

Configurer le superviseur Cisco IMC pour les serveurs des gammes C et E

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Serveurs UCS série C](#)

[Serveurs UCS, série E](#)

[Versions minimales du micrologiciel](#)

[Cartes PCIe prises en charge](#)

[Versions d'hyperviseur prises en charge](#)

[Informations générales](#)

[Configuration](#)

[Déployer le superviseur Cisco IMC](#)

[Modifier le mot de passe par défaut](#)

[Informations de licence](#)

[Découvrir le serveur](#)

[Ajouter un groupe de racks](#)

[Ajouter un compte rack](#)

[Configuration de la messagerie](#)

[Mise à niveau du micrologiciel](#)

[Exporter les données d'assistance technique vers un serveur distant](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer le superviseur IMC (Integrated Management Controller) de Cisco pour les serveurs de la gamme C et E.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Serveurs Cisco série C
- Serveurs de la gamme Cisco E

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Internet Explorer 8 ou supérieur
- Google Chrome 4.1 ou supérieur
- Firefox 3.5 ou supérieur
- Safari 4.0 ou supérieur (pour Apple MAC ou Microsoft Windows)
- Les navigateurs nécessitent le plug-in Adobe Flash Player version 11 ou ultérieure.

Serveurs UCS série C

- Cisco UCS C-220 M3
- Cisco UCS C-240 M3
- Cisco UCS C-220 M4
- Cisco UCS C-240 M4
- Cisco UCS C-22 M3
- Cisco UCS C-24 M3
- Cisco UCS C-420 M3
- Cisco UCS C-460 M4

Serveurs UCS, série E

- Cisco UCS E-140S M2
- Cisco UCS E-160D M2
- Cisco UCS EN120E M2
- Cisco UCS EN120S M2
- Cisco UCS E-180D M2
- Cisco UCS E-140S M1
- Cisco UCS E-140D M1
- Cisco UCS E-160D M1
- Cisco UCS E-140DP M1
- Cisco UCS E-160DP M1

Versions minimales du micrologiciel

Serveurs	Version minimale du micrologiciel
Serveurs UCS série C	1.5(4) et postérieures
Serveurs UCS, série E	2.3.1 et postérieures

Cartes PCiE prises en charge

- Carte d'interface virtuelle (VIC) Cisco UCS 1225
- Carte d'interface virtuelle Cisco UCS 1225T

Versions d'hyperviseur prises en charge

- ESXi 5.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Cisco IMC Supervisor est un système de gestion qui vous permet de gérer des serveurs rack à grande échelle.

Vous pouvez utiliser Cisco IMC Supervisor afin d'effectuer ces tâches pour un serveur de montage en rack :

- Prise en charge du regroupement logique des serveurs et des vues récapitulatives par groupe
- Collecter l'inventaire des serveurs
- Fournir des fonctionnalités de surveillance pour les serveurs et les groupes
- Gestion des microprogrammes comprenant le téléchargement, la mise à niveau et l'activation des microprogrammes
- Gérer les actions de serveur autonome qui incluent le contrôle de l'alimentation, le contrôle des DEL, la collecte des journaux, le lancement de clavier/vidéo/souris (KVM), le lancement de l'interface utilisateur CIMC et les alertes par e-mail
- Contrôle d'accès basé sur les rôles (RBAC) afin de restreindre l'accès et les fonctionnalités

Configuration

Déployer le superviseur Cisco IMC

1. Complétez ces étapes afin de déployer Cisco IMC Supervisor.

Étape 1. Afin de télécharger le fichier zip pour Cisco IMC Supervisor à partir de Cisco.com, accédez à **Products > Servers-Unified Computing > Integrated Management Controller (IMC) Supervisor** comme indiqué dans l'image.

Downloads Home > Products > Servers - Unified Computing

Find: Product Name e.g. 2811

Products Recently Used Products My Added Devices Add Device	Application Networking Services Cisco Interfaces and Modules Cloud and Systems Management Collaboration Endpoints Conferencing Connected Safety and Security Customer Collaboration IOS and NX-OS Software Optical Networking Routers Security Servers - Unified Computing Service Exchange Storage Networking Switches Unified Communications Universal Gateways and Access Servers Video Wireless	C800 Series Integrated Management Controller (IMC) Supervisor ← UCS B-Series Blade Server Software UCS C-Series Rack-Mount Standalone Server Software UCS C-Series Rack-Mount UCS-Managed Server Software UCS Central Software UCS Director UCS E-Series Software UCS Express UCS Infrastructure and UCS Manager Software UCS Invicta Series Solid State Systems UCS Management Partner Ecosystem Software UCS Performance Manager Virtual Application Container Services (VACS)
---	--	--

Étape 2. Sélectionnez **IMC Supervisor 1.0** comme indiqué dans l'image.

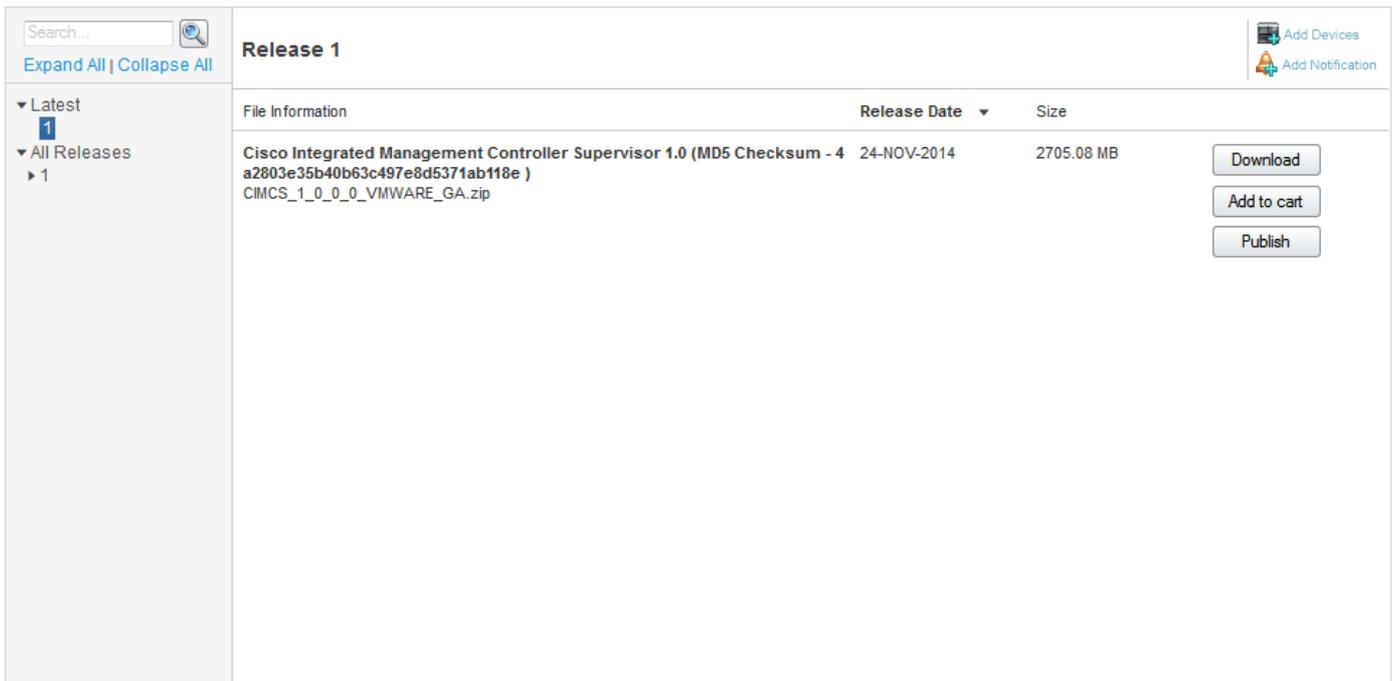
Downloads Home > Products > Servers - Unified Computing > Integrated Management Controller (IMC) Supervisor

Find: Product Name e.g. 2811

Products Recently Used Products My Added Devices Add Device	C800 Series Integrated Management Controller (IMC) Supervisor UCS B-Series Blade Server Software UCS C-Series Rack-Mount Standalone Server Software UCS C-Series Rack-Mount UCS-Managed Server Software UCS Central Software UCS Director UCS E-Series Software UCS Express UCS Infrastructure and UCS Manager Software UCS Invicta Series Solid State Systems UCS Management Partner Ecosystem Software UCS Performance Manager Virtual Application Container Services (VACS)	IMC Supervisor 1.0
---	--	--------------------

Étape 3. Cliquez sur **Télécharger** comme indiqué dans l'image.

IMC Supervisor 1.0



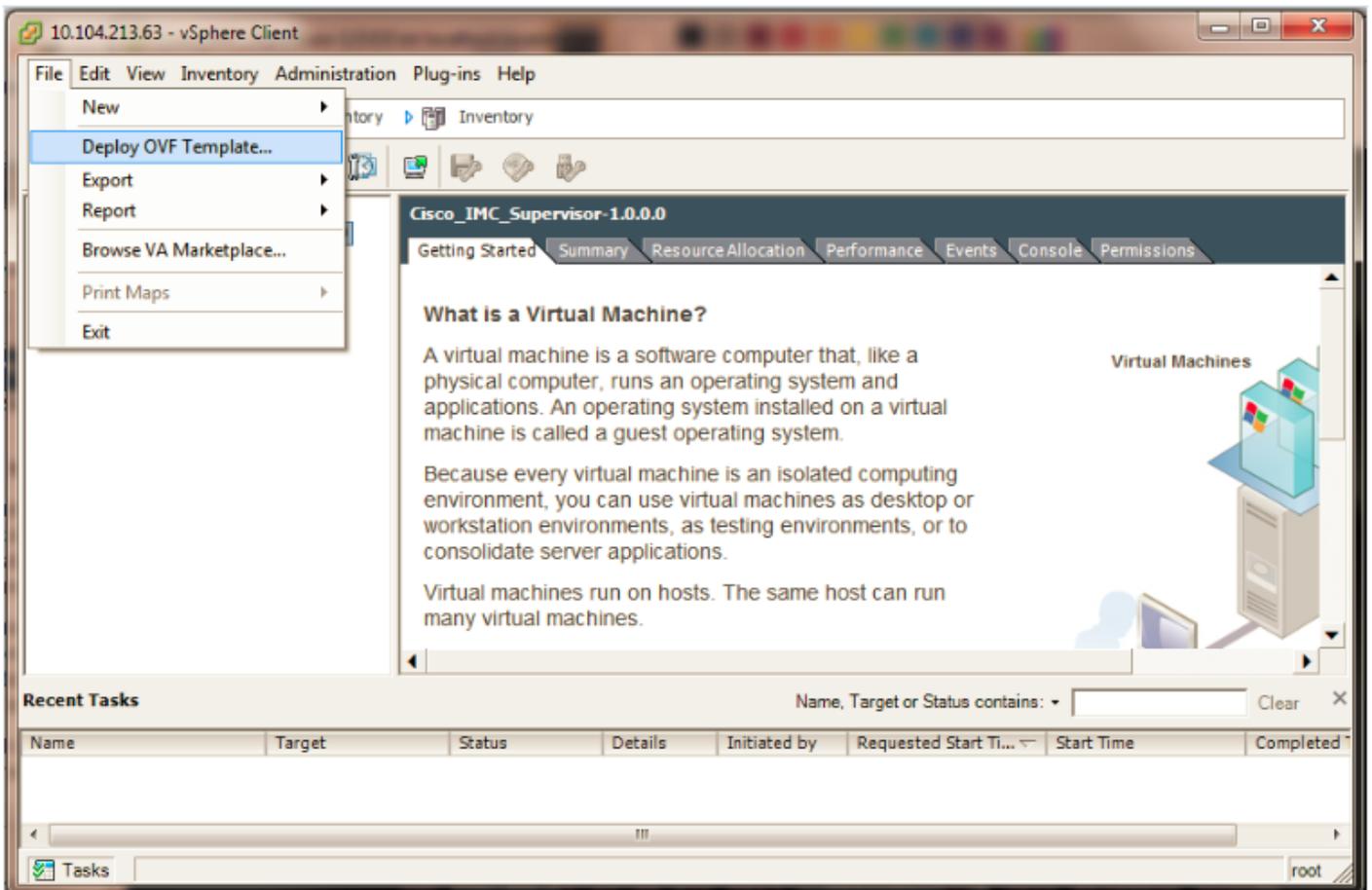
Search... 

[Expand All](#) | [Collapse All](#)

Release 1 [Add Devices](#)
[Add Notification](#)

File Information	Release Date	Size	
Cisco Integrated Management Controller Supervisor 1.0 (MD5 Checksum - 4 a2803e35b40b63c497e8d5371ab118e) CIMCS_1_0_0_0_VMWARE_GA.zip	24-NOV-2014	2705.08 MB	Download Add to cart Publish

Étape 4. Afin de déployer l'Open Virtual Appliance (OVA), naviguez jusqu'à **Fichier > Déployer le modèle OVF** comme indiqué dans l'image.



