Maglev用户密码重置故障排除

目录

简介

环境

- 内部物理设备详细信息
- 虚拟设备ESXi详细信息
- 使用的组件

分辨率

- 步骤 1：确认访问权限并选择正确的工作流程
- 步骤 1a：从现场CD启动
- 步骤 1b：从实时CD VA启动 — ESXi
- 步骤 2a：加载到Ubuntu ISO
- 步骤 2b：安装所需分区
- 步骤 3：选择恢复操作（解锁帐户或重置密码）
- 步骤 3a：检查磁悬浮帐户是否已锁定
- 步骤 3b：重置失败计数
- 步骤3c:重置Maglev用户密码
- 步骤3d:正常重启到Cisco Catalyst Center环境
- 步骤3e:从Cisco Catalyst Center CLI更新Maglev用户密码

原因

相关内容

- 分步视频指南

简介

本文档介绍如何解锁或重置Maglev用户的密码。

环境

此操作适用于本地物理设备和虚拟设备VMware ESXi部署。

内部物理设备详细信息

- 从Ubuntu Desktop下载页面下载Ubuntu 18.04或更高版本的ISO映像。建议使用Ubuntu 18.04作为与Cisco Catalyst Center相同的版本。
- 将ISO下载到本地系统后，将其安装到思科集成管理控制器(CIMC)KVM。

- 将ISO安装到KVM后，从ISO启动。
- 在Ubuntu可访问后，将根目录和var目录安装到系统。
- 在安装root目录和var目录后，解锁或更改Maglev用户帐户。
- 最后，重新启动设备，确认可以使用磁悬浮登录，并使用配置向导重置密码。

虚拟设备ESXi详细信息

- 下载Ubuntu ISO映像。
- 将ISO上传到vSphere vCenter中的Datastore ISO文件位置或内容库。
- 将CD/DVD-ROM驱动器添加到虚拟机。
- 将引导延迟更改为更大的值。

使用的组件

此操作在Ubuntu 18.04映像上运行；不同的图像会产生不同的时间和结果。在某些环境中，到达Ubuntu桌面最多需要2小时，但是对于大多数用户来说，此过程在30分钟内完成。

此操作不限于Ubuntu桌面版本。您只需要访问外壳。提供外壳访问的任何Ubuntu映像都可用于此操作。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

注意：同样的过程也适用于灾难恢复(DR)环境。在继续操作之前，请查看这些考虑事项。

警告：在尝试任何密码恢复或重置过程之前，请确保灾难恢复(DR)处于暂停状态。在1+1+1 DR部署中，当此过程完成时，相应的站点处于关闭状态。在3+3+3 DR部署中，如果必须在所有三个节点上更新密码，则一次更新一个节点以保持其他两个节点可用，并避免不必要的DR故障切换。

