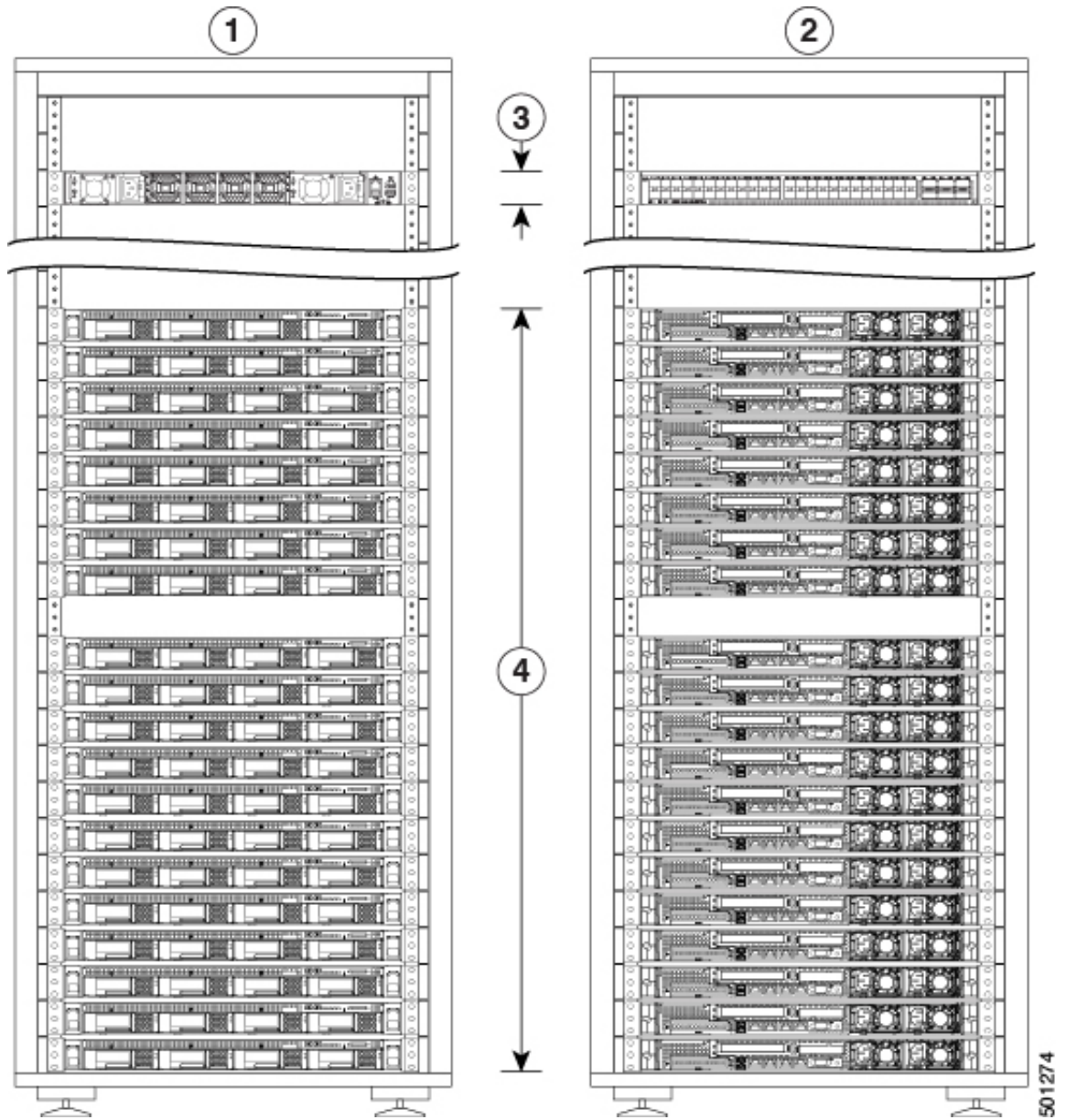
1	Front (cold aisle view)	**2**	Rear (hot aisle view)
3	Leaf 2 switch (RU 40)	**4**	Eight serving servers (RU 14 to 21) and 12 base servers (RU 1 to 12)

The following figure shows the front and rear of the C1-Tetration-M.

Figure 4: C1-Tetration-M Front and Rear
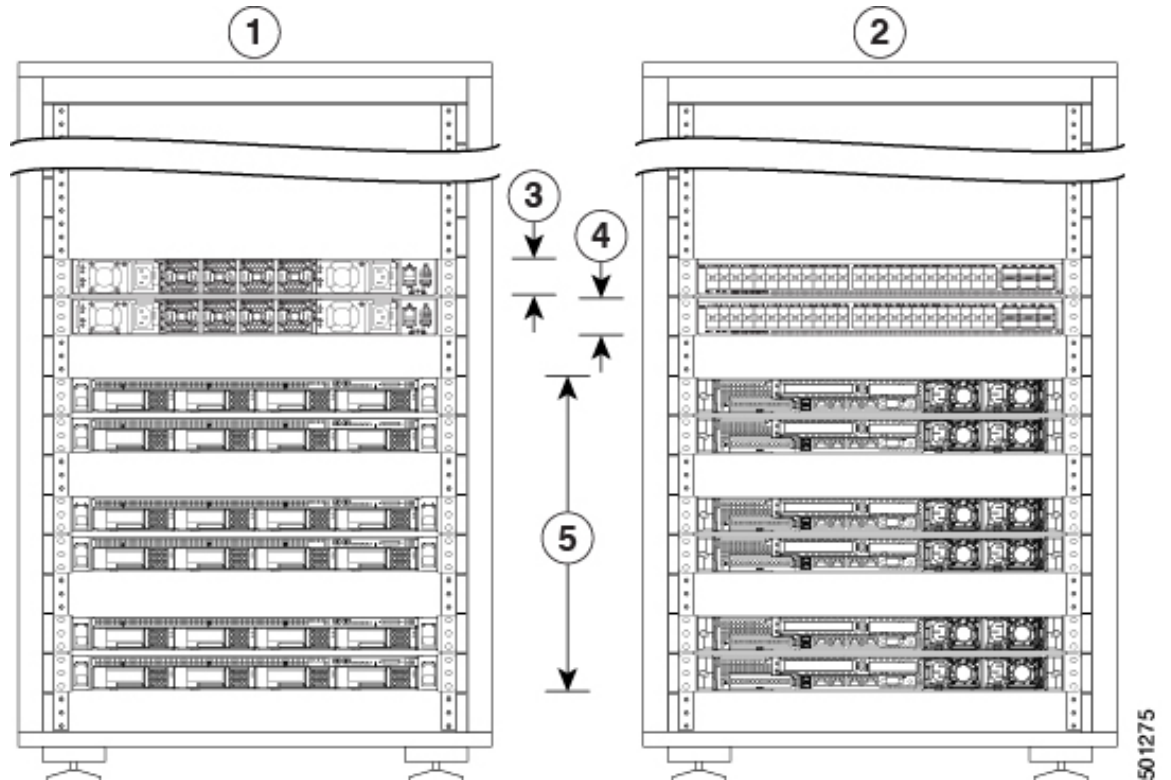
1	Front (cold aisle view)	**2**	Rear (hot aisle view)
3	Leaf 1 switch (RU 12)	**4**	Leaf 2 switch (RU 11)
5	Six universal servers (RU 2, 3, 5, 6, 8, and 9)		—

Cisco UCS C220 M5 Server (SFF Drives) Front Panel

The following figure shows the front panel of the UCS C220 M5 server with small form-factor (SFF) drives.

See Cisco UCS C220 M5 Server Installation and Service Guide for more information.

Figure 5: Cisco UCS C220 M5 Server (SFF Drives) Front Panel

1	Drive bays 1 to 10 Support for SAS/SATA HDDs and SSDs	2	• Drive bays 1 and 2 support NVMe PCIe SSDs (model UCSC-220-M5SX). • Drive bays 1 to 10 support *only* NVMe PCIe SSDs (model UCSC-220-M5SN).
3	Power button/power status LED	4	Unit identification button/LED
5	System status LED	6	Power supply status LED
7	Fan status LED	8	Network link activity LED
9	Temperature status LED	10	Pullout asset card
11	KVM connector Used with a KVM cable that provides one DB-15 VGA, one DB-9 serial, and two USB connectors.		—

Cisco UCS C220 M5 Server Rear Panel

The following figure shows the rear panel of the UCS C220 M5 Server.

See Cisco UCS C220 M5 Server Installation and Service Guide for more information.

