Dépannage de la réinitialisation du mot de passe utilisateur Maglev

Table des matières

- Introduction
- Environnement
  - Détails sur l'appliance physique On-Prem
  - Détails ESXi de l'appliance virtuelle
  - Composants utilisés
- Résolution
  - Étape 1: Confirmer l'accès et sélectionner le workflow correct
  - Étape 1a : Démarrage à partir d'un CD Live sur site
  - Étape 1b : Démarrage à partir d'un CD-ROM en direct VA - ESXi
  - Étape 2a: Charger dans l'ISO Ubuntu
  - Étape 2b : Montage des partitions requises
  - Étape 3: Sélectionnez l'action de récupération (Déverrouiller le compte ou Réinitialiser le mot de passe)
  - Étape 3a: Vérifiez si le compte Maglev est verrouillé
  - Étape 3b: Echec de la réinitialisation
  - Étape 3c : Réinitialiser le mot de passe utilisateur Maglev
  - Étape 3d : Redémarrer normalement sur l'environnement Cisco Catalyst Center
  - Étape 3e : Mettre à jour le mot de passe utilisateur Maglev depuis la CLI Cisco Catalyst Center
- Motif
- Autres informations utiles
  - Guide vidéo étape par étape

Introduction

Ce document décrit comment déverrouiller ou réinitialiser le mot de passe pour l'utilisateur Maglev.

Environnement

Cette opération s'applique aux déploiements VMware ESXi d'appareils physiques et virtuels sur site.

Détails sur l'appliance physique On-Prem

- Téléchargez une image ISO Ubuntu 18.04 ou ultérieure depuis la page de téléchargement d'Ubuntu Desktop. Ubuntu 18.04 est recommandé car la version du site est identique à celle du Cisco Catalyst Center.
- Après avoir téléchargé l'ISO sur le système local, montez-le sur le KVM du contrôleur de gestion intégré Cisco (CIMC).
- Après avoir monté l'ISO sur le KVM, démarrez à partir de l'ISO.
- Une fois Ubuntu accessible, montez les répertoires racine et var sur le système.
- Une fois les répertoires racine et var montés, déverrouillez ou modifiez le compte utilisateur Maglev.
- Enfin, redémarrez l'appliance, confirmez que vous pouvez vous connecter avec Maglev et réinitialisez le mot de passe à l'aide de l'assistant de configuration.

Détails ESXi de l'appliance virtuelle

- Téléchargez l'image ISO Ubuntu.
- Téléchargez l'ISO vers l'emplacement Fichier ISO du data store ou la bibliothèque de contenu dans vSphere vCenter.
- Ajoutez un lecteur de CD/DVD-ROM à la machine virtuelle.
- Remplacez le délai de démarrage par une valeur supérieure.

Composants utilisés

Cette opération a été exécutée sur une image Ubuntu 18.04 ; une image différente produit des temps et des résultats différents. Dans certains environnements, il faut jusqu'à 2 heures pour atteindre le bureau Ubuntu, mais pour la plupart des utilisateurs, le processus se termine en 30 minutes.

Cette opération n'est pas limitée à la version de bureau d'Ubuntu. Vous n'avez besoin que d'accéder au shell. Toute image Ubuntu qui fournit un accès shell fonctionne pour cette opération.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Remarque : La même procédure s'applique dans un environnement de reprise après sinistre. Révisez ces considérations avant de continuer.

Avertissement : Assurez-vous que le DR (Disaster Recovery) est à l'état PAUSED avant de tenter une récupération de mot de passe ou une procédure de réinitialisation. Dans un déploiement de DR 1+1+1, le site correspondant est arrêté pendant la durée de ce

---

processus. Dans un déploiement de DR 3+3+3, si les mots de passe doivent être mis à jour sur les trois noeuds, mettez à jour un noeud à la fois pour garder les deux autres noeuds disponibles et éviter un basculement de DR inutile.

Résolution

Étape 1: Confirmer l'accès et sélectionner le workflow correct

1. Vérifiez si le noeud affecté est un appareil physique sur site ou un appareil virtuel sur VMware ESXi.

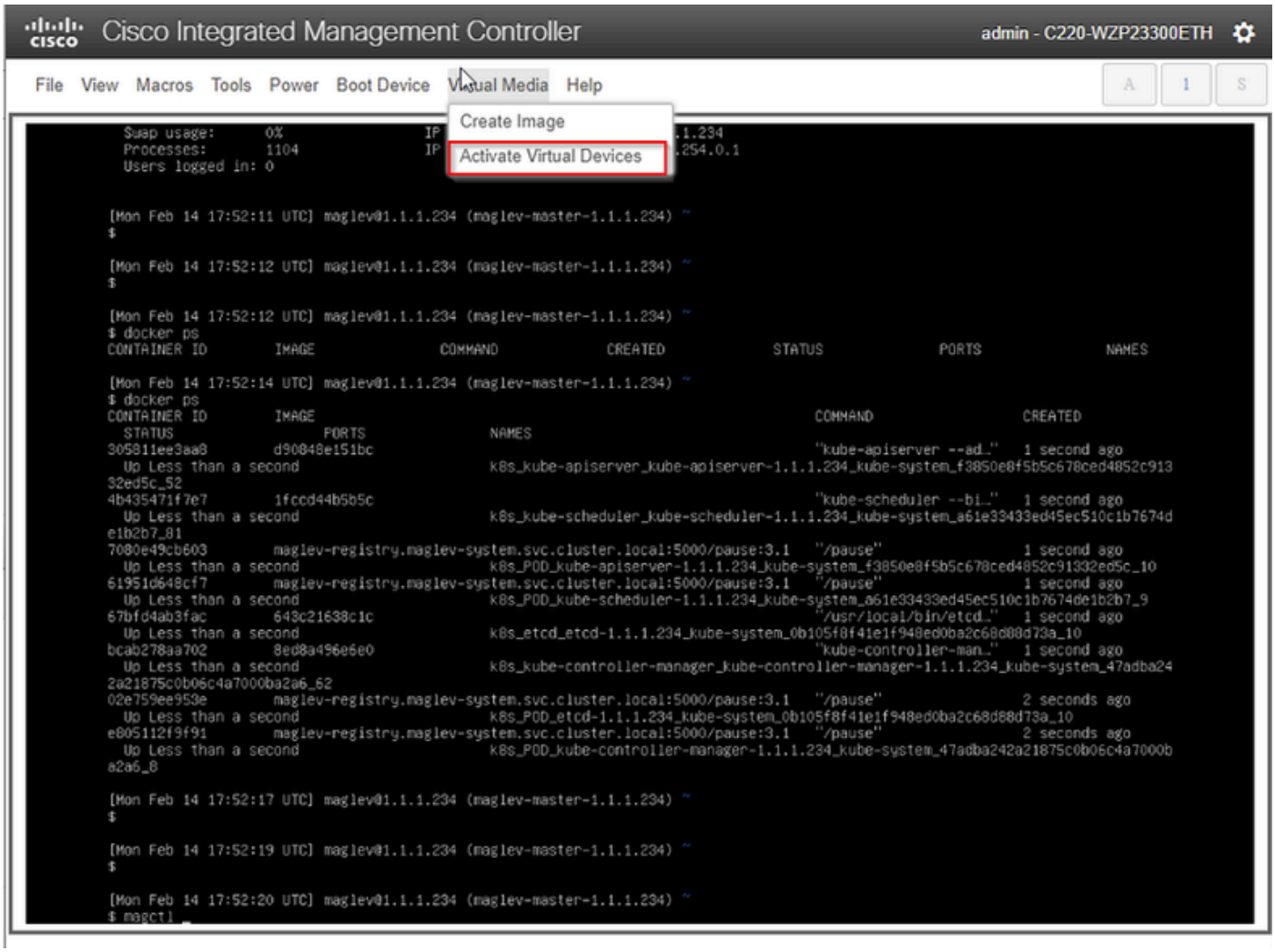
2. Vérifiez que vous disposez d'un accès administratif à l'interface de gestion pour votre déploiement : Cisco Integrated Management Controller (CIMC) pour les appareils physiques ou VMware vCenter pour les appareils virtuels.

3. Vérifiez qu'une image ISO Ubuntu (Ubuntu 18.04 ou version ultérieure) est disponible et peut être montée sur le serveur ou la machine virtuelle.

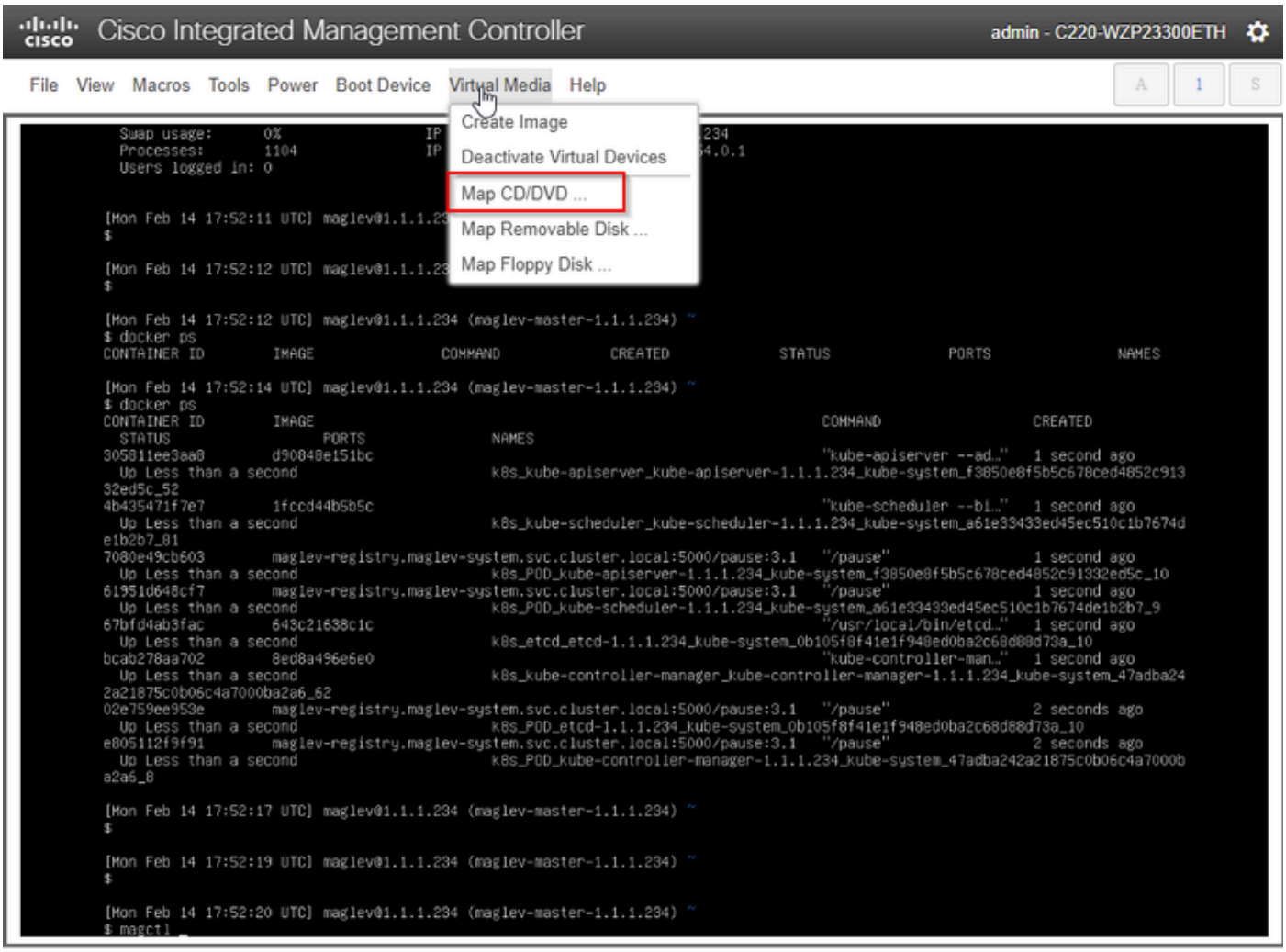
4. Si la reprise après sinistre (DR) est déployée, vérifiez que le DR est à l'état PAUSED avant de continuer.

