



Guía de despliegue del clúster M6 de Cisco Secure Workload

Primera publicación: 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 los derechos reservados.



CONTENIDO

CAPÍTULO 1

Descripción general 1

- Descripción general 1
- Panel frontal del servidor Cisco UCS C220 M6 5
- Panel trasero del servidor Cisco UCS C220 M6 6

CAPÍTULO 2

Preparar el sitio 9

- Requisitos de temperatura 9
- Requisitos relacionados con la humedad 9
- Requisitos de altitud 10
- Requisitos relacionados con el polvo y las partículas 10
- Minimizar las interferencias electromagnéticas y de radiofrecuencia 10
- Requisitos relacionados con los impactos y las vibraciones 11
- Requisitos de conexión a tierra 11
- Requisitos de alimentación 11
- Requisitos de flujo de aire 12
- Requisitos de espacio 12

CAPÍTULO 3

Conectar a tierra y conectar 13

- Conexión a tierra de los dispositivos del clúster de Cisco Secure Workload 13
- Encendido de los dispositivos del clúster de Cisco Secure Workload 13
- Conectar el clúster de Cisco Secure Workload a los routers 14

CAPÍTULO 4

Configurar la interfaz de usuario 15

- (Opcional) Requisitos y limitaciones del modo de pila dual (compatibilidad con IPv6) 15
- Configurar la interfaz de usuario 16

CAPÍTULO 5	Cableado del dispositivo del clúster de C1-Secure Workload	21
	Cableado del dispositivo del clúster de C1-Workload	21
	Cableado del dispositivo del clúster de C1-Workload-M	33

CAPÍTULO 6	Especificaciones del sistema	43
	Especificaciones ambientales	43
	Cables de alimentación	43



CAPÍTULO 1

Descripción general

- [Descripción general, en la página 1](#)
- [Panel frontal del servidor Cisco UCS C220 M6, en la página 5](#)
- [Panel trasero del servidor Cisco UCS C220 M6, en la página 6](#)

Descripción general

Puede implementar el clúster M6 de Cisco Secure Workload de cualquiera de las siguientes formas:

- Plataforma de 39 unidades de rack (RU) de formato grande (rack individual de C1-Workload) para centros de datos con más de 5000 servidores.

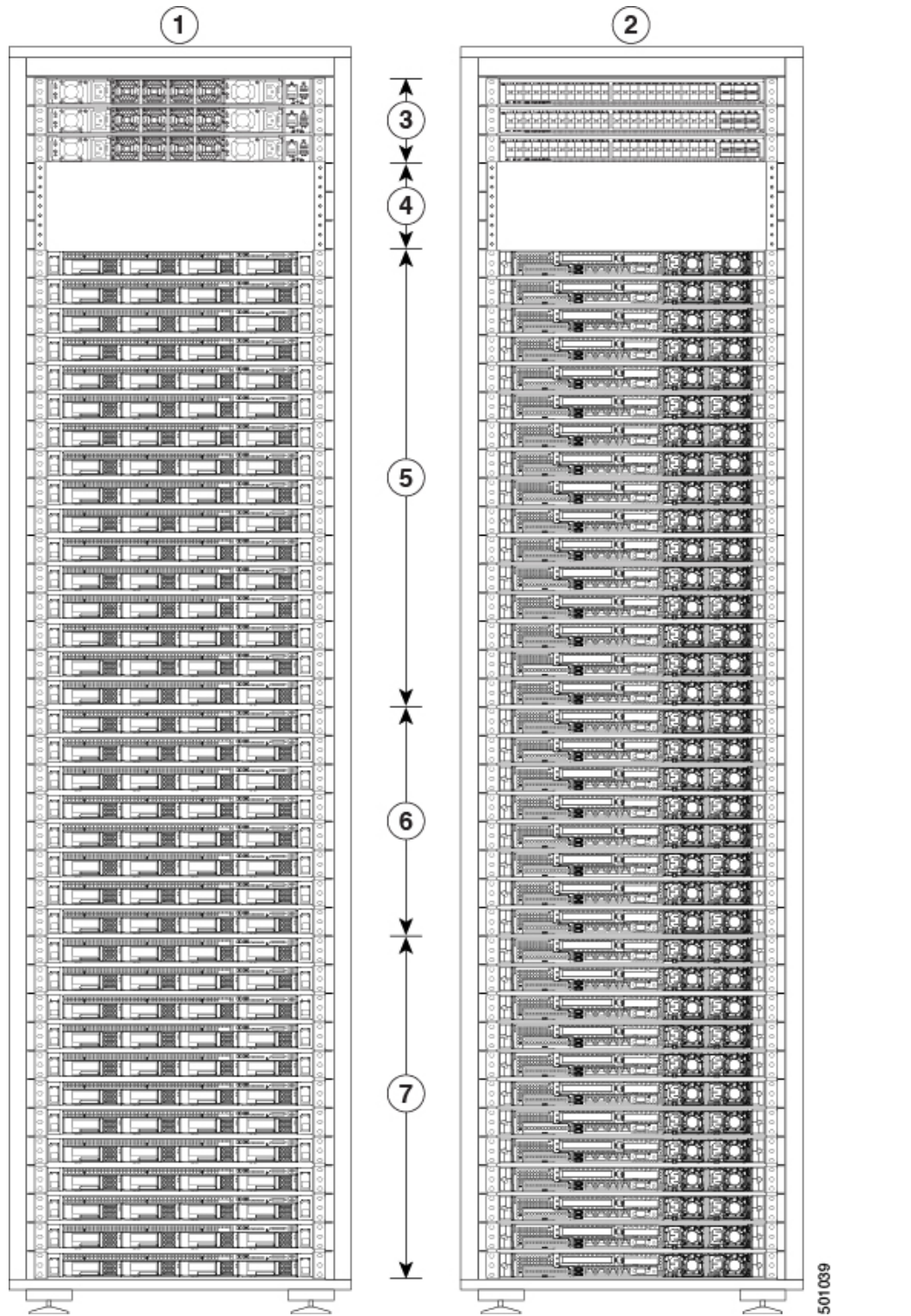


Nota Puede implementar la plataforma de formato grande en uno o dos racks, en función de sus requisitos. Consulte las siguientes figuras de un rack y dos racks de C1-Workload para ver ejemplos.

- Plataforma de 8 RU de formato pequeño (C1-Workload-M) para centros de datos con menos de 5000 servidores. Consulte la figura de C1-Workload-M para ver un ejemplo.

La siguiente figura muestra la parte frontal y trasera del rack individual de C1-Workload.

Figura 1: Parte frontal y trasera del rack individual de C1-Workload

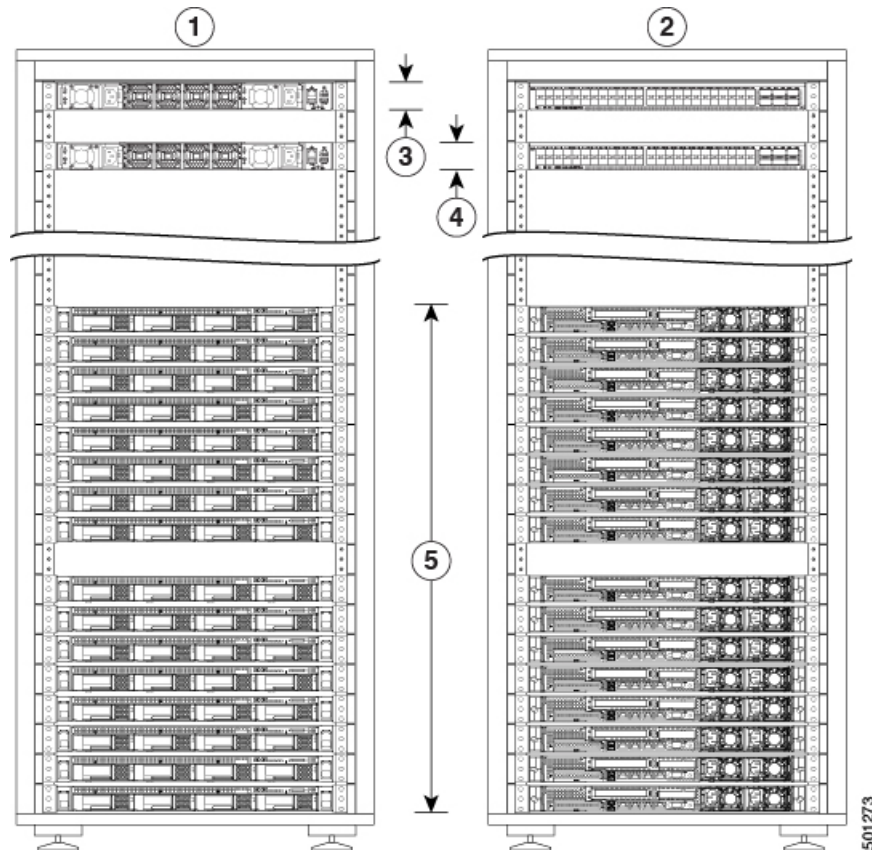


1	2
Parte frontal (vista del pasillo frío)	Parte trasera (vista del pasillo caliente)

3	Una columna (RU 42) y dos switches de hoja: hoja 2 (RU 40) y hoja 1 (RU 41)	4	Unidades de rack abiertas (RU 37 a 39)
5	16 servidores de procesamiento (RU 21 a 36)	6	Ocho servidores de servicio (RU 13 a 20)
7	12 servidores base (RU 1 a 12)		—

La siguiente figura muestra la parte frontal y trasera del rack doble de C1-Workload.

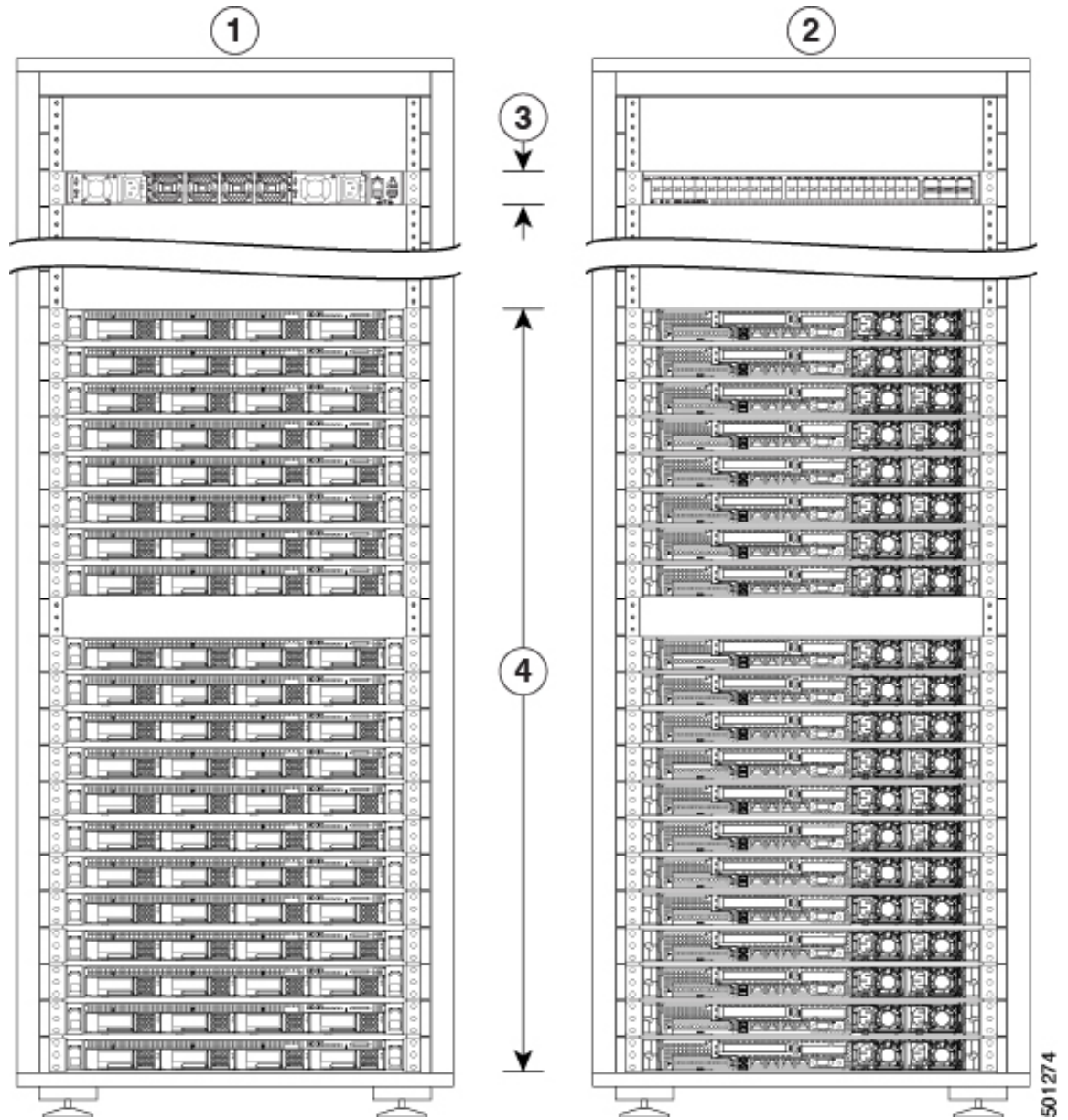
Figura 2: Parte frontal y trasera del rack 1 del rack doble de C1-Workload



1	Parte frontal (vista del pasillo frío)	2	Parte trasera (vista del pasillo caliente)
3	Un switch de columna (RU 42)	4	Switch de hoja 1 (RU 40)
5	16 servidores de procesamiento (RU 1 a 4 y 6 a 9)	6	—

La siguiente figura muestra la parte frontal y trasera del rack 2 del rack doble de C1-Workload.

