



## **Guida all'implementazione del cluster Cisco Secure Workload M6**

**Prima pubblicazione:** 2023-10-25

### **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](http://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. Tutti i diritti riservati.



## SOMMARIO

---

### CAPITOLO 1

#### **Panoramica 1**

Panoramica 1

Pannello anteriore del server Cisco UCS C220 M6 5

Pannello posteriore del server Cisco UCS C220 M6 6

---

### CAPITOLO 2

#### **Preparazione del sito 9**

Requisiti di temperatura 9

Requisiti di umidità 9

Requisiti di altitudine 10

Requisiti di polvere e particolato 10

Riduzione delle interferenze elettromagnetiche e di radiofrequenza 10

Requisiti di resistenza agli urti e alle vibrazioni 11

Requisiti di messa a terra 11

Requisiti di alimentazione 11

Requisiti del ricircolo d'aria 12

Requisiti di spazio 12

---

### CAPITOLO 3

#### **Messa a terra e collegamenti 13**

Collegare a massa i dispositivi del cluster Cisco Secure Workload 13

Accendere i dispositivi del cluster Cisco Secure Workload 13

Collegare il cluster di Cisco Secure Workload ai router 14

---

### CAPITOLO 4

#### **Configurazione dell'interfaccia utente 15**

(Facoltativo) Requisiti e limitazioni per la modalità dual-stack (supporto IPv6) 15

Configurazione dell'interfaccia utente 16

---

**CAPITOLO 5**      **Cablaggio dei dispositivi nel cluster C1 di Cisco Secure Workload**    **21**

    Cablaggio dei dispositivi nel cluster C1-Workload    **21**

    Cablaggio dei dispositivi nel cluster C1-Workload-M    **34**

---

**CAPITOLO 6**      **Specifiche del sistema**    **43**

    Specifiche ambientali    **43**

    Cavi di alimentazione    **43**



## CAPITOLO 1

# Panoramica

---

- [Panoramica](#), a pagina 1
- [Pannello anteriore del server Cisco UCS C220 M6](#), a pagina 5
- [Pannello posteriore del server Cisco UCS C220 M6](#), a pagina 6

## Panoramica

Il cluster Cisco Secure Workload M6 può essere implementato in uno dei modi seguenti:

- Piattaforma con fattore di forma grande da 39 unità rack (RU) (C1-Workload a rack singolo) per i data center con oltre 5000 server



---

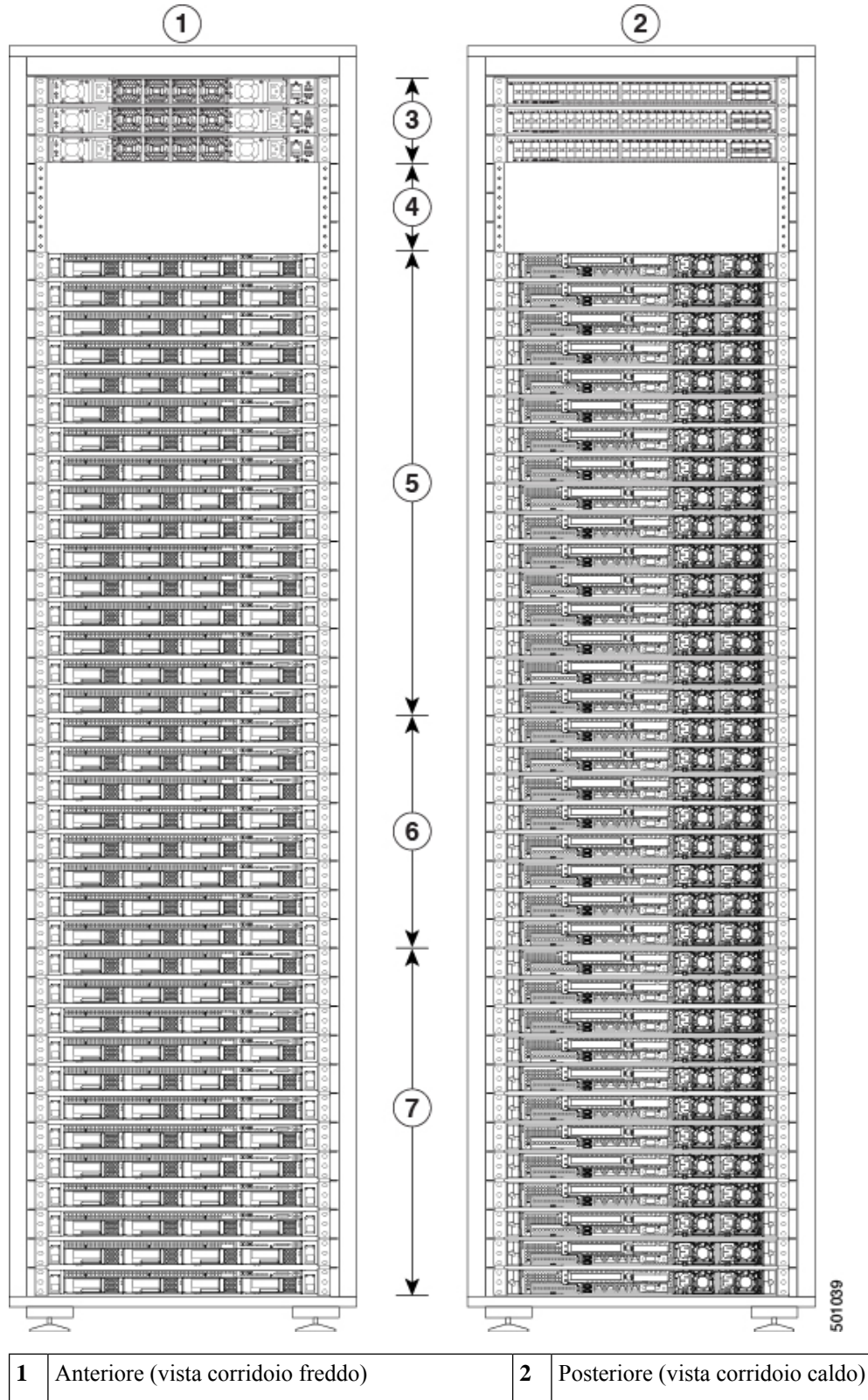
**Nota** È possibile implementare la piattaforma con fattore di forma grande in uno o due rack a seconda delle esigenze. Vedere le seguenti figure per esempi di C1-Workload a rack singolo o a due rack.

---

- Piattaforma con fattore di forma ridotto da 8 RU (C1-Workload-M) per data center con meno di 5000 server. Vedere la figura C1-Workload-M per un esempio.

Nella figura seguente vengono mostrate le parti anteriore e posteriore del C1-Workload a rack singolo.

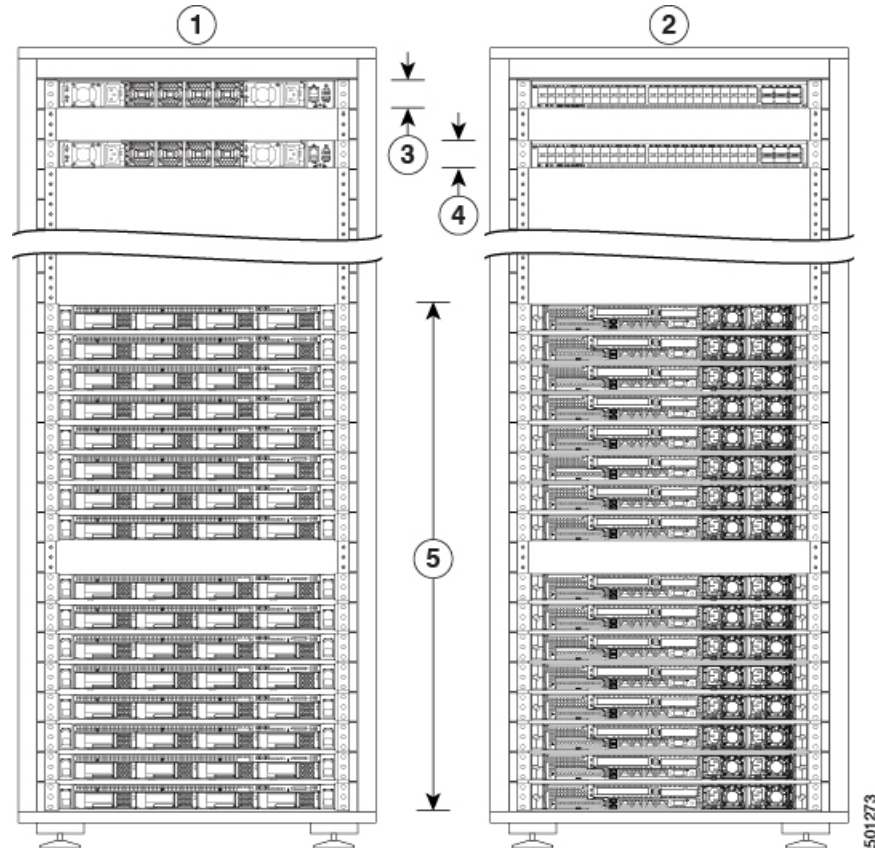
Figura 1: Vista anteriore e posteriore del C1-Workload a rack singolo



3	Uno switch spine (RU 42) e due switch leaf: leaf 2 (RU 40) e leaf 1 (RU 41)	4	Unità rack aperte (RU da 37 a 39)
5	16 server di elaborazione (RU da 21 a 36)	6	Otto server di servizio (RU da 13 a 20)
7	12 server di base (RU da 1 a 12)		—

Nella figura seguente vengono mostrate le parti anteriore e posteriore del rack 1 del C1-Workload a due rack.

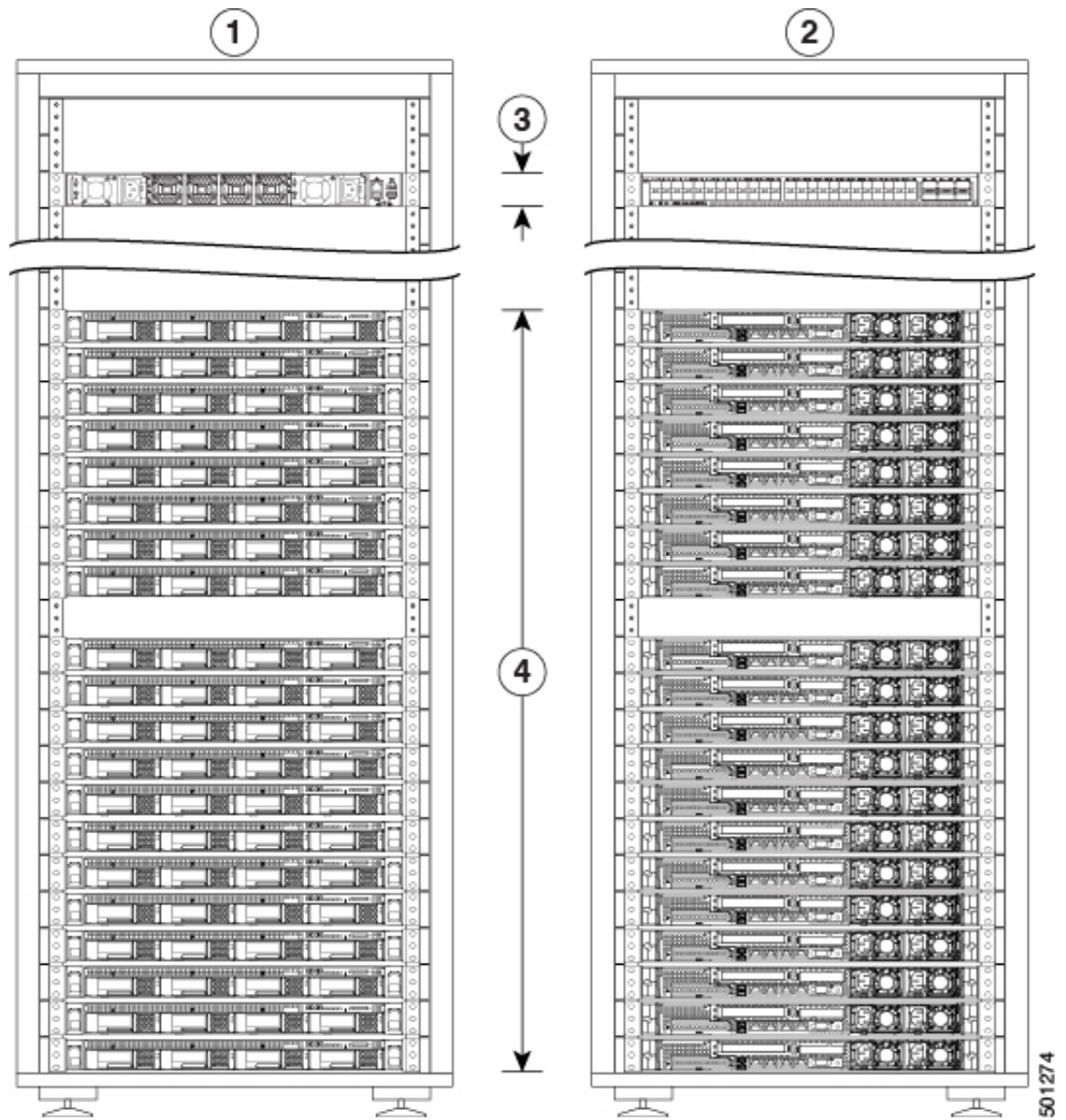
**Figura 2: C1-Workload a due rack: vista anteriore e posteriore del rack 1**



1	Anteriore (vista corridoio freddo)	2	Posteriore (vista corridoio caldo)
3	Uno switch spine (RU 42)	4	Switch leaf 1 (RU 40)
5	16 server di elaborazione (RU da 1 a 4 e da 6 a 9)	6	—

Nella figura seguente vengono mostrate le parti anteriore e posteriore del rack 2 del C1-Workload a due rack.

