



Guia de implementação do cluster Cisco Secure Workload M6

Primeira publicação: 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.

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. Todos os direitos reservados.



ÍNDICE

CAPÍTULO 1

Descrição geral 1

- Descrição geral 1
- Painel frontal do Servidor Cisco UCS C220 M6 5
- Painel traseiro do Servidor Cisco UCS C220 M6 6

CAPÍTULO 2

Preparar o local 9

- Requisitos de temperatura 9
- Requisitos de humidade 9
- Requisitos de altitude 10
- Requisitos relacionados com pó e partículas 10
- Minimizar as interferências eletromagnéticas e de radiofrequências 10
- Requisitos relacionados com impactos e vibrações 11
- Requisitos de ligação à terra 11
- Requisitos de potência 11
- Requisitos de fluxo de ar 12
- Requisitos de espaço de intervalo 12

CAPÍTULO 3

Ligação à terra e conexão 13

- Ligar os dispositivos de cluster Secure Workload à terra 13
- Ligar a alimentação dos dispositivos de cluster Secure Workload 13
- Ligar o cluster Secure Workload aos seus routers 14

CAPÍTULO 4

Configurar a interface do utilizador 15

- (Opcional) Requisitos e limitações para o modo Dual-Stack (suporte para IPv6) 15
- Configurar a interface do utilizador 16

CAPÍTULO 5	Cablagem do dispositivo de cluster C1-Secure Workload	21
	Cablagem do dispositivo de cluster C1-Workload	21
	Cablagem do dispositivo de cluster C1-Workload-M	34

CAPÍTULO 6	Especificações do sistema	43
	Especificações ambientais	43
	Cabos de alimentação	43



CAPÍTULO 1

Descrição geral

- [Descrição geral, na página 1](#)
- [Painel frontal do Servidor Cisco UCS C220 M6, na página 5](#)
- [Painel traseiro do Servidor Cisco UCS C220 M6, na página 6](#)

Descrição geral

Pode implementar o cluster Cisco Secure Workload M6 de uma das seguintes formas:

- Plataforma 39-RU de formato grande (C1-Workload de um rack) para centros de dados com mais de 5000 servidores

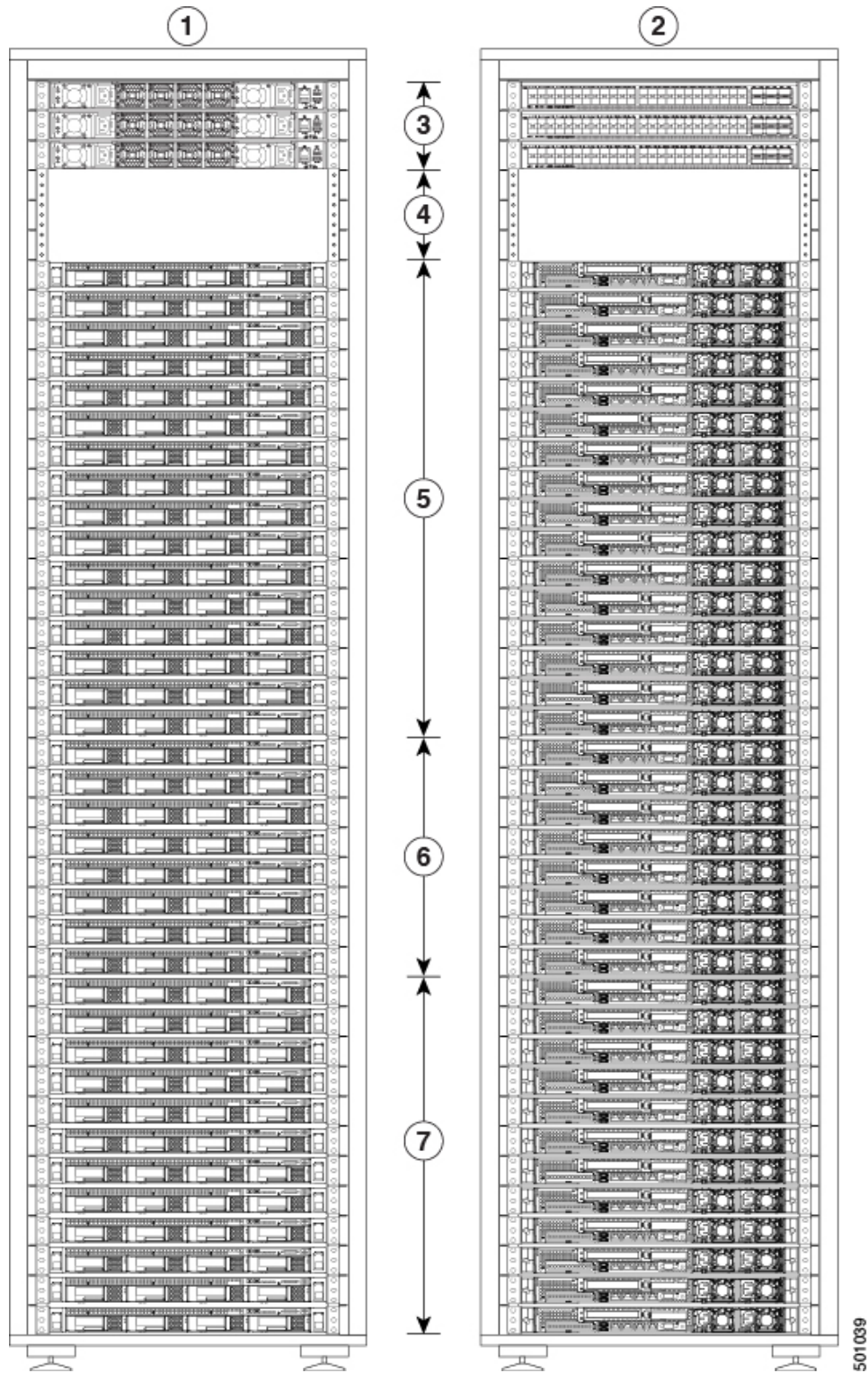


Nota Pode implementar a plataforma de formato grande em um ou dois racks, dependendo dos seus requisitos. Consulte as seguintes figuras do C1-Workload de um rack e rack duplo para obter exemplos.

- Plataforma 8-RU de formato pequeno (C1-Workload-M) para centros de dados com menos de 5000 servidores. Consulte a figura do C1-Workload-M para obter o exemplo.

A figura seguinte apresenta a frente e traseira do C1-Workload de um rack.

Figura 1: C1-Workload de um rack – Frente e traseira

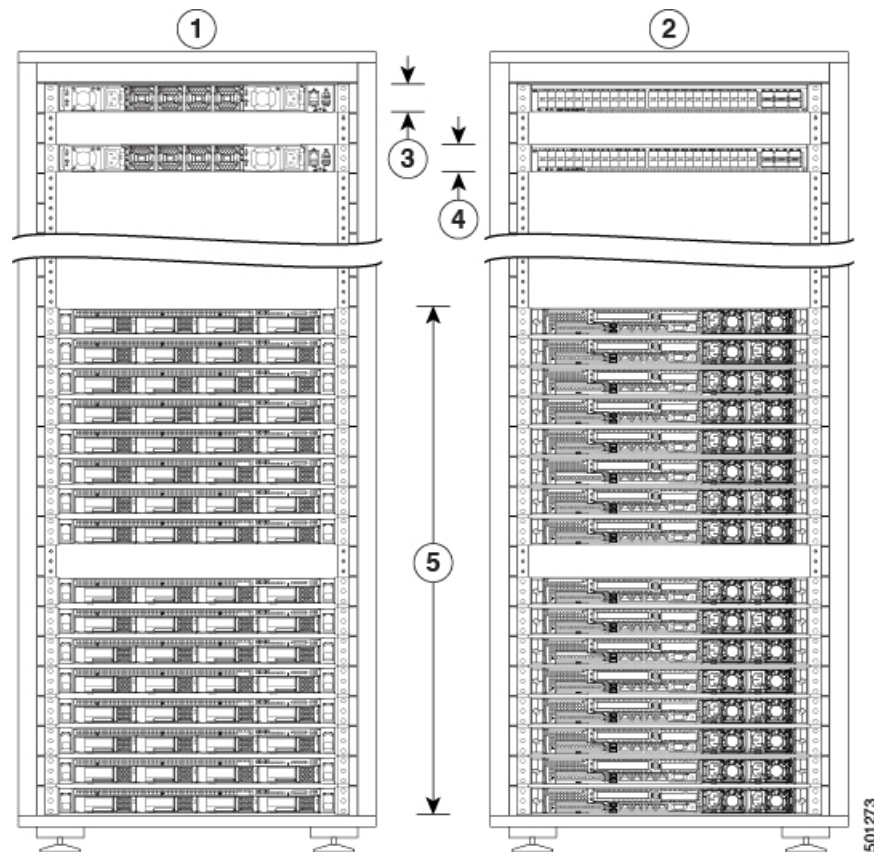


1 Frente (vista da ala fria)	2 Traseira (vista da ala quente)
------------------------------	----------------------------------

3	Um switch spine (RU 42) e dois switches leaf: leaf 2 (RU 40) e leaf 1 (RU 41)	4	Unidades de rack aberto (RU 37 a 39)
5	16 servidores de computação (RU 21 a 36)	6	Oito servidores de serviço (RU 13 a 20)
7	12 servidores base (RU 1 a 12)		—

A figura seguinte apresenta a frente e traseira do rack 1 do C1-Workload de rack duplo.