10.104.213.63 - vSphere Client

File Edit View Inventory Administration Plug-ins Help

- New
- Deploy OVF Template...**
- Export
- Report
- Browse VA Marketplace...
- Print Maps
- Exit

Inventory

Cisco_IMC_Supervisor-1.0.0.0

Getting Started Summary Resource Allocation Performance Events Console Permissions

What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

Virtual Machines 

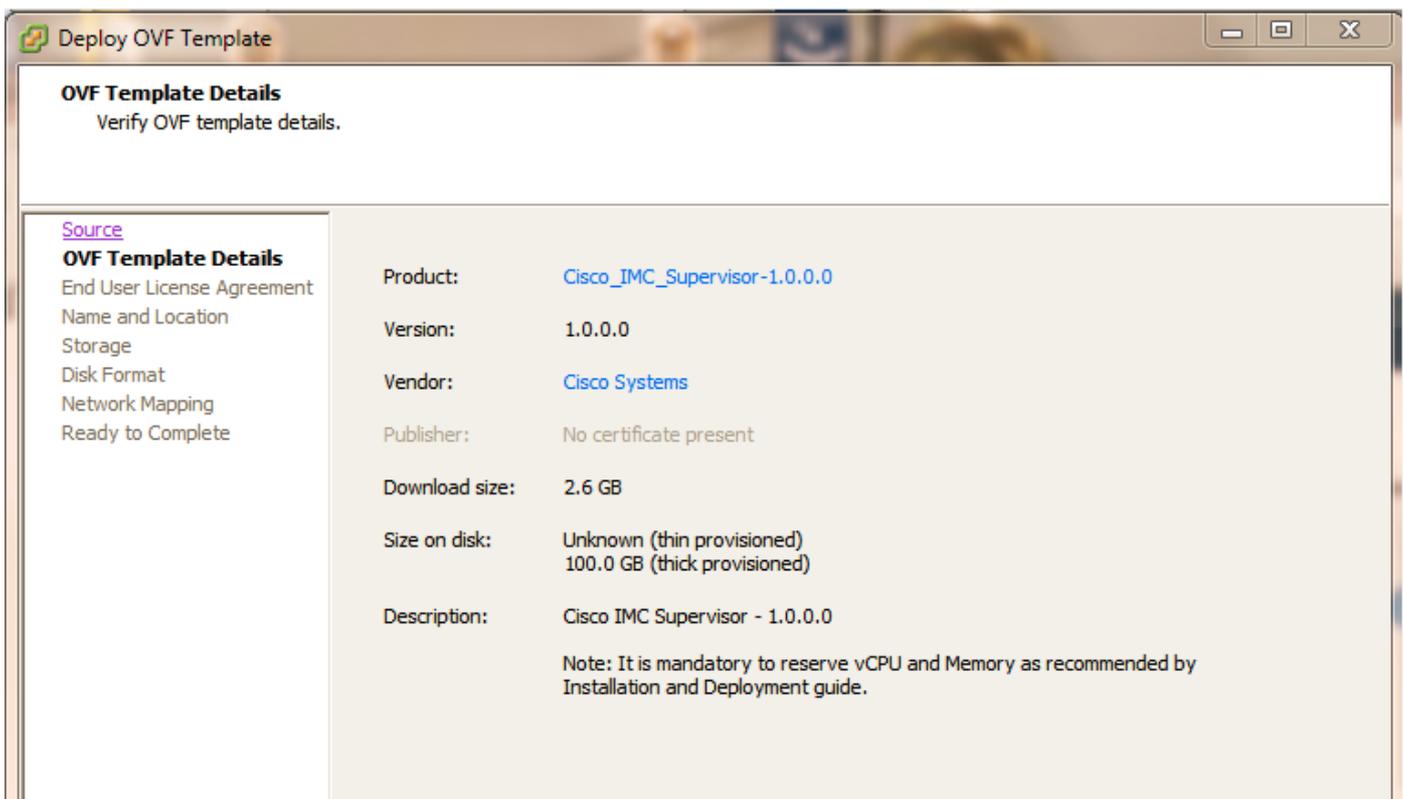
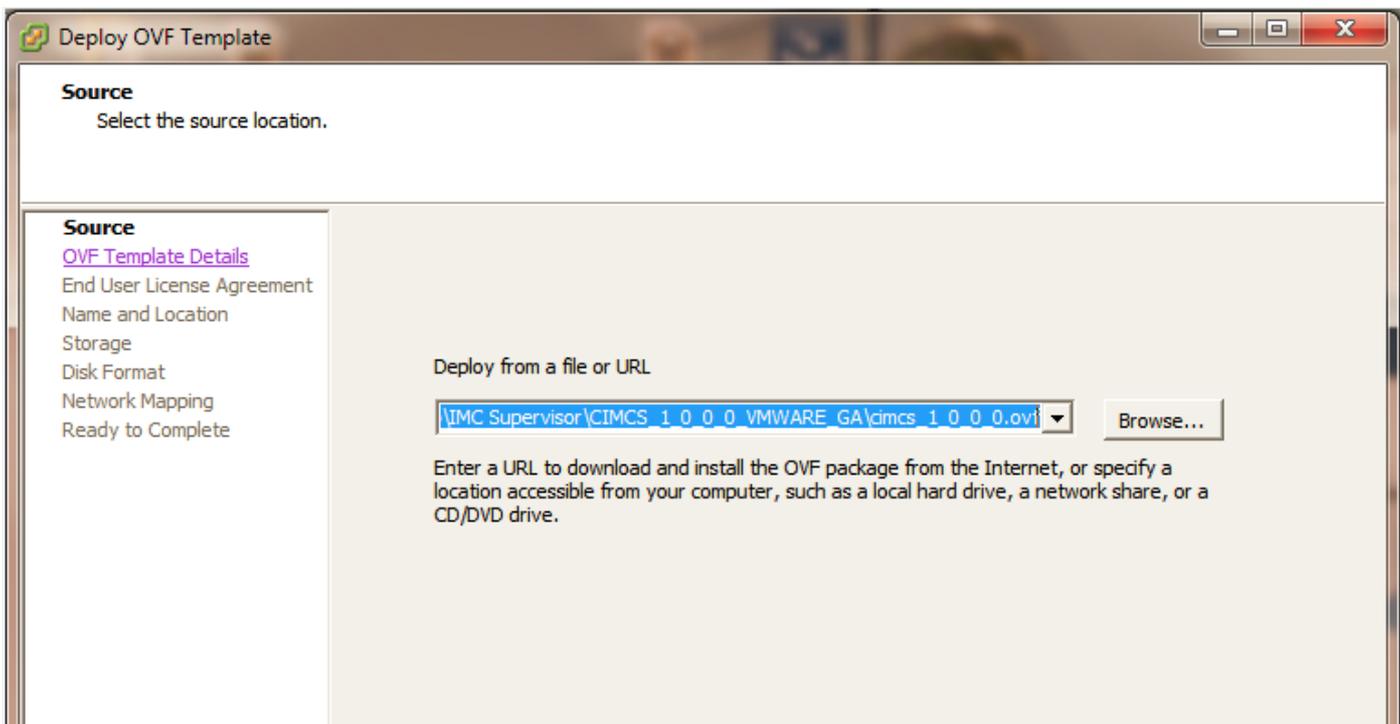
Recent Tasks

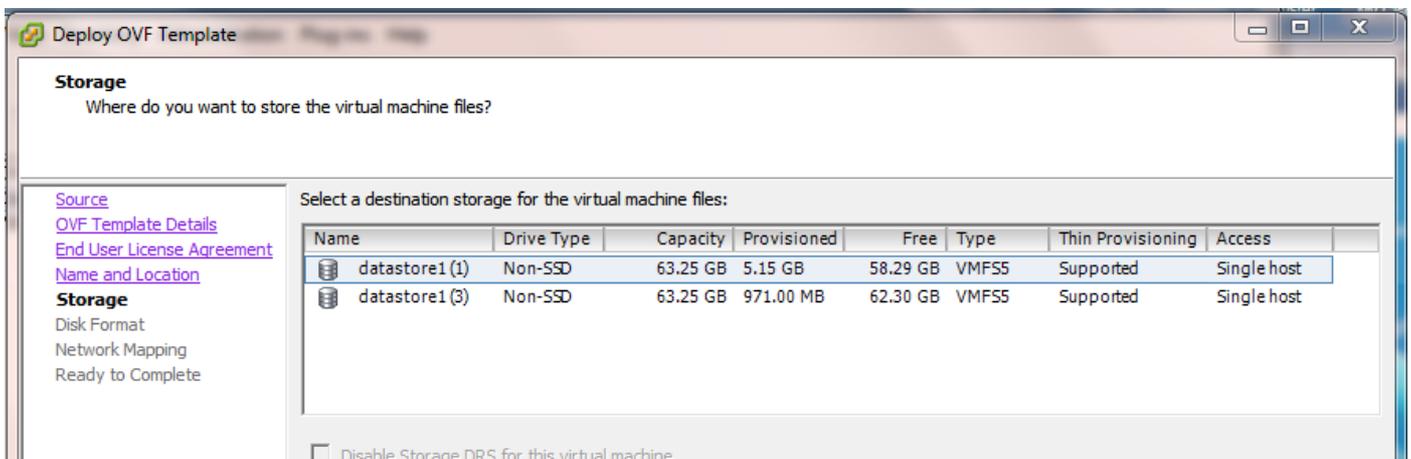
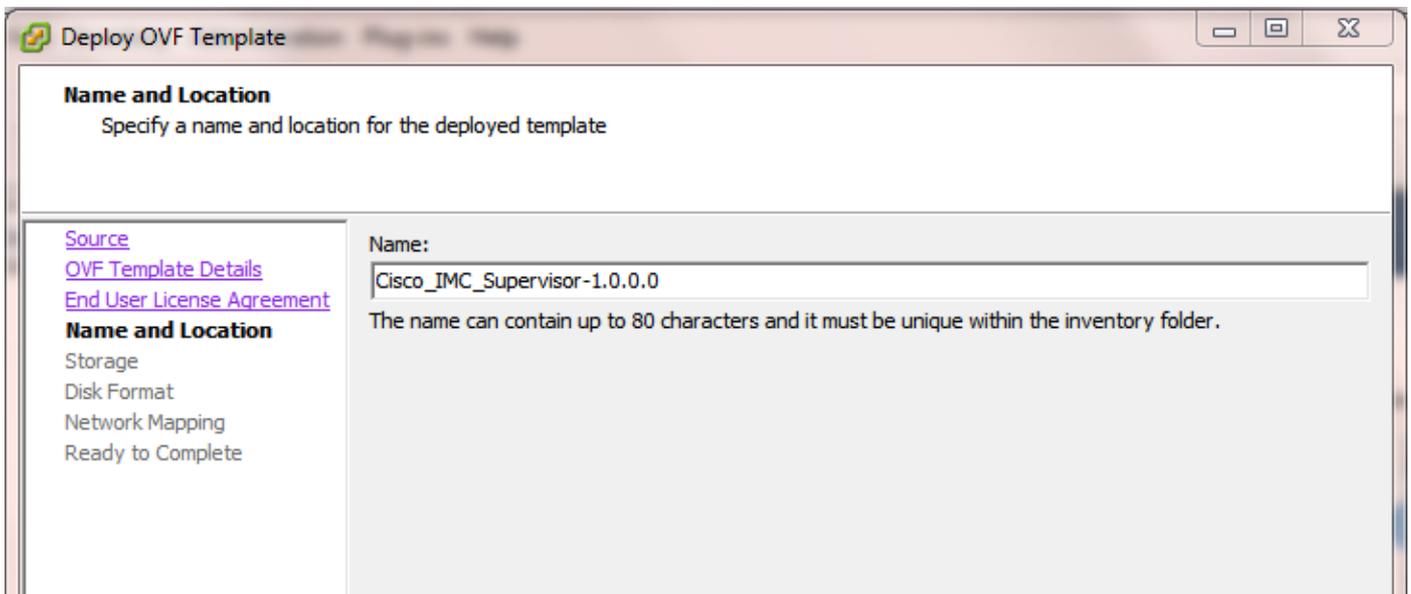
Name, Target or Status contains: Clear X

Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed
------	--------	--------	---------	--------------	-----------------------	------------	-----------

Tasks root

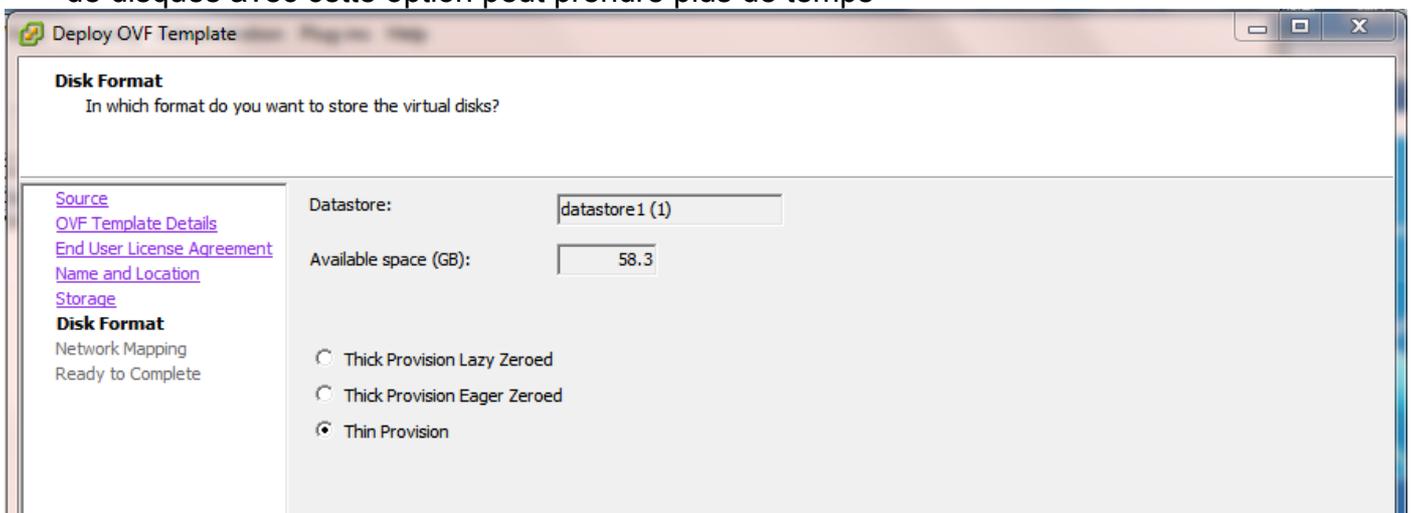
Étape 5. Poursuivez le processus étape par étape afin de déployer le modèle OVF (Open Virtualization Format) comme indiqué dans les images.



