Comprendre la procédure de réinitialisation du mot de passe de Catalyst Center 3.x Maglev(SSH)

Table des matières

Introduction

Informations générales

Conditions préalables

- Configuration requise pour On-prem (appareil physique)
- Configuration requise pour l'appliance virtuelle (ESXi)
- Composants utilisés

Étape 1a : Démarrage à partir du CD Live (sur site)

Étape 1b : Démarrage à partir d'un CD Live (VA - ESXi)

Étape 2a: Chargement dans l'ISO Ubuntu

Étape 2b : Montage des partitions requises

Cas d'utilisation 1 : Déverrouiller un compte Maglev

- Étape 1: Vérifiez que l'utilisateur maglev est déverrouillé
- Étape 2: Échec de réinitialisation du nombre

Cas d'utilisation 3 : Réinitialiser le mot de passe utilisateur Maglev

- Étape 1: Réinitialiser le mot de passe utilisateur Maglev
- Étape 2: Redémarrez normalement l'environnement Cisco Catalyst Center
- Étape 3: Mettre à jour le mot de passe utilisateur Maglev depuis la CLI Cisco Catalyst Center

Guide vidéo étape par étape

Introduction

Ce document décrit comment déverrouiller et/ou réinitialiser le mot de passe pour l'utilisateur Maglev pour les noeuds de l'appliance physique Catalyst Center 3.x et ESXi virtuel.

Informations générales

Si le compte Maglev est verrouillé, vous ne pouvez pas vous connecter pour le déverrouiller. Pour déverrouiller et/ou réinitialiser le mot de passe de l'utilisateur Maglev, vous devez monter une image sur le Cisco IMC vKVM pour les appareils physiques ou monter un CD ISO sur la machine virtuelle pour les appareils virtuels ESXi. Cela vous permet d'accéder à l'interpréteur de

commandes et de réinitialiser l'utilisateur et/ou le mot de passe.

Conditions préalables

Configuration requise pour On-prem (appareil physique)

- Vous devez télécharger une image ISO pour Ubuntu 22.04 ou version ultérieure à partir de https://ubuntu.com/download/desktop. Cela est dû à la façon dont le système de fichiers change dans Ubuntu 22.04 avec xfs.
- Une fois l'ISO téléchargé sur le système local, vous devez monter l'ISO sur le KVM du contrôleur de gestion intégré Cisco (CIMC).
- Une fois l'ISO monté sur le KVM, vous devez démarrer à partir de l'ISO.
- Une fois que vous pouvez accéder à Ubuntu, montez les répertoires racine et var sur le système.
- Après avoir monté les répertoires racine et var, vous pouvez déverrouiller et modifier le compte utilisateur Maglev.
- Enfin, vous 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.

Configuration requise pour l'appliance virtuelle (ESXi)

- Télécharger ISO
- Télécharger l'ISO vers l'emplacement du fichier ISO du data store ou la bibliothèque de contenu dans vSphere/vCenter
- Ajouter un CD/DVD à la machine virtuelle (machine virtuelle)
- Remplacer le délai de démarrage par une valeur supérieure

Composants utilisés

Cette opération a été exécutée sur l'image Ubuntu 25.10 ; une image différente produit des temps et des résultats différents.

Dans certains environnements, il a fallu jusqu'à 2 heures pour atteindre le bureau Ubuntu, mais pour la plupart des clients, le processus se termine en 30 minutes.

Cette opération n'est pas strictement limitée à la version de bureau d'Ubuntu. Tout ce qui est requis est l'accès au shell. Toute image d'Ubuntu à la version 22.04 ou plus récente qui fournit l'accès shell fonctionne pour cette opération. D'autres images peuvent également fonctionner comme Gentoo et Linux SystemRescue, mais Cisco recommande d'utiliser Ubuntu 25.10. Toute

autre tentative est à la charge de l'utilisateur lui-même.

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 : vous pouvez utiliser la même procédure dans un environnement DR. Toutefois, notez les points suivants :

*** Assurez-vous que la reprise après sinistre est en PAUSE avant d'essayer toute méthode de récupération/réinitialisation de mot de passe ***

Dans un déploiement de DR 1+1+1, le site correspondant est arrêté tant que ce processus est terminé.

Dans un modèle 3+3+3, si vos mots de passe doivent être mis à jour sur les trois noeuds, effectuez cette opération noeud par noeud pour vous assurer que les deux autres noeuds sont disponibles afin d'éviter un basculement de routeur désigné inutile.

---

lesta

Étape 1a : Démarrage à partir du CD Live (sur site)

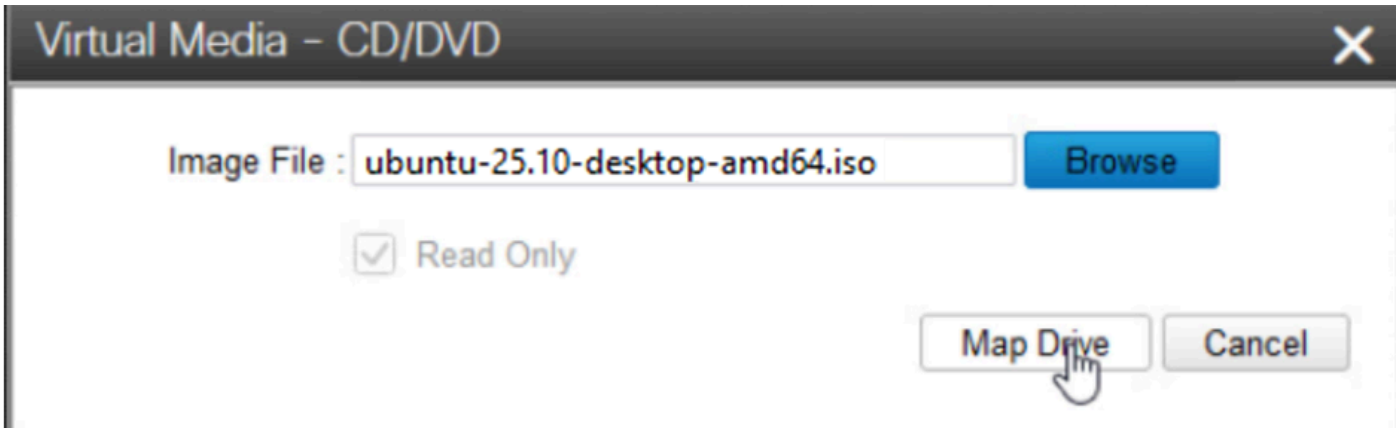
Connectez-vous à l'interface utilisateur graphique de Cisco IMC, choisissez Launch KVM, puis choisissez Virtual Media > Activate Devices.



Ensuite, revenez à Virtual Media et choisissez Map CD/DVD.