分辨率

步骤 1：确认访问权限并选择正确的工作流程

1.确认受影响的节点是内部物理设备还是VMware ESXi上的虚拟设备。

2.确认您对部署的管理界面具有管理访问权限：适用于物理设备的思科集成管理控制器(CIMC)或适

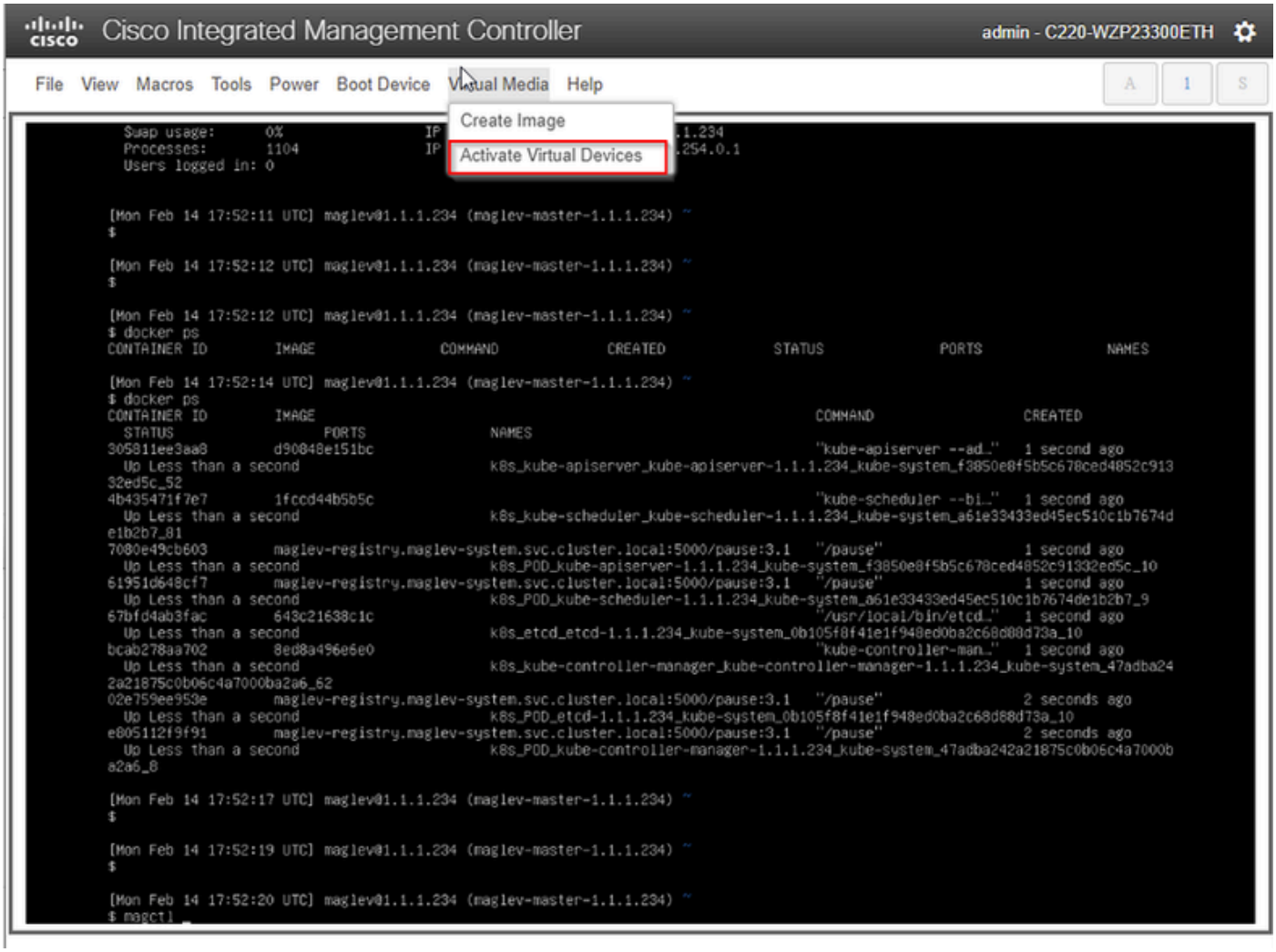
用于虚拟设备的VMware vCenter。

3.确认Ubuntu ISO映像（Ubuntu 18.04或更高版本）可用且可以安装到服务器或虚拟机。

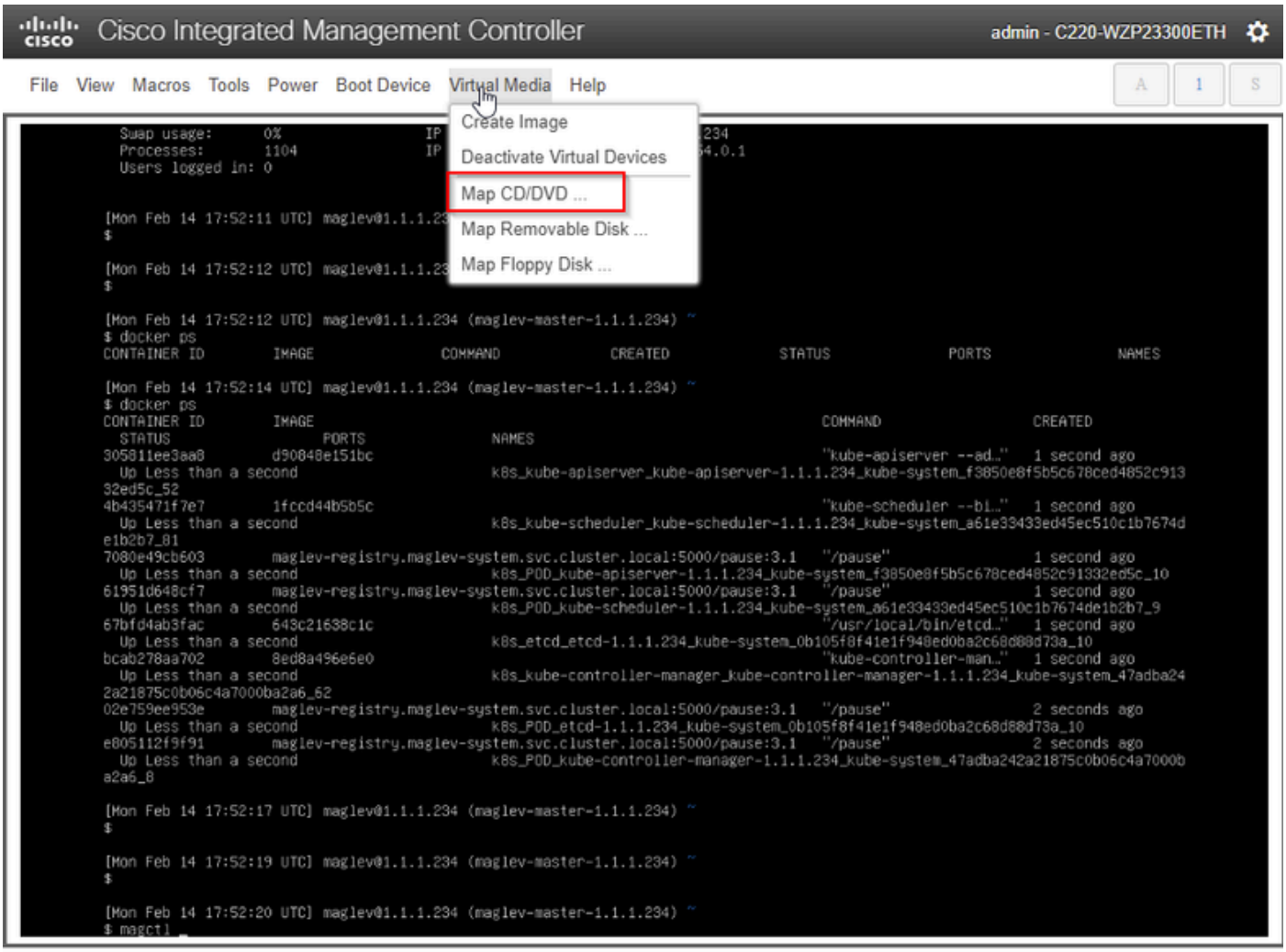
4.如果部署了灾难恢复(DR)，请确认DR处于暂停状态，然后继续。

步骤 1a：从现场CD启动

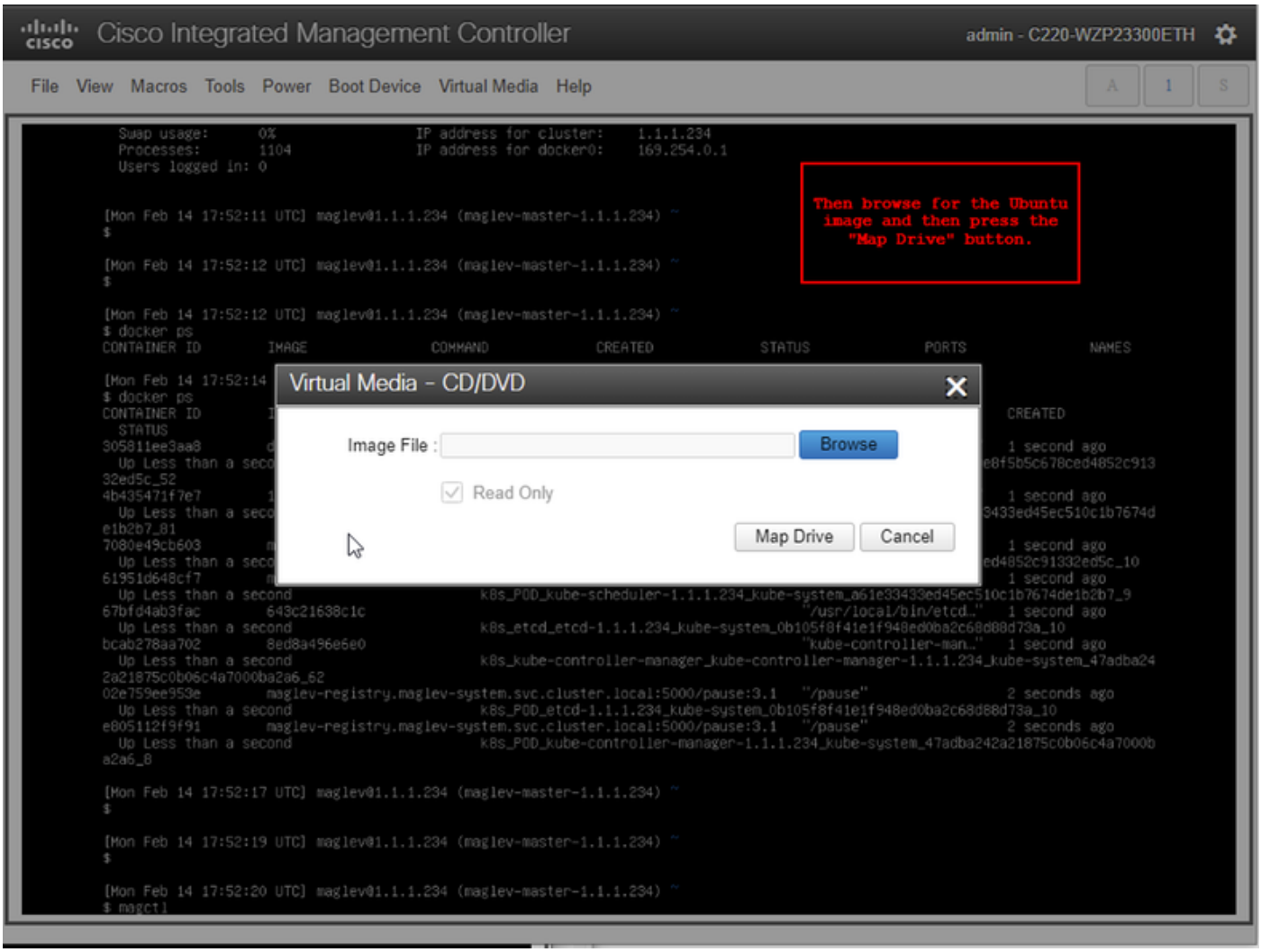
1.登录到Cisco IMC GUI，选择Launch KVM，然后选择Virtual Media > Activate Devices。