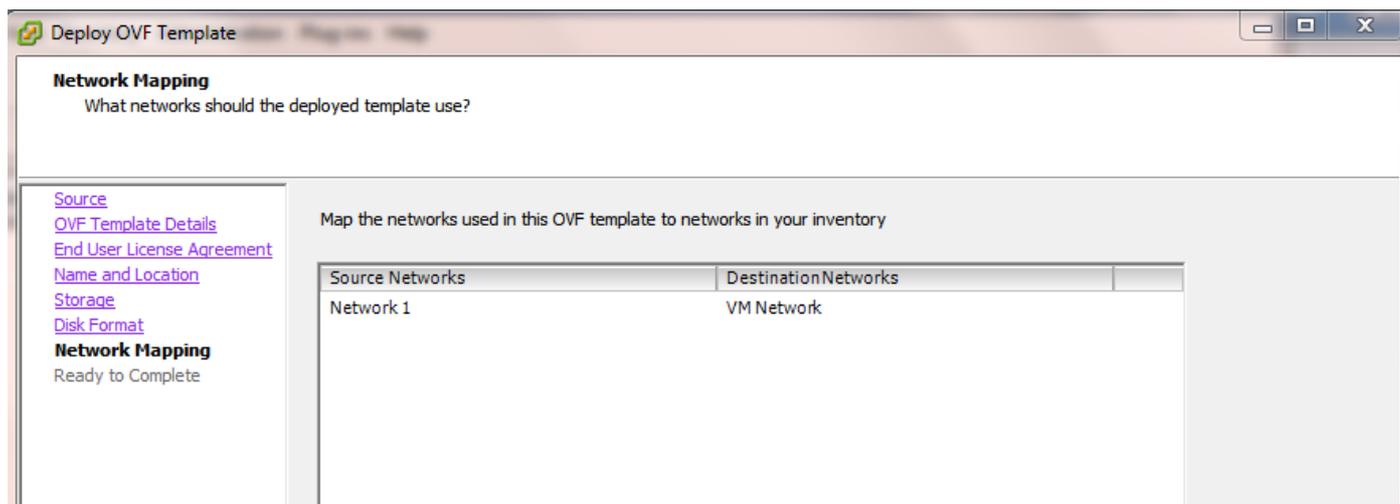


Dans le volet **Format de disque**, sélectionnez l'une des cases d'option et cliquez sur **Suivant** comme indiqué dans l'image.

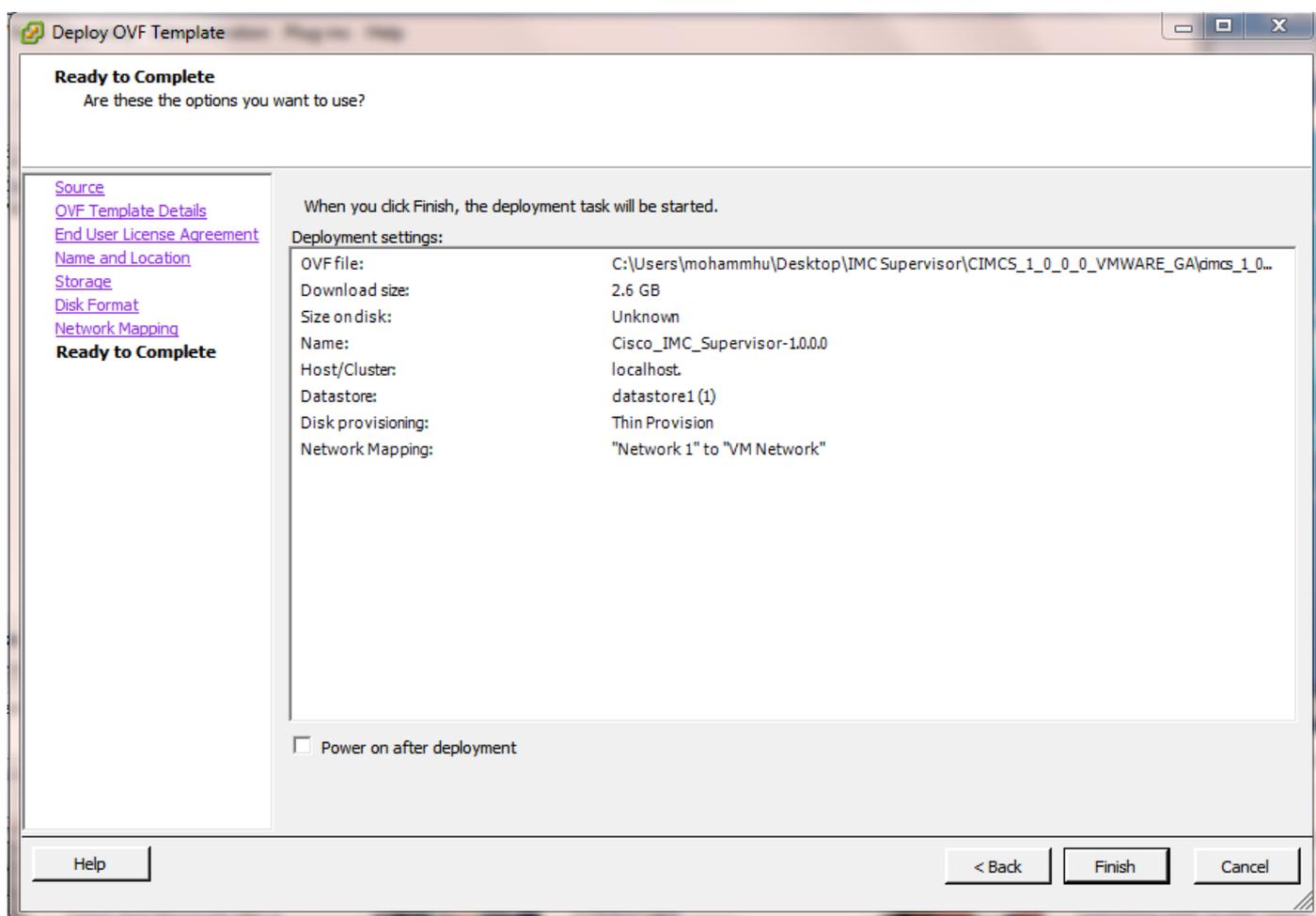
- Provisionnement léger : afin d'allouer le stockage à la demande lorsque les données sont écrites sur le disque
- Lazy Zeroed (Provisionnement épais) : afin d'allouer le stockage immédiatement en format épais
- Épais Provisionnement Eager Zeroed - Afin d'allouer le stockage en format épais. La création de disques avec cette option peut prendre plus de temps



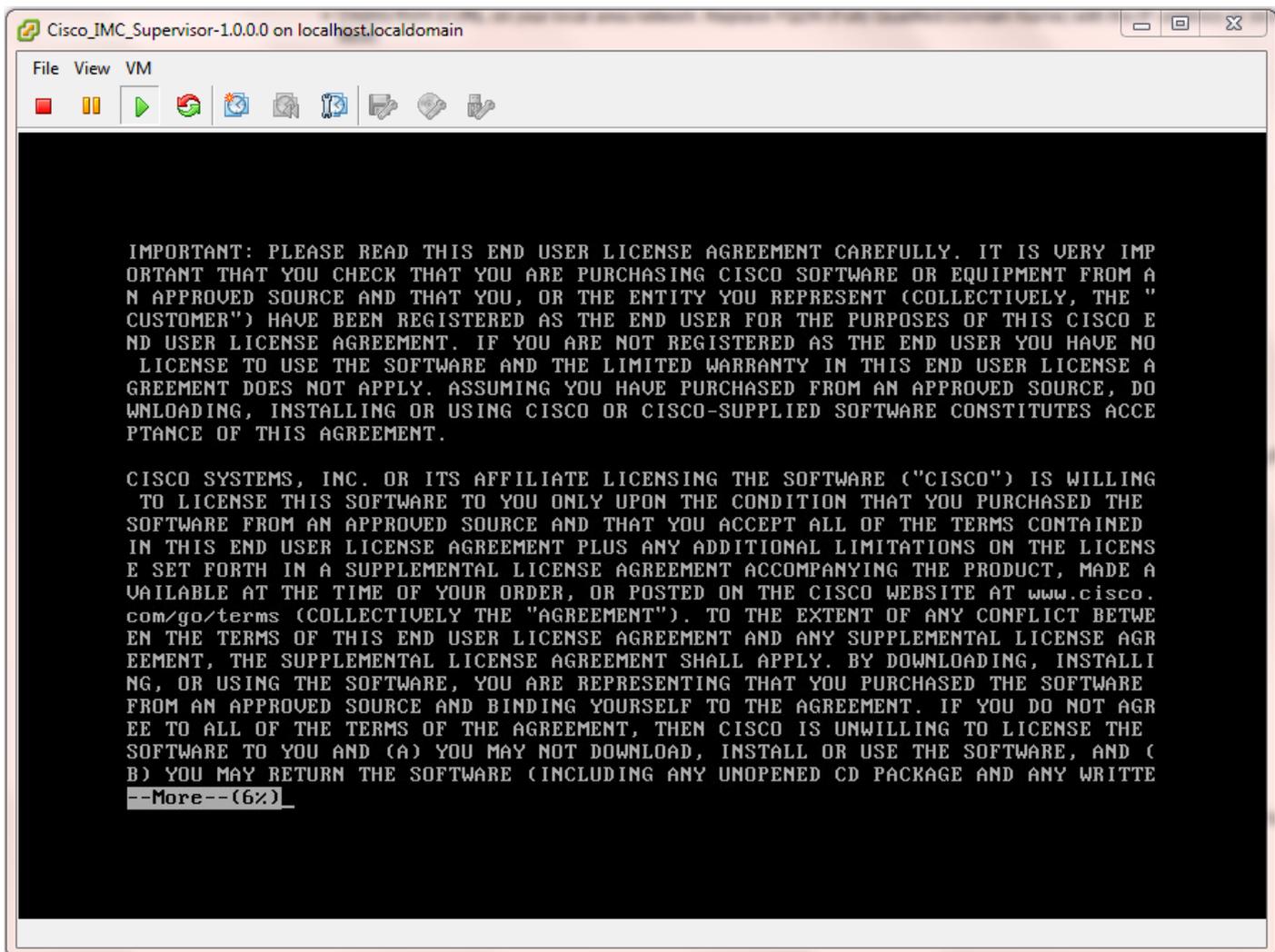
Étape 6. Sélectionnez le groupe de ports approprié pour le réseau de machines virtuelles (VM), comme indiqué dans l'image.



Étape 7. Cliquez sur **Terminer** comme indiqué dans l'image.



Étape 8. Ouvrez la console de la machine virtuelle et **acceptez** le contrat de licence comme indiqué dans l'image.



Étape 9. Une fois terminé, entrez y afin de configurer une adresse IP statique comme indiqué dans l'image.

Étape 10. Si vous voulez utiliser DHCP, entrez n afin de vous assurer que les adresses IP sont attribuées automatiquement.

```
Cisco_IMC_Supervisor-1.0.0.0 on localhost.localdomain
File View VM
not imply a partnership relationship between Cisco and any other company.

Do you agree with the terms of the End User License Agreement?
yes/no [nol]: yes

Regenerating ssh host keys...
openssh-daemon is stopped
Generating SSH1 RSA host key: [ OK ]
Generating SSH2 RSA host key: [ OK ]
Generating SSH2 DSA host key: [ OK ]
Starting sshd: [ OK ]
Regenerating keys for the root user...
Generating public/private rsa key pair.
Created directory '/root/.ssh'.
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
d7:34:b7:18:89:a2:27:3b:45:a6:96:72:97:7d:f3:de root@localhost
Generating SSL certificates for sftpd in /opt/vmware/etc/sftpd
Generating SSL certificates for lighttpd in /opt/vmware/etc/lighttpd
This script is executed on first boot only.
Configuring static IP configuration

Do you want to Configure static IP [y/n]? : y_
```

Étape 11. Si vous souhaitez utiliser une adresse IP statique, saisissez **y**, puis vous êtes invité à sélectionner **IPv4** ou **IPv6**. Entrez **V4** afin de configurer IPv4, puis entrez les informations comme indiqué dans les images :