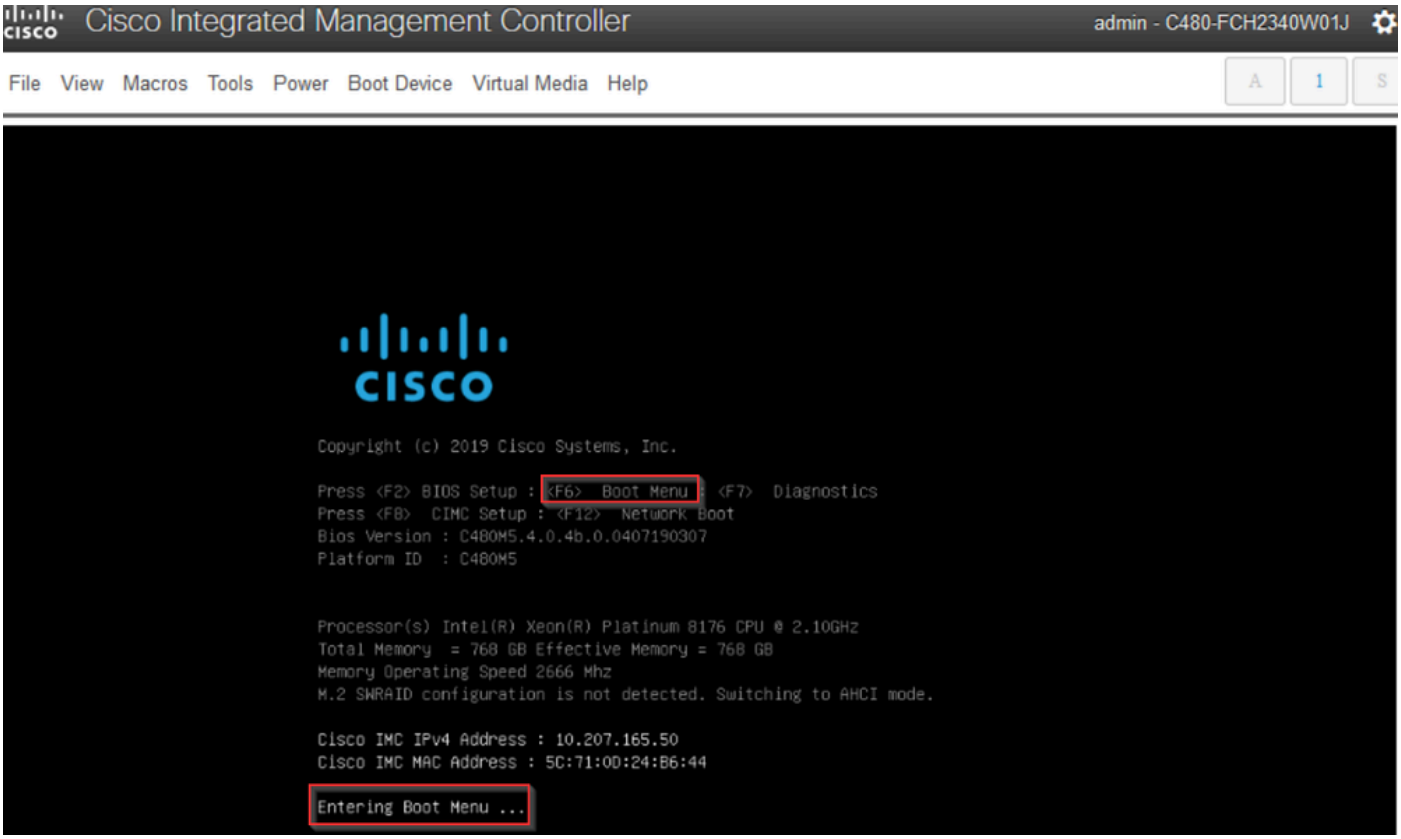
Après cela, choisissez Browse, puis sélectionnez l'image ISO Ubuntu que vous avez téléchargée sur votre système local. Après avoir sélectionné l'image Ubuntu, choisissez le bouton Mapper le lecteur.



Vous pouvez confirmer que l'image est activée et mappée en revenant à Virtual Media et en voyant l'ISO mappée comme une option.

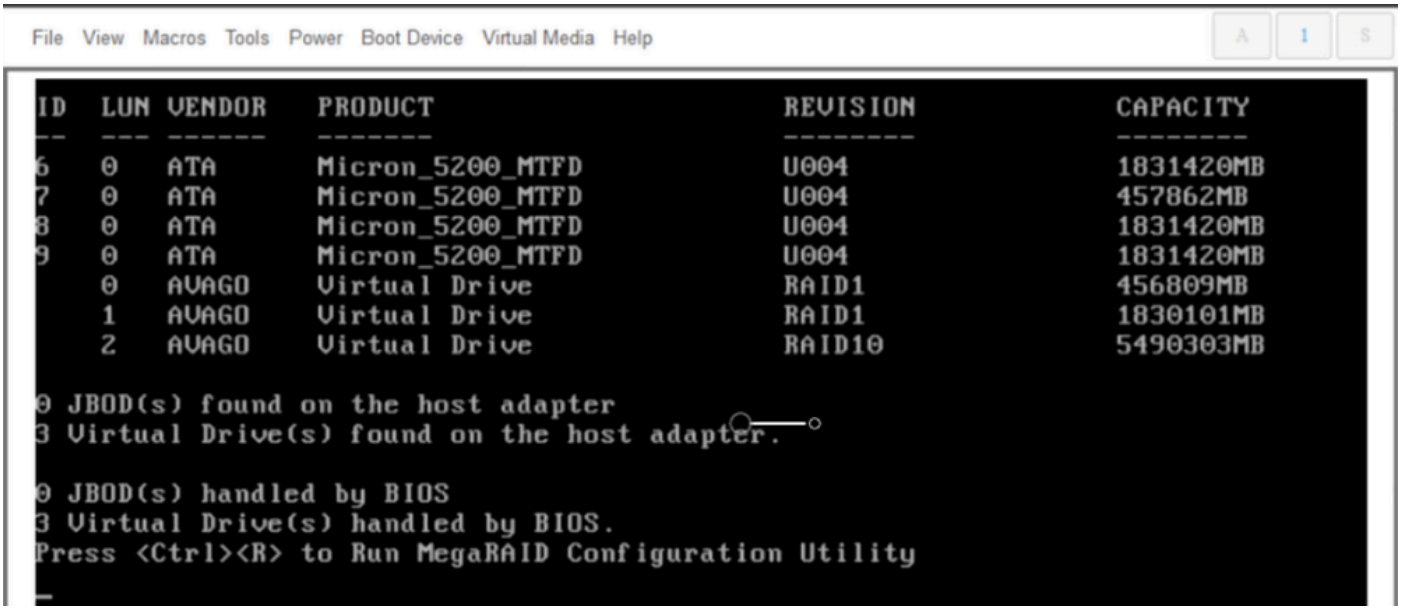
Mettez ensuite le périphérique sous tension puis sous tension avec Power > Reset System (démarrage à chaud).

