



## **Guide de déploiement du cluster Cisco Secure Workload M6**

**Première publication** : 25 octobre 2023

### **Americas Headquarters**

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

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

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

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

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

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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

© 2023 Cisco Systems, Inc. Tous droits réservés.



## TABLE DES MATIÈRES

---

<b>CHAPITRE 1</b>	<b>Vue d'ensemble</b>	<b>1</b>
	Vue d'ensemble	1
	Façade du serveur Cisco UCS C220 M6	5
	Panneau arrière du serveur Cisco UCS C220 M6	6

---

<b>CHAPITRE 2</b>	<b>Préparer le site</b>	<b>9</b>
	Exigences relatives aux températures	9
	Exigences relatives à l'humidité	9
	Exigences en matière d'altitude	10
	Exigences relatives à la poussière et aux particules	10
	Minimiser les perturbations électromagnétiques et radioélectriques	10
	Exigences relatives aux chocs et aux vibrations	11
	Exigences relatives à la mise à la terre	11
	Alimentation requise	11
	Exigences relatives à la circulation de l'air	12
	Espace libre nécessaire	12

---

<b>CHAPITRE 3</b>	<b>Mettre à la terre et raccorder les périphériques du cluster</b>	<b>13</b>
	Mettre à la terre les équipements du cluster Cisco Secure Workload	13
	Alimenter les équipements du cluster Cisco Secure Workload	13
	Connecter le cluster Cisco Secure Workload à vos routeurs	14

---

<b>CHAPITRE 4</b>	<b>Configurer l'interface utilisateur</b>	<b>15</b>
	(Facultatif) Exigences et restrictions pour le mode double pile (prise en charge d'IPv6)	15
	Configurer l'interface utilisateur	16

---

<b>CHAPITRE 5</b>	<b>Câblage des équipements du cluster C1-Cisco Secure Workload</b>	<b>23</b>
	Câblage des équipements du cluster C1-Workload	23
	Câblage des équipements du cluster C1-Workload-M	36

---

<b>CHAPITRE 6</b>	<b>Spécifications système</b>	<b>45</b>
	Caractéristiques environnementales	45
	Cordons d'alimentation	45



# CHAPITRE 1

## Vue d'ensemble

---

- [Vue d'ensemble, à la page 1](#)
- [Façade du serveur Cisco UCS C220 M6, à la page 5](#)
- [Panneau arrière du serveur Cisco UCS C220 M6, à la page 6](#)

## Vue d'ensemble

Vous pouvez déployer le cluster Cisco Secure Workload M6 de l'une des manières suivantes :

- Plateforme grand format à 39 unités de rack (RU) (rack unique C1-Workload) pour data centers avec plus de 5 000 serveurs



---

**Remarque**

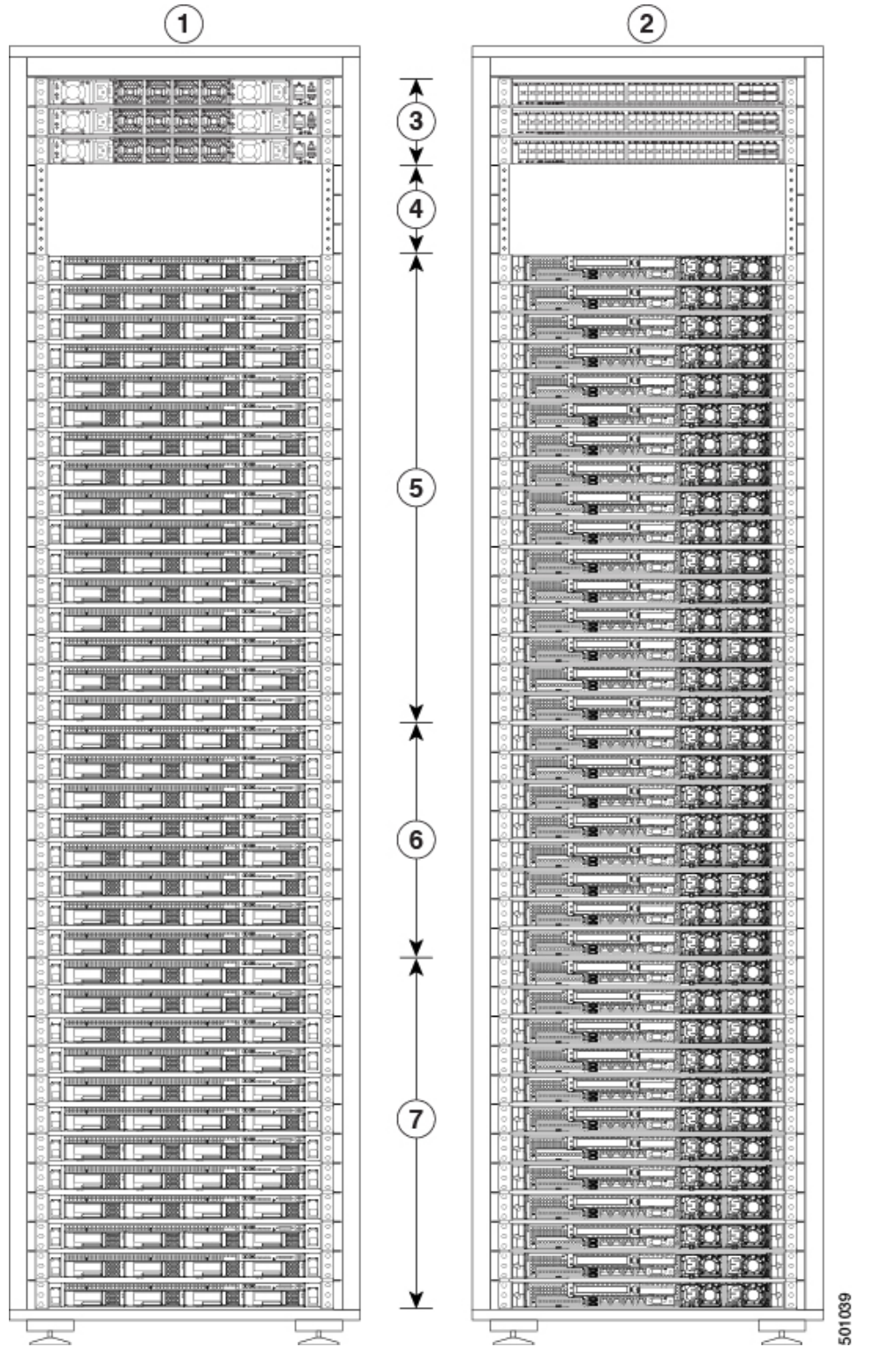
Vous pouvez déployer la plateforme grand format dans un ou deux racks selon vos besoins. Reportez-vous aux illustrations ci-dessous pour obtenir un exemple des modèles à un et deux racks C1-Workload.

---

- Plateforme petit format à 8 RU (C1-Workload-M) pour data centers avec moins de 5 000 serveurs. Reportez-vous à la figure C1-Workload-M pour obtenir un exemple.

La figure suivante illustre l'avant et l'arrière du rack unique C1-Workload.

Illustration 1 : Rack unique C1-Workload : faces avant et arrière



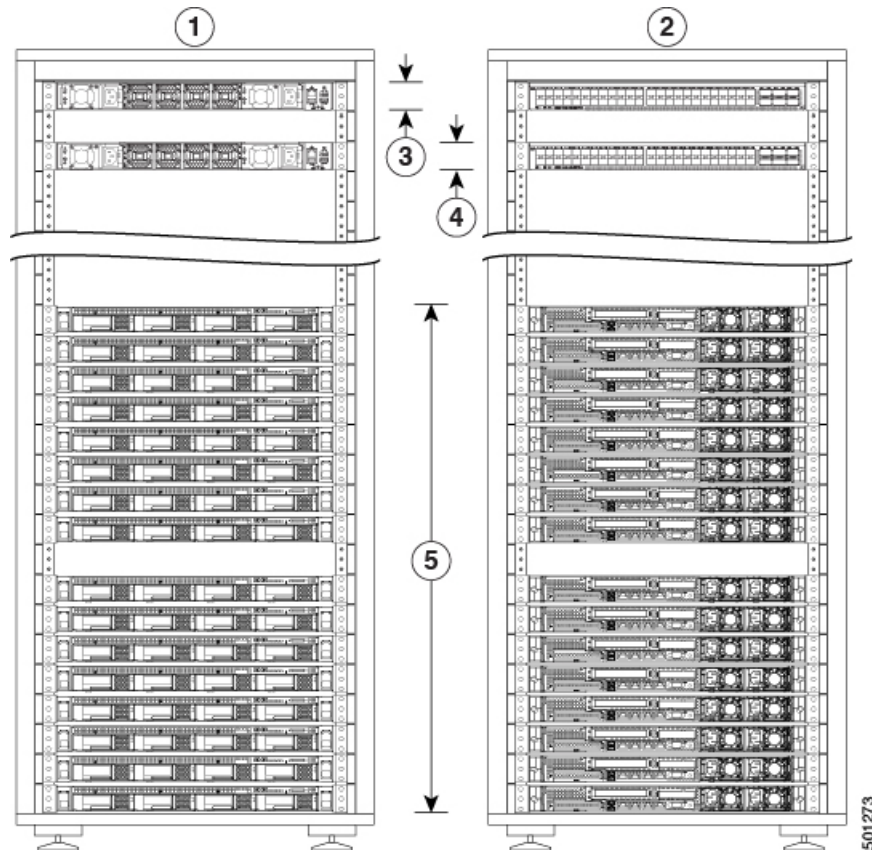
501 039

1 Face avant (vue de l'allée froide)	2 Face arrière (vue de l'allée chaude)
--------------------------------------	--

3	Un commutateur Spine (RU 42) et deux commutateurs Leaf : Leaf 2 (RU 40) et Leaf 1 (RU 41)	4	Racks ouverts (RU 37 à 39)
5	16 serveurs de calcul (RU 21 à 36)	6	8 serveurs de service (RU 13 à 20)
7	12 serveurs de base (RU 1 à 12)		—

La figure suivante illustre l'avant et l'arrière du rack 1 du double rack C1-Workload.

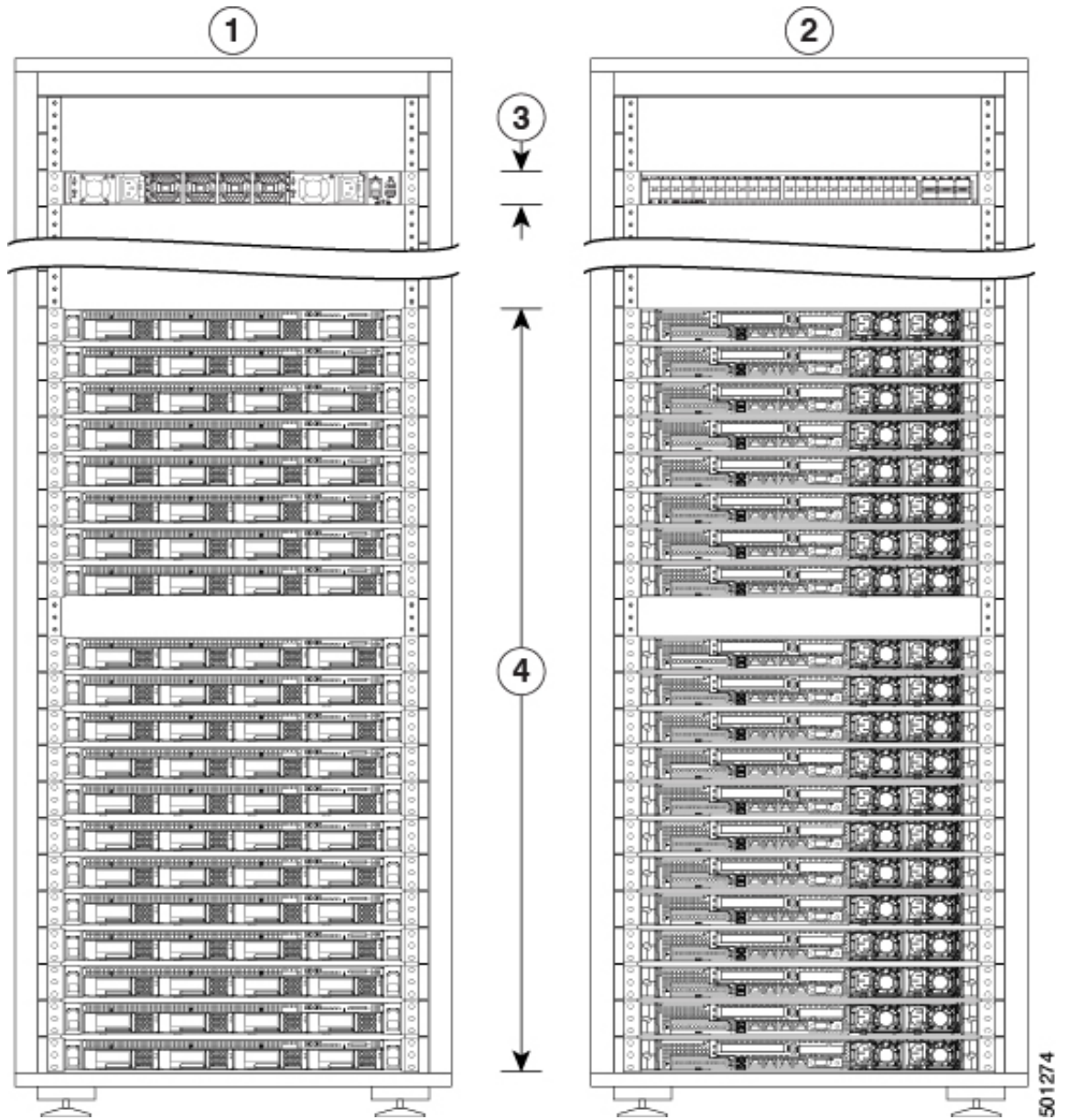
**Illustration 2 : Double rack C1-Workload : faces avant et arrière du rack 1**



1	Face avant (vue de l'allée froide)	2	Face arrière (vue de l'allée chaude)
3	Un commutateur Spine (RU 42)	4	Commutateur Leaf 1 (RU 40)
5	16 serveurs de calcul (RU 1 à 4 et 6 à 9)	6	—

La figure suivante illustre l'avant et l'arrière du rack 2 du double rack C1-Workload.