Étape 1a : Démarrage à partir d'un CD Live sur site

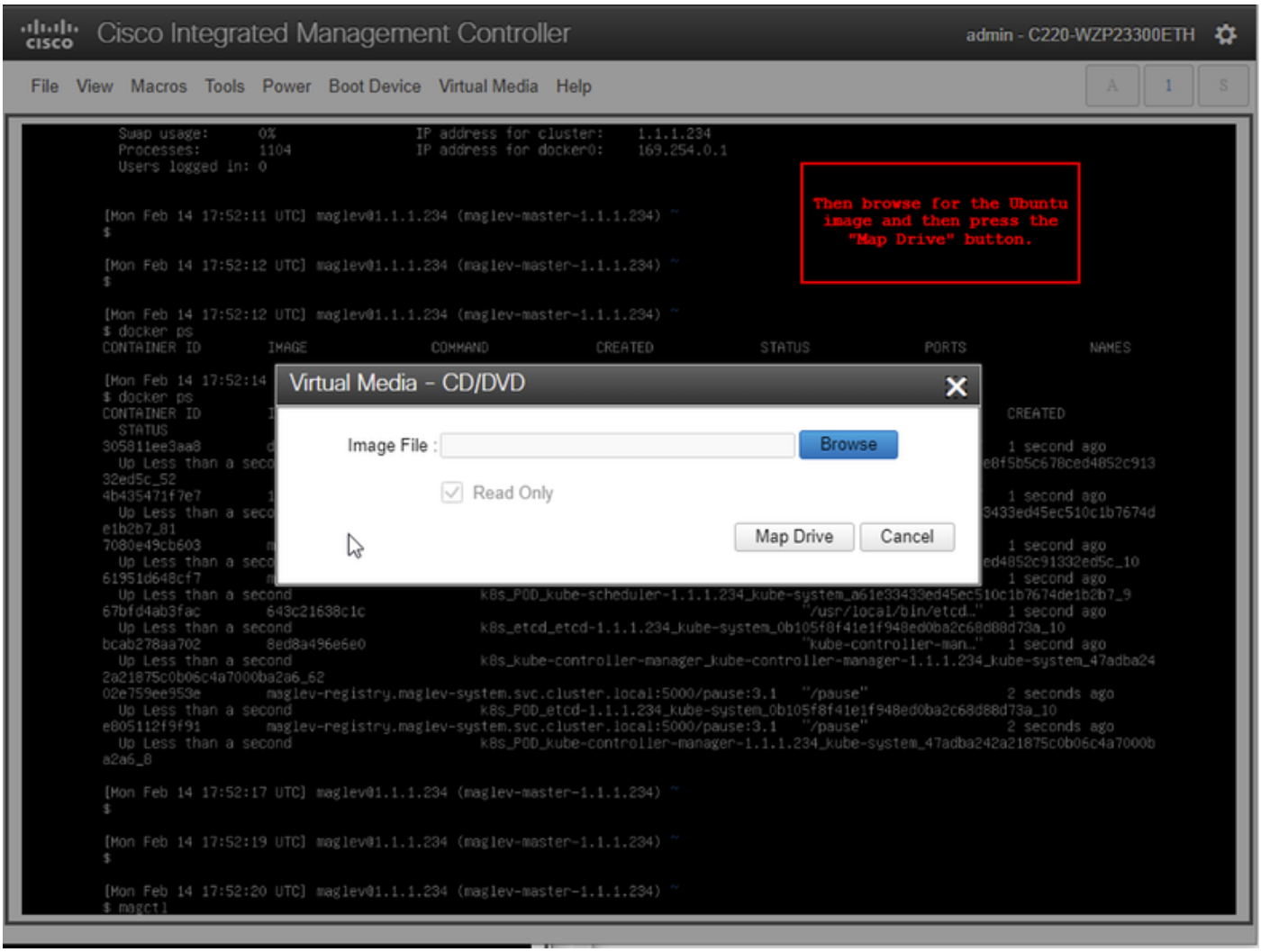
1. Connectez-vous à l'interface utilisateur graphique de Cisco IMC, choisissez Launch KVM, puis sélectionnez Virtual Media > Activate Devices.

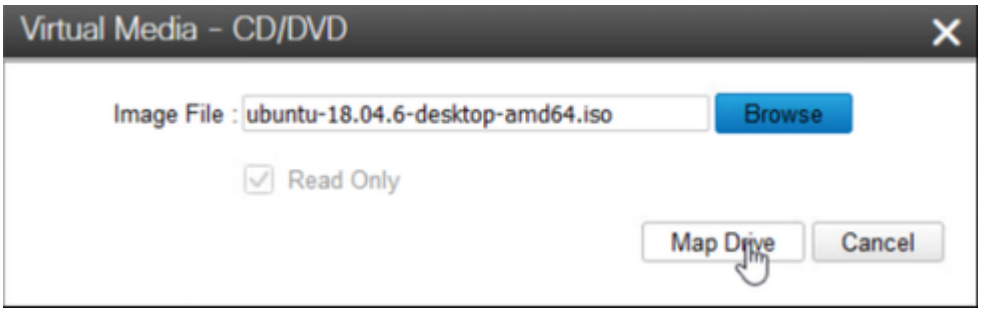


2. Choisissez ensuite Mapper CD/DVD.

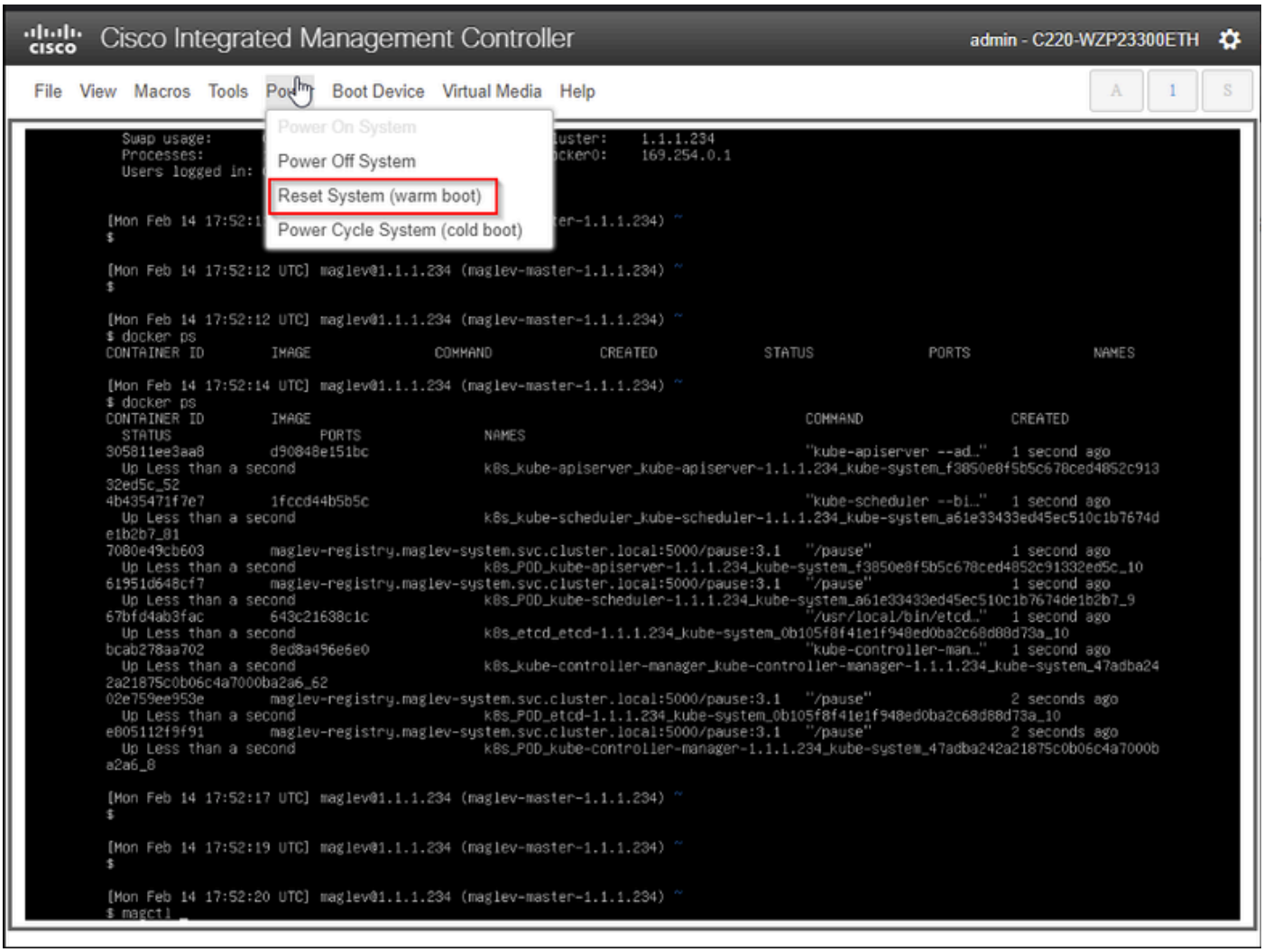


3. Cliquez sur Browse, puis sélectionnez l'image ISO Ubuntu téléchargée sur le système local. Après avoir sélectionné l'image Ubuntu, cliquez sur Map Drive.