- Adresse IP Masque de réseau Passerelle

Note: Actuellement, seul IPv4 est pris en charge afin de configurer des adresses IP statiques.

```
Cisco_IMC_Supervisor-1.0.0.0 on localhost.localdomain
File View VM
Regenerating keys for the root user...
Generating public/private rsa key pair.
Created directory '/root/.ssh'.
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
d7:34:b7:18:89:a2:27:3b:45:a6:96:72:97:7d:f3:de root@localhost
Generating SSL certificates for sfcfb in /opt/vmware/etc/sfcfb
Generating SSL certificates for lighttpd in /opt/vmware/etc/lighttpd
This script is executed on first boot only.
Configuring static IP configuration

Do you want to Configure static IP [y/n]? : y
Do you want to configure IPv4/IPv6 [v4/v6] ? : v4

Configuring static IP for appliance. Provide the necessary access credentials

IP Address: 10.104.213.77
Netmask: 255.255.255.0
Gateway: 10.104.213.1

Configuring Network with : IP(10.104.213.77), Netmask(255.255.255.0), Gateway(10.104.213.1)

Do you want to continue [y/n]? : y_
```

```
Cisco_IMC_Supervisor-1.0.0.0 on localhost.localdomain
File View VM
Cisco_IMC_Supervisor-1.0.0.0 - 1.0.0.0
To manage this VM browse to https://10.104.213.77:443/

*Login
Configure Network
Set Timezone (Current:UTC)

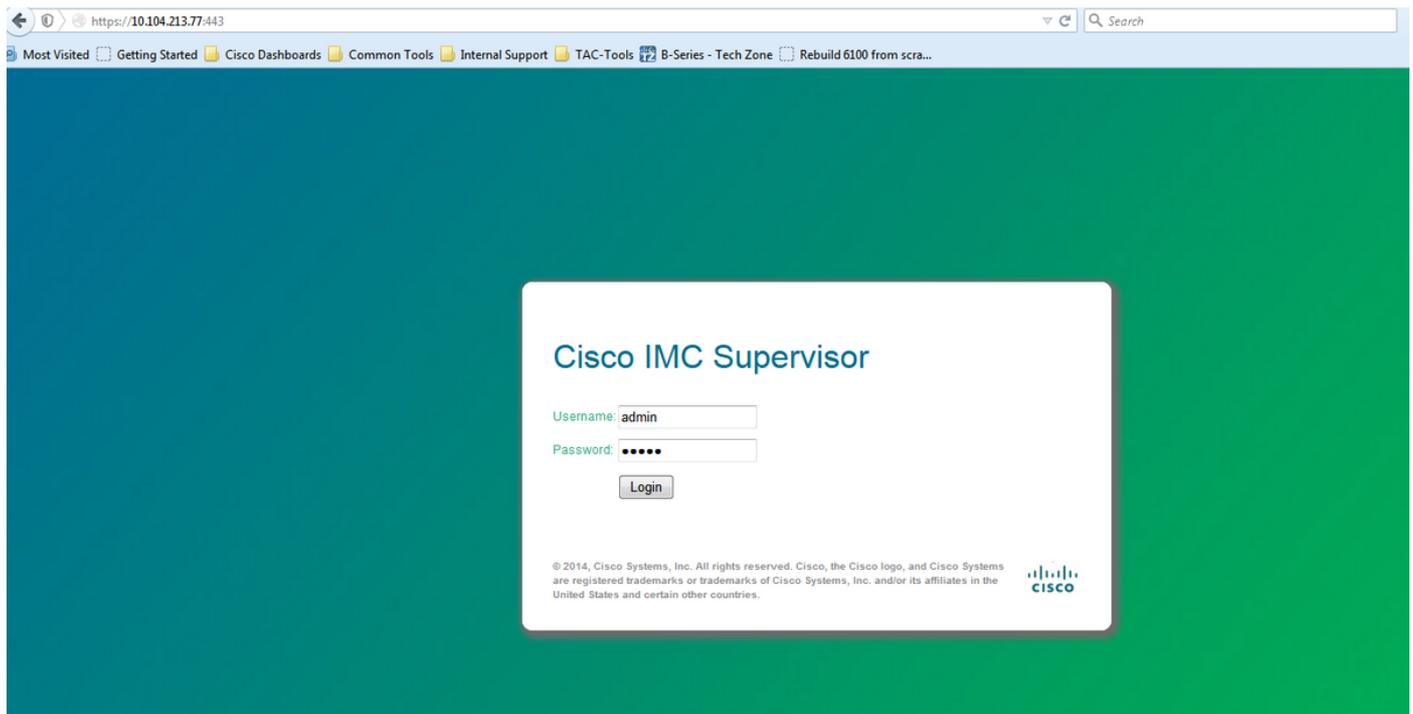
Use Arrow Keys to navigate
and <ENTER> to select your choice.
```

Étape 12. Après le démarrage de l'appliance, transférez l'adresse IP du superviseur Cisco IMC dans un navigateur Web pris en charge afin d'accéder à la page de connexion.

Sur la page Connexion, entrez **admin** comme nom d'utilisateur et **admin** comme mot de passe.

Note: Vous pouvez modifier votre mot de passe admin après cette première connexion.

L'interface utilisateur du superviseur IMC de Cisco est représentée sur l'image.



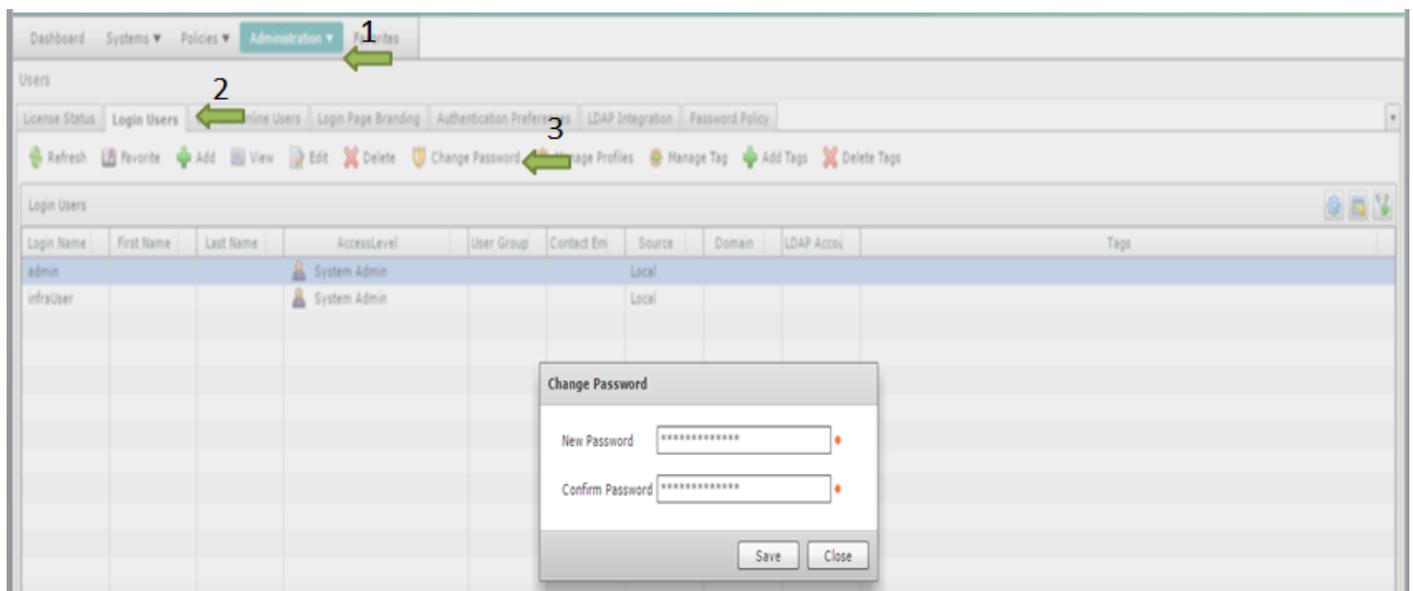
Modifier le mot de passe par défaut

2. Complétez ces étapes afin de modifier le mot de passe par défaut.

Étape 1. Accédez à **Administration > Users**.

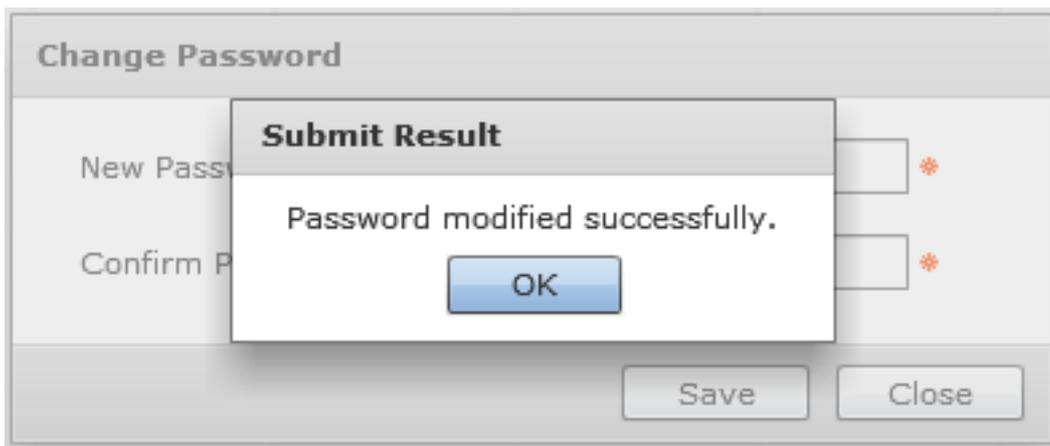
Étape 2. Cliquez sur l'onglet **Utilisateurs de connexion**.

Étape 3. Dans la liste des utilisateurs, sélectionnez le rôle d'utilisateur pour lequel vous souhaitez modifier le mot de passe comme indiqué dans l'image.



Étape 4. Après avoir spécifié le nouveau mot de passe, cliquez sur **Enregistrer** et cliquez sur **OK**

sur le **résultat d'envoi** comme indiqué dans l'image.



Informations de licence

3. Le superviseur IMC de Cisco nécessite que vous ayez ces licences valides :

- Licence de base du superviseur Cisco IMC.
- Licence d'activation de point de terminaison en bloc Cisco IMC Supervisor que vous installez après la licence de base Cisco IMC Supervisor, comme illustré sur l'image.

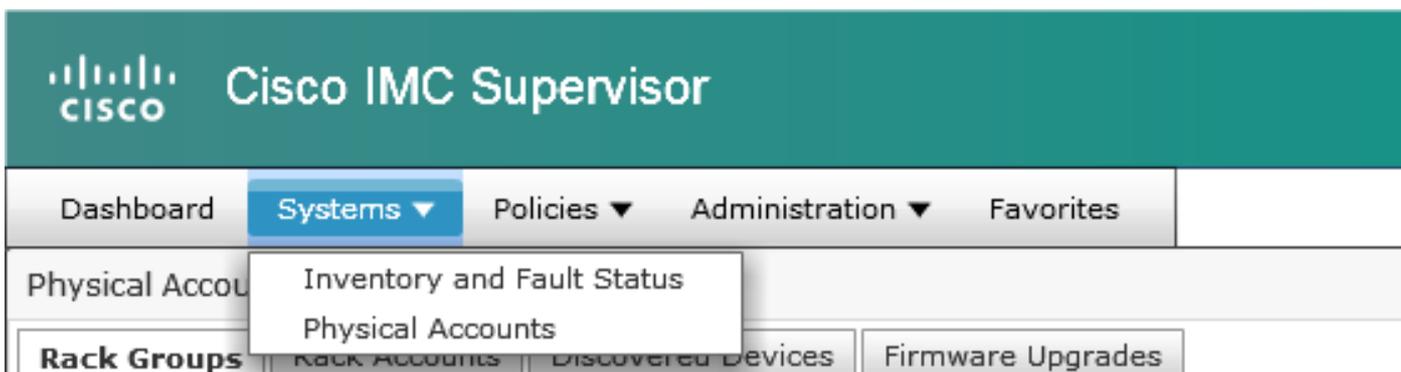
License	Licensed Lim	Available	Used	Status	Remarks
CIMC SUP Base	1		1	✔ Licensed	
Physical Servers	200	200	0	✔ Licensed	Licensed Limit = CIMC-SUP-B01(=2) * 100+ CIMC-SUP-B02(=0) * 250+ CIMC-SUP-B10(=0) * 1000

Note: À moins d'avoir ces licences, les tâches telles que le regroupement de serveurs dans un compte rack, etc., ne peuvent pas être effectuées.

Découvrir le serveur

4. Effectuez ces actions afin de détecter les serveurs.

Étape 1. Accédez à **Système > Comptes physiques > Périphériques découverts** comme indiqué dans l'image.



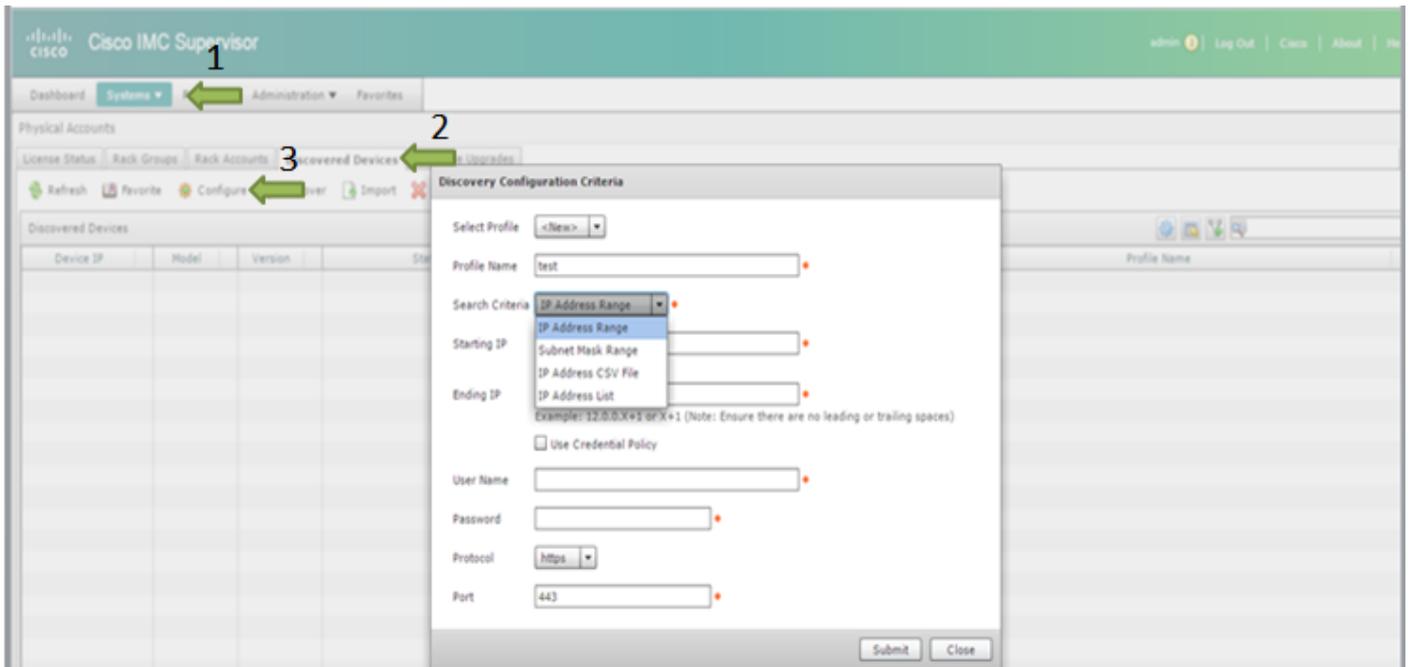
Étape 2. Cliquez sur Configurer.