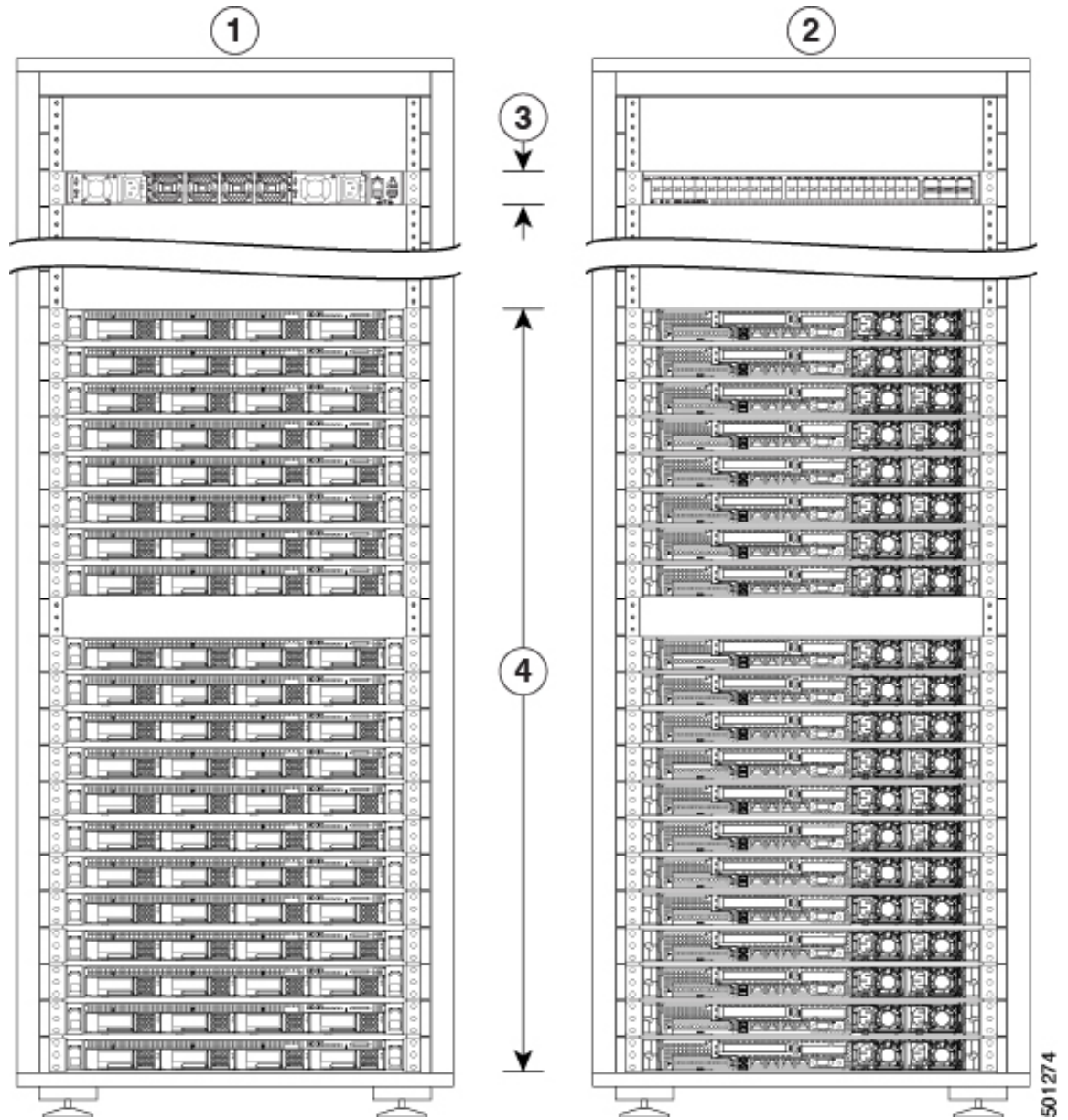
Figura 2: C1-Workload de rack duplo—Rack 1 frente e traseira



1	Frente (vista da ala fria)	2	Traseira (vista da ala quente)
3	Um switch spine (RU 42)	4	Switch Leaf 1 (RU 40)
5	16 servidores de computação (RU 1 a 4 e 6 a 9)	6	—

A figura seguinte apresenta a frente e traseira do rack 2 do C1-Workload de rack duplo.

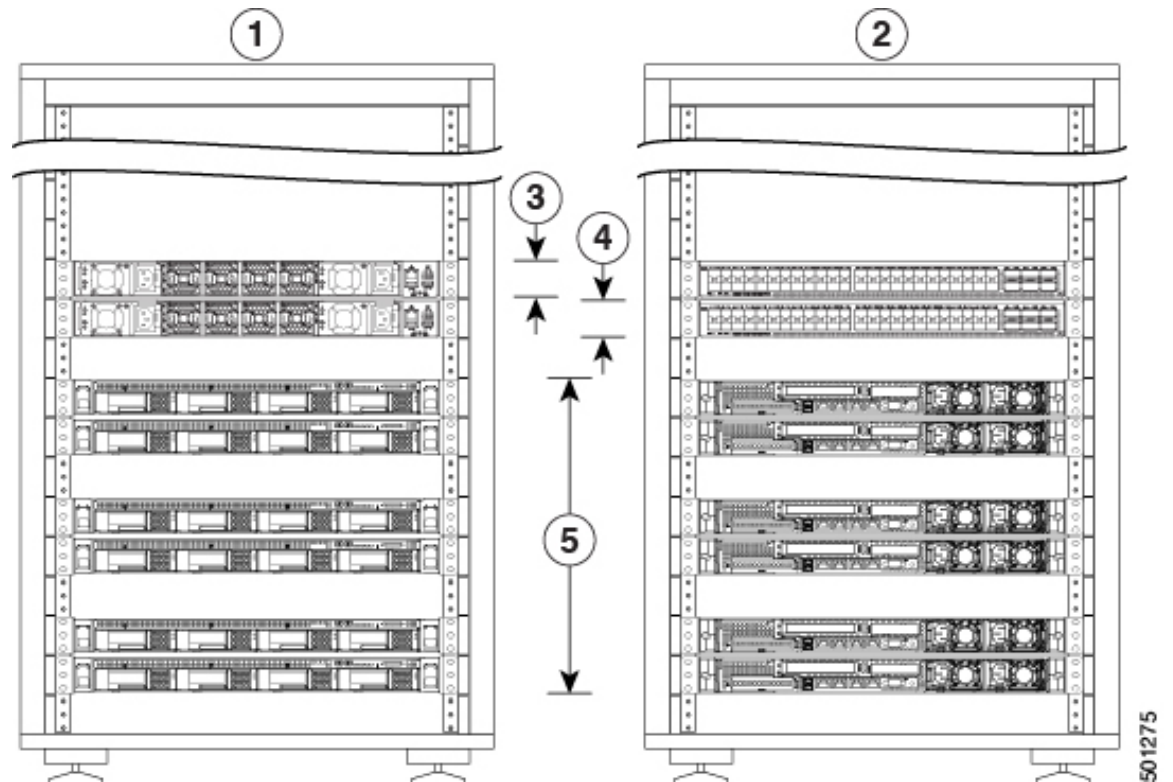
Figura 3: C1-Workload de rack duplo—Rack 2 frente e traseira



<p>1 Frente (vista da ala fria)</p>	<p>2 Traseira (vista da ala quente)</p>
<p>3 Switch Leaf 2 (RU 40)</p>	<p>4 Oito servidores de serviço (RU 14 a 21) e 12 servidores base (RU 1 a 12)</p>

A figura seguinte apresenta a frente e traseira do C1-Workload-M.

Figura 4: C1-Workload-M – Frente e traseira



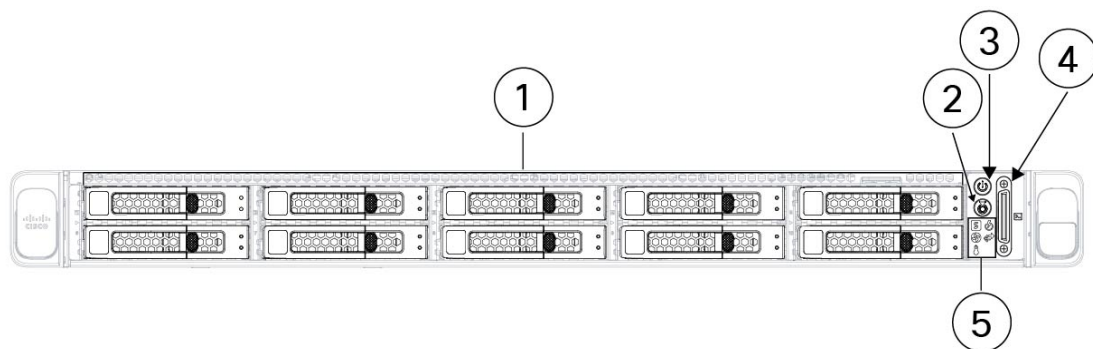
1	Frente (vista da ala fria)	2	Traseira (vista da ala quente)
3	Switch Leaf 1 (RU 12)	4	Switch Leaf 2 (RU 11)
5	Seis servidores universais (RU 2, 3, 5, 6, 8 e 9)		—

Painel frontal do Servidor Cisco UCS C220 M6

A figura seguinte apresenta o painel frontal do servidor UCS C220 M6 com unidades de formato pequeno (SFF).

Consulte o [Guia de serviço e instalação do Servidor Cisco UCS C220 M6](#) para mais informações.

Figura 5: Painel frontal do Servidor Cisco UCS C220 M6



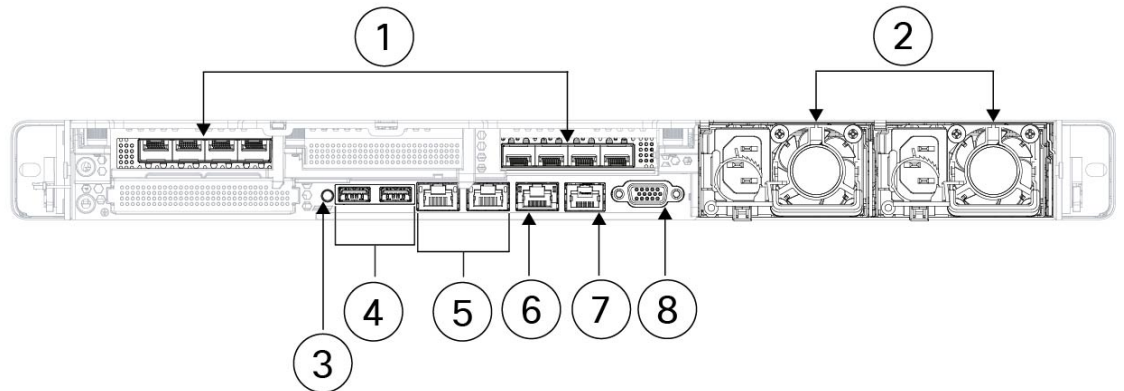
<p>1 Compartimentos de unidades 1 a 10, numerados da esquerda para a direita, de cima para baixo</p> <p>Suporta HDDs e SSDs SAS/SATA. Como opção, os compartimentos de unidades 1 a 4 podem conter até 4 unidades NVMe em qualquer número, até 4. Os compartimentos de unidades 5 a 10 apenas suportam HDDs ou SSDs SAS/SATA.</p>	<p>2 Botão de identificação de unidade/LED</p>
<p>3 LED de estado de alimentação/botão de alimentação</p>	<p>4 Conector KVM</p> <p>Utilizado com um cabo KVM que fornece um conector VGA DB-15, um DB-9 de série e dois USB 2.0.</p>
<p>5 LEDs do sistema:</p> <ul style="list-style-type: none"> • LED de estado da ventoinha • LED de estado do sistema • LED de estado da fonte de alimentação • LED de atividade de ligação de rede • LED de estado da temperatura 	<p>—</p>

Painel traseiro do Servidor Cisco UCS C220 M6

A figura seguinte apresenta o painel traseiro do Servidor UCS C220 M6.

Consulte o [Guia de serviço e instalação do Servidor Cisco UCS C220 M6](#) para mais informações.