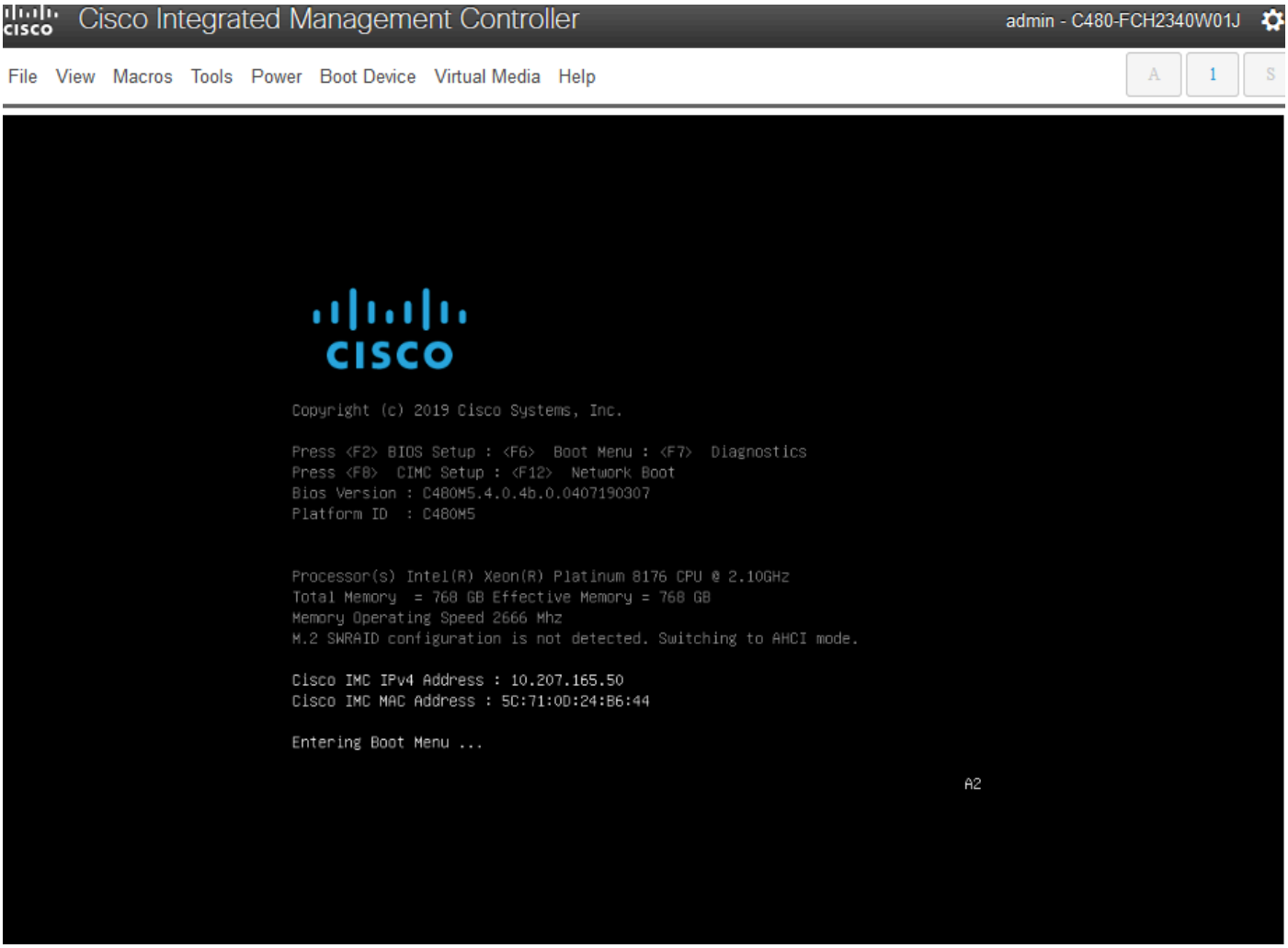


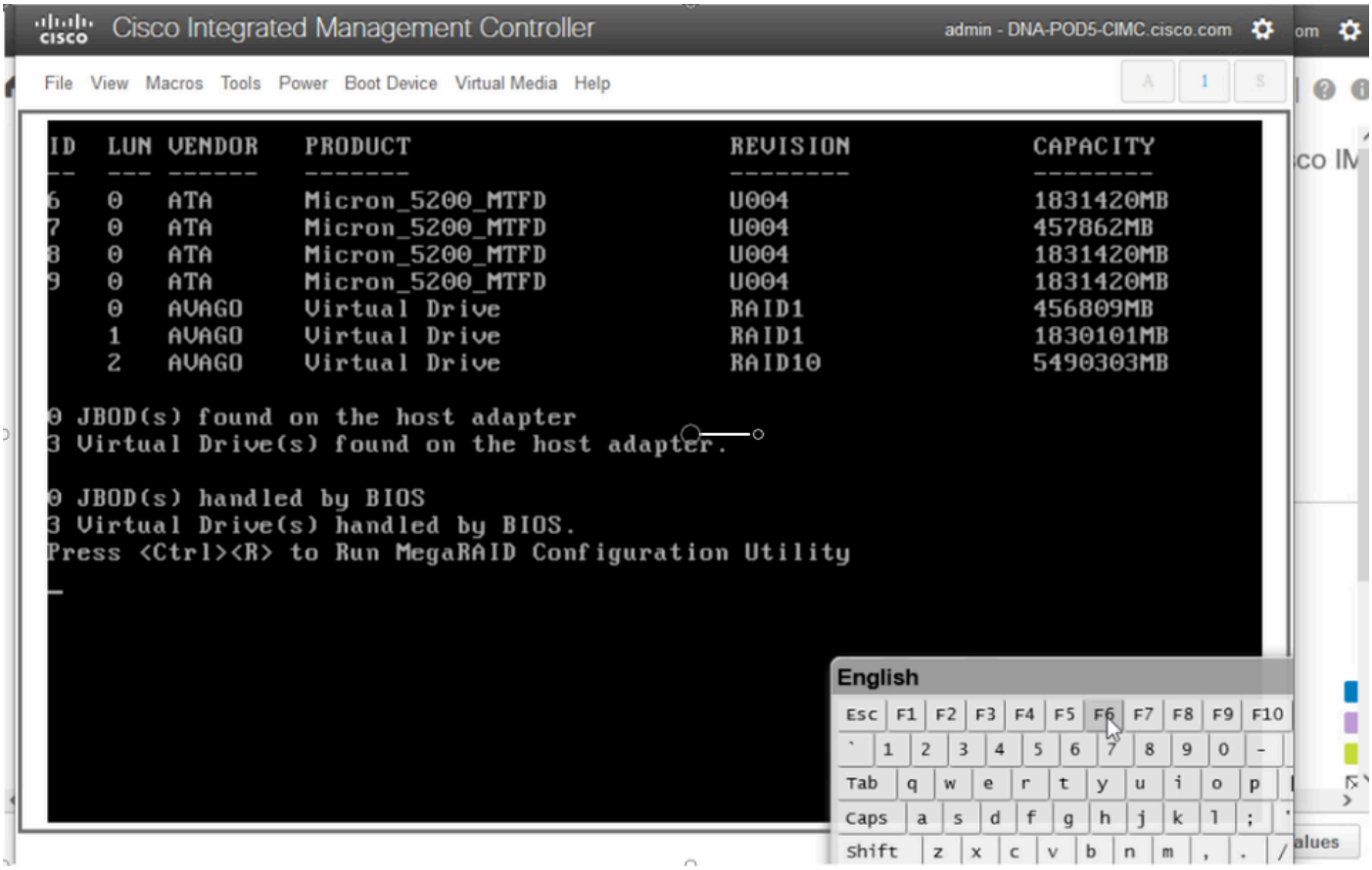


4. Mettez ensuite le périphérique sous tension puis sous tension avec Power > Reset System (démarrage à chaud).

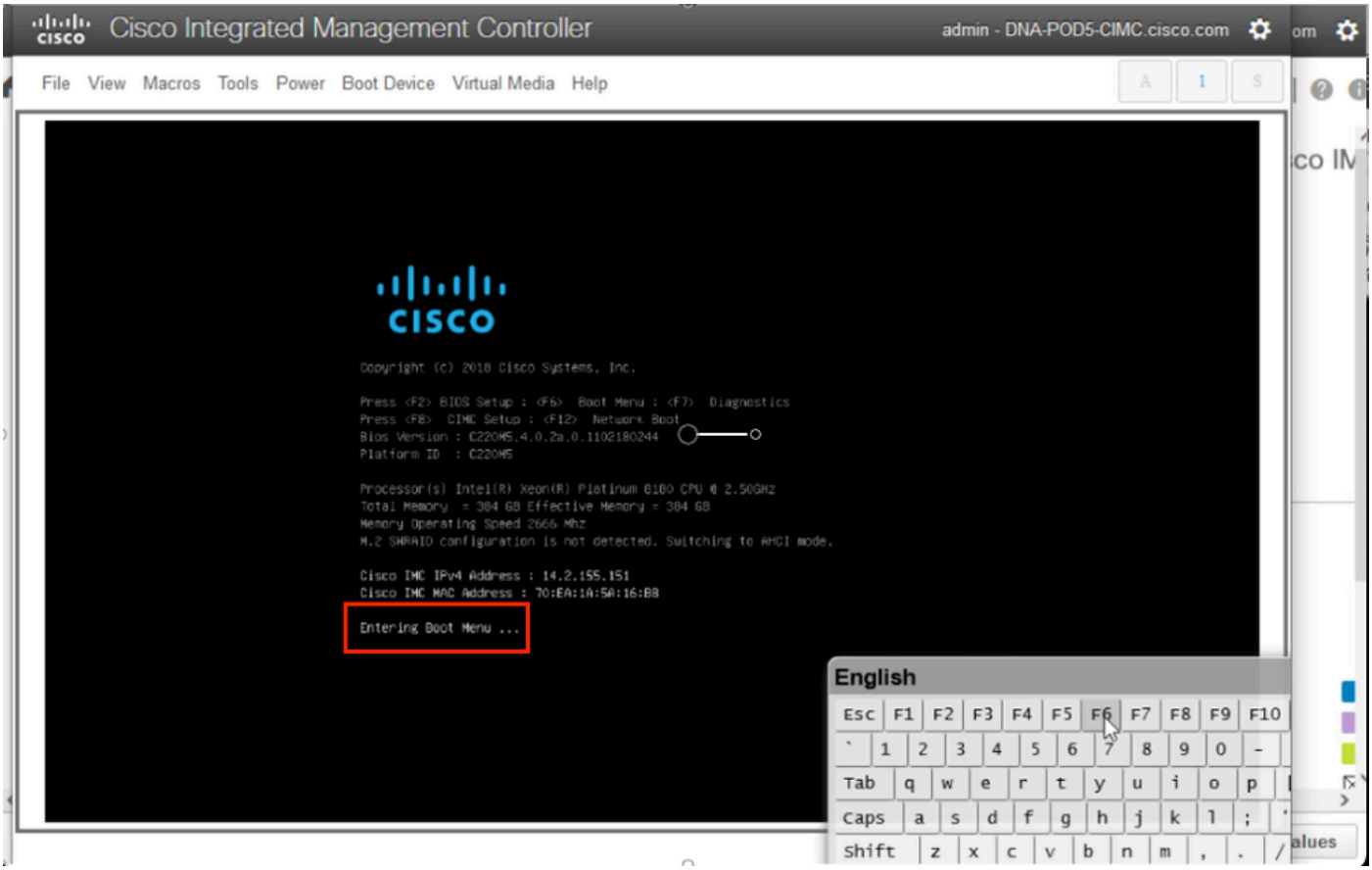


5. Après le redémarrage du système, appuyez sur F6 lorsque le logo Cisco apparaît.

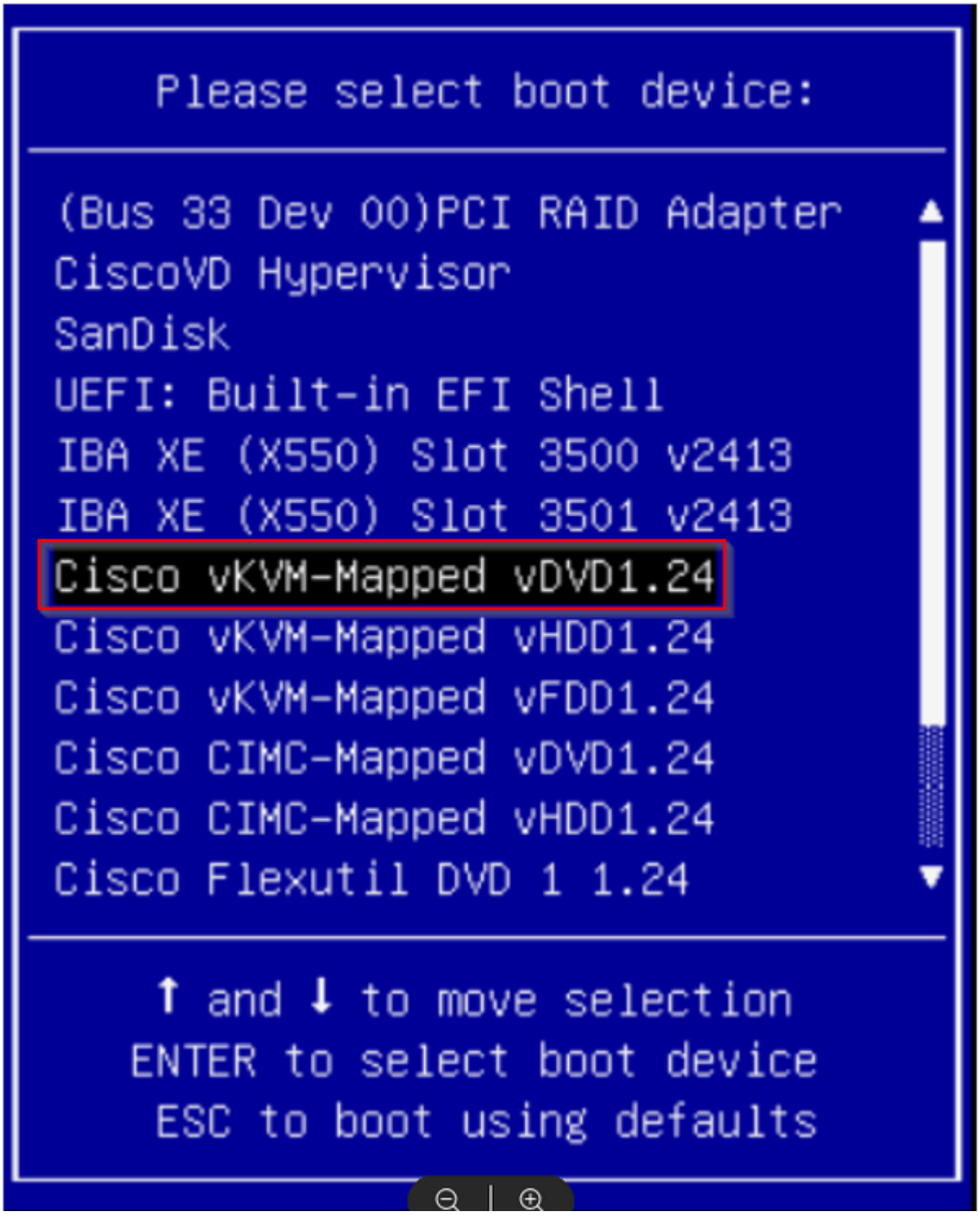

Cisco Integrated Management Controller
admin - C480-FCH2340W01J
File View Macros Tools Power Boot Device Virtual Media Help
Copyright (c) 2019 Cisco Systems, Inc.
Press <F2> BIOS Setup : <F6> Boot Menu : <F7> Diagnostics
Press <F8> CIMC Setup : <F12> Network Boot
Bios Version : C480M5.4.0.4b.0.0407190307
Platform ID : C480M5
Processor(s) Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz
Total Memory = 768 GB Effective Memory = 768 GB
Memory Operating Speed 2666 Mhz
M.2 SWRAID configuration is not detected. Switching to AHCI mode.
Cisco IMC IPv4 Address : 10.207.165.50
Cisco IMC MAC Address : 5C:71:0D:24:B6:44
Entering Boot Menu ...
A2


Cisco Integrated Management Controller
admin - DNA-POD5-CIMC.cisco.com
File View Macros Tools Power Boot Device Virtual Media Help
ID LUN VENDOR PRODUCT REVISION CAPACITY
6 0 ATA Micron_5200_MTFD U004 1831420MB
7 0 ATA Micron_5200_MTFD U004 457862MB
8 0 ATA Micron_5200_MTFD U004 1831420MB
9 0 ATA Micron_5200_MTFD U004 1831420MB
0 AVAGO Virtual Drive RAID1 456809MB
1 AVAGO Virtual Drive RAID1 1830101MB
2 AVAGO Virtual Drive RAID10 5490303MB
0 JBOD(s) found on the host adapter
3 Virtual Drive(s) found on the host adapter.
0 JBOD(s) handled by BIOS
3 Virtual Drive(s) handled by BIOS.
Press <Ctrl><R> to Run MegaRAID Configuration Utility
English

6. Un deuxième écran apparaît et le système entre dans le menu d'amorçage. Si vous n'avez pas appuyé sur F6 sur le premier écran de Cisco, appuyez ici.