Figura 3: C1-Workload a due rack: vista anteriore e posteriore del rack 2

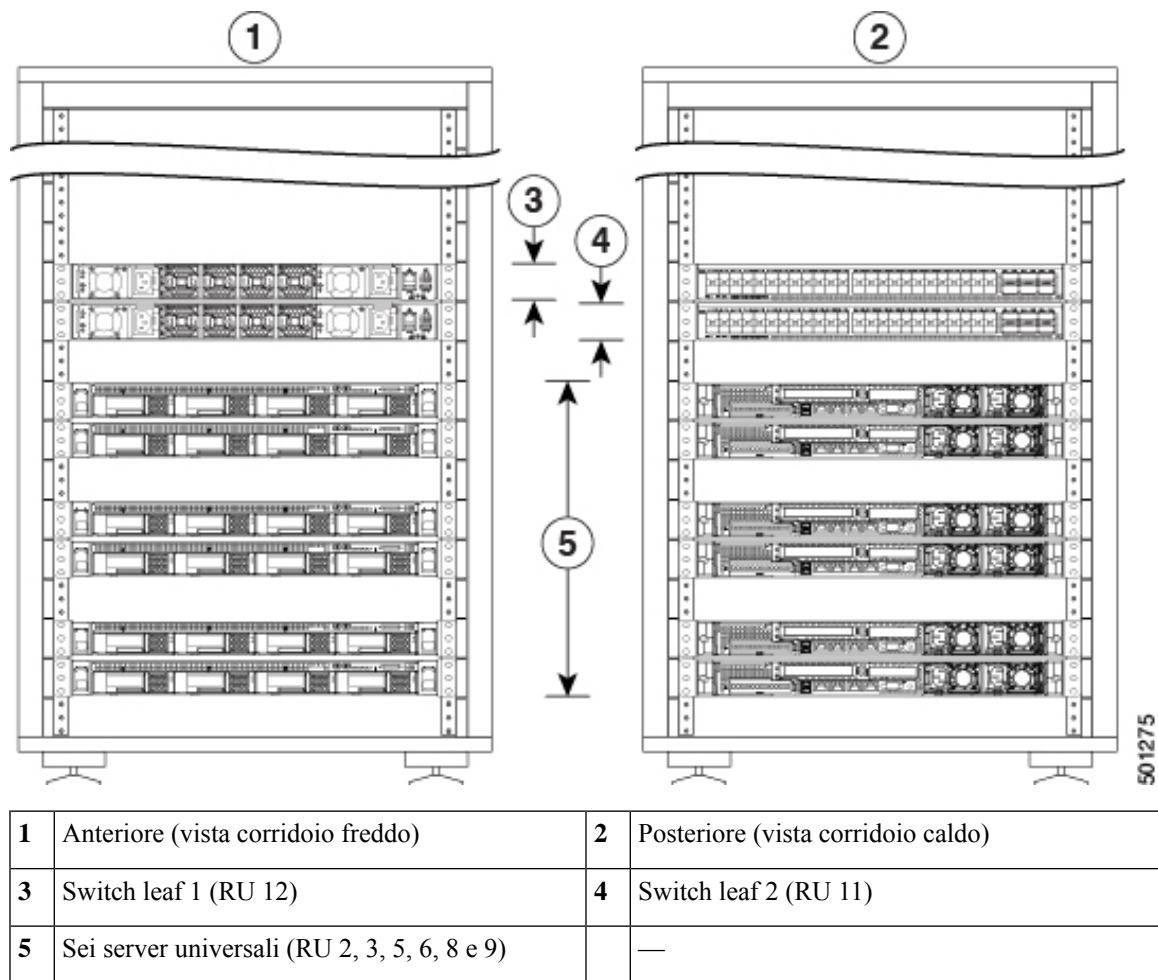


1	Anteriore (vista corridoio freddo)	2	Posteriore (vista corridoio caldo)
3	Switch leaf 2 (RU 40)	4	Otto server di servizio (RU da 14 a 21) e 12 server di base (RU da 1 a 12)

Nella figura seguente vengono mostrate le parti anteriore e posteriore del C1-Workload-M.



Figura 4: Vista anteriore e posteriore del C1-Workload-M



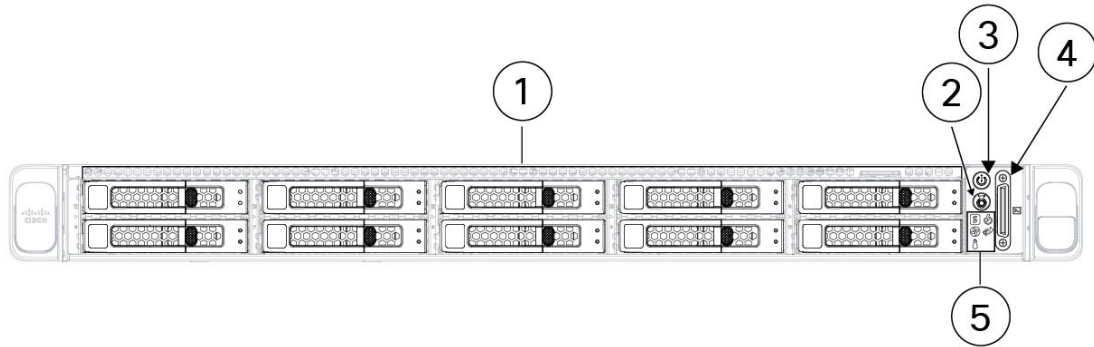
501275

## Pannello anteriore del server Cisco UCS C220 M6

Nella figura seguente viene mostrato il pannello anteriore del server UCS C220 M6 con unità SFF (Small Form-Factor).

Per ulteriori informazioni, vedere la [Guida all'installazione e alla manutenzione del server Cisco UCS C220 M6](#).

Figura 5: Pannello anteriore del server Cisco UCS C220 M6



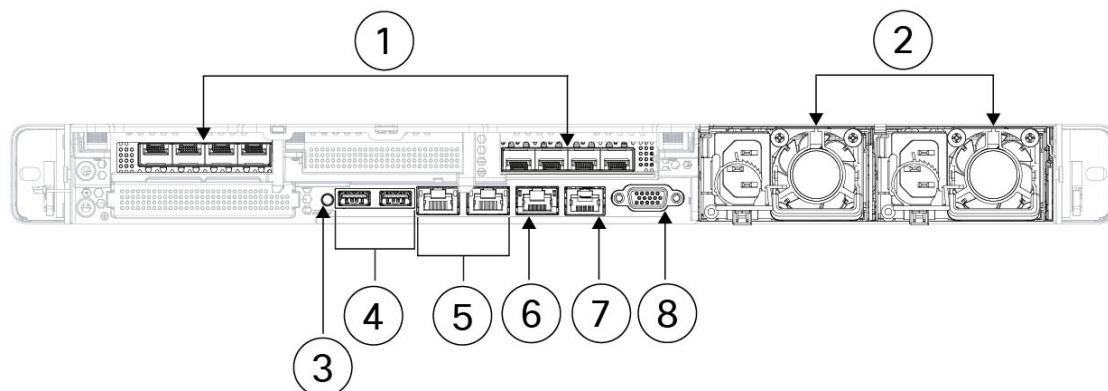
<p><b>1</b> Alloggiamenti per unità da 1 a 10, numerati da sinistra a destra, dall'alto verso il basso</p> <p>Supporto per HDD e SSD SAS/SATA. Opzionalmente, gli alloggiamenti da 1 a 4 possono contenere unità NVMe in qualsiasi numero fino a 4. Gli alloggiamenti per unità da 5 a 10 supportano solo unità HDD o SSD SAS/SATA.</p>	<p><b>2</b> LED/pulsante di identificazione dell'unità</p>
<p><b>3</b> LED del pulsante di accensione e dello stato di alimentazione</p>	<p><b>4</b> Connettore KVM</p> <p>Utilizzato con il cavo KVM, completo di un connettore DB-15 VGA, un connettore DB-9 seriale e due connettori USB 2.0.</p>
<p><b>5</b> LED di sistema:</p> <ul style="list-style-type: none"> <li>• LED dello stato della ventola</li> <li>• LED dello stato del sistema</li> <li>• LED dello stato dell'alimentazione</li> <li>• LED dell'attività dei collegamenti di rete</li> <li>• LED dello stato della temperatura</li> </ul>	<p>—</p>

## Pannello posteriore del server Cisco UCS C220 M6

Nella figura seguente viene mostrato il pannello posteriore del server UCS C220 M6.

Per ulteriori informazioni, vedere la [Guida all'installazione e alla manutenzione del server Cisco UCS C220 M6](#).

Figura 6: Pannello posteriore del server Cisco UCS C220 M6



1	<p>Due slot PCIe</p> <ul style="list-style-type: none"> <li>• Riser 1 (controllato dalla CPU 1) <ul style="list-style-type: none"> <li>• Supporta uno slot PCIe (slot 1)</li> <li>• Lo slot 1 è a metà altezza, 3/4 di lunghezza, x16</li> </ul> </li> <li>• Riser 3 (controllato dalla CPU 2) <ul style="list-style-type: none"> <li>• Supporta uno slot PCIe (slot 3)</li> <li>• Lo slot 3 è a metà altezza, 3/4 lunghezza, x16</li> </ul> </li> </ul>	2	<p>Due alimentatori (PSU), ridondanti se configurati in modalità di alimentazione 1+1</p>
3	<p>Pulsante/LED di identificazione dell'unità</p>	4	<p>Due porte USB 3.0</p>
5	<p>Due porte da 1 Gb/10 Gb 1-Gb Ethernet (LAN1 e LAN2)</p> <p>Le due porte LAN supportano velocità di 1 Gbps e 10 Gbps a seconda della capacità del partner di collegamento.</p>	6	<p>Porta di gestione dedicata da 1 Gb Ethernet</p>
7	<p>Porta COM (connettore RJ-45)</p>	8	<p>Porta video VGA (connettore DB-15)</p>





## CAPITOLO 2

# Preparazione del sito

---

- [Requisiti di temperatura, a pagina 9](#)
- [Requisiti di umidità, a pagina 9](#)
- [Requisiti di altitudine, a pagina 10](#)
- [Requisiti di polvere e particolato, a pagina 10](#)
- [Riduzione delle interferenze elettromagnetiche e di radiofrequenza, a pagina 10](#)
- [Requisiti di resistenza agli urti e alle vibrazioni, a pagina 11](#)
- [Requisiti di messa a terra, a pagina 11](#)
- [Requisiti di alimentazione, a pagina 11](#)
- [Requisiti del ricircolo d'aria, a pagina 12](#)
- [Requisiti di spazio, a pagina 12](#)

## Requisiti di temperatura

Gli switch e i server del cluster Cisco Secure Workload richiedono una temperatura di esercizio compresa tra 5 a 35 °C (tra 41 e 95 °F) con una diminuzione della temperatura massima di 1 °C ogni 305 m (1000 piedi) sopra il livello del mare. In condizioni di inattività, la temperatura deve essere compresa tra -40 e 65 °C (tra -40 e 149 °F).

## Requisiti di umidità

Un'umidità elevata può penetrare negli switch e nei server. L'umidità può causare la corrosione dei componenti interni e il conseguente degrado di proprietà come la resistenza elettrica, la conducibilità termica, la forza fisica e le dimensioni. Gli switch e i server sono classificati per funzionare a un'umidità relativa dal 10 al 90% con incrementi del 10 per cento all'ora. In condizioni non operative, questi dispositivi possono resistere a un'umidità relativa compresa tra il 5 e il 93%.

Gli edifici con aria condizionata nei mesi più caldi e riscaldamento in quelli più freddi solitamente mantengono un livello di umidità accettabile per i dispositivi. Se tuttavia i dispositivi sono installati in un locale più umido del normale, utilizzare un deumidificatore per mantenere un livello di umidità accettabile.