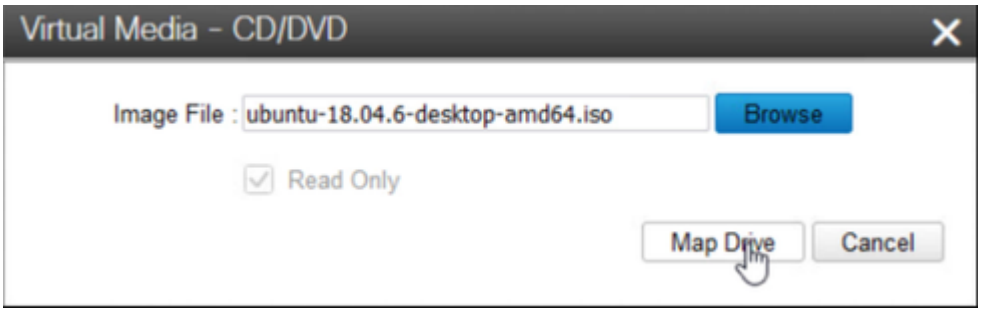


2.下一步，选择Map CD/DVD。

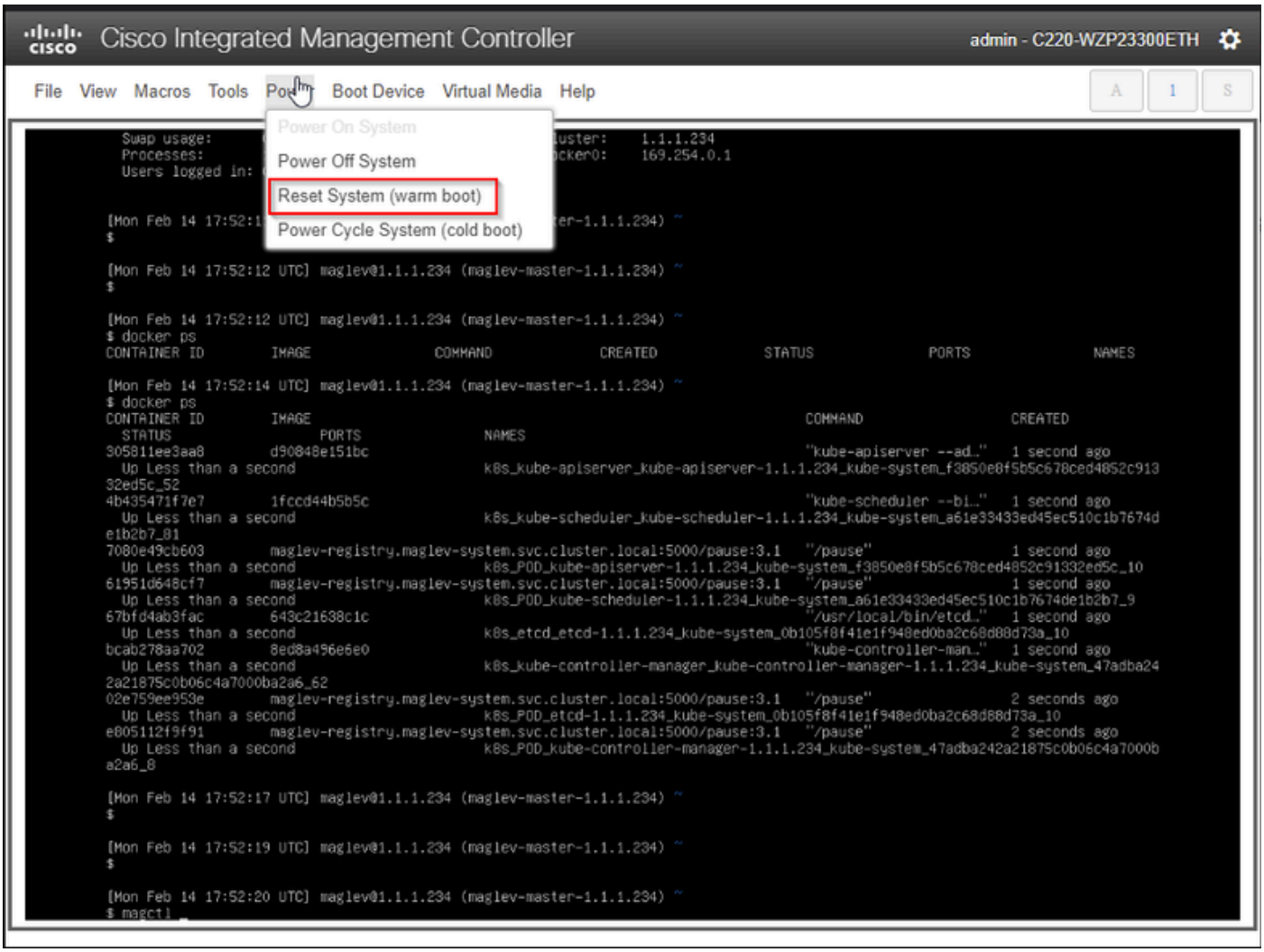


3.单击Browse，然后选择下载到本地系统的Ubuntu ISO映像。选择Ubuntu映像后，单击映射驱动器。

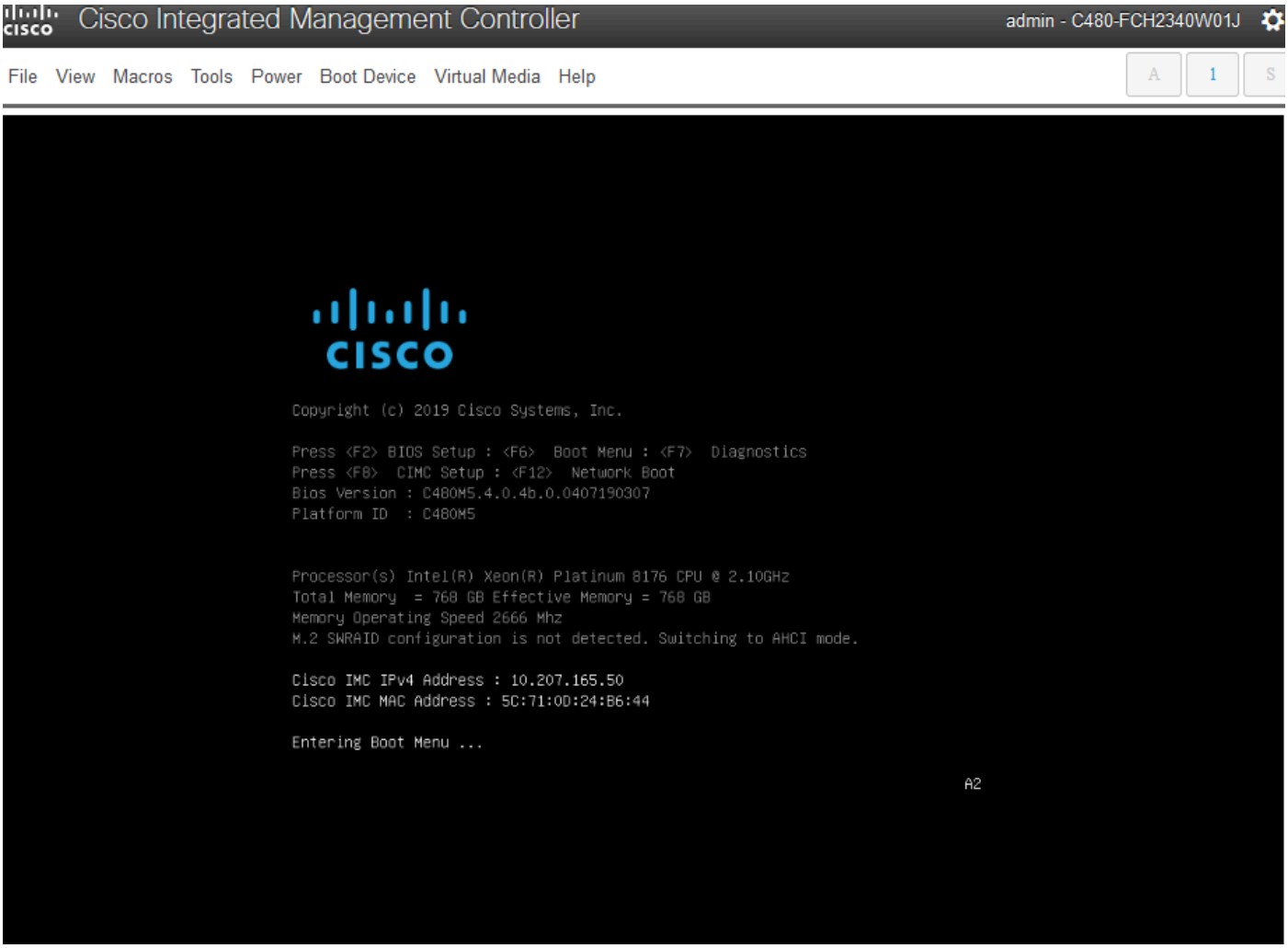


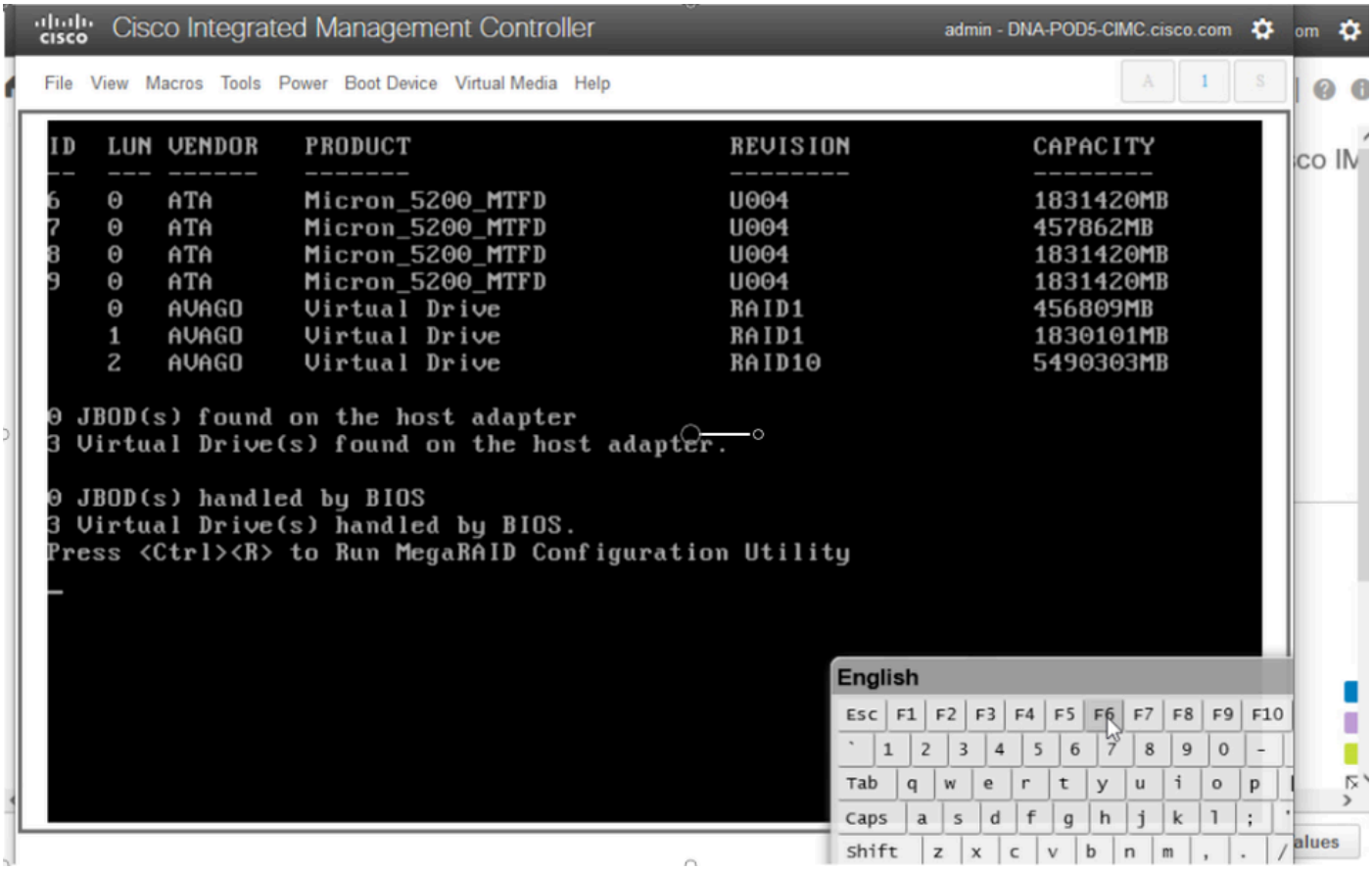