Étape 3. Dans la boîte de dialogue **Critères de configuration de découverte**, vous pouvez créer un nouveau profil ou modifier un profil existant.

Étape 4. La création d'un **nouveau** profil est illustrée dans l'image.

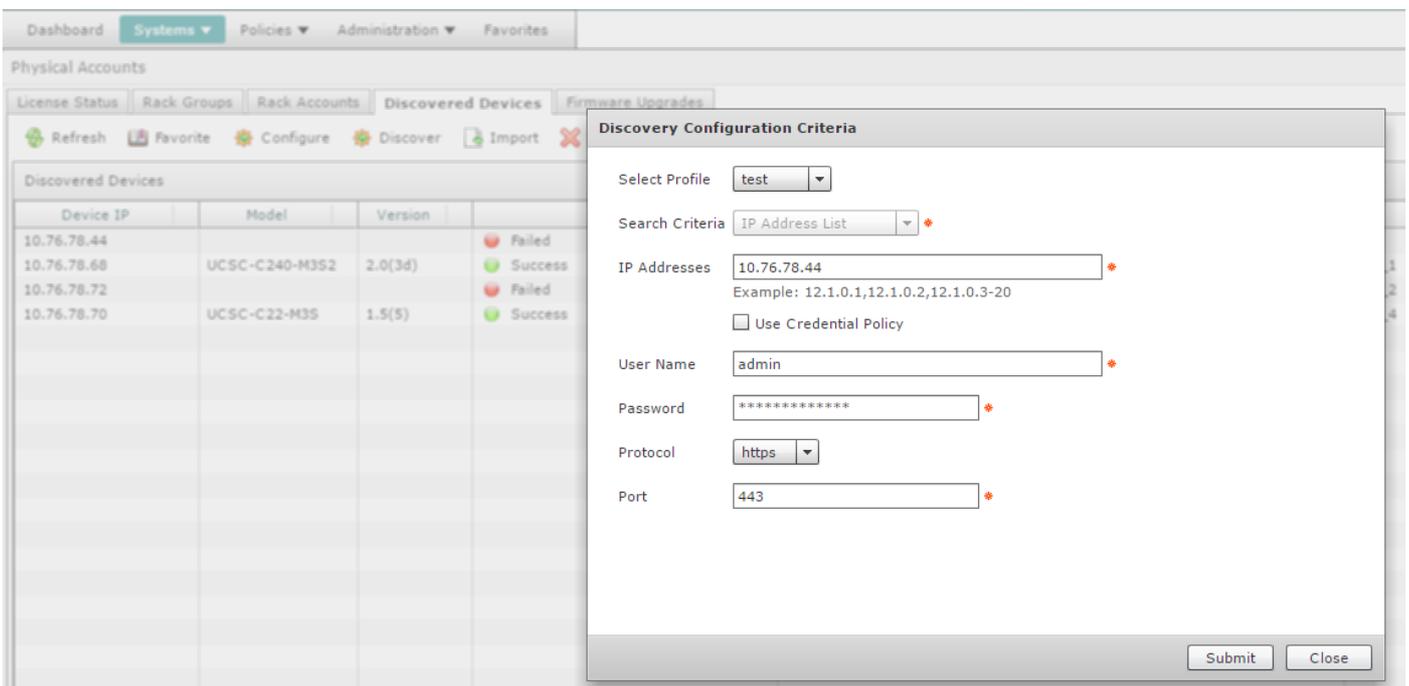
Étape 5. Dans les critères de recherche, vous pouvez choisir la méthode appropriée afin de découvrir les serveurs.

Étape 6. Choisissez **IP Address List**, pour cet exemple.

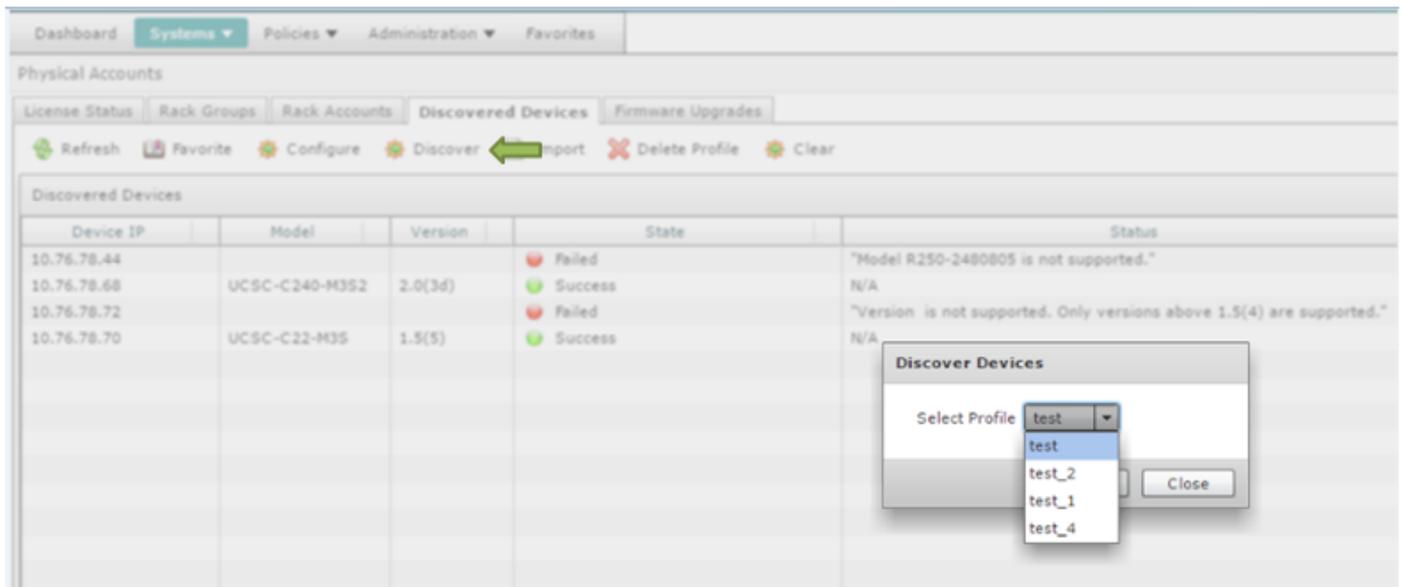


Étape 7. Saisissez l'adresse IP du serveur que vous souhaitez détecter.

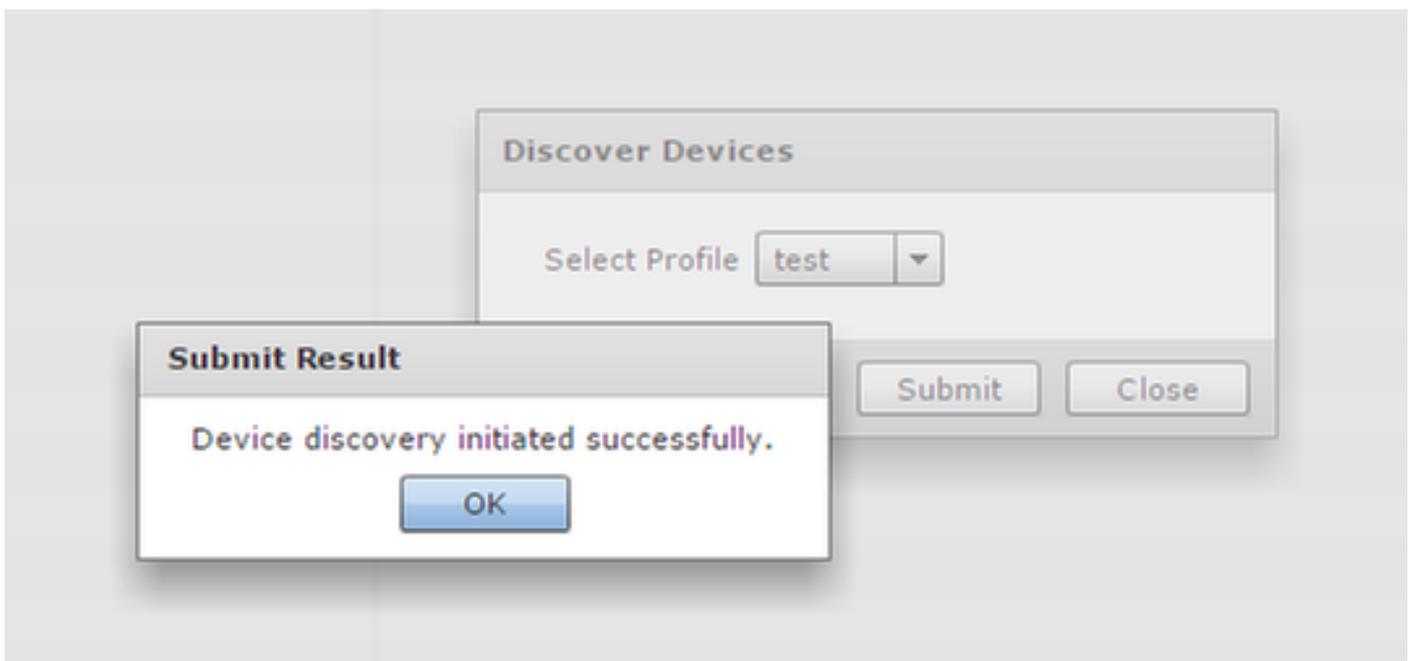
Étape 8. Saisissez le nom d'utilisateur et le mot de passe que vous utilisez pour vous connecter au serveur (informations d'identification CIMC), comme indiqué dans l'image.



Étape 9. Une fois le profil créé, cliquez sur **Découvrir** et sélectionner un profil dans la liste déroulante, comme illustré dans l'image.



Étape 10. Après avoir sélectionné le profil approprié, cliquez sur **Soumettre** et cliquez sur **OK** sur Envoyer le résultat comme indiqué dans l'image.



Étape 11. Si le ou les périphériques de votre profil ne correspondent pas aux critères minimaux pris en charge, la raison pour laquelle le périphérique n'a pas été découvert est indiquée dans la section **État** comme indiqué dans l'image.

Device IP	Model	Version	State	Status	
10.76.78.44			Failed	"Model R250-2480805 is not supported."	test_1
10.76.78.68	UCSC-C240-M3S2	2.0(3d)	Success	N/A	test_2
10.76.78.72			Failed	"Version is not supported. Only versions above 1.5(4) are supported."	test_4
10.76.78.70	UCSC-C22-M3S	1.5(5)	Success	N/A	

Ajouter un groupe de racks

5. Procédez comme suit lorsque vous souhaitez ajouter un nouveau groupe de racks dans le superviseur IMC de Cisco.

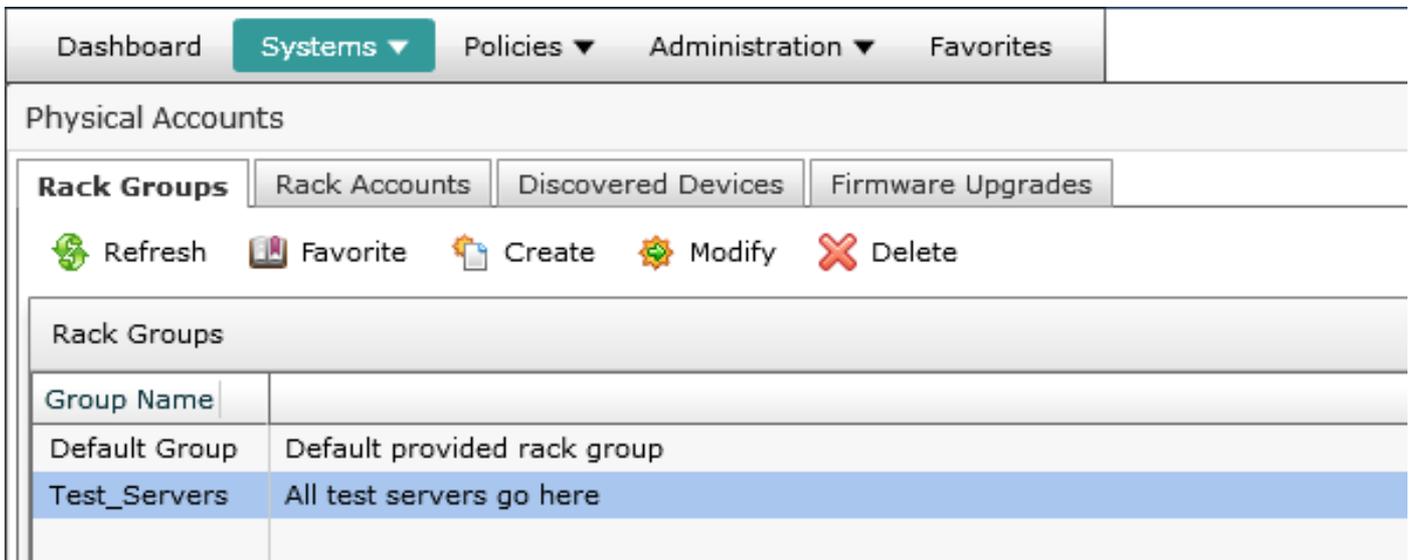
Étape 1. Accédez à **Systèmes > Comptes physiques > Groupes de racks**.

Étape 2. Cliquez sur **Create**.

Étape 3. Spécifiez un **nom de groupe** et une **description** dans la zone Créer un groupe de rack.

Étape 4. Cliquez sur **Créer** comme indiqué dans l'image.

Étape 5. Une fois créé, le nom du groupe doit s'afficher comme indiqué dans l'image.