## Requisiti di altitudine

Se i dispositivi rack vengono utilizzati a quote elevate (bassa pressione), l'efficienza del raffreddamento forzato e per convezione si riduce, con conseguente formazione di archi elettrici o scariche a corona. In queste condizioni, inoltre, i componenti sigillati che hanno una certa pressione interna, come i condensatori elettrolitici, possono andare in avaria o funzionare con minore efficienza. Questi dispositivi sono progettati per funzionare ad altitudini comprese tra 0 e 3.050 m (tra 0 e 10.000 piedi) e possono essere conservati ad altitudini tra 0 e 12.000 m (tra 0 e 40.000 piedi).

## Requisiti di polvere e particolato

Le ventole raffreddano gli alimentatori, gli switch e i server aspirando l'aria ed espellendola tramite varie aperture presenti nello chassis. Le ventole tuttavia aspirano anche polvere e altre particelle che creano un accumulo di contaminanti nello switch e aumentano la temperatura interna dello chassis. Un ambiente operativo pulito può ridurre notevolmente gli effetti negativi di polvere e altre particelle, che agiscono come isolanti e interferiscono con i componenti meccanici degli switch e dei server.

Oltre alla pulizia regolare, attenersi alle seguenti precauzioni per evitare la contaminazione degli switch e dei server del rack:

- Non permettere che si fumi in prossimità del rack.
- Non permettere che si mangi o si beva in prossimità del rack.

## Riduzione delle interferenze elettromagnetiche e di radiofrequenza

Le interferenze elettromagnetiche (EMI, Electromagnetic Interference) e le interferenze di radiofrequenza (RFI, Radio Frequency Interference) dei dispositivi nel rack del cluster Cisco Secure Workload possono influire negativamente su altri dispositivi, quali ricevitori di radio e televisioni (TV) che funzionano in prossimità del rack. Le frequenze radio provenienti dai dispositivi del rack possono interferire anche con i telefoni cordless o a basso consumo energetico. Al contrario, le RFI emesse da telefoni con elevato consumo energetico possono causare la comparsa di caratteri spuri sul monitor del sistema.

Le interferenze di radiofrequenza (RFI) sono interferenze elettromagnetiche (EMI) superiori a 10 kHz. Questo tipo di interferenze può viaggiare dallo switch ad altri dispositivi tramite il cavo di alimentazione e l'alimentatore o attraverso l'aria sotto forma di onde radio trasmesse. La Federal Communications Commission (FCC) pubblica regolamenti specifici per limitare la quantità di EMI e RFI emesse dalle apparecchiature informatiche. Tutti gli switch sono conformi ai regolamenti della FCC.

Quando i cavi corrono per una distanza significativa all'interno di un campo elettromagnetico, tra il campo e i segnali sui fili possono verificarsi interferenze con le seguenti implicazioni:

- Se l'assetto del cablaggio è carente, quest'ultimo potrà emanare interferenze radio.
- Una forte EMI, specie se causata da fulmini o radiotrasmettitori, può distruggere i driver e i ricevitori di segnali nello chassis, e addirittura creare un rischio elettrico, conducendo sovratensioni nelle linee interne delle attrezzature.



**Nota** Per calcolare preventivamente e correggere le EMI di forte intensità, consultare un esperto in RFI.

Se si utilizzano cavi a doppino intrecciato con un'adeguata distribuzione dei conduttori di messa a terra, è improbabile che il cablaggio del sito produca interferenze radio. Se si superano le distanze consigliate, utilizzare ove necessario un cavo a doppino intrecciato di alta qualità con un conduttore di terra per ogni segnale dati.



**Attenzione** Se i cavi superano le distanze consigliate o passano tra diversi edifici, considerare in particolare gli effetti di un fulmine nelle vicinanze. L'impulso elettromagnetico causato da fulmini o altri fenomeni ad alta energia può facilmente scaricare nei conduttori non schermati una quantità di energia sufficiente a distruggere i dispositivi elettronici. Se in passato si sono verificati problemi di questo tipo, contattare esperti in soppressione e schermatura di sovratensioni.

## Requisiti di resistenza agli urti e alle vibrazioni

I dispositivi del cluster Cisco Secure Workload sono stati sottoposti a test antiurto e antivibrazioni per gli intervalli operativi, la movimentazione e gli standard antisismici.

## Requisiti di messa a terra

I dispositivi nel cluster Cisco Secure Workload sono sensibili alle variazioni di tensione degli alimentatori. Sovratensioni, sottotensioni, transienti o picchi possono cancellare i dati dalla memoria o causare guasti ai componenti. Per proteggersi da questo tipo di problemi, accertarsi di avere un collegamento di messa a terra per i dispositivi. Il rack deve essere collegato alla messa a terra dell'edificio.

I punti di messa a terra sullo chassis sono dimensionati per le viti M5. È necessario fornire le proprie viti, il terminale di messa a terra e il cavo di messa a terra. Il terminale di messa a terra deve avere due fori per viti M5. Il cavo di messa a terra fornito deve essere di 14 AWG (2 mm), resistente ad almeno 60 °C o comunque conforme alle normative locali.

## Requisiti di alimentazione

I cluster Cisco Secure Workload devono avere alimentatori che erogano le seguenti quantità di potenza per le operazioni:

- Piattaforma con fattore di forma grande da 39 RU, rack singolo: 22.500 W
- Piattaforma con fattore di forma grande da 39 RU, due rack: 11.500 W per ciascun rack
- Piattaforma con fattore di forma ridotto da 8 RU: 6.500 W

Per la ridondanza di alimentazione  $n+n$  richiesta, sono necessari due alimentatori CA, in grado di erogare ciascuno la quantità di potenza indicata.

Ogni chassis del rack ha due alimentatori, uno per le operazioni e l'altro per la ridondanza. Ogni alimentatore è collegato a una multipresa diversa sul rack e ogni multipresa è collegata a una fonte di alimentazione CA

diversa. In caso di guasto a un alimentatore, l'altro fornisce l'alimentazione necessaria per ogni switch o server del rack.

## Requisiti del ricircolo d'aria

Per il cluster Cisco Secure Workload, occorre posizionare ciascun rack con alimentatori e ventole ogni tre switch in un corridoio freddo. Se posizionati in questo modo, tutti i dispositivi nel rack aspirano aria di raffreddamento da un corridoio freddo e scaricano l'aria calda in un corridoio caldo.

## Requisiti di spazio

Nella tabella seguente viene indicato lo spazio necessario per installare il cluster Cisco Secure Workload con fattore di forma grande da 39 RU (rack singolo o due rack) o il fattore di forma ridotto da 8 RU. Il corridoio di installazione deve essere largo più di 59,69 cm (23,5 pollici) per poter spostare il rack. Inoltre, è necessario disporre di spazio sufficiente affinché una persona possa accedere alla parte anteriore e posteriore per effettuare interventi di manutenzione.

**Tabella 1: Requisiti di spazio**

Tipo di installazione	Larghezza minima del corridoio <sup>1</sup>	Spazio minimo per l'installazione in rack
Installazione di C1-Workload (rack singolo)	59,69 cm (23,5 pollici)	Larghezza 59,69 cm (23,5 pollici) x Profondità 126,492 cm (49,8 pollici)
C1-Workload (due rack)	59,69 cm (23,5 pollici)	Larghezza 119,38 cm (47 pollici) x Profondità 126,492 cm (49,8 pollici)
C1-Workload-M	59,69 cm (23,5 pollici)	Larghezza 59,69 cm (23,5 pollici) x Profondità 126,492 cm (49,8 pollici)

<sup>1</sup> Il corridoio di installazione e il corridoio su cui si apre la porta anteriore del rack devono essere larghi almeno 59,69 cm (23,5 pollici). L'altro corridoio, su cui si aprono le due porte dell'armadio, deve essere largo almeno 29,845 cm (11,75 pollici) per permettere l'apertura completa delle porte; tuttavia, per consentire l'accesso per la manutenzione, sono necessari almeno 59,69 cm (23,5 pollici).

Il rack è posizionato con le ventole degli switch (lato del rack con la porta più grande) rivolte verso il corridoio freddo e le porte degli switch (lato del rack con porte doppie) rivolte verso il corridoio caldo.





## CAPITOLO 3

# Messa a terra e collegamenti

---

- [Collegare a massa i dispositivi del cluster Cisco Secure Workload, a pagina 13](#)
- [Accendere i dispositivi del cluster Cisco Secure Workload, a pagina 13](#)
- [Collegare il cluster di Cisco Secure Workload ai router, a pagina 14](#)

## Collegare a massa i dispositivi del cluster Cisco Secure Workload

I collegamenti dei dispositivi del cluster Cisco Secure Workload sul rack sono metallo su metallo, quindi non appena si collega il rack (o i rack nelle installazioni a due rack) alla massa del data center, i dispositivi che fanno parte del rack vengono collegati a terra. Per collegare a terra un rack, collegare le ruote del rack alla messa a terra.

## Accendere i dispositivi del cluster Cisco Secure Workload

Per accendere lo switch, è necessario collegare due multiprese collegate al rack a due alimentatori CA.



---

**Nota** Collegare l'apparecchiatura alla rete CA dotata di un dispositivo di protezione da sovratensione (SPD) sull'apparecchiatura di servizio conforme alla norma NFPA 70, National Electrical Code (NEC).

Leggere le istruzioni di installazione prima di utilizzare, installare o collegare il sistema all'alimentatore.

Non sovraccaricare il cablaggio quando si collegano le unità al circuito di alimentazione.

---

### Prima di iniziare


- I rack devono essere installati nel data center e fissati in posizione con le prese d'aria posizionate in un corridoio freddo.
- I rack devono essere collegati alla messa a terra del data center.
- Il cluster deve essere collegato a due router forniti dal cliente (ciascun router collegato a uno switch leaf separato).

- Devono essere presenti due alimentatori che soddisfino i requisiti di alimentazione del rack a portata del cavo della multipresa.

**Passaggio 1**

Collegare il cavo di alimentazione di una multipresa a un alimentatore CA e il cavo di alimentazione della seconda multipresa a un diverso alimentatore CA.

**Passaggio 2**

Osservare gli alimentatori installati nei dispositivi del rack per verificare che il LED  sia acceso in verde.

- Se nessuno dei LED è acceso, verificare che l'alimentatore sia acceso e che l'interruttore di accensione/spengimento sulla multipresa del rack sia acceso.
- Se solo alcuni di questi LED sono accesi, verificare che il cavo di alimentazione proveniente dall'alimentatore sia collegato saldamente nella multipresa del rack.

## Collegare il cluster di Cisco Secure Workload ai router

Il cluster Cisco Secure Workload deve essere collegato a due router.

**Passaggio 1**

Per installare un cluster a due rack con fattore di forma grande da 39 RU, collegare i cavi dell'interfaccia parzialmente connessa a ciascun rack. Collegare quindi ciascun cavo alla porta etichettata sull'altro rack.

**Passaggio 2**

Utilizzare un cavo da 10 Gigabit per collegare un router alla porta E1/39 sullo switch leaf 1 per implementazioni a 39 RU oppure alla porta E1/47 per implementazioni a 8 RU. Lo switch leaf 1 si trova nella posizione seguente:

- Piattaforma a rack singolo con fattore di forma grande da 39 RU: RU 40 nel rack della piattaforma
- Piattaforma a due rack con fattore di forma grande da 39 RU: RU 40 nel rack 1
- Piattaforma con fattore di forma ridotto da 8 RU: RU 12 nel rack della piattaforma

**Passaggio 3**

Utilizzare un cavo da 10 Gigabit per collegare un router alla porta E1/39 sullo switch leaf 2 per implementazioni a 39 RU oppure alla porta E1/47 per implementazioni a 8 RU. Lo switch leaf 2 si trova nella posizione seguente:

- Piattaforma a rack singolo con fattore di forma grande da 39 RU: RU 41 nel rack della piattaforma
- Piattaforma a due rack con fattore di forma grande da 39 RU: RU 41 nel rack 2
- Piattaforma con fattore di forma ridotto da 8 RU: RU 11 nel rack della piattaforma



## CAPITOLO 4

# Configurazione dell'interfaccia utente

- (Facoltativo) [Requisiti e limitazioni per la modalità dual-stack \(supporto IPv6\)](#), a pagina 15
- [Configurazione dell'interfaccia utente](#), a pagina 16

## (Facoltativo) Requisiti e limitazioni per la modalità dual-stack (supporto IPv6)

I cluster Secure Workload eseguiti su hardware fisico possono essere configurati per utilizzare IPv6 oltre a IPv4 per determinate comunicazioni da e verso il cluster.



**Nota** È possibile utilizzare la modalità dual-stack (supporto IPv6) durante l'installazione o l'aggiornamento alle versioni 3.6.1.5, 3.7.1.5 e 3.8.1.1; tuttavia, l'opzione per abilitare la funzionalità non è disponibile durante l'installazione o l'aggiornamento di patch.

