



Bereitstellungsleitfaden für das Cisco Secure Workload-M6-Cluster

Erste Veröffentlichung: 25. Oktober 2023

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

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 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 NON-INFRINGEMENT 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 THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. Alle Rechte vorbehalten.



INHALTSVERZEICHNIS

KAPITEL 1

Übersicht 1

Übersicht 1

Cisco UCS C220 M6-Server – Vorderseite 5

Cisco UCS C220 M6-Server – Rückseite 6

KAPITEL 2

Vorbereiten des Standorts 9

Anforderungen bezüglich der Temperatur 9

Anforderungen bezüglich der Luftfeuchtigkeit 9

Anforderungen bezüglich der Höhe 10

Anforderungen bezüglich Staub und Feinstaub 10

Minimieren von elektromagnetischen und Funkinterferenzen 10

Anforderungen bezüglich Erschütterungen und Vibration 11

Anforderungen bezüglich der Erdung 11

Stromversorgung 11

Anforderungen bezüglich der Luftströmung 12

Anforderungen bezüglich Abständen 12

KAPITEL 3

Erden und Anschließen 13

Erden der Cisco Secure Workload-Cluster-Geräte 13

Einschalten der Cisco Secure Workload-Cluster-Geräte 13

Verbinden des Cisco Secure Workload-Clusters mit Ihren Routern 14

KAPITEL 4

Einrichten der Benutzeroberfläche 15

(Optional) Anforderungen und Einschränkungen für den Dual-Stack-Modus (IPv6-Unterstützung) 15

Einrichten der Benutzeroberfläche 16

KAPITEL 5	C1 – Cisco Secure Workload-Cluster – Geräteverkabelung	23
	C1 – Workload-Cluster – Geräteverkabelung	23
	C1 – Workload-M-Cluster – Geräteverkabelung	36

KAPITEL 6	Systemspezifikationen	45
	Umgebungsbedingungen	45
	Netzkabel	45



KAPITEL 1

Übersicht

- [Übersicht, auf Seite 1](#)
- [Cisco UCS C220 M6-Server – Vorderseite, auf Seite 5](#)
- [Cisco UCS C220 M6-Server – Rückseite, auf Seite 6](#)

Übersicht

Sie können das Cisco Secure Workload-M6-Cluster auf eine der folgenden Arten bereitstellen:

- 39-HE-LFF-Plattform (C1-Workload mit einzelmem Rack) für Rechenzentren mit mehr als 5.000 Servern

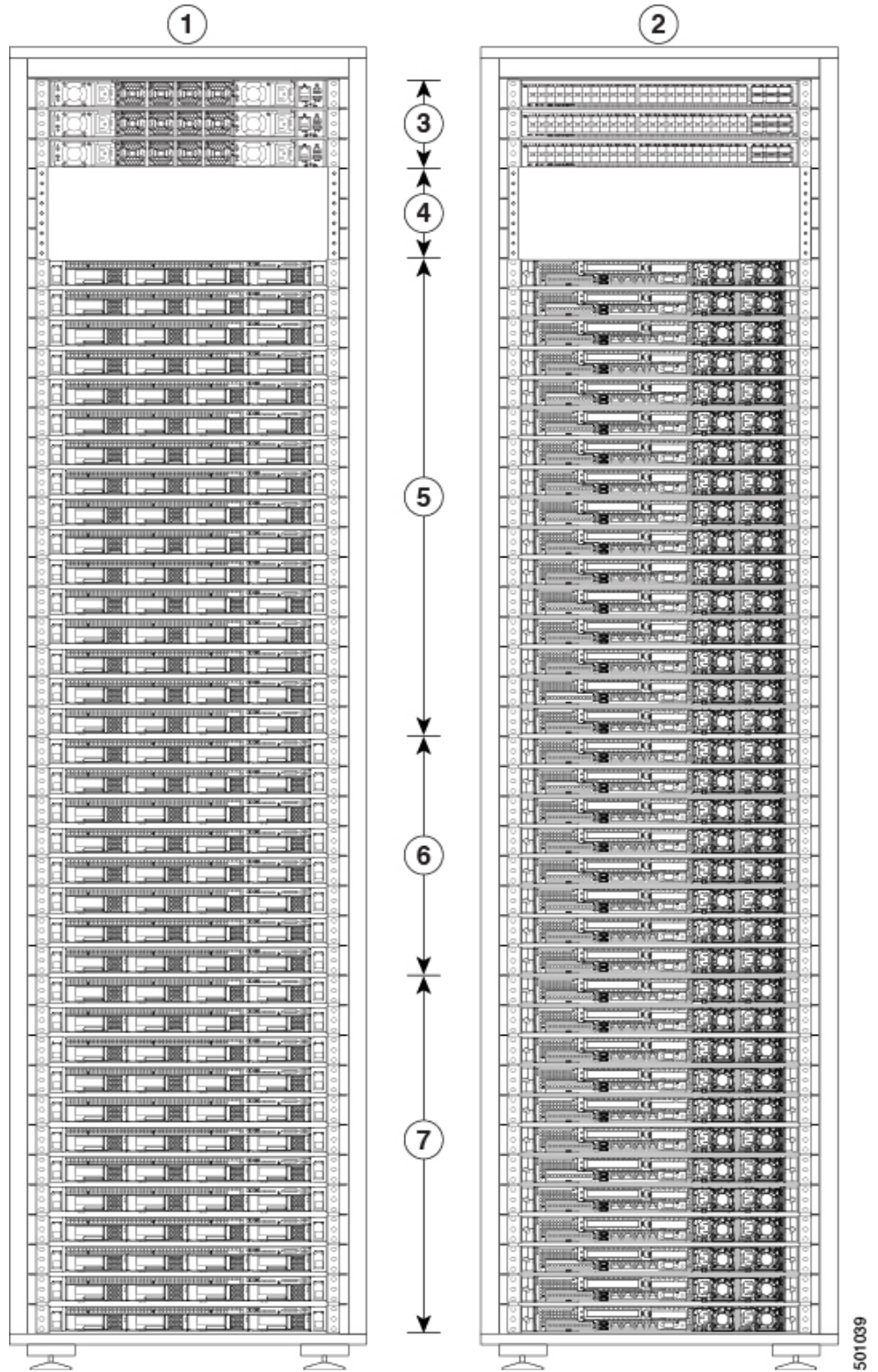


Hinweis Sie können die LFF-Plattform (Large Form Factor) je nach Bedarf in einem oder zwei Racks bereitstellen. Beispiele finden Sie in den folgenden Abbildungen zu C1-Workload mit einem einzelnen Rack und mit zwei Racks.

- 8-HE-SFF-Plattform (C1-Workload-M) für Rechenzentren mit weniger als 5.000 Servern. Beispiel siehe Abbildung zu C1-Workload-M.

Die folgende Abbildung zeigt die Vorder- und Rückseite von C1-Workload mit einem einzelnen Rack.

Abbildung 1: C1-Workload mit einem einzelnen Rack – Vorder- und Rückseite



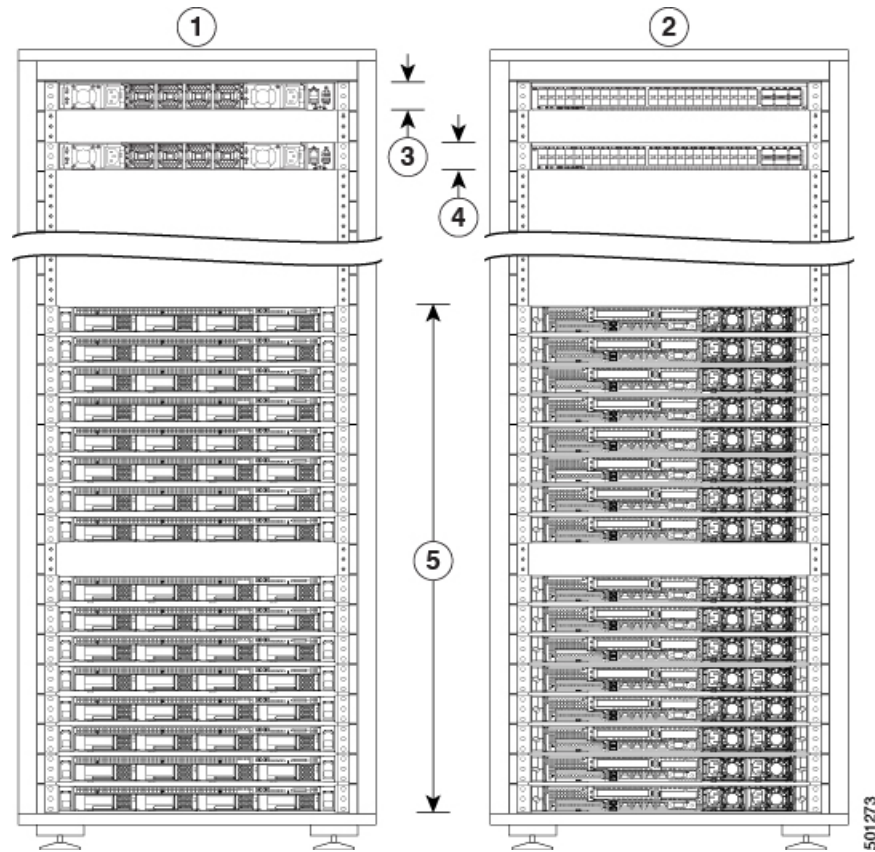
1 Vorderseite (Ansicht Kaltgang)	2 Rückseite (Ansicht Warmgang)
----------------------------------	--------------------------------

501 039

3	Ein Spine-Switch (HE 42) und zwei Leaf-Switches: Leaf 2 (HE 40) und Leaf 1 (HE 41)	4	Offene Rack-Einheiten (HE 37 bis 39)
5	16 Compute-Server (HE 21 bis 36)	6	8 Serving-Server (HE 13 bis 20)
7	12 Basisserver (HE 1 bis 12)		—

Die folgende Abbildung zeigt die Vorder- und Rückseite von Rack 1 bei C1-Workload mit zwei Racks.

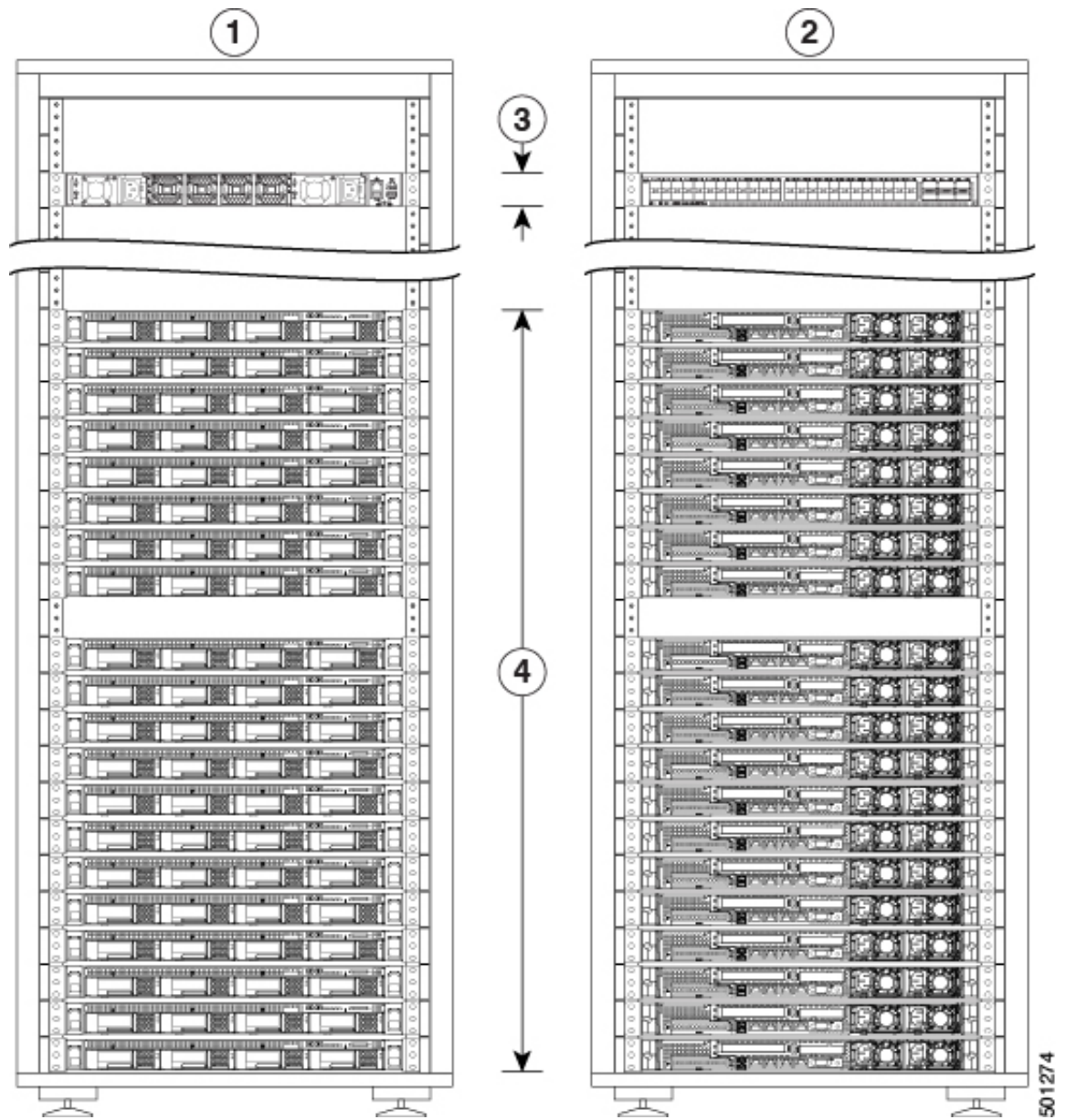
Abbildung 2: C1-Workload mit zwei Racks – Vorder- und Rückseite von Rack 1



1	Vorderseite (Ansicht Kaltgang)	2	Rückseite (Ansicht Warmgang)
3	1 Spine-Switch (HE 42)	4	Leaf 1-Switch (HE 40)
5	16 Compute-Server (HE 1 bis 4 und 6 bis 9)	6	—

Die folgende Abbildung zeigt die Vorder- und Rückseite von Rack 2 bei C1-Workload mit zwei Racks.