4.使用Power > Reset System (warm boot)，再次对设备重新通电。

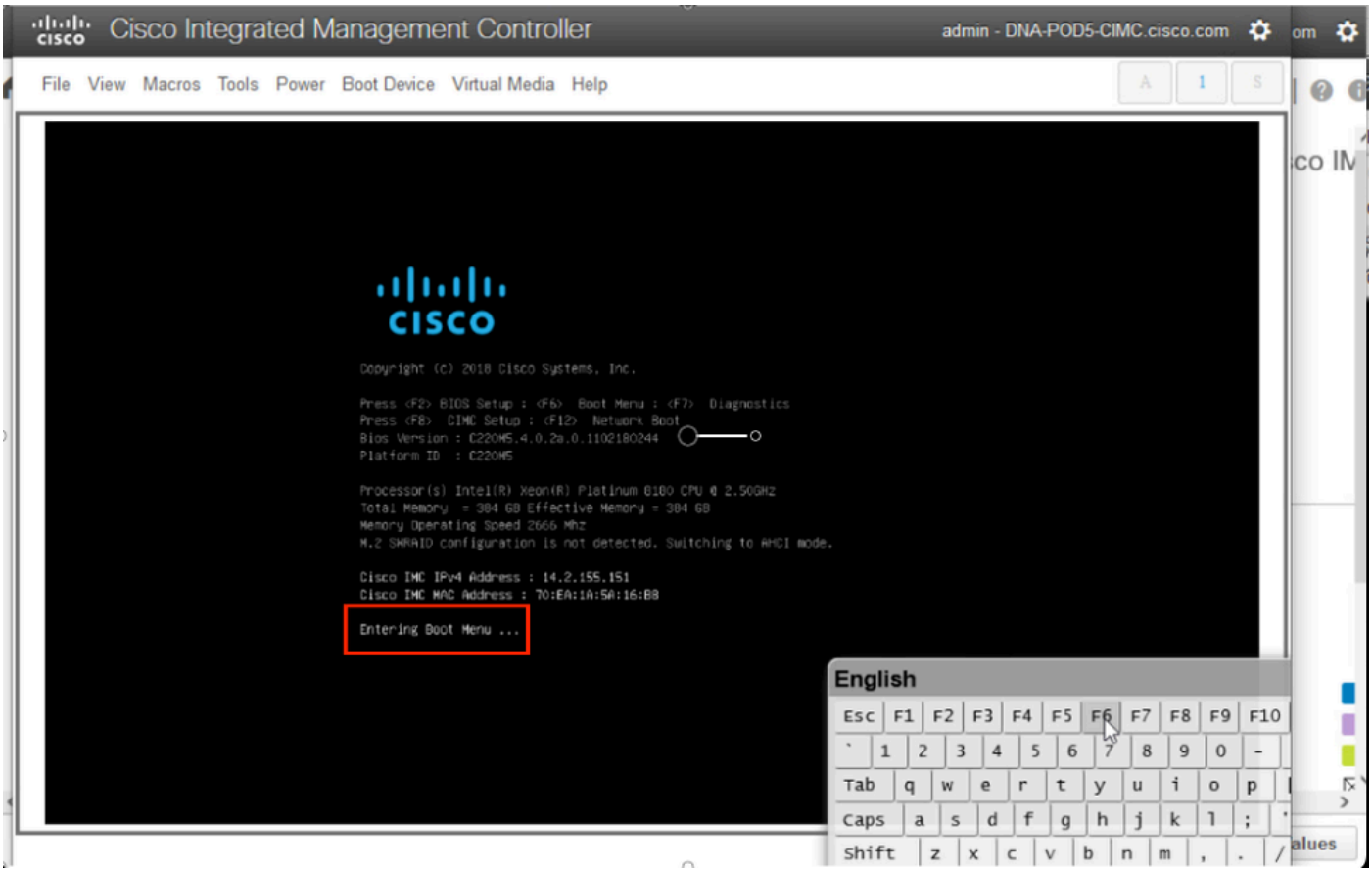


5.系统重新启动后，出现Cisco徽标时按F6。

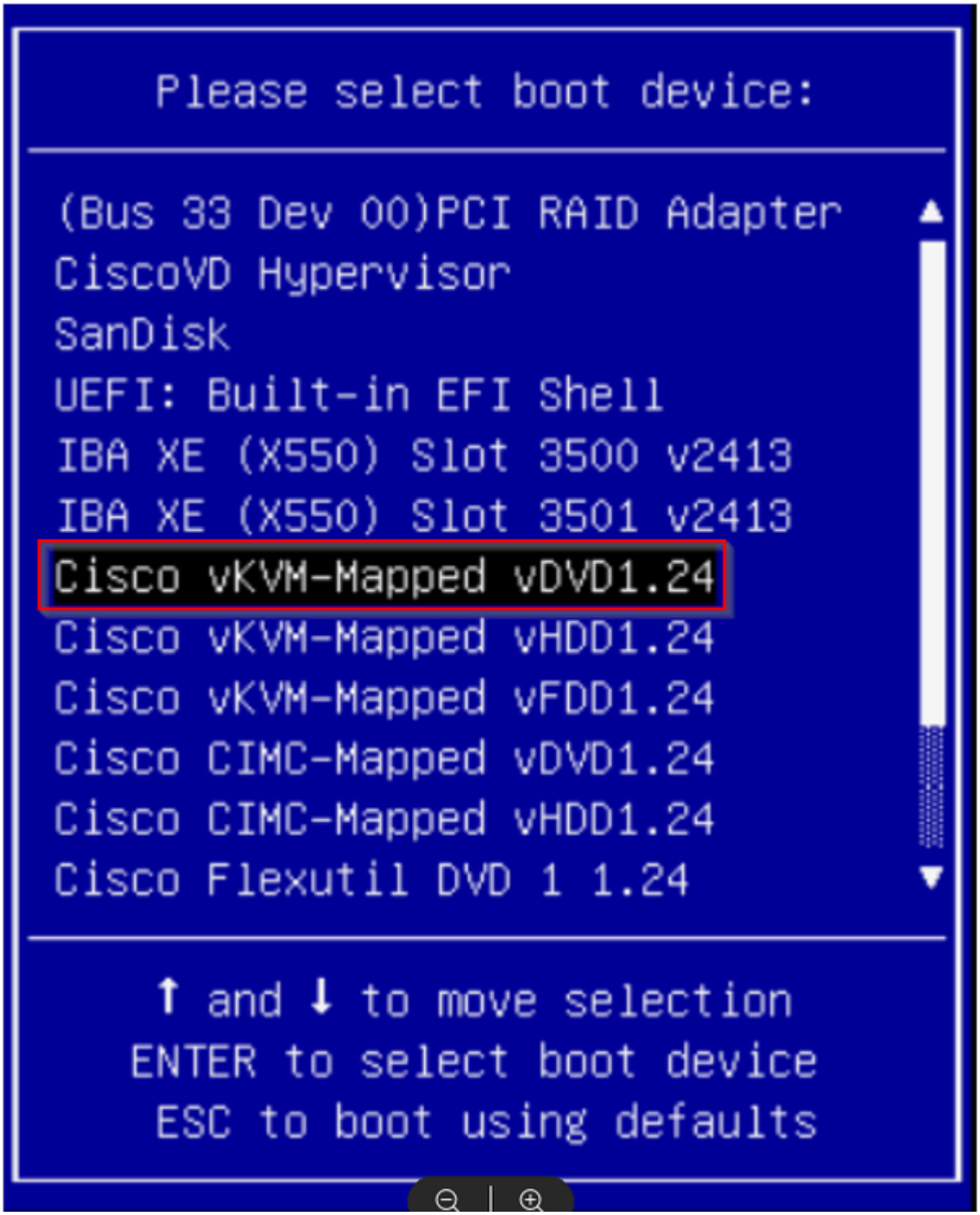

Cisco Integrated Management Controller
admin - C480-FCH2340W01J
File View Macros Tools Power Boot Device Virtual Media Help
Copyright (c) 2019 Cisco Systems, Inc.
Press <F2> BIOS Setup : <F6> Boot Menu : <F7> Diagnostics
Press <F8> CIMC Setup : <F12> Network Boot
Bios Version : C480M5.4.0.4b.0.0407190307
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.出现第二个屏幕，系统进入引导菜单。如果未在第一个Cisco屏幕上按F6，请在此处按。