Ajouter un compte rack

6. Procédez comme suit lorsque vous souhaitez ajouter un nouveau groupe de racks dans le superviseur IMC de Cisco.

Étape 1. Dans la barre de menus, sélectionnez **Système**.

Étape 2. Cliquez sur l'onglet.

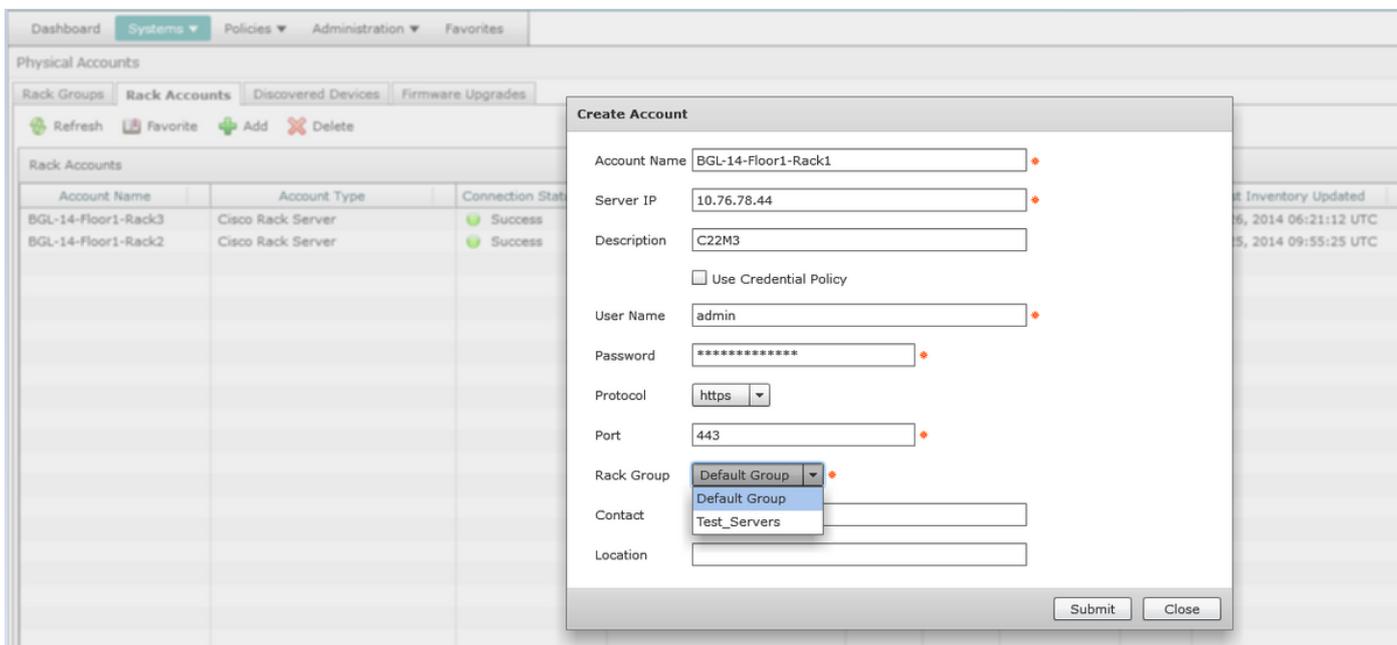
Étape 3. Cliquez sur.

Étape 4. Dans la boîte de dialogue Créer un compte, renseignez les champs suivants :

Champ	Description
champ	Nom descriptif du compte rack
champ	Adresse IP du serveur de montage en rack
Champ Description	(Facultatif) Description du compte rack
case à cocher	(Facultatif) Si vous avez déjà créé des stratégies d'informations d'identification, cochez cette case afin de sélectionner la stratégie dans la liste déroulante.
Si vous cochez la case	
liste déroulante	Choisissez une stratégie dans la liste déroulante
Si vous décochez la case	
champ	ID de connexion du serveur de montage en rack
Champ Mot de passe	Mot de passe de l'ID de connexion du serveur de montage en rack
Liste déroulante Protocole	Choisissez https ou http dans la liste
Champ Port	Numéro de port associé au protocole sélectionné
Liste déroulante Groupe de racks	Sélectionnez un groupe de racks dans la liste.
Champ Contact	(Facultatif) Adresse e-mail du contact pour le compte
Champ Emplacement	(Facultatif) Emplacement du compte

Étape 1. Dans la liste déroulante du groupe de racks, vous pouvez choisir le **groupe par défaut** ou le groupe défini précédemment, comme indiqué dans l'image.

Étape 2. Une fois cette action terminée, les serveurs spécifiés doivent se trouver sous le groupe de racks que vous sélectionnez.



Configuration de la messagerie

7. Suivez cette procédure afin de configurer votre message de configuration.

Étape 1. Accédez à **Administration > Mail Setup**.

Étape 2. Saisissez les détails demandés.

Étape 3. Vous pouvez cocher la case **Envoyer un e-mail de test** et vérifier si vous avez reçu le message de test sur l'adresse e-mail que vous avez fournie, comme indiqué dans l'image.

[Dashboard](#)[Systems ▼](#)[Policies ▼](#)[Administration ▼](#)[Favorites](#)

System

[System Information](#)**Mail Setup**[System Tasks](#)[User Roles](#)[Email Alert Rules](#)

Outgoing Email Server (SMTP)



Outgoing SMTP Port



Outgoing SMTP User

Outgoing SMTP Password

Outgoing Email Sender Email Address



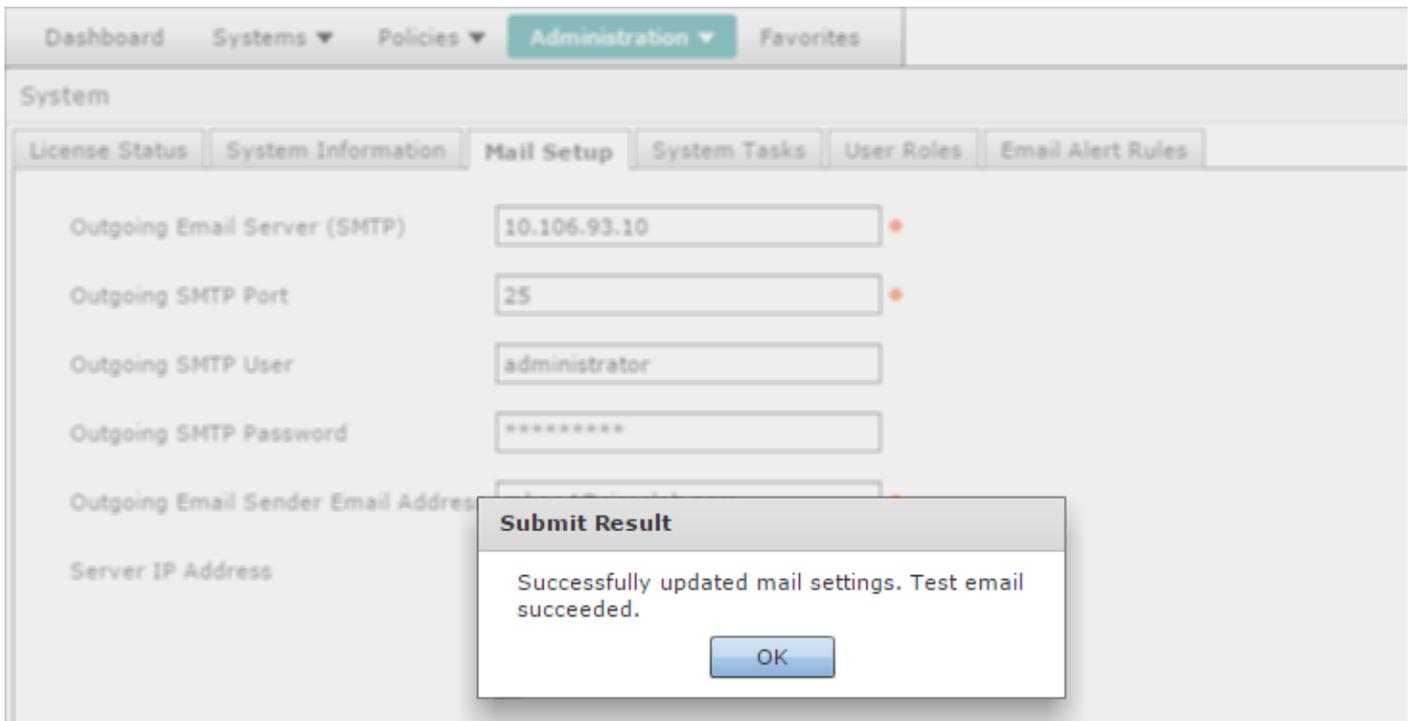
Server IP Address

 Send Test Email

Test Email Address

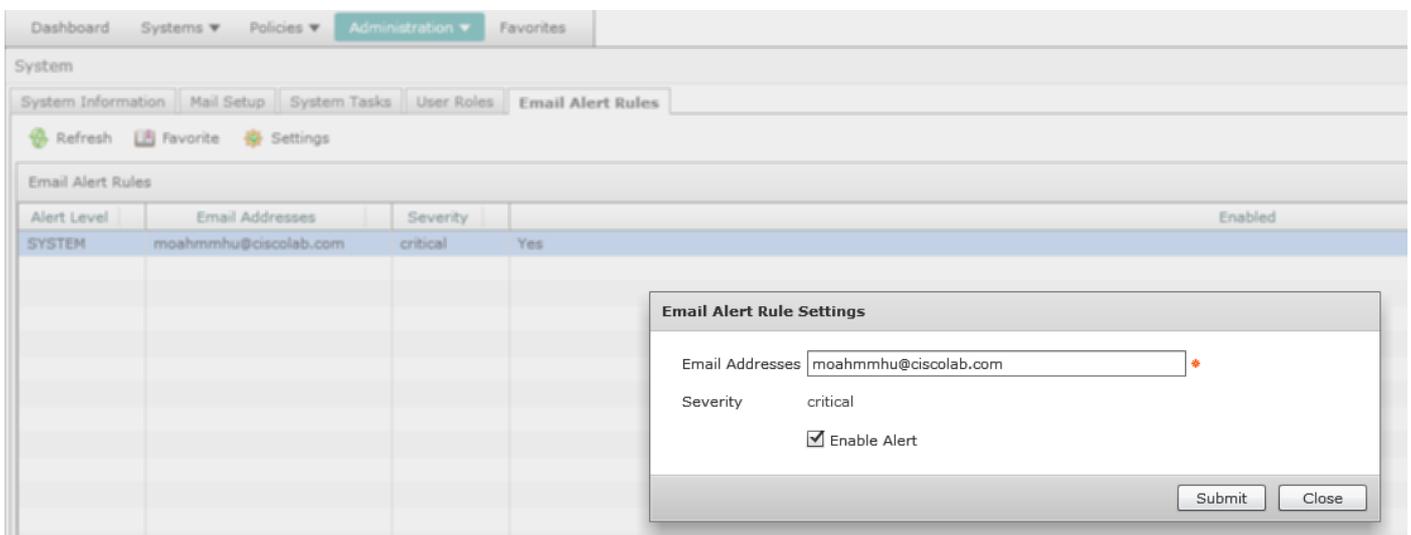


Étape 4. Vous devez ensuite recevoir le message de test comme indiqué dans l'image.



Étape 5. Dans la même section, accédez à **Paramètres des règles d'alerte par e-mail** et cochez la case **Activer l'alerte** comme indiqué dans l'image.

Note: À ce stade (avec la version 1.0 de Cisco IMC Supervisor), les notifications pour les pannes critiques et de niveau supérieur sont prises en charge.



Étape 6. Si votre système rencontre une erreur critique, vous devez recevoir un message comme indiqué dans l'image, à condition que la configuration de votre courrier fonctionne correctement.

Server IP	Host name	Severity	Code	Cause	Description	Created	Affected DN
10.76.78.70	bgl-sv-c22-m3-01	critical	F1007	equipment-inoperable	Storage Virtual Drive 0 is inoperable: Check storage controller, or reseal the storage drive	Thu Dec 25 12:10:19 2014	sys/rack-unit-1/board/storage-SAS-SLOT-2/vd-0

Mise à niveau du micrologiciel

8. Procédez comme suit lorsque vous souhaitez mettre à niveau le micrologiciel.

Étape 1. Accédez à **Systèmes > Comptes physiques**.

Étape 2. Cliquez sur l'onglet.

Étape 3. Cliquez sur **Configurer le profil**.

Étape 4. Dans la boîte de dialogue **Télécharger le micrologiciel**, vous pouvez créer un nouveau profil ou modifier un profil existant.

Champ

Champ
liste déroulante

champ
champ
case à cocher

Case à cocher Activer
l'authentification proxy

Liste déroulante Plate-forme
liste déroulante

Description

Sélectionnez **Nouveau** dans la liste déroulante.

Nom descriptif du profil.

Choisissez l'une des options suivantes :

- Serveur HTTP local : l'image .iso est stockée dans le superviseur IMC local de Cisco.
- Chemin d'accès au réseau : l'image .iso est stockée dans le réseau.

Saisissez votre nom d'utilisateur de connexion Cisco.

Saisissez votre mot de passe de connexion Cisco.

(Facultatif) Cochez cette case afin d'activer la configuration du proxy et renseignez les champs suivants :

- Champ Nom d'hôte : saisissez un nom d'hôte pour la configuration du proxy.
- Champ Port : saisissez le port pour la configuration du proxy.