### Limiti

Per abilitare la modalità dual-stack, tenere presente quanto segue:

- È possibile abilitare la connettività IPv6 solo durante l'implementazione iniziale o l'aggiornamento a una versione principale (non è possibile abilitare questa funzione durante l'installazione di patch di aggiornamento).
- La modalità dual-stack è supportata solo su hardware fisico o cluster bare metal.
- Il supporto per la modalità solo IPv6 non è disponibile.
- Non è possibile ripristinare la modalità solo IPv4 dopo aver abilitato la modalità dual-stack per il cluster.
- Il backup e il ripristino dei dati (DBR) non sono supportati se è stata abilitata la connettività dual-stack.
- Non abilitare la modalità dual-stack per i cluster configurati con la Federazione.
- Le seguenti funzionalità usano sempre e solo IPv4 (ricordiamo che IPv4 è sempre abilitato, anche quando è abilitato IPv6):
  - (Applicabile alle versioni 3.8.1.1, 3.7.1.5 e 3.6.x) Applicazione sugli agenti AIX
  - (Applicabile solo alla release 3.6.x) Comunicazione dell'agente hardware con il cluster

- (Applicabile solo alla versione 3.6.x) Connettori per l'acquisizione di flussi, l'arricchimento dell'inventario o le notifiche di avviso

### Requisiti

- Configurare i record DNS A e AAAA per il nome di dominio completo prima di abilitare la modalità dual-stack per il cluster.
- Per motivi di ridondanza, i servizi esterni come NTP, SMTP e DNS devono essere disponibili sia su IPv4 che su IPv6.
- Per configurare la modalità dual-stack per un cluster:
  - A ciascuno dei due switch leaf del cluster deve essere assegnato un indirizzo IPv6 instradabile su due reti diverse, per motivi di ridondanza, ed è necessario fornire gateway predefiniti per ciascuna rete.
  - Per i cluster da 39RU, è necessaria una rete IPv6 indirizzabile al sito con spazio per almeno 29 indirizzi host.
  - Per i cluster da 8RU, è necessaria una rete IPv6 indirizzabile al sito con spazio per almeno 20 indirizzi host.
  - I primi tre indirizzi host della rete IPv6 indirizzabile al sito sono riservati alla configurazione HSRP del cluster Cisco Secure Workload e non devono essere utilizzati da altri dispositivi.

### Informazioni aggiuntive

Gli agenti comunicano con il cluster utilizzando IPv4, a meno che non siano configurati per utilizzare IPv6. Per istruzioni, vedere la Guida per l'utente di Cisco Secure Workload.

## Configurazione dell'interfaccia utente

### Prima di iniziare

- Per completare questa configurazione, è necessario un dispositivo come un laptop con una porta Ethernet e accesso a Internet.
- È inoltre necessario un cavo Ethernet per collegare il dispositivo al server più in alto nel cluster Cisco Secure Workload.
- Google Chrome è l'unico browser supportato per il portale di configurazione, obbligatorio per parte di questo processo.
- (Facoltativo) A partire dalla versione 3.6, è possibile configurare il cluster in modalità dual-stack, che consente di utilizzare sia IPv4 che IPv6 per la comunicazione tra alcuni componenti di Cisco Secure Workload e tra Cisco Secure Workload e servizi di rete come NTP e DNS. Cisco Secure Workload gestisce già il traffico IPv6, anche se non si abilita la modalità dual-stack. È possibile abilitare questo supporto solo durante l'implementazione o l'aggiornamento.

Per abilitare il supporto per IPv6, vedere [\(Facoltativo\) Requisiti e limitazioni per la modalità dual-stack \(supporto IPv6\)](#), a pagina 15.



---

**Importante** Immettere gli indirizzi IPv4 in tutti i campi della procedura seguente, a meno che il nome del campo non indichi esplicitamente IPv6.

---

**Passaggio 1** Configurare il dispositivo Internet con un indirizzo IP 2.2.2.1/30 (255.255.255.252).

**Passaggio 2** Utilizzare un cavo Ethernet per collegare la porta Ethernet sul dispositivo Internet alla porta LOM 2 (LAN2) sul server più in alto del cluster Cisco Secure Workload.

**Passaggio 3** Sul dispositivo Internet, aprire il browser Chrome e accedere a <http://2.2.2.2:9000>.

**Nota** Il browser Chrome è l'unico browser testato con questa procedura.

Viene visualizzata la pagina di configurazione della diagnostica.

**Passaggio 4** In caso di errori sulla pagina di diagnostica, verificare che le connessioni di cablaggio tra i dispositivi del cluster non siano interrotte e che i cavi non siano disposti in modo errato prima di continuare con questa procedura. Al termine, tornare al passaggio 2.

Vedere [Cablaggio dei dispositivi nel cluster C1-Workload, a pagina 21](#) e [Cablaggio dei dispositivi nel cluster C1-Workload-M, a pagina 34](#) per i cablaggi corretti.

**Passaggio 5** Fare clic su **Continue** (Continua).

Viene visualizzata la pagina di caricamento RPM.

**Nota** Se invece si apre la pagina di configurazione del sito, inserire il seguente URL per aprire la pagina di caricamento RPM:

**`http://2.2.2.2:9000 /upload`**

**Passaggio 6** Caricare i file RPM sul cloud di Cisco Secure Workload.

I file devono essere caricati nel seguente ordine:

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

- a) Fare clic su **Choose File** (Scegli file).
- b) Individuare un RPM, selezionarlo e fare clic su **Open** (Apri).
- c) Fare clic su **Upload** (Carica).

Quando si carica un RPM, l'elenco degli RPM sulla pagina non viene aggiornato. Si tratta di un comportamento normale.

Se viene visualizzato un errore durante il caricamento del file `tetration_os_mother_rpm_k9-2.1.1.31-1.e16.x86_64.rpm`, attendere circa 5-10 minuti e ricaricare la pagina. Dopo aver ricaricato la pagina, l'elenco dovrebbe includere anche gli RPM caricati. L'errore è dovuto al riavvio dell'orchestrator e non è un problema.

d) Ripetere i passaggi da a) a c) per ogni RPM.

Al termine del caricamento degli RPM, viene visualizzata la pagina di configurazione del sito.

### Passaggio 7

Utilizzare la pagina di configurazione del sito per impostare il nuovo sito nel modo seguente:

- Fare clic su **General** (Generale).

1. Nel campo **Site Name** (Nome sito), immettere il nome univoco del cluster.
2. Nel campo **SSH Public Key** (Chiave pubblica SSH), incollare la chiave di autenticazione.

**Nota** Generare la propria coppia di chiavi SSH utilizzabile per accedere all'SSH del cluster. Si raccomanda di tenere la chiave SSH in un luogo sicuro, non deteriorabile e accessibile per poterla usare nella risoluzione dei problemi o per ripristinare il cluster utilizzando l'accesso `ta_guest`.

3. Fare clic su **Next** (Avanti).

- Fare clic su **Email** (E-mail).

1. Inserire gli indirizzi e-mail richiesti.
2. Fare clic su **Next** (Avanti).

- Fare clic su **L3**.

Inserire gli indirizzi richiesti. Tutti i campi contrassegnati da \* sono obbligatori.

Immettere tutti gli indirizzi come IPv4, a meno che il nome del campo non specifichi IPv6.

(Facoltativo) Se si sta installando il software versione 3.6 o successive, per abilitare la modalità dual-stack (supporto per IPv4 e IPv6):

1. Selezionare la casella di controllo IPv6.
2. Immettere l'indirizzo IPv6 in notazione CIDR per gli switch leaf 1 e leaf 2.
3. Immettere il gateway predefinito IPv6 leaf 1 e leaf 2.
4. Fare clic su **Next** (Avanti).

- Fare clic su **Network** (Rete).

Immettere tutti gli indirizzi come IPv4, a meno che il nome del campo non specifichi IPv6.

1. Nel campo **Internal network IP address** (Indirizzo IP della rete interna), incollare l'indirizzo restituito dall'implementazione dell'orchestrator.
2. Nel campo **External network IP address** (Indirizzo IP della rete esterna), incollare l'indirizzo restituito dall'implementazione dell'orchestrator.
3. Nel campo **External gateway IP address** (Indirizzo IP del gateway esterno), incollare l'indirizzo restituito dall'implementazione dell'orchestrator.
4. Nel campo **DNS resolver IP address** (Indirizzo IP del resolver DNS), incollare l'indirizzo restituito dall'implementazione dell'orchestrator.
5. Nel campo **DNS domain** (Dominio DNS), inserire il dominio DNS (ad esempio, `cisco.com`).

6. (Versione software 3.6 o successive) Se è stato abilitato sulla pagina L3, **IPv6** viene selezionato automaticamente.

Se si seleziona IPv6, è necessario specificare gli indirizzi IPv6 riservati per l'utilizzo di Cisco Secure Workload:

- Immettere la **rete IPv6 esterna**.

I primi 3 indirizzi IPv6 nel campo IPv6 External Network (Rete esterna IPv6) sono sempre riservati agli switch del cluster Cisco Secure Workload e non devono essere utilizzati per altri scopi.

- Se si desidera utilizzare IPv6 solo per determinati indirizzi, immetterli nel campo **External IPv6 IPs** (IP IPv6 esterni).

- Nota**
- Per un cluster da 39 RU, verificare che nella rete esterna IPv6 o nell'elenco degli IP IPv6 esterni siano disponibili almeno 29 indirizzi IPv6.
  - Per un cluster da 8 RU, verificare che nella rete esterna IPv6 o nell'elenco degli IP IPv6 esterni siano disponibili almeno 20 indirizzi IPv6.

7. Fare clic su **Next** (Avanti).

- Fare clic su **Service** (Servizio).

1. Nel campo **NTP Servers** (Server NTP), inserire l'elenco separato da spazi dei nomi dei server NTP o degli indirizzi IP restituiti dall'implementazione dell'orchestrator.
2. Nel campo **SMTP Server** (Server SMTP), inserire il nome o l'indirizzo IP di un server SMTP utilizzabile da Cisco Secure Workload per inviare i messaggi e-mail. Questo server deve essere accessibile da Cisco Secure Workload.
3. Nel campo **SMTP Port** (Porta SMTP), inserire il numero di porta del server SMTP. AWS limita l'uso delle porte 25 e 465. È necessario configurare l'account correttamente o utilizzare la porta 587.
4. (Facoltativo) Nel campo **SMTP Username** (Nome utente SMTP), inserire il nome utente per l'autenticazione SMTP.
5. (Facoltativo) Nel campo **SMTP Password** (Password SMTP), inserire la password per l'autenticazione SMTP.
6. (Facoltativo) Nel campo **HTTP Proxy Server** (Server proxy HTTP), inserire il nome o l'indirizzo IP di un server proxy HTTP utilizzabile da Cisco Secure Workload per accedere ai servizi esterni su Internet.
7. (Facoltativo) Nel campo **HTTP Proxy Port** (Porta proxy HTTP), inserire il numero di porta per il server proxy HTTP.
8. (Facoltativo) Nel campo **HTTPs Proxy Server** (Server proxy HTTP), inserire il nome o l'indirizzo IP di un server proxy HTTPs utilizzabile da Cisco Secure Workload per accedere ai servizi esterni su Internet.
9. (Facoltativo) Nel campo **HTTPs Proxy Port** (Porta proxy HTTPs), inserire il numero di porta per il server proxy HTTPs.
10. (Facoltativo) Nel campo **Syslog Server** (Server syslog), inserire il nome o l'indirizzo IP di un server syslog utilizzabile da Cisco Secure Workload per inviare avvisi.

11. (Facoltativo) Nel campo **Syslog Port** (Porta syslog), inserire il numero di porta del server syslog.
  12. (Facoltativo) Nel campo **Syslog Severity** (Gravità syslog), inserire il livello di gravità dei messaggi syslog. Il livello può essere informativo, nota, avvertenza, errore, critico, avviso ed emergenza.
  13. Fare clic su **Next** (Avanti).
- Fare clic su **UI** (Interfaccia utente).
    1. Nel campo **UI VRRP VRID** (VRID VRRP UI), immettere **77** a meno che non si abbia bisogno di un VRID univoco.
    2. Nel campo **UI FQDN** (Nome di dominio completo UI), inserire il nome di dominio completo usato per accedere al cluster.
    3. Lasciare vuoto il campo **UI Airbrake Key** (Chiave Airbrake UI).
    4. Fare clic su **Next** (Avanti).  
Tetration (Cisco Secure Workload) convalida le impostazioni di configurazione e ne visualizza lo stato.
  - Fare clic su **Advanced** (Avanzate).
    1. Nel campo **External IPs** (IP esterni), inserire gli indirizzi IPv4.
    2. Fare clic su **Continue** (Continua).

**Passaggio 8**

In caso di errori, fare clic su **Back** (Indietro) e modificare la configurazione (vedere il passaggio 7).

**Nota** Una volta lasciata la pagina, non è più possibile modificare le impostazioni nella GUI di configurazione. Tuttavia, è sempre possibile modificare le impostazioni in un secondo momento dalla pagina dell'azienda nella GUI.

**Passaggio 9**

Se non si rilevano errori e non è necessario apportare modifiche alla configurazione, fare clic su **Continue** (Continua).