Figura 6: Painel traseiro do Servidor Cisco UCS C220 M6



1	<p>Duas ranhuras PCIe</p> <ul style="list-style-type: none"> • Riser 1 (controlado pela CPU 1) <ul style="list-style-type: none"> • Suporta uma ranhura PCIe (ranhura 1) • A ranhura 1 tem meia altura, 3/4 de comprimento, x16 • Riser 3 (controlado pela CPU 2) <ul style="list-style-type: none"> • Suporta uma ranhura PCIe (ranhura 3) • A ranhura 3 tem meia altura, 3/4 de comprimento, x16 	2	<p>Duas unidades de fonte de alimentação (PSUs), que são redundantes quando configuradas no modo de alimentação 1+1</p>
3	Botão de identificação de sistema/LED	4	Duas portas USB 3.0
5	<p>Portas Ethernet duplas 1 Gb/10 Gb (LAN1 e LAN2)</p> <p>As portas LAN duplas suportam 1 Gbps e 10 Gbps, dependendo da capacidade do parceiro de ligação.</p>	6	Porta de gestão dedicada Ethernet de 1 Gb
7	Porta COM (conector RJ-45)	8	Porta de vídeo VGA (conector DB-15)



CAPÍTULO 2

Preparar o local

- [Requisitos de temperatura, na página 9](#)
- [Requisitos de humidade, na página 9](#)
- [Requisitos de altitude, na página 10](#)
- [Requisitos relacionados com pó e partículas, na página 10](#)
- [Minimizar as interferências eletromagnéticas e de radiofrequências, na página 10](#)
- [Requisitos relacionados com impactos e vibrações, na página 11](#)
- [Requisitos de ligação à terra, na página 11](#)
- [Requisitos de potência, na página 11](#)
- [Requisitos de fluxo de ar, na página 12](#)
- [Requisitos de espaço de intervalo, na página 12](#)

Requisitos de temperatura

Os switches e servidores do cluster Secure Workload requerem uma temperatura de funcionamento de 5 a 35 °C, com uma redução da temperatura máxima de 1 °C por cada 305 m de elevação acima do nível do mar. Se estes dispositivos não estiverem a funcionar, a temperatura tem de situar-se entre -40 e 65 °C.

Requisitos de humidade

Um grau de humidade elevado pode provocar a entrada de humidade nos switches e servidores. A humidade pode provocar a corrosão de componentes internos e a degradação de propriedades como resistência elétrica, condutividade térmica, resistência física e dimensões. Os switches e os servidores estão classificados para funcionarem com uma humidade relativa de 10 a 90%, com uma gradação de humidade de 10% por hora. Em condições de não funcionamento, estes dispositivos resistem a uma humidade relativa entre 5 e 93%.

Os edifícios em que o ambiente é controlado por ar condicionado nos meses mais quentes e por aquecimento durante os meses mais frios mantêm, normalmente, um nível aceitável de humidade para os dispositivos. No entanto, se os dispositivos se encontrarem num local exceccionalmente húmido, deve utilizar um desumidificador por forma a manter a humidade dentro de um grau aceitável.

Requisitos de altitude

Se utilizar os dispositivos de rack a uma alta altitude (baixa pressão), a eficiência da refrigeração forçada e de convecção é reduzida e pode resultar em problemas elétricos relacionados com efeitos de arco elétrico e corona. Esta situação também pode provocar a falha ou a redução de eficiência de componentes selados com pressão interna, como condensadores eletrolíticos. A classificação destes dispositivos permite o seu funcionamento a altitudes de 0 a 3050 m e o seu armazenamento a altitudes de 12 200 m.

Requisitos relacionados com pó e partículas

As ventoinhas refrigeram as fontes de alimentação, os switches e os servidores puxando ar para dentro e extraíndo ar através das várias aberturas do chassi. No entanto, as ventoinhas também puxam pó e outras partículas, provocando uma acumulação de agentes contaminantes no switch e um aumento da temperatura interna do chassi. Um ambiente de operação limpo permite reduzir significativamente os efeitos negativos do pó e outras partículas, os quais atuam como isolamento e interferem com os componentes mecânicos nos switches e servidores.

Além da limpeza regular, siga estas precauções para evitar uma contaminação dos switches e servidores de rack:

- Não permita que se fume próximo do rack.
- Não permita que se coma ou beba próximo do rack.

Minimizar as interferências eletromagnéticas e de radiofrequências

As interferências eletromagnéticas (EMI) e interferências de radiofrequências (RFI) dos dispositivos no rack do cluster Secure Workload podem afetar negativamente outros dispositivos, como recetores de rádio e televisão (TV) a funcionar próximo do rack. As radiofrequências emitidas pelos dispositivos no rack também podem interferir em telefones sem fios e de baixa potência. Por outro lado, as interferências de radiofrequência (RFI) de telefones de alta potência podem levar ao aparecimento de falsos caracteres nos monitores dos dispositivos.

As RFI são quaisquer interferências eletromagnéticas (EMI) com uma frequência superior a 10 kHz. Este tipo de interferência pode passar do switch para outros dispositivos através do cabo de alimentação e da fonte de alimentação ou pelo ar, como ondas de rádio. A Comissão Federal de Comunicações (FCC) publica regulamentos específicos que limitam a quantidade de EMI e RFI que pode ser emitida por equipamento informático. Todos os switches cumprem estes regulamentos da FCC.

Se passarem fios ao longo de uma distância significativa num campo eletromagnético, podem ocorrer interferências entre o campo e os sinais nos fios, com as seguintes implicações:

- Uma instalação elétrica incorreta pode provocar interferências de rádio emitidas pela cablagem da instalação.

- EMI fortes, especialmente quando provocadas por relâmpagos ou transmissores de rádio, podem destruir os controladores de sinal e recetores no chassi e até resultar em perigo elétrico pela passagem de picos de corrente nas linhas para o equipamento.



Nota Para prever e prevenir interferências eletromagnéticas (EMI) fortes, consulte especialistas em interferências de radiofrequência (RFI).

A cablagem não deverá emitir interferências de rádio se utilizar um cabo de par trançado com boa distribuição de condutores de ligação à terra. Se exceder as distâncias recomendadas, utilize um cabo de par trançado de alta qualidade com um condutor de ligação à terra para cada sinal de dados, se aplicável.



Atenção Se os fios excederem as distâncias recomendadas ou se passarem entre edifícios, tenha especial atenção ao efeito de um relâmpago nas proximidades. O impulso eletromagnético provocado por relâmpagos ou outros fenómenos de elevada energia pode transmitir facilmente a condutores não blindados níveis de energia suficientes para destruir dispositivos eletrónicos. Consulte especialistas em supressão de picos elétricos e blindagem se já tiver passado por problemas semelhantes anteriormente.

Requisitos relacionados com impactos e vibrações

Os dispositivos de cluster Secure Workload foram testados a nível de impactos e vibrações de acordo com padrões de gamas operacionais, manuseamento e sismos.

Requisitos de ligação à terra

Os dispositivos no cluster Secure Workload são sensíveis a variações de tensão das fontes de alimentação. Situações de sobretensão, subtensão e transientes (ou picos) podem apagar dados da memória ou provocar a falha dos componentes. Como proteção contra estes tipos de problemas, certifique-se de que há ligação à terra para os dispositivos. Tem de ligar o rack à instalação de terra do edifício.

Os pontos de ligação à terra no chassi têm um tamanho adequado para parafusos M5. O utilizador tem de providenciar os seus próprios parafusos, lingueta de terra e fio de terra. A lingueta de terra tem de ser uma lingueta de orifício duplo compatível com parafusos M5. O cabo de ligação à terra que providenciar tem de ser um fio 14 AWG (2 mm), para 60 °C, no mínimo, ou conforme permitido pelas normas locais.

Requisitos de potência

Os clusters Secure Workload têm de ter fontes de alimentação que forneçam as seguintes quantidades de energia para as operações:

- Plataforma de formato grande 39-RU, um rack: 22 500 W
- Plataforma de formato grande 39-RU, rack duplo: 11 500 W para cada rack
- Plataforma de formato pequeno 8-RU: 6500 W

Para a redundância de energia $n+n$ necessária, são precisas duas fontes de alimentação CA que forneçam, cada uma, essa quantidade de energia.

Cada chassi no rack tem duas fontes de alimentação, uma para as operações e outra para redundância. Cada fonte de alimentação é ligada a uma extensão elétrica diferente no rack, e cada extensão elétrica é ligada a uma fonte de alimentação CA diferente. Se uma fonte de alimentação falhar, a outra fornece a energia necessária para cada switch ou servidor no rack.

Requisitos de fluxo de ar

O cluster Secure Workload requer que posicione cada rack com as fontes de alimentação e as ventoinhas nos três switches numa ala fria. Quando posicionado desta forma, todos os dispositivos no rack recebem ar de refrigeração de uma ala fria e expulsam o ar quente para uma ala quente.

Requisitos de espaço de intervalo

A tabela seguinte indica a quantidade de espaço necessário para instalar o cluster Secure Workload de formato grande 39-RU (um rack ou rack duplo) ou de formato pequeno 8-RU. O corredor de instalação tem de ter uma largura superior a 59,69 cm para possibilitar a colocação do rack no sítio. Adicionalmente, tem de existir um espaço suficiente que permita aceder à parte frontal e traseira, para realização de manutenção.

Tabela 1: Requisitos de espaço de intervalo

Tipo de instalação	Largura mínima do corredor ¹	Espaço mínimo para instalação do rack
Instalação do C1-Workload (um rack)	59,69 cm	59,69 cm de largura x 126,492 cm de profundidade
C1-Workload (rack duplo)	59,69 cm	119,38 cm de largura x 126,492 cm de profundidade
C1-Workload-M	59,69 cm	59,69 cm de largura x 126,492 cm de profundidade

¹ O corredor de instalação e o corredor que dá acesso à porta frontal do rack têm de ter uma largura mínima de 59,69 cm. O outro corredor, que dá acesso às portas do armário duplo, tem de ter uma largura mínima de 29,845 cm para permitir a abertura total das portas, mas é necessária uma largura mínima de 59,69 cm para permitir a realização de manutenção.

O rack é posicionado com as ventoinhas do switch (o lado do rack com a porta maior) viradas para a ala fria e as portas do switch (o lado do rack com as portas duplas) viradas para a ala quente.



CAPÍTULO 3

Ligação à terra e conexão

- [Ligar os dispositivos de cluster Secure Workload à terra, na página 13](#)
- [Ligar a alimentação dos dispositivos de cluster Secure Workload, na página 13](#)
- [Ligar o cluster Secure Workload aos seus routers, na página 14](#)

Ligar os dispositivos de cluster Secure Workload à terra

Os dispositivos de cluster Secure Workload têm ligações metal-a-metal ao seu rack, por isso, logo que liga o rack à terra (ou os racks numa instalação de rack duplo) do seu centro de dados, os dispositivos no rack são ligados à terra. Para ligar um rack à terra, ligue as rodas do rack à terra.

Ligar a alimentação dos dispositivos de cluster Secure Workload

Para ligar o switch, tem de ligar as duas extensões elétricas ligadas ao rack a duas fontes de alimentação CA.



Nota Ligue este equipamento a uma tomada de alimentação CA com um dispositivo de proteção contra picos (SPD) no equipamento de serviço, em conformidade com a NFPA 70, National Electrical Code (NEC).

Leia as instruções de instalação antes da utilização, instalação ou ligação do sistema à fonte de energia.


Não sobrecarregue a cablagem ao ligar as unidades ao circuito de alimentação.

Antes de começar

- Os racks têm de ser instalados no centro de dados e fixados no sítio com as entradas de ar posicionadas numa ala fria.
- Os racks têm de ser ligados à terra do centro de dados.
- O cluster tem de ser ligado a dois routers providenciados pelo cliente (cada router ligado a um switch leaf separado).

- Têm de existir duas fontes de alimentação que cumpram os requisitos de potência de rack ao alcance de cada cabo de extensão elétrica de rack.