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

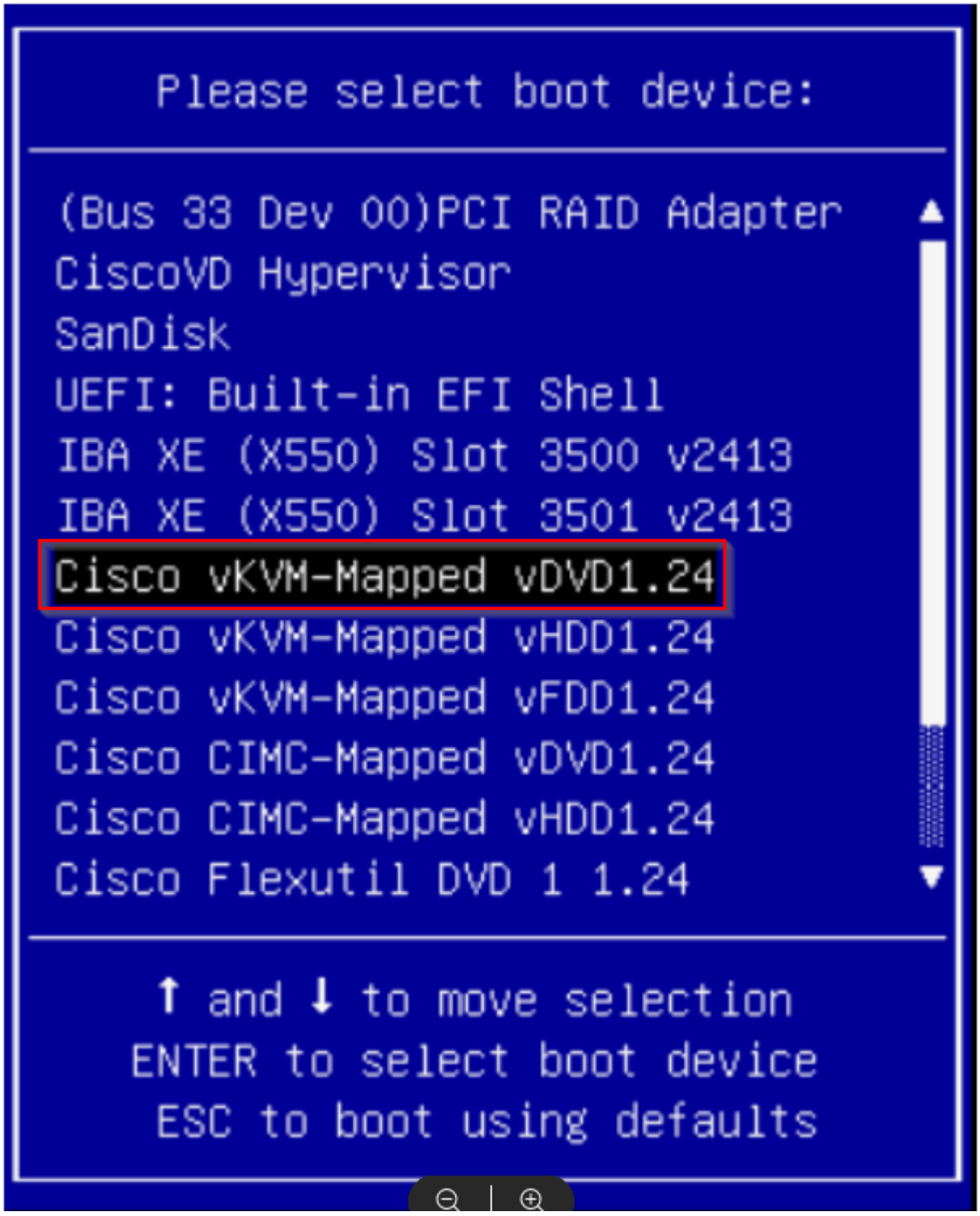


Nous savons si cela fonctionne car vous voyez "Entering Boot Menu ..." en bas de l'écran.

Mais un deuxième écran apparaît et nous pouvons voir qu'il entre dans le menu de démarrage. Si nous avons oublié d'appuyer sur F6 sur le premier écran Cisco, nous pouvons appuyer dessus ici.

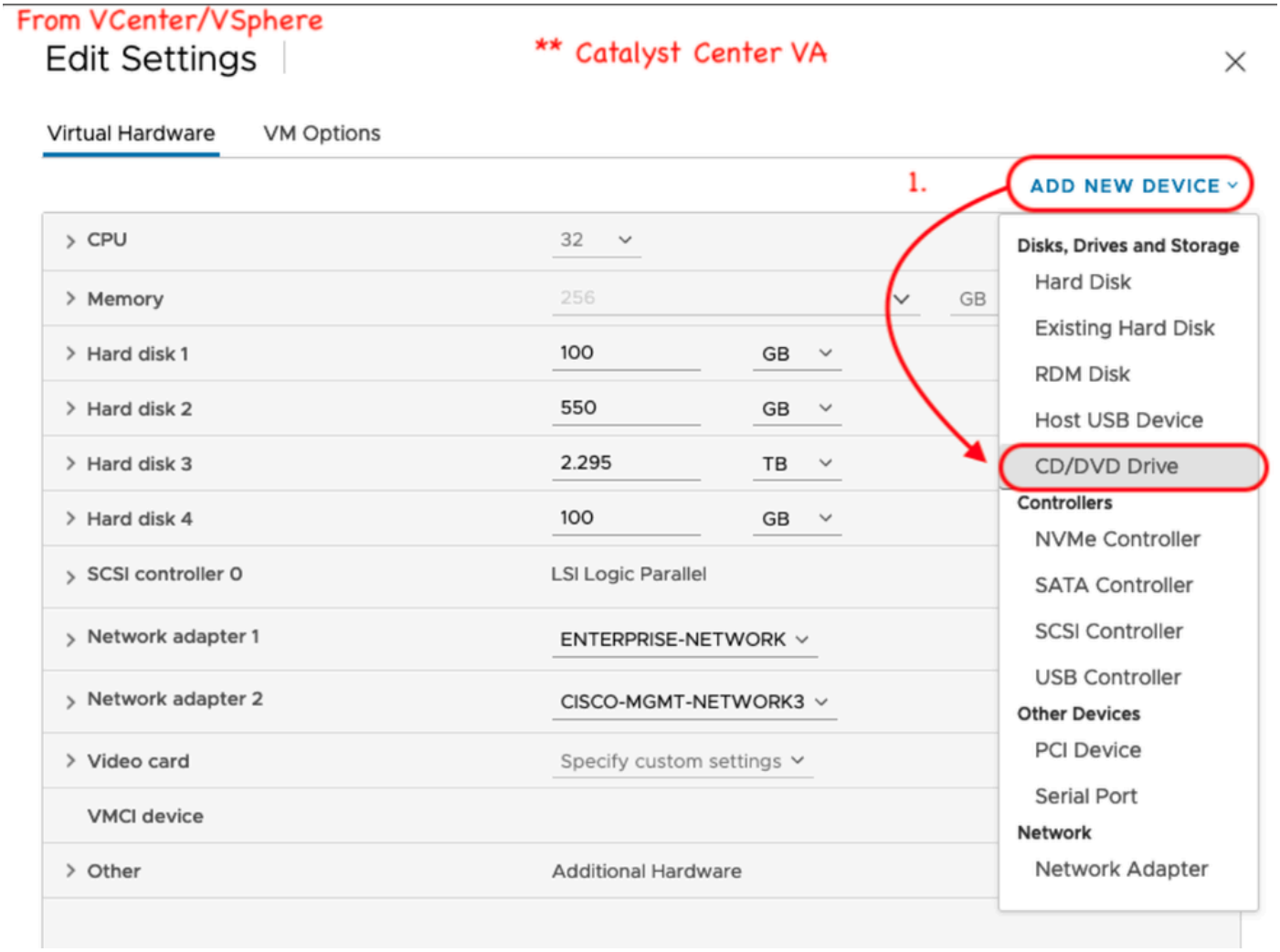


Lorsque le menu d'amorçage apparaît, choisissez l'option qui indique Cisco vKVM-Mapped vDVD1.24. Cela entraîne l'amorçage du matériel à partir de l'image Ubuntu mappée sélectionnée précédemment.