Illustration 3 : Double rack C1-Workload : faces avant et arrière du rack 2

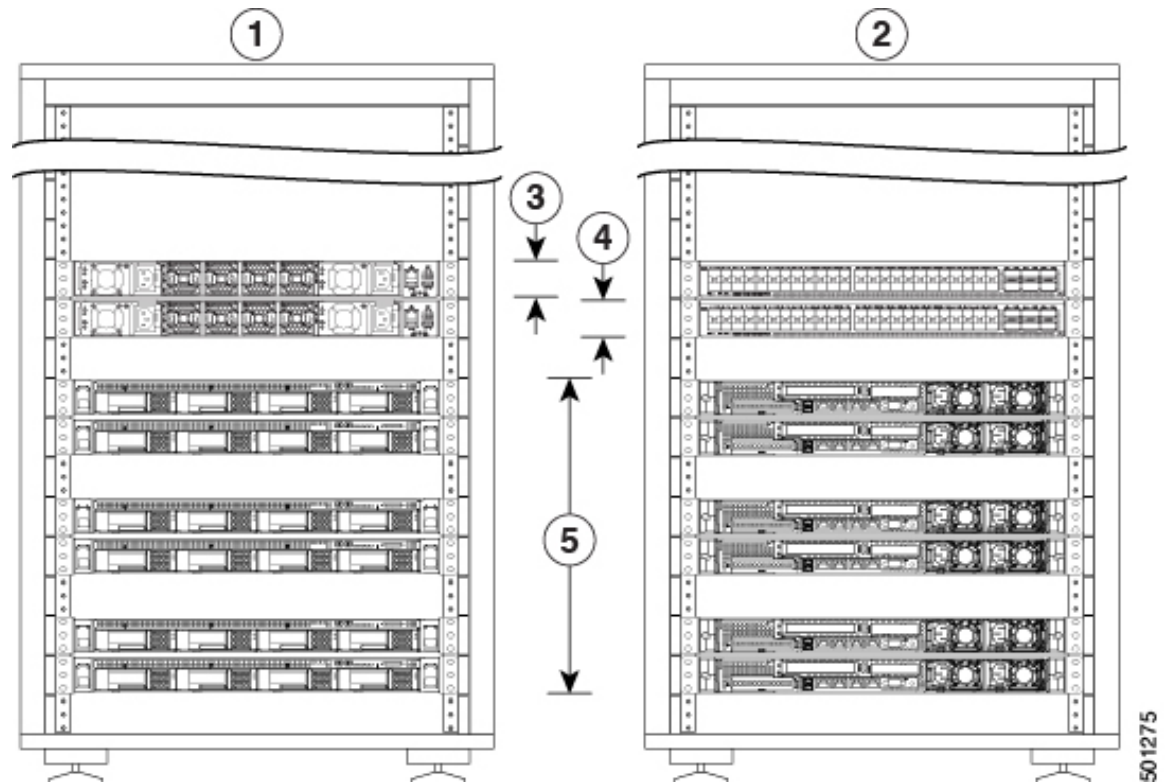


1	Face avant (vue de l'allée froide)	2	Face arrière (vue de l'allée chaude)
3	Commutateur Leaf 2 (RU 40)	4	8 serveurs de service (RU 14 à 21) et 12 serveurs de base (RU 1 à 12)

La figure suivante illustre l'avant et l'arrière du rack C1-Workload-M.



Illustration 4 : Rack C1-Workload-M : faces avant et arrière



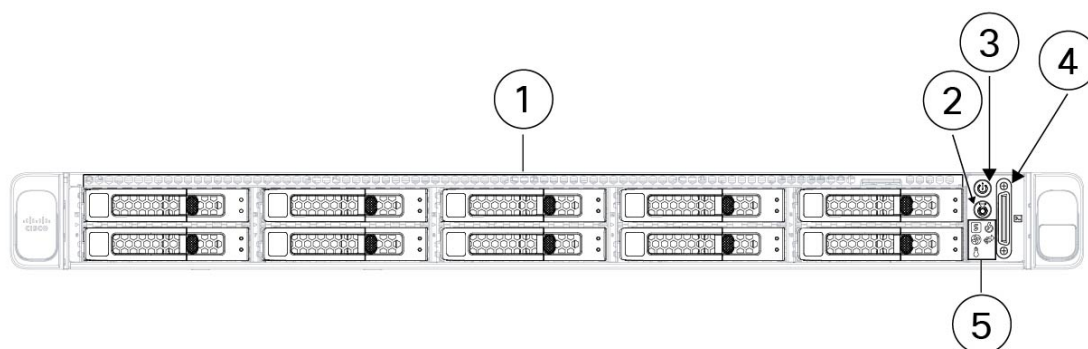
1	Face avant (vue de l'allée froide)	2	Face arrière (vue de l'allée chaude)
3	Commutateur Leaf 1 (RU 12)	4	Commutateur Leaf 2 (RU 11)
5	6 serveurs universels (RU 2, 3, 5, 6, 8 et 9)		—

## Façade du serveur Cisco UCS C220 M6

La figure suivante illustre la façade du serveur UCS C220 M6 avec des disques au format SFF.

Consultez le [Guide d'installation et de maintenance du serveur Cisco UCS C220 M6](#) pour en savoir plus.

Illustration 5 : Façade du serveur Cisco UCS C220 M6



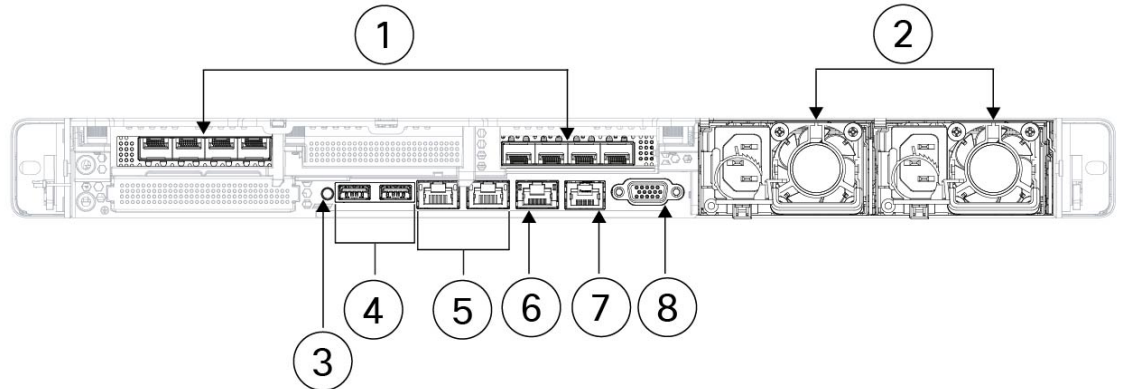
<b>1</b> Baies de disques 1 à 10, numérotées de gauche à droite et de haut en bas  Prise en charge des disques durs et des disques SSD SAS/SATA. En option, les baies de disques 1 à 4 peuvent contenir entre 1 et 4 disques NVMe de votre choix. Les baies de disques 5 à 10 prennent uniquement en charge les disques durs ou les disques SSD SAS/SATA.	<b>2</b> Bouton/voyant d'identification de l'unité
<b>3</b> Bouton d'alimentation/voyant d'état de l'alimentation	<b>4</b> Connecteur KVM  Utilisé avec un câble KVM, il fournit un connecteur DB-15 VGA, un port série DB-9 et deux connecteurs USB 2.0.
<b>5</b> Voyants système : <ul style="list-style-type: none"> <li>• Voyant d'état du ventilateur</li> <li>• Voyant d'état du système</li> <li>• Voyant d'état du module d'alimentation</li> <li>• Voyant d'activité des liaisons du réseau</li> <li>• Voyant d'état de la température</li> </ul>	—

## Panneau arrière du serveur Cisco UCS C220 M6

La figure suivante présente le panneau arrière du serveur UCS C220 M6.

Consultez le [Guide d'installation et de maintenance du serveur Cisco UCS C220 M6](#) pour en savoir plus.

Illustration 6 : Panneau arrière du serveur Cisco UCS C220 M6



<p><b>1</b></p>	<p>Deux connecteurs PCIe</p> <ul style="list-style-type: none"> <li>• Carte de montage 1 (contrôlée par le processeur 1) <ul style="list-style-type: none"> <li>• Prend en charge un connecteur PCIe (connecteur 1)</li> <li>• Le connecteur 1 est mi-hauteur, avec une longueur de 3/4, x16</li> </ul> </li> <li>• Carte de montage 3 (contrôlée par le processeur 2) <ul style="list-style-type: none"> <li>• Prend en charge un connecteur PCIe (connecteur 3)</li> <li>• Le connecteur 3 est mi-hauteur, avec une longueur de 3/4, x16</li> </ul> </li> </ul>	<p><b>2</b></p> <p>Deux blocs d'alimentation, qui sont redondants lorsqu'ils sont configurés en mode d'alimentation 1+1</p>
<p><b>3</b></p>	<p>Bouton/voyant d'identification du système</p>	<p><b>4</b></p> <p>Deux ports USB 3.0</p>
<p><b>5</b></p>	<p>Deux ports Ethernet 1 Go/10 Go (LAN1 et LAN2)</p> <p>Les deux ports LAN prennent en charge 1 Gbit/s et 10 Gbit/s selon la capacité du partenaire de liaison.</p>	<p><b>6</b></p> <p>Port de gestion Ethernet 1 Gbit/s dédié</p>
<p><b>7</b></p>	<p>Port COM (connecteur RJ-45)</p>	<p><b>8</b></p> <p>Port vidéo VGA (connecteur DB-15)</p>





## CHAPITRE 2

### Préparer le site

---

- [Exigences relatives aux températures, à la page 9](#)
- [Exigences relatives à l'humidité, à la page 9](#)
- [Exigences en matière d'altitude, à la page 10](#)
- [Exigences relatives à la poussière et aux particules, à la page 10](#)
- [Minimiser les perturbations électromagnétiques et radioélectriques, à la page 10](#)
- [Exigences relatives aux chocs et aux vibrations, à la page 11](#)
- [Exigences relatives à la mise à la terre, à la page 11](#)
- [Alimentation requise, à la page 11](#)
- [Exigences relatives à la circulation de l'air, à la page 12](#)
- [Espace libre nécessaire, à la page 12](#)

### Exigences relatives aux températures

La température de fonctionnement des commutateurs et des serveurs du cluster Cisco Secure Workload doit être comprise entre 5 et 35 °C (41 à 95 °F) avec un écart de température maximal de 1 °C tous les 305 m (1 000 pieds) d'altitude au-dessus du niveau de la mer. Si ces périphériques ne fonctionnent pas, la température doit être comprise entre -40 et 65 °C (-40 et 149 °F).

### Exigences relatives à l'humidité

Un taux d'humidité élevé peut entraîner la formation de condensation à l'intérieur des commutateurs et des serveurs, ce qui risque de conduire à la corrosion des composants internes et à l'altération de leurs propriétés, à savoir leur résistance électrique, leur conductivité thermique, leur résistance physique ou leur taille. Les commutateurs et les serveurs ont été conçus pour fonctionner dans un environnement présentant un taux d'humidité relative compris entre 10 et 90 %, avec une gradation d'humidité de 10 % par heure. Lorsqu'ils sont éteints, ces équipements supportent une humidité relative comprise entre 5 et 93 %.

Les bâtiments climatisés en périodes de forte chaleur et chauffés durant les mois les plus froids maintiennent généralement un niveau d'humidité qui convient aux périphériques. Néanmoins, si les périphériques sont situés dans un endroit particulièrement humide, utilisez un déshumidificateur pour maintenir un taux d'humidité correct.