Passo 1 Ligue o cabo de alimentação para uma extensão elétrica a uma fonte de alimentação CA e ligue o cabo de alimentação para a segunda extensão elétrica a outra fonte de alimentação CA.

Passo 2 Observe cada fonte de alimentação instalada em cada dispositivo de rack para confirmar que o LED  está aceso com luz verde.

- Se nenhum dos LEDs estiver aceso, certifique-se de que a fonte de alimentação está ligada e que o interruptor ligar/desligar na extensão elétrica do rack está na posição de ligado.
- Se alguns destes LEDs estiverem acesos e outros não, certifique-se de que o cabo de alimentação proveniente da fonte de alimentação está totalmente conectado à extensão elétrica do rack.

Ligar o cluster Secure Workload aos seus routers

Tem de ligar o cluster Secure Workload a dois routers.

Passo 1 Se estiver a instalar um cluster de rack duplo de formato grande 39-RU, ligue os cabos de interface parcialmente ligados de cada rack. Ligue cada um destes cabos à porta identificada no outro rack.

Passo 2 Utilize um cabo 10 Gigabit para ligar um router à porta E1/39 no switch leaf 1 para uma implementação 39-RU ou à porta E1/47 para uma implementação 8-RU. O switch leaf 1 está situado no seguinte local:

- Plataforma de um rack de formato grande 39-RU—RU 40 no rack de plataforma
- Plataforma de rack duplo de formato grande 39-RU—RU 40 no rack 1
- Plataforma de formato pequeno 8-RU—RU 12 no rack de plataforma

Passo 3 Utilize um cabo 10 Gigabit para ligar um router à porta E1/39 no switch leaf 2 para uma implementação 39-RU ou à porta E1/47 para uma implementação 8-RU. O switch leaf 2 está situado no seguinte local:

- Plataforma de um rack de formato grande 39-RU—RU 41 no rack de plataforma
 - Plataforma de rack duplo de formato grande 39-RU—RU 41 no rack 2
 - Plataforma de formato pequeno 8-RU—RU 11 no rack de plataforma
-



CAPÍTULO 4

Configurar a interface do utilizador

- (Opcional) [Requisitos e limitações para o modo Dual-Stack \(suporte para IPv6\)](#), na página 15
- [Configurar a interface do utilizador](#), na página 16

(Opcional) Requisitos e limitações para o modo Dual-Stack (suporte para IPv6)

Os clusters Secure Workload executados em hardware físico podem ser configurados para utilizar IPv6 além de IPv4 para determinadas comunicações de e para o cluster.



Nota Pode utilizar a funcionalidade Modo Dual-Stack (suporte para IPv6) ao instalar ou atualizar para as versões 3.6.1.5, 3.7.1.5 e 3.8.1.1. No entanto, a opção para ativar a funcionalidade não está disponível quando instalar ou atualizar para lançamentos de patches.

Limitações

Se estiver a considerar ativar o modo Dual-Stack, tenha em atenção o seguinte:

- Só pode ativar a conectividade IPv6 durante a implementação inicial ou a atualização para uma versão principal (não é possível ativar esta funcionalidade durante atualizações de patches).
- O modo Dual-Stack só é compatível com hardware físico ou clusters bare metal.
- Não existe suporte para o modo apenas IPv6.
- Não pode reverter para o modo apenas IPv4 depois de o modo Dual-Stack ter sido ativado para o cluster.
- A Cópia de segurança e restauro de dados (DBR) não será suportada se a conectividade Dual-Stack estiver ativada.
- Não ative o modo Dual-Stack para clusters configurados com o Federation.
- As funcionalidades a seguir utilizam sempre e apenas IPv4 (tenha em atenção que o IPv4 está sempre ativado, mesmo que o IPv6 esteja ativado):
 - (Aplicável para as versões 3.8.1.1, 3.7.1.5 e 3.6.x) Aplicação em agentes AIX
 - (Aplicável apenas para a versão 3.6.x) Comunicação do agente de hardware com o cluster

- (Aplicável apenas para a versão 3.6.x) Conectores para ingestão de fluxo, enriquecimento de inventário ou notificações de alerta

Requisitos

- Configure os registos DNS A e AAAA para FQDN antes de ativar o modo Dual-Stack para o seu cluster.
- Os serviços externos, como NTP, SMTP e DNS, têm de estar disponíveis através de IPv4 e IPv6, para fins de redundância.
- Para configurar o modo Dual-Stack para um cluster:
 - Têm de ser atribuídos endereços IPv6 encaminháveis a cada um dos dois switches leaf do cluster em duas redes diferentes, para redundância, e têm de ser fornecidos gateways predefinidos para cada rede.
 - Para clusters 39-RU, é necessária uma rede IPv6 encaminhável para sites com espaço para, pelo menos, 29 endereços de anfitrião.
 - Para clusters 8-RU, é necessária uma rede IPv6 encaminhável para sites com espaço para, pelo menos, 20 endereços de anfitrião.
 - Os três primeiros endereços de anfitrião da rede IPv6 encaminhável para sites são reservados para a configuração HSRP do cluster Cisco Secure Workload e não devem ser utilizados por nenhum outro dispositivo.

Informações adicionais

Os agentes comunicam com o cluster através de IPv4, a menos que os configure para que utilizem IPv6. Para obter instruções, consulte o Manual do utilizador do Cisco Secure Workload.

Configurar a interface do utilizador

Antes de começar

- Para concluir esta configuração, é necessário um dispositivo como um computador portátil com porta Ethernet e acesso à Internet.
- É necessário um cabo Ethernet para ligar o dispositivo ao servidor mais elevado no cluster Secure Workload.
- O Google Chrome é o único browser compatível com o portal de configuração, necessário para parte deste processo.
- (Opcional) A partir da versão 3.6 e posteriores, pode configurar o cluster no modo Dual-Stack, o que permite utilizar IPv4 e IPv6 para a comunicação entre determinados componentes do Secure Workload e entre o Secure Workload e serviços de rede, como NTP e DNS. (O Secure Workload já processa tráfego IPv6, independentemente do facto de ativar ou não o modo Dual-Stack.) Só pode ativar este suporte durante a implementação ou a atualização.

Se está a considerar ativar o suporte para IPv6, consulte [\(Opcional\) Requisitos e limitações para o modo Dual-Stack \(suporte para IPv6\), na página 15](#).



Importante Introduza endereços IPv4 em todos os campos do procedimento abaixo, a menos que o nome do campo indique explicitamente IPv6.

Passo 1 Configure o dispositivo de Internet com o endereço IP 2.2.2.1/30 (255.255.255.252).

Passo 2 Utilize um cabo Ethernet para ligar a porta Ethernet no dispositivo de Internet à porta LOM 2 (LAN2) no servidor mais elevado na parte superior do cluster Secure Workload.

Passo 3 No dispositivo de Internet, abra o browser Chrome e aceda a <http://2.2.2.2:9000>.

Nota O browser Chrome é o único browser testado com este processo.

É aberta a página de Diagnóstico de instalação.

Passo 4 Se existirem erros na página de Diagnóstico, verifique as ligações de cablagem entre os dispositivos do cluster quanto a ruturas de ligações ou cabos encaminhados incorretamente antes de continuar com este procedimento. Quando terminar, regresse ao Passo 2.

Consulte [Cablagem do dispositivo de cluster C1-Workload, na página 21](#) e [Cablagem do dispositivo de cluster C1-Workload-M, na página 34](#) acerca da cablagem correta.

Passo 5 Clique em **Continuar**.

É aberta a página de Carregamento RPM.

Nota Se, em vez disso, for aberta a página Configuração do site, introduza o seguinte URL para a página de Carregamento RPM:

`http://2.2.2.2:9000 /upload`

Passo 6 Carregue os ficheiros RPM para a nuvem do Secure Workload.

Tem de carregar os ficheiros pela ordem seguinte:

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

- a) Clique em **Selecionar ficheiro**.
- b) Navegue para um RPM, selecione-o e clique em **Abrir**.
- c) Clique em **Carregar**.

A lista de RPMs na página não é atualizada enquanto carrega cada RPM. Isso é normal.

Se vir um erro após carregar o ficheiro `tetration_os_mother_rpm_k9-2.1.1.31-1.e16.x86_64.rpm`, aguarde aproximadamente 5 a 10 minutos e recarregue a página. Deve ver uma lista dos RPMs carregados após recarregar a página. O erro deve-se a um reinício do Orquestrador e não é um problema.

- d) Repita os passos a até c para cada RPM.

Após terminar de carregar os RPMs, é aberta a página Configuração do site.

Passo 7 Utilize a página Configuração do site para configurar o novo site da seguinte forma:

- Clique em **Geral**.
 1. No campo **Nome do site**, introduza o nome único do cluster.
 2. No campo **Chave pública SSH**, cole a chave de autenticação.

Nota Gere o seu próprio par de chaves SSH, que pode ser utilizado para acesso ao SSH do cluster.

Recomendamos vivamente que mantenha a chave SSH num local seguro e facilmente acessível, de forma a possibilitar a resolução de problemas ou recuperação do cluster através de um acesso `ta_guest`.
 3. Clique em **Seguinte**.
- Clique em **E-mail**.
 1. Preencha os endereços de e-mail necessários.
 2. Clique em **Seguinte**.
- Clique em **L3**.

Introduza cada um dos endereços solicitados. Todos os campos com * são campos obrigatórios.

Introduza todos os endereços como IPv4, a menos que o nome do campo especifique IPv6.

(Opcional) Se estiver a instalar a versão 3.6 ou posterior do software: para ativar o modo Dual-Stack (suporte para IPv4 e IPv6):

 1. Marque a caixa de seleção IPv6.
 2. Introduza o endereço IPv6 na notação CIDR para os switches Leaf 1 e Leaf 2.
 3. Introduza o gateway predefinido IPv6 Leaf 1 e Leaf 2.
 4. Clique em **Seguinte**.
- Clique em **Rede**.

Introduza todos os endereços como IPv4, a menos que o nome do campo especifique IPv6.

 1. No campo **Endereço IP de rede interna**, cole o endereço da saída de implementação do Orquestrador.
 2. No campo **Endereço IP de rede externa**, cole o endereço da saída de implementação do Orquestrador.
 3. No campo **Endereço IP de gateway externo**, cole o endereço da saída de implementação do Orquestrador.
 4. No campo **Endereço IP da resolução de DNS**, cole o endereço da saída de implementação do Orquestrador.
 5. No campo **Domínio DNS**, introduza o seu domínio DNS (por exemplo, `cisco.com`).
 6. (Versão 3.6 ou posterior do software) Se ativou o IPv6 na página L3, o **IPv6** será selecionado automaticamente.

Se o IPv6 for selecionado, deverá especificar endereços IPv6 reservados para a utilização do Secure Workload:

 - Introduza a **Rede IPv6 externa**.

Os três primeiros endereços IPv6 no campo Rede IPv6 externa são sempre reservados para os switches do cluster Secure Workload e não devem ser utilizados para qualquer outra finalidade.

- Se pretender utilizar o IPv6 apenas para determinados endereços, introduza esses endereços no campo **IPs IPv6 externos**.

Nota

- Para um cluster 39-RU, certifique-se de que estão disponíveis, pelo menos, 29 endereços IPv6 na Rede IPv6 externa ou na lista de IPs IPv6 externos.
- Para um cluster 8-RU, certifique-se de que estão disponíveis, pelo menos, 20 endereços IPv6 na Rede IPv6 externa ou na lista de IPs IPv6 externos.