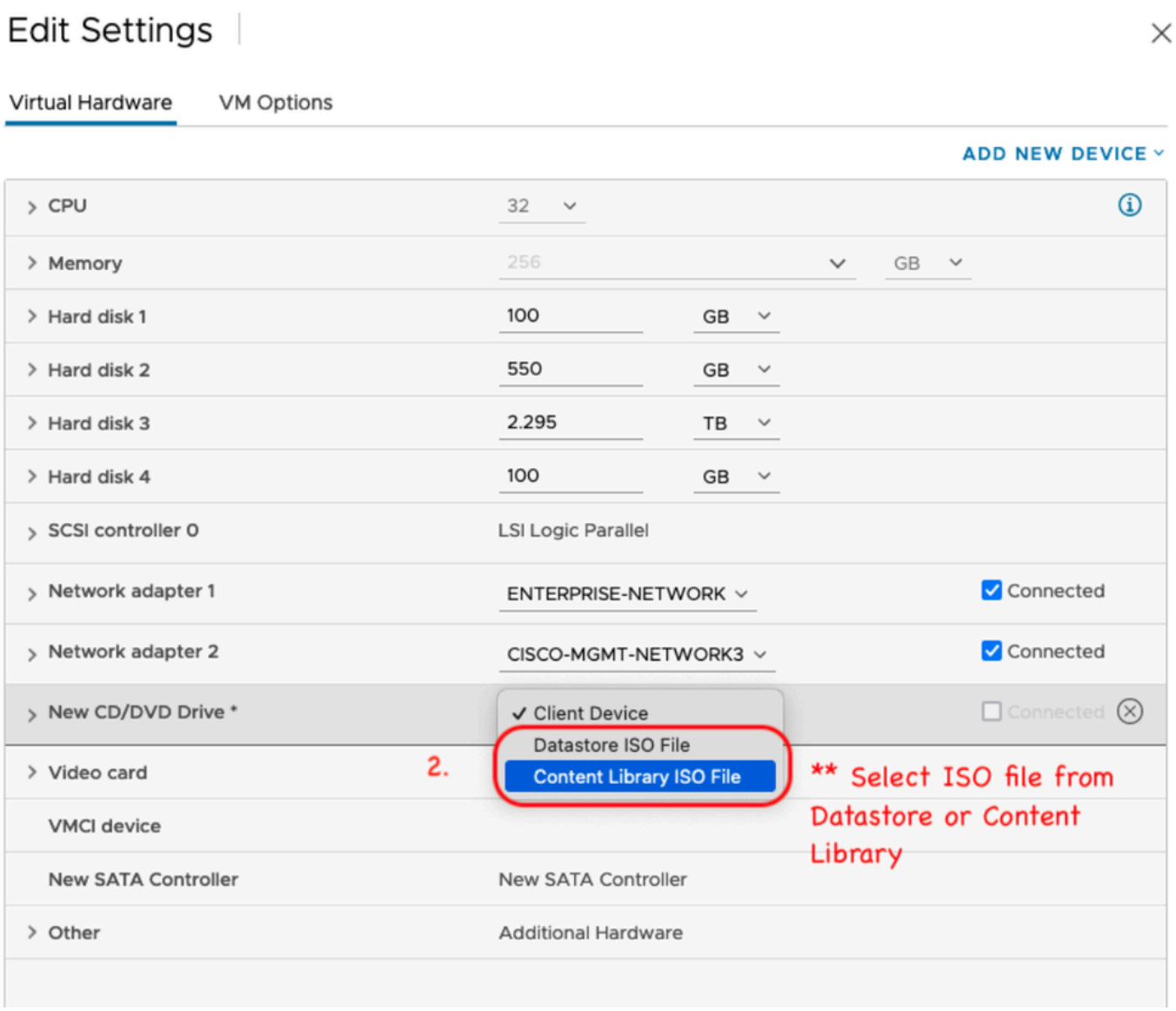


Étape 1b : Démarrage à partir d'un CD Live (VA - ESXi)

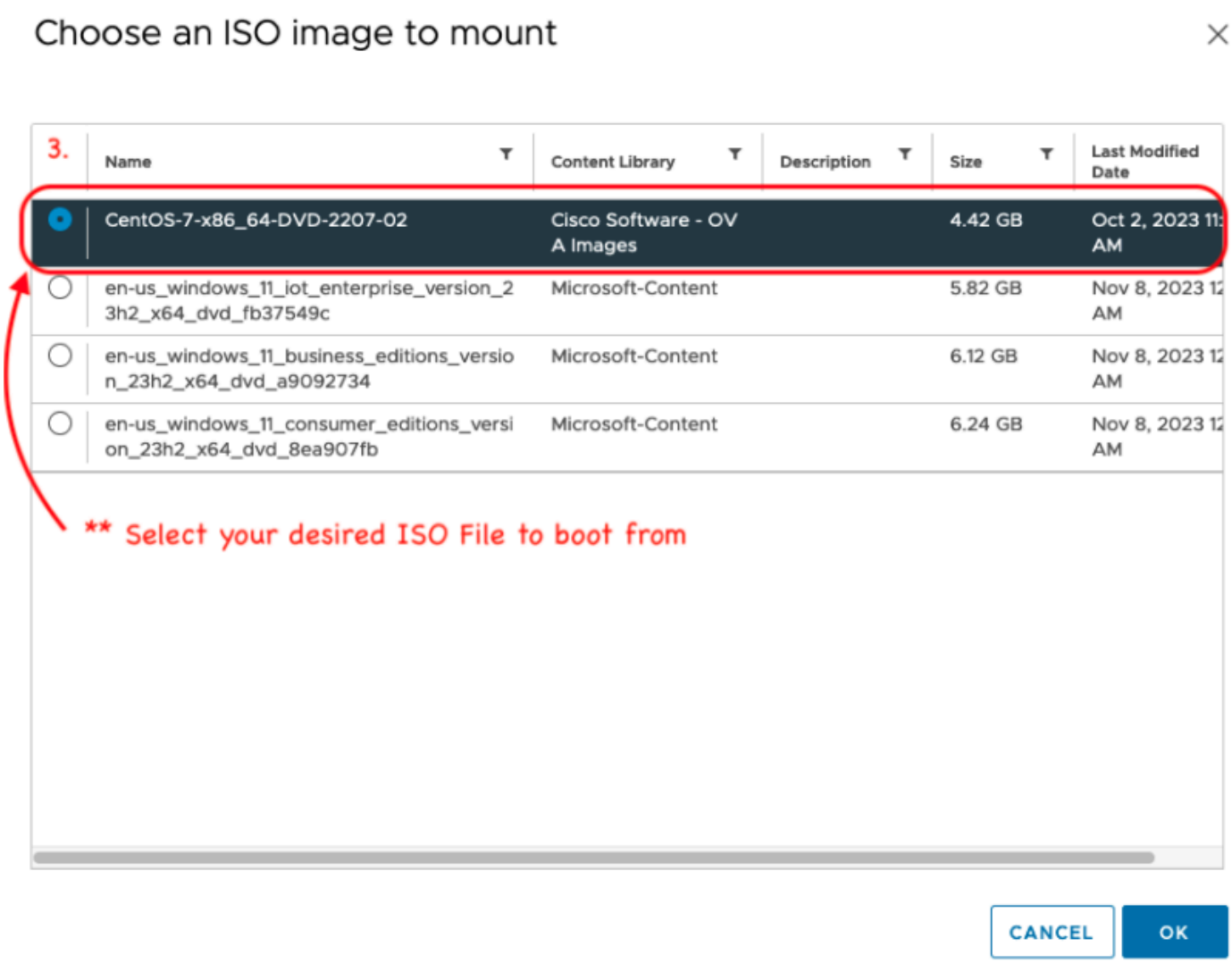
Dans vCenter/vSphere, accédez à l'emplacement de la VM, cliquez avec le bouton droit sur la VM et cliquez sur Edit Settings. Cliquez ensuite sur ADD NEW DEVICE, puis sélectionnez CD/DVD Drive.