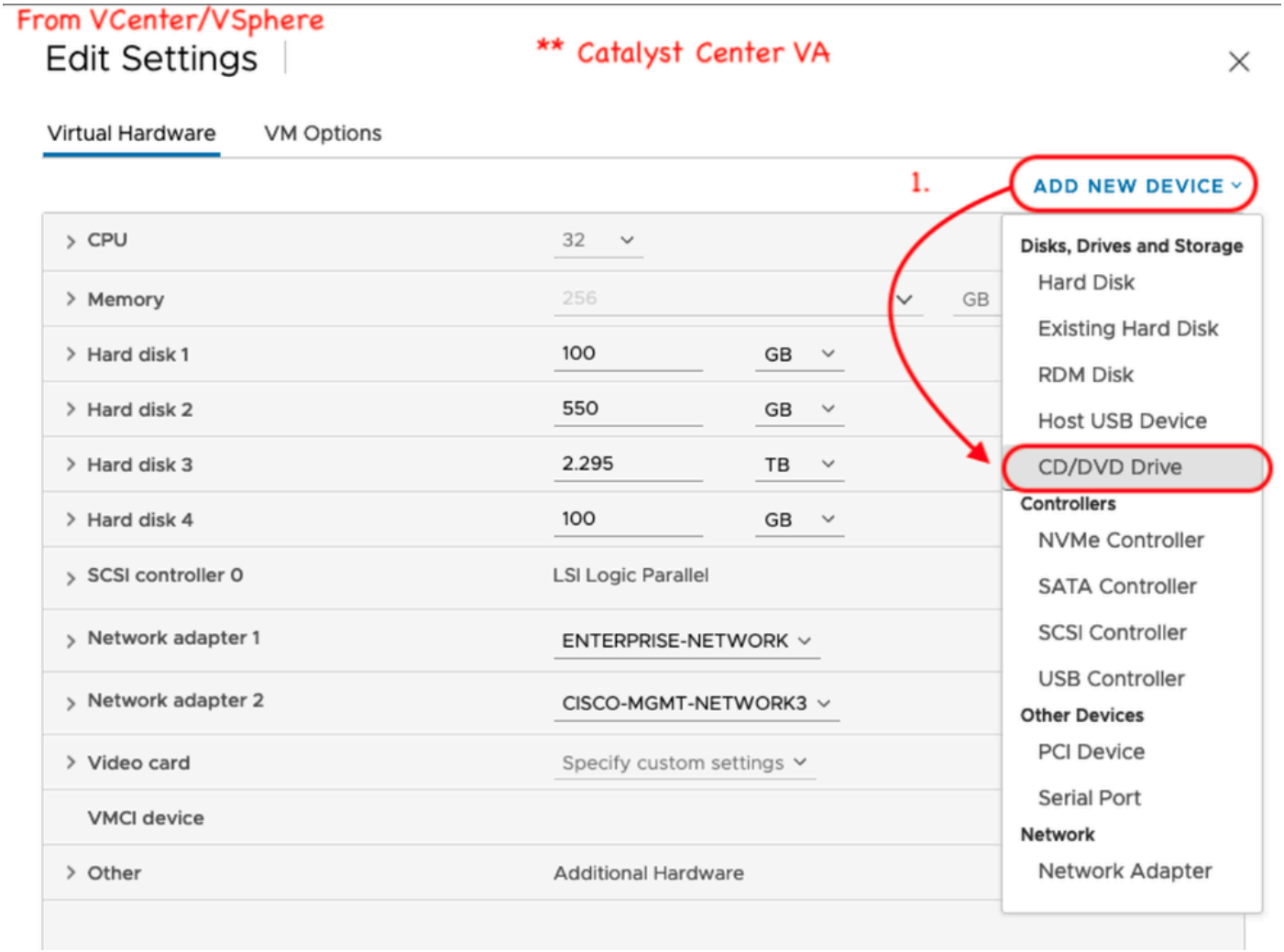


7. Lorsque le menu d'amorçage apparaît, sélectionnez Cisco vKVM-Mapped vDVD1.24. L'appareil démarre à partir de l'image ISO Ubuntu mappée.

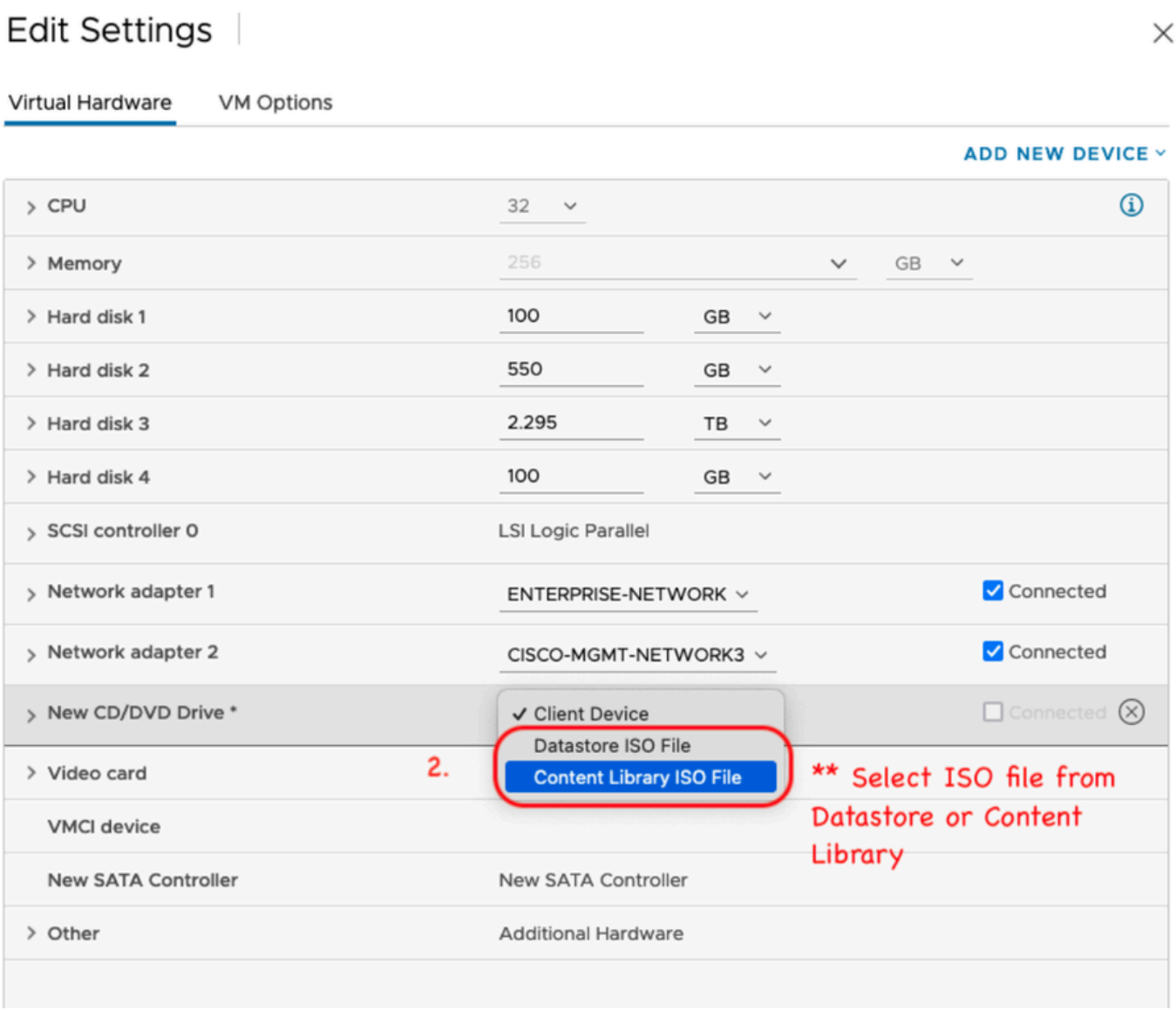


Étape 1b : Démarrage à partir d'un CD-ROM en direct VA - ESXi

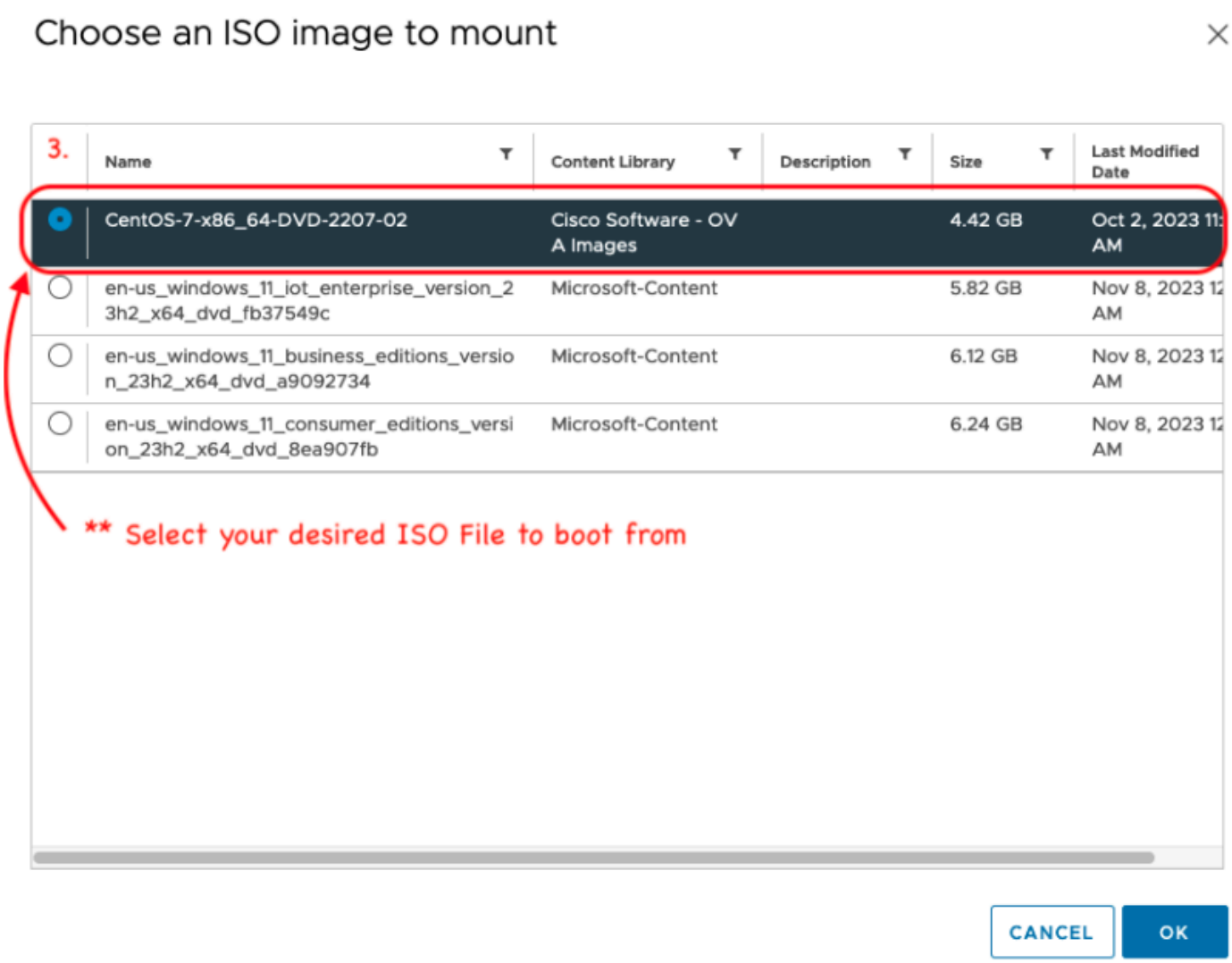
1. Dans VMware vCenter, accédez à la VM, cliquez avec le bouton droit sur la VM, puis choisissez Modifier les paramètres. Cliquez sur ADD NEW DEVICE, puis choisissez CD/DVD Drive.



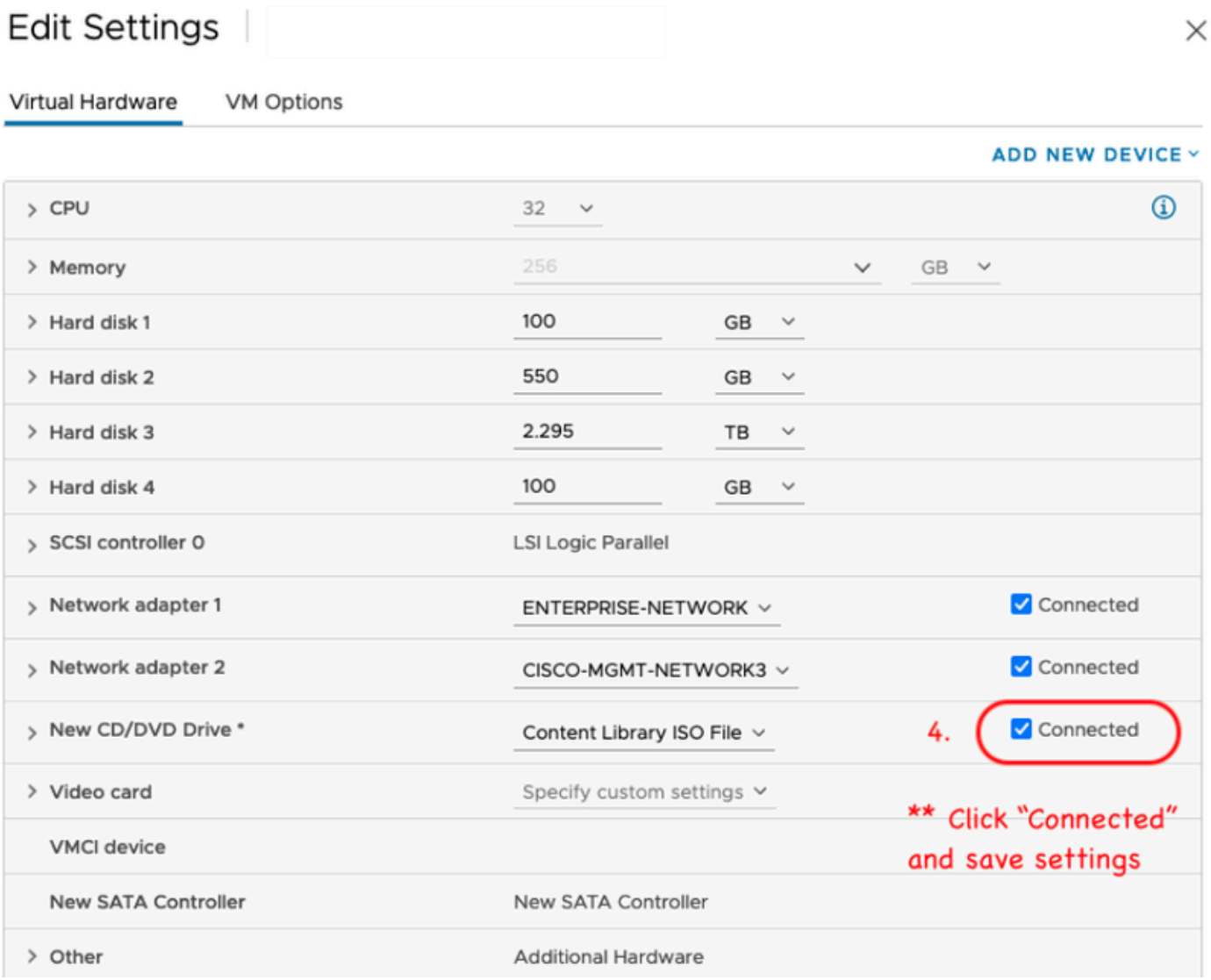
2. Le lecteur de CD/DVD s'affiche désormais dans la page des paramètres en tant que nouveau lecteur de CD/DVD. Si l'ISO a été téléchargé dans le fichier ISO du data store, choisissez cette option pour le CD/DVD. Sinon, choisissez Fichier ISO de la bibliothèque de contenu.