## Exigences en matière d'altitude

Si vous utilisez des périphériques du rack à des altitudes élevées (basse pression), vous réduisez l'efficacité du système de refroidissement forcé et par convection, ce qui risque d'entraîner des problèmes électriques liés aux effets d'arc électrique et de couronne. Cela risque également de provoquer une défaillance des composants scellés avec pression interne, tels que les condensateurs électrolytiques, ou du moins de diminuer leurs performances. Ces périphériques sont conçus pour fonctionner à des altitudes comprises entre 0 et 3 050 m (0 à 10 000 pieds) et peuvent être stockés entre 12 200 m (0 et 40 000 pieds).

## Exigences relatives à la poussière et aux particules

Les ventilateurs refroidissent les modules d'alimentation, les commutateurs et les serveurs en aspirant et en évacuant l'air via diverses ouvertures dans le châssis. Néanmoins, les ventilateurs se chargent en poussière et en particules, ce qui entraîne une accumulation de contaminants dans le commutateur et augmente la température interne du châssis. Un environnement de fonctionnement propre réduit de façon significative les effets négatifs de la poussière et des autres particules, qui agissent comme des isolants et interfèrent avec les composants mécaniques des commutateurs et des serveurs.

Outre un nettoyage régulier, prenez les précautions suivantes pour éviter toute contamination des commutateurs et des serveurs :

- Ne fumez pas à proximité du rack.
- Ne mangez pas et ne buvez pas à proximité du rack.

## Minimiser les perturbations électromagnétiques et radioélectriques

Les perturbations électromagnétiques (EMI) et les perturbations radioélectriques (RFI) générées par les équipements dans le rack du cluster Cisco Secure Workload peuvent avoir un effet nuisible sur d'autres équipements, tels que des récepteurs radio et télévisuels (TV), fonctionnant à proximité du rack. Les radiofréquences qui émanent des périphériques du rack peuvent également perturber le fonctionnement des téléphones sans fil et basse puissance. À l'inverse, les perturbations radioélectriques (RFI) des téléphones haute puissance peuvent provoquer l'apparition de caractères erronés sur les écrans des périphériques.

Une perturbation radioélectrique (RFI) est une perturbation électromagnétique dont la fréquence est supérieure à 10 kHz. Ce type de perturbation peut transiter du commutateur vers d'autres équipements via le câble d'alimentation et la source d'alimentation ou par les ondes radio. La Federal Communications Commission (FCC) publie des réglementations spécifiques visant à limiter la quantité de perturbations EMI et RFI émises par les équipements informatiques. Nos commutateurs sont conformes aux réglementations de la FCC.

Lorsque des câbles sont tirés sur une grande distance dans un champ électromagnétique donné, des perturbations peuvent survenir entre le champ et les signaux sur les câbles, engendrant les conséquences suivantes :

- Un mauvais câblage peut provoquer l'émission de perturbations radioélectriques.

- De fortes perturbations EMI, en particulier lorsqu'elles sont provoquées par la foudre ou par des émetteurs radioélectriques, peuvent détruire les émetteurs et les récepteurs de signaux dans le châssis, voire provoquer une électrocution en raison des surtensions présentes sur les lignes conduisant à l'équipement.

**Remarque**

Pour prévoir et éviter les fortes perturbations électromagnétiques, consultez des experts en perturbations radioélectriques.

Il est peu probable que les câbles émettent des perturbations radioélectriques si vous utilisez des câbles à paire torsadée avec une bonne répartition des conducteurs de terre. Si vous dépassez les distances recommandées, utilisez un câble à paires torsadées de bonne qualité, avec un conducteur de terre pour chaque signal de données, si nécessaire.

**Avertissement**

Si les câbles dépassent les distances recommandées ou s'ils traversent différents bâtiments, tenez compte de l'effet de la foudre à proximité. L'impulsion électromagnétique provoquée par la foudre ou tout autre phénomène à haute énergie peut facilement coupler suffisamment d'énergie dans les conducteurs non blindés pour détruire les équipements électroniques. Si vous avez déjà rencontré ce genre de problèmes, consultez des experts en blindage et en suppression des surtensions électriques.

## Exigences relatives aux chocs et aux vibrations

Les équipements du cluster Cisco Secure Workload ont été soumis à des tests de résistance aux chocs et aux vibrations pour répondre aux standards de fonctionnement et de manipulation ainsi qu'aux standards parasismiques.

## Exigences relatives à la mise à la terre

Les équipements du cluster Cisco Secure Workload sont sensibles aux variations de tensions provenant des sources d'alimentation. La surtension, la sous-tension et les transitoires (ou pics) peuvent effacer les données en mémoire, voire entraîner la défaillance des composants. Pour vous éviter ces types de problèmes, assurez-vous que les périphériques sont reliés à la terre. Vous devez connecter le rack à la prise de terre de l'installation.

Les points de mise à la terre du châssis sont dimensionnés pour les vis M5. Vous devez disposer de vos propres vis, cosse de mise à la terre et câble de mise à la terre. La cosse de mise à la terre doit être une cosse à deux trous adaptée aux vis M5. Le câble de mise à la terre doit être un câble de 14 AWG (2 mm) de 60 °C minimum ou certifié par le code électrique local.

## Alimentation requise

Pour fonctionner, les clusters Cisco Secure Workload doivent être alimentés via des sources d'alimentation fournissant les quantités d'énergie suivantes :

- Plateforme grand format à 39 RU, rack unique : 22 500 W

- Plateforme grand format à 39 RU, double rack : 11 500 W pour chaque rack
- Plateforme compacte à 8 RU : 6 500 W

Pour obtenir la redondance  $n+n$  requise, deux sources d'alimentation CA sont nécessaires.

Chaque châssis du rack dispose de deux modules d'alimentation, un pour le fonctionnement et l'autre pour la redondance. Chaque module d'alimentation est raccordé à un bloc multiprise différent sur le rack, et chaque bloc multiprise est connecté à une source d'alimentation CA distincte. Si une source d'alimentation tombe en panne, l'autre fournit l'alimentation requise pour chaque commutateur ou serveur dans le rack.

## Exigences relatives à la circulation de l'air

Pour utiliser le cluster Cisco Secure Workload, vous devez placer chaque rack avec les modules d'alimentation et les ventilateurs sur les trois commutateurs dans une allée froide. Positionnés de cette manière, tous les périphériques du rack aspirent l'air de refroidissement d'une allée froide et évacuent l'air chaud vers une allée chaude.

## Espace libre nécessaire

Le tableau suivant détermine l'espace requis pour installer le cluster Cisco Secure Workload grand format à 39 RU (rack unique ou double rack) ou compact à 8 RU. La largeur de l'allée d'installation doit être supérieure à 59,69 cm (23,5 po) pour permettre le déplacement du rack. En outre, vous devez disposer de suffisamment d'espace pour qu'une personne puisse accéder à l'avant et à l'arrière en vue d'effectuer la maintenance.

**Tableau 1 : Espace libre nécessaire**

Type d'installation	Largeur minimale de l'allée <sup>1</sup>	Espace minimal pour l'installation du rack
Installation du cluster C1-Workload (rack unique)	59,69 cm (23,5 po)	59,69 cm (23,5 po) de large pour 126,492 cm (49,8 po) de profondeur
C1-Workload (double rack)	59,69 cm (23,5 po)	119,38 cm (47 po) de large pour 126,492 cm (49,8 po) de profondeur
C1-Workload-M	59,69 cm (23,5 po)	59,69 cm (23,5 po) de large pour 126,492 cm (49,8 po) de profondeur

<sup>1</sup> La largeur de l'allée d'installation du rack et celle de l'allée d'ouverture de la porte avant doivent être d'au moins 59,69 cm (23,5 po). La largeur de l'autre allée doit être d'au moins 29,845 cm (11,75 po) pour permettre l'ouverture complète des deux portes de l'armoire, bien qu'au moins 59,69 cm (23,5 po) soient nécessaires pour effectuer la maintenance.

Il est nécessaire de positionner le rack en orientant les ventilateurs du commutateur (côté du rack avec la porte la plus grande) face à l'allée froide et les ports du commutateur (côté du rack avec les doubles portes) face à l'allée chaude.





## CHAPITRE 3

# Mettre à la terre et raccorder les périphériques du cluster

---

- [Mettre à la terre les équipements du cluster Cisco Secure Workload, à la page 13](#)
- [Alimenter les équipements du cluster Cisco Secure Workload, à la page 13](#)
- [Connecter le cluster Cisco Secure Workload à vos routeurs, à la page 14](#)

## Mettre à la terre les équipements du cluster Cisco Secure Workload

Les équipements du cluster Cisco Secure Workload disposent de connexions métal sur métal à leur rack. Dès que vous mettez à la terre le rack (ou les racks pour une installation à double rack) via le dispositif de mise à la terre du data center, les équipements du rack sont mis à la terre. Pour mettre à la terre un rack, connectez les roues du rack à la terre.

## Alimenter les équipements du cluster Cisco Secure Workload

Pour mettre le commutateur sous tension, vous devez brancher les deux blocs multiprises connectés au rack à deux sources d'alimentation CA.



### Remarque

Branchez cet équipement sur le secteur via un parasurtenseur de protection au niveau de l'équipement de service, conformément à la directive NFPA 70 du code NEC (National Electrical Code).

Avant d'utiliser, d'installer ou de brancher le système sur la source d'alimentation, consultez les instructions d'installation.

Ne surchargez pas le câblage lorsque vous connectez les unités au circuit d'alimentation.


---

### Avant de commencer

- Il est nécessaire d'installer et de fixer les racks dans le data center en positionnant les entrées d'air dans une allée froide.

- Les racks doivent être reliés à la terre du data center.
- Le cluster doit être connecté à deux routeurs fournis par le client (chaque routeur étant connecté à un commutateur Leaf distinct).
- Deux sources d'alimentation répondant aux exigences d'alimentation du rack doivent se trouver à proximité de chaque câble multiprise.

**Étape 1** Branchez le câble d'alimentation du premier bloc multiprise à une source d'alimentation CA, et le câble d'alimentation du deuxième bloc multiprise à une source d'alimentation CA distincte.

**Étape 2** Examinez chaque module d'alimentation installé dans chaque périphérique du rack pour vérifier que le voyant  est allumé en vert.

- Si aucun des voyants n'est allumé, assurez-vous que la source d'alimentation est sous tension et que l'interrupteur marche/arrêt du bloc multiprise est activé.
- Si certains de ces voyants sont allumés et que d'autres ne le sont pas, assurez-vous que le câble d'alimentation provenant de ce module d'alimentation est correctement connecté au bloc multiprise du rack.

## Connecter le cluster Cisco Secure Workload à vos routeurs

Vous devez connecter le cluster Cisco Secure Workload à deux routeurs.

**Étape 1** Si vous installez un cluster double rack grand format à 39 RU, raccordez les câbles d'interface partiellement connectés sur chaque rack. Connectez chacun de ces câbles au port indiqué sur l'autre rack.

**Étape 2** Utilisez un câble 10 Gigabit pour connecter un routeur au port E1/39 sur le commutateur Leaf 1 pour un déploiement à 39 RU ou au port E1/47 pour un déploiement à 8 RU. Le commutateur Leaf 1 se trouve à l'emplacement suivant :

- Plateforme à rack unique grand format à 39 RU—40 RU dans le rack de la plateforme
- Plateforme à double rack grand format de 39 RU—40 RU dans le rack 1
- Plateforme compacte à 8 RU—12 RU dans le rack de la plateforme

**Étape 3** Utilisez un câble 10 Gigabit pour connecter un routeur au port E1/39 sur le commutateur Leaf 2 pour un déploiement à 39 RU ou au port E1/47 pour un déploiement à 8 RU. Le commutateur Leaf 2 se trouve à l'emplacement suivant :

- Plateforme à rack unique grand format à 39 RU—41 RU dans le rack de la plateforme
- Plateforme à double rack grand format de 39 RU—41 RU dans le rack 2
- Plateforme compacte à 8 RU—11 RU dans le rack de la plateforme



## CHAPITRE 4

# Configurer l'interface utilisateur

- (Facultatif) Exigences et restrictions pour le mode double pile (prise en charge d'IPv6), à la page 15
- Configurer l'interface utilisateur, à la page 16

## (Facultatif) Exigences et restrictions pour le mode double pile (prise en charge d'IPv6)

Les clusters Cisco Secure Workload exécutés sur du matériel physique peuvent être configurés pour utiliser IPv6 en plus d'IPv4 pour certaines communications vers et depuis le cluster.



**Remarque** Vous pouvez utiliser le mode double pile (prise en charge d'IPv6) lors de l'installation ou de la mise à niveau vers les versions 3.6.1.5, 3.7.1.5 et 3.8.1.1. Toutefois, l'option permettant d'activer cette fonctionnalité n'est pas disponible lorsque vous installez ou mettez à niveau des correctifs.