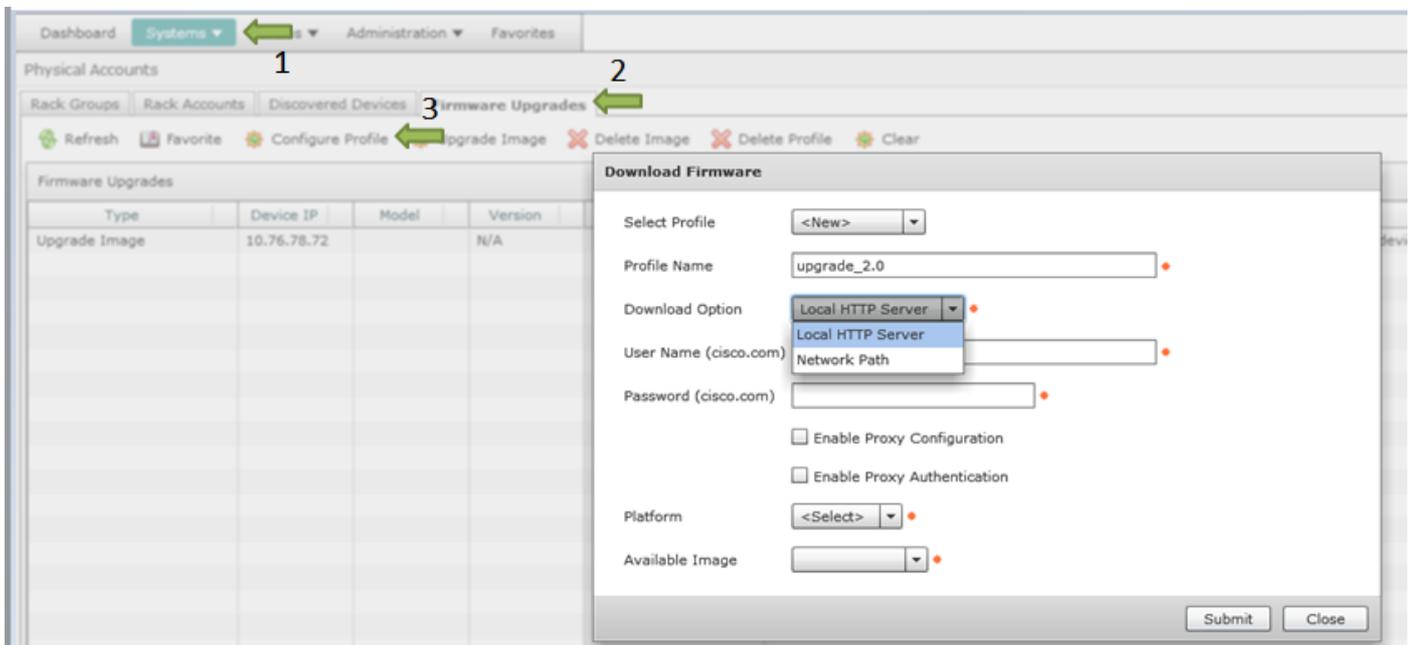
(Facultatif) Cochez cette case afin d'activer l'authentification proxy et renseignez les champs suivants :

- Champ Nom d'utilisateur du proxy : saisissez un nom d'utilisateur du proxy pour l'authentification du proxy.
- Champ Proxy Password (Mot de passe du proxy) : saisissez le mot de passe du nom d'utilisateur du proxy.

Sélectionnez une plate-forme dans la liste déroulante.

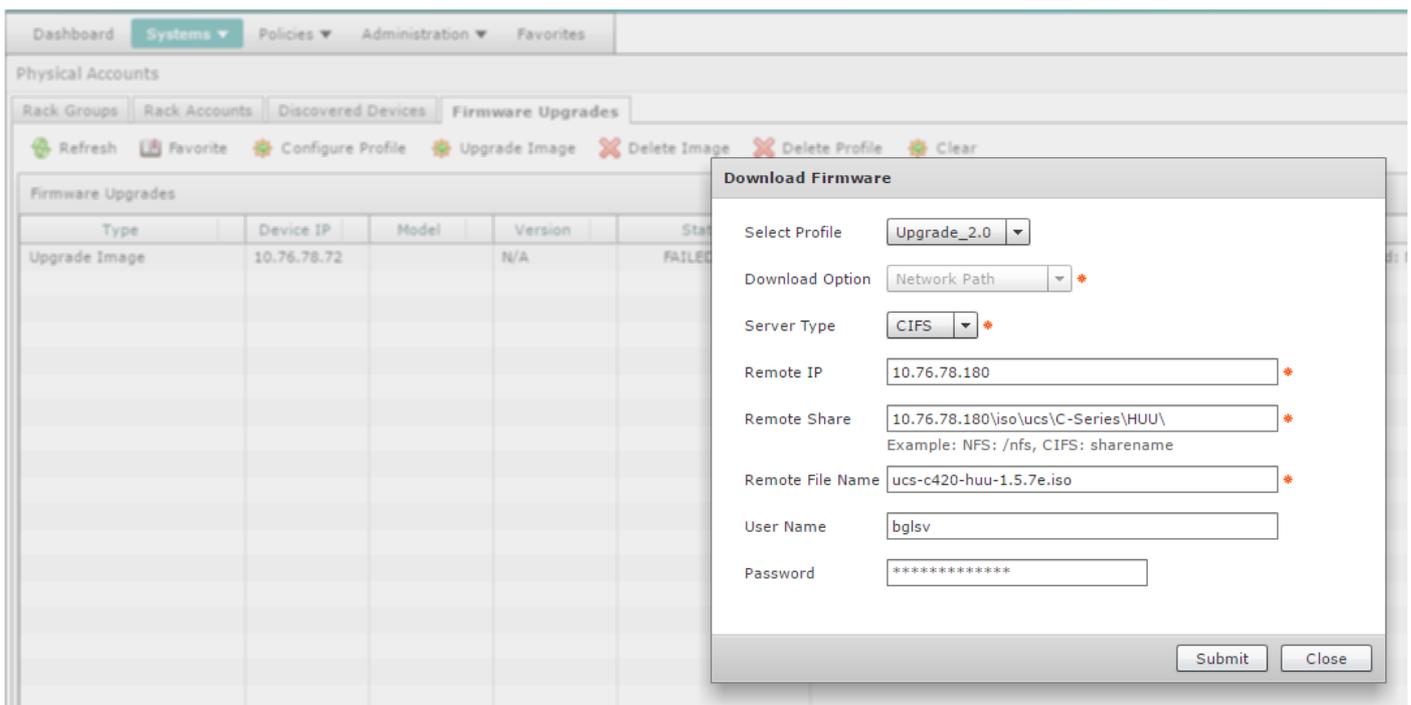
Sélectionnez l'image .iso dans la liste déroulante.

Étape 5. Configurez un **nouveau** profil comme indiqué dans l'image.



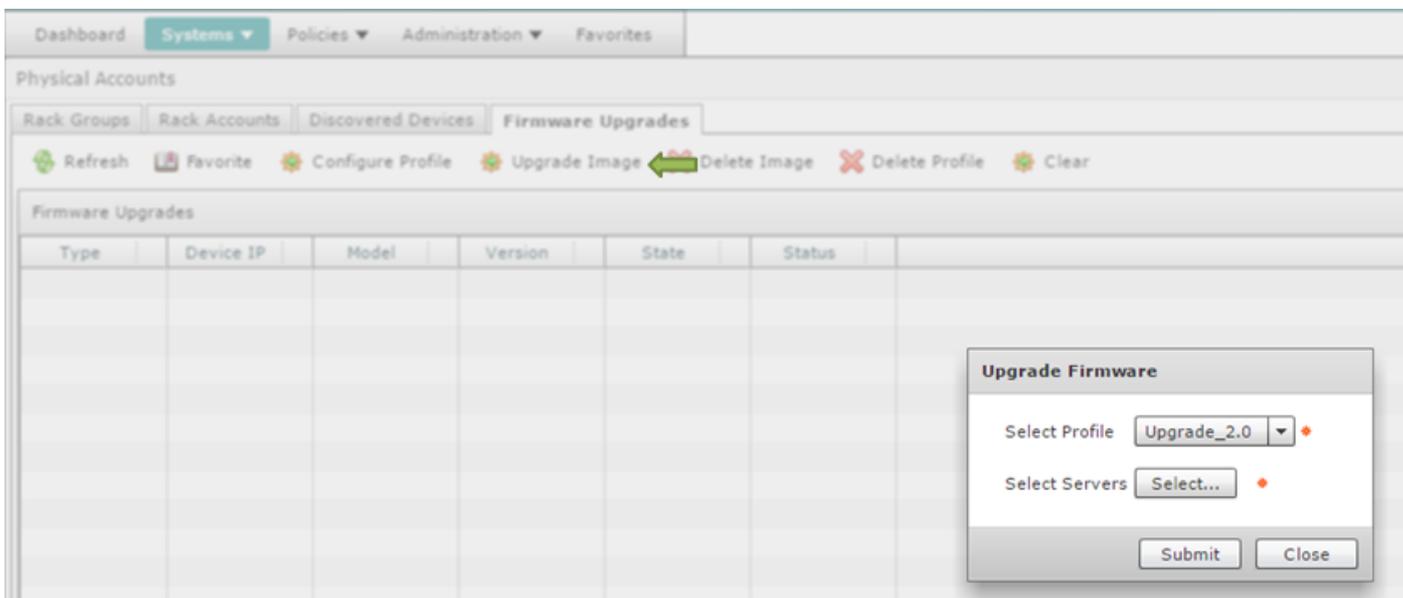
Étape 6. Choisissez **Chemin d'accès réseau** comme option de téléchargement pour cet exemple. (Vous avez CIFS et NFS comme options)

Étape 7. Cliquez sur **Soumettre** comme indiqué dans l'image.



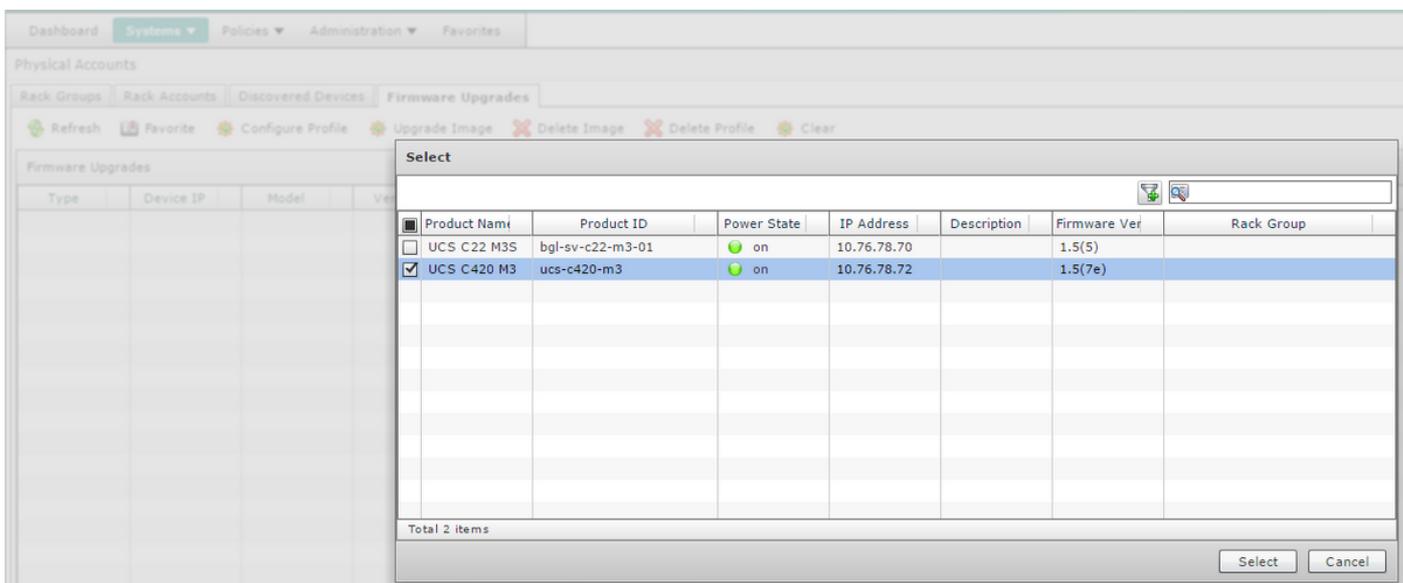
Étape 8. Cliquez sur **Mettre à niveau l'image**.

Étape 9. Cliquez sur **Sélectionner...** afin de sélectionner les serveurs que vous voulez mettre à niveau comme indiqué dans l'image.



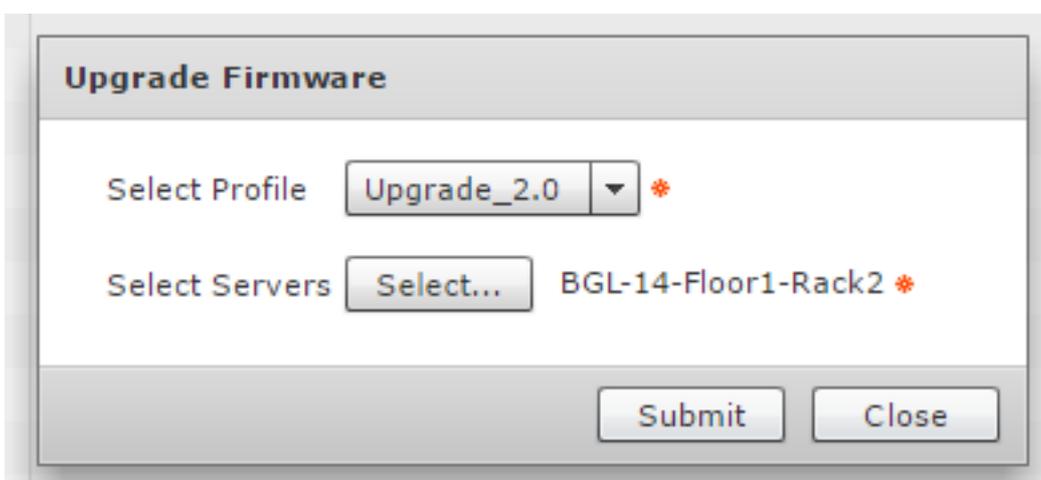
Étape 10. Un seul serveur est sélectionné pour cet exemple.