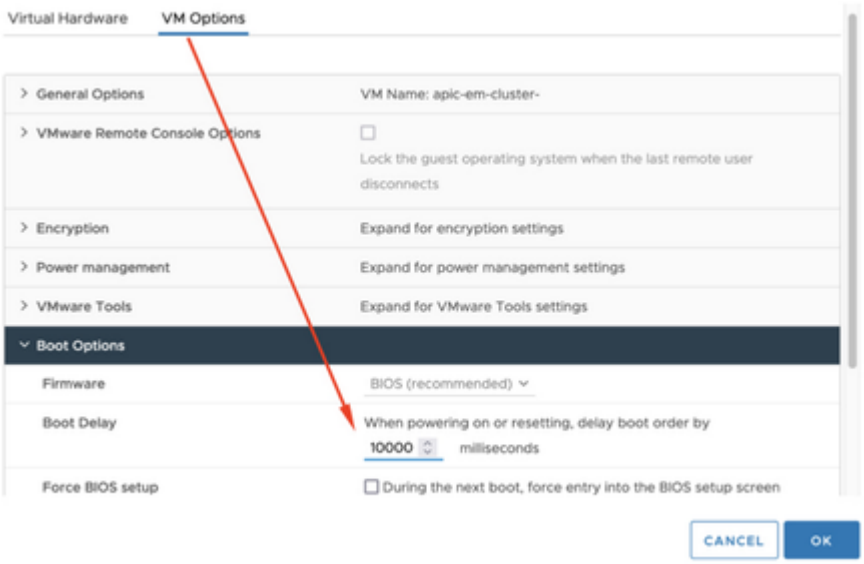
3. Sélectionnez le fichier ISO à partir duquel démarrer. Pour cette procédure, utilisez l'ISO Ubuntu 18.04.



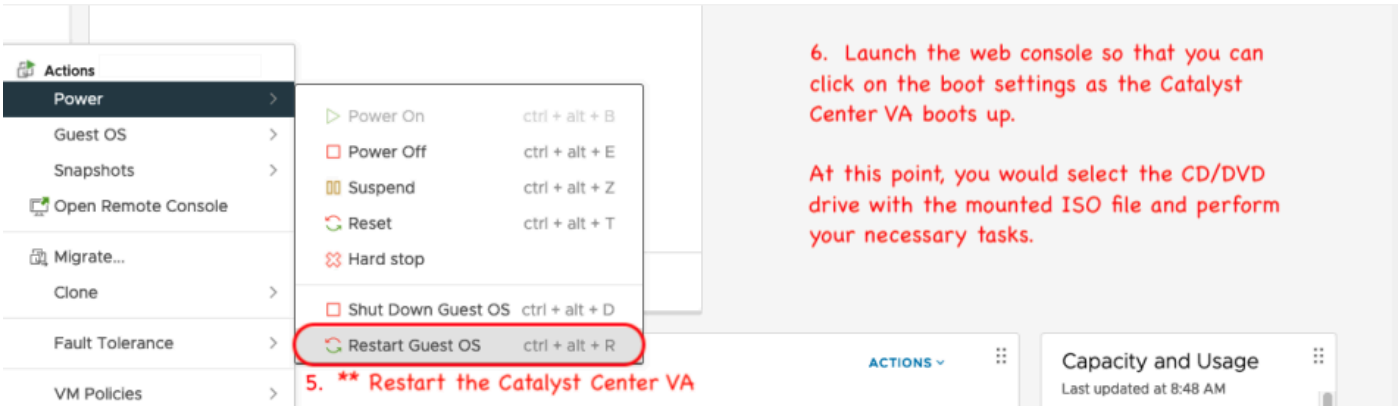
4. Assurez-vous ensuite que Connected est activé à droite de New CD/DVD Drive.

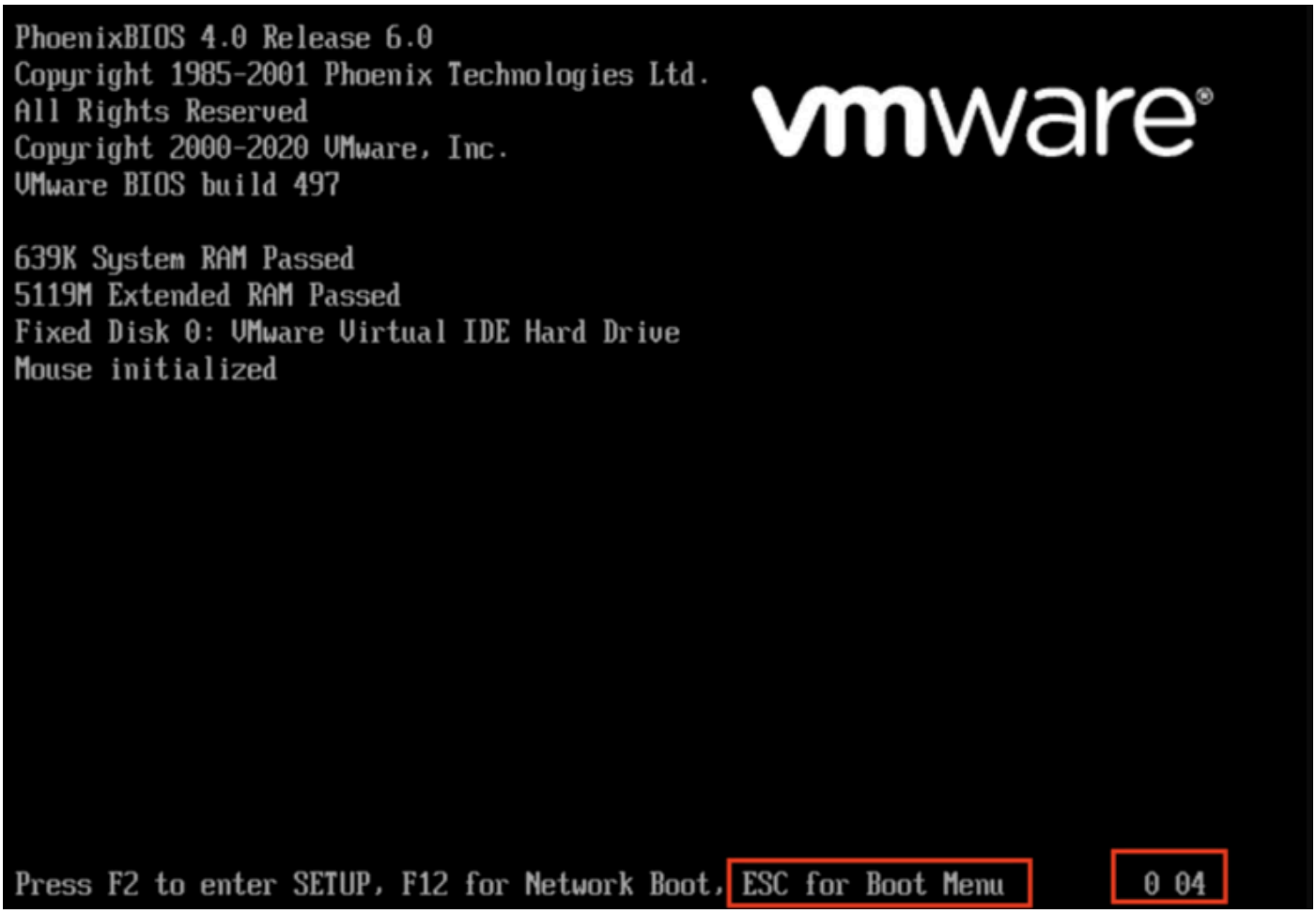


5. Cliquez sur Options VM en haut de l'écran des paramètres. Cliquez sur la flèche vers le bas pour Options de démarrage, puis modifiez Délai de démarrage à une valeur plus grande (par exemple, 10000). L'augmentation du délai affiche l'option de menu d'amorçage suffisamment longtemps pour sélectionner l'ISO après le redémarrage de la VM.



6. Ensuite, redémarrez la machine virtuelle pour accéder au menu d'amorçage et démarrer à partir de l'ISO.





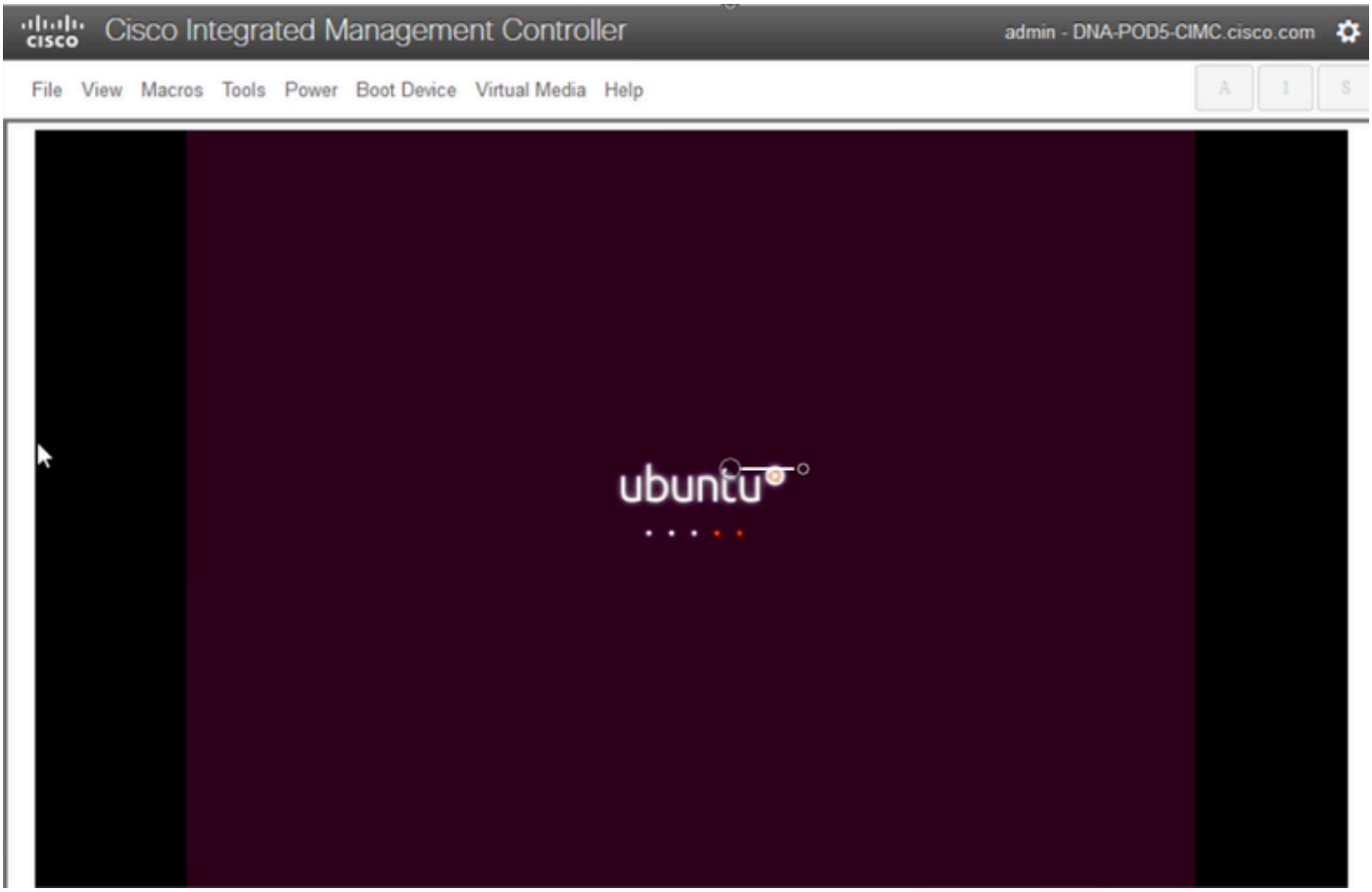
Étape 2a: Charger dans l'ISO Ubuntu

Remarque : Les captures d'écran illustrent le temps nécessaire pour atteindre le bureau Ubuntu.