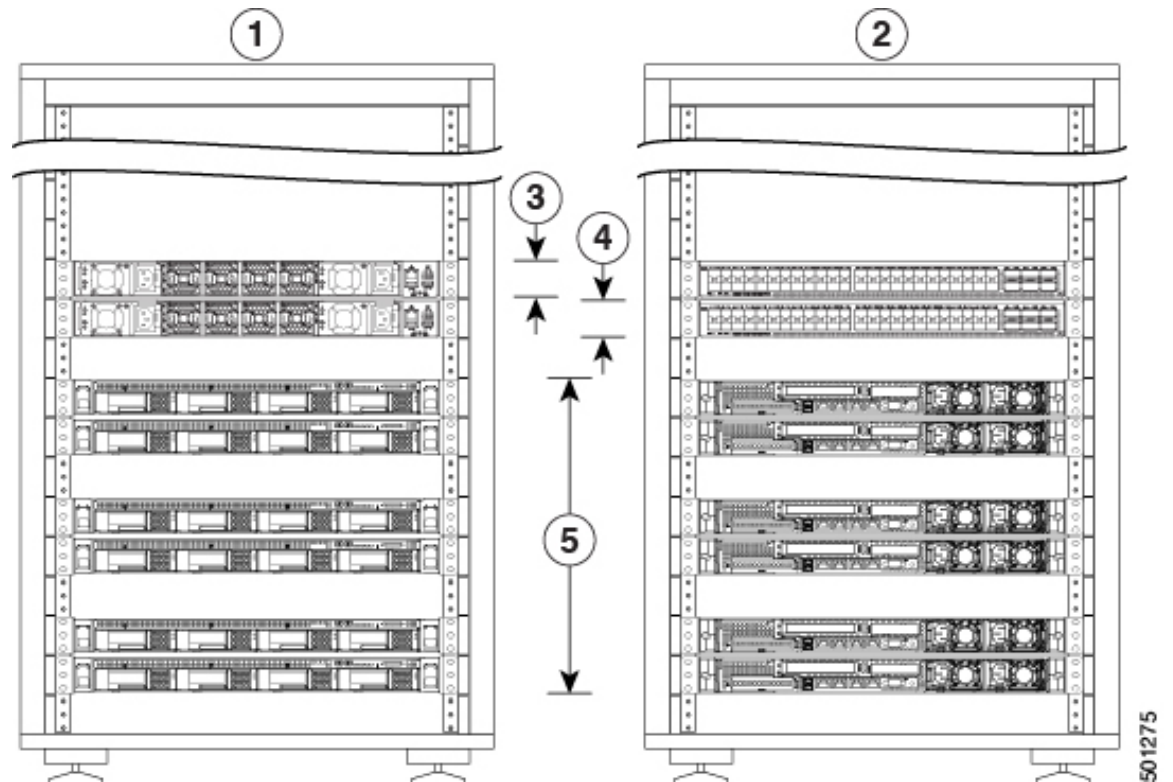
Figura 3: Parte frontal y trasera del rack 2 del rack doble de C1-Workload



<p>1 Parte frontal (vista del pasillo frío)</p>	<p>2 Parte trasera (vista del pasillo caliente)</p>
<p>3 Switch de hoja 2 (RU 40)</p>	<p>4 Ocho servidores de servicio (RU 14 a 21) y 12 servidores base (RU 1 a 12)</p>

La siguiente figura muestra la parte frontal y trasera del rack individual de C1-Workload-M.

Figura 4: Parte delantera y trasera de C1-Workload-M



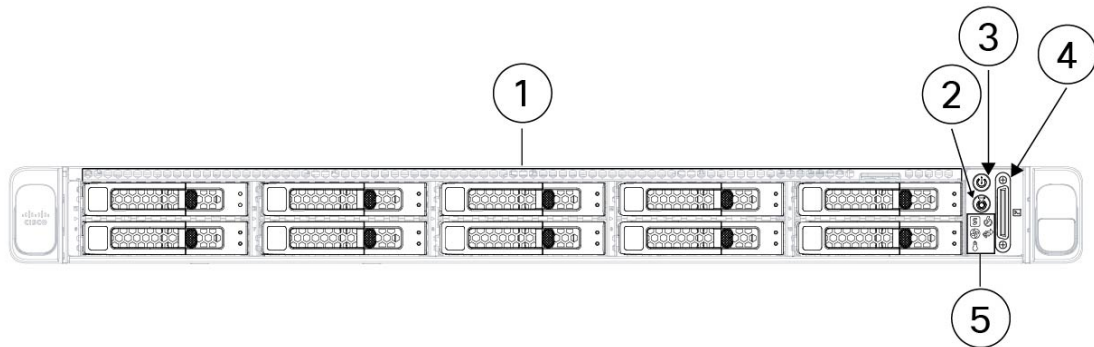
1	Parte frontal (vista del pasillo frío)	2	Parte trasera (vista del pasillo caliente)
3	Switch de hoja 1 (RU 12)	4	Switch de hoja 2 (RU 11)
5	Seis servidores universales (RU 2, 3, 5, 6, 8 y 9)	—	

Panel frontal del servidor Cisco UCS C220 M6

La siguiente figura muestra el panel frontal del servidor UCS C220 M6 con unidades de formato pequeño (SFF).

Consulte la [Guía de instalación y servicio del servidor Cisco UCS C220 M6](#) para obtener más información.

Figura 5: Panel frontal del servidor Cisco UCS C220 M6



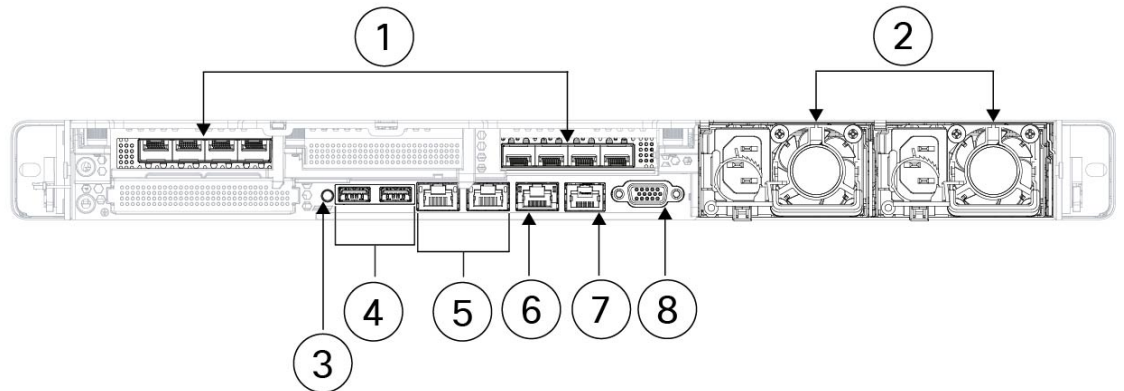
<p>1 Bahías de unidad 1 a 10, numeradas de izquierda a derecha, de arriba a abajo</p> <p>Es compatible con HDD y SDD SAS/SATA. Como opción, las bahías de unidad 1 a 4 pueden contener hasta 4 unidades NVMe en cualquier número hasta 4. Las bahías de unidad 5 a 10 solo son compatibles con HDD o SSD SAS/SATA.</p>	<p>2 LED/botón de identificación de la unidad</p>
<p>3 Botón de encendido/LED de estado de la alimentación</p>	<p>4 Conector KVM</p> <p>Se utiliza con un cable KVM que ofrece un VGA DB-15, un puerto serie DB-9 y dos conectores USB 2.0.</p>
<p>5 LED del sistema:</p> <ul style="list-style-type: none"> • LED de estado del ventilador • LED de estado del sistema • LED de estado de la fuente de alimentación • LED de la actividad de enlace de red • LED de estado de la temperatura 	<p>—</p>

Panel trasero del servidor Cisco UCS C220 M6

La siguiente figura muestra el panel trasero del servidor UCS C220 M6.

Consulte la [Guía de instalación y servicio del servidor Cisco UCS C220 M6](#) para obtener más información.

Figura 6: Panel trasero del servidor Cisco UCS C220 M6



<p>1</p>	<p>Dos ranuras PCIe</p> <ul style="list-style-type: none"> • Canal vertical 1 (controlado por la CPU 1) <ul style="list-style-type: none"> • Compatible con una ranura PCIe (ranura 1) • La ranura 1 es de media altura, 3/4 de longitud, x16 • Canal vertical 3 (controlado por la CPU 2) <ul style="list-style-type: none"> • Compatible con una ranura PCIe (ranura 3) • La ranura 3 es de media altura, 3/4 de longitud, x16 	<p>2</p> <p>Dos unidades de fuente de alimentación (PSU), que son redundantes cuando se configuran en el modo de alimentación 1+1</p>
<p>3</p>	<p>LED/botón de identificación del sistema</p>	<p>4</p> <p>Dos puertos USB 3.0</p>
<p>5</p>	<p>Puertos Ethernet dobles de 1 Gb/10 Gb (LAN1 y LAN2)</p> <p>Los puertos LAN dobles admiten 1 Gbps y 10 Gbps en función de la capacidad del partner del enlace.</p>	<p>6</p> <p>Puerto Ethernet de gestión exclusivo de 1 Gb</p>
<p>7</p>	<p>Puerto COM (conector RJ-45)</p>	<p>8</p> <p>Puerto VGA de vídeo (conector DB-15)</p>



CAPÍTULO 2

Preparar el sitio

- [Requisitos de temperatura, en la página 9](#)
- [Requisitos relacionados con la humedad, en la página 9](#)
- [Requisitos de altitud, en la página 10](#)
- [Requisitos relacionados con el polvo y las partículas, en la página 10](#)
- [Minimizar las interferencias electromagnéticas y de radiofrecuencia, en la página 10](#)
- [Requisitos relacionados con los impactos y las vibraciones, en la página 11](#)
- [Requisitos de conexión a tierra, en la página 11](#)
- [Requisitos de alimentación, en la página 11](#)
- [Requisitos de flujo de aire, en la página 12](#)
- [Requisitos de espacio, en la página 12](#)

Requisitos de temperatura

Los switches y los servidores del clúster de Cisco Secure Workload requieren una temperatura de funcionamiento de 5 a 35 °C (41 a 95 °F) con una disminución de la temperatura máxima de 1 °C por cada 305 m (1000 pies) de altitud sobre el nivel del mar. Si estos dispositivos no funcionan, la temperatura debe estar a entre -40 y 65 °C (-40 y 149 °F).

Requisitos relacionados con la humedad

Un nivel elevado de humedad puede hacer que esta se introduzca en los switches y los servidores. La humedad puede provocar corrosión de los componentes internos y degradación de propiedades como la resistencia eléctrica, la conductividad térmica, la resistencia física y el tamaño. Los switches y los servidores están preparados para funcionar a entre un 10 y un 90 % de humedad relativa, con un grado de humedad del 10 % por hora. En condiciones no operativas, estos dispositivos pueden resistir del 5 al 93 % de humedad relativa.

Los edificios en los que el clima se controla mediante aire acondicionado en los meses más cálidos y mediante calefacción en los más fríos normalmente mantienen un nivel aceptable de humedad para los dispositivos. Sin embargo, si los dispositivos están ubicados en una zona excepcionalmente húmeda, debe utilizar un deshumidificador para mantener la humedad dentro de un intervalo aceptable.