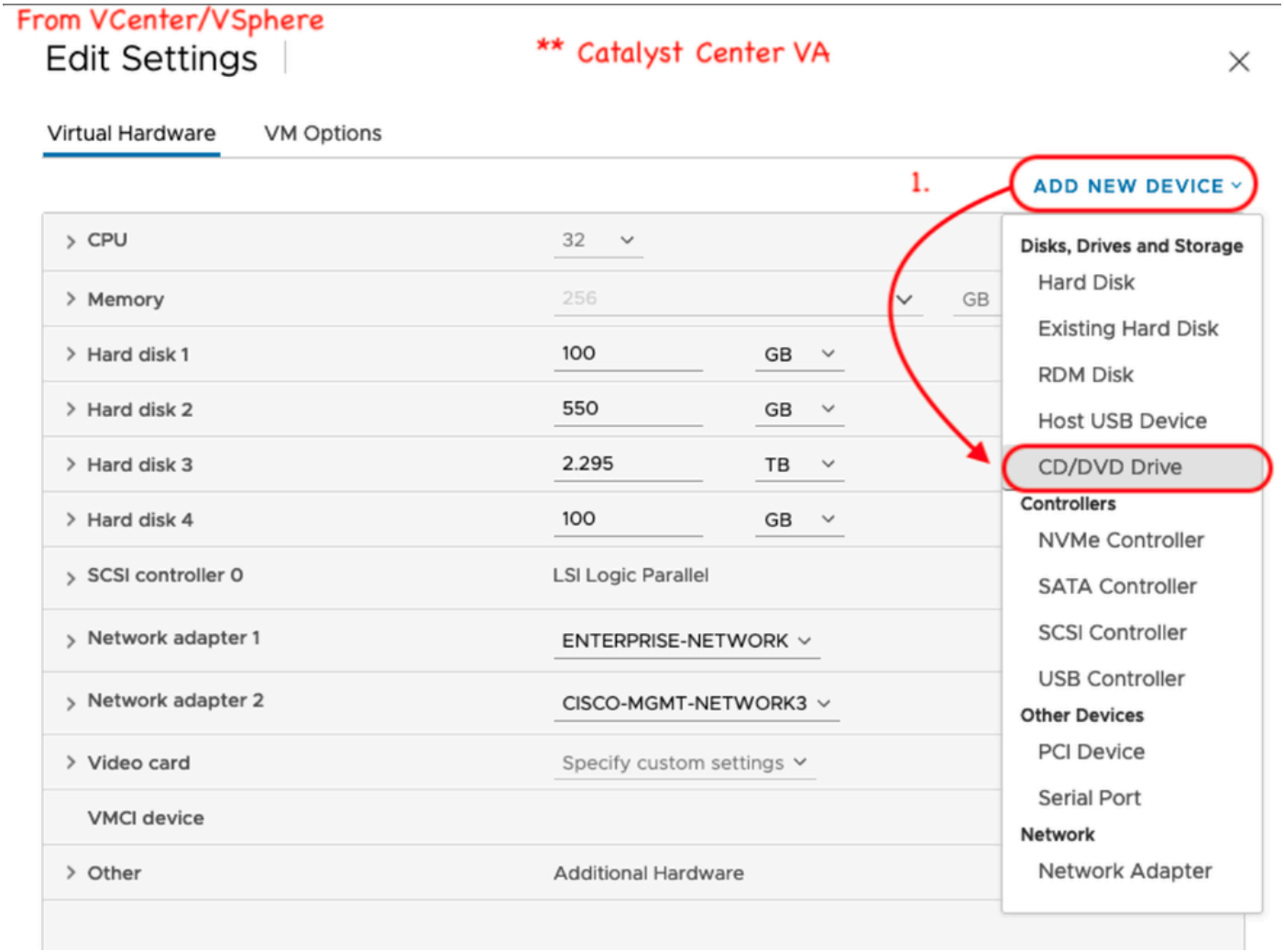


7.出现启动菜单时，选择Cisco vKVM-Mapped vDVD1.24。设备从映射的Ubuntu ISO映像启动。

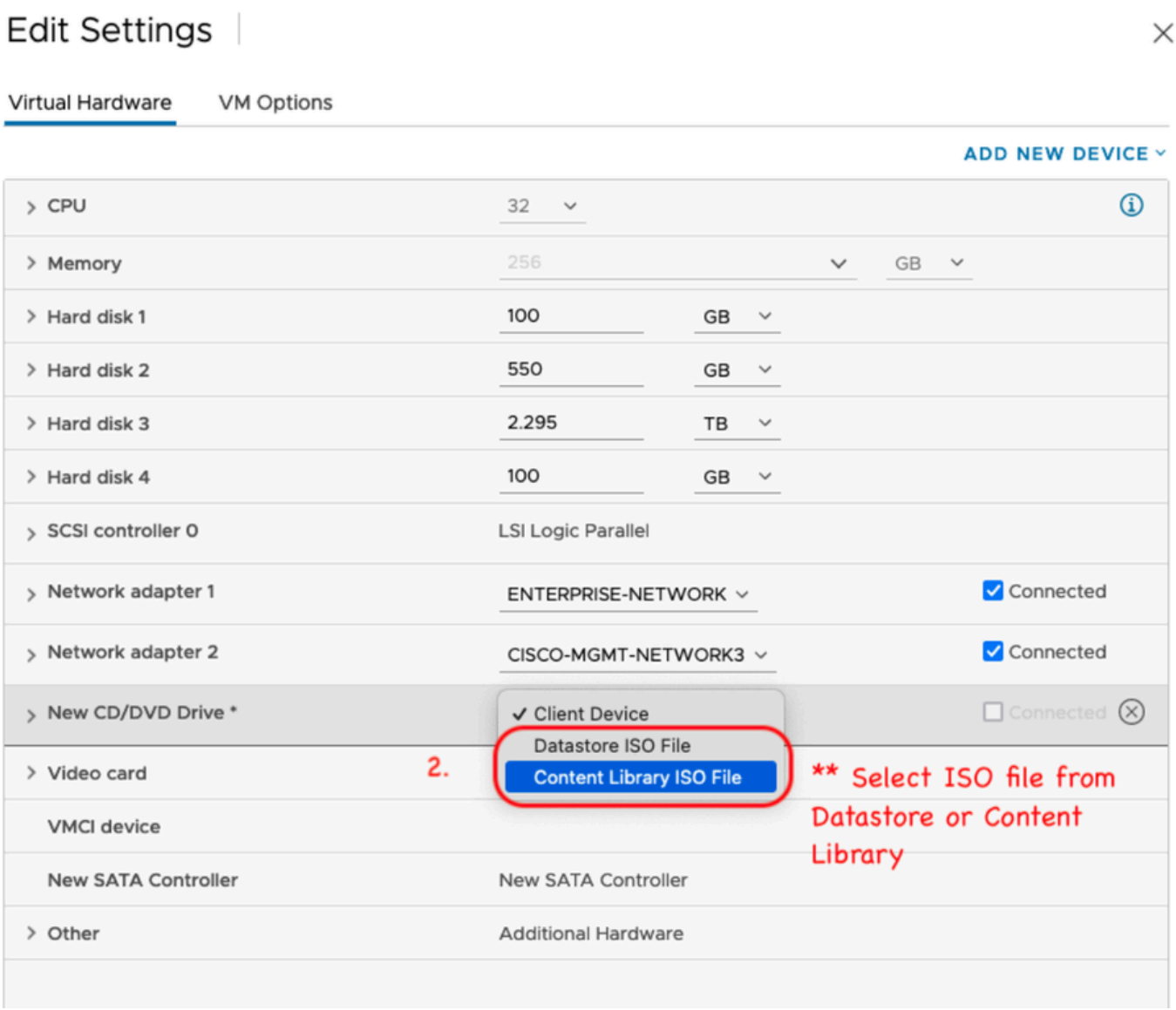


步骤 1b：从实时CD VA启动 — ESXi

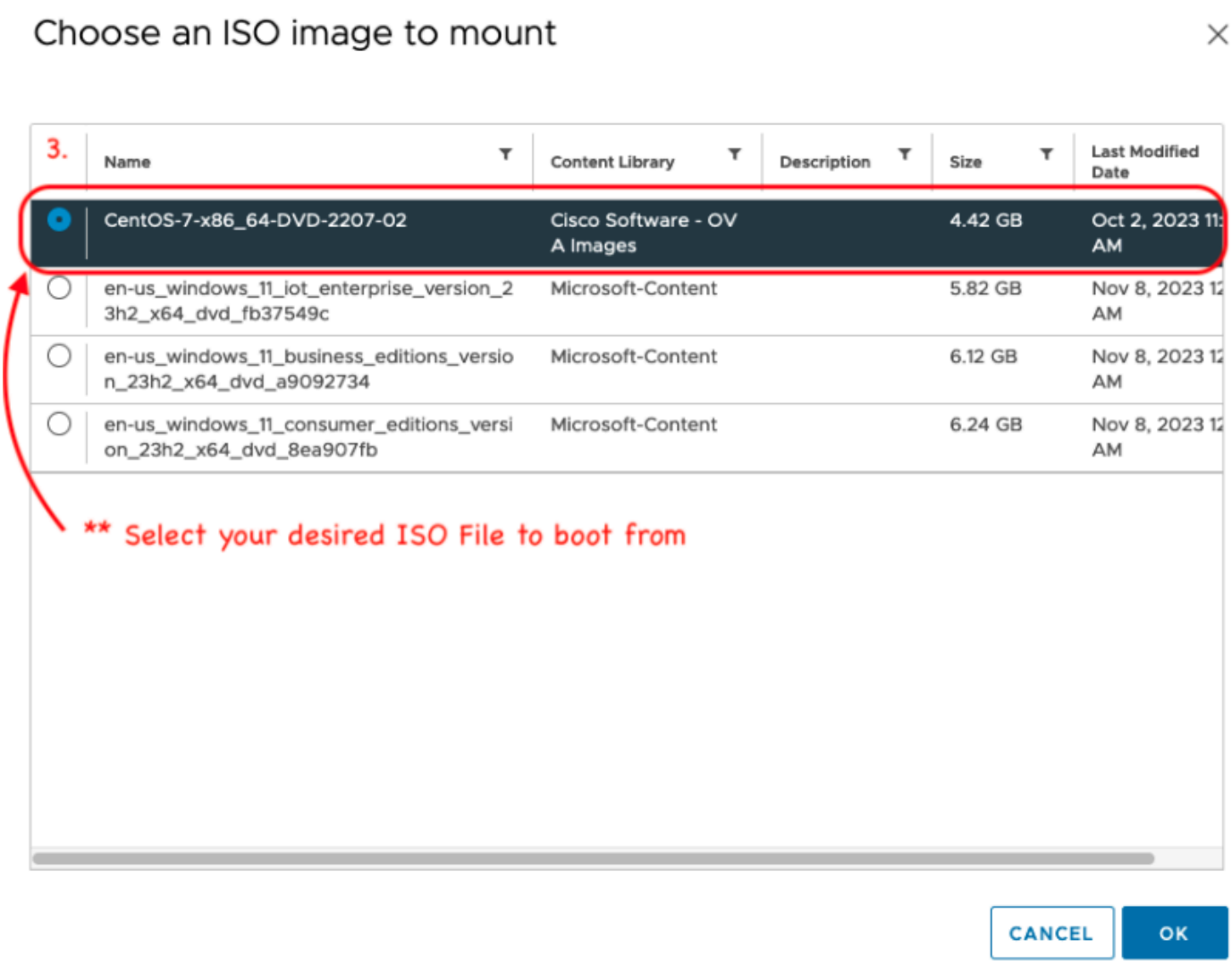
1.在VMware vCenter中，导航到虚拟机，右键单击VM，然后选择编辑设置。单击添加新设备，然后选择CD/DVD驱动器。