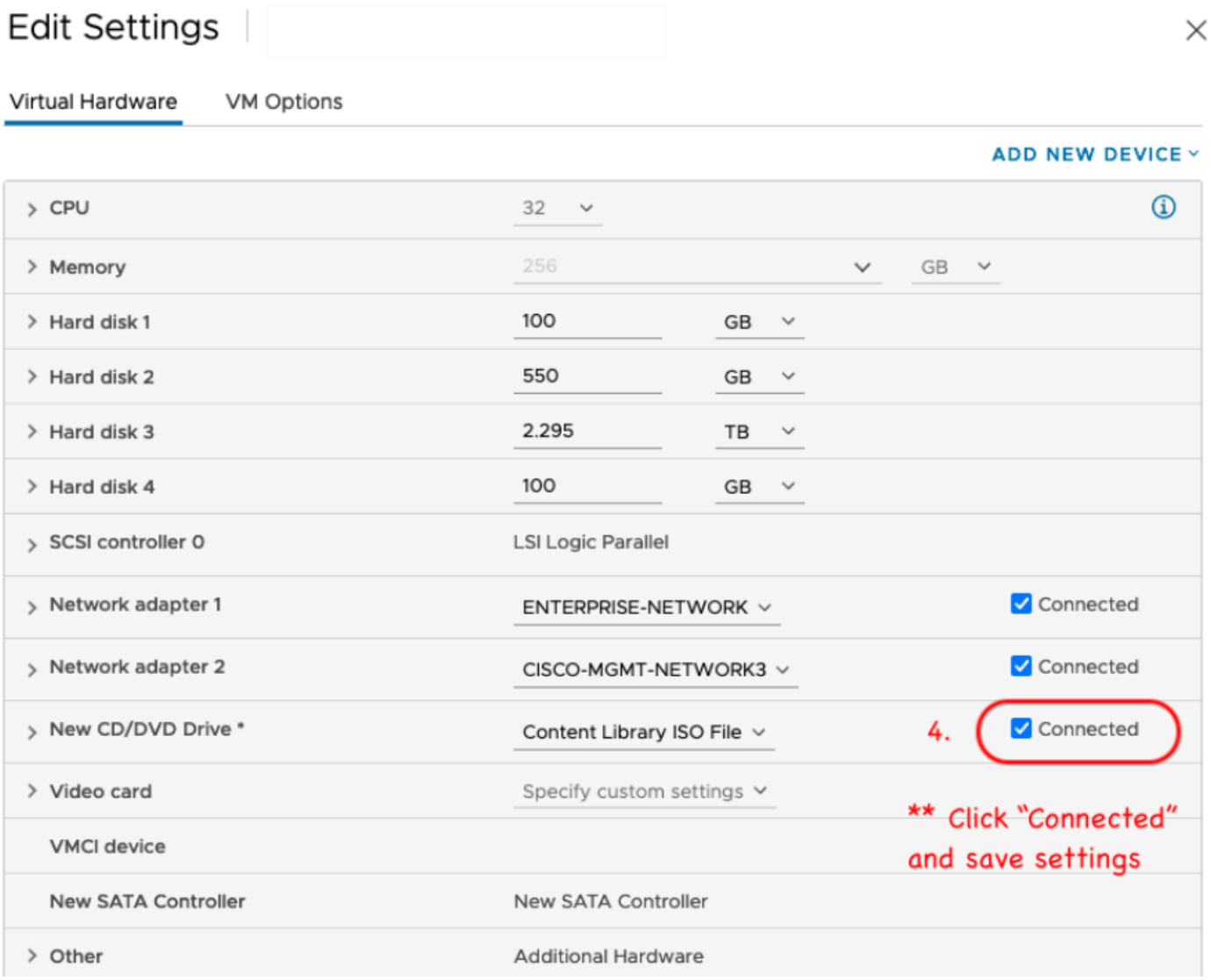
Le lecteur de CD/DVD s'affiche désormais dans la page des paramètres comme Nouveau lecteur de CD/DVD. Si vous avez téléchargé l'ISO dans le fichier ISO du data store, choisissez cette option pour le CD/DVD. Sinon, choisissez Fichier ISO de la bibliothèque de contenu.



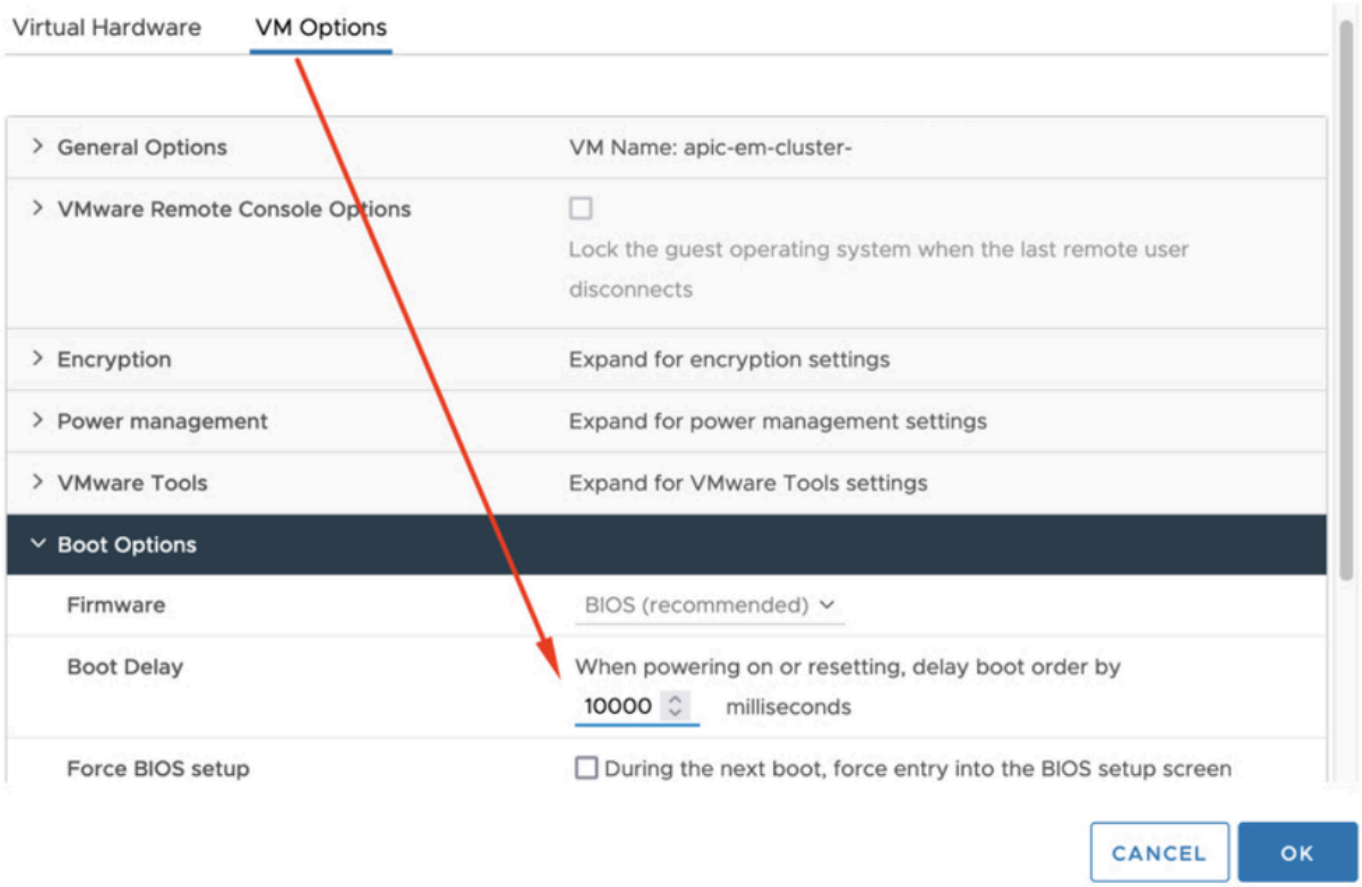
Sélectionnez le fichier ISO à partir duquel démarrer. Pour cette procédure, utilisez l'Ubuntu 25.10 ISO.