Cisco Secure Workload viene configurato in base alle impostazioni specificate. Questo processo richiede da una a due ore senza alcuna interazione da parte dell'utente.

**Operazioni successive**

Se è stato implementato il software 3.6 o versioni successive ed è stata abilitata la connettività IPv6:

- È possibile accedere al portale web Cisco Secure Workload utilizzando IPv4 o IPv6.
- Per impostazione predefinita, gli agenti software comunicano con il cluster Cisco Secure Workload utilizzando IPv4 anche se il cluster è abilitato a supportare IPv6. Per fare in modo che gli agenti supportati utilizzino IPv6 a questo scopo, è necessario configurare il campo **Sensor VIP FQDN** (Sensore VIP FQDN) nella pagina **Platform > Cluster Configuration** (Piattaforma > Configurazione cluster) del portale web Cisco Secure Workload. Per istruzioni importanti vedere la guida per l'utente, disponibile online sul portale web Cisco Secure Workload o all'indirizzo <https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html>.





## CAPITOLO 5

# Cablaggio dei dispositivi nel cluster C1 di Cisco Secure Workload

---

- [Cablaggio dei dispositivi nel cluster C1-Workload, a pagina 21](#)
- [Cablaggio dei dispositivi nel cluster C1-Workload-M, a pagina 34](#)

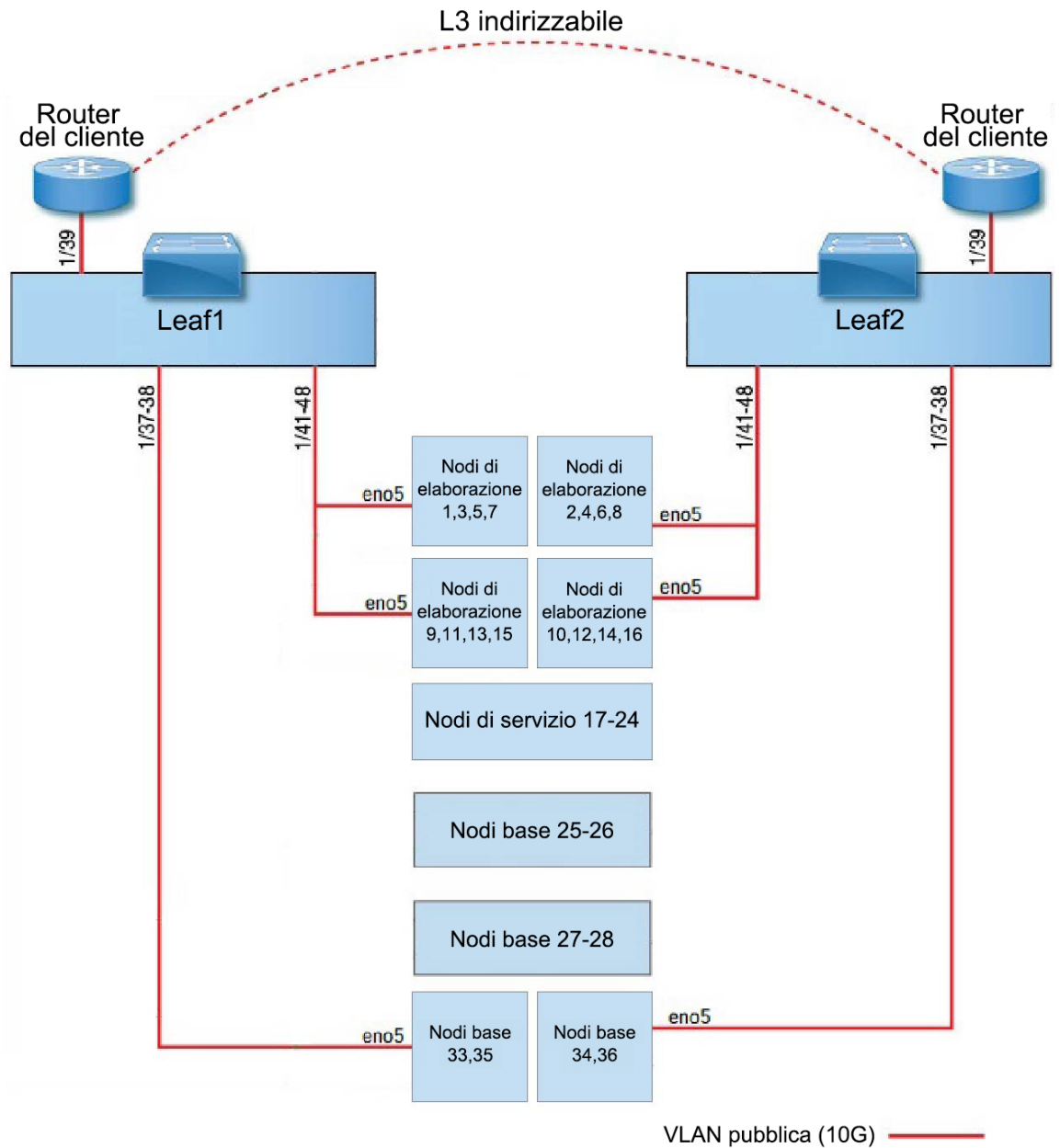
## Cablaggio dei dispositivi nel cluster C1-Workload

Prestare attenzione alle seguenti informazioni di configurazione quando si collega la scheda di interfaccia virtuale (VIC) M6 sul rack da 39 RU:

- Per tutti i nodi sono disponibili due interfacce private.
- Il rack da 39 RU ha un'interfaccia pubblica per 20 nodi.
- L'hardware M6 ha quattro porte per VIC.
- I nomi dell'interfaccia bare metal, ossia i server fisici del cluster noti come nodo di base, nodo di elaborazione e nodo di servizio, iniziano con "eno" (Ethernet onboard).

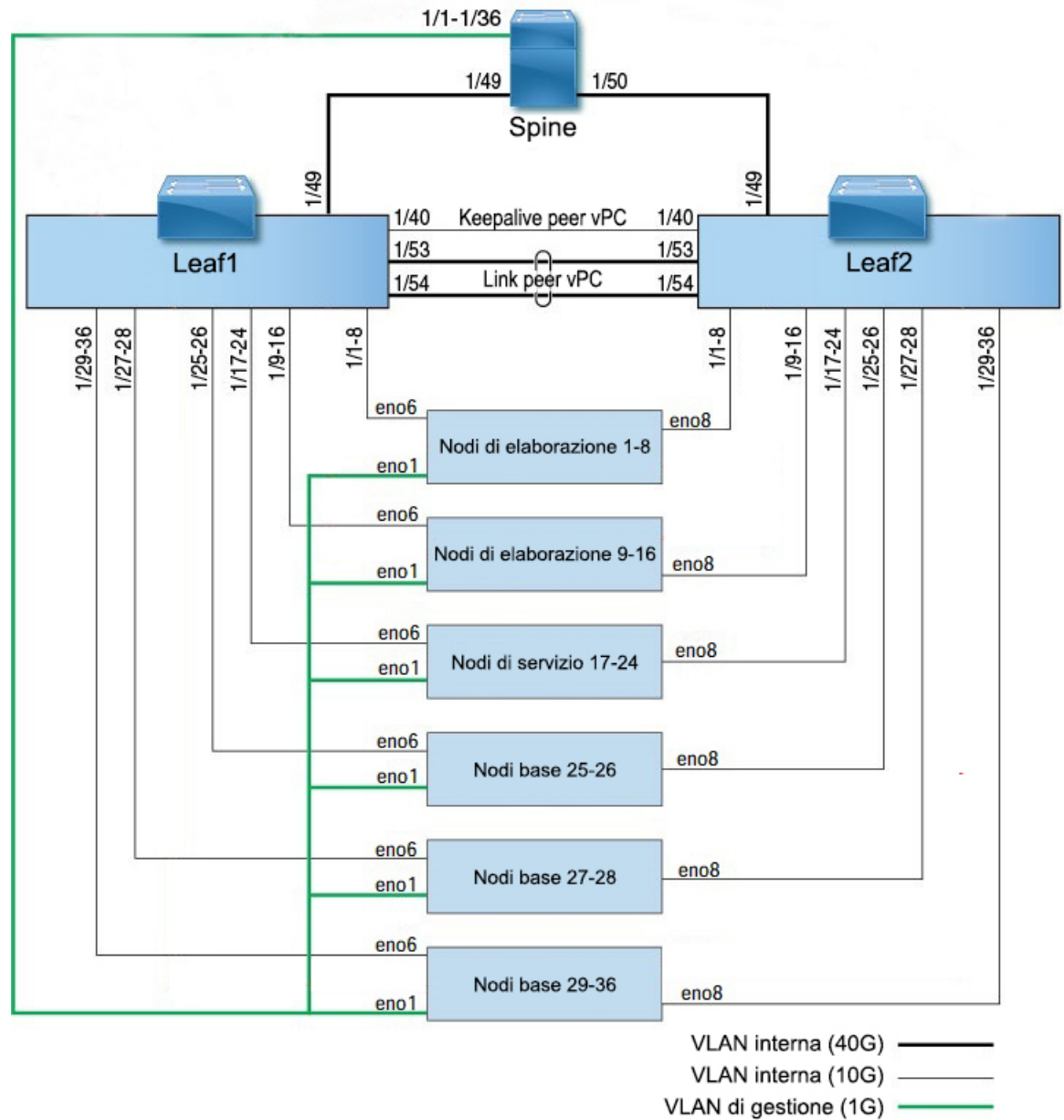
Nel diagramma seguente viene mostrato il cablaggio dei dispositivi per la configurazione pubblica/esterna del rack C1-Workload. Per un elenco dettagliato delle connessioni, vedere le tabelle che seguono i diagrammi.

Figura 7: Cablaggio dei dispositivi nel rack C1-Workload (pubblico/esterno)



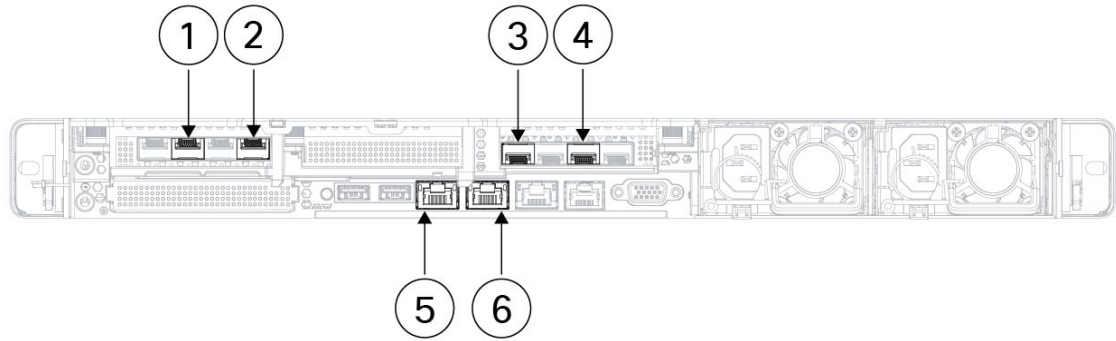
Nel diagramma seguente viene mostrato il cablaggio dei dispositivi per la configurazione interna/di gestione del rack C1-Workload. Per un elenco dettagliato delle connessioni, vedere le tabelle seguenti.