Requisitos de altitud

Si utiliza los dispositivos del rack a una altitud superior (baja presión), la eficacia de la refrigeración forzada y de convección se ve reducida y puede generar problemas eléctricos que están relacionados con el efecto corona y el de arco. Esta condición también puede provocar que fallen los componentes sellados con presión interna, como los condensadores electrolíticos, o que actúen con una eficacia reducida. Estos dispositivos están capacitados para funcionar a altitudes de 0 a 3050 m (0 a 10 000 pies) y se pueden almacenar a altitudes de 0 a 12 200 m (0 a 40 000 pies).

Requisitos relacionados con el polvo y las partículas

Los ventiladores enfrían las fuentes de alimentación, los switches y los servidores al aspirar aire y extraerlo a través de varias aperturas en el chasis. Sin embargo, los ventiladores también tragan polvo y otras partículas, lo cual crea una acumulación de contaminantes en el switch y aumenta la temperatura interna del chasis. Un entorno operativo limpio puede reducir en gran medida los efectos negativos del polvo y otras partículas, que actúan como aislantes e interfieren en los componentes mecánicos de los switches y los servidores.

Además de limpiar de manera regular, siga las siguientes precauciones para evitar que los switches y servidores del rack se contaminen:

- No permita que se fume cerca del rack.
- No permita que se consuma comida o bebida cerca del rack.

Minimizar las interferencias electromagnéticas y de radiofrecuencia

La interferencia electromagnética (EMI) y la interferencia de radiofrecuencia (RFI) de los dispositivos del rack del clúster de Cisco Secure Workload pueden afectar negativamente a otros dispositivos, como los receptores de radio y televisión (TV) que funcionen cerca del rack. Las radiofrecuencias que surgen de los dispositivos del rack también pueden interferir en teléfonos inalámbricos y de baja potencia. Por el contrario, la RFI de teléfonos de alta potencia puede provocar que aparezcan caracteres falsos en la pantalla de los dispositivos.

La RFI es cualquier EMI con una frecuencia por encima de 10 kHz. Este tipo de interferencia puede viajar del switch a otros dispositivos a través del cable de alimentación y de la fuente de alimentación, o a través del aire, como se transmiten las ondas de radio. La Comisión Federal de Comunicaciones (FCC) publica normas específicas para limitar la cantidad de EMI y RFI que pueden emitir los equipos informáticos. Cada switch cumple estas normas de la FCC.

Cuando los cables funcionan a cualquier distancia significativa en un campo electromagnético, pueden producirse interferencias entre el campo y las señales de los cables, con las siguientes implicaciones:

- Un mal cableado puede provocar que el cableado de planta emita interferencias de radio.
- Una EMI intensa, especialmente cuando está provocada por transmisores de luz o radio, puede destruir los emisores y receptores de señal del chasis e incluso crear un peligro eléctrico al conducir subidas de potencia al equipo a través de las líneas.



Nota Para predecir y evitar las EMI intensas, consulte a expertos en RFI.

Es poco probable que el cableado emita interferencias de radio si utiliza un cable de par trenzado con una buena distribución de los conductores a tierra. Si supera las distancias recomendadas, utiliza un cable de par trenzado de gran calidad con un conductor a tierra para cada señal de datos, cuando sea necesario.



Precaución Si los cables superan las distancias recomendadas, o si pasan entre edificios, preste especial atención al efecto de los rayos en sus inmediaciones. El pulso electromagnético provocado por rayos u otros fenómenos de alta potencia puede reunir suficiente energía en conductores desprotegidos como para destruir dispositivos electrónicos. Consulte a expertos en protección y supresión de sobretensión eléctrica si ha tenido problemas similares con anterioridad.

Requisitos relacionados con los impactos y las vibraciones

Los dispositivos del clúster de Cisco Secure Workload se han probado en relación con vibraciones e impactos para los estándares de rango de funcionamiento, manipulación y terremotos.

Requisitos de conexión a tierra

Los dispositivos del clúster de Cisco Secure Workload son sensibles a las variaciones de tensión suministradas por las fuentes de alimentación. La sobretensión, la subtensión y los transitorios (o picos) pueden eliminar datos de la memoria o provocar daños en los componentes. Para protegerse ante este tipo de problemas, asegúrese de que haya una conexión de toma a tierra en los dispositivos. Debe conectar el rack a la toma de tierra de la instalación.

Los puntos de conexión a tierra del chasis están diseñados para los tornillos M5. Debe proporcionar sus propios tornillos, terminal de toma a tierra y cable de toma a tierra. El terminal de toma a tierra debe ser un terminal de doble orificio que se ajuste a los tornillos M5. El cable de toma a tierra que proporcione debe ser un cable AWG de tamaño 14 (2 mm), un mínimo de 60 °C o según lo permita el código local.

Requisitos de alimentación

Los clústeres de Cisco Secure Workload deben estar provistos de fuentes de alimentación que proporcionen las siguientes cantidades de energía para las operaciones:

- Plataforma de formato grande de 39 RU, rack individual: 22 500 W
- Plataforma de formato grande de 39 RU, rack doble: 11 500 W para cada rack
- Plataforma de formato pequeño de 8 RU: 6500 W

Para obtener la redundancia de alimentación $n+n$ necesaria, se necesitan dos fuentes de alimentación de CA que proporcionen cada una esa cantidad de energía.

Cada chasis del rack tiene dos fuentes de alimentación, una para las operaciones y otra para la redundancia. Cada fuente de alimentación está conectada a una regleta diferente del rack y cada regleta está conectada a una fuente de alimentación de CA diferente. Si falla una fuente de alimentación, la otra proporciona la alimentación necesaria para cada switch o servidor del rack.

Requisitos de flujo de aire

El clúster de Cisco Secure Workload requiere que se coloque cada rack con las fuentes de alimentación y los ventiladores de los tres switches en un pasillo frío. Cuando se colocan de esta manera, todos los dispositivos del rack incorporan aire de refrigeración de un pasillo frío y expulsan aire caliente a un pasillo caliente.

Requisitos de espacio

La siguiente tabla enumera la cantidad de espacio necesaria para instalar el clúster de Cisco Secure Workload de formato grande de 39 RU (rack individual o doble) o de formato pequeño de 8 RU. El pasillo de instalación debe tener más de 23,5 pulgadas (59,69 cm) de ancho para mover el rack a su sitio. Además, debe tener suficiente espacio para que una persona pueda acceder a la parte frontal y trasera para realizar el mantenimiento.

Tabla 1: Requisitos de espacio

Tipo de instalación	Ancho mínimo del pasillo ¹	Espacio mínimo de instalación del rack
Instalación de C1-Workload (rack individual)	23,5 pulgadas (59,69 cm)	23,5 pulgadas (59,69 cm) de ancho por 49,8 pulgadas (126,492 cm) de profundidad
C1-Workload (rack doble)	23,5 pulgadas (59,69 cm)	47 pulgadas (119,38 cm) de ancho por 49,8 pulgadas (126,492 cm) de profundidad
C1-Workload-M	23,5 pulgadas (59,69 cm)	23,5 pulgadas (59,69 cm) de ancho por 49,8 pulgadas (126,492 cm) de profundidad

¹ El pasillo de instalación y el pasillo en el que se abre la puerta frontal del rack deben tener al menos 23,5 pulgadas (59,69 cm) de ancho. El otro pasillo, en el que se abren las puertas del armario doble, debe tener al menos 11,75 pulgadas (29,845 cm) de ancho para que las puertas se abran completamente, pero se necesitan al menos 23,5 pulgadas (59,69 cm) para que una persona realice el mantenimiento.

El rack se coloca con los ventiladores del switch (el lado del rack con la puerta más grande) orientados hacia el pasillo frío y los puertos del switch (el lado del rack con puertas dobles) orientados hacia el pasillo caliente.



CAPÍTULO 3

Conectar a tierra y conectar

- [Conexión a tierra de los dispositivos del clúster de Cisco Secure Workload, en la página 13](#)
- [Encendido de los dispositivos del clúster de Cisco Secure Workload, en la página 13](#)
- [Conectar el clúster de Cisco Secure Workload a los routers, en la página 14](#)

Conexión a tierra de los dispositivos del clúster de Cisco Secure Workload

Los dispositivos del clúster de Cisco Secure Workload tienen conexiones de metal a metal a su rack, por lo que, en cuanto se conecte el rack (o los racks en caso de una instalación de rack doble) a la toma a tierra del centro de datos, los dispositivos del rack estarán conectados a tierra. Para conectar a tierra un rack, conecte las ruedas del rack a la toma a tierra.

Encendido de los dispositivos del clúster de Cisco Secure Workload

Para encender el switch, debe conectar las dos regletas de alimentación conectadas al rack a dos fuentes de alimentación de CA.



Nota Conecte este equipo a una red eléctrica de CA que tenga un dispositivo de protección contra sobretensiones (SPD) en el equipo de servicio que sea compatible con la NFPA 70, el National Electrical Code (NEC).

Lea las instrucciones de instalación antes de usar, instalar o conectar el sistema a la fuente de alimentación.


No sobrecargue el cableado cuando conecte las unidades al circuito de alimentación.

Antes de empezar

- Los racks deben instalarse en el centro de datos y fijarse en su lugar con las entradas de aire colocadas en un pasillo frío.
- Los racks deben conectarse a la toma de tierra del centro de datos.

- El clúster debe conectarse a dos routers suministrados por el cliente (y cada router debe conectarse a un switch de hoja distinto).
- Debe haber dos fuentes de alimentación que cumplan los requisitos de alimentación del rack al alcance de cada cable de la regleta de alimentación del rack.

Paso 1 Conecte el cable de alimentación de una regleta a una fuente de alimentación de CA y el cable de alimentación de la segunda regleta a otra fuente de alimentación de CA.

Paso 2 Observe cada una de las fuentes de alimentación instaladas en cada uno de los dispositivos del rack para comprobar que el LED  esté encendido y de color verde.

- Si ninguno de los LED está encendido, asegúrese de que la fuente de alimentación esté encendida y de que el switch de encendido/apagado de la regleta esté encendido.
- Si algunos de los LED están encendidos y otros no, asegúrese de que el cable de alimentación que proviene de esa fuente de alimentación esté totalmente conectado a la regleta del rack.

Conectar el clúster de Cisco Secure Workload a los routers

Debe conectar el clúster de Cisco Secure Workload a los dos routers.

Paso 1 Si está instalando un clúster de doble rack de formato grande de 39 RU, conecte los cables de interfaz parcialmente conectados a cada rack. Con cada uno de estos cables, conéctelo al puerto etiquetado del otro rack.

Paso 2 Utilice un cable de 10 Gigabit para conectar un router al puerto E1/39 del switch de hoja 1 para una implementación de 39 RU o al puerto E1/47 para una implementación de 8 RU. El switch de hoja 1 se encuentra en la siguiente ubicación:

- Plataforma de rack individual de formato grande de 39 RU: RU 40 en el rack de la plataforma
- Plataforma de rack doble de formato grande de 39 RU: RU 40 en el rack 1
- Plataforma de formato pequeño de 8 RU: RU 12 en el rack de la plataforma

Paso 3 Utilice un cable de 10 Gigabit para conectar un router al puerto E1/39 del switch de hoja 2 para una implementación de 39 RU o al puerto E1/47 para una implementación de 8 RU. El switch de la hoja 2 se encuentra en la siguiente ubicación:

- Plataforma de rack individual de formato grande de 39 RU: RU 41 en el rack de la plataforma
- Plataforma de rack doble de formato grande de 39 RU: RU 41 en el rack 2
- Plataforma de formato pequeño de 8 RU: RU 11 en el rack de la plataforma



CAPÍTULO 4

Configurar la interfaz de usuario

- (Opcional) Requisitos y limitaciones del modo de pila dual (compatibilidad con IPv6), en la página 15
- Configurar la interfaz de usuario, en la página 16

(Opcional) Requisitos y limitaciones del modo de pila dual (compatibilidad con IPv6)

Los clústeres de Cisco Secure Workload que se ejecutan en hardware físico se pueden configurar para utilizar IPv6 además de IPv4 para determinadas comunicaciones hacia y desde el clúster.



Nota Puede utilizar la función del modo de pila dual (compatibilidad con IPv6) al instalar o actualizar a las versiones 3.6.1.5, 3.7.1.5 y 3.8.1.1; sin embargo, la opción para activar la función no está disponible al instalar o actualizar versiones de parches.