Étape 11. Cliquez sur **Sélectionner** comme indiqué dans l'image.



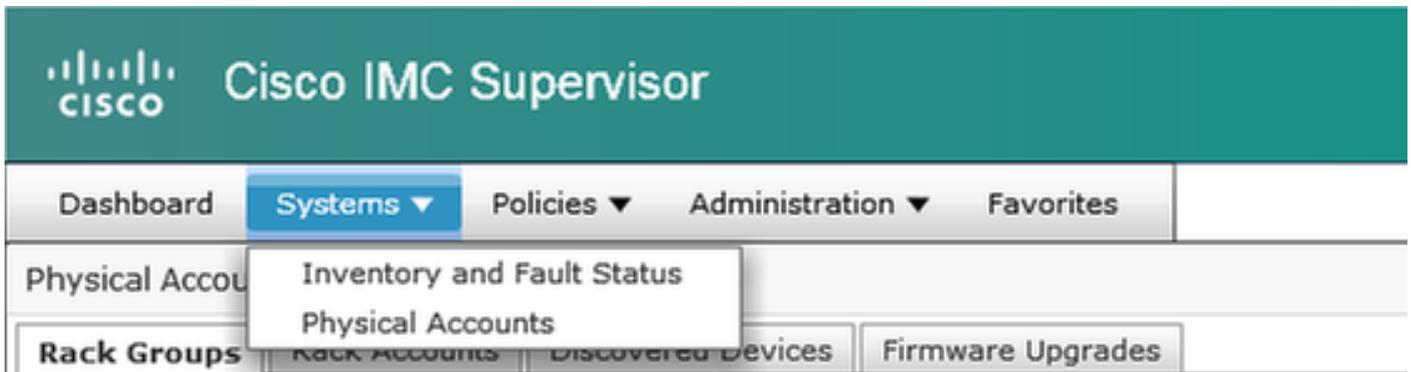
Étape 12. Le serveur sélectionné s'affiche.

Étape 13. Cliquez sur **Soumettre** comme indiqué dans l'image.



Note: Si vous mettez à niveau Cisco IMC version 2.0(x), vous devez modifier le mot de passe Cisco IMC par défaut.

Étape 14. Afin de vérifier l'état de la mise à niveau, accédez à **System > Inventory and Fault Status** comme indiqué dans l'image.



Étape 15. Développez **Groupes de racks**, choisissez le groupe approprié dans lequel les serveurs ont été renseignés plus tôt.

Étape 16. Cliquez sur **Serveurs rack** et choisissez le serveur approprié.

Étape 17. Une fois cette opération effectuée, une ligne supplémentaire avec des options distantes doit apparaître.

Étape 18. Cliquez sur **Console KVM** à partir de cette ligne et vous pouvez voir la mise à niveau en action comme l'illustre l'image.



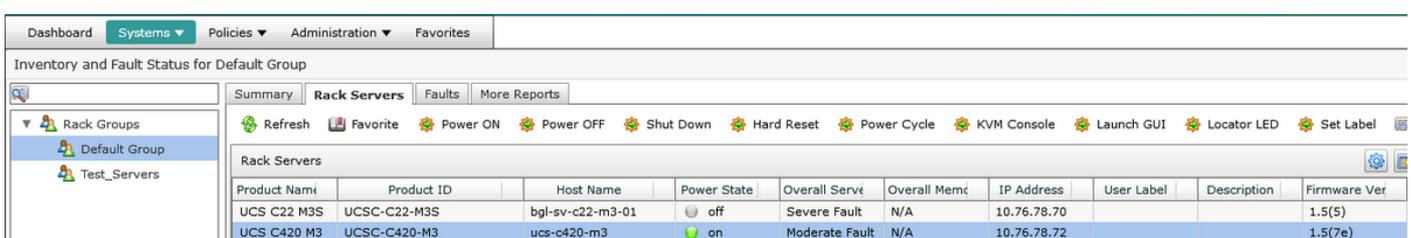
Exporter les données d'assistance technique vers un serveur distant

9. Effectuez ces actions afin d'extraire les données d'assistance technique.

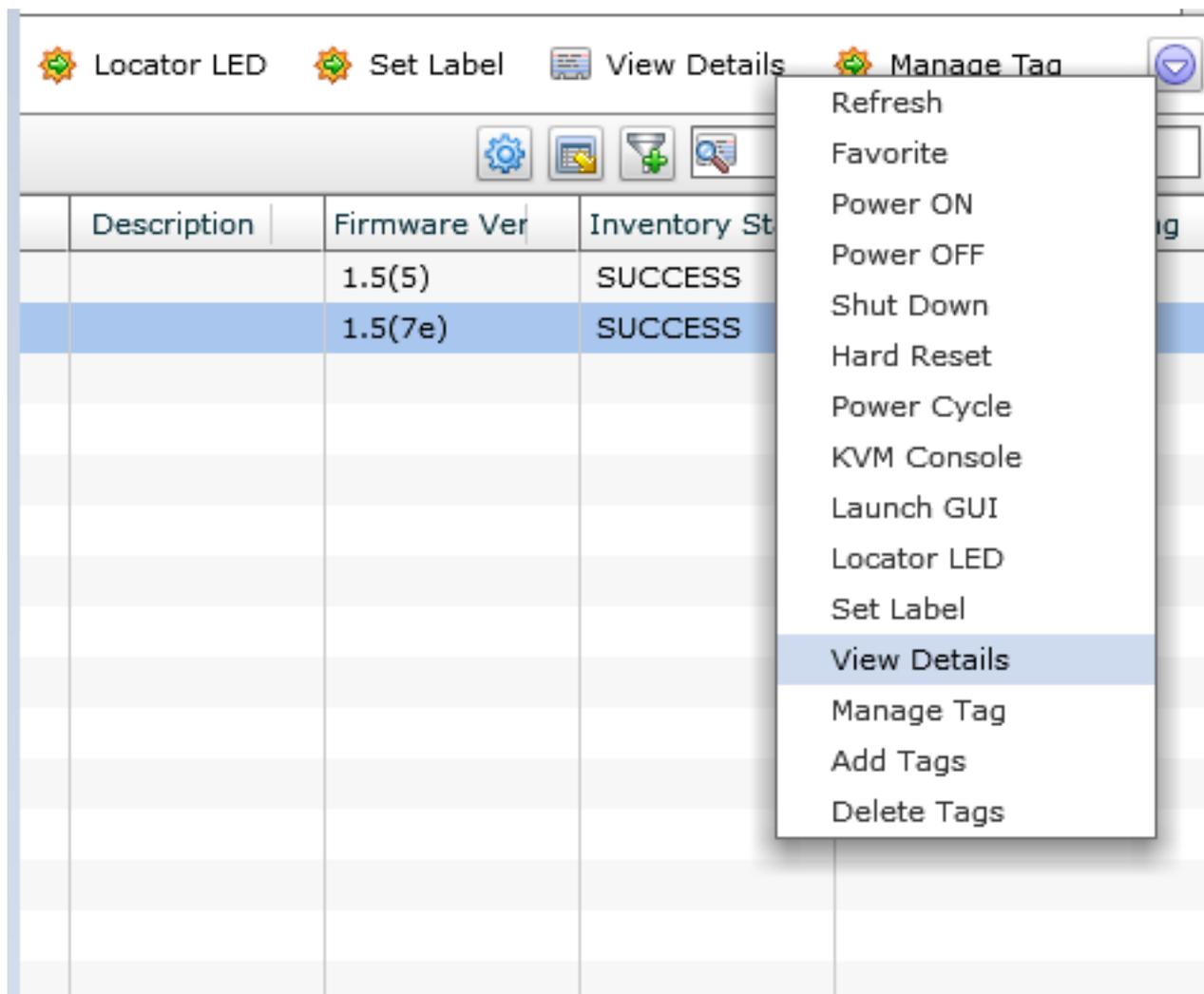
Étape 1. Accédez à **Systèmes > Inventaire et état des pannes pour le groupe par défaut**.

Étape 2. Développez **Groupes de racks** et sélectionnez le groupe de racks qui contient le ou les serveurs.

Étape 3. Sélectionnez l'onglet **Serveurs rack** comme indiqué dans l'image.

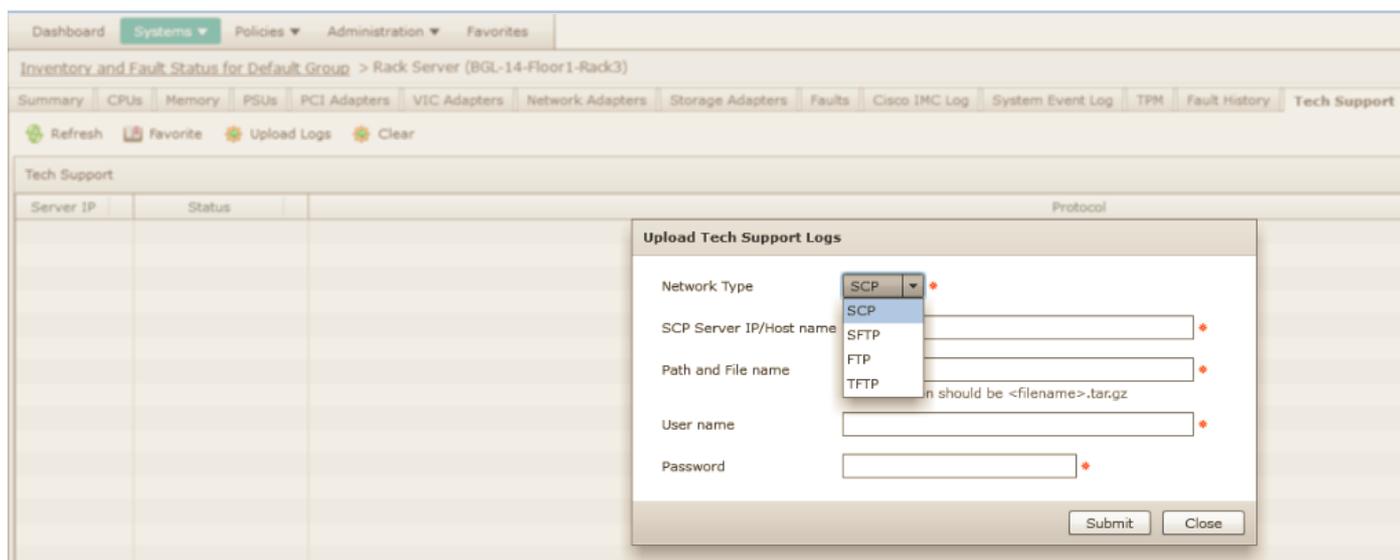


Étape 4. Double-cliquez sur le serveur dans la liste afin d'afficher les détails ou cliquez sur le serveur dans la liste, puis dans la flèche vers le bas à droite, cliquez sur **Afficher les détails** comme indiqué dans l'image.



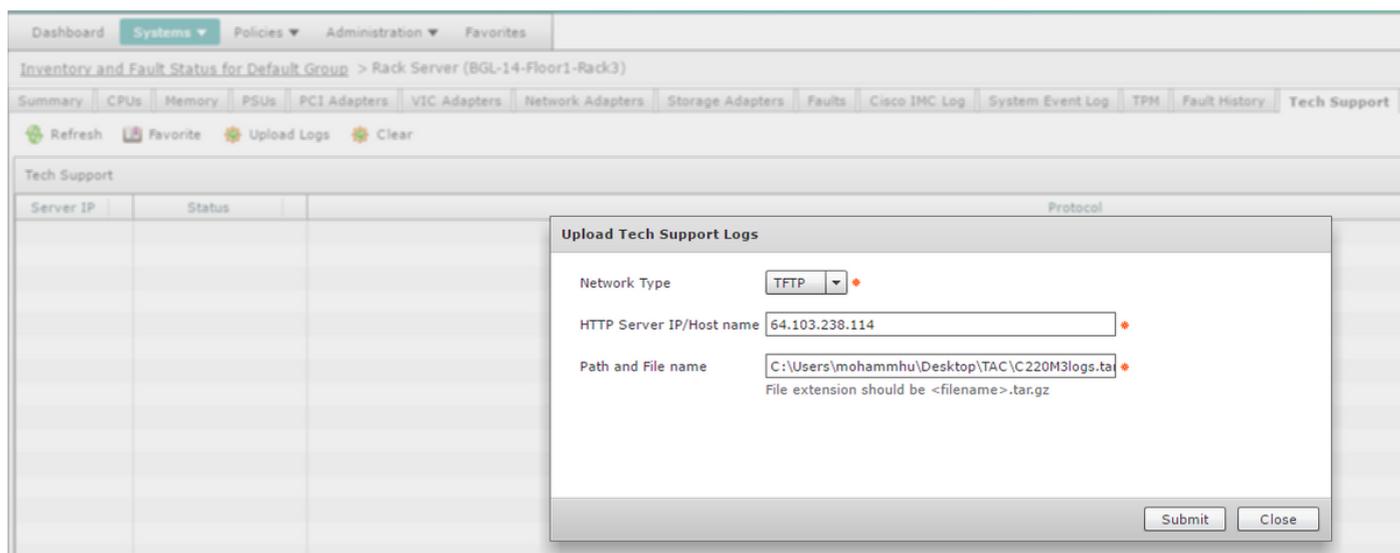
Étape 5. Cliquez sur l'onglet **Support technique**.

Étape 6. Choisissez le type de réseau approprié afin de télécharger les fichiers comme indiqué dans l'image.



Étape 7. Choisissez **TFTP** pour cet exemple.

Étape 8. Cliquez sur **Soumettre** comme indiqué dans l'image.



Étape 9. La capture d'écran montre que les journaux ont été téléchargés avec succès à l'emplacement spécifié.



Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.