7. Clique em Seguinte.• Clique em **Serviço**.

1. No campo **Servidores NTP**, introduza a lista separada por espaços de nomes de servidor NTP ou endereços IP da saída de implementação do orquestrador.
2. No campo **Servidor SMTP**, introduza o nome ou o endereço IP de um servidor SMTP que pode ser utilizado pelo Secure Workload para enviar mensagens de e-mail. Este servidor tem de poder ser acedido pelo Secure Workload.
3. No campo **Porta SMTP**, introduza o número da porta do servidor SMTP. A AWS restringe a utilização das portas 25 e 465. Tem de configurar a sua conta corretamente ou utilizar a porta 587.
4. (Opcional) No campo **Nome do utilizador SMTP**, introduza o nome do utilizador para a autenticação SMTP.
5. (Opcional) No campo **Palavra-passe SMTP**, introduza a palavra-passe para a autenticação SMTP.
6. (Opcional) No campo **Servidor proxy HTTP**, introduza o nome ou o endereço IP de um servidor proxy HTTP que pode ser utilizado pelo Secure Workload para aceder a serviços externos na Internet.
7. (Opcional) No campo **Porta proxy HTTP**, introduza o número da porta para o servidor proxy HTTP.
8. (Opcional) No campo **Servidor proxy HTTPs**, introduza o nome ou o endereço IP de um servidor proxy HTTPs que pode ser utilizado pelo Secure Workload para aceder a serviços externos na Internet.
9. (Opcional) No campo **Porta proxy HTTPs**, introduza o número da porta para o servidor proxy HTTPs.
10. (Opcional) No campo **Servidor Syslog**, introduza o nome ou o endereço IP de um servidor syslog que pode ser utilizado pelo Secure Workload para enviar alertas.
11. (Opcional) No campo **Porta Syslog**, introduza o número da porta para o servidor Syslog.
12. (Opcional) No campo **Gravidade Syslog**, introduza o nível de gravidade para as mensagens de syslog. Os valores possíveis incluem informativo, anúncio, aviso, erro, crítico, alerta e emergência.
13. Clique em **Seguinte**.

• Clique em **UI**.

1. No campo **UI VRRP VRID**, introduza **77**, exceto se necessitar de um VRID único.
2. No campo **UI FQDN**, introduza o nome de domínio completamente qualificado, onde pode aceder ao cluster.

3. Deixe o campo **UI Airbrake Key** em branco.
4. Clique em **Seguinte**.

O Tetration (Secure Workload) valida as suas definições de configuração e apresenta o estado das definições.

- Clicar em **Avançado**.
 1. No campo **IPs externos**, introduza endereços IPv4.
 2. Clique em **Continuar**.

Passo 8 Se ocorrerem falhas, clique em **Voltar** e edite a configuração (ver Passo 7).

Nota Não pode modificar estas definições na GUI de instalação após sair desta página. Contudo, pode modificar as definições mais tarde a partir da página da empresa na GUI.

Passo 9 Se não ocorrerem falhas na sua configuração e não precisar de efetuar alterações, clique em **Continuar**.

O Secure Workload é configurado de acordo com as definições que tiver especificado. Este processo demora uma a duas horas e não requer qualquer interação da sua parte.

O que fazer a seguir

Se implementou a versão 3.6 ou posterior do software e ativou a conectividade IPv6:

- Pode aceder ao portal Web do Secure Workload com IPv4 ou IPv6.
- Por predefinição, os agentes do software comunicam com o cluster Secure Workload através de IPv4, mesmo que o cluster esteja ativado para suportar IPv6. Se pretender que os agentes suportados utilizem IPv6 para esta finalidade, tem de configurar o campo **Sensor VIP FQDN** na página **Plataforma > Configuração de cluster** no portal Web do Secure Workload. Para obter instruções importantes, consulte o manual do utilizador, disponível como ajuda online no portal Web do Secure Workload ou em <https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html>.



CAPÍTULO 5

Cablagem do dispositivo de cluster C1-Secure Workload

- [Cablagem do dispositivo de cluster C1-Workload, na página 21](#)
- [Cablagem do dispositivo de cluster C1-Workload-M, na página 34](#)

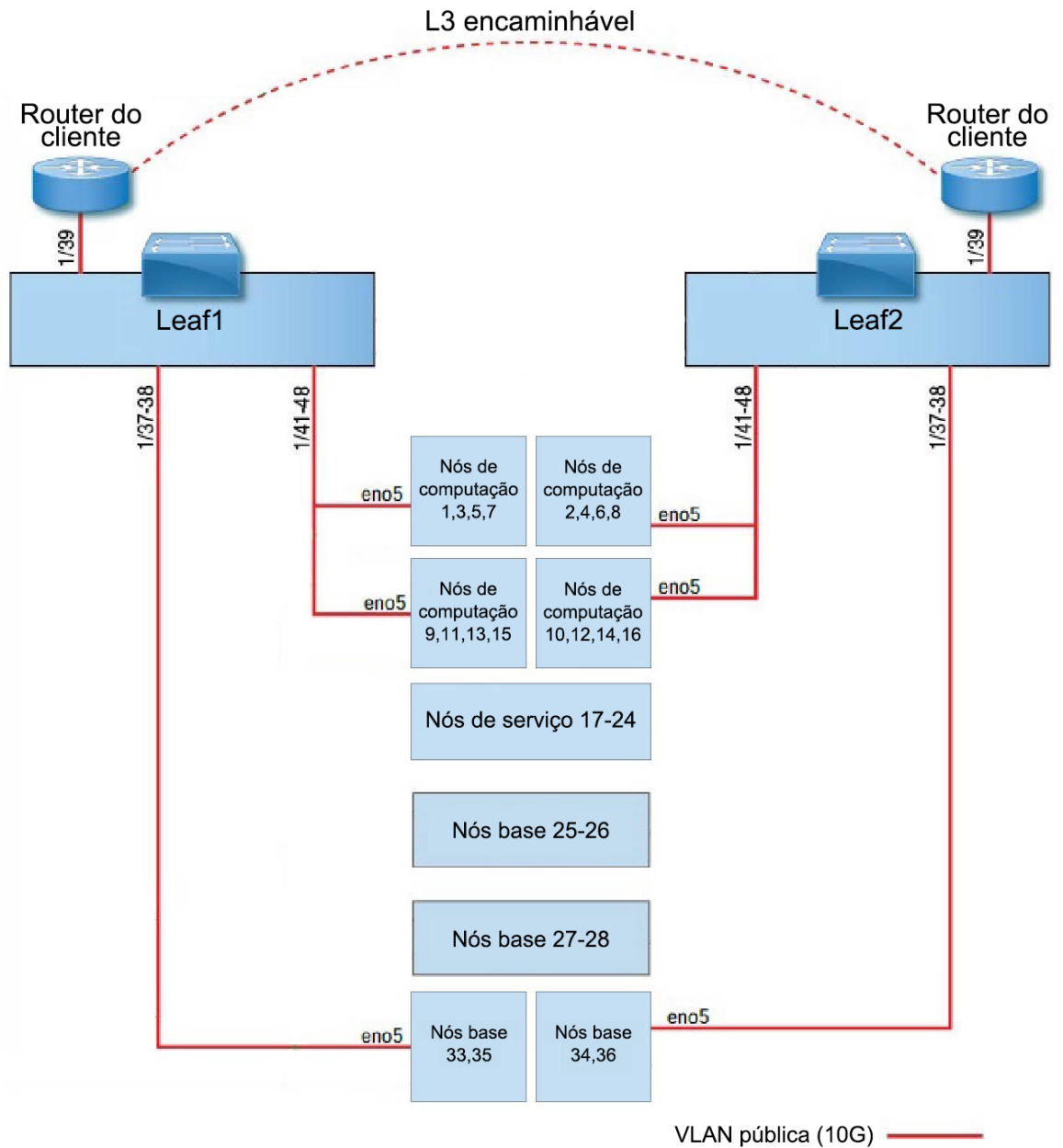
Cablagem do dispositivo de cluster C1-Workload

Preste atenção à seguinte informação de configuração quando ligar a cablagem da Placa de Interface Virtual M6 (VIC) no rack 39-RU:

- Existem duas interfaces privadas para todos os nós.
- O rack 39-RU tem uma interface pública para 20 nós.
- O hardware M6 tem quatro portas por VIC.
- Os nomes para a interface bare metal—os servidores físicos no cluster conhecidos como nós base, de computação e serviço—começam com "eno" (Ethernet onboard).

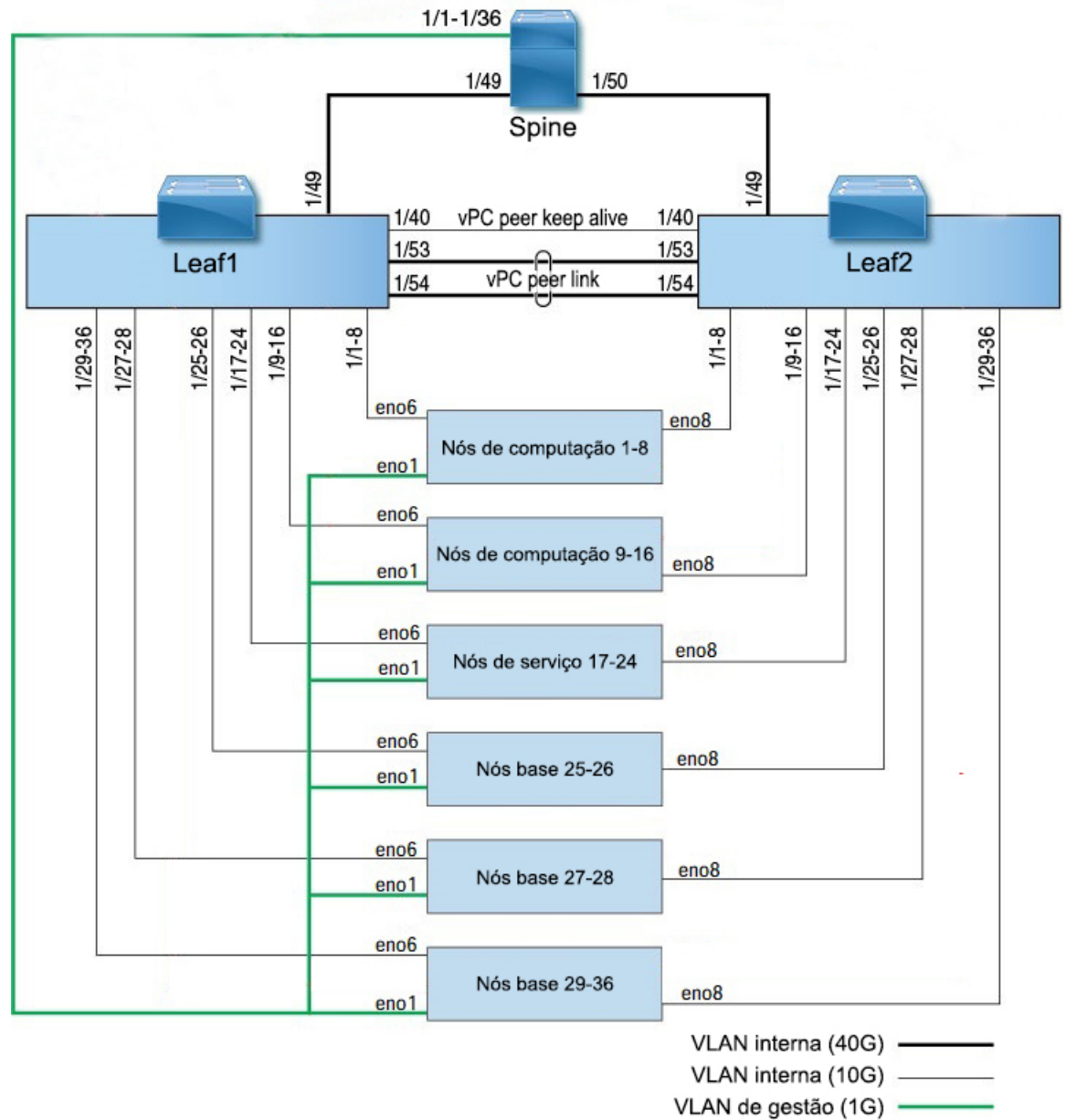
O esquema seguinte apresenta a cablagem do dispositivo para a configuração pública/externa do rack C1-Workload. Para uma lista detalhada das ligações, consulte as tabelas apresentadas a seguir aos esquemas.