### Restrictions

Si vous envisagez d'activer le mode double pile, tenez compte des points suivants :

- Vous pouvez activer la connectivité IPv6 uniquement lors du déploiement initial ou de la mise à niveau vers une version majeure (vous ne pouvez pas activer cette fonctionnalité lors de la mise à niveau des correctifs).
- Le mode double pile est pris en charge uniquement sur le matériel physique ou les clusters sans système d'exploitation.
- Le mode IPv6 uniquement n'est pas pris en charge.
- Vous ne pouvez pas revenir au mode IPv4 uniquement après avoir activé le mode double pile pour le cluster.
- La sauvegarde et la restauration des données (DBR) ne sont pas prises en charge si la connectivité double pile est activée.
- N'activez pas le mode double pile pour les clusters configurés avec la fédération.
- Les fonctionnalités suivantes utilisent toujours et uniquement IPv4 (notez qu'IPv4 est toujours activé, même si IPv6 est activé) :

- (applicable pour les versions 3.8.1.1, 3.7.1.5 et 3.6.x) Application sur les agents AIX
- (applicable uniquement pour la version 3.6.x) Communication de l'agent matériel avec le cluster
- (applicable uniquement pour la version 3.6.x) Connecteurs pour l'intégration de flux, l'enrichissement de l'inventaire ou les notifications d'alerte

### Conditions requises

- Configurez les enregistrements DNS A et AAAA pour le nom de domaine complet avant d'activer le mode double pile pour votre cluster.
- Les services externes tels que NTP, SMTP et DNS doivent être disponibles sur IPv4 et IPv6, pour des raisons de redondance.
- Pour configurer le mode double pile pour un cluster :
  - À des fins de redondance, des adresses IPv6 routables sur deux réseaux différents doivent être allouées à chacun des deux commutateurs Leaf du cluster, et des passerelles par défaut doivent être fournies pour chaque réseau.
  - Pour les clusters 39 RU, un réseau IPv6 routable sur site avec suffisamment d'espace pour au moins 29 adresses d'hôtes est requis.
  - Pour les clusters 8 RU, un réseau IPv6 routable sur site avec suffisamment d'espace pour au moins 20 adresses d'hôtes est requis.
  - Les trois premières adresses d'hôte du réseau IPv6 routable sur site sont réservées à la configuration HSRP du cluster Cisco Secure Workload et ne doivent pas être utilisées par d'autres équipements.

### Informations complémentaires

Les agents communiquent avec le cluster à l'aide d'IPv4, sauf si vous les configurez pour utiliser IPv6. Pour obtenir des instructions, consultez le Guide de l'utilisateur de Cisco Secure Workload.

## Configurer l'interface utilisateur

### Avant de commencer

- Pour terminer cette configuration, vous devez disposer d'un équipement tel qu'un ordinateur portable doté d'un port Ethernet et d'un accès à Internet.
- Vous avez également besoin d'un câble Ethernet pour connecter l'équipement au serveur le plus élevé du cluster Cisco Secure Workload.
- Google Chrome est le seul navigateur pris en charge pour le portail de configuration, requis pour une partie de ce processus.
- (Facultatif) À partir de la version 3.6, vous pouvez configurer votre cluster en mode double pile, ce qui permet d'utiliser IPv4 et IPv6 pour la communication entre certains composants Cisco Secure Workload et entre Cisco Secure Workload et les services réseau tels que NTP et DNS. (Cisco Secure Workload

traite déjà le trafic IPv6, que vous activez ou non le mode double pile.) Vous pouvez activer cette prise en charge uniquement lors du déploiement ou de la mise à niveau.

Si vous envisagez d'activer la prise en charge d'IPv6, reportez-vous à la section [\(Facultatif\) Exigences et restrictions pour le mode double pile \(prise en charge d'IPv6\)](#), à la page 15.



---

**Important** Saisissez les adresses IPv4 dans tous les champs de la procédure ci-dessous, à moins que le nom du champ n'indique explicitement IPv6.

---

**Étape 1** Configurez le périphérique Internet avec l'adresse IP 2.2.2.1/30 (255.255.255.252).

**Étape 2** Utilisez un câble Ethernet pour connecter le port Ethernet de l'équipement Internet au port LOM 2 (LAN2) sur le serveur le plus élevé du cluster Cisco Secure Workload.

**Étape 3** Sur l'équipement Internet, ouvrez le navigateur Chrome et accédez à l'adresse `http://2.2.2.2:9000`.

**Remarque** Le navigateur Chrome est le seul navigateur testé avec ce processus.

La page Setup Diagnostics (Diagnostics de configuration) s'affiche.

**Étape 4** Si la page de diagnostics contient des erreurs, vérifiez que les câbles qui relient les périphériques du cluster sont correctement raccordés ou que les câbles sont correctement acheminés avant de poursuivre cette procédure. Lorsque vous avez terminé, revenez à l'étape 2.

Reportez-vous aux rubriques [Câblage des équipements du cluster C1-Workload](#), à la page 23 et [Câblage des équipements du cluster C1-Workload-M](#), à la page 36 pour savoir comment raccorder correctement les câbles.

**Étape 5** Cliquez sur **Continuer** (Continuer).

La page RPM Upload (Chargement du fichier RPM) s'ouvre.

**Remarque** Si vous accédez à la page Site Config (Configuration du site), saisissez l'URL suivante pour ouvrir la page de chargement du fichier RPM :

`http://2.2.2.2:9000 /upload`

**Étape 6** Chargez les fichiers RPM dans le cloud Cisco Secure Workload.

Vous devez charger les fichiers dans l'ordre suivant :

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

- a) Cliquez sur **Choose File** (Choisir un fichier).
- b) Recherchez un fichier RPM, sélectionnez-le et cliquez sur **Open** (Ouvrir).
- c) Cliquez sur **Upload** (Charger).

Lorsque vous téléchargez les fichiers RPM, la liste n'est pas mise à jour sur la page. Ce comportement est tout à fait normal.

Si une erreur se produit après le chargement du fichier

`tetration_os_mother_rpm_k9-2.1.1.31-1.el6.x86_64.rpm`, attendez 5 à 10 minutes, puis chargez de nouveau la page. La liste des fichiers RPM chargés devrait s'afficher une fois la page chargée à nouveau. Cette erreur, qui n'indique toutefois aucun problème, est due au redémarrage de l'orchestrateur.

d) Répétez les étapes a à c pour chaque fichier RPM.

Une fois le chargement des fichiers RPM terminé, la page Site Config (Configuration du site) s'affiche.

## Étape 7

Utilisez la page Site Config (Configuration du site) pour configurer le nouveau site comme suit :

- Cliquez sur **General** (Général).

1. Dans le champ **Site Name** (Nom du site), saisissez le nom du cluster unique.
2. Dans le champ **SSH Public Key** (Clé publique SSH), collez la clé d'authentification.

**Remarque** Générez votre propre paire de clés SSH pour accéder au cluster via l'authentification unique.

Nous vous recommandons vivement de conserver la clé SSH dans un emplacement sécurisé, durable et accessible à des fins de dépannage ou de récupération du cluster à l'aide de l'accès `ta_guest`.

3. Cliquez sur **Next** (Suivant).

- Cliquez sur **Email**.

1. Indiquez les adresses e-mail requises.
2. Cliquez sur **Next** (Suivant).

- Cliquez sur **L3**.

Saisissez chacune des adresses demandées. Tous les champs signalés par \* sont obligatoires.

Saisissez toutes les adresses au format IPv4, sauf si le nom de champ spécifie IPv6.

(Facultatif) Si vous installez la version 3.6 ou une version ultérieure du logiciel, pour activer le mode double pile (prise en charge IPv4 et IPv6) :

1. Cochez la case IPv6.
2. Saisissez l'adresse IPv6 au format CIDR pour les commutateurs Leaf 1 et Leaf 2.
3. Indiquez la passerelle IPv6 Leaf 1 et Leaf 2 par défaut.
4. Cliquez sur **Suivant**.

- Cliquez sur **Network** (Réseau).

Saisissez toutes les adresses au format IPv4, sauf si le nom de champ spécifie IPv6.

1. Dans le champ **Internal network IP address** (Adresse IP du réseau interne), collez l'adresse obtenue suite au déploiement de l'orchestrateur.
2. Dans le champ **External network IP address** (Adresse IP du réseau externe), collez l'adresse obtenue suite au déploiement de l'orchestrateur.

3. Dans le champ **External gateway IP address** (Adresse IP de la passerelle externe), collez l'adresse obtenue suite au déploiement de l'orchestrateur.
4. Dans le champ **DNS resolver IP address** (Adresse IP du résolveur DNS), collez l'adresse obtenue suite au déploiement de l'orchestrateur.
5. Dans le champ **DNS domain** (Domaine DNS), saisissez votre domaine DNS (par exemple, **cisco.com**).
6. (Version logicielle 3.6 ou ultérieure) Si vous avez activé IPv6 sur la page L3, **IPv6** est automatiquement sélectionné.

Si IPv6 est sélectionné, vous devez spécifier les adresses IPv6 réservées à l'utilisation de Cisco Secure Workload :

- Saisissez le **réseau IPv6 externe**.

Les 3 premières adresses IPv6 du champ IPv6 External Network (Réseau externe IPv6) sont toujours réservées aux commutateurs du cluster Cisco Secure Workload et ne doivent pas être utilisées à d'autres fins.

- Si vous souhaitez utiliser IPv6 uniquement pour certaines adresses, saisissez-les dans le champ **External IPv6 IPs** (Adresses IPv6 externes).

- Remarque**
- Pour un cluster de 39 RU, assurez-vous qu'au moins 29 adresses IPv6 sont disponibles dans la liste des réseaux externes IPv6 ou des adresses IPv6 externes.
  - Pour un cluster de 8 RU, assurez-vous qu'au moins 20 adresses IPv6 sont disponibles dans la liste des réseaux externes IPv6 ou des adresses IPv6 externes.

7. Cliquez sur **Next** (Suivant).

- Cliquez sur **Service**.

1. Dans le champ **NTP Servers** (Serveurs NTP), saisissez la liste (séparée par des espaces) des noms de serveur NTP ou des adresses IP obtenus suite au déploiement de l'orchestrateur.
2. Dans le champ **SMTP Server** (Serveur SMTP), saisissez le nom ou l'adresse IP d'un serveur SMTP que Cisco Secure Workload peut utiliser pour envoyer des e-mails. Ce serveur doit être accessible par Cisco Secure Workload.
3. Dans le champ **SMTP Port** (Port SMTP), saisissez le numéro de port du serveur SMTP. AWS limite l'utilisation des ports 25 et 465. Vous devez configurer votre compte correctement ou utiliser le port 587.
4. (Facultatif) Dans le champ **SMTP Username** (Nom d'utilisateur SMTP), saisissez le nom d'utilisateur pour l'authentification SMTP.
5. (Facultatif) Dans le champ **SMTP Password** (Mot de passe SMTP), saisissez le mot de passe pour l'authentification SMTP.
6. (Facultatif) Dans le champ **HTTP Proxy Server** (Serveur proxy HTTP), saisissez le nom ou l'adresse IP d'un serveur proxy HTTP que Cisco Secure Workload peut utiliser pour accéder à des services externes sur Internet.
7. (Facultatif) Dans le champ **HTTP Proxy Port** (Port du proxy HTTP), saisissez le numéro de port du serveur proxy HTTP.

8. (Facultatif) Dans le champ **HTTPs Proxy Server** (Serveur proxy HTTPs), saisissez le nom ou l'adresse IP d'un serveur proxy HTTPs que Cisco Secure Workload peut utiliser pour accéder à des services externes sur Internet.
  9. (Facultatif) Dans le champ **HTTPs Proxy Port** (Port du proxy HTTPs), saisissez le numéro de port du serveur proxy HTTPs.
  10. (Facultatif) Dans le champ **Syslog Server** (Serveur Syslog), saisissez le nom ou l'adresse IP d'un serveur Syslog que Cisco Secure Workload peut utiliser pour envoyer des alertes.
  11. (Facultatif) Dans le champ **Syslog Port** (Port Syslog), saisissez le numéro de port du serveur Syslog.
  12. (Facultatif) Dans le champ **Syslog Severity** (Gravité Syslog), saisissez le niveau de gravité des messages Syslog. Les valeurs disponibles sont les suivantes : information, notification, avertissement, erreur, critique, alerte et urgence.
  13. Cliquez sur **Next** (Suivant).
- Cliquez sur **UI** (Interface utilisateur).
    1. Dans le champ **UI VRRP VRID** \*(VRID VRRP de l'interface utilisateur), saisissez **77**, sauf si vous avez besoin d'un VRID unique.
    2. Dans le champ **UI FQDN** (Nom de domaine complet de l'interface utilisateur), saisissez le nom de domaine complet avec lequel vous accédez au cluster.
    3. Laissez le champ **UI Airbrake Key** (Clé Airbrake de l'interface utilisateur) vide.
    4. Cliquez sur **Next** (Suivant).  
Tetration (Cisco Secure Workload) valide vos paramètres de configuration et affiche l'état de ces paramètres.
  - Cliquez sur **Advanced** (Options avancées).
    1. Dans le champ **External IPs** (Adresses IP externes), saisissez les adresses IPv4.
    2. Cliquez sur **Continue** (Continuer).