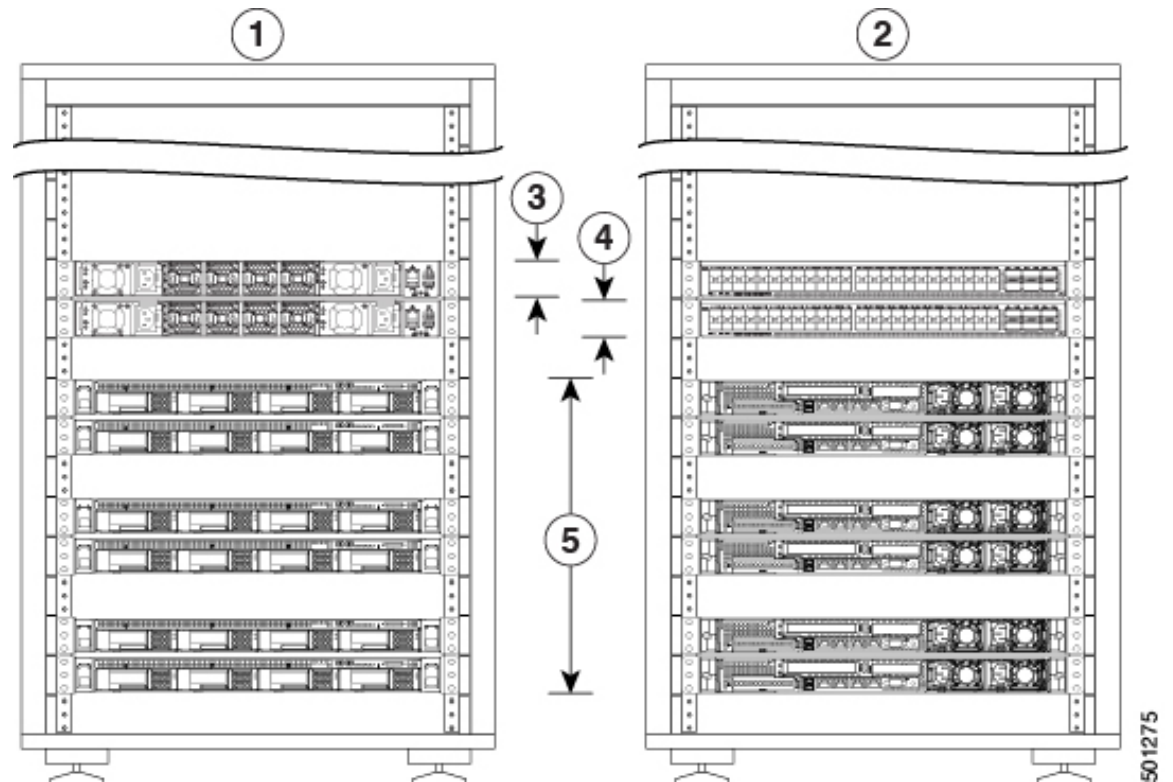
Abbildung 3: C1-Workload mit zwei Racks – Vorder- und Rückseite von Rack 2



1 Vorderseite (Ansicht Kaltgang)	2 Rückseite (Ansicht Warmgang)
3 Leaf 2-Switch (HE 40)	4 8 Serving-Server (HE 14 bis 21) und 12 Basisserver (HE 1 bis 12)

Die folgende Abbildung zeigt die Vorder- und Rückseite von C1-Workload-M.

Abbildung 4: C1-Workload-M – Vorder- und Rückseite



1	Vorderseite (Ansicht Kaltgang)	2	Rückseite (Ansicht Warmgang)
3	Leaf 1-Switch (HE 12)	4	Leaf 2-Switch (HE 11)
5	6 universelle Server (HE 2, 3, 5, 6, 8 und 9)		—

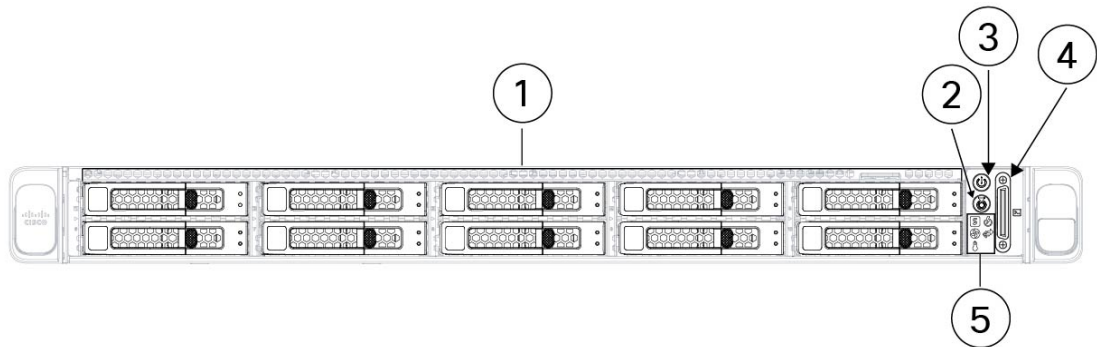
501275

Cisco UCS C220 M6-Server – Vorderseite

Die folgende Abbildung zeigt die Vorderseite des UCS C220 M6-Servers mit SFF-Laufwerken (Small Form Factor).

Weitere Informationen finden Sie im [Cisco UCS C220 M6-Server-Installations- und Serviceleitfaden](#).

Abbildung 5: Cisco UCS C220 M6-Server – Vorderseite



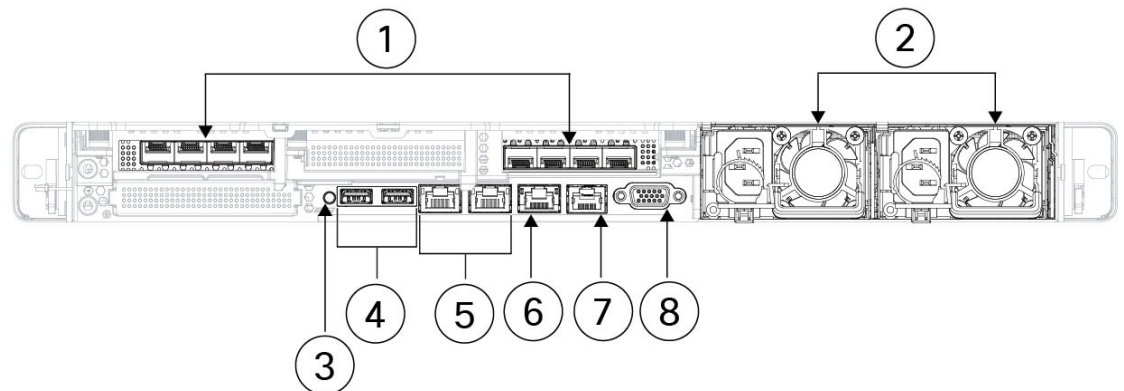
1 Laufwerkseinschübe 1 bis 10, nummeriert von links nach rechts und von oben nach unten Unterstützt SAS-/SATA-HDDs und -SSDs. Optional können die Laufwerkseinschübe 1 bis 4 bis zu 4 NVMe-Laufwerke enthalten. Die Laufwerkseinschübe 5 bis 10 unterstützen nur SAS-/SATA-HDDs oder -SSDs.	2 Taste/LED zur Geräteidentifizierung
3 Ein-Aus-Schalter/Status-LED	4 KVM-Steckverbinder Wird mit einem KVM-Kabel verwendet, das über einen DB-15-VGA-, einen seriellen DB-9- und zwei USB-2.0-Anschlüsse verfügt.
5 System-LEDs: <ul style="list-style-type: none"> • Lüfterstatus-LED • Systemstatus-LED • Netzteilstatus-LED • Netzwerkaktivitäts-LED • Temperaturstatus-LED 	—

Cisco UCS C220 M6-Server – Rückseite

Die folgende Abbildung zeigt die Rückseite des UCS C220 M6-Servers.

Weitere Informationen finden Sie im [Cisco UCS C220 M6-Server-Installations- und Serviceleitfaden](#).

Abbildung 6: Cisco UCS C220 M6-Server – Rückseite



1	<p>2 PCIe-Steckplätze</p> <ul style="list-style-type: none"> • Riser 1 (gesteuert von CPU 1) <ul style="list-style-type: none"> • Unterstützt einen PCIe-Steckplatz (Steckplatz 1) • Steckplatz 1 ist halb hoch, 3/4 lang, x16 • Riser 3 (gesteuert von CPU 2) <ul style="list-style-type: none"> • Unterstützt einen PCIe-Steckplatz (Steckplatz 3) • Steckplatz 3 ist halb hoch, 3/4 lang, x16 	2	Zwei Netzteile (PSUs), die bei Konfiguration im 1+1-Netzstrommodus redundant sind
3	Taste/LED zur Systemidentifizierung	4	Zwei USB 3.0-Ports
5	<p>Zwei 1-Gb/10-Gb-Ethernet-Ports (LAN1 und LAN2)</p> <p>Die zwei LAN-Ports unterstützen je nach Verbindungspartner 1 Gbit/s und 10 Gbit/s.</p>	6	Ein dedizierter 1-GbE-Management-Port
7	COM-Port (RJ-45-Anschluss)	8	VGA-Video-Port (DB-15-Stecker)



KAPITEL 2

Vorbereiten des Standorts

- Anforderungen bezüglich der Temperatur, auf Seite 9
- Anforderungen bezüglich der Luftfeuchtigkeit, auf Seite 9
- Anforderungen bezüglich der Höhe, auf Seite 10
- Anforderungen bezüglich Staub und Feinstaub, auf Seite 10
- Minimieren von elektromagnetischen und Funkinterferenzen, auf Seite 10
- Anforderungen bezüglich Erschütterungen und Vibration, auf Seite 11
- Anforderungen bezüglich der Erdung, auf Seite 11
- Stromversorgung, auf Seite 11
- Anforderungen bezüglich der Luftströmung, auf Seite 12
- Anforderungen bezüglich Abständen, auf Seite 12

Anforderungen bezüglich der Temperatur

Für die Cisco Secure Workload-Cluster-Switches und -Server gilt eine Betriebstemperatur von 5 bis 35 °C, wobei der Wert sich um 1 °C pro 305 m ü. NN. verringert. Wenn die Geräte nicht in Betrieb sind, darf die Temperatur zwischen -40 °C und 65 °C liegen.

Anforderungen bezüglich der Luftfeuchtigkeit

Bei hoher Luftfeuchtigkeit kann Feuchtigkeit in die Switches und Server eindringen. Feuchtigkeit kann zu Korrosion der internen Komponenten und zur Verschlechterung von Eigenschaften wie dem elektrischen Widerstand, der Wärmeleitfähigkeit, der physischen Festigkeit und der Größe führen. Die Switches und Server sind auf den Betrieb bei einer relativen Luftfeuchtigkeit zwischen 10 und 90 % mit einer Feuchtigkeitsänderung von 10 % pro Stunde ausgelegt. Außerhalb des Betriebs widerstehen die Geräte einer relativen Luftfeuchtigkeit zwischen 5 und 93 %.

In Gebäuden, deren Raumklima in den wärmeren Monaten durch eine Klimaanlage und in den kälteren Monaten durch eine Heizung geregelt wird, ist die Luftfeuchtigkeit normalerweise akzeptabel für den Betrieb der Geräte. Wenn die Geräte jedoch an einem ungewöhnlich feuchten Ort aufgestellt werden, sollten Sie einen Luftentfeuchter verwenden, um die Luftfeuchtigkeit innerhalb eines akzeptablen Bereichs zu halten.

Anforderungen bezüglich der Höhe

Wenn Sie Rack-Geräte in größerer Höhe (geringer Luftdruck) betreiben, ist die Effizienz von Zwangs- und Konvektionskühlung herabgesetzt. Dies kann zu elektrischen Problemen mit Lichtbögen und Koronaeffekten führen. Außerdem kann es zum Versagen oder zu einer geringeren Effizienz versiegelter Komponenten mit Innendruck, etwa Elektrolytkondensatoren, kommen. Diese Geräte sind für den Betrieb in Höhen von 0 bis 3.050 m ausgelegt und können in Höhen von bis zu 12.200 m gelagert werden.