Limitaciones

Si se está planteando activar el modo de pila dual, tenga en cuenta lo siguiente:

- Puede activar la conectividad IPv6 solo durante el despliegue inicial o actualizar a una versión principal (no puede activar esta función durante las actualizaciones de parches).
- El modo de pila dual solo es compatible con hardware físico o clústeres de hardware físico.
- No es compatible con el modo de solo IPv6.
- No puede volver al modo de solo IPv4 después de habilitar el modo de pila dual para el clúster.
- La copia de seguridad y restauración de datos (Data Backup and Restore, DBR) no es compatible si está activada la conectividad de doble pila.
- No active el modo de pila dual para los clústeres configurados con Federation.
- Las siguientes funciones siempre utilizan IPv4 (tenga en cuenta que IPv4 siempre está activado incluso si IPv6 está activado):
 - (Aplicable a las versiones 3.8.1.1, 3.7.1.5 y 3.6.x) Aplicación en agentes AIX
 - (Aplicable solo a la versión 3.6.x) Comunicación del agente de hardware con el clúster

- (Aplicable solo a la versión 3.6.x) Conectores para ingestión de flujos, enriquecimiento del inventario o notificaciones de alertas

Requisitos

- Configure los registros DNS A y AAAA para FQDN antes de habilitar el modo de pila dual para su clúster.
- Los servicios externos como NTP, SMTP y DNS deben estar disponibles tanto en IPv4 como en IPv6, por motivos de redundancia.
- Para configurar el modo de pila doble para un clúster:
 - A cada uno de los dos switches hoja del cluster se le deben asignar direcciones IPv6 enrutables en dos redes diferentes, por redundancia, y se deben proporcionar gateways predeterminadas para cada red.
 - Para los clústeres de 39 RU, se requiere una red IPv6 enrutable en el sitio con espacio para al menos 29 direcciones de host.
 - Para los clústeres de 8 RU, se requiere una red IPv6 enrutable en el sitio con espacio para al menos 20 direcciones de host.
 - Las tres primeras direcciones de host de la red IPv6 enrutable del sitio están reservadas para la configuración de HSRP del clúster de Cisco Secure Workload y no deben ser utilizadas por ningún otro dispositivo.

Información adicional

Los agentes se comunican con el clúster mediante IPv4 a menos que los configure para usar IPv6. Para obtener instrucciones, consulte la Guía de usuario de Cisco Secure Workload.

Configurar la interfaz de usuario

Antes de empezar

- Para completar esta configuración, necesita un dispositivo como un ordenador portátil con un puerto Ethernet y acceso a Internet.
- Necesita un cable Ethernet para conectar el dispositivo al servidor más alto del clúster de Cisco Secure Workload.
- Google Chrome es el único navegador compatible con el portal de configuración, que es necesario para parte de este proceso.
- (Opcional) A partir de la versión 3.6 y posteriores, puede configurar el clúster en modo de pila dual, lo que permite utilizar tanto IPv4 como IPv6 para la comunicación entre determinados componentes de Cisco Secure Workload y servicios de red como NTP y DNS. (Cisco Secure Workload ya gestiona el tráfico IPv6, tanto si activa el modo de pila dual como si no). Puede habilitar esta compatibilidad solo durante el despliegue o la actualización.

Si está pensando en activar la compatibilidad para IPv6, consulte [\(Opcional\) Requisitos y limitaciones del modo de pila dual \(compatibilidad con IPv6\)](#), en la página 15.



Importante Introduzca las direcciones IPv4 en todos los campos del siguiente procedimiento, a menos que el nombre del campo indique explícitamente IPv6.

Paso 1 Configure el dispositivo de Internet con una dirección IP de 2.2.2.1/30 (255.255.255.252).

Paso 2 Utilice un cable Ethernet para conectar el puerto Ethernet del dispositivo de Internet al puerto 2 de LOM (LAN2) del servidor más alto de la parte superior del clúster de Cisco Secure Workload.

Paso 3 En el dispositivo de Internet, abra el navegador Chrome y vaya a <http://2.2.2.2:9000>.

Nota El navegador Chrome es el único navegador probado con este proceso.

Se abre la página de diagnóstico de la configuración.

Paso 4 Si hay errores en la página de diagnóstico, compruebe las conexiones del cableado entre los dispositivos del clúster en busca de conexiones rotas o cables mal enrutados antes de continuar con este procedimiento. Cuando haya terminado, vuelva al paso 2.

Consulte [Cableado del dispositivo del clúster de C1-Workload, en la página 21](#) y [Cableado del dispositivo del clúster de C1-Workload-M, en la página 33](#) para obtener información sobre el cableado correcto.

Paso 5 Haga clic en **Continue** (Continuar).

Se abre la página de carga de RPM.

Nota Si en su lugar se abre la página de configuración del sitio, introduzca la siguiente URL para abrir la página de carga de RPM:

`http://2.2.2.2:9000 /upload`

Paso 6 Cargue archivos RPM en la nube de Cisco Secure Workload.

Debe cargar los archivos en el siguiente orden:

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

- a) Haga clic en **Choose File (Seleccionar archivo)**.
- b) Vaya a un RPM, selecciónelo y haga clic en **Open (Abrir)**.
- c) Haga clic en **Upload (Cargar)**.

La lista de RPM de la página no se actualiza a medida que carga cada RPM. Este es el comportamiento esperado.

Si ve un error después de cargar el archivo

`tetration_os_mother_rpm_k9-2.1.1.31-1.e16.x86_64.rpm`, espere de 5 a 10 minutos y vuelva a

cargar la página. Debería ver la lista de RPM cargados después de volver a cargar la página. El error se debe al reinicio del Orquestador y no es un problema.

d) Repita los pasos del a al c con cada RPM.

Después de terminar de cargar los RPM, se abre la página de configuración del sitio.

Paso 7 Utilice la página Configuración del sitio para configurar el nuevo sitio de la siguiente manera:

- Haga clic en **General**.

1. En el campo **Site Name (Nombre del sitio)**, introduzca el nombre exclusivo del clúster.
2. En el campo **SSH Public Key (Clave pública de SSH)**, pegue la clave de autenticación.

Nota Genere un par de claves SSH propio que pueda utilizarse para el acceso SSH del clúster.

Le recomendamos encarecidamente que mantenga la clave SSH en una ubicación segura, duradera y accesible con el fin de solucionar problemas o recuperar el clúster mediante `ta_guest access`.

3. Haga clic en **Next (Siguiente)**.

- Haga clic en **Email (Correo electrónico)**.

1. Rellene las direcciones de correo electrónico necesarias.
2. Haga clic en **Next (Siguiente)**.

- Haga clic en **L3**.

Introduzca cada una de las direcciones solicitadas. Todos los campos marcados con * son obligatorios.

Introduzca todas las direcciones como IPv4 a menos que el nombre del campo especifique IPv6.

(Opcional) Si está instalando la versión 3.6 o posterior del software: Activar el modo de pila dual (compatibilidad con IPv4 e IPv6):

1. Seleccione la casilla de verificación IPv6.
2. Introduzca la dirección IPv6 en notación CIDR para los switches de hoja 1 y 2.
3. Introduzca la gateway predeterminada IPv6 de hoja 1 y 2.
4. Haga clic en **Siguiente**.

- Haga clic en **Network (Red)**.

Introduzca todas las direcciones como IPv4 a menos que el nombre del campo especifique IPv6.

1. En el campo **Internal network IP address (Dirección IP de red interna)**, pegue la dirección de la salida de la implementación del Orquestador.
2. En el campo **External network IP address (Dirección IP de red externa)**, pegue la dirección de la salida de la implementación del Orquestador.
3. En el campo **External gateway IP address (Dirección IP de gateway externa)**, pegue la dirección de la salida de la implementación del Orquestador.
4. En el campo **DNS resolver IP address (Dirección IP de analizador de DNS)**, pegue la dirección de la salida de la implementación del Orquestador.

5. En el campo **DNS domain (Dominio DNS)**, introduzca su dominio DNS (por ejemplo, **cisco.com**).
6. (Versión de software 3.6 o posterior) Si activó IPv6 en la página L3, **IPv6** se selecciona automáticamente. Si selecciona IPv6, debe especificar las direcciones IPv6 reservadas para el uso de Cisco Secure Workload:

- Introduzca la **red IPv6 externa**.

Las primeras 3 direcciones IPv6 del campo de red IPv6 externa siempre están reservadas para los switches del clúster de Cisco Secure Workload y no deben utilizarse para ningún otro propósito.

- Si desea utilizar IPv6 solo para determinadas direcciones, introdúzcalas en el campo **IP IPv6 externas**.

Nota

- Para un clúster de 39 RU, asegúrese de que haya al menos 29 direcciones IPv6 disponibles en la red IPv6 externa o en la lista de IP IPv6 externas.
- Para un clúster de 8 RU, asegúrese de que haya al menos 20 direcciones IPv6 disponibles en la red IPv6 externa o en la lista de IP IPv6 externas.

7. Haga clic en **Next (Siguiente)**.

- Haga clic en **Service (Servicio)**.

1. En el campo **NTP Servers (Servidores NTP)**, introduzca la lista separada por espacios de nombres de servidores NTP o direcciones IP de la salida de la implementación del orquestador.
2. En el campo **SMTP Server (Servidor SMTP)**, introduzca el nombre o la dirección IP de un servidor SMTP que pueda utilizar Cisco Secure Workload para enviar mensajes de correo electrónico. Cisco Secure Workload debe poder acceder a este servidor.
3. En el campo **SMTP Port (Puerto de SMTP)**, introduzca el número de puerto del servidor SMTP. AWS restringe el uso de los puertos 25 y 465. Debe configurar su cuenta correctamente o utilizar el puerto 587.
4. (Opcional) En el campo **SMTP Username (Nombre de usuario SMTP)**, introduzca el nombre de usuario de autenticación SMTP.
5. (Opcional) En el campo **SMTP Password (Contraseña SMTP)**, introduzca la contraseña de autenticación SMTP.
6. (Opcional) En el campo **HTTP Proxy Server (Servidor proxy HTTP)**, introduzca el nombre o la dirección IP de un servidor proxy HTTP que pueda utilizar Cisco Secure Workload para acceder a servicios externos de Internet.
7. (Opcional) En el campo **HTTP Proxy Port (Puerto de proxy HTTP)**, introduzca el número de puerto del servidor proxy HTTP.
8. (Opcional) En el campo **HTTPs Proxy Server (Servidor proxy HTTPs)**, introduzca el nombre o la dirección IP de un servidor proxy HTTPs que pueda utilizar Cisco Secure Workload para acceder a servicios externos de Internet.
9. (Opcional) En el campo **HTTPs Proxy Port (Puerto de proxy HTTPs)**, introduzca el número de puerto del servidor proxy HTTPs.
10. (Opcional) En el campo **Syslog Server (Servidor syslog)**, introduzca el nombre o la dirección IP de un servidor syslog que pueda utilizar Cisco Secure Workload para enviar alertas.
11. (Opcional) En el campo **Syslog Port (Puerto de syslog)**, introduzca el número de puerto del servidor syslog.

12. (Opcional) En el campo **Syslog Severity (Gravedad de syslog)**, introduzca el nivel de gravedad de los mensajes de syslog. Entre los posibles valores se incluyen: informativo, aviso, advertencia, error, crítico, alerta y emergencia.
 13. Haga clic en **Next (Siguiente)**.
- Haga clic en **UI (IU)**.
 1. En el campo **UI VRRP VRID (VRID de VRRP de IU)**, introduzca **77** a menos que necesite un VRID único.
 2. En el campo **UI FQDN (FQDN de IU)**, introduzca el nombre de dominio completo con el que accede al clúster.
 3. Deje el campo **UI Airbrake Key (Clave de Airbrake de IU)** en blanco.
 4. Haga clic en **Next (Siguiente)**.

Tetration (Cisco Secure Workload) valida los ajustes de configuración y muestra el estado de la configuración.
 - Haga clic en **Advanced (Opciones avanzadas)**.
 1. En el campo **IP externas**, introduzca direcciones IPv4.
 2. Haga clic en **Continue (Continuar)**.

Paso 8 Si hay algún fallo, haga clic en **Back (Atrás)** y edite la configuración (consulte el paso 7).

Nota No puede modificar estos ajustes en la GUI de configuración después de salir de esta página. Sin embargo, puede modificar la configuración más adelante desde la página de la empresa en la GUI.