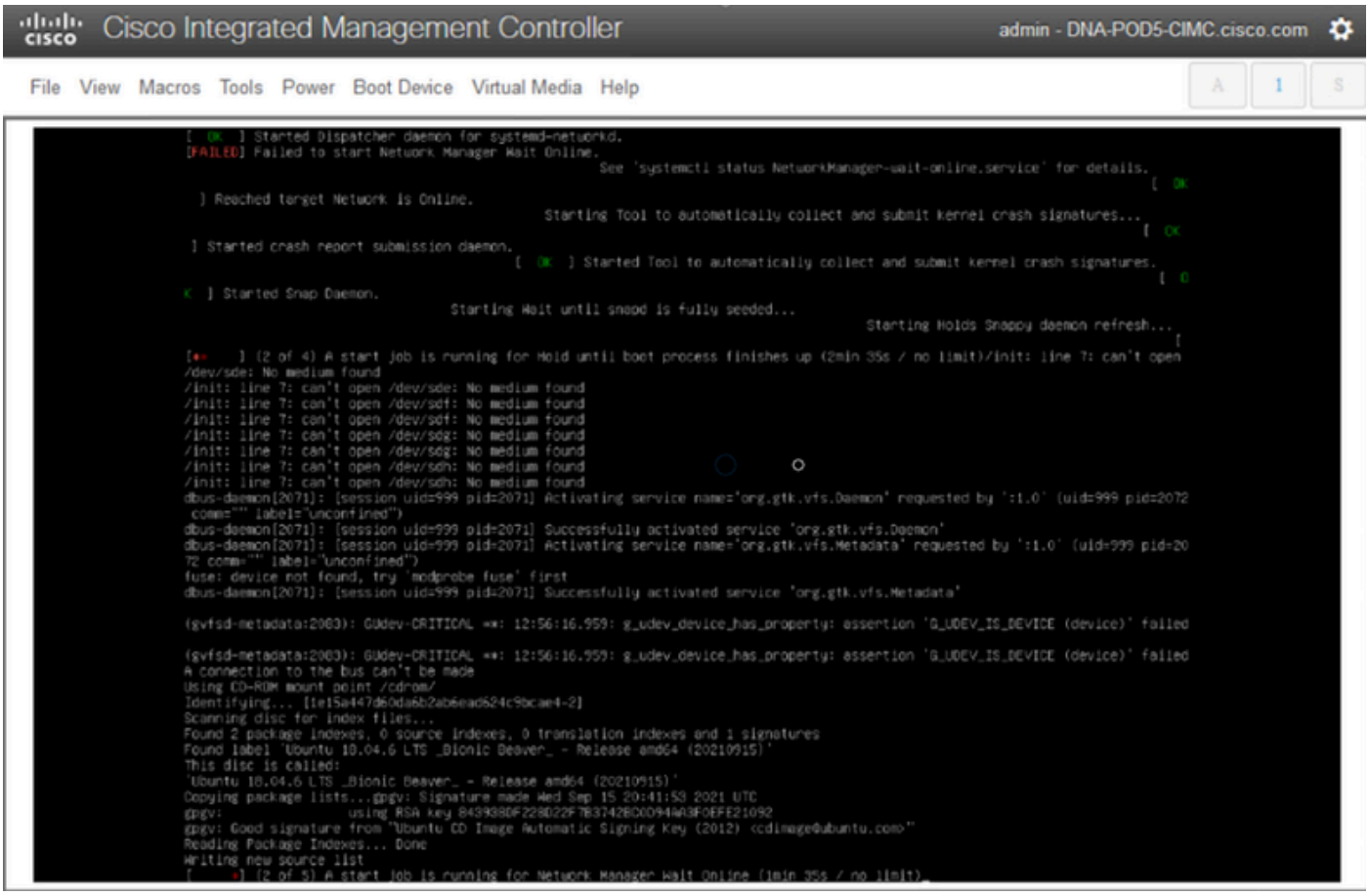
1. Il s'agit du premier écran affiché, il peut apparaître inactif (attendez l'écran suivant). Au cours des travaux pratiques, cet écran est resté affiché pendant 40 secondes.



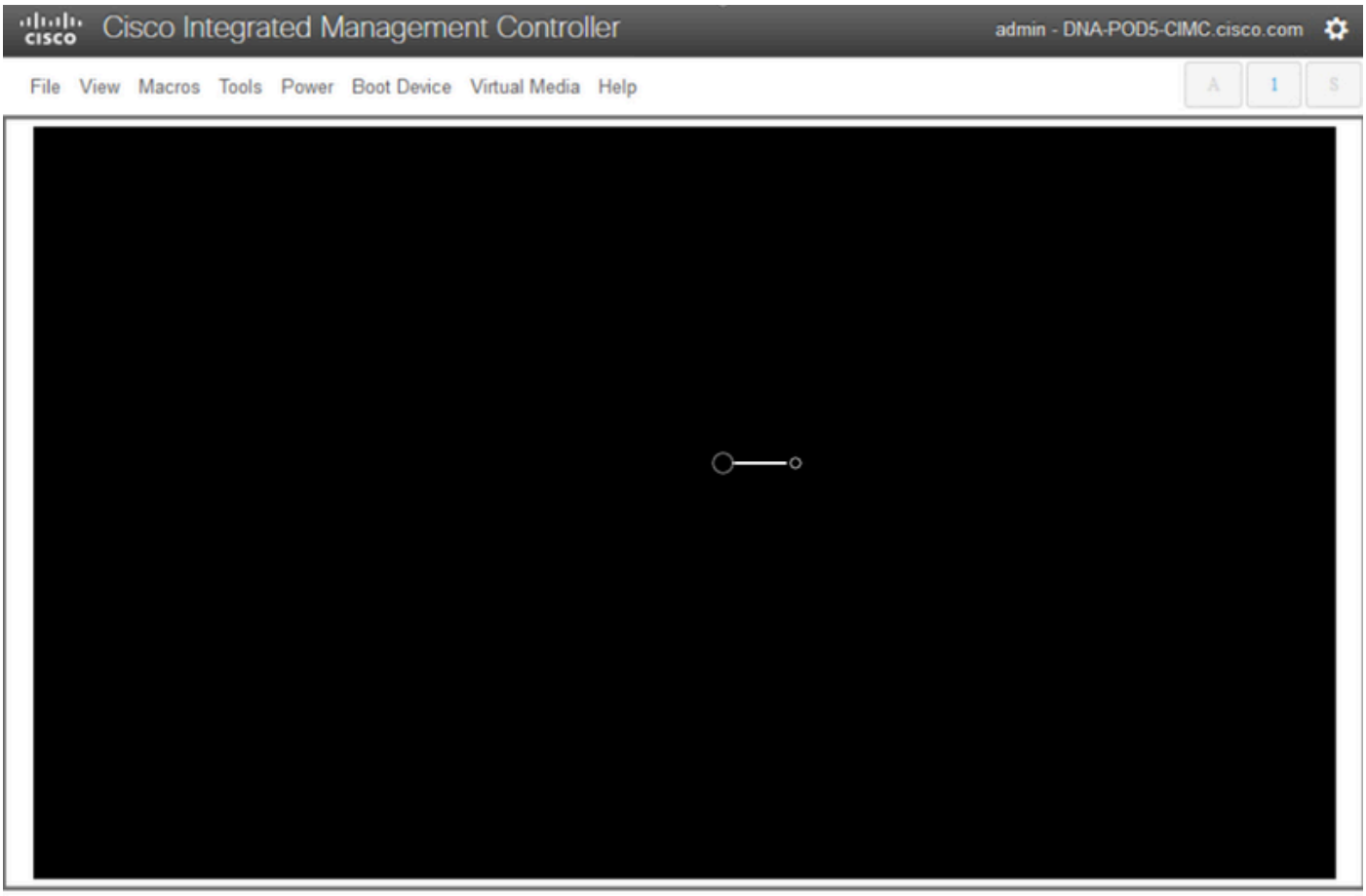
2. Après cela, l'écran est devenu complètement noir pendant environ 30 secondes avant qu'un écran de chargement Ubuntu n'apparaisse. Au cours des travaux pratiques, cet écran est resté pendant un peu plus de 5 minutes avant de passer à la suite, mais les délais peuvent varier d'un déploiement à l'autre.



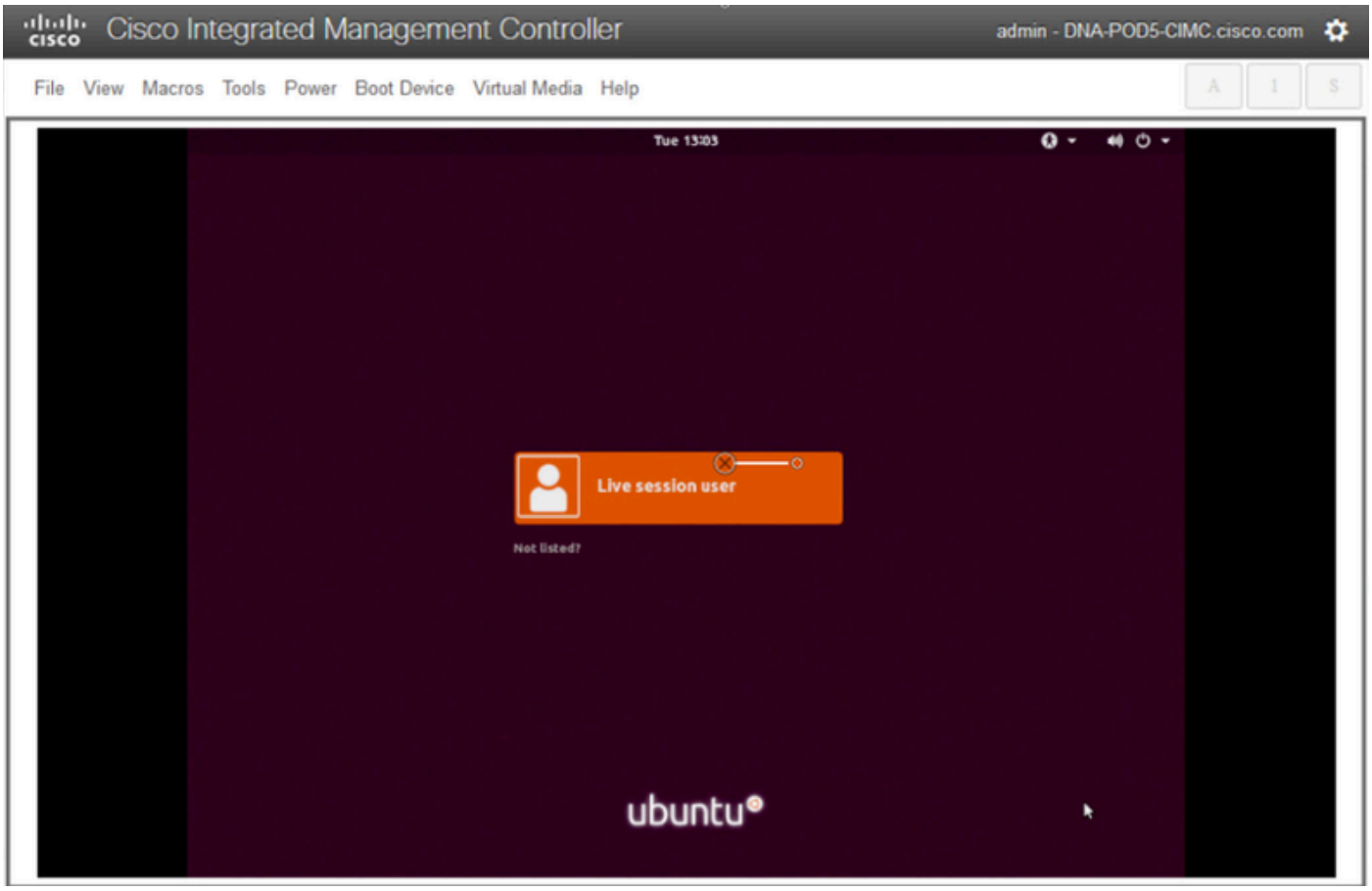
3. Ensuite, un écran apparaît qui peut suggérer que quelque chose s'est mal passé, mais c'est prévu. Au cours des travaux pratiques, cet écran est resté allumé pendant 2 minutes avant de continuer.