Anforderungen bezüglich Staub und Feinstaub

Die Lüfter kühlen Netzteile, Switches und Server, indem Luft angesaugt und dann durch verschiedene Öffnungen im Chassis wieder abgegeben wird. Dabei saugen sie jedoch auch Staub und andere Partikel an, wodurch sich Verunreinigungen im Switch ansammeln und die Chassistemperatur steigt. Eine saubere Betriebsumgebung kann die negativen Auswirkungen von Staub und anderen Partikeln, die als Isolatoren fungieren und die mechanischen Komponenten der Switches und Server stören, erheblich reduzieren.

Befolgen Sie neben einer regelmäßigen Reinigung diese Sicherheitshinweise, um eine Verunreinigung Ihrer Rack-Switches und -Server zu vermeiden:

- Verboten Sie das Rauchen in der Nähe des Racks.
- Verboten Sie Essen und Trinken in der Nähe des Racks.

Minimieren von elektromagnetischen und Funkinterferenzen

Elektromagnetische Interferenzen (EMI) und Funkinterferenzen (RFI) von den Geräten im Cisco Secure Workload-Cluster können andere Geräte, beispielsweise Radio- und Fernsehempfänger, in der Nähe des Racks beeinträchtigen. Die von den Geräten im Rack ausgehenden Funkfrequenzen können außerdem Schnurlostelefone und Telefone mit niedriger Sendeleistung stören. Umgekehrt können RFI von Telefonen mit hoher Sendeleistung fehlerhafte Zeichen auf den Gerätemonitoren verursachen.

Als RFI gelten EMI mit einer Frequenz von mehr als 10 kHz. Diese Art von Interferenz kann vom Switch über das Netzkabel und die Stromquelle oder durch die Luft als Funkwellen an andere Geräte übertragen werden. Die Federal Communications Commission (FCC) veröffentlicht spezifische Regelungen, um die Menge der EMI und RFI, die von Computerausstattung abgegeben werden darf, zu begrenzen. Jeder Switch erfüllt diese FCC-Bestimmungen.

Wenn Kabel über eine erhebliche Strecke durch ein elektromagnetisches Feld geführt werden, kann es zu Interferenz zwischen dem Feld und den Signalen in den Kabeln kommen, was folgende Auswirkungen hat:

- Schlechte Verkabelung kann dazu führen, dass von der Verkabelung der Anlage Funkstörungen ausgehen.
- Starke EMI, insbesondere wenn sie von Blitzen oder Funksendern verursacht wird, kann die Signaltreiber und Empfänger im Chassis zerstören und sogar zu Stromschlag Gefahr führen, wenn Spannungsschläge durch Leitungen in Geräte gelangen.



Hinweis Wenden Sie sich an einen RFI-Experten, um starke EMI vorhersagen und verhindern zu können.

Es ist unwahrscheinlich, dass Funkinterferenzen von Kabeln ausgehen, wenn Sie Twisted-Pair-Kabel mit ordnungsgemäßer Verteilung von Erdungsleitern verwenden. Wenn Sie die empfohlenen Abstände überschreiten, verwenden Sie ggf. ein hochwertiges Twisted-Pair-Kabel mit einem Erdungsleiter pro Datensignal.



Vorsicht Wenn Sie die empfohlenen Entfernungen überschreiten oder Kabel zwischen Gebäuden verlegen müssen, berücksichtigen Sie unbedingt die Folgen eines möglichen Blitzschlags in der Nähe. Durch den elektromagnetischen Impuls eines Blitzschlags o. ä. können sehr leicht extrem hohe Spannungen in ungeschirmte Leitungen induziert werden und elektronische Geräte zerstören. Wenn in der Vergangenheit bereits Probleme dieser Art aufgetreten sind, sollten Sie Experten für elektrischen Überspannungsschutz und Abschirmung konsultieren.

Anforderungen bezüglich Erschütterungen und Vibration

Die Geräte im Cisco Secure Workload-Cluster wurden in Bezug auf Normen zu Betriebsbereichen, Handhabung und Erdbebensicherheit hinsichtlich Erschütterungen und Vibrationen geprüft.

Anforderungen bezüglich der Erdung

Die Geräte im Cisco Secure Workload-Cluster reagieren empfindlich auf Schwankungen der von den Stromquellen gelieferten Spannung. Überspannung, Unterspannung und Transienten (Spitzen) können Daten aus dem Speicher löschen oder zum Ausfall von Komponenten führen. Zum Schutz vor Problemen dieser Art sollten Sie sicherstellen, dass die Geräte stets geerdet sind. Sie müssen das Rack mit der Erdung der Einrichtung verbinden.

Die Erdungspunkte am Chassis sind auf M5-Schrauben ausgelegt. Sie müssen Ihre eigenen Schrauben, Erdungsklemme und Erdungskabel bereitstellen. Die Erdungsklemme muss eine Doppelloch-Klemme sein, die für M5-Schrauben passt. Das Erdungskabel, das Sie bereitstellen, muss ein 2-mm-Kabel (14 AWG) für mindestens 60 °C sein (oder den örtlichen Vorschriften entsprechend).

Stromversorgung

Die Cisco Secure Workload-Cluster müssen mit Stromquellen bereitgestellt werden, bei denen die folgenden Strommengen für den Betrieb gegeben sind:

- 39-HE-LFF-Plattform, einzelnes Rack: 22.500 W
- 39-HE-LFF-Plattform, zwei Racks: 11.500 W pro Rack
- 8-HE-SFF-Plattform: 6.500 W

Für die erforderliche $N+N$ -Redundanz der Stromversorgung benötigen Sie zwei Wechselstromquellen, die jeweils die gleiche Menge Strom liefern.

Jedes Chassis im Rack verfügt über zwei Netzteile: eines für den Betrieb und eines zu Redundanzzwecken. Jedes Netzteil ist mit einer anderen Mehrfachsteckdose im Rack verbunden, und jede Mehrfachsteckdose ist

mit einer anderen Wechselstromquelle verbunden. Wenn eine Stromquelle ausfällt, liefert die andere den erforderlichen Strom für die Switches oder Server im Rack.

Anforderungen bezüglich der Luftströmung

Beim Cisco Secure Workload-Cluster muss jedes Rack so aufgestellt werden, dass die Netzteile und Lüfter der drei Switches in einen Kaltgang weisen. In dieser Position nehmen alle Geräte im Rack Kühlluft aus einem Kaltgang auf und leiten Warmluft in einen Warmgang ab.

Anforderungen bezüglich Abständen

Aus der folgenden Tabelle geht hervor, wie viel Platz für den Aufbau des Cisco Secure Workload-Clusters mit 39 HE (LFF; einzelnes Rack oder zwei Racks) oder mit 8 HE (SFF) erforderlich ist. Der Installationsgang muss mehr als 59,69 cm breit sein, damit das Rack in Position gebracht werden kann. Darüber hinaus muss genügend Platz vorhanden sein, damit eine Person an der Vorder- und Rückseite Wartungsarbeiten durchführen kann.

Tabelle 1: Anforderungen bezüglich Abständen

Installationstyp	Mindestbreite des Gangs ¹	Minimaler Platzbedarf für die Rack-Installation
C1-Workload-Installation (einzelnes Rack)	59,69 cm	59,69 cm x 126,49 cm (Breite x Tiefe)
C1-Workload (zwei Racks)	59,69 cm	119,38 cm x 126,49 cm (Breite x Tiefe)
C1-Workload-M	59,69 cm	59,69 cm x 126,49 cm (Breite x Tiefe)

¹ Der Installationsgang und der Gang, in den sich die vordere Klappe des Racks öffnet, müssen jeweils mindestens 59,69 cm breit sein. Der andere Gang, in den sich die Türen des Doppelschranks öffnen, muss mindestens 29,85 cm breit sein, damit die Türen vollständig geöffnet werden können. Für die Durchführung von Wartungsarbeiten sind jedoch mindestens 59,69 cm erforderlich.

Das Rack ist so positioniert, dass die Switch-Lüfter (die Seite des Racks mit der größten Tür) zum Kaltgang zeigen und die Switch-Ports (die Seite des Racks mit den Doppeltüren) zum Warmgang.



KAPITEL 3

Erden und Anschließen

- [Erden der Cisco Secure Workload-Cluster-Geräte, auf Seite 13](#)
- [Einschalten der Cisco Secure Workload-Cluster-Geräte, auf Seite 13](#)
- [Verbinden des Cisco Secure Workload-Clusters mit Ihren Routern, auf Seite 14](#)

Erden der Cisco Secure Workload-Cluster-Geräte

Die Cisco Secure Workload-Cluster-Geräte haben Metall-an-Metall-Verbindungen zum jeweiligen Rack. Sobald Sie also das Rack/die Racks über die Erdung Ihres Rechenzentrums erden, werden die Geräte im Rack geerdet. Um ein Rack zu erden, verbinden Sie die Räder des Racks mit der Erdung.

Einschalten der Cisco Secure Workload-Cluster-Geräte


Um den Switch einzuschalten, müssen Sie die mit dem Rack verbundenen zwei Mehrfachsteckdosen an zwei Wechselstromquellen anschließen.



-
- Hinweis** Diese Geräte müssen an ein Wechselstromnetz mit am Betriebsmittel befindlichem Überspannungsschutz angeschlossen werden, der NFPA 70 (National Electrical Code, NEC) entspricht.
- Lesen Sie die Installationshinweise, bevor Sie das System nutzen, installieren oder an die Stromversorgung anschließen.
- Überlasten Sie die Kabel nicht, wenn Sie die Geräte an den Versorgungsstromkreis anschließen.
-

Vorbereitungen

- Die Racks müssen im Rechenzentrum aufgestellt und fixiert werden, wobei die Luftzufuhr aus dem Kaltgang erfolgen muss.
- Die Racks müssen über die Erdung des Rechenzentrums geerdet werden.
- Das Cluster muss mit zwei vom Kunden bereitgestellten Routern verbunden werden (wobei jeder Router mit einem separaten Leaf-Switch verbunden wird).
- Es müssen zwei Stromquellen vorhanden sein, die die Stromanforderungen des Racks in der Reichweite der Mehrfachsteckdose erfüllen.

-
- Schritt 1** Verbinden Sie das Netzkabel einer Mehrfachsteckdose mit einer Wechselstromquelle und das Netzkabel der zweiten Mehrfachsteckdose mit einer anderen Wechselstromquelle.
- Schritt 2** Vergewissern Sie sich, dass die -LED der in den Rack-Geräten installierten Netzteile grün leuchtet.
- Wenn keine der LEDs leuchtet, überprüfen Sie, ob die Stromzufuhr eingeschaltet ist und der Netzschalter an der Rack-Mehrfachsteckdose auf „Ein“ steht.
 - Wenn einige der LEDs leuchten und andere nicht, vergewissern Sie sich, dass das Netzkabel des zugehörigen Netzteils vollständig mit der Mehrfachsteckdose im Rack verbunden ist.
-

Verbinden des Cisco Secure Workload-Clusters mit Ihren Routern

Sie müssen das Cisco Secure Workload-Cluster mit zwei Routern verbinden.

-
- Schritt 1** Wenn Sie ein 39-HE-LFF-Cluster mit zwei Racks installieren, schließen Sie die teilweise verbundenen Schnittstellenkabel an jedem Rack an. Verbinden Sie jedes dieser Kabel mit dem beschrifteten Port am anderen Rack.
- Schritt 2** Verwenden Sie ein 10-Gigabit-Kabel, um einen Router mit Port E1/39 auf dem Leaf 1-Switch (bei einer 39-HE-Bereitstellung) bzw. mit Port E1/47 (bei einer 8-HE-Bereitstellung) zu verbinden. Der Leaf 1-Switch befindet sich an der folgenden Stelle:
- 39-HE-LFF-Plattform mit einzeltem Rack: HE 40 im Plattform-Rack
 - 39-HE-LFF-Plattform mit zwei Racks: HE 40 in Rack 1
 - 8-HE-SFF-Plattform: HE 12 im Plattform-Rack
- Schritt 3** Verwenden Sie ein 10-Gigabit-Kabel, um einen Router mit Port E1/39 auf dem Leaf 2-Switch (bei einer 39-HE-Bereitstellung) bzw. mit Port E1/47 (bei einer 8-HE-Bereitstellung) zu verbinden. Der Leaf 2-Switch befindet sich an der folgenden Stelle:
- 39-HE-LFF-Plattform mit einzeltem Rack: HE 41 im Plattform-Rack
 - 39-HE-LFF-Plattform mit zwei Racks: HE 41 in Rack 2
 - 8-HE-SFF-Plattform: HE 11 im Plattform-Rack
-



KAPITEL 4

Einrichten der Benutzeroberfläche

- (Optional) Anforderungen und Einschränkungen für den Dual-Stack-Modus (IPv6-Unterstützung), auf Seite 15
- Einrichten der Benutzeroberfläche, auf Seite 16

(Optional) Anforderungen und Einschränkungen für den Dual-Stack-Modus (IPv6-Unterstützung)

Cisco Secure Workload-Cluster, die auf physischer Hardware ausgeführt werden, können so konfiguriert werden, dass für bestimmte Kommunikationen zum und vom Cluster IPv6 zusätzlich zu IPv4 verwendet wird.



Hinweis Sie können den Dual-Stack-Modus (IPv6-Unterstützung) bei der Installation oder dem Upgrade auf Version 3.6.1.5, 3.7.1.5 und 3.8.1.1 verwenden. Die Option zum Aktivieren der Funktion ist jedoch nicht verfügbar, wenn Sie eine Installation von oder ein Upgrade auf Patch-Versionen durchführen.