Figura 7: Cablagem do dispositivo de rack C1-Workload (pública/externa)



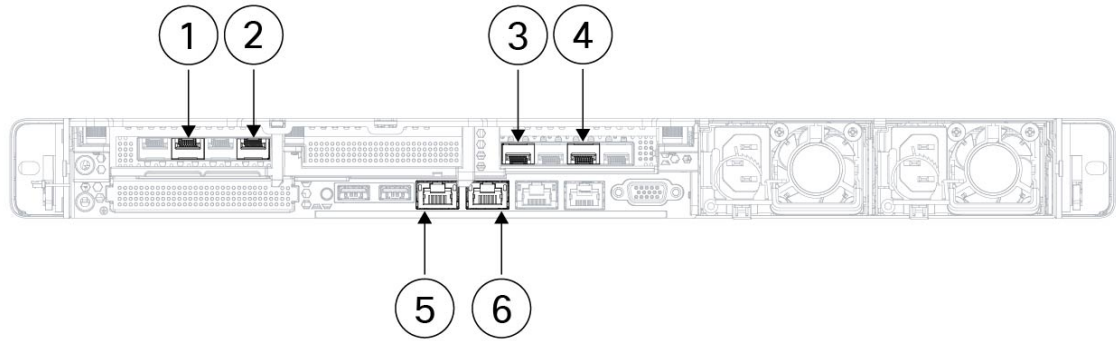
O esquema seguinte apresenta a cablagem do dispositivo para a configuração interna/de gestão do rack C1-Workload. Para uma lista detalhada das ligações, consulte as tabelas seguintes.

Figura 8: Cablagem do dispositivo de rack C1-Workload (interna/de gestão)



A figura seguinte indica as portas no servidor M6 que correspondem às portas "eno" nas figuras acima:

Figura 9: Portas do Servidor M6



1	Leaf 1 ou leaf 2 público dependendo do servidor Porta de interface do servidor = eno5 Designação CIMC = adaptador 1/porta física 2/vic-1-eth1	2	Leaf 1 privado Porta de interface do servidor = eno6 Designação CIMC = adaptador 1/porta física 0/vic-1-eth0
3	Leaf 2 privado Porta de interface do servidor = eno8 Designação CIMC = adaptador 3/porta física 0/vic-3-eth0	4	Não utilizado Porta de interface do servidor = eno7 Designação CIMC = adaptador 3/porta física 2/vic-3-eth1
5	CIMC Porta de interface do servidor = eno1 Designação CIMC = LOM 1	6	MGMT 2.2.2.2 Porta de interface do servidor = eno2 Designação CIMC = LOM 2

Tabela 2: Ligações de Switch Spine (RU 42 em instalações de um rack e instalações de rack duplo)

Porta Spine	Tipo de ligação	Ligação			
		Dispositivo	RU em um rack	RU em rack duplo	Porta
1/1	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 1 (nó de computação)	RU 36	Rack1 RU 17	eno1
1/2	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 2 (nó de computação)	RU 35	Rack1 RU 16	eno1
1/3	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 3 (nó de computação)	RU 34	Rack1 RU 15	eno1
1/4	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 4 (nó de computação)	RU 33	Rack1 RU 14	eno1

Porta Spine	Tipo de ligação	Ligação			
		Dispositivo	RU em rack	RU em rack duplo	Porta
1/5	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 5 (nó de computação)	RU 32	Rack 1 RU 13	eno1
1/6	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 6 (nó de computação)	RU 31	Rack 1 RU 12	eno1
1/7	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 7 (nó de computação)	RU 30	Rack 1 RU 11	eno1
1/8	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 8 (nó de computação)	RU 29	Rack 1 RU 10	eno1
1/9	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 9 (nó de computação)	RU 28	Rack 1 RU 8	eno1
1/10	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 10 (nó de computação)	RU 27	Rack 1 RU 7	eno1
1/11	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 11 (nó de computação)	RU 26	Rack 1 RU 6	eno1
1/12	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 12 (nó de computação)	RU 25	Rack 1 RU 5	eno1
1/13	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 13 (nó de computação)	RU 24	Rack 1 RU 4	eno1
1/14	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 14 (nó de computação)	RU 23	Rack 1 RU 3	eno1
1/15	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 15 (nó de computação)	RU 22	Rack 1 RU 2	eno1
1/16	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 16 (nó de computação)	RU 21	Rack 1 RU 1	eno1
1/17	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 17 (nó de serviço)	RU 20	Rack 2 RU 21	eno1
1/18	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 18 (nó de serviço)	RU 19	Rack 2 RU 20	eno1
1/19	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 19 (nó de serviço)	RU 18	Rack 2 RU 19	eno1
1/20	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 20 (nó de serviço)	RU 17	Rack 2 RU 18	eno1

Porta Spine	Tipo de ligação	Ligação			
		Dispositivo	RU em um rack	RU em rack duplo	Porta
1/21	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 21 (nó de serviço)	RU 16	Rack2 RU 17	eno1
1/22	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 22 (nó de serviço)	RU 15	Rack2 RU 16	eno1
1/23	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 23 (nó de serviço)	RU 14	Rack2 RU 15	eno1
1/24	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 24 (nó de serviço)	RU 13	Rack2 RU 14	eno1
1/25	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 25 (nó base)	RU 12	Rack2 RU 12	eno1
1/26	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 26 (nó base)	RU 11	Rack2 RU 11	eno1
1/27	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 27 (nó base)	RU 10	Rack2 RU 10	eno1
1/28	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 28 (nó base)	RU 9	Rack2 RU 9	eno1
1/29	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 29 (nó base)	RU 8	Rack2 RU 8	eno1
1/30	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 30 (nó base)	RU 7	Rack2 RU 7	eno1
1/31	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 31 (nó base)	RU 6	Rack2 RU 6	eno1
1/32	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 32 (nó base)	RU 5	Rack2 RU 5	eno1
1/33	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 33 (nó base)	RU 4	Rack2 RU 4	eno1
1/34	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 34 (nó base)	RU 3	Rack2 RU 3	eno1
1/35	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 35 (nó base)	RU 2	Rack2 RU 2	eno1
1/36	CIMC VLAN (1 Gigabit)	Servidor UCS anfitrião 36 (nó base)	RU 1	Rack2 RU 1	eno1

Porta Spine	Tipo de ligação	Ligação			
		Dispositivo	RU em um rack	RU em rack duplo	Porta
1/49	VLAN interna (40 Gigabit)	Switch Leaf 1 (RU 41 em um rack ou RU 40 em rack 1 de rack duplo)	RU 40	Rack 1 RU 40	1/49
1/50	VLAN interna (40 Gigabit)	Switch Leaf 2 (RU 40 em um rack ou RU 40 em rack 2 de rack duplo) porta 49	RU 41	Rack 2 RU 40	1/50

Tabela 3: Ligações de Switch Leaf 1 (RU 41 em instalações de um rack ou RU 40 em rack 1 de instalações de rack duplo)

Porta Leaf 1	Tipo de ligação	Ligação			
		Dispositivo	RU em um rack	RU em rack duplo	Porta
1/1	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 1 (nó de computação)	RU 36	Rack 1 RU 17	eno6
1/2	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 2 (nó de computação)	RU 35	Rack 1 RU 16	eno6
1/3	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 3 (nó de computação)	RU 34	Rack 1 RU 15	eno6
1/4	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 4 (nó de computação)	RU 33	Rack 1 RU 14	eno6
1/5	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 5 (nó de computação)	RU 32	Rack 1 RU 13	eno6
1/6	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 6 (nó de computação)	RU 31	Rack 1 RU 12	eno6
1/7	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 7 (nó de computação)	RU 30	Rack 1 RU 11	eno6
1/8	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 8 (nó de computação)	RU 29	Rack 1 RU 10	eno6
1/9	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 9 (nó de computação)	RU 28	Rack 1 RU 8	eno6
1/10	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 10 (nó de computação)	RU 27	Rack 1 RU 7	eno6
1/11	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 11 (nó de computação)	RU 26	Rack 1 RU 6	eno6

Porta Leaf 1	Tipo de ligação	Ligação			
		Dispositivo	RU em um rack	RU em rack duplo	Porta
1/12	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 12 (nó de computação)	RU 25	Rack1 RU 5	eno6
1/13	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 13 (nó de computação)	RU 24	Rack1 RU 4	eno6
1/14	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 14 (nó de computação)	RU 23	Rack1 RU 3	eno6
1/15	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 15 (nó de computação)	RU 22	Rack1 RU 2	eno6
1/16	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 16 (nó de computação)	RU 21	Rack1 RU 1	eno6
1/17	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 17 (nó de serviço)	RU 20	Rack2 RU 21	eno6
1/18	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 18 (nó de serviço)	RU 19	Rack2 RU 20	eno6
1/19	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 19 (nó de serviço)	RU 18	Rack2 RU 19	eno6
1/20	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 20 (nó de serviço)	RU 17	Rack2 RU 18	eno6
1/21	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 21 (nó de serviço)	RU 16	Rack2 RU 17	eno6
1/22	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 22 (nó de serviço)	RU 15	Rack2 RU 16	eno6
1/23	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 23 (nó de serviço)	RU 14	Rack2 RU 15	eno6
1/24	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 24 (nó de serviço)	RU 13	Rack2 RU 14	eno6
1/25	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 25 (nó base)	RU 12	Rack2 RU 12	eno6
1/26	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 26 (nó base)	RU 11	Rack2 RU 11	eno6
1/27	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 27 (nó base)	RU 10	Rack2 RU 10	eno6