**Étape 8** En cas d'échec, cliquez sur **Back** (Précédent) et modifiez la configuration (voir l'étape 7).

**Remarque** Vous ne pouvez pas modifier ces paramètres dans l'interface utilisateur après avoir quitté cette page. Vous pouvez toutefois modifier les paramètres ultérieurement via la page de l'entreprise dans l'interface utilisateur.

**Étape 9** Si votre configuration est correcte et qu'aucune modification n'est nécessaire, cliquez sur **Continue** (Continuer).

Cisco Secure Workload est configuré en fonction des paramètres que vous avez spécifiés. Ce processus prend une à deux heures sans aucune intervention de votre part.

### Que faire ensuite

Si vous avez déployé la version 3.6 ou ultérieure du logiciel et si vous avez activé la connectivité IPv6 :

- Vous pouvez accéder au portail web Cisco Secure Workload à l'aide d'IPv4 ou d'IPv6.



- Par défaut, les agents logiciels communiquent avec le cluster Cisco Secure Workload via IPv4, même si le cluster prend en charge IPv6. Si vous souhaitez que les agents pris en charge utilisent IPv6 à cette fin, vous devez configurer le champ **Sensor VIP FQDN** (Nom de domaine complet de l'adresse VIP du capteur) sur la page **Platform > Cluster Configuration** (Plateforme > Configuration du cluster) du portail web Cisco Secure Workload. Pour obtenir des instructions importantes, consultez le guide de l'utilisateur, disponible dans l'aide en ligne sur le portail web Cisco Secure Workload ou sur la page <https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html>.





## CHAPITRE 5

# Câblage des équipements du cluster C1-Cisco Secure Workload

---

- [Câblage des équipements du cluster C1-Workload, à la page 23](#)
- [Câblage des équipements du cluster C1-Workload-M, à la page 36](#)

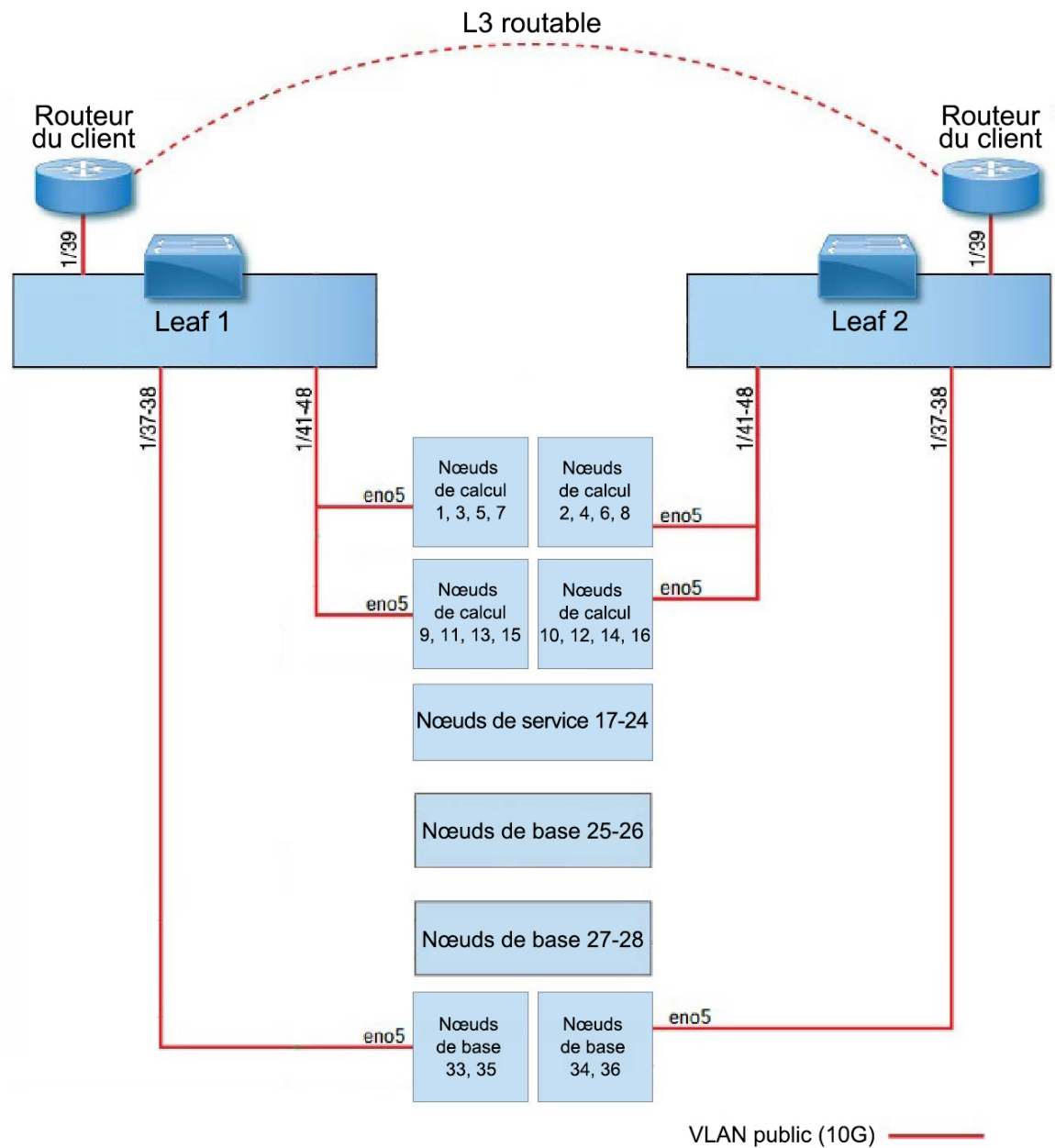
## Câblage des équipements du cluster C1-Workload

Pour câbler la carte d'interface virtuelle M6 sur le rack 39 RU, lisez les informations de configuration suivantes :

- Il existe deux interfaces privées pour tous les nœuds.
- Le rack 39 RU possède une interface publique pour 20 nœuds.
- Le matériel M6 est équipé de quatre ports par carte d'interface virtuelle.
- Les noms de l'interface sans système d'exploitation (les serveurs physiques dans le cluster connus sous le nom de nœuds de base, de calcul et de service) commencent par « eno » (Ethernet onboard, soit Ethernet intégré).

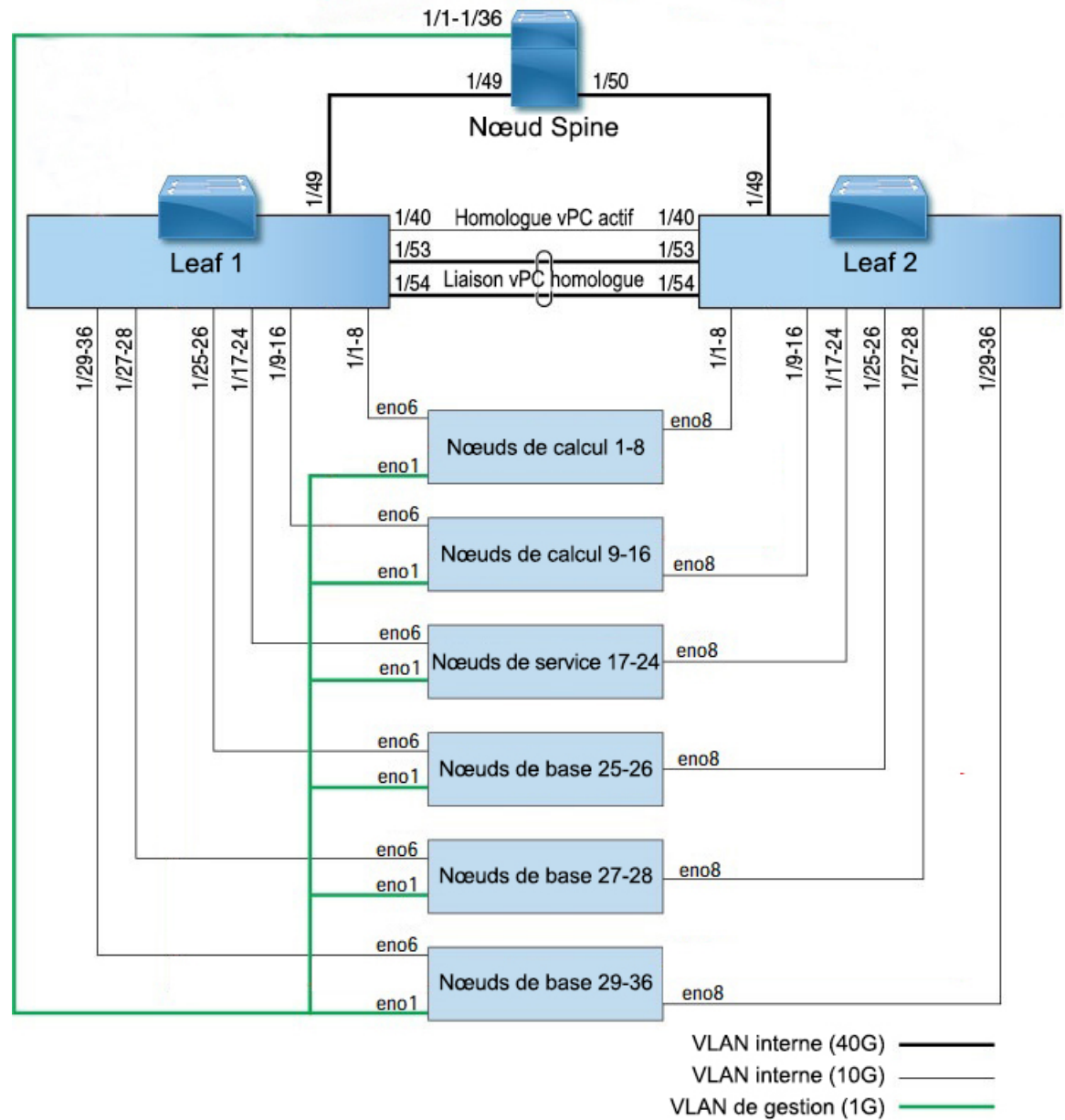
Le schéma suivant présente le câblage des équipements pour la configuration publique/externe du rack C1-Workload. Pour obtenir une liste détaillée des connexions, consultez les tableaux qui suivent les schémas.

Illustration 7 : Câblage des équipements du rack C1-Workload (configuration publique/externe)



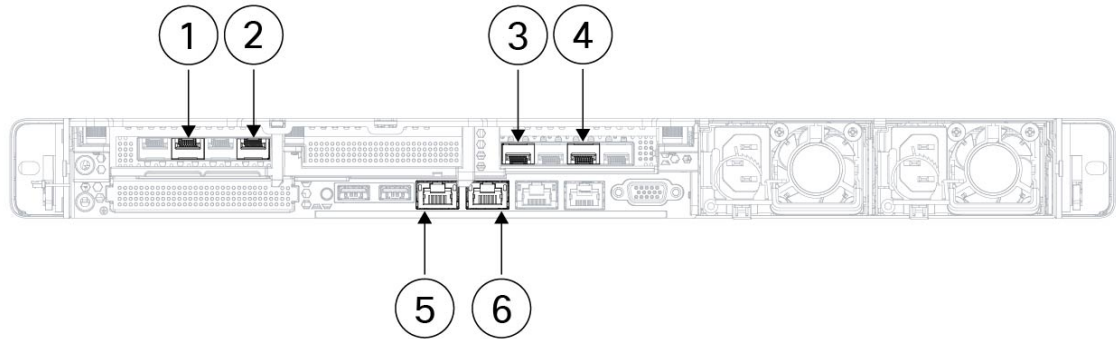
Le schéma suivant présente le câblage des équipements pour la configuration interne/de gestion du rack C1-Workload. Pour obtenir une liste détaillée des connexions, consultez les tableaux suivants.