Figure 6: Cisco UCS C220 M5 Server Rear Panel
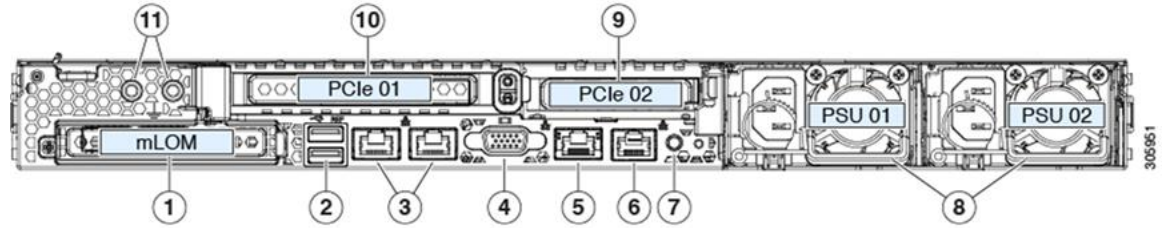
1	Modular LAN-on-motherboard (mLOM) card bay (x16 PCIe lane)	2	Two USB 3.0 ports
3	Dual 1-Gb/10-Gb Ethernet ports (referred to as LAN1 and LAN2, or LOM port 1 and LOM port 2) The dual LAN ports can support 1 Gbps and 10 Gbps depending on the link partner capability.	4	VGA video port (DB-15 connector)
5	1-Gb Ethernet dedicated management port	6	Serial port (RJ-45 connector)
7	Rear unit identification button/LED	8	Two power supplies (redundant as 1+1)
9	PCIe riser 2/slot 2 (x16 lane) Includes PCIe cable connectors for front-loading NVMe SSDs (x8 lane)	10	PCIe riser 1/slot 1 (x16 lane)
11	Threaded holes for dual-hole grounding lug		—

Prepare the Site

Temperature Requirements

The Tetration (Secure Workload) cluster switches and servers require an operating temperature of 41 to 95°F (5 to 35°C) with a derating of the maximum temperature by 1°C for every 1000 feet (305 m) in elevation above sea level. If these devices are not operating, the temperature must be between -40 to 149°F (-40 to 65°C).

Humidity Requirements

High humidity can cause moisture to enter the switches and servers. Moisture can cause corrosion of internal components and degradation of properties such as electrical resistance, thermal conductivity, physical strength, and size. The switches and servers are rated to operate at 10 to 90 percent relative humidity with a humidity gradation of 10 percent per hour. For nonoperating conditions, these devices can withstand from 5 to 93 percent relative humidity.

Buildings in which the climate is controlled by air conditioning in the warmer months and by heat during the colder months usually maintain an acceptable level of humidity for the devices. However, if the devices are located in an unusually humid location, you should use a dehumidifier to maintain the humidity within an acceptable range.

Altitude Requirements

If you operate rack devices at a high altitude (low pressure), the efficiency of forced and convection cooling is reduced and can result in electrical problems that are related to arcing and corona effects. This condition can also cause sealed components with internal pressure, such as electrolytic capacitors, to fail or to perform at a reduced efficiency. These devices are rated to operate at altitudes from 0 to 10,000 feet (0 to 3,050 m), and can be stored at altitudes of 0 to 40,000 feet (12,200 m).

Dust and Particulate Requirements

Fans cool power supplies, switches, and servers by drawing in air and exhausting air out through various openings in the chassis. However, fans also ingest dust and other particles, causing contaminant buildup in the switch and increased internal chassis temperature. A clean operating environment can greatly reduce the negative effects of dust and other particles, which act as insulators and interfere with the mechanical components in the switches and servers.

In addition to regular cleaning, follow these precautions to avoid contamination of rack switches and servers:

- Do not permit smoking near the rack.

- Do not permit food or drink near the rack.

Minimize Electromagnetic and Radio Frequency Interference

Electromagnetic interference (EMI) and radio frequency interference (RFI) from the devices in the Tetration (Secure Workload) cluster rack can adversely affect other devices such as radio and television (TV) receivers operating near the rack. Radio frequencies that emanate from the devices in the rack can also interfere with cordless and low-power telephones. Conversely, RFI from high-power telephones can cause spurious characters to appear on the device monitors.

RFI is any EMI with a frequency above 10 kHz. This type of interference can travel from the switch to other devices through the power cable and power source or through the air as transmitted radio waves. The Federal Communications Commission (FCC) publishes specific regulations to limit the amount of EMI and RFI that can be emitted by computing equipment. Each switch meets these FCC regulations.

When wires are run for any significant distance in an electromagnetic field, interference can occur between the field and the signals on the wires with the following implications:

- Bad wiring can result in radio interference emanating from the plant wiring.

- Strong EMI, especially when it is caused by lightning or radio transmitters, can destroy the signal drivers and receivers in the chassis and even create an electrical hazard by conducting power surges through lines into equipment.

Note   To predict and prevent strong EMI, consult experts in RFI.

The wiring is unlikely to emit radio interference if you use twisted-pair cable with a good distribution of grounding conductors. If you exceed the recommended distances, use a high-quality twisted-pair cable with one ground conductor for each data signal when applicable.

⚠

Caution   If the wires exceed the recommended distances, or if wires pass between buildings, give special consideration to the effect of a lightning strike in your vicinity. The electromagnetic pulse caused by lightning or other high-energy phenomena can easily couple enough energy into unshielded conductors to destroy electronic devices. Consult experts in electrical surge suppression and shielding if you have had similar problems in the past.

Shock and Vibration Requirements

The devices in the Tetration (Secure Workload) cluster devices have been shock- and vibration-tested for operating ranges, handling, and earthquake standards.

Grounding Requirements

The devices in the Tetration (Secure Workload) cluster are sensitive to variations in voltage supplied by the power sources. Overvoltage, undervoltage, and transients (or spikes) can erase data from the memory or cause components to fail. To protect against these types of problems, make sure that there is an earth-ground connection for the devices. You must connect the rack to the facility earth ground.

The grounding points on the chassis are sized for M5 screws. You must provide your own screws, grounding lug, and grounding wire. The grounding lug must be a dual-hole lug that fits M5 screws. The grounding cable that you provide must be 14 AWG (2 mm), minimum 60°C wire, or as permitted by the local code.

Power Requirements

The Tetration (Secure Workload) clusters must be provisioned with power sources that provide the following amounts of power for operations:

- 39-RU large-form factor platform, single rack: 22,500 W

- 39-RU large-form factor platform, dual rack: 11,500 W for each rack

- 8-RU small-form factor platform: 5,500 W

For the required *n+n* power redundancy, you need two AC power sources that each provide that amount of power.

Each chassis in the rack has two power supplies, one for operations and the other for redundancy. Each power supply is connected to a different power strip on the rack, and each power strip is connected to a different AC power source. If one power source fails, the other one provides the required power for each switch or server in the rack.

Airflow Requirements

The Tetration (Secure Workload) cluster requires that you position each rack with the power supplies and fans on the three switches in a cold aisle. When positioned this way, all the devices in the rack take in cooling air from a cold aisle and exhaust hot air to a hot aisle.

Clearance Requirements

The following table lists the amount of space required to install the 39-RU large-form factor (single- or dual-rack) or 8-RU small-form factor Tetration (Secure Workload) cluster. The installation aisle must be more than 23.5 inches (59.69 cm) wide for moving the rack into place. Additionally, you must have enough room for a person to access the front and rear to perform maintenance.

Table 1: Clearance Requirements

Installation Type	Aisle Minimum Width[1]	Rack Installation Minimum Space
C1-Tetration (Single-Rack) Installation	23.5 inches (59.69 cm)	23.5 inches (59.69 cm) wide by 49.8 inches (126.492 cm) deep
C1-Tetration (Dual-Rack)	23.5 inches (59.69 cm)	47 inches (119.38 cm) wide by 49.8 inches (126.492 cm) deep
C1-Tetration-M	23.5 inches (59.69 cm)	23.5 inches (59.69 cm) wide by 49.8 inches (126.492 cm) deep

[1] The Installation aisle and the aisle that the front door of the rack opens must be at least 23.5 inches (59.69 cm) wide. The other aisle, in which the double cabinet doors open must be at least 11.75 inches (29.845 cm) wide for the doors to fully open but at least 23.5 inches (59.69 cm) is needed for a person to perform maintenance.

The rack is positioned with the switch fans (the side of the rack with the largest door) facing the cold aisle and the switch ports (the side of the rack with double doors) facing the hot aisle.

CHAPTER 3

Ground and Connect

Ground the Tetration (Secure Workload) Cluster Devices

The Tetration (Secure Workload) cluster devices have metal-to-metal connections to their rack, so as soon as you ground the rack (or racks for a dual-rack installation) to your data center earth ground, the devices in the rack are grounded. To ground a rack, connect the rack wheels to the earth ground.

Power Up the Tetration (Secure Workload) Cluster Devices

To power up the switch, you must connect two power strips that are attached to the rack to two AC power sources.

Note Connect this equipment to AC mains that have a surge protective device (SPD) at the service equipment that complies with NFPA 70, the National Electrical Code (NEC).

Read the installation instructions before using, installing, or connecting the system to the power source.

Do not overload the wiring when you connect the units to the supply circuit.

Before you begin

• The racks must be installed in the data center and secured in place with their air intakes positioned in a cold aisle.

• The racks must be grounded to the data center earth ground.

• The cluster must be connected to two customer-supplied routers (each router connected to a separate leaf switch).

• There must be two power sources that meet the rack power requirements within reach of each rack power-strip cable.

Step 1 Plug the power cable for one power strip into an AC power source and plug the power cable for the second power strip into another AC power source.

Step 2 Look at each power supply installed in each of the rack devices to verify that the ⏻ LED is lit and green.

- If none of the LEDs are lit, make sure that the power source is turned on and that the on/off switch on the rack power strip is turned on.

- If some of these LEDs are lit and others are not lit, make sure that the power cable coming from that power supply is fully connected to the power strip on the rack.

Connect the Tetration (Secure Workload) Cluster to Your Routers

You must connect the Tetration (Secure Workload) cluster to two routers.

Step 1 If you are installing a 39-RU large-form factor dual-rack cluster, connect the partially connected interface cables on each rack. For each of these cables, connect it to the labeled port on the other rack.