Porta Leaf 1	Tipo de ligação	Ligação			
		Dispositivo	RU em rack	RU em rack duplo	Porta
1/28	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 28 (nó base)	RU 9	Rack2 RU 9	eno6
1/29	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 29 (nó base)	RU 8	Rack2 RU 8	eno6
1/30	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 30 (nó base)	RU 7	Rack2 RU 7	eno6
1/31	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 31 (nó base)	RU 6	Rack2 RU 6	eno6
1/32	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 32 (nó base)	RU 5	Rack2 RU 5	eno6
1/33	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 33 (nó base)	RU 4	Rack2 RU 4	eno6
1/34	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 34 (nó base)	RU 3	Rack2 RU 3	eno6
1/35	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 35 (nó base)	RU 2	Rack2 RU 2	eno6
1/36	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 36 (nó base)	RU 1	Rack2 RU 1	eno6
1/37	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 33 (nó base)	RU 3	Rack2 RU 3	eno5
1/38	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 35 (nó base)	RU 1	Rack2 RU 1	eno5
1/39	VLAN interna (10 Gigabit)	Router do cliente 1	—	—	—
1/40	VLAN interna (10 Gigabit)	Leaf 1	RU 40	Rack 1 RU 40	1/40
1/41	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 1 (nó de computação)	RU 35	Rack 1 RU 16	eno5
1/42	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 3 (nó de computação)	RU 33	Rack 1 RU 14	eno5
1/43	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 5 (nó de computação)	RU 31	Rack 1 RU 12	eno5

Porta Leaf 1	Tipo de ligação	Ligação			
		Dispositivo	RU em um rack	RU em rack duplo	Porta
1/44	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 7 (nó de computação)	RU 29	Rack 1 RU 10	eno5
1/45	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 9 (nó de computação)	RU 27	Rack 1 RU 8	eno5
1/46	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 11 (nó de computação)	RU 25	Rack 1 RU 6	eno5
1/47	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 13 (nó de computação)	RU 23	Rack 1 RU 4	eno5
1/48	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 15 (nó de computação)	RU 21	Rack 1 RU 2	eno5
1/49	VLAN interna (40 Gigabit)	Switch Spine	RU 42	Rack 1 RU 42	1/49
1/50	—	—	—	—	—
1/51	—	—	—	—	—
1/52	—	—	—	—	—
1/53	VLAN interna (40 Gigabit)	Switch Leaf 1	RU 40	Rack 1 RU 40	1/53
1/54	VLAN interna (40 Gigabit)	Switch Leaf 1	RU 40	Rack 1 RU 40	1/54

Tabela 4: Ligações de Switch Leaf 2 (RU 41 em instalações de um rack ou RU 40 em rack 2 de instalações de rack duplo)

Porta Leaf 2	Tipo de ligação	Ligação			
		Dispositivo	RU em um rack	RU em rack duplo	Porta
1/1	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 1 (nó de computação)	RU 36	Rack 1 RU 17	eno8
1/2	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 2 (nó de computação)	RU 35	Rack 1 RU 16	eno8

Porta Leaf 2	Tipo de ligação	Ligação			
		Dispositivo	RU em um rack	RU em rack duplo	Porta
1/3	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 3 (nó de computação)	RU 34	Rack 1 RU 15	eno8
1/4	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 4 (nó de computação)	RU 33	Rack 1 RU 14	eno8
1/5	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 5 (nó de computação)	RU 32	Rack 1 RU 13	eno8
1/6	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 6 (nó de computação)	RU 31	Rack 1 RU 12	eno8
1/7	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 7 (nó de computação)	RU 30	Rack 1 RU 11	eno8
1/8	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 8 (nó de computação)	RU 29	Rack 1 RU 10	eno8
1/9	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 9 (nó de computação)	RU 28	Rack 1 RU 8	eno8
1/10	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 10 (nó de computação)	RU 27	Rack 1 RU 7	eno8
1/11	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 11 (nó de computação)	RU 26	Rack 1 RU 6	eno8
1/12	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 12 (nó de computação)	RU 25	Rack 1 RU 5	eno8
1/13	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 13 (nó de computação)	RU 24	Rack 1 RU 4	eno8
1/14	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 14 (nó de computação)	RU 23	Rack 1 RU 3	eno8
1/15	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 15 (nó de computação)	RU 22	Rack 1 RU 2	eno8
1/16	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 16 (nó de computação)	RU 21	Rack 1 RU 1	eno8
1/17	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 17 (nó de serviço)	RU 20	Rack 2 RU 21	eno8
1/18	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 18 (nó de serviço)	RU 19	Rack 2 RU 20	eno8

Porta Leaf 2	Tipo de ligação	Ligação			
		Dispositivo	RU em um rack	RU em rack duplo	Porta
1/19	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 19 (nó de serviço)	RU 18	Rack2 RU 19	eno8
1/20	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 20 (nó de serviço)	RU 17	Rack2 RU 18	eno8
1/21	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 21 (nó de serviço)	RU 16	Rack2 RU 17	eno8
1/22	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 22 (nó de serviço)	RU 15	Rack2 RU 16	eno8
1/23	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 23 (nó de serviço)	RU 14	Rack2 RU 15	eno8
1/24	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 24 (nó de serviço)	RU 13	Rack2 RU 14	eno8
1/25	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 25 (nó base)	RU 12	Rack2 RU 12	eno8
1/26	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 26 (nó base)	RU 11	Rack2 RU 11	eno8
1/27	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 27 (nó base)	RU 10	Rack2 RU 10	eno8
1/28	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 28 (nó base)	RU 9	Rack2 RU 9	eno8
1/29	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 29 (nó base)	RU 8	Rack2 RU 8	eno8
1/30	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 30 (nó base)	RU 7	Rack2 RU 7	eno8
1/31	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 31 (nó base)	RU 6	Rack2 RU 6	eno8
1/32	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 32 (nó base)	RU 5	Rack2 RU 5	eno8
1/33	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 33 (nó base)	RU 4	Rack2 RU 4	eno8
1/34	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 34 (nó base)	RU 3	Rack2 RU 3	eno8
1/35	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 35 (nó base)	RU 2	Rack2 RU 2	eno8

Porta Leaf 2	Tipo de ligação	Ligação			
		Dispositivo	RU em um rack	RU em rack duplo	Porta
1/36	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 36 (nó base)	RU 1	Rack2 RU 1	eno8
1/37	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 34 (nó base)	RU 4	Rack2 RU 8	eno5
1/38	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 36 (nó base)	RU 2	Rack2 RU 6	eno5
1/39	VLAN interna (10 Gigabit)	Router do cliente 1	—	—	—
1/40	VLAN interna (10 Gigabit)	Switch Leaf 2	RU 41	Rack2 RU 40	1/40
1/41	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 2 (nó de computação)	RU 36	Rack 1 RU 17	eno5
1/42	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 4 (nó de computação)	RU 34	Rack 1 RU 15	eno5
1/43	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 6 (nó de computação)	RU 32	Rack 1 RU 13	eno5
1/44	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 8 (nó de computação)	RU 30	Rack 1 RU 11	eno5
1/45	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 10 (nó de computação)	RU 28	Rack 1 RU 9	eno5
1/46	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 12 (nó de computação)	RU 26	Rack 1 RU 7	eno5
1/47	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 14 (nó de computação)	RU 24	Rack 1 RU 5	eno5
1/48	VLAN pública (10 Gigabit)	Servidor UCS anfitrião 16 (nó de computação)	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

Porta Leaf 2	Tipo de ligação	Ligação			
		Dispositivo	RU em um rack	RU em rack duplo	Porta
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

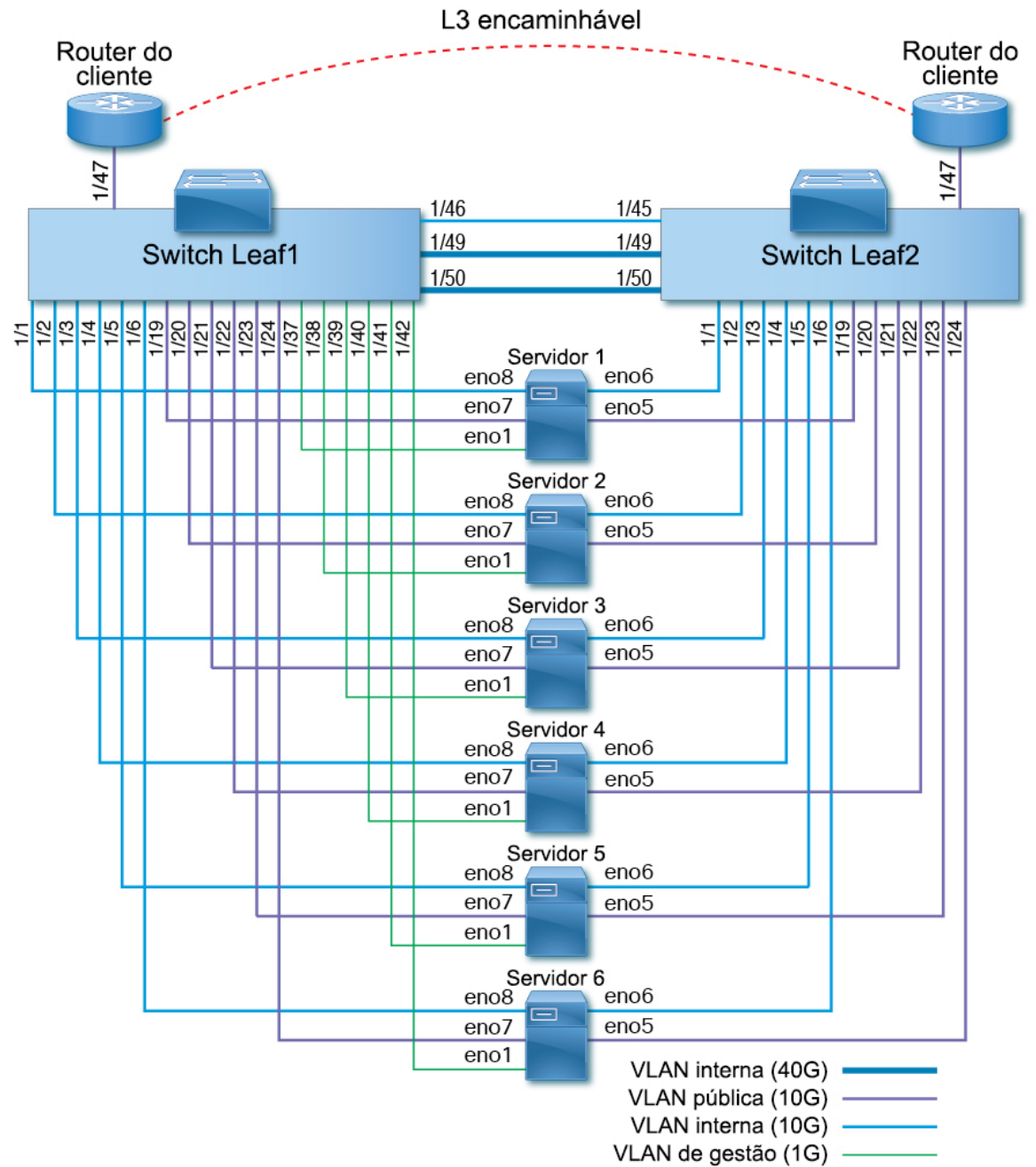
Cablagem do dispositivo de cluster C1-Workload-M

Para efetuar a cablagem do M6 VIC no rack 8-RU, preste atenção à seguinte informação de configuração:

- Existem duas interfaces privadas para todos os nós.
- O rack 8-RU tem duas interfaces públicas para todos os seis nós.
- O hardware M6 tem quatro portas por VIC.
- Os nomes para a interface bare metal—o servidor físico no cluster conhecido como nós universais—começam com "eno" (Ethernet onboard).