Illustration 8 : Câblage des équipements du rack C1-Workload (configuration interne/de gestion)



L'illustration suivante indique les ports du serveur M6 correspondant aux ports « eno » dans les schémas ci-dessus :

Illustration 9 : Ports du serveur M6



<b>1</b>	Commutateur Leaf 1 ou Leaf 2 public selon le serveur Port d'interface du serveur = eno5 Désignation CIMC = adaptateur 1/port physique 2/vic-1-eth1	<b>2</b>	Commutateur Leaf 1 privé Port d'interface du serveur = eno6 Désignation CIMC = adaptateur 1/port physique 0/vic-1-eth0
<b>3</b>	Commutateur Leaf 2 privé Port d'interface du serveur = eno8 Désignation CIMC = adaptateur 3/port physique 0/vic-3-eth0	<b>4</b>	Non utilisé Port d'interface du serveur = eno7 Désignation CIMC = adaptateur 3/port physique 2/vic-3-eth1
<b>5</b>	CIMC Port d'interface du serveur = eno1 Désignation CIMC = LOM 1	<b>6</b>	MGMT 2.2.2.2 Port d'interface du serveur = eno2 Désignation CIMC = LOM 2

Tableau 2 : Connexions du commutateur Spine (RU 42 dans les installations à rack unique et les installations à double rack)

Port Spine	Type de connexion	Connexion			
		Appareil	RU dans un rack unique	RU dans un double rack	Port
1/1	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 1 (nœud de calcul)	RU 36	Rack 1 RU 17	eno1
1/2	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 2 (nœud de calcul)	RU 35	Rack 1 RU 16	eno1
1/3	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 3 (nœud de calcul)	RU 34	Rack 1 RU 15	eno1
1/4	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 4 (nœud de calcul)	RU 33	Rack 1 RU 14	eno1

Port Spine	Type de connexion	Connexion			
		Appareil	RU dans un rack unique	RU dans un double rack	Port
1/5	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 5 (nœud de calcul)	RU 32	Rack 1 RU 13	eno1
1/6	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 6 (nœud de calcul)	RU 31	Rack 1 RU 12	eno1
1/7	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 7 (nœud de calcul)	RU 30	Rack 1 RU 11	eno1
1/8	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 8 (nœud de calcul)	RU 29	Rack 1 RU 10	eno1
1/9	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 9 (nœud de calcul)	RU 28	Rack 1 RU 8	eno1
1/10	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 10 (nœud de calcul)	RU 27	Rack 1 RU 7	eno1
1/11	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 11 (nœud de calcul)	RU 26	Rack 1 RU 6	eno1
1/12	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 12 (nœud de calcul)	RU 25	Rack 1 RU 5	eno1
1/13	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 13 (nœud de calcul)	RU 24	Rack 1 RU 4	eno1
1/14	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 14 (nœud de calcul)	RU 23	Rack 1 RU 3	eno1
1/15	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 15 (nœud de calcul)	RU 22	Rack 1 RU 2	eno1
1/16	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 16 (nœud de calcul)	RU 21	Rack 1 RU 1	eno1
17/1	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 17 (nœud de service)	RU 20	Rack 2 RU 21	eno1
1/18	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 18 (nœud de service)	RU 19	Rack 2 RU 20	eno1
1/19	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 19 (nœud de service)	RU 18	Rack 2 RU 19	eno1
1/20	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 20 (nœud de service)	RU 17	Rack 2 RU 18	eno1

Port Spine	Type de connexion	Connexion			
		Appareil	RU dans un rack unique	RU dans un double rack	Port
1/21	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 21 (nœud de service)	RU 16	Rack 2 RU 17	eno1
1/22	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 22 (nœud de service)	RU 15	Rack 2 RU 16	eno1
1/23	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 23 (nœud de service)	RU 14	Rack 2 RU 15	eno1
1/24	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 24 (nœud de service)	RU 13	Rack 2 RU 14	eno1
1/25	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 25 (nœud de base)	RU 12	Rack 2 RU 12	eno1
1/26	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 26 (nœud de base)	RU 11	Rack 2 RU 11	eno1
1/27	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 27 (nœud de base)	RU 10	Rack 2 RU 10	eno1
1/28	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 28 (nœud de base)	RU 9	Rack 2 RU 9	eno1
1/29	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 29 (nœud de base)	RU 8	Rack 2 RU 8	eno1
1/30	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 30 (nœud de base)	RU 7	Rack 2 RU 7	eno1
1/31	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 31 (nœud de base)	RU 6	Rack 2 RU 6	eno1
1/32	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 32 (nœud de base)	RU 5	Rack 2 RU 5	eno1
1/33	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 33 (nœud de base)	RU 4	Rack 2 RU 4	eno1
1/34	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 34 (nœud de base)	RU 3	Rack 2 RU 3	eno1
1/35	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 35 (nœud de base)	RU 2	Rack 2 RU 2	eno1
1/36	VLAN CIMC (1 Gigabit)	Hôte de serveur UCS 36 (nœud de base)	RU 1	Rack 2 RU 1	eno1



Port Spine	Type de connexion	Connexion			
		Appareil	RU dans un rack unique	RU dans un double rack	Port
1/49	VLAN interne (40 Gigabit)	Commutateur Leaf 1 (RU 41 dans le rack unique ou RU 40 dans le rack 1 du double rack)	RU 40	Rack 1 RU 40	1/49
1/50	VLAN interne (40 Gigabit)	Commutateur Leaf 2 (RU 40 dans le rack unique ou RU 40 du rack 2 dans le double rack) port 49	RU 41	Rack 2 RU 40	1/50

**Tableau 3 : Connexions du commutateur Leaf 1 (RU 41 dans les installations à un rack unique ou RU 40 dans le rack 1 des installations à double rack)**

Port Leaf 1	Type de connexion	Connexion			
		Appareil	RU dans un rack unique	RU dans un double rack	Port
1/1	VLAN interne (10 Gigabit)	Hôte de serveur UCS 1 (nœud de calcul)	RU 36	Rack 1 RU 17	eno6
1/2	VLAN interne (10 Gigabit)	Hôte de serveur UCS 2 (nœud de calcul)	RU 35	Rack 1 RU 16	eno6
1/3	VLAN interne (10 Gigabit)	Hôte de serveur UCS 3 (nœud de calcul)	RU 34	Rack 1 RU 15	eno6
1/4	VLAN interne (10 Gigabit)	Hôte de serveur UCS 4 (nœud de calcul)	RU 33	Rack 1 RU 14	eno6
1/5	VLAN interne (10 Gigabit)	Hôte de serveur UCS 5 (nœud de calcul)	RU 32	Rack 1 RU 13	eno6
1/6	VLAN interne (10 Gigabit)	Hôte de serveur UCS 6 (nœud de calcul)	RU 31	Rack 1 RU 12	eno6
1/7	VLAN interne (10 Gigabit)	Hôte de serveur UCS 7 (nœud de calcul)	RU 30	Rack 1 RU 11	eno6
1/8	VLAN interne (10 Gigabit)	Hôte de serveur UCS 8 (nœud de calcul)	RU 29	Rack 1 RU 10	eno6
1/9	VLAN interne (10 Gigabit)	Hôte de serveur UCS 9 (nœud de calcul)	RU 28	Rack 1 RU 8	eno6
1/10	VLAN interne (10 Gigabit)	Hôte de serveur UCS 10 (nœud de calcul)	RU 27	Rack 1 RU 7	eno6
1/11	VLAN interne (10 Gigabit)	Hôte de serveur UCS 11 (nœud de calcul)	RU 26	Rack 1 RU 6	eno6

Port Leaf 1	Type de connexion	Connexion			
		Appareil	RU dans un rack unique	RU dans un double rack	Port
1/12	VLAN interne (10 Gigabit)	Hôte de serveur UCS 12 (nœud de calcul)	RU 25	Rack 1 RU 5	eno6
1/13	VLAN interne (10 Gigabit)	Hôte de serveur UCS 13 (nœud de calcul)	RU 24	Rack 1 RU 4	eno6
1/14	VLAN interne (10 Gigabit)	Hôte de serveur UCS 14 (nœud de calcul)	RU 23	Rack 1 RU 3	eno6
1/15	VLAN interne (10 Gigabit)	Hôte de serveur UCS 15 (nœud de calcul)	RU 22	Rack 1 RU 2	eno6
1/16	VLAN interne (10 Gigabit)	Hôte de serveur UCS 16 (nœud de calcul)	RU 21	Rack 1 RU 1	eno6
17/1	VLAN interne (10 Gigabit)	Hôte de serveur UCS 17 (nœud de service)	RU 20	Rack 2 RU 21	eno6
1/18	VLAN interne (10 Gigabit)	Hôte de serveur UCS 18 (nœud de service)	RU 19	Rack 2 RU 20	eno6
1/19	VLAN interne (10 Gigabit)	Hôte de serveur UCS 19 (nœud de service)	RU 18	Rack 2 RU 19	eno6
1/20	VLAN interne (10 Gigabit)	Hôte de serveur UCS 20 (nœud de service)	RU 17	Rack 2 RU 18	eno6
1/21	VLAN interne (10 Gigabit)	Hôte de serveur UCS 21 (nœud de service)	RU 16	Rack 2 RU 17	eno6
1/22	VLAN interne (10 Gigabit)	Hôte de serveur UCS 22 (nœud de service)	RU 15	Rack 2 RU 16	eno6
1/23	VLAN interne (10 Gigabit)	Hôte de serveur UCS 23 (nœud de service)	RU 14	Rack 2 RU 15	eno6
1/24	VLAN interne (10 Gigabit)	Hôte de serveur UCS 24 (nœud de service)	RU 13	Rack 2 RU 14	eno6
1/25	VLAN interne (10 Gigabit)	Hôte de serveur UCS 25 (nœud de base)	RU 12	Rack 2 RU 12	eno6
1/26	VLAN interne (10 Gigabit)	Hôte de serveur UCS 26 (nœud de base)	RU 11	Rack 2 RU 11	eno6
1/27	VLAN interne (10 Gigabit)	Hôte de serveur UCS 27 (nœud de base)	RU 10	Rack 2 RU 10	eno6

Port Leaf 1	Type de connexion	Connexion			
		Appareil	RU dans un rack unique	RU dans un double rack	Port
1/28	VLAN interne (10 Gigabit)	Hôte de serveur UCS 28 (nœud de base)	RU 9	Rack 2 RU 9	eno6
1/29	VLAN interne (10 Gigabit)	Hôte de serveur UCS 29 (nœud de base)	RU 8	Rack 2 RU 8	eno6
1/30	VLAN interne (10 Gigabit)	Hôte de serveur UCS 30 (nœud de base)	RU 7	Rack 2 RU 7	eno6
1/31	VLAN interne (10 Gigabit)	Hôte de serveur UCS 31 (nœud de base)	RU 6	Rack 2 RU 6	eno6
1/32	VLAN interne (10 Gigabit)	Hôte de serveur UCS 32 (nœud de base)	RU 5	Rack 2 RU 5	eno6
1/33	VLAN interne (10 Gigabit)	Hôte de serveur UCS 33 (nœud de base)	RU 4	Rack 2 RU 4	eno6
1/34	VLAN interne (10 Gigabit)	Hôte de serveur UCS 34 (nœud de base)	RU 3	Rack 2 RU 3	eno6
1/35	VLAN interne (10 Gigabit)	Hôte de serveur UCS 35 (nœud de base)	RU 2	Rack 2 RU 2	eno6
1/36	VLAN interne (10 Gigabit)	Hôte de serveur UCS 36 (nœud de base)	RU 1	Rack 2 RU 1	eno6
1/37	VLAN public (10 Gigabit)	Hôte de serveur UCS 33 (nœud de base)	RU 3	Rack 2 RU 3	eno5
1/38	VLAN public (10 Gigabit)	Hôte de serveur UCS 35 (nœud de base)	RU 1	Rack 2 RU 1	eno5
1/39	VLAN interne (10 Gigabit)	Routeur du client 1	—	—	—
1/40	VLAN interne (10 Gigabit)	Leaf 1	RU 40	Rack 1 RU 40	1/40
1/41	VLAN public (10 Gigabit)	Hôte de serveur UCS 1 (nœud de calcul)	RU 35	Rack 1 RU 16	eno5
1/42	VLAN public (10 Gigabit)	Hôte de serveur UCS 3 (nœud de calcul)	RU 33	Rack 1 RU 14	eno5
1/43	VLAN public (10 Gigabit)	Hôte de serveur UCS 5 (nœud de calcul)	RU 31	Rack 1 RU 12	eno5
1/44	VLAN public (10 Gigabit)	Hôte de serveur UCS 7 (nœud de calcul)	RU 29	Rack 1 RU 10	eno5

Port Leaf 1	Type de connexion	Connexion			
		Appareil	RU dans un rack unique	RU dans un double rack	Port
1/45	VLAN public (10 Gigabit)	Hôte de serveur UCS 9 (nœud de calcul)	RU 27	Rack 1 RU 8	eno5
1/46	VLAN public (10 Gigabit)	Hôte de serveur UCS 11 (nœud de calcul)	RU 25	Rack 1 RU 6	eno5
1/47	VLAN public (10 Gigabit)	Hôte de serveur UCS 13 (nœud de calcul)	RU 23	Rack 1 RU 4	eno5
1/48	VLAN public (10 Gigabit)	Hôte de serveur UCS 15 (nœud de calcul)	RU 21	Rack 1 RU 2	eno5
1/49	VLAN interne (40 Gigabit)	Commutateur Spine	RU 42	Rack 1 RU 42	1/49
1/50	—	—	—	—	—
1/51	—	—	—	—	—
1/52	—	—	—	—	—
1/53	VLAN interne (40 Gigabit)	Commutateur Leaf 1	RU 40	Rack 1 RU 40	1/53
1/54	VLAN interne (40 Gigabit)	Commutateur Leaf 1	RU 40	Rack 1 RU 40	1/54