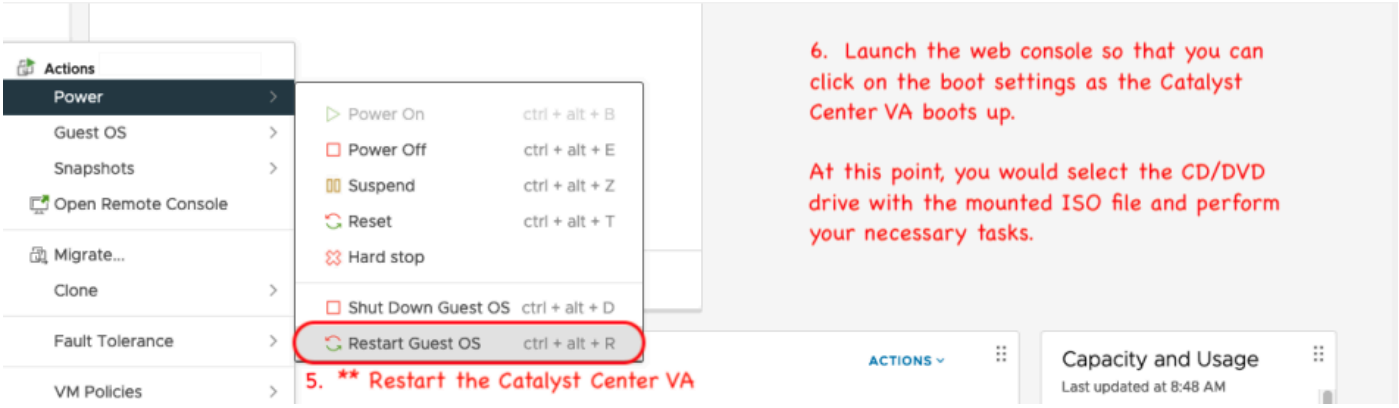
Assurez-vous ensuite d'activer la case Connected à droite du New CD/DVD Drive.



Cliquez sur VM Options en haut de l'écran des paramètres. Cliquez ensuite sur la flèche vers le bas pour Options de démarrage et modifiez la valeur de Délai de démarrage à une valeur plus grande, telle que 10000. Cela vous donne le temps de voir l'option pour entrer dans le menu de démarrage après le redémarrage de la VM.



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

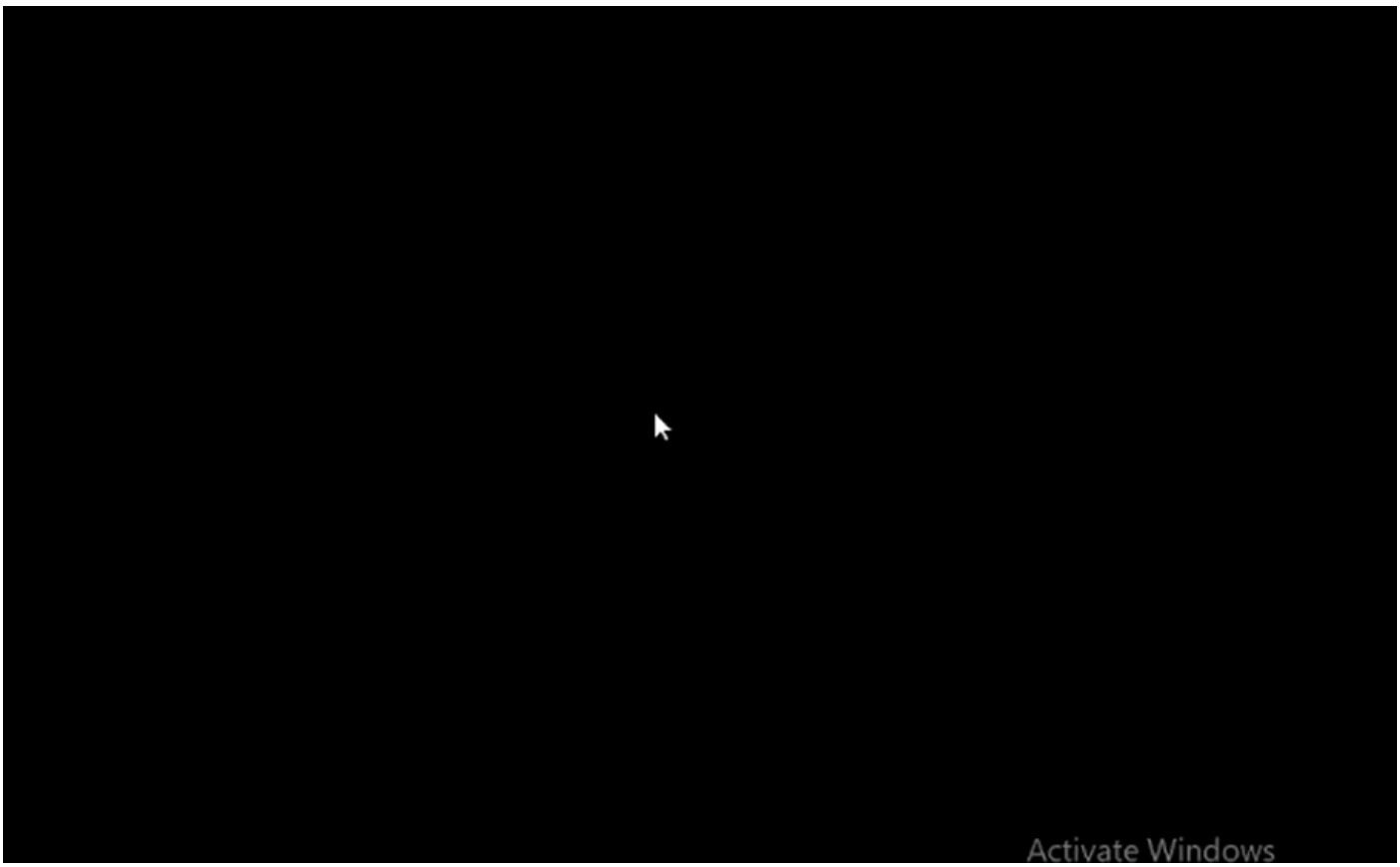


Étape 2a: Chargement dans l'ISO Ubuntu

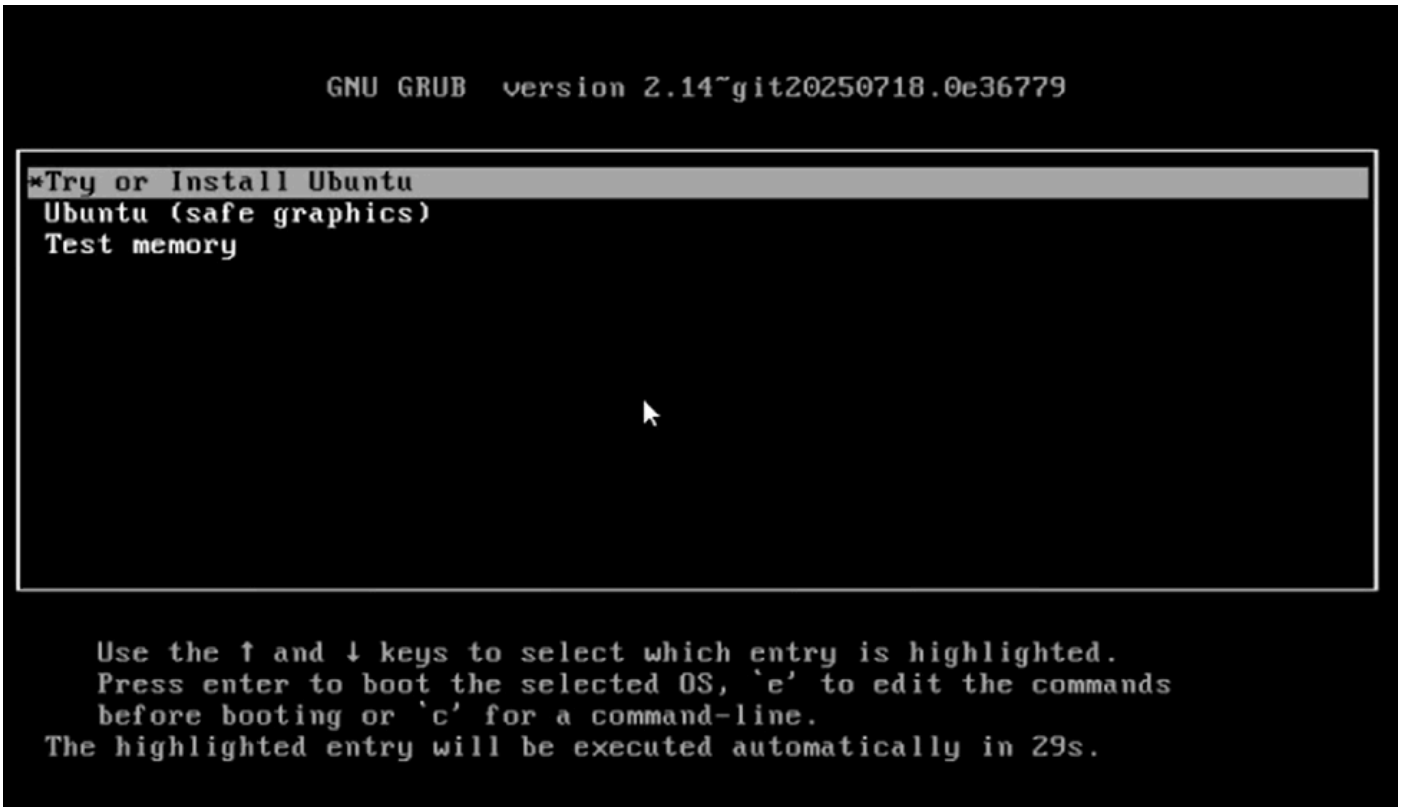
Remarque : *** Les captures d'écran illustrent le temps nécessaire pour atteindre le bureau Ubuntu dans les travaux pratiques. Ils diffèrent selon l'environnement et l'image