Einschränkungen

Wenn Sie die Aktivierung des Dual-Stack-Modus in Betracht ziehen, beachten Sie die folgenden Hinweise:

- Sie können die IPv6-Verbindung nur bei der Erstbereitstellung aktivieren oder ein Upgrade auf eine Hauptversion durchführen (Sie können diese Funktion während Patch-Upgrades nicht aktivieren).
- Der Dual-Stack-Modus wird nur auf physischer Hardware oder Bare-Metal-Clustern unterstützt.
- Der reine IPv6-Modus wird nicht unterstützt.
- Sie können nicht mehr zum reinen IPv4-Modus zurückkehren, nachdem der Dual-Stack-Modus für das Cluster aktiviert wurde.
- Data Backup and Restore (DBR) wird nicht unterstützt, wenn eine Dual-Stack-Verbindung aktiviert ist.
- Aktivieren Sie den Dual-Stack-Modus für Cluster, die mit Federation konfiguriert sind.
- Die folgenden Funktionen verwenden immer und nur IPv4 (beachten Sie, dass IPv4 immer aktiviert ist, auch wenn IPv6 aktiviert ist):
 - (Gültig für die Versionen 3.8.1.1, 3.7.1.5 und 3.6.x) Durchsetzung auf AIX-Agenten

- (gilt nur für Version 3.6.x) Kommunikation des Hardware-Agenten mit dem Cluster
- (gilt nur für Version 3.6.x) Connectors für Flow-Erfassung, Bestandsbereicherung oder Warnbenachrichtigungen

Anforderungen

- Konfigurieren Sie sowohl A- als auch AAAA-DNS-Einträge für FQDN, bevor Sie den Dual-Stack-Modus für Ihr Cluster aktivieren.
- Externe Dienste wie NTP, SMTP und DNS müssen aus Redundanzgründen über IPv4 und IPv6 verfügbar sein.
- So konfigurieren Sie den Dual-Stack-Modus für einen Cluster:
 - Jedem der beiden Cluster-Leaf-Switches müssen routbare IPv6-Adressen in zwei verschiedenen Netzwerken für Redundanz zugewiesen werden. Für jedes Netzwerk müssen Standardgateways bereitgestellt werden.
 - Für 39-HE-Cluster ist ein routbares IPv6-Netzwerk mit Platz für mindestens 29 Host-Adressen erforderlich.
 - Für 8-HE-Cluster ist ein routbares IPv6-Netzwerk mit Platz für mindestens 20 Host-Adressen erforderlich.
 - Die ersten drei Host-Adressen des routbaren IPv6-Netzwerks sind für die HSRP-Konfiguration des Cisco Secure Workload-Clusters reserviert und dürfen von keinen anderen Geräten verwendet werden.

Zusätzliche Informationen

Die Agenten kommunizieren mit dem Cluster über IPv4, es sei denn, Sie konfigurieren sie für die Verwendung von IPv6. Anweisungen finden Sie im Benutzerhandbuch zu Cisco Secure Workload.

Einrichten der Benutzeroberfläche

Vorbereitungen

- Um diese Konfiguration abzuschließen, benötigen Sie ein Gerät wie einen Laptop mit einem Ethernet-Port und Zugang zum Internet.
- Sie benötigen außerdem ein Ethernet-Kabel, um das Gerät mit dem höchsten Server im Cisco Secure Workload-Cluster zu verbinden.
- Google Chrome ist der einzige unterstützte Browser für das Einrichtungsportal, das für einen Teil dieses Prozesses erforderlich ist.
- (Optional) Ab Version 3.6 können Sie Ihren Cluster im Dual-Stack-Modus konfigurieren, sodass sowohl IPv4 als auch IPv6 für die Kommunikation zwischen bestimmten Cisco Secure Workload-Komponenten sowie zwischen Cisco Secure Workload und Netzwerkdiensten wie NTP und DNS verwendet werden können. (Cisco Secure Workload verarbeitet bereits IPv6-Datenverkehr, unabhängig davon, ob Sie den

Dual-Stack-Modus aktivieren oder nicht.) Sie können diese Unterstützung nur während der Bereitstellung oder des Upgrades aktivieren.

Wenn Sie erwägen, die Unterstützung für IPv6 zu aktivieren, siehe [\(Optional\) Anforderungen und Einschränkungen für den Dual-Stack-Modus \(IPv6-Unterstützung\)](#), auf Seite 15.



Wichtig Geben Sie im folgenden Verfahren in alle Felder IPv4-Adressen ein, es sei denn, im Feldnamen ist explizit IPv6 angegeben.

Schritt 1 Konfigurieren Sie das Internetgerät mit der IP-Adresse 2.2.2.1/30 (255.255.255.252).

Schritt 2 Verwenden Sie ein Ethernet-Kabel, um den Ethernet-Port des Internetgeräts mit LOM-Port 2 (LAN2) auf dem höchsten Server oben im Secure Workload-Cluster zu verbinden.

Schritt 3 Öffnen Sie auf dem Internetgerät den Chrome-Browser, und rufen Sie `http://2.2.2.2:9000` auf.

Hinweis Der Chrome-Browser ist der einzige Browser, der für diesen Prozess getestet wurde.

Die Seite mit der Setup-Diagnose wird geöffnet.

Schritt 4 Wenn auf der Diagnosesite Fehler angezeigt werden, überprüfen Sie die Kabelverbindungen zwischen den Cluster-Geräten auf unterbrochene Verbindungen oder falsch verlegte Kabel, bevor Sie mit diesem Verfahren fortfahren. Kehren Sie anschließend zu Schritt 2 zurück.

Informationen zur richtigen Verkabelung finden Sie hier: [C1 – Workload-Cluster – Geräteverkabelung](#), auf Seite 23 und [C1 – Workload-M-Cluster – Geräteverkabelung](#), auf Seite 36.

Schritt 5 Klicken Sie auf **Continue** (Weiter).

Die RPM-Upload-Seite wird geöffnet.

Hinweis Wenn stattdessen die Seite für die Standortkonfiguration geöffnet wird, geben Sie die folgende URL ein, um die RPM-Upload-Seite zu öffnen:

`http://2.2.2.2:9000 /upload`

Schritt 6 Laden Sie RPM-Dateien in die Cisco Secure Workload-Cloud hoch.

Sie müssen die Dateien in der folgenden Reihenfolge hochladen:

- `tetration_os_rpminstall_k9`
- `tetration_os_UcsFirmware_k9`
- `tetration_os_adhoc_k9`
- `tetration_os_mother_rpm_k9`
- `tetration_os_base_rpm_k9`

- a) Klicken Sie auf **Choose File** (Datei auswählen).
- b) Navigieren Sie zu einer RPM-Datei, wählen Sie sie aus, und klicken Sie auf **Open** (Öffnen).
- c) Klicken Sie auf **Upload** (Hochladen).

Die Liste der RPMs auf der Seite wird nicht aktualisiert, wenn Sie die einzelnen RPMs hochladen. Dies ist ein erwartungsgemäßes Verhalten.

Wenn nach dem Hochladen der Datei

`tetration_os_mother_rpm_k9-2.1.1.31-1.el6.x86_64.rpm` ein Fehler angezeigt wird, warten Sie etwa 5 bis 10 Minuten, und laden Sie die Seite dann neu. Nach dem erneuten Laden der Seite sollte die Liste der hochgeladenen RPMs angezeigt werden. Der Fehler ist auf einen Neustart des Orchestrators zurückzuführen und stellt kein Problem dar.

d) Wiederholen Sie die Schritte a bis c für jede RPM-Datei.

Nachdem Sie die RPMs hochgeladen haben, wird die Seite zur Standortkonfiguration geöffnet.

Schritt 7

Verwenden Sie die Seite „Standortkonfiguration“, um den neuen Standort wie folgt einzurichten:

- Klicken Sie auf **General** (Allgemein).

1. Geben Sie im Feld **Site Name** (Standortname) den eindeutigen Namen des Clusters ein.
2. Fügen Sie im Feld **SSH Public Key** (Öffentlicher SSH-Schlüssel) den Authentifizierungsschlüssel ein.

Hinweis Generieren Sie Ihr eigenes SSH-Schlüsselpaar, das für den Cluster-SSH-Zugriff verwendet werden kann.

Wir empfehlen Ihnen dringend, den SSH-Schlüssel an einem sicheren, langlebigen und leicht zugänglichen Ort aufzubewahren, um das Cluster mithilfe des `ta_guest`-Zugriffs reparieren oder wiederherstellen zu können.

3. Klicken Sie auf **Next** (Weiter).

- Klicken Sie auf **Email** (E-Mail).

1. Geben Sie die erforderlichen E-Mail-Adressen ein.
2. Klicken Sie auf **Next** (Weiter).

- Klicken Sie auf **L3**.

Geben Sie die angeforderten Adressen ein. Alle Felder mit * sind Pflichtfelder.

Geben Sie alle Adressen als IPv4 ein, es sei denn, im Feldnamen ist IPv6 angegeben.

(Optional) Wenn Sie die Software-Version 3.6 oder höher installieren: So aktivieren Sie den Dual-Stack-Modus (Unterstützung für IPv4 und IPv6):

1. Aktivieren Sie das Kontrollkästchen „IPv6“.
2. Geben Sie die IPv6-Adresse in CIDR-Notation für die Switches Leaf 1 und Leaf 2 ein.
3. Geben Sie das IPv6-Standardgateway für Leaf 1 und Leaf 2 ein.
4. Klicken Sie auf **Next** (Weiter).

- Klicken Sie auf **Netzwerk**.

Geben Sie alle Adressen als IPv4 ein, es sei denn, im Feldnamen ist IPv6 angegeben.

1. Fügen Sie im Feld **Internal network IP address** (IP-Adresse des internen Netzwerks) die Adresse aus der Orchestrator-Bereitstellungsausgabe ein.

2. Fügen Sie im Feld **External network IP address** (IP-Adresse des externen Netzwerks) die Adresse aus der Orchestrator-Bereitstellungsausgabe ein.
3. Fügen Sie im Feld **External gateway IP address** (IP-Adresse des externen Gateways) die Adresse aus der Orchestrator-Bereitstellungsausgabe ein.
4. Fügen Sie im Feld **DNS resolver IP address** (IP-Adresse des DNS-Resolvers) die Adresse aus der Orchestrator-Bereitstellungsausgabe ein.
5. Geben Sie im Feld **DNS domain** (DNS-Domäne) Ihre DNS-Domäne ein (z. B. **cisco.com**).
6. (Software-Version 3.6 oder höher) Wenn Sie auf der Seite L3 IPv6 aktiviert haben, wird **IPv6** automatisch ausgewählt.

Wenn IPv6 ausgewählt ist, müssen Sie IPv6-Adressen angeben, die für die Verwendung durch Cisco Secure Workload reserviert sind:

- Geben Sie das **externe IPv6-Netzwerk** ein.

Die ersten drei IPv6-Adressen im Feld für das externe IPv6-Netzwerk sind immer für die Switches des Cisco Secure Workload-Clusters reserviert und sollten für keine anderen Zwecke verwendet werden.

- Wenn Sie IPv6 nur für bestimmte Adressen verwenden möchten, geben Sie diese Adressen in das Feld **External IPv6 IPs** (Externe IPv6-IPs) ein.

Hinweis

- Stellen Sie für einen Cluster mit 39 HE sicher, dass mindestens 29 IPv6-Adressen im externen IPv6-Netzwerk oder in der Liste der externen IPv6-IPs verfügbar sind.
- Stellen Sie bei einem 8-HE-Cluster sicher, dass mindestens 20 IPv6-Adressen im externen IPv6-Netzwerk oder in der Liste der externen IPv6-IPs verfügbar sind.

7. Klicken Sie auf **Next** (Weiter).

- Klicken Sie auf **Service**.

1. Geben Sie im Feld **NTP Servers** (NTP-Server) die durch Leerzeichen getrennte Liste der NTP-Servernamen oder IP-Adressen aus der Orchestrator-Bereitstellungsausgabe ein.
2. Geben Sie im Feld **SMTP Server** (SMTP-Server) den Namen oder die IP-Adresse eines SMTP-Servers ein, der von Cisco Secure Workload zum Senden von E-Mail-Nachrichten verwendet werden kann. Cisco Secure Workload muss auf diesen Server zugreifen können.
3. Geben Sie im Feld **SMTP Port** (SMTP-Port) die Portnummer des SMTP-Servers ein. AWS beschränkt die Verwendung der Ports 25 und 465. Sie müssen Ihr Konto richtig konfigurieren oder Port 587 verwenden.
4. (Optional) Geben Sie im Feld **SMTP Username** (SMTP-Benutzername) den Benutzernamen für die SMTP-Authentifizierung ein.
5. (Optional) Geben Sie im Feld **SMTP Password** (SMTP-Kennwort) das Kennwort für die SMTP-Authentifizierung ein.
6. (Optional) Geben Sie im Feld **HTTP Proxy Server** (HTTP-Proxy-Server) den Namen oder die IP-Adresse eines HTTP-Proxy-Servers ein, der von Cisco Secure Workload für den Zugriff auf externe Services im Internet verwendet werden kann.