Figura 8: Cablaggio dei dispositivi nel rack C1-Workload (interno/di gestione)



Nella figura seguente vengono mostrate quali porte del server M6, indicate nelle figure sopra, corrispondono alle porte "eno":

Figura 9: Porte del server M6



<b>1</b>	Leaf 1 o leaf 2 pubblico a seconda del server Porta interfaccia server = eno5 Designazione CIMC = adattatore 1/porta fisica 2/vic-1-eth1	<b>2</b>	Leaf 1 privato Porta interfaccia server = eno6 Designazione CIMC = adattatore 1/porta fisica 0/vic-1-eth0
<b>3</b>	Leaf 2 privato Porta interfaccia server = eno8 Designazione CIMC = adattatore 3/porta fisica 0/vic-3-eth0	<b>4</b>	Non utilizzato Porta interfaccia server = eno7 Designazione CIMC = adattatore 3/porta fisica 2/vic-3-eth1
<b>5</b>	CIMC Porta interfaccia server = eno1 Designazione CIMC = LOM 1	<b>6</b>	MGMT 2.2.2.2 Porta interfaccia server = eno2 Designazione CIMC = LOM 2

Tabella 2: Connessioni degli switch spine (RU 42 nelle installazioni a rack singolo e nelle installazioni a due rack)

Porta spine	Tipo di connessione	Connessione			
		Dispositivo	RU nel rack singolo	RU in due rack	Porta
1/1	VLAN CIMC (1 Gigabit)	Host server UCS 1 (nodo di elaborazione)	RU 36	Rack1 RU 17	eno1
1/2	VLAN CIMC (1 Gigabit)	Host server UCS 2 (nodo di elaborazione)	RU 35	Rack1 RU 16	eno1
1/3	VLAN CIMC (1 Gigabit)	Host server UCS 3 (nodo di elaborazione)	RU 34	Rack1 RU 15	eno1
1/4	VLAN CIMC (1 Gigabit)	Host server UCS 4 (nodo di elaborazione)	RU 33	Rack1 RU 14	eno1
1/5	VLAN CIMC (1 Gigabit)	Host server UCS 5 (nodo di elaborazione)	RU 32	Rack1 RU 13	eno1

Porta spine	Tipo di connessione	Connessione			
		Dispositivo	RU nel rack singolo	RU in due rack	Porta
1/6	VLAN CIMC (1 Gigabit)	Host server UCS 6 (nodo di elaborazione)	RU 31	Rack 1 RU 12	eno1
1/7	VLAN CIMC (1 Gigabit)	Host server UCS 7 (nodo di elaborazione)	RU 30	Rack 1 RU 11	eno1
1/8	VLAN CIMC (1 Gigabit)	Host server UCS 8 (nodo di elaborazione)	RU 29	Rack 1 RU 10	eno1
1/9	VLAN CIMC (1 Gigabit)	Host server UCS 9 (nodo di elaborazione)	RU 28	Rack 1 RU 8	eno1
1/10	VLAN CIMC (1 Gigabit)	Host server UCS 10 (nodo di elaborazione)	RU 27	Rack 1 RU 7	eno1
1/11	VLAN CIMC (1 Gigabit)	Host server UCS 11 (nodo di elaborazione)	RU 26	Rack 1 RU 6	eno1
1/12	VLAN CIMC (1 Gigabit)	Host server UCS 12 (nodo di elaborazione)	RU 25	Rack 1 RU 5	eno1
1/13	VLAN CIMC (1 Gigabit)	Host server UCS 13 (nodo di elaborazione)	RU 24	Rack 1 RU 4	eno1
1/14	VLAN CIMC (1 Gigabit)	Host server UCS 14 (nodo di elaborazione)	RU 23	Rack 1 RU 3	eno1
1/15	VLAN CIMC (1 Gigabit)	Host server UCS 15 (nodo di elaborazione)	RU 22	Rack 1 RU 2	eno1
1/16	VLAN CIMC (1 Gigabit)	Host server UCS 16 (nodo di elaborazione)	RU 21	Rack 1 RU 1	eno1
1/17	VLAN CIMC (1 Gigabit)	Host server UCS 17 (nodo di servizio)	RU 20	Rack 2 RU 21	eno1
1/18	VLAN CIMC (1 Gigabit)	Host server UCS 18 (nodo di servizio)	RU 19	Rack 2 RU 20	eno1
1/19	VLAN CIMC (1 Gigabit)	Host server UCS 19 (nodo di servizio)	RU 18	Rack 2 RU 19	eno1
1/20	VLAN CIMC (1 Gigabit)	Host server UCS 20 (nodo di servizio)	RU 17	Rack 2 RU 18	eno1
1/21	VLAN CIMC (1 Gigabit)	Host server UCS 21 (nodo di servizio)	RU 16	Rack 2 RU 17	eno1

Porta spine	Tipo di connessione	Connessione			
		Dispositivo	RU nel rack singolo	RU in due rack	Porta
1/22	VLAN CIMC (1 Gigabit)	Host server UCS 22 (nodo di servizio)	RU 15	Rack2 RU 16	eno1
1/23	VLAN CIMC (1 Gigabit)	Host server UCS 23 (nodo di servizio)	RU 14	Rack2 RU 15	eno1
1/24	VLAN CIMC (1 Gigabit)	Host server UCS 24 (nodo di servizio)	RU 13	Rack2 RU 14	eno1
1/25	VLAN CIMC (1 Gigabit)	Host server UCS 25 (nodo base)	RU 12	Rack2 RU 12	eno1
1/26	VLAN CIMC (1 Gigabit)	Host server UCS 26 (nodo base)	RU 11	Rack2 RU 11	eno1
1/27	VLAN CIMC (1 Gigabit)	Host server UCS 27 (nodo base)	RU 10	Rack2 RU 10	eno1
1/28	VLAN CIMC (1 Gigabit)	Host server UCS 28 (nodo base)	RU 9	Rack2 RU 9	eno1
1/29	VLAN CIMC (1 Gigabit)	Host server UCS 29 (nodo base)	RU 8	Rack2 RU 8	eno1
1/30	VLAN CIMC (1 Gigabit)	Host server UCS 30 (nodo base)	RU 7	Rack2 RU 7	eno1
1/31	VLAN CIMC (1 Gigabit)	Host server UCS 31 (nodo base)	RU 6	Rack2 RU 6	eno1
1/32	VLAN CIMC (1 Gigabit)	Host server UCS 32 (nodo base)	RU 5	Rack2 RU 5	eno1
1/33	VLAN CIMC (1 Gigabit)	Host server UCS 33 (nodo base)	RU 4	Rack2 RU 4	eno1
1/34	VLAN CIMC (1 Gigabit)	Host server UCS 34 (nodo base)	RU 3	Rack2 RU 3	eno1
1/35	VLAN CIMC (1 Gigabit)	Host server UCS 35 (nodo base)	RU 2	Rack2 RU 2	eno1
1/36	VLAN CIMC (1 Gigabit)	Host server UCS 36 (nodo base)	RU 1	Rack2 RU 1	eno1
1/49	VLAN interna (40 Gigabit)	Switch leaf 1 (RU 41 nel rack singolo o RU 40 nel rack 1 in una configurazione a due rack)	RU 40	Rack1 RU 40	1/49

Porta spine	Tipo di connessione	Connessione			
		Dispositivo	RU nel rack singolo	RU in due rack	Porta
1/50	VLAN interna (40 Gigabit)	Switch leaf 2 (RU 40 nel rack singolo o RU 40 nel rack 2 in una configurazione a due rack), porta 49	RU 41	Rack 2 RU 40	1/50

**Tabella 3: Connessioni dello switch leaf 1 (RU 41 nelle installazioni a rack singolo e RU 40 nel rack 1 nelle installazioni a due rack)**

Porta leaf 1	Tipo di connessione	Connessione			
		Dispositivo	RU nel rack singolo	RU in due rack	Porta
1/1	VLAN interna (10 Gigabit)	Host server UCS 1 (nodo di elaborazione)	RU 36	Rack 1 RU 17	eno6
1/2	VLAN interna (10 Gigabit)	Host server UCS 2 (nodo di elaborazione)	RU 35	Rack 1 RU 16	eno6
1/3	VLAN interna (10 Gigabit)	Host server UCS 3 (nodo di elaborazione)	RU 34	Rack 1 RU 15	eno6
1/4	VLAN interna (10 Gigabit)	Host server UCS 4 (nodo di elaborazione)	RU 33	Rack 1 RU 14	eno6
1/5	VLAN interna (10 Gigabit)	Host server UCS 5 (nodo di elaborazione)	RU 32	Rack 1 RU 13	eno6
1/6	VLAN interna (10 Gigabit)	Host server UCS 6 (nodo di elaborazione)	RU 31	Rack 1 RU 12	eno6
1/7	VLAN interna (10 Gigabit)	Host server UCS 7 (nodo di elaborazione)	RU 30	Rack 1 RU 11	eno6
1/8	VLAN interna (10 Gigabit)	Host server UCS 8 (nodo di elaborazione)	RU 29	Rack 1 RU 10	eno6
1/9	VLAN interna (10 Gigabit)	Host server UCS 9 (nodo di elaborazione)	RU 28	Rack 1 RU 8	eno6
1/10	VLAN interna (10 Gigabit)	Host server UCS 10 (nodo di elaborazione)	RU 27	Rack 1 RU 7	eno6
1/11	VLAN interna (10 Gigabit)	Host server UCS 11 (nodo di elaborazione)	RU 26	Rack 1 RU 6	eno6
1/12	VLAN interna (10 Gigabit)	Host server UCS 12 (nodo di elaborazione)	RU 25	Rack 1 RU 5	eno6

Porta leaf 1	Tipo di connessione	Connessione			
		Dispositivo	RU nel rack singolo	RU in due rack	Porta
1/13	VLAN interna (10 Gigabit)	Host server UCS 13 (nodo di elaborazione)	RU 24	Rack1 RU 4	eno6
1/14	VLAN interna (10 Gigabit)	Host server UCS 14 (nodo di elaborazione)	RU 23	Rack1 RU 3	eno6
1/15	VLAN interna (10 Gigabit)	Host server UCS 15 (nodo di elaborazione)	RU 22	Rack1 RU 2	eno6
1/16	VLAN interna (10 Gigabit)	Host server UCS 16 (nodo di elaborazione)	RU 21	Rack1 RU 1	eno6
1/17	VLAN interna (10 Gigabit)	Host server UCS 17 (nodo di servizio)	RU 20	Rack2 RU 21	eno6
1/18	VLAN interna (10 Gigabit)	Host server UCS 18 (nodo di servizio)	RU 19	Rack2 RU 20	eno6
1/19	VLAN interna (10 Gigabit)	Host server UCS 19 (nodo di servizio)	RU 18	Rack2 RU 19	eno6
1/20	VLAN interna (10 Gigabit)	Host server UCS 20 (nodo di servizio)	RU 17	Rack2 RU 18	eno6
1/21	VLAN interna (10 Gigabit)	Host server UCS 21 (nodo di servizio)	RU 16	Rack2 RU 17	eno6
1/22	VLAN interna (10 Gigabit)	Host server UCS 22 (nodo di servizio)	RU 15	Rack2 RU 16	eno6
1/23	VLAN interna (10 Gigabit)	Host server UCS 23 (nodo di servizio)	RU 14	Rack2 RU 15	eno6
1/24	VLAN interna (10 Gigabit)	Host server UCS 24 (nodo di servizio)	RU 13	Rack2 RU 14	eno6
1/25	VLAN interna (10 Gigabit)	Host server UCS 25 (nodo base)	RU 12	Rack2 RU 12	eno6
1/26	VLAN interna (10 Gigabit)	Host server UCS 26 (nodo base)	RU 11	Rack2 RU 11	eno6
1/27	VLAN interna (10 Gigabit)	Host server UCS 27 (nodo base)	RU 10	Rack2 RU 10	eno6
1/28	VLAN interna (10 Gigabit)	Host server UCS 28 (nodo base)	RU 9	Rack2 RU 9	eno6



Porta leaf 1	Tipo di connessione	Connessione			
		Dispositivo	RU nel rack singolo	RU in due rack	Porta
1/29	VLAN interna (10 Gigabit)	Host server UCS 29 (nodo base)	RU 8	Rack2 RU 8	eno6
1/30	VLAN interna (10 Gigabit)	Host server UCS 30 (nodo base)	RU 7	Rack2 RU 7	eno6
1/31	VLAN interna (10 Gigabit)	Host server UCS 31 (nodo base)	RU 6	Rack2 RU 6	eno6
1/32	VLAN interna (10 Gigabit)	Host server UCS 32 (nodo base)	RU 5	Rack2 RU 5	eno6
1/33	VLAN interna (10 Gigabit)	Host server UCS 33 (nodo base)	RU 4	Rack2 RU 4	eno6
1/34	VLAN interna (10 Gigabit)	Host server UCS 34 (nodo base)	RU 3	Rack2 RU 3	eno6
1/35	VLAN interna (10 Gigabit)	Host server UCS 35 (nodo base)	RU 2	Rack2 RU 2	eno6
1/36	VLAN interna (10 Gigabit)	Host server UCS 36 (nodo base)	RU 1	Rack2 RU 1	eno6
1/37	VLAN pubblica (10 Gigabit)	Host server UCS 33 (nodo base)	RU 3	Rack2 RU 3	eno5
1/38	VLAN pubblica (10 Gigabit)	Host server UCS 35 (nodo base)	RU 1	Rack2 RU 1	eno5
1/39	VLAN interna (10 Gigabit)	Router cliente 1	—	—	—
1/40	VLAN interna (10 Gigabit)	Leaf 1	RU 40	Rack 1 RU 40	1/40
1/41	VLAN pubblica (10 Gigabit)	Host server UCS 1 (nodo di elaborazione)	RU 35	Rack 1 RU 16	eno5
1/42	VLAN pubblica (10 Gigabit)	Host server UCS 3 (nodo di elaborazione)	RU 33	Rack 1 RU 14	eno5
1/43	VLAN pubblica (10 Gigabit)	Host server UCS 5 (nodo di elaborazione)	RU 31	Rack 1 RU 12	eno5
1/44	VLAN pubblica (10 Gigabit)	Host server UCS 7 (nodo di elaborazione)	RU 29	Rack 1 RU 10	eno5
1/45	VLAN pubblica (10 Gigabit)	Host server UCS 9 (nodo di elaborazione)	RU 27	Rack 1 RU 8	eno5