Paso 9 Si no se detectan fallos en su configuración y no necesita realizar ningún cambio, haga clic en **Continue (Continuar)**. Cisco Secure Workload se configura según los parámetros que haya especificado. Este proceso tarda de una a dos horas sin ninguna interacción por su parte.

Qué hacer a continuación

Si ha desplegado la versión 3.6 o posterior del software y ha activado la conectividad IPv6:

- Puede acceder al portal web de Cisco Secure Workload mediante IPv4 o IPv6.
- De forma predeterminada, los agentes de software se comunican con el clúster de Cisco Secure Workload mediante IPv4 incluso si el clúster está habilitado para ser compatible con IPv6. Si desea que los agentes compatibles utilicen IPv6 para este fin, debe configurar el campo **FQDN del VIP del sensor** en la página **Plataforma > Configuración del clúster** del portal web de Cisco Secure Workload. Para obtener instrucciones importantes, consulte la guía de usuario, disponible como ayuda en línea en el portal web de Cisco Secure Workload o en <https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html>.



CAPÍTULO 5

Cableado del dispositivo del clúster de C1-Secure Workload

- [Cableado del dispositivo del clúster de C1-Workload, en la página 21](#)
- [Cableado del dispositivo del clúster de C1-Workload-M, en la página 33](#)

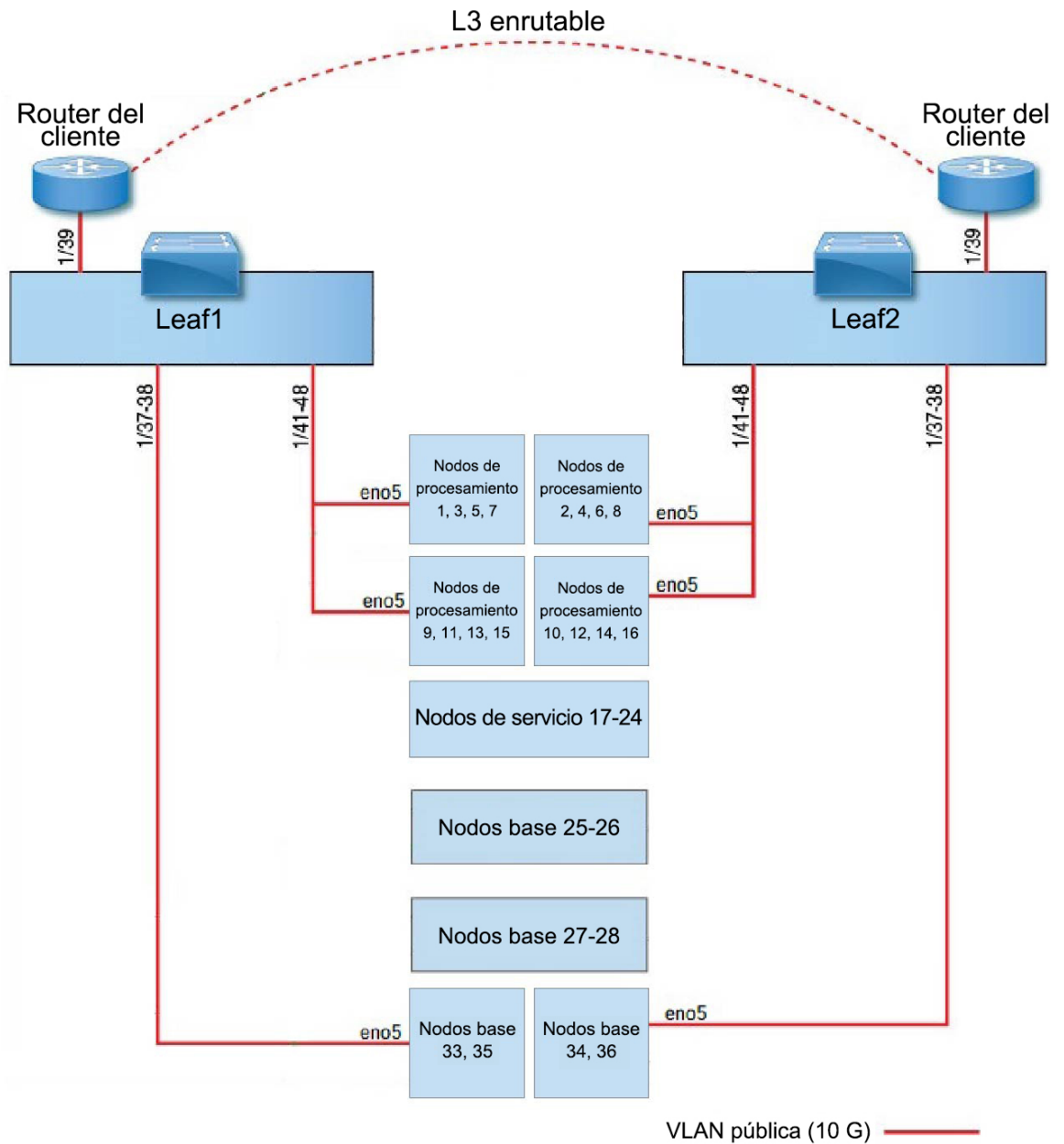
Cableado del dispositivo del clúster de C1-Workload

Preste atención a la siguiente información de configuración cuando cablee la tarjeta de interfaz virtual (VIC) M6 en el rack de 39 RU:

- Hay dos interfaces privadas para todos los nodos.
- El rack de 39 RU tiene una interfaz pública para 20 nodos.
- El hardware M6 tiene cuatro puertos por VIC.
- Los nombres de la interfaz de hardware físico (los servidores físicos del clúster conocidos como nodos base, de procesamiento y de servicio) comienzan con "eno" (Ethernet incluido).

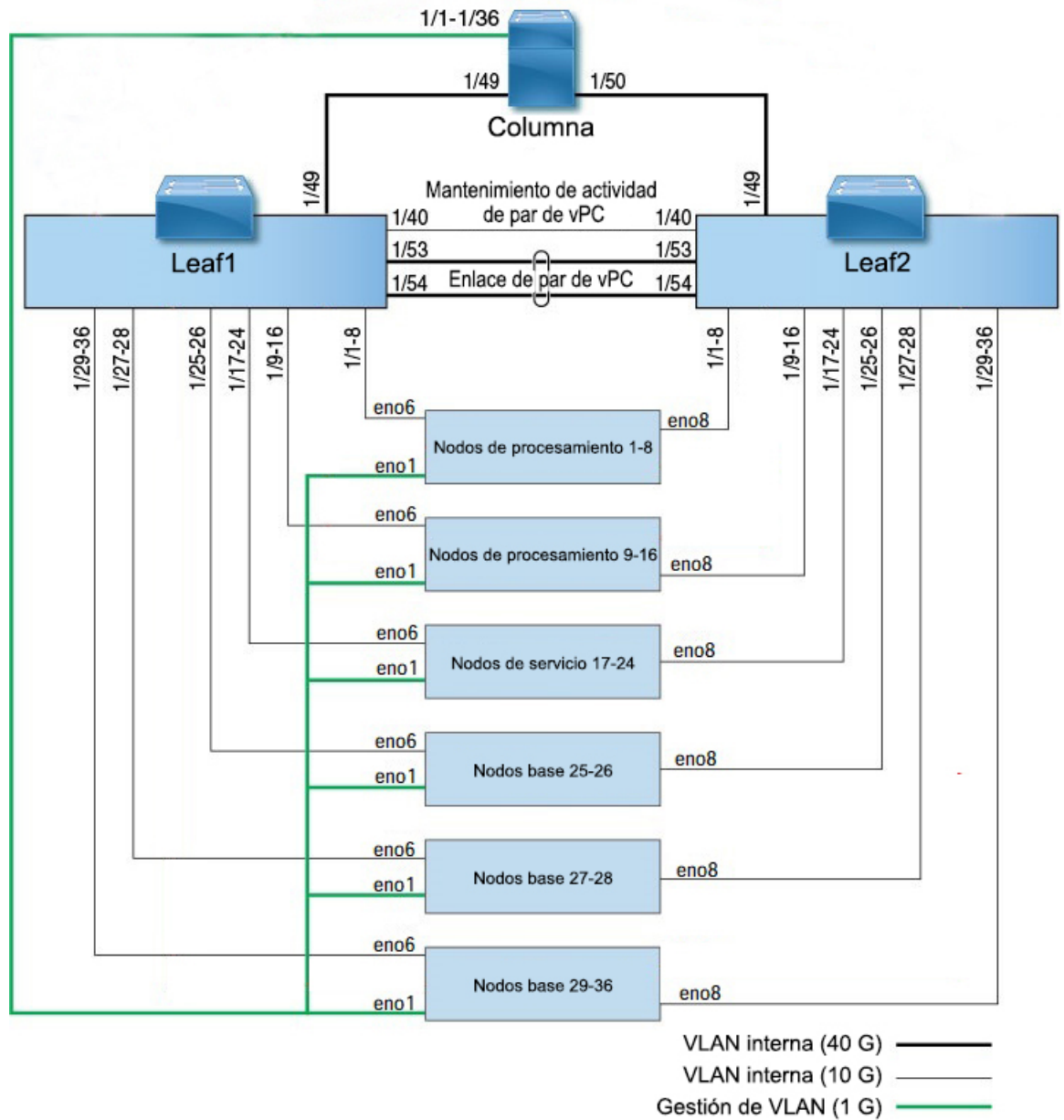
El siguiente diagrama muestra el cableado de los dispositivos para la configuración pública/externa del rack de C1-Workload. Para obtener una lista detallada de las conexiones, consulte las tablas que acompañan a los diagramas.

Figura 7: Cableado de los dispositivos del rack de C1-Workload (público/externo)



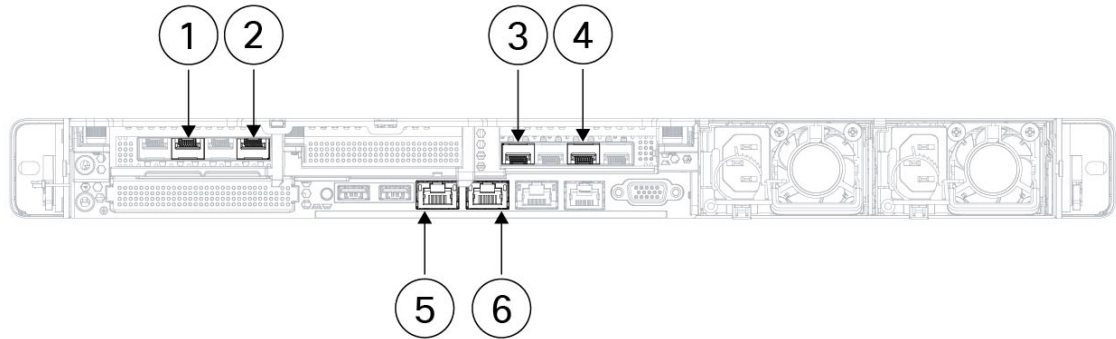
El siguiente diagrama muestra el cableado de los dispositivos para la configuración interna/de gestión del rack de C1-Workload. Para obtener una lista detallada de las conexiones, consulte las siguientes tablas.