7. (Optional) Geben Sie im Feld **HTTP Proxy Port** (HTTP-Proxy-Port) die Portnummer für den HTTP-Proxy-Server ein.
 8. (Optional) Geben Sie im Feld **HTTPs Proxy Server** (HTTPs-Proxy-Server) den Namen oder die IP-Adresse eines HTTPs-Proxy-Servers ein, der von Cisco Secure Workload für den Zugriff auf externe Services im Internet verwendet werden kann.
 9. (Optional) Geben Sie im Feld **HTTPs Proxy Port** (HTTPs-Proxy-Port) die Portnummer für den HTTP-Proxy-Server ein.
 10. (Optional) Geben Sie im Feld **Syslog Server** (Syslog-Server) den Namen oder die IP-Adresse eines Syslog-Servers ein, der von Cisco Secure Workload zum Senden von Warnungen verwendet werden kann.
 11. (Optional) Geben Sie im Feld **Syslog Port** (Syslog-Port) die Portnummer für den Syslog-Server ein.
 12. (Optional) Geben Sie im Feld **Syslog Severity** (Syslog-Schweregrad) den Schweregrad für die Syslog-Nachrichten ein. Zu den möglichen Werten gehören: Information, Benachrichtigung, Warnmeldung, Fehler, Kritisch, Warnung und Notfall.
 13. Klicken Sie auf **Next** (Weiter).
- Klicken Sie auf **UI**.
 1. Geben Sie im Feld **UI VRRP VRID** den Wert **77** ein, sofern Sie keine eindeutige VRID benötigen.
 2. Geben Sie im Feld **UI FQDN** (FQDN der Benutzeroberfläche) den vollständigen Domännennamen ein, unter dem Sie auf das Cluster zugreifen.
 3. Lassen Sie das Feld **UI Airbrake Key** (Airbrake-Schlüssel der Benutzeroberfläche) leer.
 4. Klicken Sie auf **Next** (Weiter).
Tetration (Cisco Secure Workload) validiert Ihre Konfigurationseinstellungen und zeigt den Status der Einstellungen an.
 - Klicken Sie auf **Advanced** (Erweitert).
 1. Geben Sie im Feld **External IPs** (Externe IPs) IPv4-Adressen ein.
 2. Klicken Sie auf **Continue** (Weiter).

Schritt 8

Wenn Fehler auftreten, klicken Sie auf **Back** (Zurück), und bearbeiten Sie die Konfiguration (siehe Schritt 7).

Hinweis Sie können diese Einstellungen nach dem Verlassen der Seite nicht mehr in der Setup-GUI ändern. Sie können die Einstellungen jedoch später auf der Unternehmensseite in der GUI ändern.

Schritt 9

Wenn keine Fehler in Ihrer Konfiguration festgestellt wurden und Sie keine Änderungen vornehmen müssen, klicken Sie auf **Continue** (Weiter).

Cisco Secure Workload wird gemäß den von Ihnen festgelegten Einstellungen konfiguriert. Dieser Prozess dauert ein bis zwei Stunden, ohne dass Sie eingreifen müssen.

Nächste Maßnahme

Wenn Sie Softwareversion 3.6 oder höher bereitgestellt und die IPv6-Verbindung aktiviert haben:

- Sie können über IPv4 oder IPv6 auf das Cisco Secure Workload-Webportal zugreifen.
- Standardmäßig kommunizieren Software-Agents mit dem Cisco Secure Workload-Cluster über IPv4, selbst wenn der Cluster für die Unterstützung von IPv6 aktiviert ist. Wenn Sie möchten, dass unterstützte Agents für diesen Zweck IPv6 verwenden, müssen Sie im Cisco Secure Workload-Webportal auf der Seite **Plattform > Clusterkonfiguration** das Feld **Sensor VIP FQDN** konfigurieren. Wichtige Anweisungen finden Sie im Benutzerhandbuch, das als Online-Hilfe im Cisco Secure Workload-Webportal oder über <https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html> verfügbar ist.



KAPITEL 5

C1 – Cisco Secure Workload-Cluster – Geräteverkabelung

- [C1 – Workload-Cluster – Geräteverkabelung, auf Seite 23](#)
- [C1 – Workload-M-Cluster – Geräteverkabelung, auf Seite 36](#)

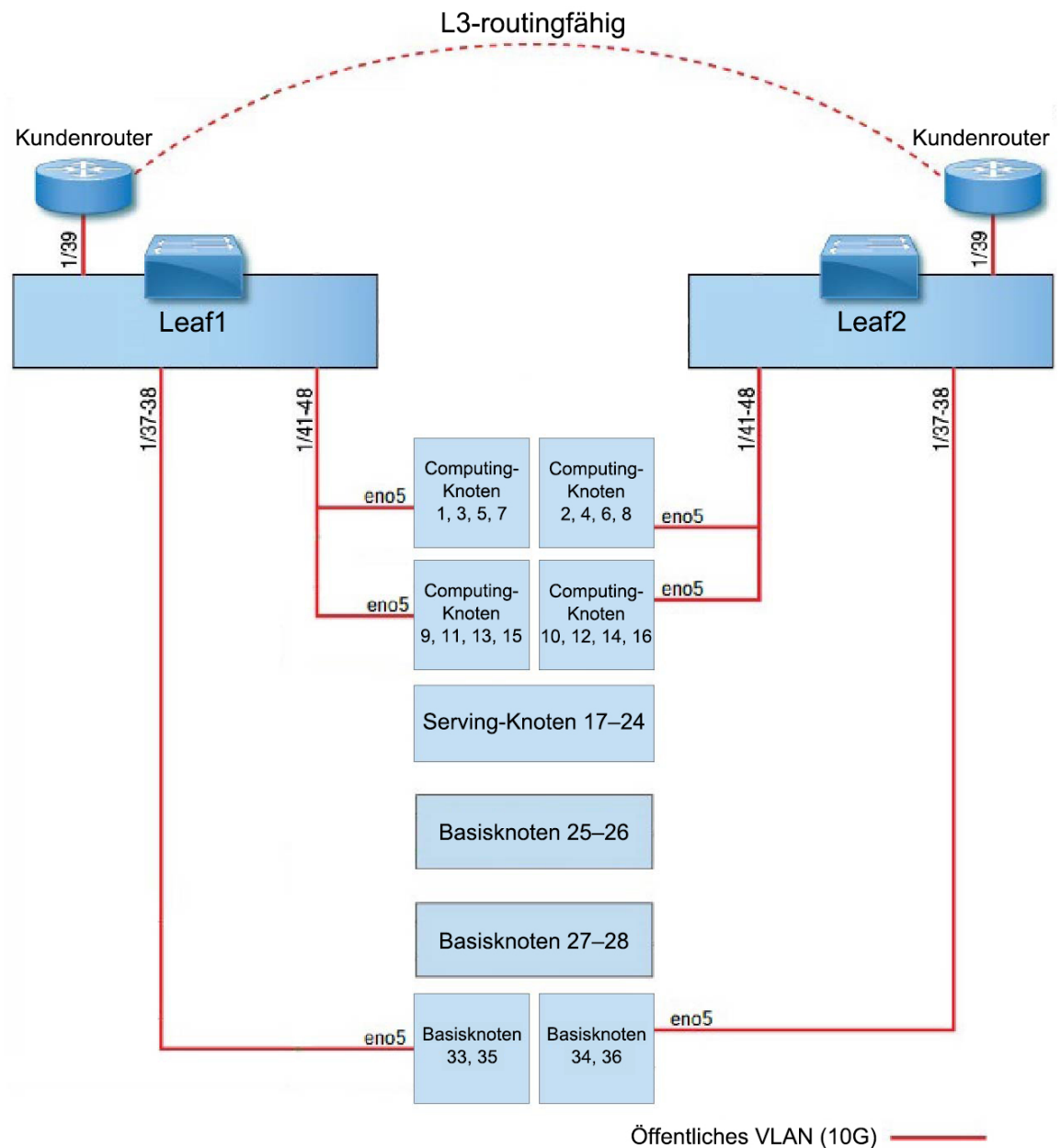
C1 – Workload-Cluster – Geräteverkabelung

Beachten Sie die folgenden Konfigurationsinformationen, wenn Sie die M6 Virtual Interface Card (VIC) im 39-HE-Rack verkabeln:

- Es gibt zwei private Schnittstellen für alle Knoten.
- Das 39-HE-Rack verfügt über eine öffentliche Schnittstelle für 20 Knoten.
- Bei der M6-Hardware sind vier Ports pro VIC vorhanden.
- Die Namen für die Bare-Metal-Schnittstelle – die physischen Server im Cluster, die als Basis-, Compute- und Serving-Knoten bekannt sind – beginnen mit „eno“ (Ethernet onboard).

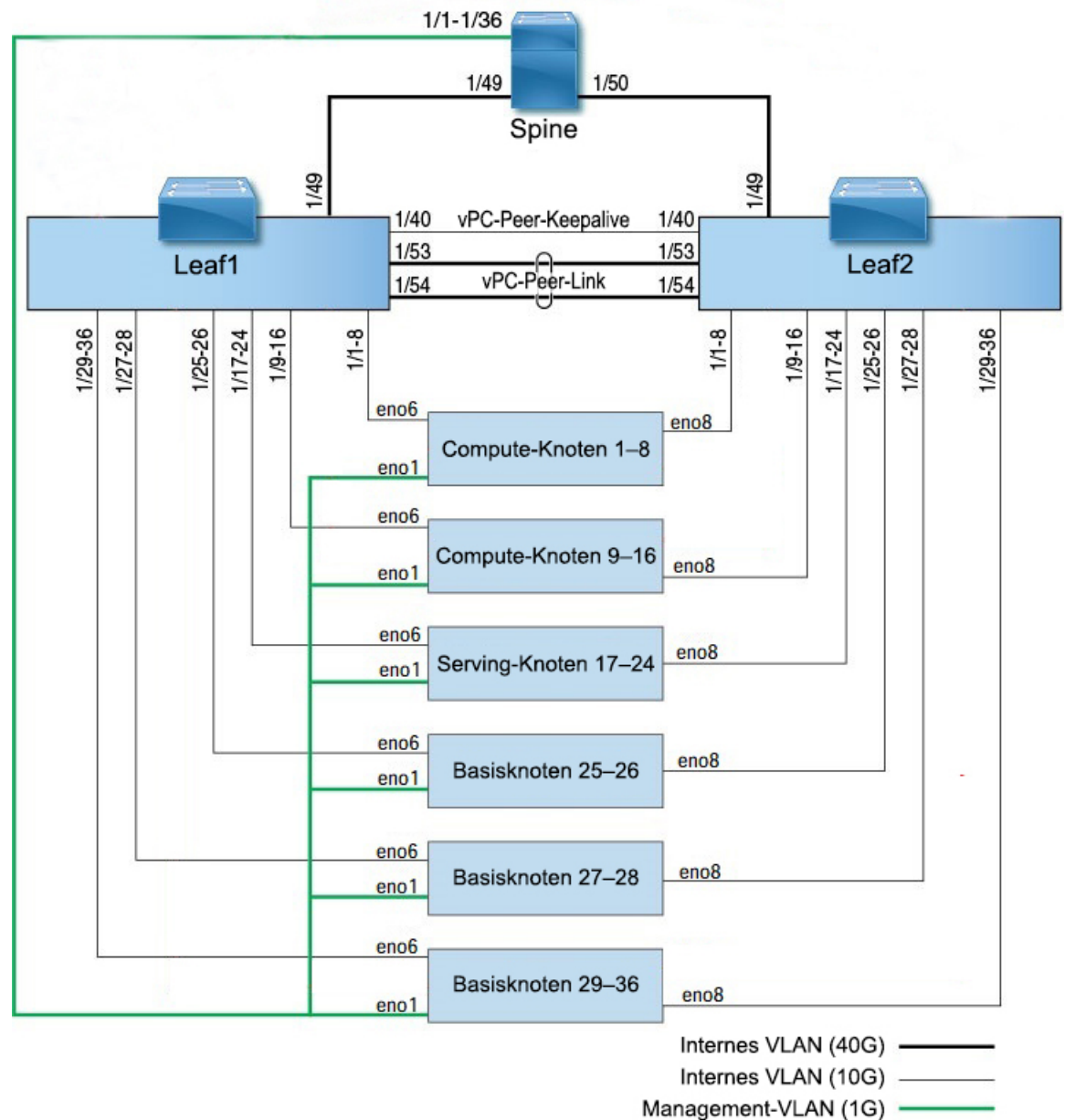
Das folgende Diagramm zeigt die Geräteverkabelung für die öffentliche/externe Konfiguration des C1-Workload-Racks. Eine detaillierte Liste der Verbindungen finden Sie in den Tabellen, die auf die Diagramme folgen.

Abbildung 7: C1-Workload-Rack-Geräteverkabelung (öffentlich/extern)



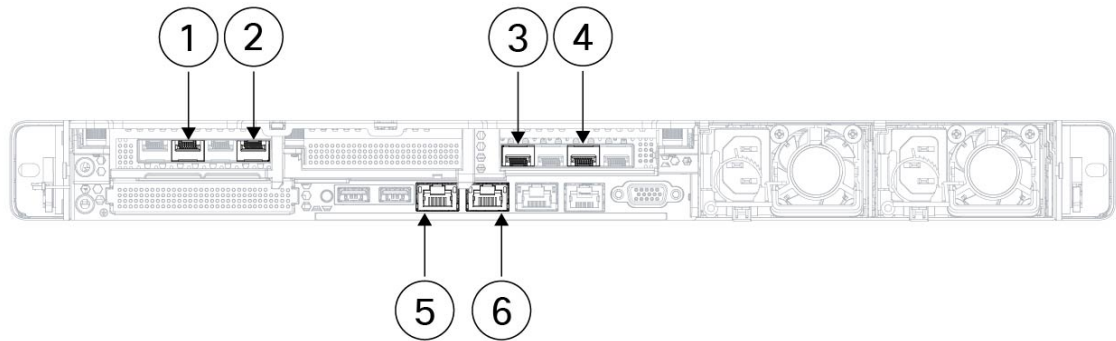
Das folgende Diagramm zeigt die Geräteverkabelung für die interne/Managementkonfiguration des C1-Workload-Racks. Eine detaillierte Liste der Verbindungen finden Sie in den folgenden Tabellen.