utilisés pour la récupération ***

C'est le premier écran qui nous est présenté. On dirait que rien ne se passe, mais attendez. Au cours des travaux pratiques, nous restons sur cet écran pendant 40 secondes



Après cela, on nous a présenté ces options. Choisissez Try or Install Ubuntu pour continuer.



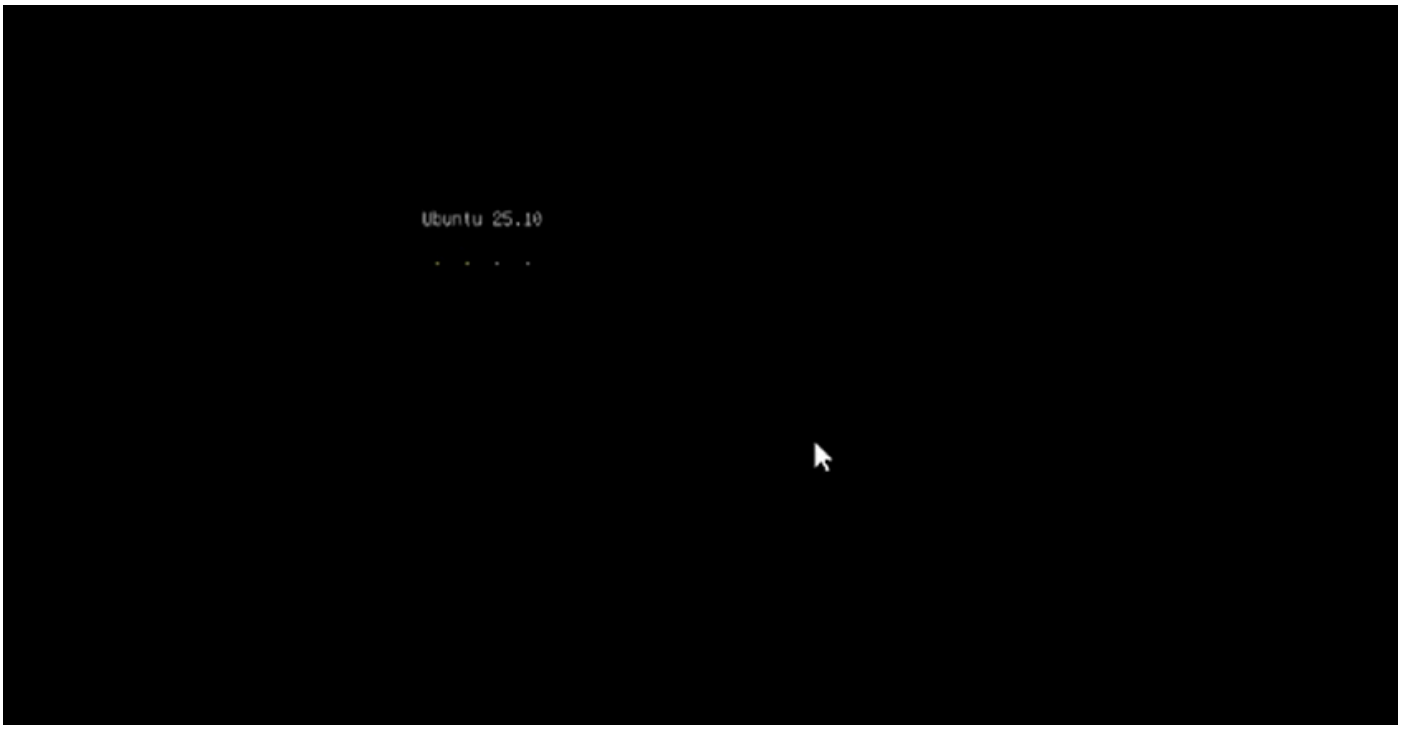
Ensuite, le processus a pris environ 3 minutes pour atteindre cet écran.



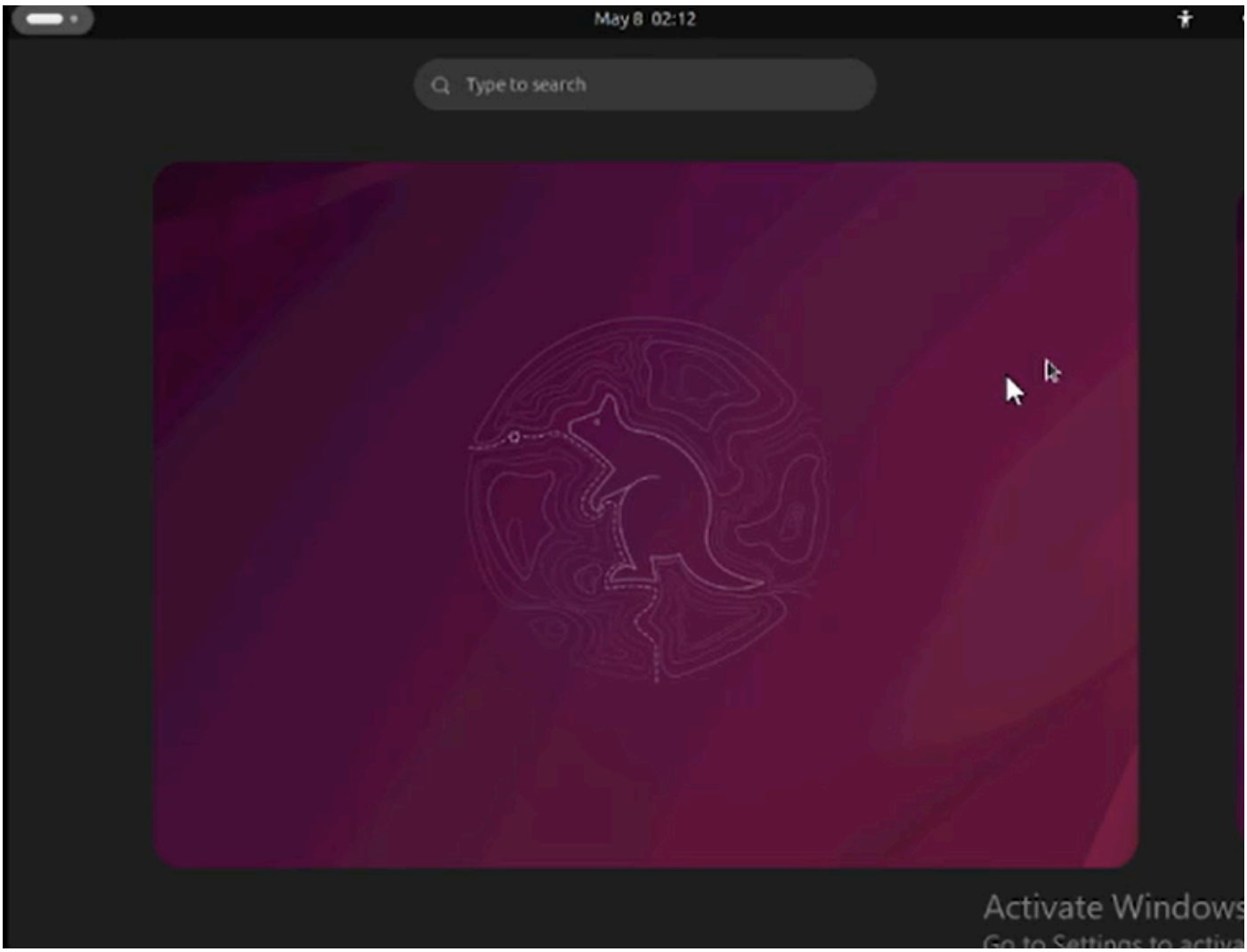
Après 11 minutes supplémentaires, l'écran affichait toujours l'Ubuntu 25.10.