Step 2 Use a 10-Gigabit cable to connect a router to port E1/39 on the leaf 1 switch for a 39-RU deployment, or to port E1/47 for an 8-RU deployment. The leaf 1 switch is located in the following location:

- 39-RU large-form factor single rack platform—RU 40 in the platform rack

- 39-RU large-form factor dual rack platform—RU 40 in rack 1

- 8-RU small-form factor platform—RU 12 in the platform rack

Step 3 Use a 10-Gigabit cable to connect a router to port E1/39 on the leaf 2 switch for a 39-RU deployment, or to port E1/47 for an 8-RU deployment. The leaf 2 switch is located in the following location:

- 39-RU large-form factor single rack platform—RU 41 in the platform rack

- 39-RU large-form factor dual rack platform—RU 41 in rack 2

- 8-RU small-form factor platform—RU 11 in the platform rack

Set Up the User Interface

(Optional) Requirements and Limitations for Dual-Stack Mode (IPv6 Support)

Secure Workload clusters running on physical hardware can be configured to use IPv6 in addition to IPv4 for certain communications to and from the cluster.

Note   You can use the Dual-Stack Mode (IPv6 support) feature when installing or upgrading to 3.6.1.5 and 3.7.1.5 releases, however, the feature is not available when you are installing or upgrading to patch releases.

Limitations

If you are considering enabling dual stack mode, note the following:

- You can enable IPv6 connectivity only during initial deployment or upgrade to a major release (you cannot enable this feature during patch upgrades.)

- Dual-stack mode is supported only on physical hardware/bare-metal clusters.

- There is no support for an IPv6-only mode.

- You cannot revert to IPv4-only mode after dual stack mode is enabled for the cluster.

- Data Backup and Restore (DBR) is not supported if dual-stack connectivity is enabled.

- Do not enable dual-stack mode for clusters configured with Federation.

- The following features always and only use IPv4 (note that IPv4 is always enabled even if IPv6 is enabled):

  - (Applicable for release 3.7.1.5 and 3.6.x) Enforcement on AIX agents

  - (Applicable for release 3.6.x) Hardware agent communication with the cluster

  - (Applicable for release 3.6.x) Connectors for flow ingestion, inventory enrichment, or alert notifications

Requirements

- You must configure both A and AAAA DNS records for FQDN. You must configure this before you enable dual stack mode for your cluster.

- External services such as NTP, SMTP, and DNS should be available over both IPv4 and IPv6, for redundancy purposes.

- In order to configure dual stack mode for a cluster:

  - The two cluster leaf switches will each need to be allocated routable IPv6 addresses on two different networks, for redundancy, and default gateways will need to be provided for each network.

  - For 39RU clusters, a site routable IPv6 network with space for at least 29 host addresses is required.

  - For 8RU clusters, a site routable IPv6 network with space for at least 20 host addresses is required.

  - The first three host addresses of the site routable IPv6 network are reserved for the Cisco Secure Workload cluster HSRP configuration and must not be used by any other devices.

Additional Information

Agents communicate with the cluster using IPv4 unless you configure them to use IPv6. For instructions, see the User Guide available from the Secure Workload portal.

Set Up the User Interface

Before you begin

- To complete this configuration, you need a device such as a laptop computer with an Ethernet port and access to the internet.

- You need an Ethernet cable to connect the device to the highest server in the Secure Workload cluster.

- Google Chrome is the only supported browser for the Setup portal, which is required for part of this process.

- (Optional) Beginning with version 3.6 and later, you can configure your cluster in dual-stack mode, which allows both IPv4 and IPv6 to be used for communication between certain Secure Workload components and between Secure Workload and network services such as NTP and DNS. (Secure Workload already handles IPv6 traffic, whether or not you enable dual-stack mode.) You can enable this support only during deploy or upgrade.

  If you are considering enabling support for IPv6, see .

Important   Enter IPv4 addresses in all fields in the procedure below unless the field name explicitly states IPv6.

Step 1   Configure the internet device with an IP address of 2.2.2.1/30 (255.255.255.252).

Step 2 Use an Ethernet cable to connect the Ethernet port on the internet device to LOM port 2 (LAN2) on the highest server in the top of the Tetration (Secure Workload) cluster.

Step 3 On the internet device, open the Chrome browser and go to http://2.2.2.2:9000.

> **Note** The Chrome browser is the only browser tested with this process.

The Setup Diagnostics page opens.

Step 4 If there are errors in the Diagnostics page, check the cabling connections between cluster devices for broken connections or cables routed incorrectly before continuing with this procedure. When done, return to Step 2.

See C1-Tetration Cluster Device Cabling, on page 21 and C1-Tetration-M Cluster Device Cabling, on page 33 for the correct cabling.

Step 5 Click **Continue**.

The RPM Upload page opens.

> **Note** If the Site Config page opens instead, enter the following URL to open the RPM Upload page:
>
> **http://2.2.2.2:9000 /upload**

Step 6 Upload RPM files to the Tetration (Secure Workload) cloud.

You must upload the files in the following order:

- tetration_os_rpminstall_k9

- tetration_os_UcsFirmware_k9

- tetration_os_adhoc_k9

- tetration_os_mother_rpm_k9

- tetration_os_base_rpm_k9

a) Click **Choose File**.
b) Navigate to an RPM, choose it, and click **Open**.
c) Click **Upload**.

The list of RPMs on the page does not get updated as you upload each RPM. This is expected behavior.

If you see an error after uploading the `tetration_os_mother_rpm_k9-2.1.1.31-1.el6.x86_64.rpm` file, wait approximately 5 to 10 minutes, then reload the page. You should see the list of uploaded RPMs after reloading the page. The error is due to the Orchestrator restarting and is not an issue.

d) Repeat Steps a though c for each RPM.

After you finish uploading the RPMs, the Site Config page opens.

Step 7 Use the Site Config page to set up the new site as follows:

- Click **General**.

   a. In the **Site Name** field, enter the unique cluster name.

   b. In the **SSH Public Key** field, paste in the authentication key.

Note Generate your own SSH key pair that can be used for cluster SSH access.

We strongly recommend that you keep the SSH key in a secure, durable, and accessible location for the purposes of troubleshooting or recovering the cluster by using ta_guest access.

c. Click **Next**.

- Click **Email**.

  a. Fill in the required email addresses.

  b. Click **Next**.

- Click **L3**.

  Enter each of the requested addresses. All fields with * are required fields.

  Enter all addresses as IPv4 unless the field name specifies IPv6.

  (Optional) If you are installing software version 3.6 or later: To enable dual-stack mode (support for both IPv4 and IPv6):

  a. Select the IPv6 checkbox.

  b. Enter the IPv6 address in CIDR notation for both Leaf 1 and Leaf 2 switches.

  c. Enter the Leaf 1 and Leaf 2 IPv6 Default Gateway.

  d. Click **Next**.

- Click **Network**.

  Enter all addresses as IPv4 unless the field name specifies IPv6.

  a. In the **Internal network IP address** field, paste in the address from the Orchestrator deployment output.

  b. In the **External network IP address** field, paste in the address from the Orchestrator deployment output.

  c. In the **External gateway IP address** field, paste the address from the Orchestrator deployment output.

  d. In the **DNS resolver IP address** field, paste the address from the Orchestrator deployment output.

  e. In the **DNS domain** field, enter your DNS domain (for example, `cisco.com`).

  f. (Software version 3.6 or later) If you enabled IPv6 on the L3 page, **IPv6** is automatically selected.

  If IPv6 is selected, you must specify IPv6 addresses reserved for Secure Workload use:

  - Enter the **External IPv6 Network**.

    The first 3 IPv6 addresses in the IPv6 External Network field are always reserved for the switches of the Secure Workload cluster and should not be used for any other purpose.

  - If you want to use IPv6 only for certain addresses, enter those addresses in the **External IPv6 IPs** field.

  Note - For a 39 RU cluster, ensure that at least 29 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.

  - For an 8 RU cluster, ensure that at least 20 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.

    g. Click **Next**.

  • Click **Service**.

    a. In the **NTP Servers** field, enter the space-separated list of NTP server names or IP addresses from the Orchestrator deployment output.

    b. In the **SMTP Server** field, enter the name or IP address of an SMTP server that can be used by Tetration (Secure Workload) for sending email messages. This server must be accessible by Tetration (Secure Workload).

    c. In the **SMTP Port** field, enter the port number of the SMTP server. AWS restricts the use of ports 25 and 465. You must configure your account correctly or use port 587.

    d. (Optional) In the **SMTP Username** field, enter the username for SMTP authentication.

    e. (Optional) In the **SMTP Password** field, enter the password for SMTP authentication.

    f. (Optional) In the **HTTP Proxy Server** field, enter the name or IP address of an HTTP proxy server that can be used by Tetration (Secure Workload) to access external services on the internet.

    g. (Optional) In the **HTTP Proxy Port** field, enter the port number for the HTTP proxy server.

    h. (Optional) In the **HTTPs Proxy Server** field, enter the name or IP address of an HTTPs proxy server that can be used by Tetration (Secure Workload) to access external services on the internet.

    i. (Optional) In the **HTTPs Proxy Port** field, enter the port number for the HTTPs proxy server.

    j. (Optional) In the **Syslog Server** field, enter the name or IP address of a syslog server that can be used by Tetration (Secure Workload) to send alerts.

    k. (Optional) In the **Syslog Port** field, enter the port number of the syslog server.

    l. (Optional) In the **Syslog Severity** field, enter the severity level for the syslog messages. The possible values include informational, notice, warning, error, critical, alert, and emergency.

    m. Click **Next**.