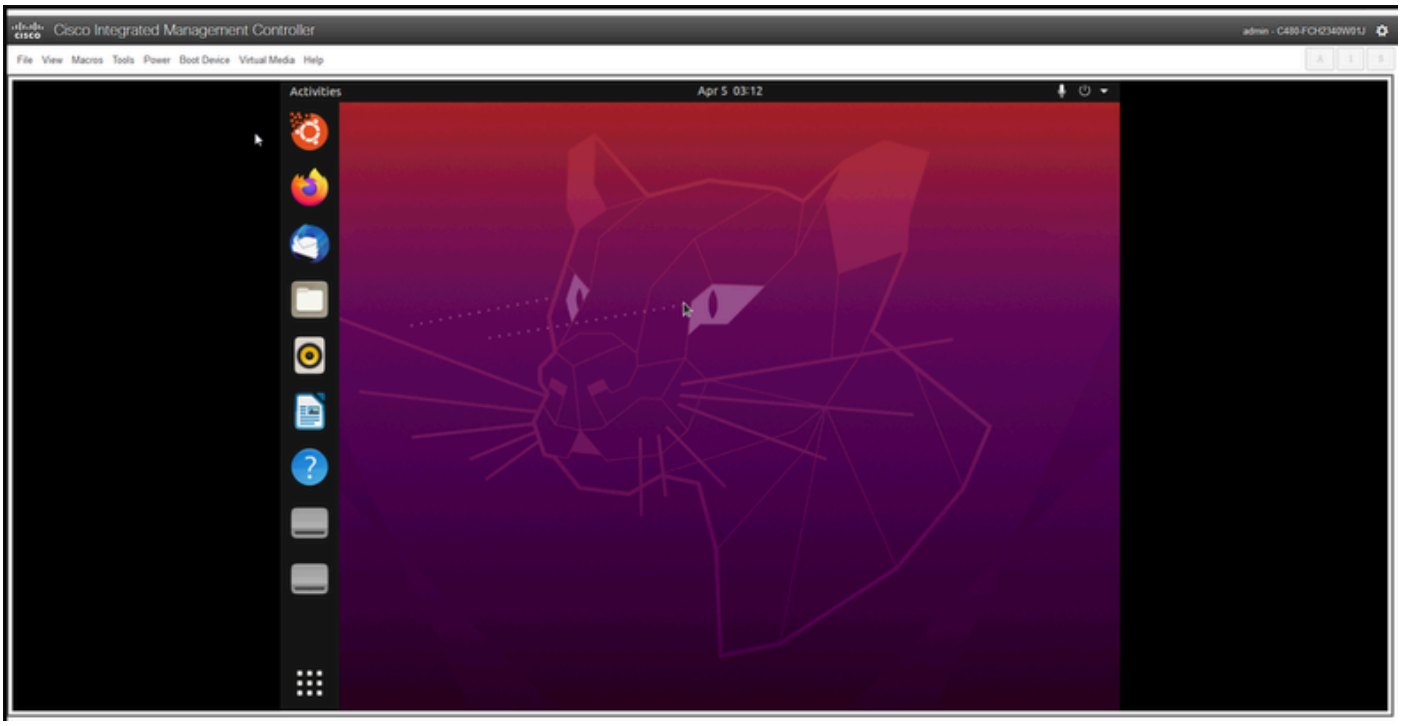
4. L'écran est revenu à un écran noir pendant environ 3 minutes, l'écran précédent a clignoté à nouveau pendant quelques minutes, puis est revenu à l'écran noir pendant encore 2 minutes.



5. Ensuite, l'option permettant de sélectionner un utilisateur de session dynamique apparaît. Si l'option pour essayer Ubuntu desktop apparaît, choisissez cette option. Sélectionnez cet utilisateur pour continuer.



6. Une fois que l'utilisateur est sélectionné, l'écran redevient noir avant que le bureau Ubuntu ne soit présenté.



Dans certains environnements, cela peut prendre jusqu'à deux heures pour atteindre ce point.

Étape 2b : Montage des partitions requises

Une fois que l'accès à l'environnement graphique du bureau Ubuntu est disponible, ouvrez l'application du terminal et procédez comme suit.

Après avoir entré l'environnement chroot plus loin dans cette procédure, vous pouvez déterminer quelle action de récupération est requise :

- Si /etc/shadow affiche un point d'exclamation (!) avant le hachage du mot de passe pour maglev, le compte est verrouillé et doit être déverrouillé.
- Si le compte n'est pas verrouillé mais que la connexion est toujours refusée, réinitialisez le compteur d'échecs de connexion pour maglev.
- Si vous devez définir un nouveau mot de passe, réinitialisez le mot de passe maglev, puis exécutez la mise à jour sudo maglev-config après le redémarrage.

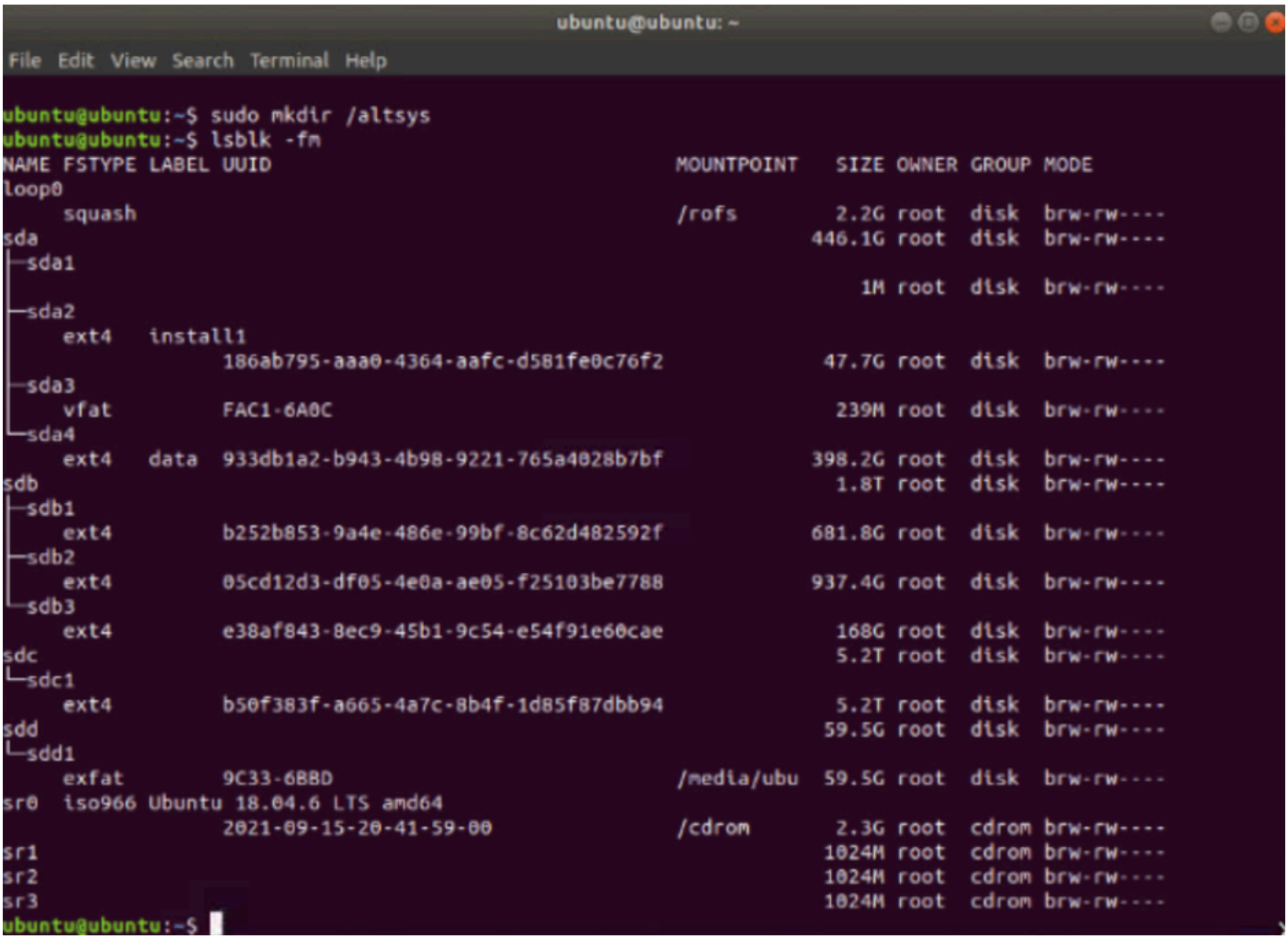
1. Créez un point de montage temporaire.
2. Montez les partitions racine et var sur le système.
3. Montez les pseudo-systèmes de fichiers sur le point de montage temporaire.

Commencez par créer le point de montage temporaire en exécutant cette commande :