**Tableau 4 : Connexions du commutateur Leaf 2 (RU 41 dans les installations à un rack unique ou RU 40 dans le rack 2 des installations à double rack)**

Port Leaf 2	Type de connexion	Connexion			
		Appareil	RU dans un rack unique	RU dans un double rack	Port
1/1	VLAN interne (10 Gigabit)	Hôte de serveur UCS 1 (nœud de calcul)	RU 36	Rack 1 RU 17	eno8
1/2	VLAN interne (10 Gigabit)	Hôte de serveur UCS 2 (nœud de calcul)	RU 35	Rack 1 RU 16	eno8
1/3	VLAN interne (10 Gigabit)	Hôte de serveur UCS 3 (nœud de calcul)	RU 34	Rack 1 RU 15	eno8
1/4	VLAN interne (10 Gigabit)	Hôte de serveur UCS 4 (nœud de calcul)	RU 33	Rack 1 RU 14	eno8

Port Leaf 2	Type de connexion	Connexion			
		Appareil	RU dans un rack unique	RU dans un double rack	Port
1/5	VLAN interne (10 Gigabit)	Hôte de serveur UCS 5 (nœud de calcul)	RU 32	Rack 1 RU 13	eno8
1/6	VLAN interne (10 Gigabit)	Hôte de serveur UCS 6 (nœud de calcul)	RU 31	Rack 1 RU 12	eno8
1/7	VLAN interne (10 Gigabit)	Hôte de serveur UCS 7 (nœud de calcul)	RU 30	Rack 1 RU 11	eno8
1/8	VLAN interne (10 Gigabit)	Hôte de serveur UCS 8 (nœud de calcul)	RU 29	Rack 1 RU 10	eno8
1/9	VLAN interne (10 Gigabit)	Hôte de serveur UCS 9 (nœud de calcul)	RU 28	Rack 1 RU 8	eno8
1/10	VLAN interne (10 Gigabit)	Hôte de serveur UCS 10 (nœud de calcul)	RU 27	Rack 1 RU 7	eno8
1/11	VLAN interne (10 Gigabit)	Hôte de serveur UCS 11 (nœud de calcul)	RU 26	Rack 1 RU 6	eno8
1/12	VLAN interne (10 Gigabit)	Hôte de serveur UCS 12 (nœud de calcul)	RU 25	Rack 1 RU 5	eno8
1/13	VLAN interne (10 Gigabit)	Hôte de serveur UCS 13 (nœud de calcul)	RU 24	Rack 1 RU 4	eno8
1/14	VLAN interne (10 Gigabit)	Hôte de serveur UCS 14 (nœud de calcul)	RU 23	Rack 1 RU 3	eno8
1/15	VLAN interne (10 Gigabit)	Hôte de serveur UCS 15 (nœud de calcul)	RU 22	Rack 1 RU 2	eno8
1/16	VLAN interne (10 Gigabit)	Hôte de serveur UCS 16 (nœud de calcul)	RU 21	Rack 1 RU 1	eno8
17/1	VLAN interne (10 Gigabit)	Hôte de serveur UCS 17 (nœud de service)	RU 20	Rack 2 RU 21	eno8
1/18	VLAN interne (10 Gigabit)	Hôte de serveur UCS 18 (nœud de service)	RU 19	Rack 2 RU 20	eno8
1/19	VLAN interne (10 Gigabit)	Hôte de serveur UCS 19 (nœud de service)	RU 18	Rack 2 RU 19	eno8
1/20	VLAN interne (10 Gigabit)	Hôte de serveur UCS 20 (nœud de service)	RU 17	Rack 2 RU 18	eno8

Port Leaf 2	Type de connexion	Connexion			
		Appareil	RU dans un rack unique	RU dans un double rack	Port
1/21	VLAN interne (10 Gigabit)	Hôte de serveur UCS 21 (nœud de service)	RU 16	Rack 2 RU 17	eno8
1/22	VLAN interne (10 Gigabit)	Hôte de serveur UCS 22 (nœud de service)	RU 15	Rack 2 RU 16	eno8
1/23	VLAN interne (10 Gigabit)	Hôte de serveur UCS 23 (nœud de service)	RU 14	Rack 2 RU 15	eno8
1/24	VLAN interne (10 Gigabit)	Hôte de serveur UCS 24 (nœud de service)	RU 13	Rack 2 RU 14	eno8
1/25	VLAN interne (10 Gigabit)	Hôte de serveur UCS 25 (nœud de base)	RU 12	Rack 2 RU 12	eno8
1/26	VLAN interne (10 Gigabit)	Hôte de serveur UCS 26 (nœud de base)	RU 11	Rack 2 RU 11	eno8
1/27	VLAN interne (10 Gigabit)	Hôte de serveur UCS 27 (nœud de base)	RU 10	Rack 2 RU 10	eno8
1/28	VLAN interne (10 Gigabit)	Hôte de serveur UCS 28 (nœud de base)	RU 9	Rack 2 RU 9	eno8
1/29	VLAN interne (10 Gigabit)	Hôte de serveur UCS 29 (nœud de base)	RU 8	Rack 2 RU 8	eno8
1/30	VLAN interne (10 Gigabit)	Hôte de serveur UCS 30 (nœud de base)	RU 7	Rack 2 RU 7	eno8
1/31	VLAN interne (10 Gigabit)	Hôte de serveur UCS 31 (nœud de base)	RU 6	Rack 2 RU 6	eno8
1/32	VLAN interne (10 Gigabit)	Hôte de serveur UCS 32 (nœud de base)	RU 5	Rack 2 RU 5	eno8
1/33	VLAN interne (10 Gigabit)	Hôte de serveur UCS 33 (nœud de base)	RU 4	Rack 2 RU 4	eno8
1/34	VLAN interne (10 Gigabit)	Hôte de serveur UCS 34 (nœud de base)	RU 3	Rack 2 RU 3	eno8
1/35	VLAN interne (10 Gigabit)	Hôte de serveur UCS 35 (nœud de base)	RU 2	Rack 2 RU 2	eno8
1/36	VLAN interne (10 Gigabit)	Hôte de serveur UCS 36 (nœud de base)	RU 1	Rack 2 RU 1	eno8
1/37	VLAN public (10 Gigabit)	Hôte de serveur UCS 34 (nœud de base)	RU 4	Rack 2 RU 8	eno5

Port Leaf 2	Type de connexion	Connexion			
		Appareil	RU dans un rack unique	RU dans un double rack	Port
1/38	VLAN public (10 Gigabit)	Hôte de serveur UCS 36 (nœud de base)	RU 2	Rack 2 RU 6	eno5
1/39	VLAN interne (10 Gigabit)	Routeur du client 1	—	—	—
1/40	VLAN interne (10 Gigabit)	Commutateur Leaf 2	RU 41	Rack 2 RU 40	1/40
1/41	VLAN public (10 Gigabit)	Hôte de serveur UCS 2 (nœud de calcul)	RU 36	Rack 1 RU 17	eno5
1/42	VLAN public (10 Gigabit)	Hôte de serveur UCS 4 (nœud de calcul)	RU 34	Rack 1 RU 15	eno5
1/43	VLAN public (10 Gigabit)	Hôte de serveur UCS 6 (nœud de calcul)	RU 32	Rack 1 RU 13	eno5
1/44	VLAN public (10 Gigabit)	Hôte de serveur UCS 8 (nœud de calcul)	RU 30	Rack 1 RU 11	eno5
1/45	VLAN public (10 Gigabit)	Hôte de serveur UCS 10 (nœud de calcul)	RU 28	Rack 1 RU 9	eno5
1/46	VLAN public (10 Gigabit)	Hôte de serveur UCS 12 (nœud de calcul)	RU 26	Rack 1 RU 7	eno5
1/47	VLAN public (10 Gigabit)	Hôte de serveur UCS 14 (nœud de calcul)	RU 24	Rack 1 RU 5	eno5
1/48	VLAN public (10 Gigabit)	Hôte de serveur UCS 16 (nœud de calcul)	RU 22	Rack 1 RU 3	eno5
1/49	VLAN interne (40 Gigabit)	Commutateur Spine	RU 42	Rack 1 RU 42	—
1/50	—	—	—	—	1/50
1/51	—	—	—	—	—
1/52	—	—	—	—	—
1/53	VLAN interne (40 Gigabit)	Commutateur Leaf 1	RU 40	Rack 1 RU 40	1/49
1/54	VLAN interne (40 Gigabit)	Commutateur Leaf 2	RU 41	Rack 2 RU 40	1/50

## Câblage des équipements du cluster C1-Workload-M

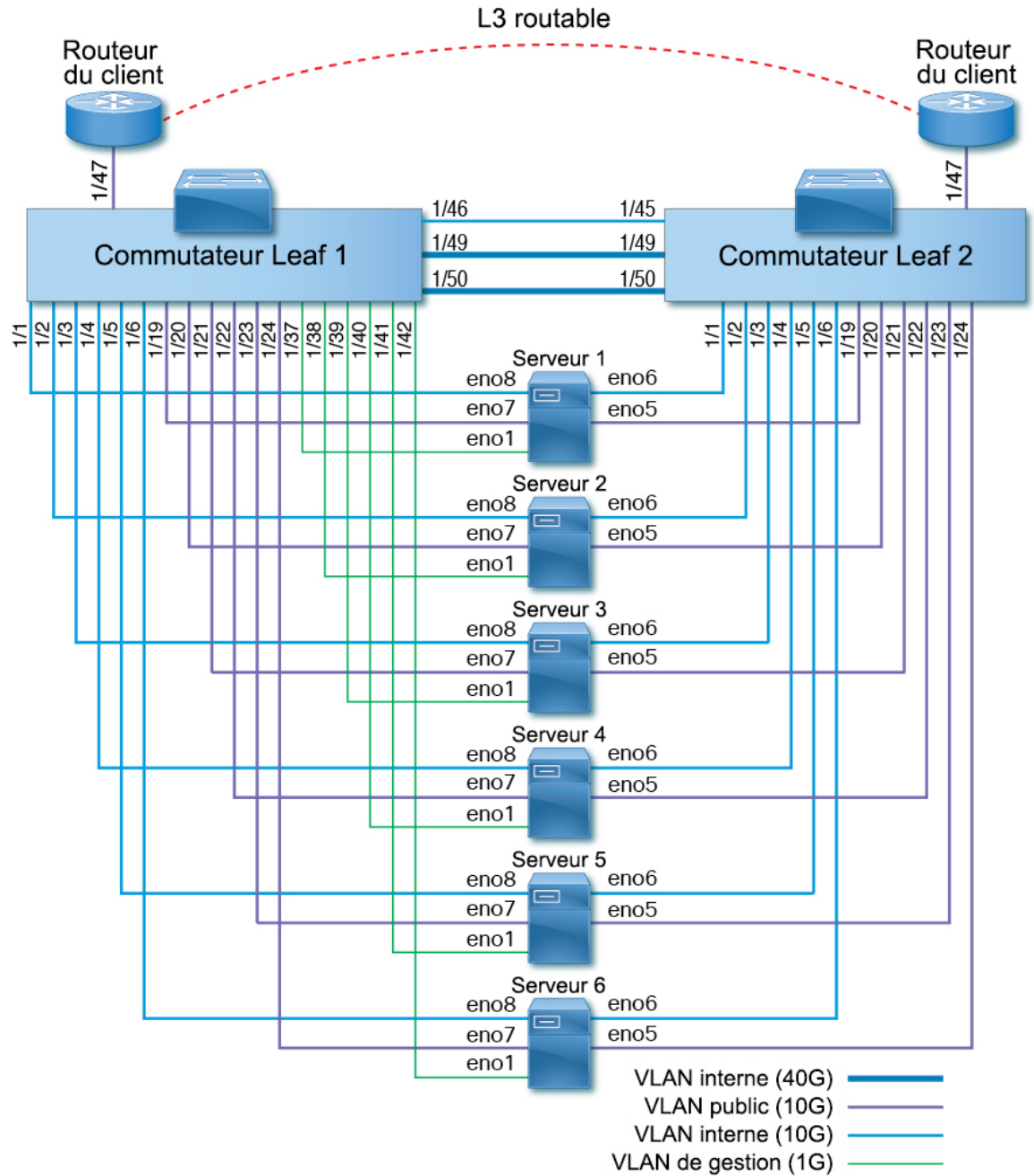
Pour câbler la carte d'interface virtuelle M6 sur le rack 8 RU, lisez les informations de configuration suivantes :

- Il existe deux interfaces privées pour tous les nœuds.
- Le rack 8 RU dispose de deux interfaces publiques pour les six nœuds.
- Le matériel M6 est équipé de quatre ports par carte d'interface virtuelle.
- Les noms de l'interface sans système d'exploitation (le serveur physique dans le cluster connu sous le nom de nœuds universels) commencent par « eno » (Ethernet onboard, soit Ethernet intégré).

Le schéma suivant présente le câblage des équipements pour la configuration interne/de gestion/publique/externe du rack 8 RU du cluster C1-Workload-M. Pour obtenir une liste détaillée des connexions, consultez les tableaux qui suivent le schéma.