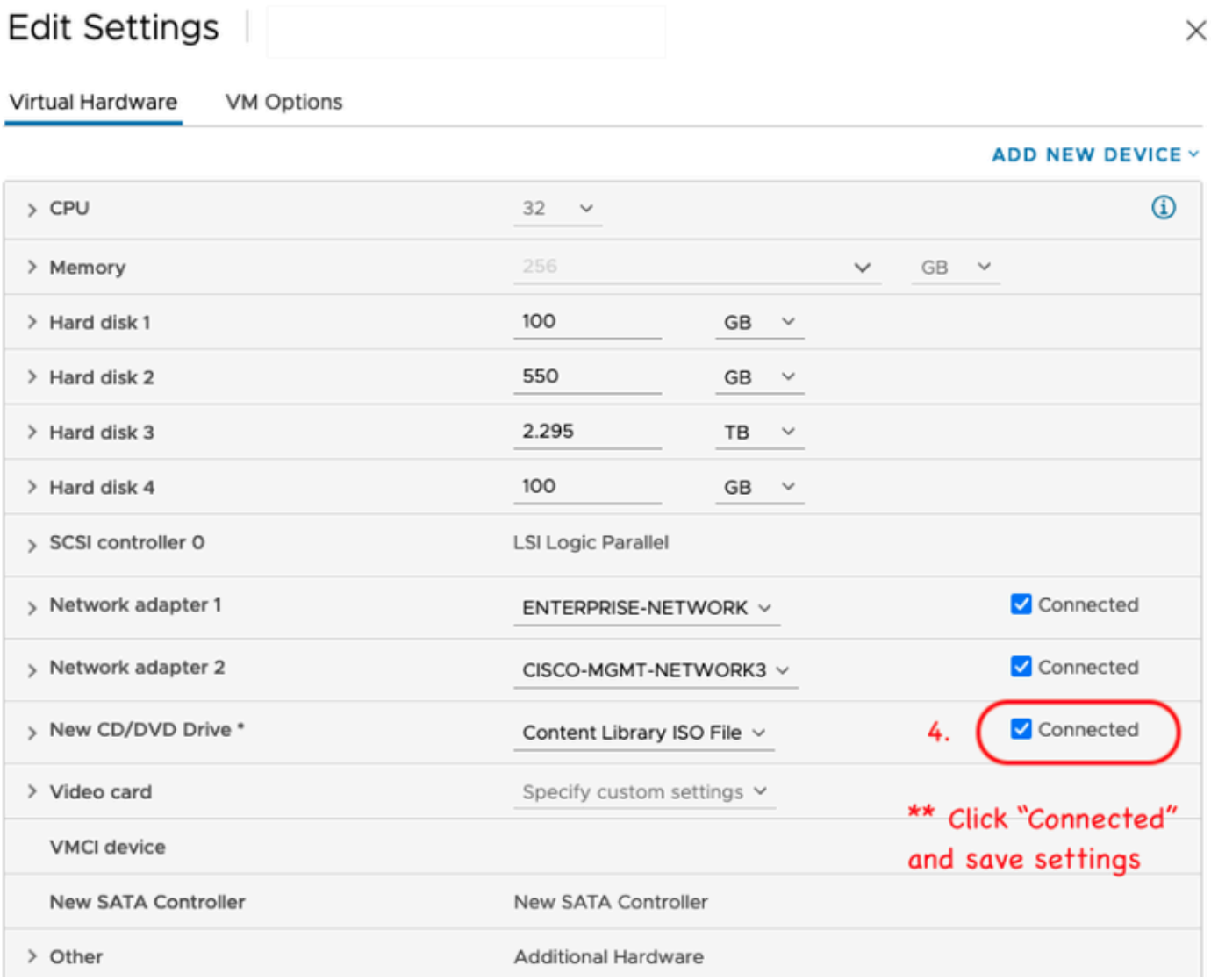
2. CD/DVD驱动器现在在设置页面中显示为新CD/DVD驱动器。如果ISO已上传到Datastore ISO文件，则为CD/DVD选择此选项。否则，请选择内容库ISO文件。



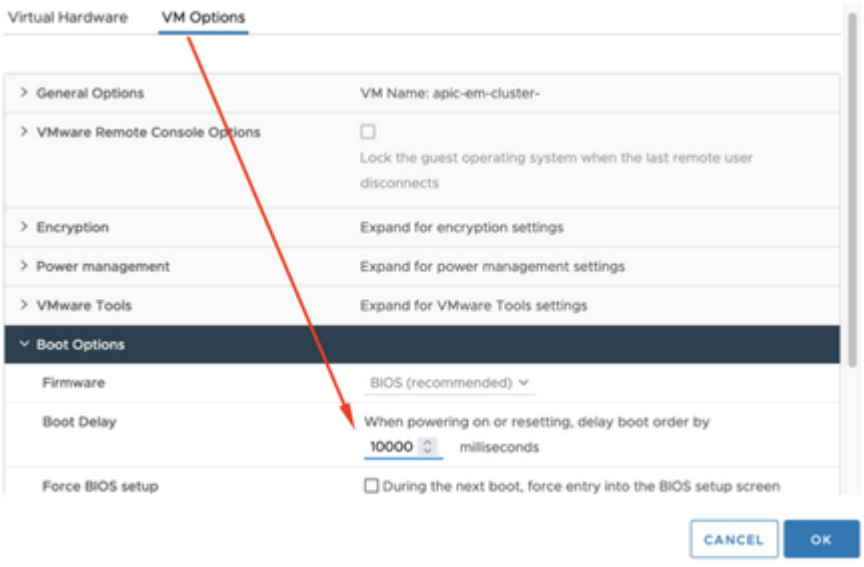
3.选择要从中启动的ISO文件。对于此过程，请使用Ubuntu 18.04 ISO。