Figura 8: Cableado de los dispositivos del rack de C1-Workload (interno/de gestión)



La siguiente figura muestra qué puertos del servidor M6 se corresponden con los puertos "eno" de las figuras anteriores:

Figura 9: Puertos del servidor M6



1	Hoja 1 u hoja 2 pública en función del servidor Puerto de interfaz del servidor = eno5 Designación CIMC = adaptador 1/puerto físico 2/vic-1-eth1	2	Hoja 1 privada Puerto de interfaz del servidor = eno6 Designación CIMC = adaptador 1/puerto físico 0/vic-1-eth0
3	Hoja 2 privada Puerto de interfaz del servidor = eno8 Designación CIMC = adaptador 3/puerto físico 0/vic-3-eth0	4	No se utiliza Puerto de interfaz del servidor = eno7 Designación CIMC = adaptador 3/puerto físico 2/vic-3-eth1
5	CIMC Puerto de interfaz del servidor = eno1 Designación CIMC = LOM 1	6	MGMT 2.2.2.2 Puerto de interfaz del servidor = eno2 Designación CIMC = LOM 2

Tabla 2: Conexiones del switch de columna (RU 42 en instalaciones de un rack y en instalaciones de dos racks)

Puerto de columna	Tipo de conexión	Conexión			
		Dispositivo	RU en rack individual	RU en rack doble	Puerto
1/1	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 1 (nodo de procesamiento)	RU 36	Rack1 RU 17	eno1
1/2	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 2 (nodo de procesamiento)	RU 35	Rack1 RU 16	eno1
1/3	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 3 (nodo de procesamiento)	RU 34	Rack1 RU 15	eno1
1/4	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 4 (nodo de procesamiento)	RU 33	Rack1 RU 14	eno1
1/5	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 5 (nodo de procesamiento)	RU 32	Rack1 RU 13	eno1

Puerto de columna	Tipo de conexión	Conexión			
		Dispositivo	RU en rack individual	RU en rack doble	Puerto
1/6	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 6 (nodo de procesamiento)	RU 31	Rack 1 RU 12	eno1
1/7	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 7 (nodo de procesamiento)	RU 30	Rack 1 RU 11	eno1
1/8	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 8 (nodo de procesamiento)	RU 29	Rack 1 RU 10	eno1
1/9	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 9 (nodo de procesamiento)	RU 28	Rack 1 RU 8	eno1
1/10	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 10 (nodo de procesamiento)	RU 27	Rack 1 RU 7	eno1
1/11	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 11 (nodo de procesamiento)	RU 26	Rack 1 RU 6	eno1
1/12	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 12 (nodo de procesamiento)	RU 25	Rack 1 RU 5	eno1
1/13	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 13 (nodo de procesamiento)	RU 24	Rack 1 RU 4	eno1
1/14	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 14 (nodo de procesamiento)	RU 23	Rack 1 RU 3	eno1
1/15	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 15 (nodo de procesamiento)	RU 22	Rack 1 RU 2	eno1
1/16	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 16 (nodo de procesamiento)	RU 21	Rack 1 RU 1	eno1
1/17	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 17 (nodo de servicio)	RU 20	Rack 2 RU 21	eno1
1/18	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 18 (nodo de servicio)	RU 19	Rack 2 RU 20	eno1
1/19	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 19 (nodo de servicio)	RU 18	Rack 2 RU 19	eno1
1/20	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 20 (nodo de servicio)	RU 17	Rack 2 RU 18	eno1
1/21	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 21 (nodo de servicio)	RU 16	Rack 2 RU 17	eno1

Puerto de columna	Tipo de conexión	Conexión			
		Dispositivo	RU en rack individual	RU en rack doble	Puerto
1/22	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 22 (nodo de servicio)	RU 15	Rack2 RU 16	eno1
1/23	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 23 (nodo de servicio)	RU 14	Rack2 RU 15	eno1
1/24	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 24 (nodo de servicio)	RU 13	Rack2 RU 14	eno1
1/25	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 25 (nodo base)	RU 12	Rack2 RU 12	eno1
1/26	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 26 (nodo base)	RU 11	Rack2 RU 11	eno1
1/27	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 27 (nodo base)	RU 10	Rack2 RU 10	eno1
1/28	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 28 (nodo base)	RU 9	Rack2 RU 9	eno1
1/29	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 29 (nodo base)	RU 8	Rack2 RU 8	eno1
1/30	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 30 (nodo base)	RU 7	Rack2 RU 7	eno1
1/31	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 31 (nodo base)	RU 6	Rack2 RU 6	eno1
1/32	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 32 (nodo base)	RU 5	Rack2 RU 5	eno1
1/33	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 33 (nodo base)	RU 4	Rack2 RU 4	eno1
1/34	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 34 (nodo base)	RU 3	Rack2 RU 3	eno1
1/35	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 35 (nodo base)	RU 2	Rack2 RU 2	eno1
1/36	VLAN DE CIMC (1 Gigabit)	Host del servidor UCS 36 (nodo base)	RU 1	Rack2 RU 1	eno1
1/49	VLAN interna (40 Gigabit)	Switch de hoja 1 (RU 41 en rack individual o RU 40 en el rack 1 del rack doble)	RU 40	Rack1 RU 40	1/49

Puerto de columna	Tipo de conexión	Conexión			
		Dispositivo	RU en rack individual	RU en rack doble	Puerto
1/50	VLAN interna (40 Gigabit)	Puerto 49 del switch de hoja 2 (RU 40 en rack individual o RU 40 del rack 2 en rack doble)	RU 41	Rack 2 RU 40	1/50

Tabla 3: Conexiones del switch de hoja 1 (RU 41 en instalaciones de un rack o RU 40 en el rack 1 de instalaciones de dos racks)

Puerto de hoja 1	Tipo de conexión	Conexión			
		Dispositivo	RU en rack individual	RU en rack doble	Puerto
1/1	VLAN interna (10 Gigabit)	Host del servidor UCS 1 (nodo de procesamiento)	RU 36	Rack 1 RU 17	eno6
1/2	VLAN interna (10 Gigabit)	Host del servidor UCS 2 (nodo de procesamiento)	RU 35	Rack 1 RU 16	eno6
1/3	VLAN interna (10 Gigabit)	Host del servidor UCS 3 (nodo de procesamiento)	RU 34	Rack 1 RU 15	eno6
1/4	VLAN interna (10 Gigabit)	Host del servidor UCS 4 (nodo de procesamiento)	RU 33	Rack 1 RU 14	eno6
1/5	VLAN interna (10 Gigabit)	Host del servidor UCS 5 (nodo de procesamiento)	RU 32	Rack 1 RU 13	eno6
1/6	VLAN interna (10 Gigabit)	Host del servidor UCS 6 (nodo de procesamiento)	RU 31	Rack 1 RU 12	eno6
1/7	VLAN interna (10 Gigabit)	Host del servidor UCS 7 (nodo de procesamiento)	RU 30	Rack 1 RU 11	eno6
1/8	VLAN interna (10 Gigabit)	Host del servidor UCS 8 (nodo de procesamiento)	RU 29	Rack 1 RU 10	eno6
1/9	VLAN interna (10 Gigabit)	Host del servidor UCS 9 (nodo de procesamiento)	RU 28	Rack 1 RU 8	eno6
1/10	VLAN interna (10 Gigabit)	Host del servidor UCS 10 (nodo de procesamiento)	RU 27	Rack 1 RU 7	eno6
1/11	VLAN interna (10 Gigabit)	Host del servidor UCS 11 (nodo de procesamiento)	RU 26	Rack 1 RU 6	eno6
1/12	VLAN interna (10 Gigabit)	Host del servidor UCS 12 (nodo de procesamiento)	RU 25	Rack 1 RU 5	eno6

Puerto de hoja 1	Tipo de conexión	Conexión			
		Dispositivo	RU en rack individual	RU en rack doble	Puerto
1/13	VLAN interna (10 Gigabit)	Host del servidor UCS 13 (nodo de procesamiento)	RU 24	Rack1 RU 4	eno6
1/14	VLAN interna (10 Gigabit)	Host del servidor UCS 14 (nodo de procesamiento)	RU 23	Rack1 RU 3	eno6
1/15	VLAN interna (10 Gigabit)	Host del servidor UCS 15 (nodo de procesamiento)	RU 22	Rack1 RU 2	eno6
1/16	VLAN interna (10 Gigabit)	Host del servidor UCS 16 (nodo de procesamiento)	RU 21	Rack1 RU 1	eno6
1/17	VLAN interna (10 Gigabit)	Host del servidor UCS 17 (nodo de servicio)	RU 20	Rack2 RU 21	eno6
1/18	VLAN interna (10 Gigabit)	Host del servidor UCS 18 (nodo de servicio)	RU 19	Rack2 RU 20	eno6
1/19	VLAN interna (10 Gigabit)	Host del servidor UCS 19 (nodo de servicio)	RU 18	Rack2 RU 19	eno6
1/20	VLAN interna (10 Gigabit)	Host del servidor UCS 20 (nodo de servicio)	RU 17	Rack2 RU 18	eno6
1/21	VLAN interna (10 Gigabit)	Host del servidor UCS 21 (nodo de servicio)	RU 16	Rack2 RU 17	eno6
1/22	VLAN interna (10 Gigabit)	Host del servidor UCS 22 (nodo de servicio)	RU 15	Rack2 RU 16	eno6
1/23	VLAN interna (10 Gigabit)	Host del servidor UCS 23 (nodo de servicio)	RU 14	Rack2 RU 15	eno6
1/24	VLAN interna (10 Gigabit)	Host del servidor UCS 24 (nodo de servicio)	RU 13	Rack2 RU 14	eno6
1/25	VLAN interna (10 Gigabit)	Host del servidor UCS 25 (nodo base)	RU 12	Rack2 RU 12	eno6
1/26	VLAN interna (10 Gigabit)	Host del servidor UCS 26 (nodo base)	RU 11	Rack2 RU 11	eno6
1/27	VLAN interna (10 Gigabit)	Host del servidor UCS 27 (nodo base)	RU 10	Rack2 RU 10	eno6
1/28	VLAN interna (10 Gigabit)	Host del servidor UCS 28 (nodo base)	RU 9	Rack2 RU 9	eno6

Puerto de hoja 1	Tipo de conexión	Conexión			
		Dispositivo	RU en rack individual	RU en rack doble	Puerto
1/29	VLAN interna (10 Gigabit)	Host del servidor UCS 29 (nodo base)	RU 8	Rack2 RU 8	eno6
1/30	VLAN interna (10 Gigabit)	Host del servidor UCS 30 (nodo base)	RU 7	Rack2 RU 7	eno6
1/31	VLAN interna (10 Gigabit)	Host del servidor UCS 31 (nodo base)	RU 6	Rack2 RU 6	eno6
1/32	VLAN interna (10 Gigabit)	Host del servidor UCS 32 (nodo base)	RU 5	Rack2 RU 5	eno6
1/33	VLAN interna (10 Gigabit)	Host del servidor UCS 33 (nodo base)	RU 4	Rack2 RU 4	eno6
1/34	VLAN interna (10 Gigabit)	Host del servidor UCS 34 (nodo base)	RU 3	Rack2 RU 3	eno6
1/35	VLAN interna (10 Gigabit)	Host del servidor UCS 35 (nodo base)	RU 2	Rack2 RU 2	eno6
1/36	VLAN interna (10 Gigabit)	Host del servidor UCS 36 (nodo base)	RU 1	Rack2 RU 1	eno6
1/37	VLAN pública (10 Gigabit)	Host del servidor UCS 33 (nodo base)	RU 3	Rack2 RU 3	eno5
1/38	VLAN pública (10 Gigabit)	Host del servidor UCS 35 (nodo base)	RU 1	Rack2 RU 1	eno5
1/39	VLAN interna (10 Gigabit)	Router del cliente 1	—	—	—
1/40	VLAN interna (10 Gigabit)	Hoja 1	RU 40	Rack 1 RU 40	1/40
1/41	VLAN pública (10 Gigabit)	Host del servidor UCS 1 (nodo de procesamiento)	RU 35	Rack 1 RU 16	eno5
1/42	VLAN pública (10 Gigabit)	Host del servidor UCS 3 (nodo de procesamiento)	RU 33	Rack 1 RU 14	eno5
1/43	VLAN pública (10 Gigabit)	Host del servidor UCS 5 (nodo de procesamiento)	RU 31	Rack 1 RU 12	eno5
1/44	VLAN pública (10 Gigabit)	Host del servidor UCS 7 (nodo de procesamiento)	RU 29	Rack 1 RU 10	eno5
1/45	VLAN pública (10 Gigabit)	Host del servidor UCS 9 (nodo de procesamiento)	RU 27	Rack 1 RU 8	eno5

Puerto de hoja 1	Tipo de conexión	Conexión			
		Dispositivo	RU en rack individual	RU en rack doble	Puerto
1/46	VLAN pública (10 Gigabit)	Host del servidor UCS 11 (nodo de procesamiento)	RU 25	Rack1 RU 6	eno5
1/47	VLAN pública (10 Gigabit)	Host del servidor UCS 13 (nodo de procesamiento)	RU 23	Rack1 RU 4	eno5
1/48	VLAN pública (10 Gigabit)	Host del servidor UCS 15 (nodo de procesamiento)	RU 21	Rack1 RU 2	eno5
1/49	VLAN interna (40 Gigabit)	Switch de columna	RU 42	Rack1 RU42	1/49
1/50	—	—	—	—	—
1/51	—	—	—	—	—
1/52	—	—	—	—	—
1/53	VLAN interna (40 Gigabit)	Switch de hoja 1	RU 40	Rack1 RU 40	1/53
1/54	VLAN interna (40 Gigabit)	Switch de hoja 1	RU 40	Rack1 RU 40	1/54

Tabla 4: Conexiones del switch de hoja 2 (RU 41 en instalaciones de un rack o RU 40 en el rack 2 de instalaciones de dos racks)