  • Click **UI**.

    a. In the **UI VRRP VRID** field, enter **77** unless you need a unique VRID.

    b. In the **UI FQDN** field, enter the fully qualified domain name where you access the cluster.

    c. Leave the **UI Airbrake Key** field blank.

    d. Click **Next**.

    Tetration (Secure Workload) validates your configuration settings and displays the status for the settings.

  • Click **Advanced**.

    a. In the **External IPs** field, enter IPv4 addresses.

    b. Click **Continue**.

Step 8 If there are any failures, click **Back** and edit the configuration (see Step 7).

    Note You cannot modify these settings in the setup GUI after leaving this page. However, you can modify the settings later from the company page in the GUI.

Step 9   If there are no failures noted for your configuration and you do not need to make any changes, click **Continue**.

Tetration (Secure Workload) is configured according to the settings that you specified. This process takes one to two hours without any interaction on your part.

What to do next

If you deployed software version 3.6 or later and you enabled IPv6 connectivity:

- You can access the Cisco Secure Workload web portal using either IPv4 or IPv6.

- By default, software agents communicate with the Secure Workload cluster using IPv4 even if the cluster is enabled to support IPv6. If you want supported agents to use IPv6 for this purpose, you must configure the **Sensor VIP FQDN** field on the **Platform > Cluster Configuration** page in the Secure Workload web portal. For important instructions, see the user guide, available as online help from the Secure Workload web portal or from https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html.

CHAPTER 5

C1-Tetration (Secure Workload) Cluster Device Cabling

C1-Tetration Cluster Device Cabling

Pay attention to the following configuration information when you cable the M5 Virtual Interface Card (VIC) on the 39-RU rack:

- There are two private interfaces for all nodes.

- The 39-RU rack has one public interface for 20 nodes.

- The M5 hardware has four ports per VIC.

- The names for the bare metal interface—the physical servers in the cluster known as the base, compute, and serving nodes—begin with "eno" (Ethernet onboard).

The following diagram shows the device cabling for the public/external configuration for the C1-Tetration rack. For a detailed list of the connections, see the tables that follow the diagrams.

Figure 7: C1-Tetration Rack Device Cabling (Public/External)
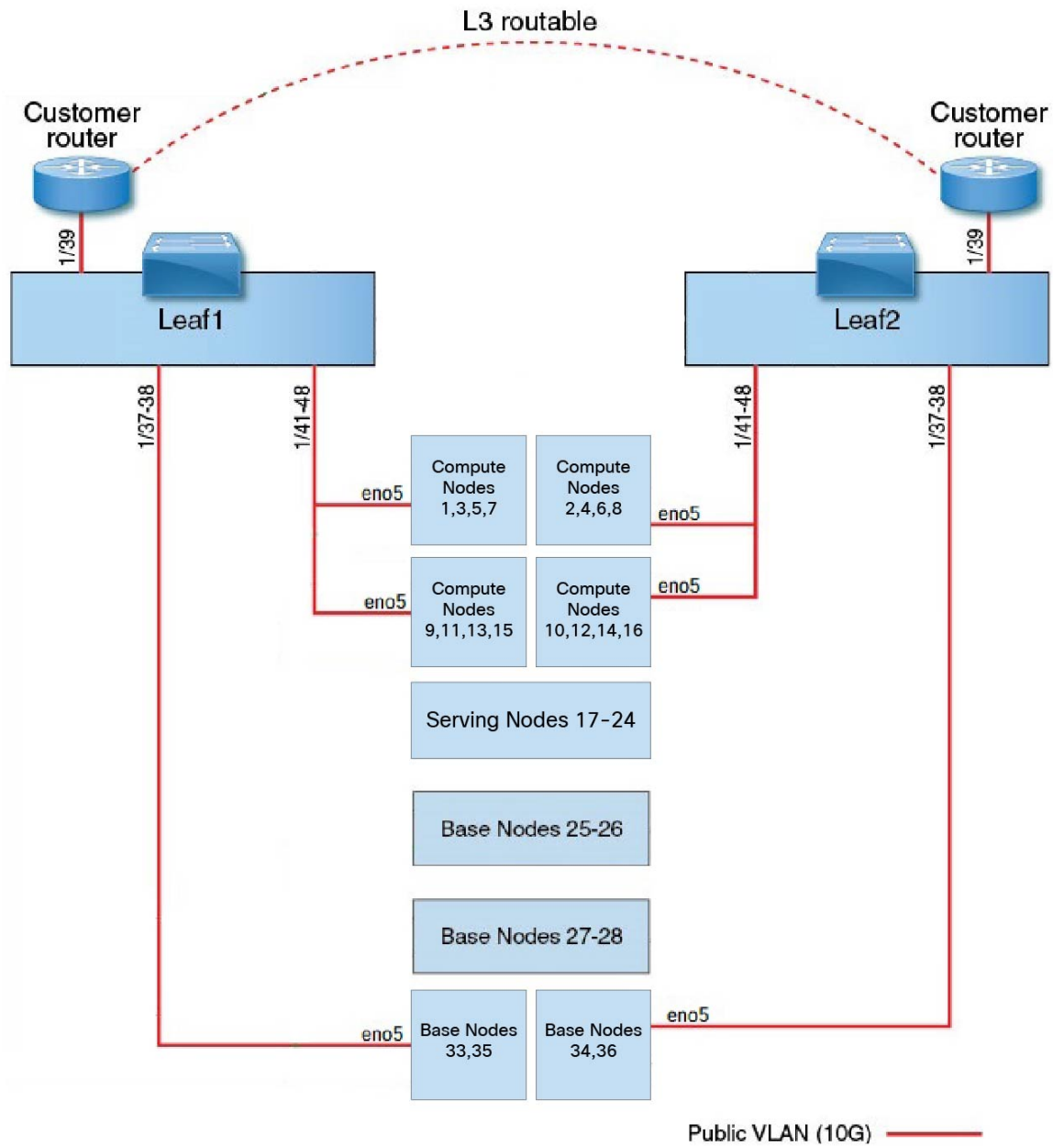
The following diagram shows the device cabling for the internal/management configuration for the C1-Tetration rack. For a detailed list of the connections, see the following tables.

Figure 8: C1-Tetration Rack Device Cabling (Internal/Management)
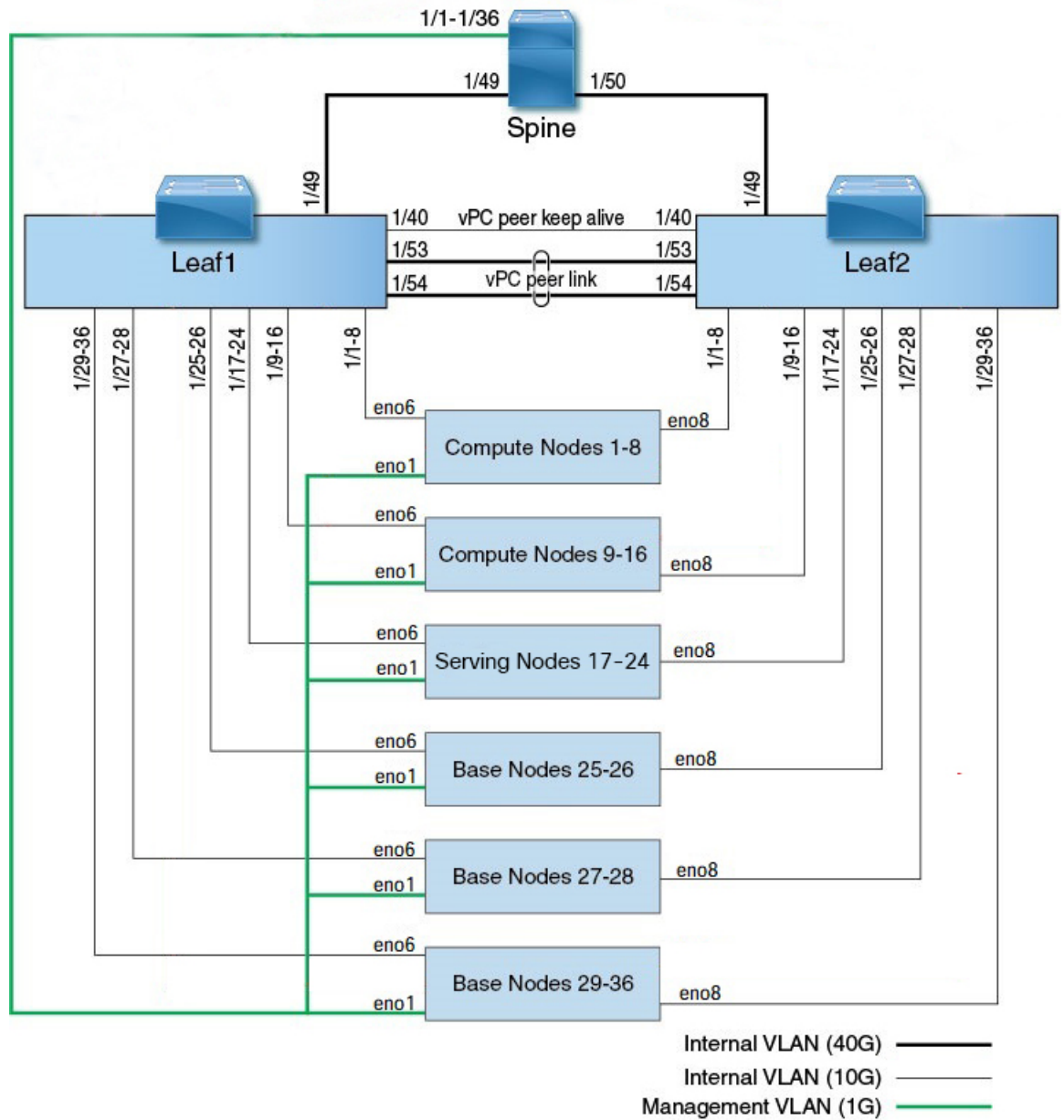
The following figure shows which ports on the M5 server correspond to the "eno" ports in the figures above:

Figure 9: M5 Server Ports
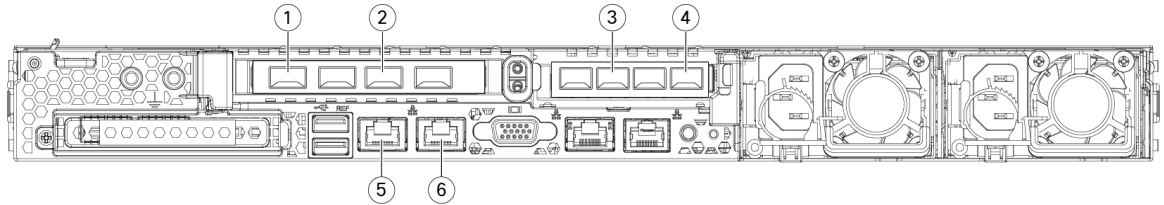
1	Leaf 1 private Server interface port = eno6 CIMC designation = adapter 1/physical port 0/vic-1-eth0	**2**	Leaf 1 or leaf 2 public depending on the server Server interface port = eno5 CIMC designation = adapter 1/physical port 2/vic-1-eth1
3	Not used Server interface port = eno7 CIMC designation = adapter 2/physical port 2/vic-2-eth1	**4**	Leaf 2 private Server interface port = eno8 CIMC designation = adapter 2/physical port 0/vic-2-eth0
5	CIMC Server interface port = eno1 CIMC designation = LOM 1	**6**	MGMT 2.2.2.2 Server interface port = eno2 CIMC designation = LOM 2

Table 2: Spine Switch Connections (RU 42 in Single-Rack Installations and in Dual-Rack Installations)

Spine Port	Connection Type	Connection			
		Device	**RU in Single Rack**	**RU in Dual Rack**	**Port**
1/1	CIMC VLAN (1 Gigabit)	UCS server host 1 (compute node)	RU 36	Rack 1 RU 17	eno1
1/2	CIMC VLAN (1 Gigabit)	UCS server host 2 (compute node)	RU 35	Rack 1 RU 16	eno1
1/3	CIMC VLAN (1 Gigabit)	UCS server host 3 (compute node)	RU 34	Rack 1 RU 15	eno1
1/4	CIMC VLAN (1 Gigabit)	UCS server host 4 (compute node)	RU 33	Rack 1 RU 14	eno1
1/5	CIMC VLAN (1 Gigabit)	UCS server host 5 (compute node)	RU 32	Rack 1 RU 13	eno1
1/6	CIMC VLAN (1 Gigabit)	UCS server host 6 (compute node)	RU 31	Rack 1 RU 12	eno1

Spine Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
1/7	CIMC VLAN (1 Gigabit)	UCS server host 7 (compute node)	RU 30	Rack 1 RU 11	eno1
1/8	CIMC VLAN (1 Gigabit)	UCS server host 8 (compute node)	RU 29	Rack 1 RU 10	eno1
1/9	CIMC VLAN (1 Gigabit)	UCS server host 9 (compute node)	RU 28	Rack 1 RU 8	eno1
1/10	CIMC VLAN (1 Gigabit)	UCS server host 10 (compute node)	RU 27	Rack 1 RU 7	eno1
1/11	CIMC VLAN (1 Gigabit)	UCS server host 11 (compute node)	RU 26	Rack 1 RU 6	eno1
1/12	CIMC VLAN (1 Gigabit)	UCS server host 12 (compute node)	RU 25	Rack 1 RU 5	eno1
1/13	CIMC VLAN (1 Gigabit)	UCS server host 13 (compute node)	RU 24	Rack 1 RU 4	eno1
1/14	CIMC VLAN (1 Gigabit)	UCS server host 14 (compute node)	RU 23	Rack 1 RU 3	eno1
1/15	CIMC VLAN (1 Gigabit)	UCS server host 15 (compute node)	RU 22	Rack 1 RU 2	eno1
1/16	CIMC VLAN (1 Gigabit)	UCS server host 16 (compute node)	RU 21	Rack 1 RU 1	eno1
1/17	CIMC VLAN (1 Gigabit)	UCS server host 17 (serving node)	RU 20	Rack 2 RU 21	eno1
1/18	CIMC VLAN (1 Gigabit)	UCS server host 18 (serving node)	RU 19	Rack 2 RU 20	eno1
1/19	CIMC VLAN (1 Gigabit)	UCS server host 19 (serving node)	RU 18	Rack 2 RU 19	eno1
1/20	CIMC VLAN (1 Gigabit)	UCS server host 20 (serving node)	RU 17	Rack 2 RU 18	eno1
1/21	CIMC VLAN (1 Gigabit)	UCS server host 21 (serving node)	RU 16	Rack 2 RU 17	eno1
1/22	CIMC VLAN (1 Gigabit)	UCS server host 22 (serving node)	RU 15	Rack 2 RU 16	eno1

Spine Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
1/23	CIMC VLAN (1 Gigabit)	UCS server host 23 (serving node)	RU 14	Rack 2 RU 15	eno1
1/24	CIMC VLAN (1 Gigabit)	UCS server host 24 (serving node)	RU 13	Rack 2 RU 14	eno1
1/25	CIMC VLAN (1 Gigabit)	UCS server host 25 (base node)	RU 12	Rack 2 RU 12	eno1
1/26	CIMC VLAN (1 Gigabit)	UCS server host 26 (base node)	RU 11	Rack 2 RU 11	eno1
1/27	CIMC VLAN (1 Gigabit)	UCS server host 27 (base node)	RU 10	Rack 2 RU 10	eno1
1/28	CIMC VLAN (1 Gigabit)	UCS server host 28 (base node)	RU 9	Rack 2 RU 9	eno1
1/29	CIMC VLAN (1 Gigabit)	UCS server host 29 (base node)	RU 8	Rack 2 RU 8	eno1
1/30	CIMC VLAN (1 Gigabit)	UCS server host 30 (base node)	RU 7	Rack 2 RU 7	eno1
1/31	CIMC VLAN (1 Gigabit)	UCS server host 31 (base node)	RU 6	Rack 2 RU 6	eno1
1/32	CIMC VLAN (1 Gigabit)	UCS server host 32 (base node)	RU 5	Rack 2 RU 5	eno1
1/33	CIMC VLAN (1 Gigabit)	UCS server host 33 (base node)	RU 4	Rack 2 RU 4	eno1
1/34	CIMC VLAN (1 Gigabit)	UCS server host 34 (base node)	RU 3	Rack 2 RU 3	eno1
1/35	CIMC VLAN (1 Gigabit)	UCS server host 35 (base node)	RU 2	Rack 2 RU 2	eno1
1/36	CIMC VLAN (1 Gigabit)	UCS server host 36 (base node)	RU 1	Rack 2 RU 1	eno1
1/49	Internal VLAN (40 Gigabit)	Leaf switch 1 (RU 41 in single rack or RU 40 in rack 1 of dual rack)	RU 40	Rack 1 RU 40	1/49
1/50	Internal VLAN (40 Gigabit)	Leaf switch 2 (RU 40 in single rack or RU 40 of rack 2 in dual rack) port 49	RU 41	Rack 2 RU 40	1/50

Table 3: Leaf Switch 1 Connections (RU 41 in Single-Rack Installations or RU 40 in Rack 1 of Dual-Rack Installations)

Leaf 1 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
1/1	Internal VLAN (10 Gigabit)	UCS server host 1 (compute node)	RU 36	Rack 1 RU 17	eno6
1/2	Internal VLAN (10 Gigabit)	UCS server host 2 (compute node)	RU 35	Rack 1 RU 16	eno6
1/3	Internal VLAN (10 Gigabit)	UCS server host 3 (compute node)	RU 34	Rack 1 RU 15	eno6
1/4	Internal VLAN (10 Gigabit)	UCS server host 4 (compute node)	RU 33	Rack 1 RU 14	eno6
1/5	Internal VLAN (10 Gigabit)	UCS server host 5 (compute node)	RU 32	Rack 1 RU 13	eno6
1/6	Internal VLAN (10 Gigabit)	UCS server host 6 (compute node)	RU 31	Rack 1 RU 12	eno6
1/7	Internal VLAN (10 Gigabit)	UCS server host 7 (compute node)	RU 30	Rack 1 RU 11	eno6
1/8	Internal VLAN (10 Gigabit)	UCS server host 8 (compute node)	RU 29	Rack 1 RU 10	eno6
1/9	Internal VLAN (10 Gigabit)	UCS server host 9 (compute node)	RU 28	Rack 1 RU 8	eno6
1/10	Internal VLAN (10 Gigabit)	UCS server host 10 (compute node)	RU 27	Rack 1 RU 7	eno6
1/11	Internal VLAN (10 Gigabit)	UCS server host 11 (compute node)	RU 26	Rack 1 RU 6	eno6
1/12	Internal VLAN (10 Gigabit)	UCS server host 12 (compute node)	RU 25	Rack 1 RU 5	eno6
1/13	Internal VLAN (10 Gigabit)	UCS server host 13 (compute node)	RU 24	Rack 1 RU 4	eno6
1/14	Internal VLAN (10 Gigabit)	UCS server host 14 (compute node)	RU 23	Rack 1 RU 3	eno6
1/15	Internal VLAN (10 Gigabit)	UCS server host 15 (compute node)	RU 22	Rack 1 RU 2	eno6
1/16	Internal VLAN (10 Gigabit)	UCS server host 16 (compute node)	RU 21	Rack 1 RU 1	eno6