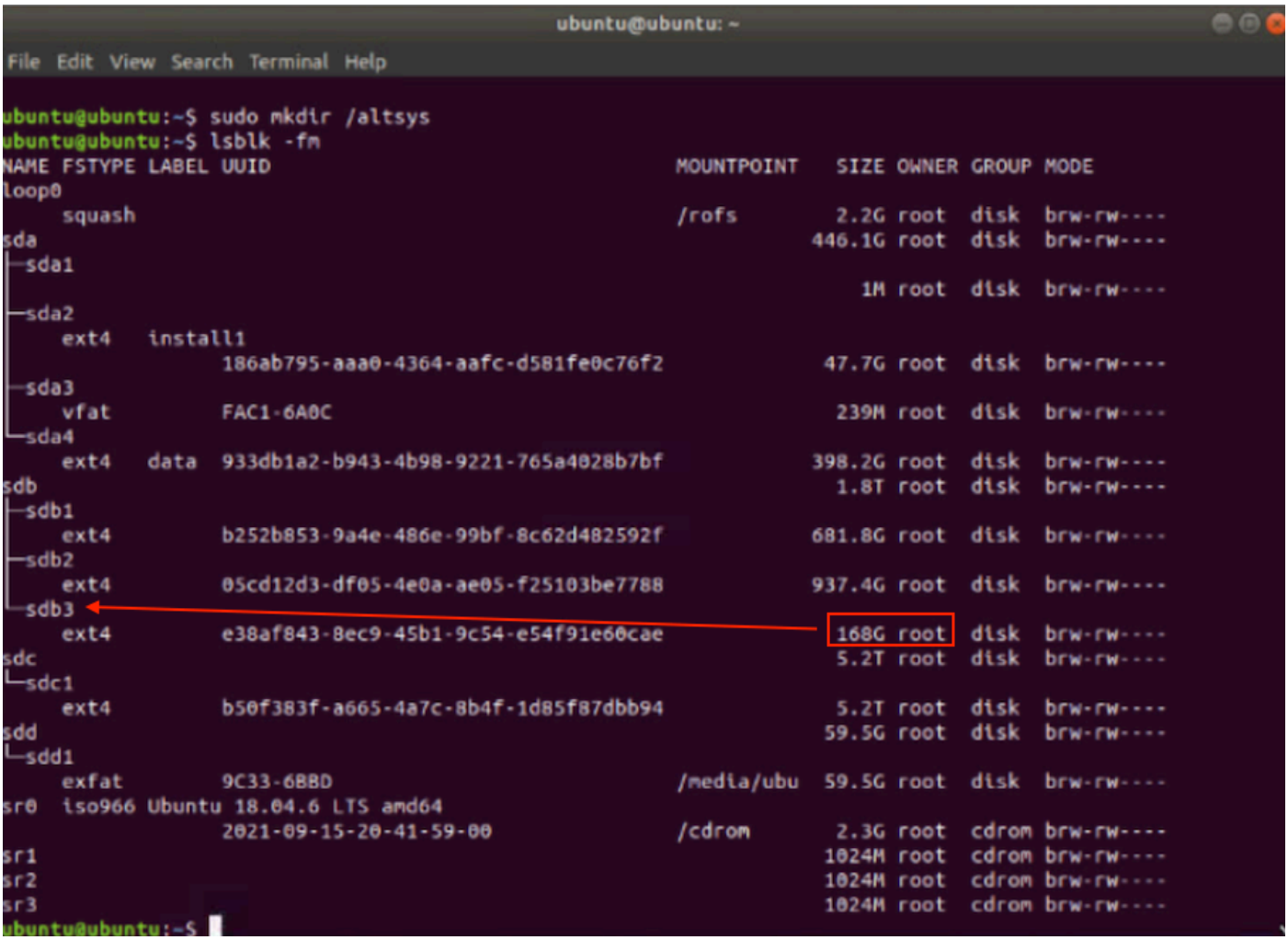
<#root>

```
sudo mkdir /altsys
```

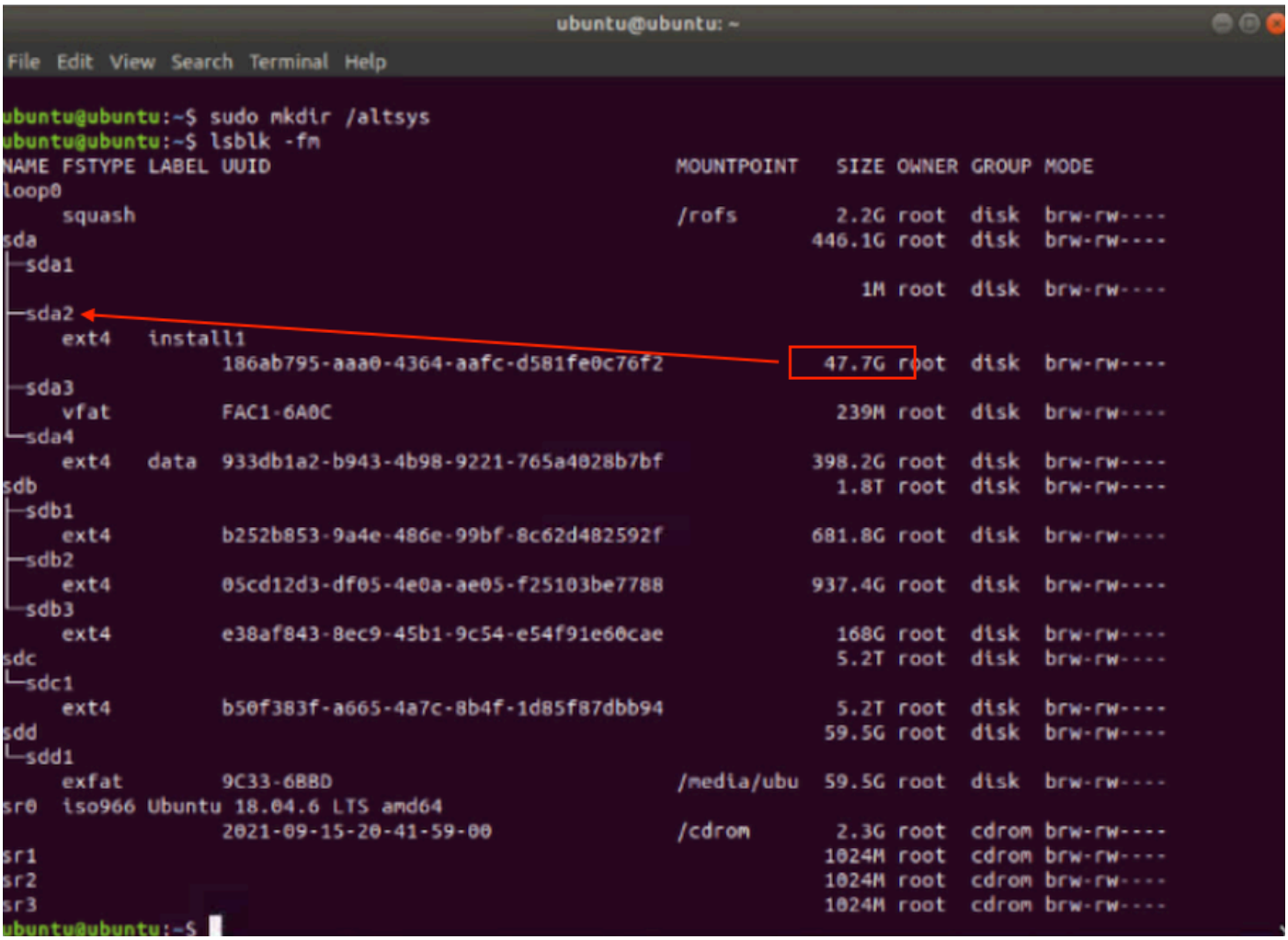
Ensuite, recherchez les partitions racine et var à monter. Exécutez la commande lsblk -fm pour identifier les partitions pour (racine) et /var. Notez les partitions identifiées pour les commandes mount à l'étape suivante.



Pour /var, recherchez une partition 9.5G ou 168G ; dans ce cas, il s'agit de sdb3.



Pour la partition / racine, recherchez la partition 28.66G ou 47.7G. Dans cet exemple, il s'agit de sda2.



Une fois que vous avez identifié les partitions var et racine, montez-les :

<#root>

```
sudo mount /dev/sda2 /altsys
```

```
   # use the disk with up to 5 or 6 partitions
```

```
sudo mount /dev/sdb3 /altsys/var
```

```
       # use the disk with up to 5 or 6 partitions
```

Une fois que la racine et la variable sont montées, montez les pseudo-systèmes de fichiers :

<#root>

```
sudo mount --bind /proc /altsys/proc
```

```
sudo mount --bind /dev  /altsys/dev
```

```
sudo mount --bind /sys  /altsys/sys
```

La dernière étape avant la modification du mot de passe ou le déverrouillage du compte Maglev consiste à passer à l'environnement de montage temporaire :

<#root>

```
sudo chroot /altsys
```

Étape 3: Sélectionnez l'action de récupération (Déverrouiller le compte ou Réinitialiser le mot de passe)

Après avoir exécuté sudo chroot /altsys, utilisez l'un des workflows suivants :

- Déverrouiller le compte : Utilisez les étapes 3a et 3b.
- Réinitialiser le mot de passe : Utilisez les étapes 3c à 3e.

Étape 3a: Vérifiez si le compte Maglev est verrouillé

<#root>

```
grep maglev /etc/shadow
```

<#root>

```
maglev:

!

<redacted_hash>:18176:0:99999:7:::
```

Vérifiez s'il y a un point d'exclamation devant le hachage du mot de passe. Si tel est le cas, le compte est verrouillé. Exécutez cette commande pour déverrouiller l'utilisateur :

<#root>

usermod -U maglev

Étape 3b: Echec de la réinitialisation

Si l'utilisateur ne dispose pas d'un point d'exclamation (!) devant le hachage du mot de passe dans le fichier /etc/shadow, la limite d'échec de connexion a été dépassée. Suivez ces étapes pour réinitialiser les tentatives de connexion ayant échoué.

1. Recherchez les tentatives de connexion ayant échoué pour l'utilisateur maglev :

<#root>

$

sudo pam_tally2 -u maglev

```
Login           Failures Latest failure     From
maglev              454    11/25/20 20:24:05  x.x.x.x
```

2. Dans cet exemple, les tentatives de connexion ayant échoué dépassent la limite par défaut de 6. Cela empêche l'utilisateur de se connecter jusqu'à ce que le nombre d'échecs soit réinitialisé ou passe sous 6. Le nombre d'échecs de connexion peut être réinitialisé en exécutant cette commande :

<#root>

sudo pam_tally2 -r -u maglev

3. Le compteur peut être confirmé comme réinitialisé :

<#root>

sudo pam_tally2 -u maglev

```
Login           Failures Latest failure     From
maglev                0
```

Étape 3c : Réinitialiser le mot de passe utilisateur Maglev

<#root>

#

passwd maglev

```
Enter new UNIX password: #Enter in the desired password

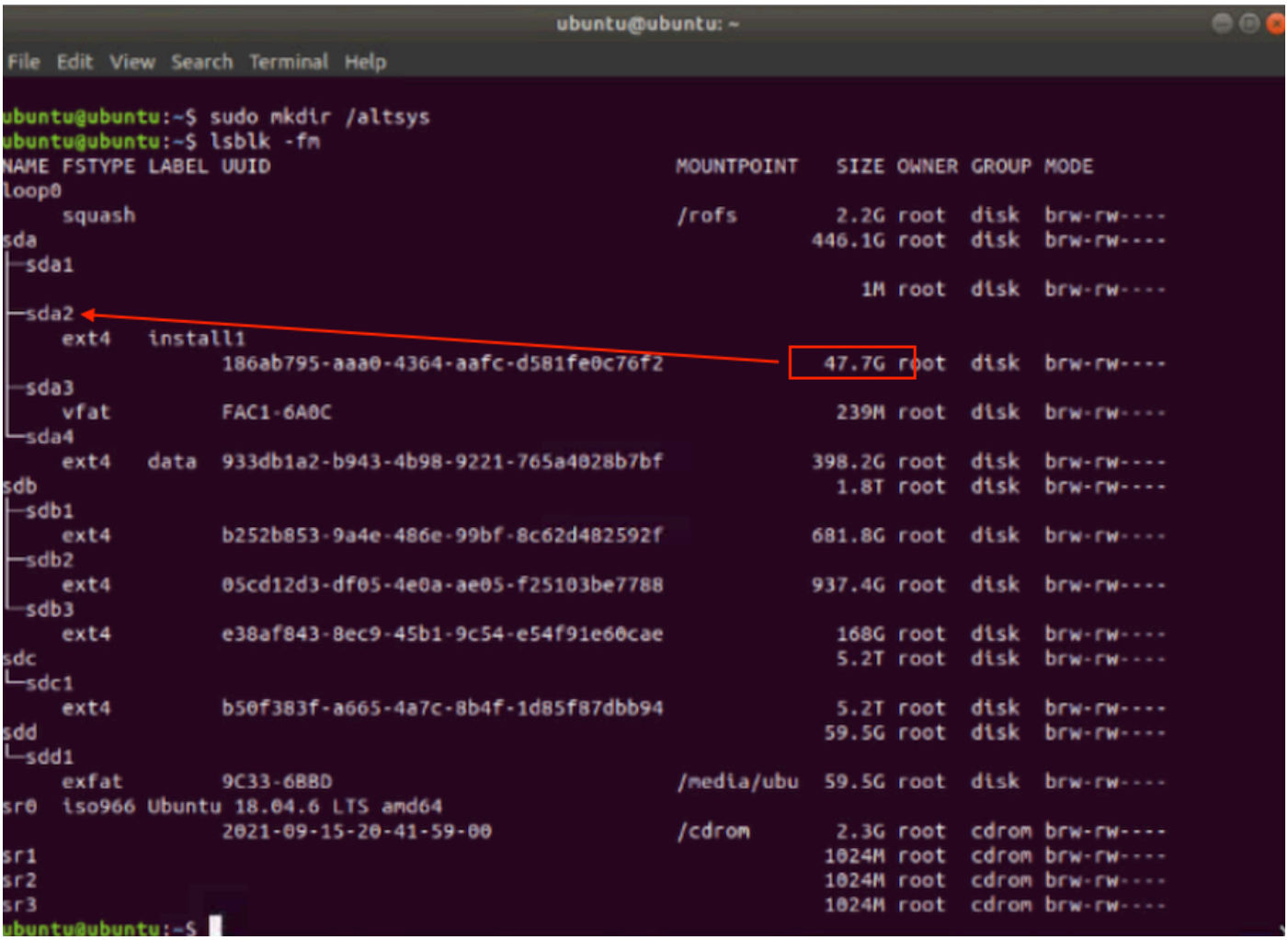
Retype new UNIX password:  #Re-enter the same password previously applied

Password has been already used.

passwd: password updated successfully  #Indicates that the password was successfully changed
```

Étape 3d : Redémarrer normalement sur l'environnement Cisco Catalyst Center

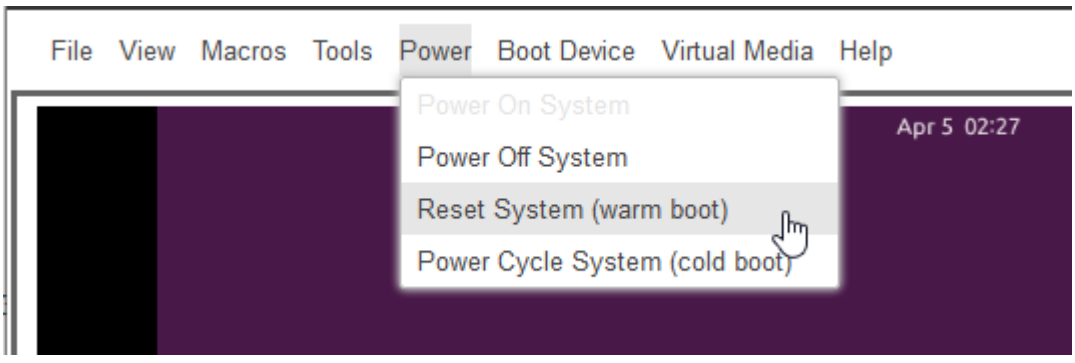
1. Cliquez sur Power dans la fenêtre KVM, puis sur Reset System (démarrage à chaud). Le système redémarre et démarre le logiciel Cisco Catalyst Center à partir du contrôleur RAID.



Étape 3e : Mettre à jour le mot de passe utilisateur Maglev depuis la CLI Cisco Catalyst Center

1. Une fois que le logiciel Cisco Catalyst Center démarre et que l'accès à la CLI est disponible, modifiez le mot de passe Maglev en exécutant la commande sudo maglev-config update. Cette étape est nécessaire pour s'assurer que le changement prend effet dans l'ensemble du système.

2. Une fois l'assistant de configuration lancé, naviguez dans l'assistant jusqu'à l'écran qui permet de définir le mot de passe Maglev à l'étape 6.



3. Après avoir saisi le mot de passe dans les champs Mot de passe Linux et Retapez le mot de passe Linux, choisissez Suivant et terminez l'Assistant. Lorsque l'assistant a terminé l'envoi de la configuration, le mot de passe a été modifié. Créez une nouvelle session SSH ou exécutez la commande sudo -i dans l'interface de ligne de commande pour vous assurer que le mot de passe a été modifié.

Motif

Lorsque le compte Maglev est verrouillé, l'utilisateur ne peut pas se connecter pour le déverrouiller. Pour déverrouiller et/ou réinitialiser le mot de passe de l'utilisateur Maglev, il est nécessaire de monter une image sur le vKVM Cisco IMC. Cela permet d'accéder au shell et de réinitialiser le compte d'utilisateur et/ou le mot de passe.

Autres informations utiles

Guide vidéo étape par étape

- Workflow de réinitialisation du mot de passe utilisateur Maglev

Images fournies par Cisco.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.