Abbildung 8: C1-Workload-Rack-Geräteverkabelung (intern/Management)



Die folgende Abbildung zeigt, welche Ports am M6-Server den „eno“-Ports in den obigen Abbildungen entsprechen:

Abbildung 9: M6-Server-Ports



1	Leaf 1 oder Leaf 2 (öffentlich), je nach Server Server-Schnittstellenport = eno5 CIMC-Bezeichnung = Adapter 1/physischer Port 2/vic-1-eth1	2	Leaf 1 (privat) Server-Schnittstellenport = eno6 CIMC-Bezeichnung = Adapter 1/physischer Port 0/vic-1-eth0
3	Leaf 2 (privat) Server-Schnittstellenport = eno8 CIMC-Bezeichnung = Adapter 3/physischer Port 0/vic-3-eth0	4	Wird nicht verwendet Server-Schnittstellenport = eno7 CIMC-Bezeichnung = Adapter 3/physischer Port 2/vic-3-eth1
5	CIMC Server-Schnittstellenport = eno1 CIMC-Bezeichnung = LOM 1	6	MGMT 2.2.2.2 Server-Schnittstellenport = eno2 CIMC-Bezeichnung = LOM 2

Tabelle 2: Spine-Switch-Verbindungen (HE 42 in Installationen mit einzelmem Rack und in Installationen mit zwei Racks)

Spine-Port	Verbindungstyp	Verbindung			
		Gerät	HE in einem Rack	HE in zwei Racks	Port
1/1	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 1 (Compute-Knoten)	HE 36	Rack1 HE 17	eno1
1/2	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 2 (Compute-Knoten)	HE 35	Rack1 HE 16	eno1
1/3	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 3 (Compute-Knoten)	HE 34	Rack1 HE 15	eno1
1/4	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 4 (Compute-Knoten)	HE 33	Rack1 HE 14	eno1
1/5	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 5 (Compute-Knoten)	HE 32	Rack1 HE 13	eno1

Spine-Port	Verbindungstyp	Verbindung			
		Gerät	HE in einem Rack	HE in zwei Racks	Port
1/6	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 6 (Compute-Knoten)	HE 31	Rack 1 HE 12	eno1
1/7	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 7 (Compute-Knoten)	HE 30	Rack 1 HE 11	eno1
1/8	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 8 (Compute-Knoten)	HE 29	Rack 1 HE 10	eno1
1/9	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 9 (Compute-Knoten)	HE 28	Rack 1 HE 8	eno1
1/10	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 10 (Compute-Knoten)	HE 27	Rack 1 HE 7	eno1
1/11	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 11 (Compute-Knoten)	HE 26	Rack 1 HE 6	eno1
1/12	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 12 (Compute-Knoten)	HE 25	Rack 1 HE 5	eno1
1/13	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 13 (Compute-Knoten)	HE 24	Rack 1 HE 4	eno1
1/14	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 14 (Compute-Knoten)	HE 23	Rack 1 HE 3	eno1
1/15	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 15 (Compute-Knoten)	HE 22	Rack 1 HE 2	eno1
1/16	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 16 (Compute-Knoten)	HE 21	Rack 1 HE 1	eno1
1/17	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 17 (Serving-Knoten)	HE 20	Rack 2 HE 21	eno1
1/18	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 18 (Serving-Knoten)	HE 19	Rack 2 HE 20	eno1
1/19	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 19 (Serving-Knoten)	HE 18	Rack 2 HE 19	eno1
1/20	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 20 (Serving-Knoten)	HE 17	Rack 2 HE 18	eno1
1/21	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 21 (Serving-Knoten)	HE 16	Rack 2 HE 17	eno1

Spine-Port	Verbindungstyp	Verbindung			
		Gerät	HE in einem Rack	HE in zwei Racks	Port
1/22	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 22 (Serving-Knoten)	HE 15	Rack2 HE 16	eno1
1/23	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 23 (Serving-Knoten)	HE 14	Rack2 HE 15	eno1
1/24	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 24 (Serving-Knoten)	HE 13	Rack2 HE 14	eno1
1/25	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 25 (Basisknoten)	HE 12	Rack2 HE 12	eno1
1/26	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 26 (Basisknoten)	HE 11	Rack2 HE 11	eno1
1/27	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 27 (Basisknoten)	HE 10	Rack2 HE 10	eno1
1/28	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 28 (Basisknoten)	HE 9	Rack2 HE 9	eno1
1/29	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 29 (Basisknoten)	HE 8	Rack2 HE 8	eno1
1/30	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 30 (Basisknoten)	HE 7	Rack2 HE 7	eno1
1/31	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 31 (Basisknoten)	HE 6	Rack2 HE 6	eno1
1/32	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 32 (Basisknoten)	HE 5	Rack2 HE 5	eno1
1/33	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 33 (Basisknoten)	HE 4	Rack2 HE 4	eno1
1/34	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 34 (Basisknoten)	HE 3	Rack2 HE 3	eno1
1/35	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 35 (Basisknoten)	HE 2	Rack2 HE 2	eno1
1/36	CIMC-VLAN (1 Gigabit)	UCS-Server-Host 36 (Basisknoten)	HE 1	Rack2 HE 1	eno1
1/49	Internes VLAN (40 Gigabit)	Leaf-Switch 1 (HE 41 im einzelnen Rack oder HE 40 in Rack 1 von zwei Racks)	HE 40	Rack1 HE 40	1/49

Spine-Port	Verbindungstyp	Verbindung			
		Gerät	HE in einem Rack	HE in zwei Racks	Port
1/50	Internes VLAN (40 Gigabit)	Leaf-Switch 2 (HE 40 im einzelnen Rack oder HE 40 in Rack 2 von zwei Racks), Port 49	HE 41	Rack 2 HE 40	1/50

Tabelle 3: Leaf-Switch 1-Verbindungen (HE 41 bei Installationen mit einzelнем Rack bzw. HE 40 in Rack 1 von zwei Racks bei Installationen mit zwei Racks)

Leaf 1-Port	Verbindungstyp	Verbindung			
		Gerät	HE in einem Rack	HE in zwei Racks	Port
1/1	Internes VLAN (10 Gigabit)	UCS-Server-Host 1 (Compute-Knoten)	HE 36	Rack 1 HE 17	eno6
1/2	Internes VLAN (10 Gigabit)	UCS-Server-Host 2 (Compute-Knoten)	HE 35	Rack 1 HE 16	eno6
1/3	Internes VLAN (10 Gigabit)	UCS-Server-Host 3 (Compute-Knoten)	HE 34	Rack 1 HE 15	eno6
1/4	Internes VLAN (10 Gigabit)	UCS-Server-Host 4 (Compute-Knoten)	HE 33	Rack 1 HE 14	eno6
1/5	Internes VLAN (10 Gigabit)	UCS-Server-Host 5 (Compute-Knoten)	HE 32	Rack 1 HE 13	eno6
1/6	Internes VLAN (10 Gigabit)	UCS-Server-Host 6 (Compute-Knoten)	HE 31	Rack 1 HE 12	eno6
1/7	Internes VLAN (10 Gigabit)	UCS-Server-Host 7 (Compute-Knoten)	HE 30	Rack 1 HE 11	eno6
1/8	Internes VLAN (10 Gigabit)	UCS-Server-Host 8 (Compute-Knoten)	HE 29	Rack 1 HE 10	eno6
1/9	Internes VLAN (10 Gigabit)	UCS-Server-Host 9 (Compute-Knoten)	HE 28	Rack 1 HE 8	eno6
1/10	Internes VLAN (10 Gigabit)	UCS-Server-Host 10 (Compute-Knoten)	HE 27	Rack 1 HE 7	eno6
1/11	Internes VLAN (10 Gigabit)	UCS-Server-Host 11 (Compute-Knoten)	HE 26	Rack 1 HE 6	eno6
1/12	Internes VLAN (10 Gigabit)	UCS-Server-Host 12 (Compute-Knoten)	HE 25	Rack 1 HE 5	eno6

Leaf 1-Port	Verbindungstyp	Verbindung			
		Gerät	HE in einem Rack	HE in zwei Racks	Port
1/13	Internes VLAN (10 Gigabit)	UCS-Server-Host 13 (Compute-Knoten)	HE 24	Rack1 HE 4	eno6
1/14	Internes VLAN (10 Gigabit)	UCS-Server-Host 14 (Compute-Knoten)	HE 23	Rack1 HE 3	eno6
1/15	Internes VLAN (10 Gigabit)	UCS-Server-Host 15 (Compute-Knoten)	HE 22	Rack1 HE 2	eno6
1/16	Internes VLAN (10 Gigabit)	UCS-Server-Host 16 (Compute-Knoten)	HE 21	Rack1 HE 1	eno6
1/17	Internes VLAN (10 Gigabit)	UCS-Server-Host 17 (Serving-Knoten)	HE 20	Rack2 HE 21	eno6
1/18	Internes VLAN (10 Gigabit)	UCS-Server-Host 18 (Serving-Knoten)	HE 19	Rack2 HE 20	eno6
1/19	Internes VLAN (10 Gigabit)	UCS-Server-Host 19 (Serving-Knoten)	HE 18	Rack2 HE 19	eno6
1/20	Internes VLAN (10 Gigabit)	UCS-Server-Host 20 (Serving-Knoten)	HE 17	Rack2 HE 18	eno6
1/21	Internes VLAN (10 Gigabit)	UCS-Server-Host 21 (Serving-Knoten)	HE 16	Rack2 HE 17	eno6
1/22	Internes VLAN (10 Gigabit)	UCS-Server-Host 22 (Serving-Knoten)	HE 15	Rack2 HE 16	eno6
1/23	Internes VLAN (10 Gigabit)	UCS-Server-Host 23 (Serving-Knoten)	HE 14	Rack2 HE 15	eno6
1/24	Internes VLAN (10 Gigabit)	UCS-Server-Host 24 (Serving-Knoten)	HE 13	Rack2 HE 14	eno6
1/25	Internes VLAN (10 Gigabit)	UCS-Server-Host 25 (Basisknoten)	HE 12	Rack2 HE 12	eno6
1/26	Internes VLAN (10 Gigabit)	UCS-Server-Host 26 (Basisknoten)	HE 11	Rack2 HE 11	eno6
1/27	Internes VLAN (10 Gigabit)	UCS-Server-Host 27 (Basisknoten)	HE 10	Rack2 HE 10	eno6
1/28	Internes VLAN (10 Gigabit)	UCS-Server-Host 28 (Basisknoten)	HE 9	Rack2 HE 9	eno6

Leaf 1-Port	Verbindungstyp	Verbindung			
		Gerät	HE in einem Rack	HE in zwei Racks	Port
1/29	Internes VLAN (10 Gigabit)	UCS-Server-Host 29 (Basisknoten)	HE 8	Rack2 HE 8	eno6
1/30	Internes VLAN (10 Gigabit)	UCS-Server-Host 30 (Basisknoten)	HE 7	Rack2 HE 7	eno6
1/31	Internes VLAN (10 Gigabit)	UCS-Server-Host 31 (Basisknoten)	HE 6	Rack2 HE 6	eno6
1/32	Internes VLAN (10 Gigabit)	UCS-Server-Host 32 (Basisknoten)	HE 5	Rack2 HE 5	eno6
1/33	Internes VLAN (10 Gigabit)	UCS-Server-Host 33 (Basisknoten)	HE 4	Rack2 HE 4	eno6
1/34	Internes VLAN (10 Gigabit)	UCS-Server-Host 34 (Basisknoten)	HE 3	Rack2 HE 3	eno6
1/35	Internes VLAN (10 Gigabit)	UCS-Server-Host 35 (Basisknoten)	HE 2	Rack2 HE 2	eno6
1/36	Internes VLAN (10 Gigabit)	UCS-Server-Host 36 (Basisknoten)	HE 1	Rack2 HE 1	eno6
1/37	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 33 (Basisknoten)	HE 3	Rack2 HE 3	eno5
1/38	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 35 (Basisknoten)	HE 1	Rack2 HE 1	eno5
1/39	Internes VLAN (10 Gigabit)	Kundenrouter 1	—	—	—
1/40	Internes VLAN (10 Gigabit)	Leaf 1	HE 40	Rack 1 HE 40	1/40
1/41	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 1 (Compute-Knoten)	HE 35	Rack 1 HE 16	eno5
1/42	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 3 (Compute-Knoten)	HE 33	Rack 1 HE 14	eno5
1/43	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 5 (Compute-Knoten)	HE 31	Rack 1 HE 12	eno5
1/44	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 7 (Compute-Knoten)	HE 29	Rack 1 HE 10	eno5