Leaf 1 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
1/17	Internal VLAN (10 Gigabit)	UCS server host 17 (serving node)	RU 20	Rack 2 RU 21	eno6
1/18	Internal VLAN (10 Gigabit)	UCS server host 18 (serving node)	RU 19	Rack 2 RU 20	eno6
1/19	Internal VLAN (10 Gigabit)	UCS server host 19 (serving node)	RU 18	Rack 2 RU 19	eno6
1/20	Internal VLAN (10 Gigabit)	UCS server host 20 (serving node)	RU 17	Rack 2 RU 18	eno6
1/21	Internal VLAN (10 Gigabit)	UCS server host 21 (serving node)	RU 16	Rack 2 RU 17	eno6
1/22	Internal VLAN (10 Gigabit)	UCS server host 22 (serving node)	RU 15	Rack 2 RU 16	eno6
1/23	Internal VLAN (10 Gigabit)	UCS server host 23 (serving node)	RU 14	Rack 2 RU 15	eno6
1/24	Internal VLAN (10 Gigabit)	UCS server host 24 (serving node)	RU 13	Rack 2 RU 14	eno6
1/25	Internal VLAN (10 Gigabit)	UCS server host 25 (base node)	RU 12	Rack 2 RU 12	eno6
1/26	Internal VLAN (10 Gigabit)	UCS server host 26 (base node)	RU 11	Rack 2 RU 11	eno6
1/27	Internal VLAN (10 Gigabit)	UCS server host 27 (base node)	RU 10	Rack 2 RU 10	eno6
1/28	Internal VLAN (10 Gigabit)	UCS server host 28 (base node)	RU 9	Rack 2 RU 9	eno6
1/29	Internal VLAN (10 Gigabit)	UCS server host 29 (base node)	RU 8	Rack 2 RU 8	eno6
1/30	Internal VLAN (10 Gigabit)	UCS server host 30 (base node)	RU 7	Rack 2 RU 7	eno6
1/31	Internal VLAN (10 Gigabit)	UCS server host 31 (base node)	RU 6	Rack 2 RU 6	eno6
1/32	Internal VLAN (10 Gigabit)	UCS server host 32 (base node)	RU 5	Rack 2 RU 5	eno6
1/33	Internal VLAN (10 Gigabit)	UCS server host 33 (base node)	RU 4	Rack 2 RU 4	eno6

Leaf 1 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
1/34	Internal VLAN (10 Gigabit)	UCS server host 34 (base node)	RU 3	Rack 2 RU 3	eno6
1/35	Internal VLAN (10 Gigabit)	UCS server host 35 (base node)	RU 2	Rack 2 RU 2	eno6
1/36	Internal VLAN (10 Gigabit)	UCS server host 36 (base node)	RU 1	Rack 2 RU 1	eno6
1/37	Public VLAN (10 Gigabit)	UCS server host 33 (base node)	RU 3	Rack 2 RU 3	eno5
1/38	Public VLAN (10 Gigabit)	UCS server host 35 (base node)	RU 1	Rack 2 RU 1	eno5
1/39	Internal VLAN (10 Gigabit)	Customer router 1	—	—	—
1/40	Internal VLAN (10 Gigabit)	Leaf 1	RU 40	Rack 1 RU 40	1/40
1/41	Public VLAN (10 Gigabit)	UCS server host 1 (compute node)	RU 35	Rack 1 RU 16	eno5
1/42	Public VLAN (10 Gigabit)	UCS server host 3 (compute node)	RU 33	Rack 1 RU 14	eno5
1/43	Public VLAN (10 Gigabit)	UCS server host 5 (compute node)	RU 31	Rack 1 RU 12	eno5
1/44	Public VLAN (10 Gigabit)	UCS server host 7 (compute node)	RU 29	Rack 1 RU 10	eno5
1/45	Public VLAN (10 Gigabit)	UCS server host 9 (compute node)	RU 27	Rack 1 RU 8	eno5
1/46	Public VLAN (10 Gigabit)	UCS server host 11 (compute node)	RU 25	Rack 1 RU 6	eno5
1/47	Public VLAN (10 Gigabit)	UCS server host 13 (compute node)	RU 23	Rack 1 RU 4	eno5
1/48	Public VLAN (10 Gigabit)	UCS server host 15 (compute node)	RU 21	Rack 1 RU 2	eno5

Leaf 1 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
1/49	Internal VLAN (40 Gigabit)	Spine switch	RU 42	Rack 1 RU 42	1/49
1/50	—	—	—	—	—
1/51	—	—	—	—	—
1/52	—	—	—	—	—
1/53	Internal VLAN (40 Gigabit)	Leaf switch 1	RU 40	Rack 1 RU 40	1/53
1/54	Internal VLAN (40 Gigabit)	Leaf switch 1	RU 40	Rack 1 RU 40	1/54

Table 4: Leaf Switch 2 Connections (RU 41 in Single-Rack Installations or RU 40 in Rack 2 of Dual-Rack Installations)

Leaf 2 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
1/1	Internal VLAN (10 Gigabit)	UCS server host 1 (compute node)	RU 36	Rack 1 RU 17	eno8
1/2	Internal VLAN (10 Gigabit)	UCS server host 2 (compute node)	RU 35	Rack 1 RU 16	eno8
1/3	Internal VLAN (10 Gigabit)	UCS server host 3 (compute node)	RU 34	Rack 1 RU 15	eno8
1/4	Internal VLAN (10 Gigabit)	UCS server host 4 (compute node)	RU 33	Rack 1 RU 14	eno8
1/5	Internal VLAN (10 Gigabit)	UCS server host 5 (compute node)	RU 32	Rack 1 RU 13	eno8
1/6	Internal VLAN (10 Gigabit)	UCS server host 6 (compute node)	RU 31	Rack 1 RU 12	eno8
1/7	Internal VLAN (10 Gigabit)	UCS server host 7 (compute node7)	RU 30	Rack 1 RU 11	eno8
1/8	Internal VLAN (10 Gigabit)	UCS server host 8 (compute node)	RU 29	Rack 1 RU 10	eno8

Leaf 2 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
1/9	Internal VLAN (10 Gigabit)	UCS server host 9 (compute node)	RU 28	Rack 1 RU 8	eno8
1/10	Internal VLAN (10 Gigabit)	UCS server host 10 (compute node)	RU 27	Rack 1 RU 7	eno8
1/11	Internal VLAN (10 Gigabit)	UCS server host 11 (compute node)	RU 26	Rack 1 RU 6	eno8
1/12	Internal VLAN (10 Gigabit)	UCS server host 12 (compute node)	RU 25	Rack 1 RU 5	eno8
1/13	Internal VLAN (10 Gigabit)	UCS server host 13 (compute node)	RU 24	Rack 1 RU 4	eno8
1/14	Internal VLAN (10 Gigabit)	UCS server host 14 (compute node)	RU 23	Rack 1 RU 3	eno8
1/15	Internal VLAN (10 Gigabit)	UCS server host 15 (compute node)	RU 22	Rack 1 RU 2	eno8
1/16	Internal VLAN (10 Gigabit)	UCS server host 16 (compute node)	RU 21	Rack 1 RU 1	eno8
1/17	Internal VLAN (10 Gigabit)	UCS server host 17 (serving node)	RU 20	Rack 2 RU 21	eno8
1/18	Internal VLAN (10 Gigabit)	UCS server host 18 (serving node)	RU 19	Rack 2 RU 20	eno8
1/19	Internal VLAN (10 Gigabit)	UCS server host 19 (serving node)	RU 18	Rack 2 RU 19	eno8
1/20	Internal VLAN (10 Gigabit)	UCS server host 20 (serving node)	RU 17	Rack 2 RU 18	eno8
1/21	Internal VLAN (10 Gigabit)	UCS server host 21 (serving node)	RU 16	Rack 2 RU 17	eno8
1/22	Internal VLAN (10 Gigabit)	UCS server host 22 (serving node)	RU 15	Rack 2 RU 16	eno8
1/23	Internal VLAN (10 Gigabit)	UCS server host 23 (serving node)	RU 14	Rack 2 RU 15	eno8
1/24	Internal VLAN (10 Gigabit)	UCS server host 24 (serving node)	RU 13	Rack 2 RU 14	eno8