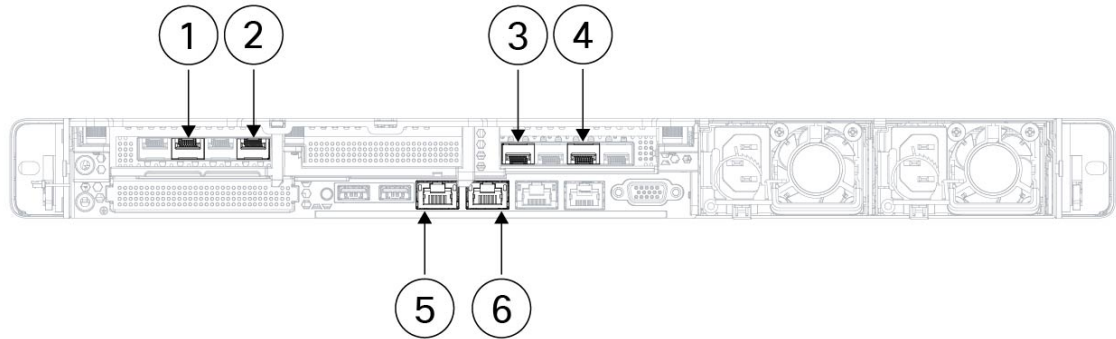


Illustration 10 : Câblage des équipements du rack du cluster C1-Workload-M (configuration interne/de gestion/publique/externe)



L'illustration suivante présente les ports du serveur correspondant aux ports « eno » du schéma ci-dessus :

Illustration 11 : Ports du serveur M6



<b>1</b>	Commutateur Leaf 2 public Port d'interface du serveur = eno5 Désignation CIMC = adaptateur 1/port physique 2/vic-1-eth1	<b>2</b>	Commutateur Leaf 2 privé Port d'interface du serveur = eno6 Désignation CIMC = adaptateur 1/port physique 0/vic-1-eth0
<b>3</b>	Commutateur Leaf 1 privé Port d'interface du serveur = eno8 Désignation CIMC = adaptateur 3/port physique 0/vic-3-eth0	<b>4</b>	Commutateur Leaf 1 public Port d'interface du serveur = eno7 Désignation CIMC = adaptateur 3/port physique 2/vic3-eth1
<b>5</b>	CIMC Port d'interface du serveur = eno1 Désignation CIMC = LOM 1	<b>6</b>	MGMT 2.2.2.2 Port d'interface du serveur = eno2 Désignation CIMC = LOM 2

Tableau 5 : Connexions du commutateur Leaf 1 (RU 12)

Port Leaf	Type de connexion	Connexion		
		Appareil	RU dans un rack unique	Port
1/1	VLAN interne (10 Gigabit)	Hôte du serveur UCS 1 (nœud universel)	RU 9	eno8
1/2	VLAN interne (10 Gigabit)	Hôte du serveur UCS 2 (nœud universel)	RU 8	eno8
1/3	VLAN interne (10 Gigabit)	Hôte du serveur UCS 3 (nœud universel)	RU 6	eno8
1/4	VLAN interne (10 Gigabit)	Hôte du serveur UCS 4 (nœud universel)	RU 5	eno8
1/5	VLAN interne (10 Gigabit)	Hôte du serveur UCS 5 (nœud universel)	RU 3	eno8
1/6	VLAN interne (10 Gigabit)	Hôte du serveur UCS 6 (nœud universel)	RU 2	eno8
1/7	—	—	—	—

Port Leaf	Type de connexion	Connexion		
		Appareil	RU dans un rack unique	Port
1/8	—	—	—	—
1/9	—	—	—	—
1/10	—	—	—	—
1/11	—	—	—	—
1/12	—	—	—	—
1/13	—	—	—	—
1/14	—	—	—	—
1/15	—	—	—	—
1/16	—	—	—	—
17/1	—	—	—	—
1/18	—	—	—	—
1/19	VLAN externe (10 Gigabit)	Hôte du serveur UCS 1 (nœud universel)	RU 9	eno7
1/20	VLAN externe (10 Gigabit)	Hôte du serveur UCS 2 (nœud universel)	RU 8	eno7
1/21	VLAN externe (10 Gigabit)	Hôte du serveur UCS 3 (nœud universel)	RU 6	eno7
1/22	VLAN externe (10 Gigabit)	Hôte du serveur UCS 4 (nœud universel)	RU 5	eno7
1/23	VLAN externe (10 Gigabit)	Hôte du serveur UCS 5 (nœud universel)	RU 3	eno7
1/24	VLAN externe (10 Gigabit)	Hôte du serveur UCS 6 (nœud universel)	RU 2	eno7
1/25	—	—	—	—
1/26	—	—	—	—
1/27	—	—	—	—
1/28	—	—	—	—
1/29	—	—	—	—
1/30	—	—	—	—
1/31	—	—	—	—

Port Leaf	Type de connexion	Connexion		
		Appareil	RU dans un rack unique	Port
1/32	—	—	—	—
1/33	—	—	—	—
1/34	—	—	—	—
1/35	—	—	—	—
1/36	—	—	—	—
1/37	VLAN de gestion (1 Gigabit)	Hôte du serveur UCS 1 (nœud universel)	RU 9	eno1
1/38	VLAN de gestion (1 Gigabit)	Hôte du serveur UCS 2 (nœud universel)	RU 8	eno1
1/39	VLAN de gestion (1 Gigabit)	Hôte du serveur UCS 3 (nœud universel)	RU 6	eno1
1/40	VLAN de gestion (1 Gigabit)	Hôte du serveur UCS 4 (nœud universel)	RU 5	eno1
1/41	VLAN de gestion (1 Gigabit)	Hôte du serveur UCS 5 (nœud universel)	RU 3	eno1
1/42	VLAN de gestion (1 Gigabit)	Hôte du serveur UCS 6 (nœud universel)	RU 2	eno1
1/43	—	—	—	—
1/44	—	—	—	—
1/45	—	—	—	—
1/46	VLAN interne (10 Gigabit)	Commutateur Leaf 2	RU 11	1/45
1/47	VLAN externe (10 Gigabit)	Routeur du client	—	—
1/48	—	—	—	—
1/49	VLAN interne (40 Gigabit)	Commutateur Leaf 2	RU 11	1/49
1/50	VLAN interne (40 Gigabit)	Commutateur Leaf 2	RU 11	1/50
1/51	—	—	—	—
1/52	—	—	—	—
1/53	—	—	—	—
1/54	—	—	—	—

Tableau 6 : Connexions du commutateur Leaf 2 (RU 11)

Port Leaf	Type de connexion	Connexion		
		Appareil	RU dans un rack unique	Port
1/1	VLAN interne (10 Gigabit)	Hôte du serveur UCS 1 (nœud universel)	9 RU	eno6
1/2	VLAN interne (10 Gigabit)	Hôte du serveur UCS 2 (nœud universel)	8 RU	eno6
1/3	VLAN interne (10 Gigabit)	Hôte du serveur UCS 3 (nœud universel)	6 RU	eno6
1/4	VLAN interne (10 Gigabit)	Hôte du serveur UCS 4 (nœud universel)	5 RU	eno6
1/5	VLAN interne (10 Gigabit)	Hôte du serveur UCS 5 (nœud universel)	3 RU	eno6
1/6	VLAN interne (10 Gigabit)	Hôte du serveur UCS 6 (nœud universel)	2 RU	eno6
1/7	—	—	—	—
1/8	—	—	—	—
1/9	—	—	—	—
1/10	—	—	—	—
1/11	—	—	—	—
1/12	—	—	—	—
1/13	—	—	—	—
1/14	—	—	—	—
1/15	—	—	—	—
1/16	—	—	—	—
17/1	—	—	—	—
1/18	—	—	—	—
1/19	VLAN externe (10 Gigabit)	Hôte du serveur UCS 1 (nœud universel)	9 RU	eno5
1/20	VLAN externe (10 Gigabit)	Hôte du serveur UCS 2 (nœud universel)	8 RU	eno5
1/21	VLAN externe (10 Gigabit)	Hôte du serveur UCS 3 (nœud universel)	6 RU	eno5
1/22	VLAN externe (10 Gigabit)	Hôte du serveur UCS 4 (nœud universel)	5 RU	eno5
1/23	VLAN externe (10 Gigabit)	Hôte du serveur UCS 5 (nœud universel)	3 RU	eno5
1/24	VLAN externe (10 Gigabit)	Hôte du serveur UCS 6 (nœud universel)	2 RU	eno5

Port Leaf	Type de connexion	Connexion		
		Appareil	RU dans un rack unique	Port
1/25	—	—	—	—
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 interne (10 Gigabit)	Commutateur Leaf 1	12 RU	1/46
1/46	—	—	—	—
1/47	VLAN externe (10 Gigabit)	Routeur du client	—	—
1/48	—	—	—	—
1/49	VLAN interne (40 Gigabit)	Commutateur Leaf 1	12 RU	1/49

Port Leaf	Type de connexion	Connexion		
		Appareil	RU dans un rack unique	Port
1/50	VLAN interne (40 Gigabit)	Commutateur Leaf 1	12 RU	1/50
1/51	—	—	—	—
1/52	—	—	—	—
1/53	—	—	—	—
1/54	—	—	—	—







# CHAPITRE 6

## Spécifications système

- [Caractéristiques environnementales, à la page 45](#)
- [Cordons d'alimentation, à la page 45](#)

## Caractéristiques environnementales

Le tableau suivant répertorie les caractéristiques environnementales requises lors de l'installation du cluster Cisco Secure Workload.

**Tableau 7 : Caractéristiques environnementales**

Environnement		Spécification
Température	Température	5 à 35 °C (41 à 95 °F) avec réduction de la température maximale de 1 °C tous les 305 m (1 000 pieds) au-dessus du niveau de la mer.
	Stockage	De -40 à 65 °C (de -40 à 149 °F)
Humidité	Température	Humidité relative de 10 à 80 % avec gradation d'humidité de 10 % par heure
	Stockage	Humidité relative de 5 à 93 %
Altitude	Température	De 0 à 3 050 m (de 0 à 10 000 pieds)
	Stockage	De 0 à 12 200 m (de 0 à 40 000 pieds)

## Cordons d'alimentation

Les tableaux suivants répertorient les câbles d'alimentation fournis avec le cluster Cisco Secure Workload M6.

**Tableau 8 : Cluster 39 RU, configuration à rack unique**

Référence	Description	Quantité
TA-RACK-UCS2-INT	Rack dynamique Cisco R42612 avec panneaux latéraux	1

Référence	Description	Quantité
TA-ETH-RJ45-SINGLE	Kit de câbles RJ-45 pour une configuration à un rack unique de 39 RU	1
TA-SFP-H10GB-CU2M	Câble 10GBASE-CU SFP+ de 2 m	16
TA-SFP-H10GB-CU1-5	Câble 10GBASE-CU SFP+ de 1,5 m	32
TA-QSFP-H40G-CU1M	Câble cuivre passif 40GBASE-CR4 de 1 m	4
TA-SFP-H10GB-CU1M	Câble 10GBASE-CU SFP+ de 1 m	25
TA-SFP-H10GB-CU2-5	Câble 10GBASE-CU SFP+ de 2,5 m	20

Tableau 9 : Cluster 39 RU, configuration à double rack

Référence	Description	Quantité
TA-RACK-UCS2-INT	Rack dynamique Cisco R42612, avec panneaux latéraux	2
TA-ETH-RJ45-DUAL	Kit de câbles RJ-45 pour une configuration à un rack unique de 39 RU	1
TA-SFP-H10GB-CU2M	Câble 10GBASE-CU SFP+ de 2 m	15
TA-SFP-H10GB-CU1-5	Câble 10GBASE-CU SFP+ de 1,5 m	19
TA-QSFP-H40G-CU1M	Câble cuivre passif 40GBASE-CR4 de 1 m	1
TA-QSFP-H40G-CU5M	Câble cuivre passif 40GBASE-CR4 de 5 m	3
TA-SFP-H10GB-CU2-5	Câble 10GBASE-CU SFP+ de 2,5 m	12
TA-SFP-H10GB-CU5M	Câble 10GBASE-CU SFP+ de 5 m	47

Tableau 10 : Cluster 8 RU

Référence	Description	Quantité
TA-RACK-UCS2-INT	Rack dynamique Cisco R42612, avec panneaux latéraux	1
CAB-ETH-S-RJ45	Câble jaune pour Ethernet, direct, RJ-45, 6 pieds	6
TA-SFP-H10GB-CU1M	Câble 10GBASE-CU SFP+ de 1 m	13
TA-SFP-H10GB-CU1-5	Câble 10GBASE-CU SFP+ de 1,5 m	12
TA-QSFP-H40G-CU1M	Câble cuivre passif 40GBASE-CR4 de 1 m	2
GLC-TE	Module émetteur-récepteur 1000BASE-T SFP pour câble de cuivre catégorie 5	6