Porta leaf 1	Tipo di connessione	Connessione			
		Dispositivo	RU nel rack singolo	RU in due rack	Porta
1/46	VLAN pubblica (10 Gigabit)	Host server UCS 11 (nodo di elaborazione)	RU 25	Rack1 RU 6	eno5
1/47	VLAN pubblica (10 Gigabit)	Host server UCS 13 (nodo di elaborazione)	RU 23	Rack1 RU 4	eno5
1/48	VLAN pubblica (10 Gigabit)	Host server UCS 15 (nodo di elaborazione)	RU 21	Rack1 RU 2	eno5
1/49	VLAN interna (40 Gigabit)	Switch spine	RU 42	Rack1 RU 42	1/49
1/50	—	—	—	—	—
1/51	—	—	—	—	—
1/52	—	—	—	—	—
1/53	VLAN interna (40 Gigabit)	Switch leaf 1	RU 40	Rack1 RU 40	1/53
1/54	VLAN interna (40 Gigabit)	Switch leaf 1	RU 40	Rack1 RU 40	1/54

**Tabella 4: Connessioni dello switch leaf 2 (RU 41 nelle installazioni a rack singolo o RU 40 nel rack 2 nelle installazioni a due rack)**

Porta leaf 2	Tipo di connessione	Connessione			
		Dispositivo	RU nel rack singolo	RU in due rack	Porta
1/1	VLAN interna (10 Gigabit)	Host server UCS 1 (nodo di elaborazione)	RU 36	Rack1 RU 17	eno8
1/2	VLAN interna (10 Gigabit)	Host server UCS 2 (nodo di elaborazione)	RU 35	Rack1 RU 16	eno8
1/3	VLAN interna (10 Gigabit)	Host server UCS 3 (nodo di elaborazione)	RU 34	Rack1 RU 15	eno8
1/4	VLAN interna (10 Gigabit)	Host server UCS 4 (nodo di elaborazione)	RU 33	Rack1 RU 14	eno8
1/5	VLAN interna (10 Gigabit)	Host server UCS 5 (nodo di elaborazione)	RU 32	Rack1 RU 13	eno8

Porta leaf 2	Tipo di connessione	Connessione			
		Dispositivo	RU nel rack singolo	RU in due rack	Porta
1/6	VLAN interna (10 Gigabit)	Host server UCS 6 (nodo di elaborazione)	RU 31	Rack 1 RU 12	eno8
1/7	VLAN interna (10 Gigabit)	Host server UCS 7 (nodo di elaborazione)	RU 30	Rack 1 RU 11	eno8
1/8	VLAN interna (10 Gigabit)	Host server UCS 8 (nodo di elaborazione)	RU 29	Rack 1 RU 10	eno8
1/9	VLAN interna (10 Gigabit)	Host server UCS 9 (nodo di elaborazione)	RU 28	Rack 1 RU 8	eno8
1/10	VLAN interna (10 Gigabit)	Host server UCS 10 (nodo di elaborazione)	RU 27	Rack 1 RU 7	eno8
1/11	VLAN interna (10 Gigabit)	Host server UCS 11 (nodo di elaborazione)	RU 26	Rack 1 RU 6	eno8
1/12	VLAN interna (10 Gigabit)	Host server UCS 12 (nodo di elaborazione)	RU 25	Rack 1 RU 5	eno8
1/13	VLAN interna (10 Gigabit)	Host server UCS 13 (nodo di elaborazione)	RU 24	Rack 1 RU 4	eno8
1/14	VLAN interna (10 Gigabit)	Host server UCS 14 (nodo di elaborazione)	RU 23	Rack 1 RU 3	eno8
1/15	VLAN interna (10 Gigabit)	Host server UCS 15 (nodo di elaborazione)	RU 22	Rack 1 RU 2	eno8
1/16	VLAN interna (10 Gigabit)	Host server UCS 16 (nodo di elaborazione)	RU 21	Rack 1 RU 1	eno8
1/17	VLAN interna (10 Gigabit)	Host server UCS 17 (nodo di servizio)	RU 20	Rack 2 RU 21	eno8
1/18	VLAN interna (10 Gigabit)	Host server UCS 18 (nodo di servizio)	RU 19	Rack 2 RU 20	eno8
1/19	VLAN interna (10 Gigabit)	Host server UCS 19 (nodo di servizio)	RU 18	Rack 2 RU 19	eno8
1/20	VLAN interna (10 Gigabit)	Host server UCS 20 (nodo di servizio)	RU 17	Rack 2 RU 18	eno8
1/21	VLAN interna (10 Gigabit)	Host server UCS 21 (nodo di servizio)	RU 16	Rack 2 RU 17	eno8

Porta leaf 2	Tipo di connessione	Connessione			
		Dispositivo	RU nel rack singolo	RU in due rack	Porta
1/22	VLAN interna (10 Gigabit)	Host server UCS 22 (nodo di servizio)	RU 15	Rack2 RU 16	eno8
1/23	VLAN interna (10 Gigabit)	Host server UCS 23 (nodo di servizio)	RU 14	Rack2 RU 15	eno8
1/24	VLAN interna (10 Gigabit)	Host server UCS 24 (nodo di servizio)	RU 13	Rack2 RU 14	eno8
1/25	VLAN interna (10 Gigabit)	Host server UCS 25 (nodo base)	RU 12	Rack2 RU 12	eno8
1/26	VLAN interna (10 Gigabit)	Host server UCS 26 (nodo base)	RU 11	Rack2 RU 11	eno8
1/27	VLAN interna (10 Gigabit)	Host server UCS 27 (nodo base)	RU 10	Rack2 RU 10	eno8
1/28	VLAN interna (10 Gigabit)	Host server UCS 28 (nodo base)	RU 9	Rack2 RU 9	eno8
1/29	VLAN interna (10 Gigabit)	Host server UCS 29 (nodo base)	RU 8	Rack2 RU 8	eno8
1/30	VLAN interna (10 Gigabit)	Host server UCS 30 (nodo base)	RU 7	Rack2 RU 7	eno8
1/31	VLAN interna (10 Gigabit)	Host server UCS 31 (nodo base)	RU 6	Rack2 RU 6	eno8
1/32	VLAN interna (10 Gigabit)	Host server UCS 32 (nodo base)	RU 5	Rack2 RU 5	eno8
1/33	VLAN interna (10 Gigabit)	Host server UCS 33 (nodo base)	RU 4	Rack2 RU 4	eno8
1/34	VLAN interna (10 Gigabit)	Host server UCS 34 (nodo base)	RU 3	Rack2 RU 3	eno8
1/35	VLAN interna (10 Gigabit)	Host server UCS 35 (nodo base)	RU 2	Rack2 RU 2	eno8
1/36	VLAN interna (10 Gigabit)	Host server UCS 36 (nodo base)	RU 1	Rack2 RU 1	eno8
1/37	VLAN pubblica (10 Gigabit)	Host server UCS 34 (nodo base)	RU 4	Rack2 RU 8	eno5
1/38	VLAN pubblica (10 Gigabit)	Host server UCS 36 (nodo base)	RU 2	Rack2 RU 6	eno5

Porta leaf 2	Tipo di connessione	Connessione			
		Dispositivo	RU nel rack singolo	RU in due rack	Porta
1/39	VLAN interna (10 Gigabit)	Router cliente 1	—	—	—
1/40	VLAN interna (10 Gigabit)	Switch leaf 2	RU 41	Rack 2 RU 40	1/40
1/41	VLAN pubblica (10 Gigabit)	Host server UCS 2 (nodo di elaborazione)	RU 36	Rack 1 RU 17	eno5
1/42	VLAN pubblica (10 Gigabit)	Host server UCS 4 (nodo di elaborazione)	RU 34	Rack 1 RU 15	eno5
1/43	VLAN pubblica (10 Gigabit)	Host server UCS 6 (nodo di elaborazione)	RU 32	Rack 1 RU 13	eno5
1/44	VLAN pubblica (10 Gigabit)	Host server UCS 8 (nodo di elaborazione)	RU 30	Rack 1 RU 11	eno5
1/45	VLAN pubblica (10 Gigabit)	Host server UCS 10 (nodo di elaborazione)	RU 28	Rack 1 RU 9	eno5
1/46	VLAN pubblica (10 Gigabit)	Host server UCS 12 (nodo di elaborazione)	RU 26	Rack 1 RU 7	eno5
1/47	VLAN pubblica (10 Gigabit)	Host server UCS 14 (nodo di elaborazione)	RU 24	Rack 1 RU 5	eno5
1/48	VLAN pubblica (10 Gigabit)	Host server UCS 16 (nodo di elaborazione)	RU 22	Rack 1 RU 3	eno5
1/49	VLAN interna (40 Gigabit)	Switch spine	RU 42	Rack 1 RU 42	—
1/50	—	—	—	—	1/50
1/51	—	—	—	—	—
1/52	—	—	—	—	—
1/53	VLAN interna (40 Gigabit)	Switch leaf 1	RU 40	Rack 1 RU 40	1/49
1/54	VLAN interna (40 Gigabit)	Switch leaf 2	RU 41	Rack 2 RU 40	1/50

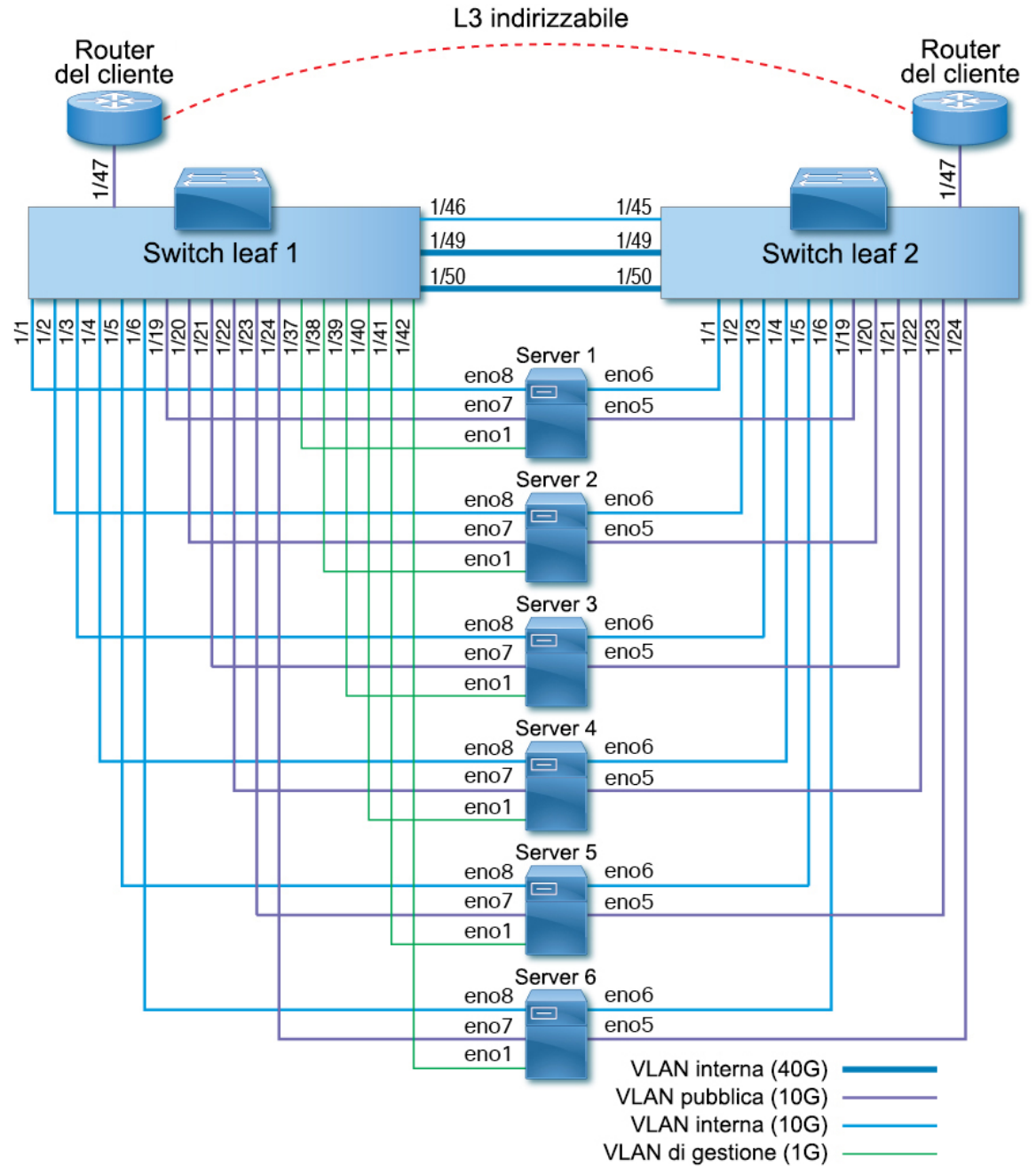
## Cablaggio dei dispositivi nel cluster C1-Workload-M

Per cablare M6 VIC sul rack a 8 RU, tenere in considerazione le seguenti informazioni sulla configurazione:

- Per tutti i nodi sono disponibili due interfacce private.
- Il rack a 8 RU ha due interfacce pubbliche per tutti e sei i nodi.
- L'hardware M6 ha quattro porte per VIC.
- I nomi dell'interfaccia bare metal, ossia il server fisico del cluster noto come nodo universale, iniziano con "eno" (Ethernet onboard).