Leaf 2 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
1/25	Internal VLAN (10 Gigabit)	UCS server host 25 (base node)	RU 12	Rack 2 RU 12	eno8
1/26	Internal VLAN (10 Gigabit)	UCS server host 26 (base node)	RU 11	Rack 2 RU 11	eno8
1/27	Internal VLAN (10 Gigabit)	UCS server host 27 (base node)	RU 10	Rack 2 RU 10	eno8
1/28	Internal VLAN (10 Gigabit)	UCS server host 28 (base node)	RU 9	Rack 2 RU 9	eno8
1/29	Internal VLAN (10 Gigabit)	UCS server host 29 (base node)	RU 8	Rack 2 RU 8	eno8
1/30	Internal VLAN (10 Gigabit)	UCS server host 30 (base node)	RU 7	Rack 2 RU 7	eno8
1/31	Internal VLAN (10 Gigabit)	UCS server host 31 (base node)	RU 6	Rack 2 RU 6	eno8
1/32	Internal VLAN (10 Gigabit)	UCS server host 32 (base node)	RU 5	Rack 2 RU 5	eno8
1/33	Internal VLAN (10 Gigabit)	UCS server host 33 (base node)	RU 4	Rack 2 RU 4	eno8
1/34	Internal VLAN (10 Gigabit)	UCS server host 34 (base node)	RU 3	Rack 2 RU 3	eno8
1/35	Internal VLAN (10 Gigabit)	UCS server host 35 (base node)	RU 2	Rack 2 RU 2	eno8
1/36	Internal VLAN (10 Gigabit)	UCS server host 36 (base node)	RU 1	Rack 2 RU 1	eno8
1/37	Public VLAN (10 Gigabit)	UCS server host 34 (base node)	RU 4	Rack 2 RU 8	eno5
1/38	Public VLAN (10 Gigabit)	UCS server host 36 (base node)	RU 2	Rack 2 RU 6	eno5
1/39	Internal VLAN (10 Gigabit)	Customer router 1	—	—	—
1/40	Internal VLAN (10 Gigabit)	Leaf switch 2	RU 41	Rack 2 RU 40	1/40
1/41	Public VLAN (10 Gigabit)	UCS server host 2 (compute node)	RU 36	Rack 1 RU 17	eno5

Leaf 2 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
1/42	Public VLAN (10 Gigabit)	UCS server host 4 (compute node)	RU 34	Rack 1 RU 15	eno5
1/43	Public VLAN (10 Gigabit)	UCS server host 6 (compute node)	RU 32	Rack 1 RU 13	eno5
1/44	Public VLAN (10 Gigabit)	UCS server host 8 (compute node)	RU 30	Rack 1 RU 11	eno5
1/45	Public VLAN (10 Gigabit)	UCS server host 10 (compute node)	RU 28	Rack 1 RU 9	eno5
1/46	Public VLAN (10 Gigabit)	UCS server host 12 (compute node)	RU 26	Rack 1 RU 7	eno5
1/47	Public VLAN (10 Gigabit)	UCS server host 14 (compute node)	RU 24	Rack 1 RU 5	eno5
1/48	Public VLAN (10 Gigabit)	UCS server host 16 (compute node)	RU 22	Rack 1 RU 3	eno5
1/49	Internal VLAN (40 Gigabit)	Spine switch	RU 42	Rack 1 RU 42	—
1/50	—	—	—	—	1/50
1/51	—	—	—	—	—
1/52	—	—	—	—	—
1/53	Internal VLAN (40 Gigabit)	Leaf 1 switch	RU 40	Rack 1 RU 40	1/49
1/54	Internal VLAN (40 Gigabit)	Leaf 2 switch	RU 41	Rack 2 RU 40	1/50

C1-Tetration-M Cluster Device Cabling

To cable the M5 VIC on the 8-RU rack, pay attention to the following configuration information:

- There are two private interfaces for all nodes.

- The 8-RU rack has two public interfaces for all six nodes.

- The M5 hardware has four ports per VIC.

- The names for the bare metal interface—the physical server in the cluster known as the universal nodes—begin with "eno" (Ethernet onboard).

The following diagram shows the device cabling for the internal/management/public/external configuration of the C1-Tetration-M Cluster 8-RU rack. For a detailed list of the connections, see the tables that follow the diagram.

Figure 10: C1-Tetration-M Cluster Rack Device Cabling (Internal/Management/Public/External)
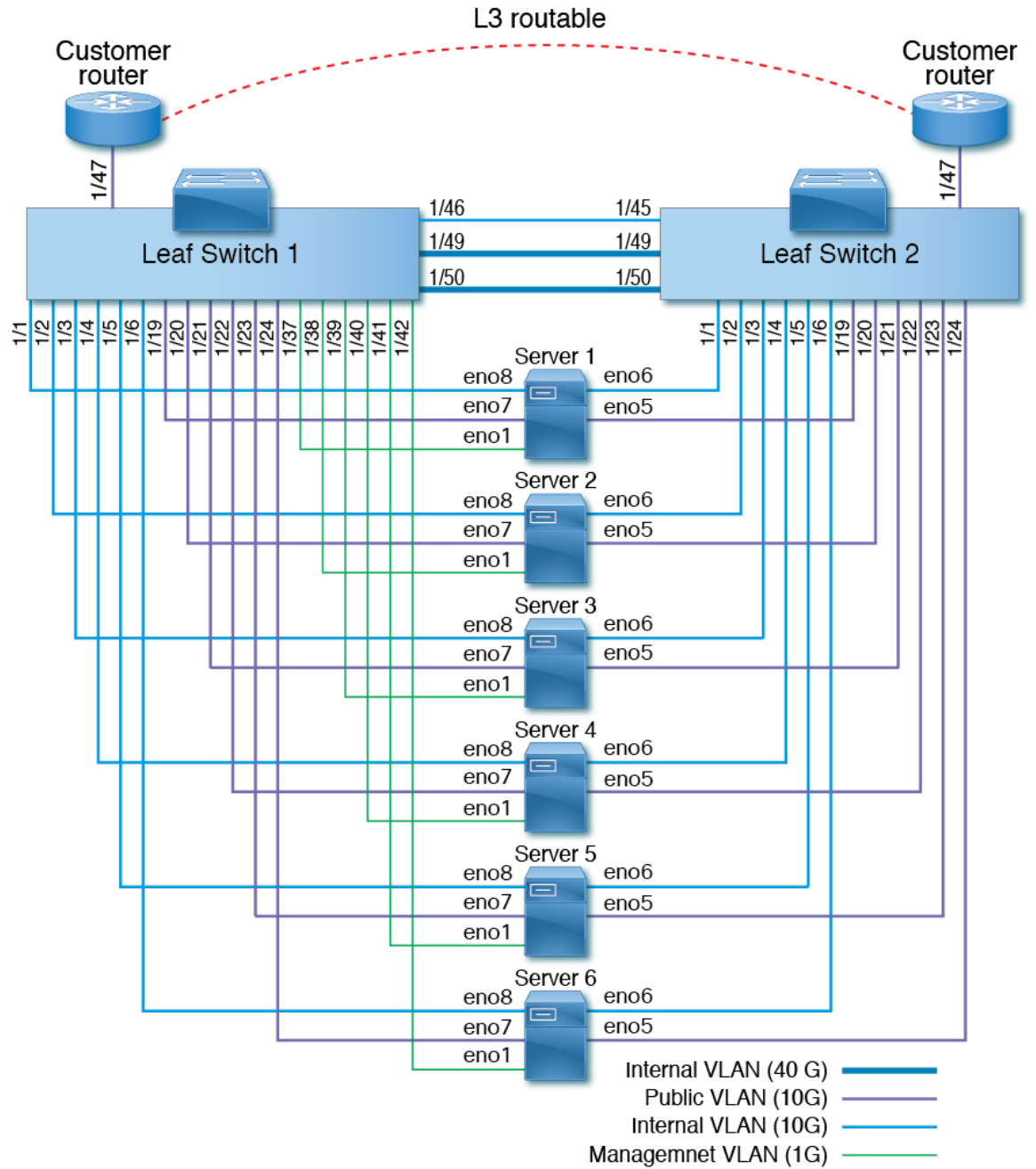
The following figure shows which ports on the server correspond to the "eno" ports in the diagram above:

Figure 11: M5 Server Ports
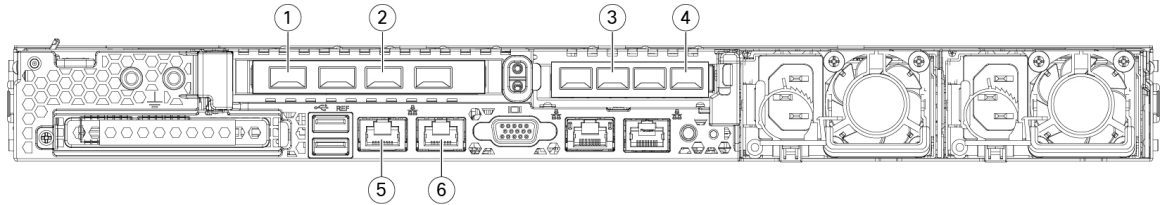
1	Leaf 2 private Server interface port = eno6 CIMC designation = adapter 1/physical port 0/vic-1-eth0	2	Leaf 2 public depending on the server Server interface port = eno5 CIMC designation = adapter 1/physical port 2/vic-1-eth1
3	Leaf 1 public Server interface port = eno7 CIMC designation = adapter 2/physical port 2/vic-2-eth1	4	Leaf 1 private Server interface port = eno8 CIMC designation = adapter 2/physical port 0/vic-2-eth0
5	CIMC Server interface port = eno1 CIMC designation = LOM 1	6	MGMT 2.2.2.2 Server interface port = eno2 CIMC designation = LOM 2