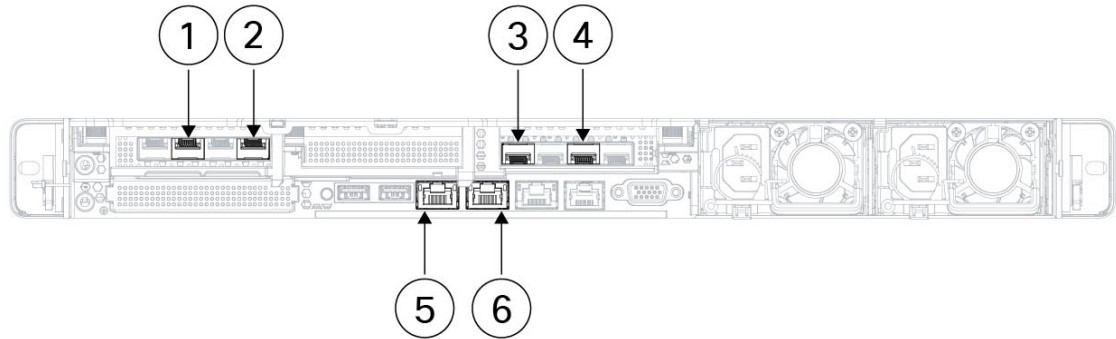
O esquema seguinte apresenta a cablagem do dispositivo para a configuração interna/de gestão/pública/externa do rack 8-RU do Cluster C1-Workload-M. Para uma lista detalhada das ligações, consulte as tabelas apresentadas a seguir ao esquema.

Figura 10: Cablagem do dispositivo do rack do Cluster C1-Workload-M (interna/de gestão/pública/externa)



A figura seguinte indica as portas no servidor que correspondem às portas "eno" no esquema acima:

Figura 11: Portas do Servidor M6



1	Leaf 2 público Porta de interface do servidor = eno5 Designação CIMC = adaptador 1/porta física 2/vic-1-eth1	2	Leaf 2 privado Porta de interface do servidor = eno6 Designação CIMC = adaptador 1/porta física 0/vic-1-eth0
3	Leaf 1 privado Porta de interface do servidor = eno8 Designação CIMC = adaptador 3/porta física 0/vic-3-eth0	4	Leaf 1 público Porta de interface do servidor = eno7 Designação CIMC = adaptador 3/porta física 2/vic3-eth1
5	CIMC Porta de interface do servidor = eno1 Designação CIMC = LOM 1	6	MGMT 2.2.2.2 Porta de interface do servidor = eno2 Designação CIMC = LOM 2

Tabela 5: Ligações do Switch Leaf 1 (RU 12)

Porta Leaf	Tipo de ligação	Ligação		
		Dispositivo	RU em um rack	Porta
1/1	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 1 (nó universal)	RU 9	eno8
1/2	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 2 (nó universal)	RU 8	eno8
1/3	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 3 (nó universal)	RU 6	eno8
1/4	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 4 (nó universal)	RU 5	eno8
1/5	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 5 (nó universal)	RU 3	eno8
1/6	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 6 (nó universal)	RU 2	eno8
1/7	—	—	—	—
1/8	—	—	—	—

Porta Leaf	Tipo de ligação	Ligação		
		Dispositivo	RU em um rack	Porta em rack
1/9	—	—	—	—
1/10	—	—	—	—
1/11	—	—	—	—
1/12	—	—	—	—
1/13	—	—	—	—
1/14	—	—	—	—
1/15	—	—	—	—
1/16	—	—	—	—
1/17	—	—	—	—
1/18	—	—	—	—
1/19	VLAN externa (10 Gigabit)	Servidor UCS anfitrião 1 (nó universal)	RU 9	eno7
1/20	VLAN externa (10 Gigabit)	Servidor UCS anfitrião 2 (nó universal)	RU 8	eno7
1/21	VLAN externa (10 Gigabit)	Servidor UCS anfitrião 3 (nó universal)	RU 6	eno7
1/22	VLAN externa (10 Gigabit)	Servidor UCS anfitrião 4 (nó universal)	RU 5	eno7
1/23	VLAN externa (10 Gigabit)	Servidor UCS anfitrião 5 (nó universal)	RU 3	eno7
1/24	VLAN externa (10 Gigabit)	Servidor UCS anfitrião 6 (nó universal)	RU 2	eno7
1/25	—	—	—	—
1/26	—	—	—	—
1/27	—	—	—	—
1/28	—	—	—	—
1/29	—	—	—	—
1/30	—	—	—	—
1/31	—	—	—	—
1/32	—	—	—	—
1/33	—	—	—	—

Porta Leaf	Tipo de ligação	Ligação		
		Dispositivo	RU em um rack	Porta
1/34	—	—	—	—
1/35	—	—	—	—
1/36	—	—	—	—
1/37	VLAN de gestão (1 Gigabit)	Servidor UCS anfitrião 1 (nó universal)	RU 9	eno1
1/38	VLAN de gestão (1 Gigabit)	Servidor UCS anfitrião 2 (nó universal)	RU 8	eno1
1/39	VLAN de gestão (1 Gigabit)	Servidor UCS anfitrião 3 (nó universal)	RU 6	eno1
1/40	VLAN de gestão (1 Gigabit)	Servidor UCS anfitrião 4 (nó universal)	RU 5	eno1
1/41	VLAN de gestão (1 Gigabit)	Servidor UCS anfitrião 5 (nó universal)	RU 3	eno1
1/42	VLAN de gestão (1 Gigabit)	Servidor UCS anfitrião 6 (nó universal)	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 externa (10 Gigabit)	Router do 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	—	—	—	—

Tabela 6: Ligações do Switch Leaf 2 (RU 11)

Porta Leaf	Tipo de ligação	Ligação		
		Dispositivo	RU em um rack	Porta um rack
1/1	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 1 (nó universal)	9 RU	eno6
1/2	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 2 (nó universal)	8 RU	eno6
1/3	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 3 (nó universal)	6 RU	eno6
1/4	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 4 (nó universal)	5 RU	eno6
1/5	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 5 (nó universal)	3 RU	eno6
1/6	VLAN interna (10 Gigabit)	Servidor UCS anfitrião 6 (nó universal)	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 externa (10 Gigabit)	Servidor UCS anfitrião 1 (nó universal)	9 RU	eno5
1/20	VLAN externa (10 Gigabit)	Servidor UCS anfitrião 2 (nó universal)	8 RU	eno5
1/21	VLAN externa (10 Gb)	Servidor UCS anfitrião 3 (nó universal)	6 RU	eno5
1/22	VLAN externa (10 Gigabit)	Servidor UCS anfitrião 4 (nó universal)	5 RU	eno5
1/23	VLAN externa (10 Gigabit)	Servidor UCS anfitrião 5 (nó universal)	3 RU	eno5
1/24	VLAN externa (10 Gigabit)	Servidor UCS anfitrião 6 (nó universal)	2 RU	eno5
1/25	—	—	—	—

Porta Leaf	Tipo de ligação	Ligação		
		Dispositivo	RU em um rack	Porta
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	VLAN interna (10 Gigabit)	Switch Leaf 1	12 RU	1/46
1/46	—	—	—	—
1/47	VLAN externa (10 Gigabit)	Router do 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	—	—	—	—

Porta Leaf	Tipo de ligação	Ligação		
		Dispositivo	RU em um rack	Porta
1/52	—	—	—	—
1/53	—	—	—	—
1/54	—	—	—	—



CAPÍTULO 6

Especificações do sistema

- [Especificações ambientais, na página 43](#)
- [Cabos de alimentação, na página 43](#)

Especificações ambientais

A tabela seguinte enumera as especificações ambientais para instalar o cluster Secure Workload.

Tabela 7: Especificações ambientais

Ambiente		Especificação
Temperatura	Funcionamento	5 a 35 °C com redução da temperatura máxima em 1 °C por cada 305 m acima do nível do mar
	Armazenamento	-40 a 65°C (-40 a 149°F)
Humidade	Funcionamento	10 a 80% de humidade relativa com uma gradação de humidade de 10% por hora
	Armazenamento	5 a 93% de humidade relativa
Altitude	Funcionamento	0 a 3050 m
	Armazenamento	0 a 12 200 m

Cabos de alimentação

As tabelas seguintes indicam os cabos de alimentação que são incluídos com o cluster Secure Workload M6.

Tabela 8: Cluster 39-RU, configuração de um rack

Número de peça	Descrição	Quantidade
TA-RACK-UCS2-INT	Rack dinâmico Cisco R42612 com painéis laterais	1
TA-ETH-RJ45-SINGLE	Kit de cabo RJ-45 para uma configuração de um rack 39-RU	1

Número de peça	Descrição	Quantidade
TA-SFP-H10GB-CU2M	10GBASE-CU SFP+ Cabo 2 m	16
TA-SFP-H10GB-CU1-5	10GBASE-CU SFP+ Cabo 1,5 m	32
TA-QSFP-H40G-CU1M	40GBASE-CR4 Cabo passivo 1 m em cobre	4
TA-SFP-H10GB-CU1M	10GBASE-CU SFP+ Cabo 1 m	25
TA-SFP-H10GB-CU2-5	10GBASE-CU SFP+ Cabo 2,5 m	20

Tabela 9: Cluster 39-RU, configuração de rack duplo

Número de peça	Descrição	Quantidade
TA-RACK-UCS2-INT	Rack dinâmico Cisco R42612, com painéis laterais	2
TA-ETH-RJ45-DUAL	Kit de cabo RJ-45 para uma configuração de um rack 39-RU	1
TA-SFP-H10GB-CU2M	10GBASE-CU SFP+ Cabo 2 m	15
TA-SFP-H10GB-CU1-5	10GBASE-CU SFP+ Cabo 1,5 m	19
TA-QSFP-H40G-CU1M	40GBASE-CR4 Cabo passivo 1 m em cobre	1
TA-QSFP-H40G-CU5M	40GBASE-CR4 Cabo passivo 5 m em cobre	3
TA-SFP-H10GB-CU2-5	10GBASE-CU SFP+ Cabo 2,5 m	12
TA-SFP-H10GB-CU5M	10GBASE-CU SFP+ Cabo 5 m	47

Tabela 10: Cluster 8-RU

Número de peça	Descrição	Quantidade
TA-RACK-UCS2-INT	Rack dinâmico Cisco R42612, com painéis laterais	1
CAB-ETH-S-RJ45	Cabo RJ-45 direto amarelo de 1,83 m para Ethernet	6
TA-SFP-H10GB-CU1M	10GBASE-CU SFP+ Cabo 1 m	13
TA-SFP-H10GB-CU1-5	10GBASE-CU SFP+ Cabo 1,5 m	12
TA-QSFP-H40G-CU1M	40GBASE-CR4 Cabo passivo 1 m em cobre	2
GLC-TE	Módulo transceptor SFP 1000BASE-T para fio de cobre de Categoria 5	6