Ensuite, l'écran est revenu à un écran noir pendant environ 30 secondes avant d'afficher Ubuntu 25.10 dessus.



Après 10 minutes supplémentaires, l'écran est passé à l'écran de chargement d'Ubuntu.



Le chargement du bureau Ubuntu prend environ 5 minutes. Le programme d'installation est automatiquement chargé et peut être quitté en toute sécurité en cliquant sur le X en haut à droite de la fenêtre du programme d'installation.



Une fois l'installateur fermé, ouvrez une fenêtre de terminal et passez à l'étape 2b.

*** RAPPEL : Dans certains environnements, il a fallu jusqu'à 2 heures pour en arriver là. Lors de cette manifestation, il a fallu environ 35 minutes pour le rejoindre. ***

Étape 2b : Montage des partitions requises

Une fois que vous avez accès à l'environnement graphique du bureau Ubuntu, vous devez ouvrir l'application de terminal et effectuer ces étapes

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

Commencez par créer le point de montage temporaire avec la commande suivante :

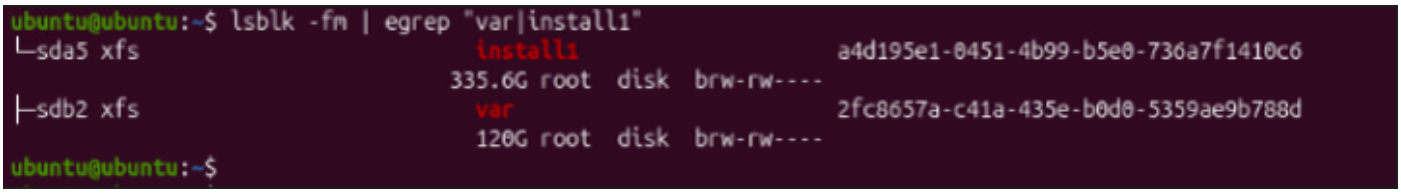
<#root>

```
sudo mkdir /altsys
```

Ensuite, nous devons trouver les partitions racine et var à monter. Nous pouvons utiliser la commande lsblk -fm | egrep "var|install1" pour rechercher la partition à monter pour "install1" (racine) et "var". Notez la partition que nous avons identifiée pour les commandes mount à l'étape suivante

Pour var, nous avons trouvé une correspondance avec la partition 120G. Nous pouvons voir dans ce cas qu'il s'agit de sdb2

Pour install1 (racine), nous avons trouvé une correspondance avec la partition 335.6G. Dans cet exemple, c'est sda5



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

<#root>

```
sudo mount /dev/sda5  /altsys
```

```
sudo mount /dev/sdb2 /altsys/var
```

Une fois que root et var ont été montés, montez les systèmes de fichiers pseudo :

<#root>

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

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

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

La dernière étape avant de modifier le mot de passe ou de déverrouiller le compte Maglev est de passer à l'environnement de montage temporaire :

<#root>

```
sudo chroot /altsys
```

Cas d'utilisation 1 : Déverrouiller un compte Maglev

Étape 1: Vérifiez que l'utilisateur maglev est déverrouillé

<#root>

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

<#root>

```
maglev:

!

$6$6jvRGoDihpcsr8Xl$RUFs.Lb.2AbbgvODfJsw4b2EnpSwiNUlwJ6NQIjEnvOtT5Svz4ePHZa4fOeUvLHl7VAFca46f2nHxqMWORY
```

Vérifiez s'il y a un point d'exclamation devant le hachage du mot de passe ou non. Si tel est le cas, cela indique que le compte est verrouillé. Entrez la commande permettant de déverrouiller l'utilisateur :

Déverrouillez l'utilisateur maglev à l'aide de la commande :

<#root>

```
usermod -U maglev
```

Étape 2: Échec de réinitialisation du nombre

Si l'utilisateur n'a pas de marque d'escalade devant le hachage dans le fichier/etc/shadowfile, alors la limite d'échec de connexion a été dépassée. Suivez ces étapes pour réinitialiser les tentatives de connexion ayant échoué.

Recherchez les tentatives de connexion infructueuses pour l'utilisateur maglev :

<#root>

faillock --user maglev

```
maglev:
When                Type  Source                                    Valid
2026-06-23 16:58:38 RHOST x.x.x.x                                       V
2026-06-23 16:58:42 RHOST x.x.x.x                                       V
2026-06-23 16:58:52 RHOST x.x.x.x                                       V
2026-06-23 16:58:56 RHOST x.x.x.x                                       V
2026-06-23 16:59:10 RHOST x.x.x.x                                       V
2026-06-23 16:59:15 RHOST x.x.x.x                                       V
```

Comme indiqué ici, les tentatives de connexion sont plus importantes que les 6 tentatives par défaut. Cela empêche l'utilisateur de se connecter jusqu'à ce que le nombre d'échecs tombe à moins de six (6). Vous pouvez réinitialiser le nombre d'échecs de connexion à l'aide de la commande :

<#root>

faillock --user maglev --reset

Vous pouvez confirmer que le compteur a été réinitialisé :

<#root>

faillock --user maglev

Si rien n'est renvoyé, les entrées ont été réinitialisées/effacées.

Cas d'utilisation 3 : Réinitialiser le mot de passe utilisateur Maglev

Étape 1: 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 2: Redémarrez normalement l'environnement Cisco Catalyst Center

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



Vous voyez probablement cette image coincée pendant environ 5 à 10 minutes. This is normal. L'écran passe ensuite à l'écran de connexion.

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

Une fois que le logiciel Cisco Catalyst Center démarre et que vous avez accès à la CLI, vous

devez modifier le mot de passe Maglev avec la commande sudo maglev-config update. Cette étape est nécessaire pour s'assurer que le changement prend effet dans l'ensemble du système.

Une fois que l'assistant de configuration a été lancé, vous devez naviguer complètement à travers l'assistant à l'écran qui nous permet de définir le mot de passe Maglev à l'étape 6.



Une fois que le mot de passe a été défini pour les deux champs Linux Password et Re-enter Linux Password, choisissez next et complétez l'assistant. Lorsque l'assistant a terminé l'envoi de la configuration, le mot de passe a été modifié. Vous pouvez créer une nouvelle session SSH ou entrer la commande sudo -i dans la CLI pour tester que le mot de passe a été modifié.

Guide vidéo étape par étape

Veuillez utiliser le lien pour accéder à la vidéo étape par étape créée pour ce flux de travail.

Images fournies par Tomas De Leon et Faisal Mehmood

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.