Leaf 1-Port	Verbindungstyp	Verbindung			
		Gerät	HE in einem Rack	HE in zwei Racks	Port
1/45	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 9 (Compute-Knoten)	HE 27	Rack 1 HE 8	eno5
1/46	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 11 (Compute-Knoten)	HE 25	Rack 1 HE 6	eno5
1/47	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 13 (Compute-Knoten)	HE 23	Rack 1 HE 4	eno5
1/48	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 15 (Compute-Knoten)	HE 21	Rack 1 HE 2	eno5
1/49	Internes VLAN (40 Gigabit)	Spine-Switch	HE 42	Rack 1 HE 42	1/49
1/50	—	—	—	—	—
1/51	—	—	—	—	—
1/52	—	—	—	—	—
1/53	Internes VLAN (40 Gigabit)	Leaf-Switch 1	HE 40	Rack 1 HE 40	1/53
1/54	Internes VLAN (40 Gigabit)	Leaf-Switch 1	HE 40	Rack 1 HE 40	1/54

Tabelle 4: Leaf-Switch 2-Verbindungen (HE 41 bei Installationen mit einzeltem Rack bzw. HE 40 in Rack 2 von zwei Racks bei Installationen mit zwei Racks)

Leaf 2-Port	Verbindungstyp	Verbindung			
		Gerät	HE in einem Rack	HE in zwei Racks	Port
1/1	Internes VLAN (10 Gigabit)	UCS-Server-Host 1 (Compute-Knoten)	HE 36	Rack 1 HE 17	eno8
1/2	Internes VLAN (10 Gigabit)	UCS-Server-Host 2 (Compute-Knoten)	HE 35	Rack 1 HE 16	eno8
1/3	Internes VLAN (10 Gigabit)	UCS-Server-Host 3 (Compute-Knoten)	HE 34	Rack 1 HE 15	eno8
1/4	Internes VLAN (10 Gigabit)	UCS-Server-Host 4 (Compute-Knoten)	HE 33	Rack 1 HE 14	eno8

Leaf 2-Port	Verbindungstyp	Verbindung			
		Gerät	HE in einem Rack	HE in zwei Racks	Port
1/5	Internes VLAN (10 Gigabit)	UCS-Server-Host 5 (Compute-Knoten)	HE 32	Rack 1 HE 13	eno8
1/6	Internes VLAN (10 Gigabit)	UCS-Server-Host 6 (Compute-Knoten)	HE 31	Rack 1 HE 12	eno8
1/7	Internes VLAN (10 Gigabit)	UCS-Server-Host 7 (Compute-Knoten 7)	HE 30	Rack 1 HE 11	eno8
1/8	Internes VLAN (10 Gigabit)	UCS-Server-Host 8 (Compute-Knoten)	HE 29	Rack 1 HE 10	eno8
1/9	Internes VLAN (10 Gigabit)	UCS-Server-Host 9 (Compute-Knoten)	HE 28	Rack 1 HE 8	eno8
1/10	Internes VLAN (10 Gigabit)	UCS-Server-Host 10 (Compute-Knoten)	HE 27	Rack 1 HE 7	eno8
1/11	Internes VLAN (10 Gigabit)	UCS-Server-Host 11 (Compute-Knoten)	HE 26	Rack 1 HE 6	eno8
1/12	Internes VLAN (10 Gigabit)	UCS-Server-Host 12 (Compute-Knoten)	HE 25	Rack 1 HE 5	eno8
1/13	Internes VLAN (10 Gigabit)	UCS-Server-Host 13 (Compute-Knoten)	HE 24	Rack 1 HE 4	eno8
1/14	Internes VLAN (10 Gigabit)	UCS-Server-Host 14 (Compute-Knoten)	HE 23	Rack 1 HE 3	eno8
1/15	Internes VLAN (10 Gigabit)	UCS-Server-Host 15 (Compute-Knoten)	HE 22	Rack 1 HE 2	eno8
1/16	Internes VLAN (10 Gigabit)	UCS-Server-Host 16 (Compute-Knoten)	HE 21	Rack 1 HE 1	eno8
1/17	Internes VLAN (10 Gigabit)	UCS-Server-Host 17 (Serving-Knoten)	HE 20	Rack 2 HE 21	eno8
1/18	Internes VLAN (10 Gigabit)	UCS-Server-Host 18 (Serving-Knoten)	HE 19	Rack 2 HE 20	eno8
1/19	Internes VLAN (10 Gigabit)	UCS-Server-Host 19 (Serving-Knoten)	HE 18	Rack 2 HE 19	eno8
1/20	Internes VLAN (10 Gigabit)	UCS-Server-Host 20 (Serving-Knoten)	HE 17	Rack 2 HE 18	eno8

Leaf 2-Port	Verbindungstyp	Verbindung			
		Gerät	HE in einem Rack	HE in zwei Racks	Port
1/21	Internes VLAN (10 Gigabit)	UCS-Server-Host 21 (Serving-Knoten)	HE 16	Rack2 HE 17	eno8
1/22	Internes VLAN (10 Gigabit)	UCS-Server-Host 22 (Serving-Knoten)	HE 15	Rack2 HE 16	eno8
1/23	Internes VLAN (10 Gigabit)	UCS-Server-Host 23 (Serving-Knoten)	HE 14	Rack2 HE 15	eno8
1/24	Internes VLAN (10 Gigabit)	UCS-Server-Host 24 (Serving-Knoten)	HE 13	Rack2 HE 14	eno8
1/25	Internes VLAN (10 Gigabit)	UCS-Server-Host 25 (Basisknoten)	HE 12	Rack2 HE 12	eno8
1/26	Internes VLAN (10 Gigabit)	UCS-Server-Host 26 (Basisknoten)	HE 11	Rack2 HE 11	eno8
1/27	Internes VLAN (10 Gigabit)	UCS-Server-Host 27 (Basisknoten)	HE 10	Rack2 HE 10	eno8
1/28	Internes VLAN (10 Gigabit)	UCS-Server-Host 28 (Basisknoten)	HE 9	Rack2 HE 9	eno8
1/29	Internes VLAN (10 Gigabit)	UCS-Server-Host 29 (Basisknoten)	HE 8	Rack2 HE 8	eno8
1/30	Internes VLAN (10 Gigabit)	UCS-Server-Host 30 (Basisknoten)	HE 7	Rack2 HE 7	eno8
1/31	Internes VLAN (10 Gigabit)	UCS-Server-Host 31 (Basisknoten)	HE 6	Rack2 HE 6	eno8
1/32	Internes VLAN (10 Gigabit)	UCS-Server-Host 32 (Basisknoten)	HE 5	Rack2 HE 5	eno8
1/33	Internes VLAN (10 Gigabit)	UCS-Server-Host 33 (Basisknoten)	HE 4	Rack2 HE 4	eno8
1/34	Internes VLAN (10 Gigabit)	UCS-Server-Host 34 (Basisknoten)	HE 3	Rack2 HE 3	eno8
1/35	Internes VLAN (10 Gigabit)	UCS-Server-Host 35 (Basisknoten)	HE 2	Rack2 HE 2	eno8
1/36	Internes VLAN (10 Gigabit)	UCS-Server-Host 36 (Basisknoten)	HE 1	Rack2 HE 1	eno8

Leaf 2-Port	Verbindungstyp	Verbindung			
		Gerät	HE in einem Rack	HE in zwei Racks	Port
1/37	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 34 (Basisknoten)	HE 4	Rack2 HE 8	eno5
1/38	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 36 (Basisknoten)	HE 2	Rack2 HE 6	eno5
1/39	Internes VLAN (10 Gigabit)	Kundenrouter 1	—	—	—
1/40	Internes VLAN (10 Gigabit)	Leaf-Switch 2	HE 41	Rack2 HE 40	1/40
1/41	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 2 (Compute-Knoten)	HE 36	Rack 1 HE 17	eno5
1/42	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 4 (Compute-Knoten)	HE 34	Rack 1 HE 15	eno5
1/43	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 6 (Compute-Knoten)	HE 32	Rack 1 HE 13	eno5
1/44	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 8 (Compute-Knoten)	HE 30	Rack 1 HE 11	eno5
1/45	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 10 (Compute-Knoten)	HE 28	Rack 1 HE 9	eno5
1/46	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 12 (Compute-Knoten)	HE 26	Rack 1 HE 7	eno5
1/47	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 14 (Compute-Knoten)	HE 24	Rack 1 HE 5	eno5
1/48	Öffentliches VLAN (10 Gigabit)	UCS-Server-Host 16 (Compute-Knoten)	HE 22	Rack 1 HE 3	eno5
1/49	Internes VLAN (40 Gigabit)	Spine-Switch	HE 42	Rack 1 HE 42	—
1/50	—	—	—	—	1/50
1/51	—	—	—	—	—
1/52	—	—	—	—	—
1/53	Internes VLAN (40 Gigabit)	Leaf 1-Switch	HE 40	Rack 1 HE 40	1/49

Leaf 2-Port	Verbindungstyp	Verbindung			
		Gerät	HE in einem Rack	HE in zwei Racks	Port
1/54	Internes VLAN (40 Gigabit)	Leaf 2-Switch	HE 41	Rack2 HE 40	1/50

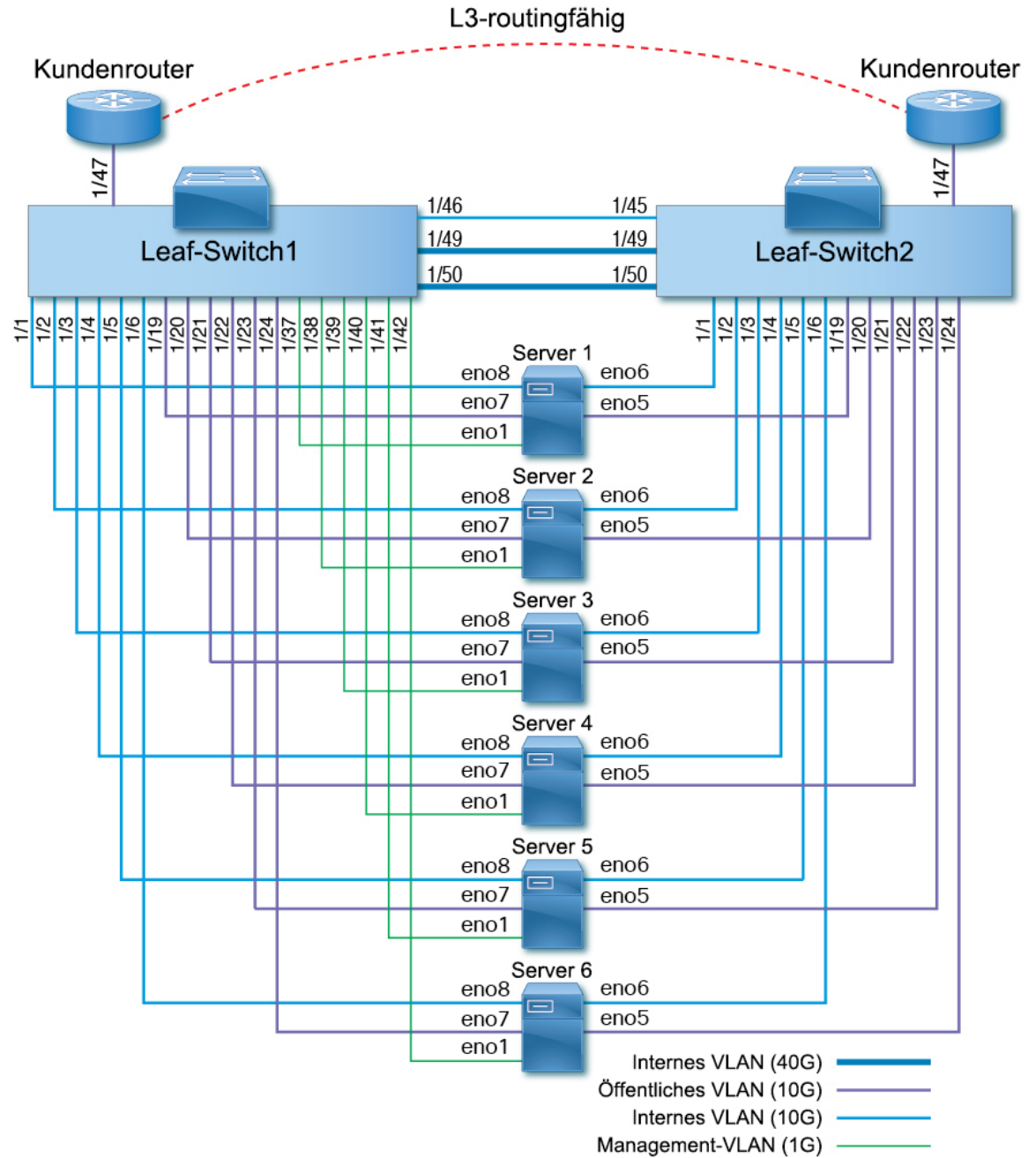
C1 – Workload-M-Cluster – Geräteverkabelung

Beachten Sie die folgenden Konfigurationsinformationen, wenn Sie die M6-VIC im 8-HE-Rack verkabeln:

- Es gibt zwei private Schnittstellen für alle Knoten.
- Das 8-HE-Rack verfügt über zwei öffentliche Schnittstellen für alle sechs Knoten.
- Bei der M6-Hardware sind vier Ports pro VIC vorhanden.
- Die Namen für die Bare-Metal-Schnittstelle – die physischen Server im Cluster, die als universelle Knoten bekannt sind – beginnen mit „eno“ (Ethernet onboard).