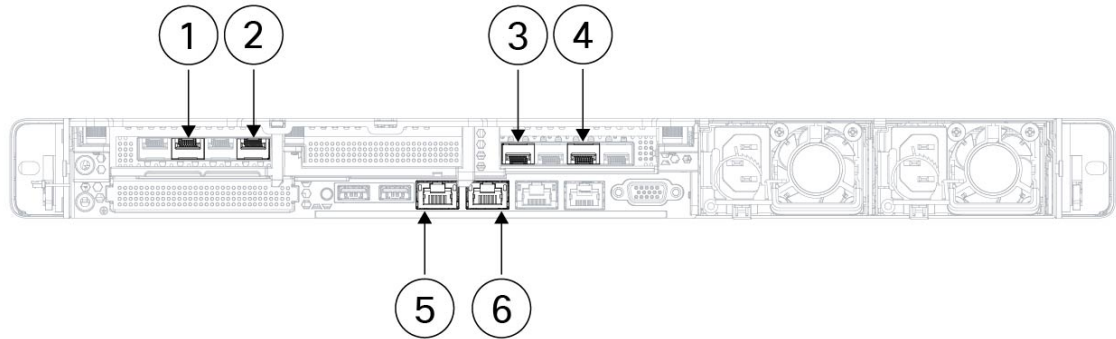
Lo schema seguente mostra il cablaggio dei dispositivi per la configurazione interna, di gestione, pubblica ed esterna del rack del cluster C1-Workload-M a 8 RU. Per un elenco dettagliato delle connessioni, vedere le tabelle che seguono il diagramma.

Figura 10: Cablaggio dei dispositivi del rack del cluster C1-Workload-M (configurazione interna, di gestione, pubblica, esterna)



Nella figura seguente vengono mostrate quali porte del server, indicate nel diagramma sopra, corrispondono alle porte "eno":

Figura 11: Porte del server M6



<b>1</b>	Leaf 2 pubblico Porta interfaccia server = eno5 Designazione CIMC = adattatore 1/porta fisica 2/vic-1-eth1	<b>2</b>	Leaf 2 privato Porta interfaccia server = eno6 Designazione CIMC = adattatore 1/porta fisica 0/vic-1-eth0
<b>3</b>	Leaf 1 privato Porta interfaccia server = eno8 Designazione CIMC = adattatore 3/porta fisica 0/vic-3-eth0	<b>4</b>	Leaf 1 pubblico Porta interfaccia server = eno7 Designazione CIMC = adattatore 3/porta fisica 2/vic3-eth1
<b>5</b>	CIMC Porta interfaccia server = eno1 Designazione CIMC = LOM 1	<b>6</b>	MGMT 2.2.2.2 Porta interfaccia server = eno2 Designazione CIMC = LOM 2

Tabella 5: Connessioni dello switch leaf 1 (RU 12)

Porta leaf	Tipo di connessione	Connessione		
		Dispositivo	RU nel rack singolo	Porta
1/1	VLAN interna (10 Gigabit)	Host server UCS 1 (nodo universale)	RU 9	eno8
1/2	VLAN interna (10 Gigabit)	Host server UCS 2 (nodo universale)	RU 8	eno8
1/3	VLAN interna (10 Gigabit)	Host server UCS 3 (nodo universale)	RU 6	eno8
1/4	VLAN interna (10 Gigabit)	Host server UCS 4 (nodo universale)	RU 5	eno8
1/5	VLAN interna (10 Gigabit)	Host server UCS 5 (nodo universale)	RU 3	eno8
1/6	VLAN interna (10 Gigabit)	Host server UCS 6 (nodo universale)	RU 2	eno8
1/7	—	—	—	—
1/8	—	—	—	—



Porta leaf	Tipo di connessione	Connessione		
		Dispositivo	RU nel rack singolo	Porta singolo
1/9	—	—	—	—
1/10	—	—	—	—
1/11	—	—	—	—
1/12	—	—	—	—
1/13	—	—	—	—
1/14	—	—	—	—
1/15	—	—	—	—
1/16	—	—	—	—
1/17	—	—	—	—
1/18	—	—	—	—
1/19	VLAN esterna (10 Gigabit)	Host server UCS 1 (nodo universale)	RU 9	eno7
1/20	VLAN esterna (10 Gigabit)	Host server UCS 2 (nodo universale)	RU 8	eno7
1/21	VLAN esterna (10 Gigabit)	Host server UCS 3 (nodo universale)	RU 6	eno7
1/22	VLAN esterna (10 Gigabit)	Host server UCS 4 (nodo universale)	RU 5	eno7
1/23	VLAN esterna (10 Gigabit)	Host server UCS 5 (nodo universale)	RU 3	eno7
1/24	VLAN esterna (10 Gigabit)	Host server UCS 6 (nodo universale)	RU 2	eno7
1/25	—	—	—	—
1/26	—	—	—	—
1/27	—	—	—	—
1/28	—	—	—	—
1/29	—	—	—	—
1/30	—	—	—	—
1/31	—	—	—	—
1/32	—	—	—	—
1/33	—	—	—	—

Porta leaf	Tipo di connessione	Connessione		
		Dispositivo	RU nel rack singolo	Porta singolo
1/34	—	—	—	—
1/35	—	—	—	—
1/36	—	—	—	—
1/37	VLAN di gestione (1 Gigabit)	Host server UCS 1 (nodo universale)	RU 9	eno1
1/38	VLAN di gestione (1 Gigabit)	Host server UCS 2 (nodo universale)	RU 8	eno1
1/39	VLAN di gestione (1 Gigabit)	Host server UCS 3 (nodo universale)	RU 6	eno1
1/40	VLAN di gestione (1 Gigabit)	Host server UCS 4 (nodo universale)	RU 5	eno1
1/41	VLAN di gestione (1 Gigabit)	Host server UCS 5 (nodo universale)	RU 3	eno1
1/42	VLAN di gestione (1 Gigabit)	Host server UCS 6 (nodo universale)	RU 2	eno1
1/43	—	—	—	—
1/44	—	—	—	—
1/45	—	—	—	—
1/46	VLAN interna (10 Gigabit)	Switch leaf 2	RU 11	1/45
1/47	VLAN esterna (10 Gigabit)	Router del cliente	—	—
1/48	—	—	—	—
1/49	VLAN interna (40 Gigabit)	Switch leaf 2	RU 11	1/49
1/50	VLAN interna (40 Gigabit)	Switch leaf 2	RU 11	1/50
1/51	—	—	—	—
1/52	—	—	—	—
1/53	—	—	—	—
1/54	—	—	—	—

Tabella 6: Connessioni dello switch leaf 2 (RU 11)

Porta leaf	Tipo di connessione	Connessione		
		Dispositivo	RU nel rack singolo	Porta singolo
1/1	VLAN interna (10 Gigabit)	Host server UCS 1 (nodo universale)	9 RU	eno6

Porta leaf	Tipo di connessione	Connessione		
		Dispositivo	RU nel rack singolo	Porta singolo
1/2	VLAN interna (10 Gigabit)	Host server UCS 2 (nodo universale)	8 RU	eno6
1/3	VLAN interna (10 Gigabit)	Host server UCS 3 (nodo universale)	6 RU	eno6
1/4	VLAN interna (10 Gigabit)	Host server UCS 4 (nodo universale)	5 RU	eno6
1/5	VLAN interna (10 Gigabit)	Host server UCS 5 (nodo universale)	3 RU	eno6
1/6	VLAN interna (10 Gigabit)	Host server UCS 6 (nodo universale)	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	VLAN esterna (10 Gigabit)	Host server UCS 1 (nodo universale)	9 RU	eno5
1/20	VLAN esterna (10 Gigabit)	Host server UCS 2 (nodo universale)	8 RU	eno5
1/21	VLAN esterna (10 Gb)	Host server UCS 3 (nodo universale)	6 RU	eno5
1/22	VLAN esterna (10 Gigabit)	Host server UCS 4 (nodo universale)	5 RU	eno5
1/23	VLAN esterna (10 Gigabit)	Host server UCS 5 (nodo universale)	3 RU	eno5
1/24	VLAN esterna (10 Gigabit)	Host server UCS 6 (nodo universale)	2 RU	eno5
1/25	—	—	—	—
1/26	—	—	—	—
1/27	—	—	—	—

Porta leaf	Tipo di connessione	Connessione		
		Dispositivo	RU nel rack singolo	Porta singolo
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	VLAN interna (10 Gigabit)	Switch leaf 1	12 RU	1/46
1/46	—	—	—	—
1/47	VLAN esterna (10 Gigabit)	Router del cliente	—	—
1/48	—	—	—	—
1/49	VLAN interna (40 Gigabit)	Switch leaf 1	12 RU	1/49
1/50	VLAN interna (40 Gigabit)	Switch leaf 1	12 RU	1/50
1/51	—	—	—	—
1/52	—	—	—	—
1/53	—	—	—	—

Porta leaf	Tipo di connessione	Connessione		
		Dispositivo	RU nel rack singolo	Porta
1/54	—	—	—	—





## CAPITOLO 6

# Specifiche del sistema

- [Specifiche ambientali, a pagina 43](#)
- [Cavi di alimentazione, a pagina 43](#)

## Specifiche ambientali

Nella seguente tabella sono elencate le specifiche ambientali necessarie per l'installazione del cluster Cisco Secure Workload.

*Tabella 7: Specifiche ambientali*

Ambiente		Specifica
Temperatura	In esercizio	Da 5 a 35 °C (da 41 a 95 °F) con riduzione della temperatura massima di 1 °C ogni 305 m (1000 piedi) sopra il livello del mare
	Archiviazione	Tra -40 e 65 °C (tra -40 e 149 °F)
Umidità	In esercizio	Dal 10 all'80% di umidità relativa con incrementi del 10% all'ora
	Archiviazione	Umidità relativa dal 5 al 93%
Altitudine	In esercizio	Da 0 a 3.050 m (da 0 a 10.000 piedi)
	Archiviazione	Da 0 a 40.000 m (da 0 a 12.200 piedi)

## Cavi di alimentazione

Nelle tabelle seguenti sono elencati i cavi di alimentazione inclusi nel cluster Cisco Secure Workload M6.

*Tabella 8: Configurazione del cluster da 39 RU a rack singolo*

Codice prodotto	Descrizione	Quantità
TA-RACK-UCS2-INT	Rack dinamico Cisco R42612 con pannelli laterali	1
TA-ETH-RJ45-SINGLE	Kit di cavi RJ-45 per una configurazione da 39 RU a rack singolo	1

Codice prodotto	Descrizione	Quantità
TA-SFP-H10GB-CU2M	Cavo 10GBASE-CU SFP+ da 2 m	16
TA-SFP-H10GB-CU1-5	Cavo 10GBASE-CU SFP+ da 1,5 m	32
TA-QSFP-H40G-CU1M	Cavo 40GBASE-CR4 in rame passivato da 1 m	4
TA-SFP-H10GB-CU1M	Cavo 10GBASE-CU SFP+ da 1 m	25
TA-SFP-H10GB-CU2-5	Cavo 10GBASE-CU SFP+ da 2,5 m	20

**Tabella 9: Configurazione del cluster da 39 RU a due rack**

Codice prodotto	Descrizione	Quantità
TA-RACK-UCS2-INT	Rack dinamico Cisco R42612 con pannelli laterali	2
TA-ETH-RJ45-DUAL	Kit di cavi RJ-45 per una configurazione da 39 RU a rack singolo	1
TA-SFP-H10GB-CU2M	Cavo 10GBASE-CU SFP+ da 2 m	15
TA-SFP-H10GB-CU1-5	Cavo 10GBASE-CU SFP+ da 1,5 m	19
TA-QSFP-H40G-CU1M	Cavo 40GBASE-CR4 in rame passivato da 1 m	1
TA-QSFP-H40G-CU5M	Cavo 40GBASE-CR4 in rame passivato da 5 m	3
TA-SFP-H10GB-CU2-5	Cavo 10GBASE-CU SFP+ da 2,5 m	12
TA-SFP-H10GB-CU5M	Cavo 10GBASE-CU SFP+ da 5 m	47

**Tabella 10: Cluster da 8 RU**

Codice prodotto	Descrizione	Quantità
TA-RACK-UCS2-INT	Rack dinamico Cisco R42612 con pannelli laterali	1
CAB-ETH-S-RJ45	Cavo RJ-45 dritto giallo da 6 piedi per Ethernet	6
TA-SFP-H10GB-CU1M	Cavo 10GBASE-CU SFP+ da 1 m	13
TA-SFP-H10GB-CU1-5	Cavo 10GBASE-CU SFP+ da 1,5 m	12
TA-QSFP-H40G-CU1M	Cavo 40GBASE-CR4 in rame passivato da 1 m	2
GLC-TE	Modulo ricetrasmittitore SFP 1000BASE-T per filo di rame categoria 5	6