Puerto de hoja 2	Tipo de conexión	Conexión			
		Dispositivo	RU en rack individual	RU en rack doble	Puerto
1/1	VLAN interna (10 Gigabit)	Host del servidor UCS 1 (nodo de procesamiento)	RU 36	Rack1 RU 17	eno8
1/2	VLAN interna (10 Gigabit)	Host del servidor UCS 2 (nodo de procesamiento)	RU 35	Rack1 RU 16	eno8
1/3	VLAN interna (10 Gigabit)	Host del servidor UCS 3 (nodo de procesamiento)	RU 34	Rack1 RU 15	eno8
1/4	VLAN interna (10 Gigabit)	Host del servidor UCS 4 (nodo de procesamiento)	RU 33	Rack1 RU 14	eno8
1/5	VLAN interna (10 Gigabit)	Host del servidor UCS 5 (nodo de procesamiento)	RU 32	Rack1 RU 13	eno8
1/6	VLAN interna (10 Gigabit)	Host del servidor UCS 6 (nodo de procesamiento)	RU 31	Rack1 RU 12	eno8

Puerto de hoja 2	Tipo de conexión	Conexión			
		Dispositivo	RU en rack individual	RU en rack doble	Puerto
1/7	VLAN interna (10 Gigabit)	Host del servidor UCS 7 (nodo de procesamiento7)	RU 30	Rack 1 RU 11	eno8
1/8	VLAN interna (10 Gigabit)	Host del servidor UCS 8 (nodo de procesamiento)	RU 29	Rack 1 RU 10	eno8
1/9	VLAN interna (10 Gigabit)	Host del servidor UCS 9 (nodo de procesamiento)	RU 28	Rack 1 RU 8	eno8
1/10	VLAN interna (10 Gigabit)	Host del servidor UCS 10 (nodo de procesamiento)	RU 27	Rack 1 RU 7	eno8
1/11	VLAN interna (10 Gigabit)	Host del servidor UCS 11 (nodo de procesamiento)	RU 26	Rack 1 RU 6	eno8
1/12	VLAN interna (10 Gigabit)	Host del servidor UCS 12 (nodo de procesamiento)	RU 25	Rack 1 RU 5	eno8
1/13	VLAN interna (10 Gigabit)	Host del servidor UCS 13 (nodo de procesamiento)	RU 24	Rack 1 RU 4	eno8
1/14	VLAN interna (10 Gigabit)	Host del servidor UCS 14 (nodo de procesamiento)	RU 23	Rack 1 RU 3	eno8
1/15	VLAN interna (10 Gigabit)	Host del servidor UCS 15 (nodo de procesamiento)	RU 22	Rack 1 RU 2	eno8
1/16	VLAN interna (10 Gigabit)	Host del servidor UCS 16 (nodo de procesamiento)	RU 21	Rack 1 RU 1	eno8
1/17	VLAN interna (10 Gigabit)	Host del servidor UCS 17 (nodo de servicio)	RU 20	Rack 2 RU 21	eno8
1/18	VLAN interna (10 Gigabit)	Host del servidor UCS 18 (nodo de servicio)	RU 19	Rack 2 RU 20	eno8
1/19	VLAN interna (10 Gigabit)	Host del servidor UCS 19 (nodo de servicio)	RU 18	Rack 2 RU 19	eno8
1/20	VLAN interna (10 Gigabit)	Host del servidor UCS 20 (nodo de servicio)	RU 17	Rack 2 RU 18	eno8
1/21	VLAN interna (10 Gigabit)	Host del servidor UCS 21 (nodo de servicio)	RU 16	Rack 2 RU 17	eno8
1/22	VLAN interna (10 Gigabit)	Host del servidor UCS 22 (nodo de servicio)	RU 15	Rack 2 RU 16	eno8

Puerto de hoja 2	Tipo de conexión	Conexión			
		Dispositivo	RU en rack individual	RU en rack doble	Puerto
1/23	VLAN interna (10 Gigabit)	Host del servidor UCS 23 (nodo de servicio)	RU 14	Rack2 RU 15	eno8
1/24	VLAN interna (10 Gigabit)	Host del servidor UCS 24 (nodo de servicio)	RU 13	Rack2 RU 14	eno8
1/25	VLAN interna (10 Gigabit)	Host del servidor UCS 25 (nodo base)	RU 12	Rack2 RU 12	eno8
1/26	VLAN interna (10 Gigabit)	Host del servidor UCS 26 (nodo base)	RU 11	Rack2 RU 11	eno8
1/27	VLAN interna (10 Gigabit)	Host del servidor UCS 27 (nodo base)	RU 10	Rack2 RU 10	eno8
1/28	VLAN interna (10 Gigabit)	Host del servidor UCS 28 (nodo base)	RU 9	Rack2 RU 9	eno8
1/29	VLAN interna (10 Gigabit)	Host del servidor UCS 29 (nodo base)	RU 8	Rack2 RU 8	eno8
1/30	VLAN interna (10 Gigabit)	Host del servidor UCS 30 (nodo base)	RU 7	Rack2 RU 7	eno8
1/31	VLAN interna (10 Gigabit)	Host del servidor UCS 31 (nodo base)	RU 6	Rack2 RU 6	eno8
1/32	VLAN interna (10 Gigabit)	Host del servidor UCS 32 (nodo base)	RU 5	Rack2 RU 5	eno8
1/33	VLAN interna (10 Gigabit)	Host del servidor UCS 33 (nodo base)	RU 4	Rack2 RU 4	eno8
1/34	VLAN interna (10 Gigabit)	Host del servidor UCS 34 (nodo base)	RU 3	Rack2 RU 3	eno8
1/35	VLAN interna (10 Gigabit)	Host del servidor UCS 35 (nodo base)	RU 2	Rack2 RU 2	eno8
1/36	VLAN interna (10 Gigabit)	Host del servidor UCS 36 (nodo base)	RU 1	Rack2 RU 1	eno8
1/37	VLAN pública (10 Gigabit)	Host del servidor UCS 34 (nodo base)	RU 4	Rack2 RU 8	eno5
1/38	VLAN pública (10 Gigabit)	Host del servidor UCS 36 (nodo base)	RU 2	Rack2 RU 6	eno5
1/39	VLAN interna (10 Gigabit)	Router del cliente 1	—	—	—

Puerto de hoja 2	Tipo de conexión	Conexión			
		Dispositivo	RU en rack individual	RU en rack doble	Puerto
1/40	VLAN interna (10 Gigabit)	Switch de hoja 2	RU 41	Rack2 RU 40	1/40
1/41	VLAN pública (10 Gigabit)	Host del servidor UCS 2 (nodo de procesamiento)	RU 36	Rack 1 RU 17	eno5
1/42	VLAN pública (10 Gigabit)	Host del servidor UCS 4 (nodo de procesamiento)	RU 34	Rack 1 RU 15	eno5
1/43	VLAN pública (10 Gigabit)	Host del servidor UCS 6 (nodo de procesamiento)	RU 32	Rack 1 RU 13	eno5
1/44	VLAN pública (10 Gigabit)	Host del servidor UCS 8 (nodo de procesamiento)	RU 30	Rack 1 RU 11	eno5
1/45	VLAN pública (10 Gigabit)	Host del servidor UCS 10 (nodo de procesamiento)	RU 28	Rack 1 RU 9	eno5
1/46	VLAN pública (10 Gigabit)	Host del servidor UCS 12 (nodo de procesamiento)	RU 26	Rack 1 RU 7	eno5
1/47	VLAN pública (10 Gigabit)	Host del servidor UCS 14 (nodo de procesamiento)	RU 24	Rack 1 RU 5	eno5
1/48	VLAN pública (10 Gigabit)	Host del servidor UCS 16 (nodo de procesamiento)	RU 22	Rack 1 RU 3	eno5
1/49	VLAN interna (40 Gigabit)	Switch de columna	RU 42	Rack 1 RU 42	—
1/50	—	—	—	—	1/50
1/51	—	—	—	—	—
1/52	—	—	—	—	—
1/53	VLAN interna (40 Gigabit)	Switch de hoja 1	RU 40	Rack 1 RU 40	1/49
1/54	VLAN interna (40 Gigabit)	Switch de hoja 2	RU 41	Rack2 RU 40	1/50

Cableado del dispositivo del clúster de C1-Workload-M

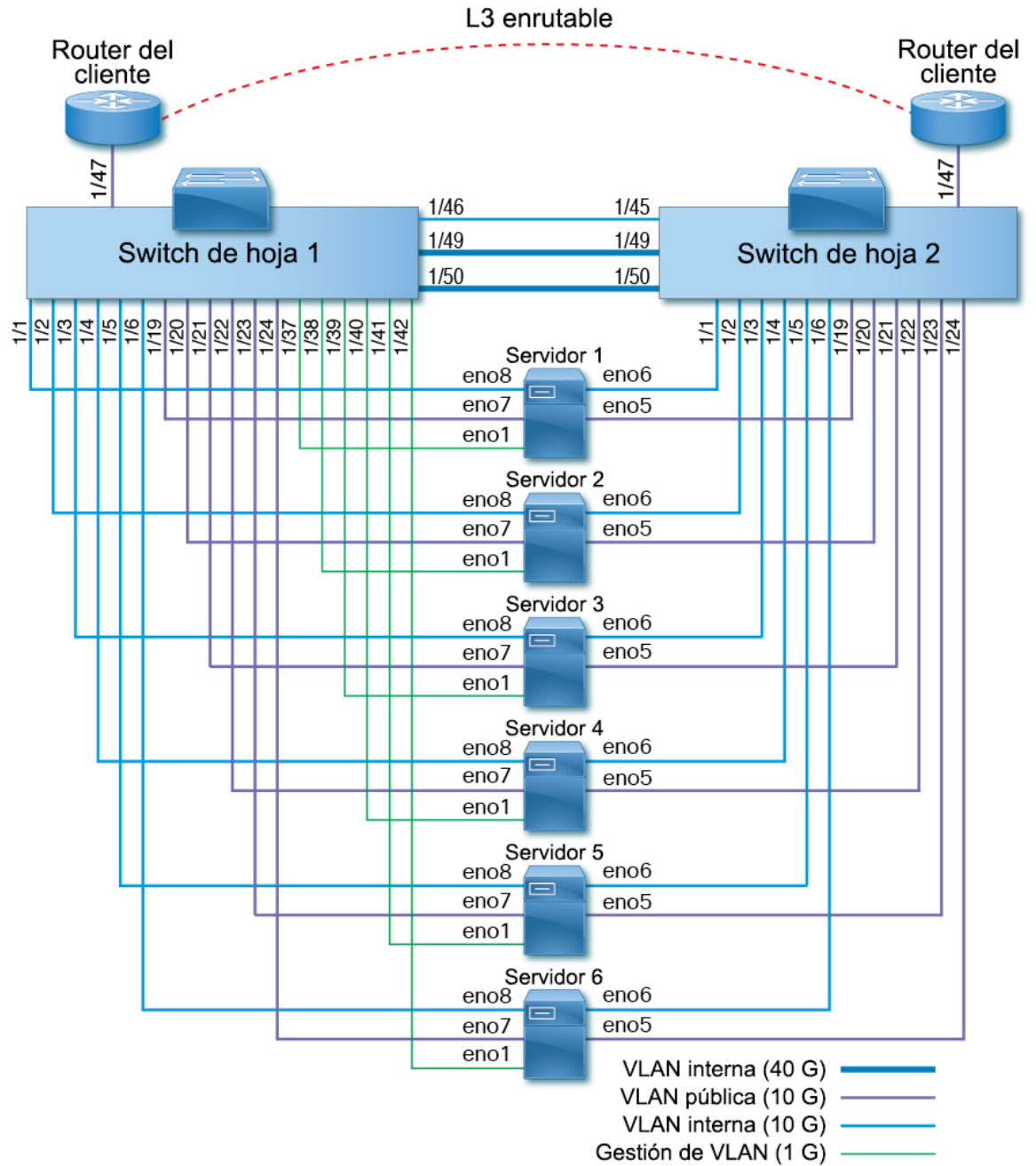
Para cablear la VIC M6 en el rack de 8 RU, preste atención a la siguiente información de configuración:

- Hay dos interfaces privadas para todos los nodos.

- El rack de 8 RU tiene dos interfaces públicas para los seis nodos.
- El hardware M6 tiene cuatro puertos por VIC.
- Los nombres de la interfaz de hardware físico (el servidor físico del clúster conocido como nodo universal) comienzan con "eno" (Ethernet incluido).