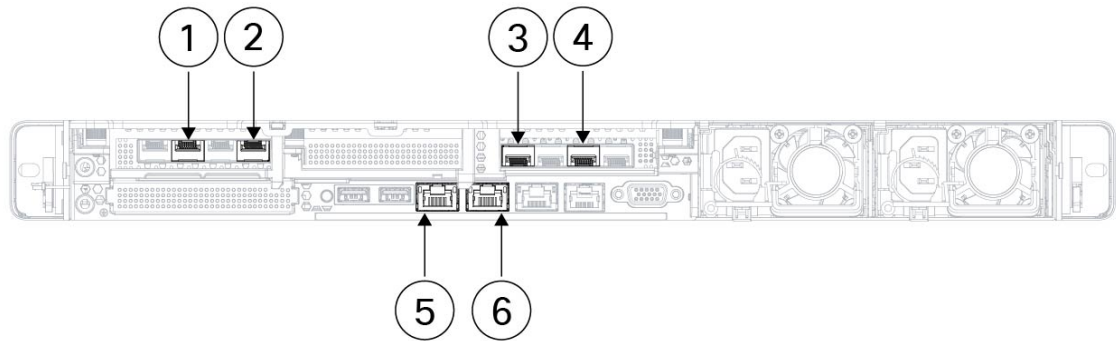
Das folgende Diagramm zeigt die Geräteverkabelung für die interne/Management-/öffentliche/externe Konfiguration des C1-Workload-M-Cluster-8-HE-Racks. Eine detaillierte Liste der Verbindungen finden Sie in den Tabellen, die auf das Diagramm folgen.

Abbildung 10: C1-Workload-M-Cluster-Rack-Geräteverkabelung (intern/Management/öffentlich/extern)



Die folgende Abbildung zeigt, welche Ports am Server den „eno“-Ports im obigen Diagramm entsprechen:

Abbildung 11: M6-Server-Ports



1	Leaf 2 (öffentlich) Server-Schnittstellenport = eno5 CIMC-Bezeichnung = Adapter 1/physischer Port 2/vic-1-eth1	2	Leaf 2 (privat) Server-Schnittstellenport = eno6 CIMC-Bezeichnung = Adapter 1/physischer Port 0/vic-1-eth0
3	Leaf 1 (privat) Server-Schnittstellenport = eno8 CIMC-Bezeichnung = Adapter 3/physischer Port 0/vic-3-eth0	4	Leaf 1 (öffentlich) Server-Schnittstellenport = eno7 CIMC-Bezeichnung = Adapter 3/physischer Port 2/vic-3-eth1
5	CIMC Server-Schnittstellenport = eno1 CIMC-Bezeichnung = LOM 1	6	MGMT 2.2.2.2 Server-Schnittstellenport = eno2 CIMC-Bezeichnung = LOM 2

Tabelle 5: Verbindungen für Leaf-Switch 1 (HE 12)

Leaf-Port	Verbindungstyp	Verbindung		
		Gerät	HE in einem Rack	Port
1/1	Internes VLAN (10 Gigabit)	UCS-Server-Host 1 (universeller Knoten)	HE 9	eno8
1/2	Internes VLAN (10 Gigabit)	UCS-Server-Host 2 (universeller Knoten)	HE 8	eno8
1/3	Internes VLAN (10 Gigabit)	UCS-Server-Host 3 (universeller Knoten)	HE 6	eno8
1/4	Internes VLAN (10 Gigabit)	UCS-Server-Host 4 (universeller Knoten)	HE 5	eno8
1/5	Internes VLAN (10 Gigabit)	UCS-Server-Host 5 (universeller Knoten)	HE 3	eno8
1/6	Internes VLAN (10 Gigabit)	UCS-Server-Host 6 (universeller Knoten)	HE 2	eno8
1/7	—	—	—	—
1/8	—	—	—	—

Leaf-Port	Verbindungstyp	Verbindung		
		Gerät	HE in einem Rack	Port
1/9	—	—	—	—
1/10	—	—	—	—
1/11	—	—	—	—
1/12	—	—	—	—
1/13	—	—	—	—
1/14	—	—	—	—
1/15	—	—	—	—
1/16	—	—	—	—
1/17	—	—	—	—
1/18	—	—	—	—
1/19	Externes VLAN (10 Gigabit)	UCS-Server-Host 1 (universeller Knoten)	HE 9	eno7
1/20	Externes VLAN (10 Gigabit)	UCS-Server-Host 2 (universeller Knoten)	HE 8	eno7
1/21	Externes VLAN (10 Gigabit)	UCS-Server-Host 3 (universeller Knoten)	HE 6	eno7
1/22	Externes VLAN (10 Gigabit)	UCS-Server-Host 4 (universeller Knoten)	HE 5	eno7
1/23	Externes VLAN (10 Gigabit)	UCS-Server-Host 5 (universeller Knoten)	HE 3	eno7
1/24	Externes VLAN (10 Gigabit)	UCS-Server-Host 6 (universeller Knoten)	HE 2	eno7
1/25	—	—	—	—
1/26	—	—	—	—
1/27	—	—	—	—
1/28	—	—	—	—
1/29	—	—	—	—
1/30	—	—	—	—
1/31	—	—	—	—
1/32	—	—	—	—
1/33	—	—	—	—

Leaf-Port	Verbindungstyp	Verbindung		
		Gerät	HE in einem Rack	Port
1/34	—	—	—	—
1/35	—	—	—	—
1/36	—	—	—	—
1/37	Management-VLAN (1 Gigabit)	UCS-Server-Host 1 (universeller Knoten)	HE 9	eno1
1/38	Management-VLAN (1 Gigabit)	UCS-Server-Host 2 (universeller Knoten)	HE 8	eno1
1/39	Management-VLAN (1 Gigabit)	UCS-Server-Host 3 (universeller Knoten)	HE 6	eno1
1/40	Management-VLAN (1 Gigabit)	UCS-Server-Host 4 (universeller Knoten)	HE 5	eno1
1/41	Management-VLAN (1 Gigabit)	UCS-Server-Host 5 (universeller Knoten)	HE 3	eno1
1/42	Management-VLAN (1 Gigabit)	UCS-Server-Host 6 (universeller Knoten)	HE 2	eno1
1/43	—	—	—	—
1/44	—	—	—	—
1/45	—	—	—	—
1/46	Internes VLAN (10 Gigabit)	Leaf 2-Switch	HE 11	1/45
1/47	Externes VLAN (10 Gigabit)	Kundenrouter	—	—
1/48	—	—	—	—
1/49	Internes VLAN (40 Gigabit)	Leaf 2-Switch	HE 11	1/49
1/50	Internes VLAN (40 Gigabit)	Leaf 2-Switch	HE 11	1/50
1/51	—	—	—	—
1/52	—	—	—	—
1/53	—	—	—	—
1/54	—	—	—	—

Tabelle 6: Verbindungen für Leaf-Switch 2 (HE 11)

Leaf-Port	Verbindungstyp	Verbindung		
		Gerät	HE in einem Rack	Port
1/1	Internes VLAN (10 Gigabit)	UCS-Server-Host 1 (universeller Knoten)	9 HE	eno6
1/2	Internes VLAN (10 Gigabit)	UCS-Server-Host 2 (universeller Knoten)	8 HE	eno6
1/3	Internes VLAN (10 Gigabit)	UCS-Server-Host 3 (universeller Knoten)	6 HE	eno6
1/4	Internes VLAN (10 Gigabit)	UCS-Server-Host 4 (universeller Knoten)	5 HE	eno6
1/5	Internes VLAN (10 Gigabit)	UCS-Server-Host 5 (universeller Knoten)	3 HE	eno6
1/6	Internes VLAN (10 Gigabit)	UCS-Server-Host 6 (universeller Knoten)	2 HE	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	Externes VLAN (10 Gigabit)	UCS-Server-Host 1 (universeller Knoten)	9 HE	eno5
1/20	Externes VLAN (10 Gigabit)	UCS-Server-Host 2 (universeller Knoten)	8 HE	eno5
1/21	Externes VLAN (10 Gigabit)	UCS-Server-Host 3 (universeller Knoten)	6 HE	eno5
1/22	Externes VLAN (10 Gigabit)	UCS-Server-Host 4 (universeller Knoten)	5 HE	eno5
1/23	Externes VLAN (10 Gigabit)	UCS-Server-Host 5 (universeller Knoten)	3 HE	eno5
1/24	Externes VLAN (10 Gigabit)	UCS-Server-Host 6 (universeller Knoten)	2 HE	eno5
1/25	—	—	—	—

Leaf-Port	Verbindungstyp	Verbindung		
		Gerät	HE in einem Rack	Port
1/26	—	—	—	—
1/27	—	—	—	—
1/28	—	—	—	—
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	Internes VLAN (10 Gigabit)	Leaf 1-Switch	12 HE	1/46
1/46	—	—	—	—
1/47	Externes VLAN (10 Gigabit)	Kundenrouter	—	—
1/48	—	—	—	—
1/49	Internes VLAN (40 Gigabit)	Leaf 1-Switch	12 HE	1/49
1/50	Internes VLAN (40 Gigabit)	Leaf 1-Switch	12 HE	1/50
1/51	—	—	—	—

Leaf-Port	Verbindungstyp	Verbindung		
		Gerät	HE in einem Rack	Port
1/52	—	—	—	—
1/53	—	—	—	—
1/54	—	—	—	—



KAPITEL 6

Systemspezifikationen

- [Umgebungsbedingungen](#), auf Seite 45
- [Netzkabel](#), auf Seite 45

Umgebungsbedingungen

In der folgenden Tabelle sind die Umgebungsbedingungen für die Installation des Cisco Secure Workload-Clusters aufgeführt.

Tabelle 7: Umgebungsbedingungen

Umgebungsbedingungen		Spezifikation
Temperatur	Betrieb	5 bis 35 °C, wobei der Wert sich um 1 °C pro 305 m ü. NN. verringert
	Speicher	-40 bis 65 °C
Luftfeuchtigkeit	Betrieb	10 bis 80 % relative Luftfeuchtigkeit mit maximaler Zu- oder Abnahme von 10 % pro Stunde
	Speicher	5 bis 93 % relative Luftfeuchtigkeit
Höhe	Betrieb	0 bis 3.050 m
	Speicher	0 bis 12.200 m

Netzkabel

In den folgenden Tabellen ist aufgeführt, welche Netzkabel im Lieferumfang des Cisco Secure Workload-M6-Clusters enthalten sind.

Tabelle 8: 39-HE-Cluster, Konfiguration mit einem einzelnen Rack

Teilenummer	Beschreibung	Menge
TA-RACK-UCS2-INT	Cisco R42612 – dynamisches Rack mit Seitenteilen	1

Teilenummer	Beschreibung	Menge
TA-ETH-RJ45-SINGLE	RJ-45-Kabelset für eine Konfiguration mit einem Rack und 39 HE	1
TA-SFP-H10GB-CU2M	10GBASE-CU-SFP+-Kabel (2 m)	16
TA-SFP-H10GB-CU1-5	10GBASE-CU-SFP+-Kabel (1,5 m)	32
TA-QSFP-H40G-CU1M	Passives 40GBASE-CR4-Kupferkabel (1 m)	4
TA-SFP-H10GB-CU1M	10GBASE-CU-SFP+-Kabel (1 m)	25
TA-SFP-H10GB-CU2-5	10GBASE-CU-SFP+-Kabel (2,5 m)	20

Tabelle 9: 39-HE-Cluster, Konfiguration mit zwei Racks

Teilenummer	Beschreibung	Menge
TA-RACK-UCS2-INT	Cisco R42612 – dynamisches Rack, mit Seitenteilen	2
TA-ETH-RJ45-DUAL	RJ-45-Kabelset für eine Konfiguration mit einem Rack und 39 HE	1
TA-SFP-H10GB-CU2M	10GBASE-CU-SFP+-Kabel (2 m)	15
TA-SFP-H10GB-CU1-5	10GBASE-CU-SFP+-Kabel (1,5 m)	19
TA-QSFP-H40G-CU1M	Passives 40GBASE-CR4-Kupferkabel (1 m)	1
TA-QSFP-H40G-CU5M	Passives 40GBASE-CR4-Kupferkabel (5 m)	3
TA-SFP-H10GB-CU2-5	10GBASE-CU-SFP+-Kabel (2,5 m)	12
TA-SFP-H10GB-CU5M	10GBASE-CU-SFP+-Kabel (5 m)	47

Tabelle 10: 8-HE-Cluster

Teilenummer	Beschreibung	Menge
TA-RACK-UCS2-INT	Cisco R42612 – dynamisches Rack, mit Seitenteilen	1
CAB-ETH-S-RJ45	RJ-45-Straight-Through-Kabel (gelb) für Ethernet (1,8 m)	6
TA-SFP-H10GB-CU1M	10GBASE-CU-SFP+-Kabel (1 m)	13
TA-SFP-H10GB-CU1-5	10GBASE-CU-SFP+-Kabel (1,5 m)	12
TA-QSFP-H40G-CU1M	Passives 40GBASE-CR4-Kupferkabel (1 m)	2
GLC-TE	1000BASE-T-SFP-Transceiver-Modul für Kupferkabel der Kategorie 5	6