Table 5: Leaf Switch 1 (RU 12) Connections

| Leaf Port	Connection Type	Connection		
		Device	RU in Single Rack	Port
1/1	Internal VLAN (10 Gigabit)	UCS server host 1 (universal node)	RU 9	eno8
1/2	Internal VLAN (10 Gigabit)	UCS server host 2 (universal node)	RU 8	eno8
1/3	Internal VLAN (10 Gigabit)	UCS server host 3 (universal node)	RU 6	eno8
1/4	Internal VLAN (10 Gigabit)	UCS server host 4 (universal node)	RU 5	eno8
1/5	Internal VLAN (10 Gigabit)	UCS server host 5 (universal node)	RU 3	eno8
1/6	Internal VLAN (10 Gigabit)	UCS server host 6 (universal node)	RU 2	eno8
1/7	—	—	—	—
1/8	—	—	—	—
1/9	—	—	—	—
1/10	—	—	—	—

Leaf Port	Connection Type	Connection		
		Device	RU in Single Rack	Port
1/11	—	—	—	—
1/12	—	—	—	—
1/13	—	—	—	—
1/14	—	—	—	—
1/15	—	—	—	— –
1/16	—	—	—	—
1/17	—	—	—	—
1/18	—	—	—	—
1/19	External VLAN (10 Gigabit)	UCS server host 1 (universal node)	RU 9	eno7
1/20	External VLAN (10 Gigabit)	UCS server host 2 (universal node)	RU 8	eno7
1/21	External VLAN (10 Gigabit)	UCS server host 3 (universal node)	RU 6	eno7
1/22	External VLAN (10 Gigabit)	UCS server host 4 (universal node)	RU 5	eno7
1/23	External VLAN (10 Gigabit)	UCS server host 5 (universal node)	RU 3	eno7
1/24	External VLAN (10 Gigabit)	UCS server host 6 (universal node)	RU 2	eno7
1/25	—	—	—	—
1/26	—	—	—	—
1/27	—	—	—	—
1/28	—	—	—	—
1/29	—	—	—	—
1/30	—	—	—	—
1/31	—	—	—	—
1/32	—	—	—	—
1/33	—	—	—	—
1/34	—	—	—	—
1/35	—	—	—	—

Leaf Port	Connection Type	Connection		
		Device	RU in Single Rack	Port
1/36	—	—	—	—
1/37	Management VLAN (1 Gigabit)	UCS server host 1 (universal node)	RU 9	eno1
1/38	Management VLAN (1 Gigabit)	UCS server host 2 (universal node)	RU 8	eno1
1/39	Management VLAN (1 Gigabit)	UCS server host 3 (universal node)	RU 6	eno1
1/40	Management VLAN (1 Gigabit)	UCS server host 4 (universal node)	RU 5	eno1
1/41	Management VLAN (1 Gigabit)	UCS server host 5 (universal node)	RU 3	eno1
1/42	Management VLAN (1 Gigabit)	UCS server host 6 (universal node)	RU 2	eno1
1/43	—	—	—	—
1/44	—	—	—	—
1/45	—	–	—	—
1/46	Internal VLAN (10 Gigabit)	Leaf 2 switch	RU 11	1/45
1/47	External VLAN (10 Gigabit)	Customer router	—	—
1/48	—	—	—	—
1/49	Internal VLAN (40 Gigabit)	Leaf 2 switch	RU 11	1/49
1/50	Internal VLAN (40 Gigabit)	Leaf 2 switch	RU 11	1/50
1/51	—	—	—	—
1/52	—	—	—	—
1/53	—	—	—	—
1/54	—	—	—	—

Table 6: Leaf Switch 2 (RU 11) Connections

Leaf Port	Connection Type	Connection		
		Device	RU in Single Rack	Port
1/1	Internal VLAN (10 Gigabit)	UCS server host 1 (universal node)	9 RU	eno6
1/2	Internal VLAN (10 Gigabit)	UCS server host 2 (universal node)	8 RU	eno6

Leaf Port	Connection Type	Connection		
		Device	**RU in Single Rack**	**Port**
1/3	Internal VLAN (10 Gigabit)	UCS server host 3 (universal node)	6 RU	eno6
1/4	Internal VLAN (10 Gigabit)	UCS server host 4 (universal node)	5 RU	eno6
1/5	Internal VLAN (10 Gigabit)	UCS server host 5 (universal node)	3 RU	eno6
1/6	Internal VLAN (10 Gigabit)	UCS server host 6 (universal node)	2 RU	eno6
1/7	—	—	—	—
1/8	—	—	—	—
1/9	—	—	—	—
1/10	—	—	—	—
1/11	—	—	—	—
1/12	—	—	—	—
1/13	—	—	—	—
1/14	—	—	—	—
1/15	—	—	—	—
1/16	—	—	—	—
1/17	—	—	—	—
1/18	—	—	—	—
1/19	External VLAN (10 Gigabit)	UCS server host 1 (universal node)	9 RU	eno5
1/20	External VLAN (10 Gigabit)	UCS server host 2 (universal node)	8 RU	eno5
1/21	External VLAN (10 Gb)	UCS server host 3 (universal node)	6 RU	eno5
1/22	External VLAN (10 Gigabit)	UCS server host 4 (universal node)	5 RU	eno5
1/23	External VLAN (10 Gigabit)	UCS server host 5 (universal node)	3 RU	eno5
1/24	External VLAN (10 Gigabit)	UCS server host 6 (universal node)	2 RU	eno5
1/25	—	—	—	—
1/26	—	—	—	—
1/27	—	—	—	—
1/28	—	—	—	—

Leaf Port	Connection Type	Connection		
		Device	**RU in Single Rack**	**Port**
1/29	—	—	—	—
1/30	—	—	—	—
1/31	—	—	—	—
1/32	—	—	—	—
1/33	—	—	—	—
1/34	—	—	—	—
1/35	—	—	—	—
1/36	—	—	—	—
1/37	—	—	—	—
1/38	—	—	—	—
1/39	—	—	—	—
1/40	—	—	—	—
1/41	—	—	—	—
1/42	—	—	—	—
1/43	—	—	—	—
1/44	—	—	—	—
1/45	Internal VLAN (10 Gigabit)	Leaf 1 switch	12 RU	1/46
1/46	—	—	—	—
1/47	External VLAN (10 Gigabit)	Customer router	—	—
1/48	—	—	—	—
1/49	Internal VLAN (40 Gigabit)	Leaf 1 switch	12 RU	1/49
1/50	Internal VLAN (40 Gigabit)	Leaf 1 switch	12 RU	1/50
1/51	—	—	—	—
1/52	—	—	—	—
1/53	—	—	—	—
1/54	—	—	—	—

System Specifications

- Environmental Specifications, on page 41
- Power Cables, on page 41

Environmental Specifications

The following table lists the environmental specifications required for installing the Tetration (Secure Workload) cluster.

Table 7: Environmental Specifications

Environment		Specification
Temperature	Operating	41 to 95°F (5 to 35°C) with derating the maximum temperature by 1°C for every 1000 ft (305 m) above sea level
	Storage	-40 to 149°F (-40 to 65°C)
Humidity	Operating	10 to 80% relative humidity with a humidity gradation of 10% per hour
	Storage	5 to 93% relative humidity
Altitude	Operating	0 to 10,000 ft (0 to 3050 m)
	Storage	0 to 40,000 ft (0 to 12,200 m)

Power Cables

The following tables list the power cables that are included with the Tetration (Secure Workload) M5 cluster.

Table 8: 39-RU Cluster, Single-Rack Configuration

Part Number	Description	Quantity
TA-RACK-UCS2-INT	Cisco R42612 dynamic rack with side panels	1
TA-ETH-RJ45-SINGLE	RJ-45 cable kit for a 39-RU single-rack configuration	1
TA-SFP-H10GB-CU2M	10GBASE-CU SFP+ 2-m cable	16
TA-SFP-H10GB-CU1-5	10GBASE-CU SFP+ 1.5-m cable	32
TA-QSFP-H40G-CU1M	40GBASE-CR4 passive copper 1-m cable	4
TA-SFP-H10GB-CU1M	10GBASE-CU SFP+ 1-m cable	25
TA-SFP-H10GB-CU2-5	10GBASE-CU SFP+ 2.5-m cable	20

Table 9: 39-RU Cluster, Dual-Rack Configuration

Part Number	Description	Quantity
TA-RACK-UCS2-INT	Cisco R42612 dynamic rack, with side panels	2
TA-ETH-RJ45-DUAL	RJ-45 cable kit for a 39-RU single-rack configuration	1
TA-SFP-H10GB-CU2M	10GBASE-CU SFP+ 2-m cable	15
TA-SFP-H10GB-CU1-5	10GBASE-CU SFP+ 1.5-m cable	19
TA-QSFP-H40G-CU1M	40GBASE-CR4 passive copper 1-m cable	1
TA-QSFP-H40G-CU5M	40GBASE-CR4 passive copper 5-m cable	3
TA-SFP-H10GB-CU2-5	10GBASE-CU SFP+ 2.5-m cable	12
TA-SFP-H10GB-CU5M	10GBASE-CU SFP+ 5-m cable	47

Table 10: 8-RU Cluster

Part Number	Description	Quantity
TA-RACK-UCS2-INT	Cisco R42612 dynamic rack, with side panels	1
CAB-ETH-S-RJ45	RJ-45 straight-through yellow 6-ft cable for Ethernet	6
TA-SFP-H10GB-CU1M	10GBASE-CU SFP+ 1-m cable	13
TA-SFP-H10GB-CU1-5	10GBASE-CU SFP+ 1.5-m cable	12
TA-QSFP-H40G-CU1M	40GBASE-CR4 passive copper 1-m cable	2
GLC-TE	1000BASE-T SFP transceiver module for Category 5 copper wire	6