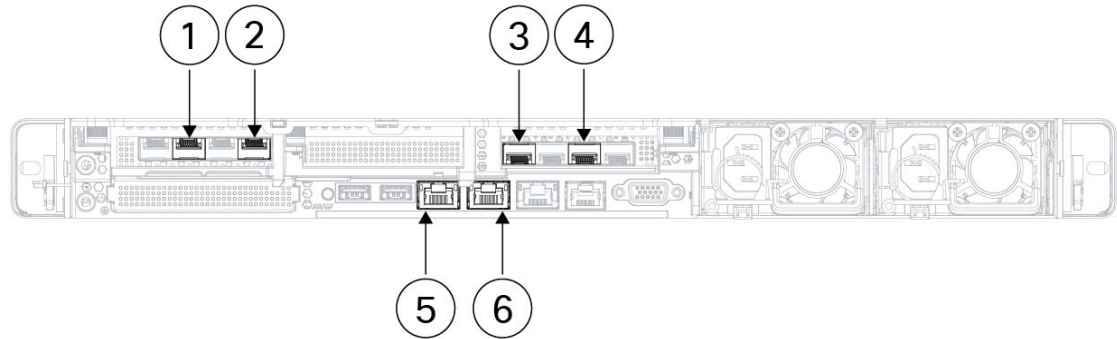
El siguiente diagrama muestra el cableado de los dispositivos para la configuración interna/de gestión/pública/externa del rack de 8 RU del clúster de C1-Workload-M. Para obtener una lista detallada de las conexiones, consulte las tablas que acompañan al diagrama.

Figura 10: Cableado de los dispositivos del rack del clúster de C1-Workload-M (interno/de gestión/público/externo)



La siguiente figura muestra qué puertos del servidor se corresponden con los puertos "eno" del diagrama anterior:

Figura 11: Puertos del servidor M6



1	Hoja 2 pública Puerto de interfaz del servidor = eno5 Designación CIMC = adaptador 1/puerto físico 2/vic-1-eth1	2	Hoja 2 privada Puerto de interfaz del servidor = eno6 Designación CIMC = adaptador 1/puerto físico 0/vic-1-eth0
3	Hoja 1 privada Puerto de interfaz del servidor = eno8 Designación CIMC = adaptador 3/puerto físico 0/vic-3-eth0	4	Hoja 1 pública Puerto de interfaz del servidor = eno7 Designación CIMC = adaptador 3/puerto físico 2/vic3-eth1
5	CIMC Puerto de interfaz del servidor = eno1 Designación CIMC = LOM 1	6	MGMT 2.2.2.2 Puerto de interfaz del servidor = eno2 Designación CIMC = LOM 2

Tabla 5: Conexiones del switch de hoja 1 (RU 12)

Puerto de hoja	Tipo de conexión	Conexión		
		Dispositivo	RU en rack individual	Puerto
1/1	VLAN interna (10 Gigabit)	Host del servidor UCS 1 (nodo universal)	RU 9	eno8
1/2	VLAN interna (10 Gigabit)	Host del servidor UCS 2 (nodo universal)	RU 8	eno8
1/3	VLAN interna (10 Gigabit)	Host del servidor UCS 3 (nodo universal)	RU 6	eno8
1/4	VLAN interna (10 Gigabit)	Host del servidor UCS 4 (nodo universal)	RU 5	eno8
1/5	VLAN interna (10 Gigabit)	Host del servidor UCS 5 (nodo universal)	RU 3	eno8
1/6	VLAN interna (10 Gigabit)	Host del servidor UCS 6 (nodo universal)	RU 2	eno8
1/7	—	—	—	—
1/8	—	—	—	—

Puerto de hoja	Tipo de conexión	Conexión		
		Dispositivo	RU en rack individual	Puerto individual
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)	Host del servidor UCS 1 (nodo universal)	RU 9	eno7
1/20	VLAN externa (10 Gigabit)	Host del servidor UCS 2 (nodo universal)	RU 8	eno7
1/21	VLAN externa (10 Gigabit)	Host del servidor UCS 3 (nodo universal)	RU 6	eno7
1/22	VLAN externa (10 Gigabit)	Host del servidor UCS 4 (nodo universal)	RU 5	eno7
1/23	VLAN externa (10 Gigabit)	Host del servidor UCS 5 (nodo universal)	RU 3	eno7
1/24	VLAN externa (10 Gigabit)	Host del servidor UCS 6 (nodo universal)	RU 2	eno7
1/25	—	—	—	—
1/26	—	—	—	—
1/27	—	—	—	—
1/28	—	—	—	—
1/29	—	—	—	—
1/30	—	—	—	—
1/31	—	—	—	—
1/32	—	—	—	—
1/33	—	—	—	—

Puerto de hoja	Tipo de conexión	Conexión		
		Dispositivo	RU en rack individual	Puerto individual
1/34	—	—	—	—
1/35	—	—	—	—
1/36	—	—	—	—
1/37	VLAN de gestión (1 Gigabit)	Host del servidor UCS 1 (nodo universal)	RU 9	eno1
1/38	VLAN de gestión (1 Gigabit)	Host del servidor UCS 2 (nodo universal)	RU 8	eno1
1/39	VLAN de gestión (1 Gigabit)	Host del servidor UCS 3 (nodo universal)	RU 6	eno1
1/40	VLAN de gestión (1 Gigabit)	Host del servidor UCS 4 (nodo universal)	RU 5	eno1
1/41	VLAN de gestión (1 Gigabit)	Host del servidor UCS 5 (nodo universal)	RU 3	eno1
1/42	VLAN de gestión (1 Gigabit)	Host del servidor UCS 6 (nodo universal)	RU 2	eno1
1/43	—	—	—	—
1/44	—	—	—	—
1/45	—	—	—	—
1/46	VLAN interna (10 Gigabit)	Switch de hoja 2	RU 11	1/45
1/47	VLAN externa (10 Gigabit)	Router del cliente	—	—
1/48	—	—	—	—
1/49	VLAN interna (40 Gigabit)	Switch de hoja 2	RU 11	1/49
1/50	VLAN interna (40 Gigabit)	Switch de hoja 2	RU 11	1/50
1/51	—	—	—	—
1/52	—	—	—	—
1/53	—	—	—	—
1/54	—	—	—	—

Tabla 6: Conexiones del switch de hoja 2 (RU 11)

Puerto de hoja	Tipo de conexión	Conexión		
		Dispositivo	RU en rack individual	Puerto individual
1/1	VLAN interna (10 Gigabit)	Host del servidor UCS 1 (nodo universal)	9 RU	eno6

Puerto de hoja	Tipo de conexión	Conexión		
		Dispositivo	RU en rack individual	Puerto individual
1/2	VLAN interna (10 Gigabit)	Host del servidor UCS 2 (nodo universal)	8 RU	eno6
1/3	VLAN interna (10 Gigabit)	Host del servidor UCS 3 (nodo universal)	6 RU	eno6
1/4	VLAN interna (10 Gigabit)	Host del servidor UCS 4 (nodo universal)	5 RU	eno6
1/5	VLAN interna (10 Gigabit)	Host del servidor UCS 5 (nodo universal)	3 RU	eno6
1/6	VLAN interna (10 Gigabit)	Host del servidor UCS 6 (nodo 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)	Host del servidor UCS 1 (nodo universal)	9 RU	eno5
1/20	VLAN externa (10 Gigabit)	Host del servidor UCS 2 (nodo universal)	8 RU	eno5
1/21	VLAN externa (10 Gb)	Host del servidor UCS 3 (nodo universal)	6 RU	eno5
1/22	VLAN externa (10 Gigabit)	Host del servidor UCS 4 (nodo universal)	5 RU	eno5
1/23	VLAN externa (10 Gigabit)	Host del servidor UCS 5 (nodo universal)	3 RU	eno5
1/24	VLAN externa (10 Gigabit)	Host del servidor UCS 6 (nodo universal)	2 RU	eno5
1/25	—	—	—	—
1/26	—	—	—	—
1/27	—	—	—	—

Puerto de hoja	Tipo de conexión	Conexión		
		Dispositivo	RU en rack individual	Puerto individual
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 de hoja 1	12 RU	1/46
1/46	—	—	—	—
1/47	VLAN externa (10 Gigabit)	Router del cliente	—	—
1/48	—	—	—	—
1/49	VLAN interna (40 Gigabit)	Switch de hoja 1	12 RU	1/49
1/50	VLAN interna (40 Gigabit)	Switch de hoja 1	12 RU	1/50
1/51	—	—	—	—
1/52	—	—	—	—
1/53	—	—	—	—

Puerto de hoja	Tipo de conexión	Conexión		
		Dispositivo	RU en rack individual	Puerto individual
1/54	—	—	—	—



CAPÍTULO 6

Especificaciones del sistema

- [Especificaciones ambientales, en la página 43](#)
- [Cables de alimentación, en la página 43](#)

Especificaciones ambientales

En la siguiente tabla, se enumeran las especificaciones ambientales necesarias para la instalación del clúster de Cisco Secure Workload.

Tabla 7: Especificaciones ambientales

Entorno		Especificación
Temperatura	Datos operativos	5 a 35 °C (41 a 95 °F) con una disminución de la temperatura máxima de 1 °C por cada 305 m (1000 pies) sobre el nivel del mar
	Almacenamiento	De -40 a 65 °C (de -40 a 149 °F)
Humedad	Datos operativos	Humedad relativa de un 10 a un 80 % con un grado de humedad del 10 % por hora
	Almacenamiento	Humedad relativa de un 5 a un 93 %
Altitud	Datos operativos	De 0 a 3050 m (de 0 a 10 000 pies)
	Almacenamiento	De 0 a 12 200 m (de 0 a 40 000 pies)

Cables de alimentación

Las siguientes tablas indican los cables de alimentación que se incluyen con el clúster de Cisco Secure Workload M6.

Tabla 8: Clúster de 39 RU, configuración de un rack

Número de componente	Descripción	Cantidad
TA-RACK-UCS2-INT	Rack dinámico Cisco R42612 con paneles laterales	1

Número de componente	Descripción	Cantidad
TA-ETH-RJ45-SINGLE	Kit de cables RJ-45 para la configuración de un solo rack de 39 RU	1
TA-SFP-H10GB-CU2M	Cable 10GBASE-CU SFP+ de 2 m	16
TA-SFP-H10GB-CU1-5	Cable 10GBASE-CU SFP+ de 1,5 m	32
TA-QSFP-H40G-CU1M	Cable de cobre pasivo 40GBASE-CR4 de 1 m	4
TA-SFP-H10GB-CU1M	Cable 10GBASE-CU SFP+ de 1 m	25
TA-SFP-H10GB-CU2-5	Cable 10GBASE-CU SFP+ de 2,5 m	20

Tabla 9: Clúster de 39 RU, configuración de dos racks

Número de componente	Descripción	Cantidad
TA-RACK-UCS2-INT	Rack dinámico Cisco R42612, con paneles laterales	2
TA-ETH-RJ45-DUAL	Kit de cables RJ-45 para la configuración de un solo rack de 39 RU	1
TA-SFP-H10GB-CU2M	Cable 10GBASE-CU SFP+ de 2 m	15
TA-SFP-H10GB-CU1-5	Cable 10GBASE-CU SFP+ de 1,5 m	19
TA-QSFP-H40G-CU1M	Cable de cobre pasivo 40GBASE-CR4 de 1 m	1
TA-QSFP-H40G-CU5M	Cable de cobre pasivo 40GBASE-CR4 de 5 m	3
TA-SFP-H10GB-CU2-5	Cable 10GBASE-CU SFP+ de 2,5 m	12
TA-SFP-H10GB-CU5M	Cable 10GBASE-CU SFP+ de 5 m	47

Tabla 10: Clúster de 8 RU

Número de componente	Descripción	Cantidad
TA-RACK-UCS2-INT	Rack dinámico Cisco R42612, con paneles laterales	1
CAB-ETH-S-RJ45	Cable directo amarillo RJ-45 de 2 m para Ethernet	6
TA-SFP-H10GB-CU1M	Cable 10GBASE-CU SFP+ de 1 m	13
TA-SFP-H10GB-CU1-5	Cable 10GBASE-CU SFP+ de 1,5 m	12
TA-QSFP-H40G-CU1M	Cable de cobre pasivo 40GBASE-CR4 de 1 m	2
GLC-TE	Módulo transmisor SFP 1000BASE-T para cable de cobre de categoría 5	6