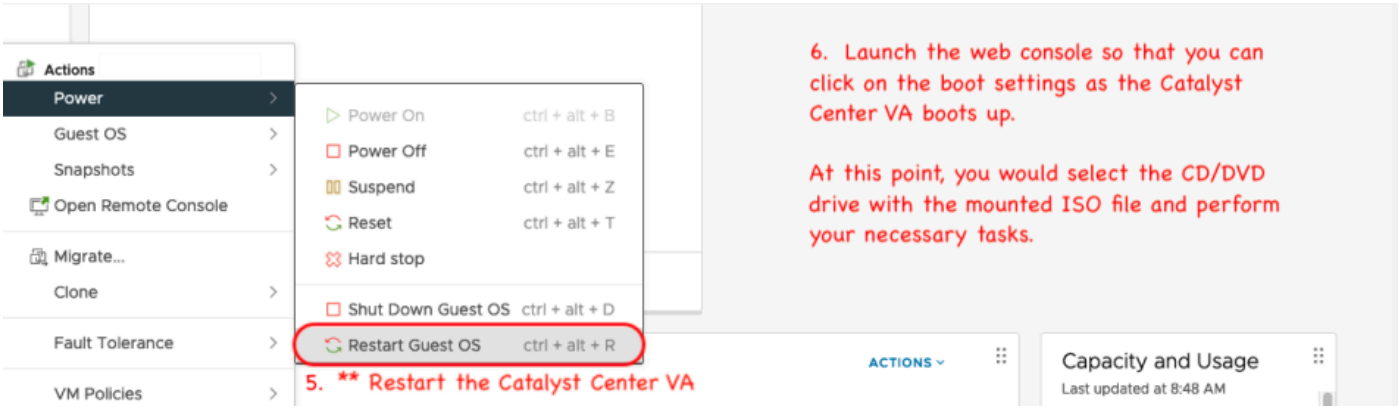
4.下一步，确保新CD/DVD驱动器右侧启用了Connected。

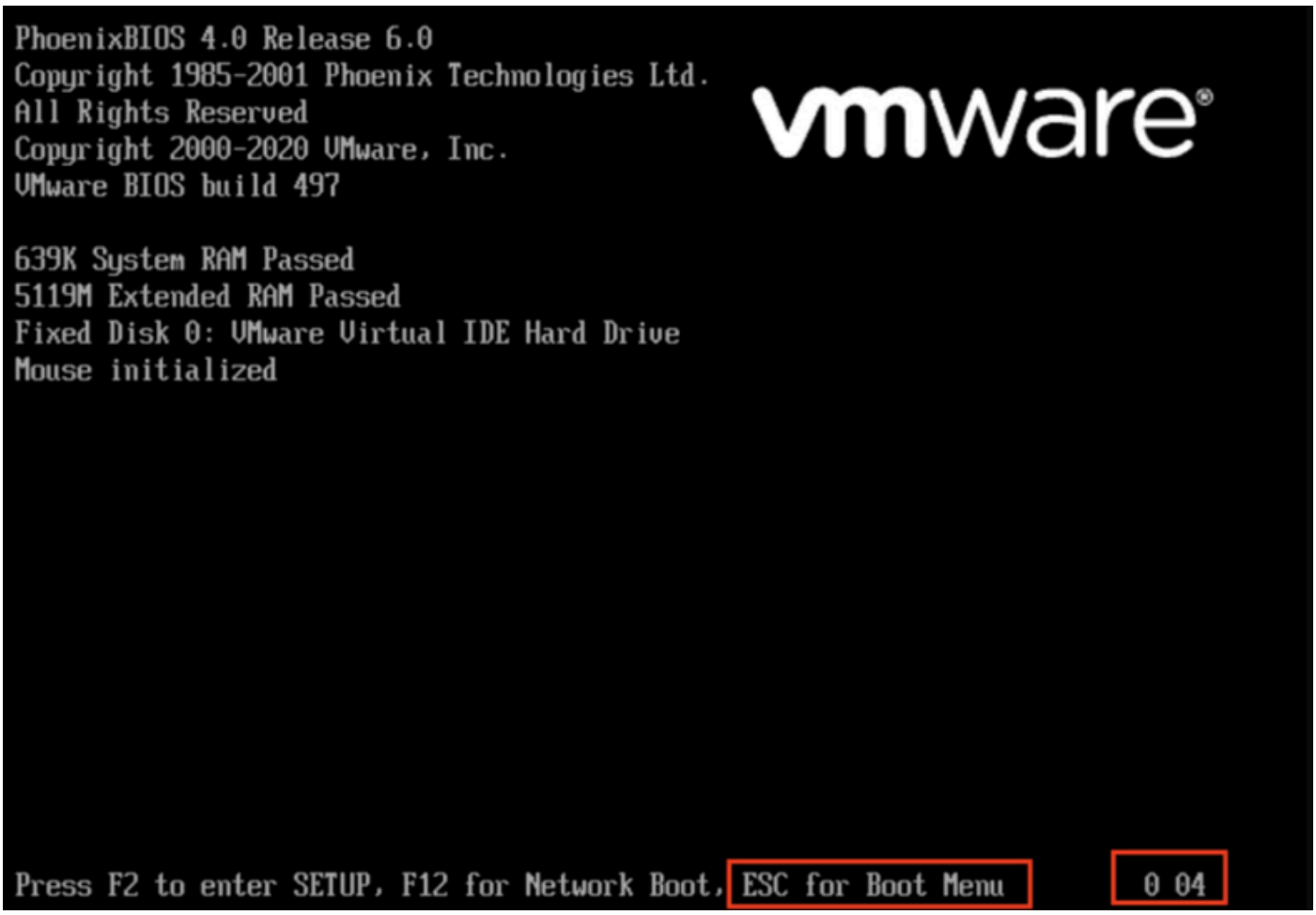


5.点击设置屏幕顶部的VM Options。单击Boot Options的下箭头，然后将Boot Delay更改为更大的值（例如10000）。 增加的延迟显示启动菜单选项的时间足够长，以在VM重新启动后选择ISO。



6.接下来，重新启动VM，以便您可以访问启动菜单并从ISO启动。





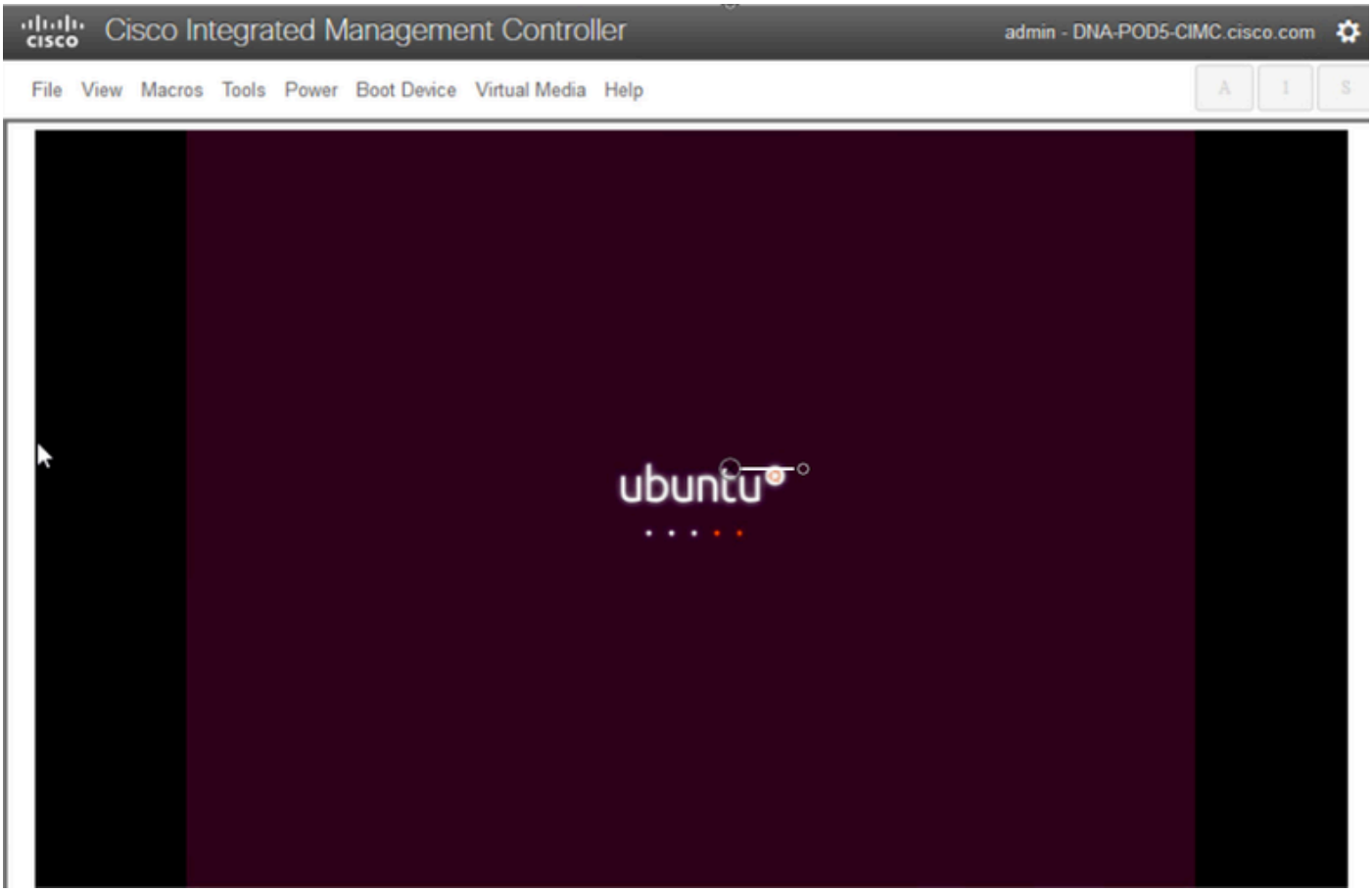
步骤 2a：加载到Ubuntu ISO

注意：屏幕截图显示了到达Ubuntu桌面需要多长时间。

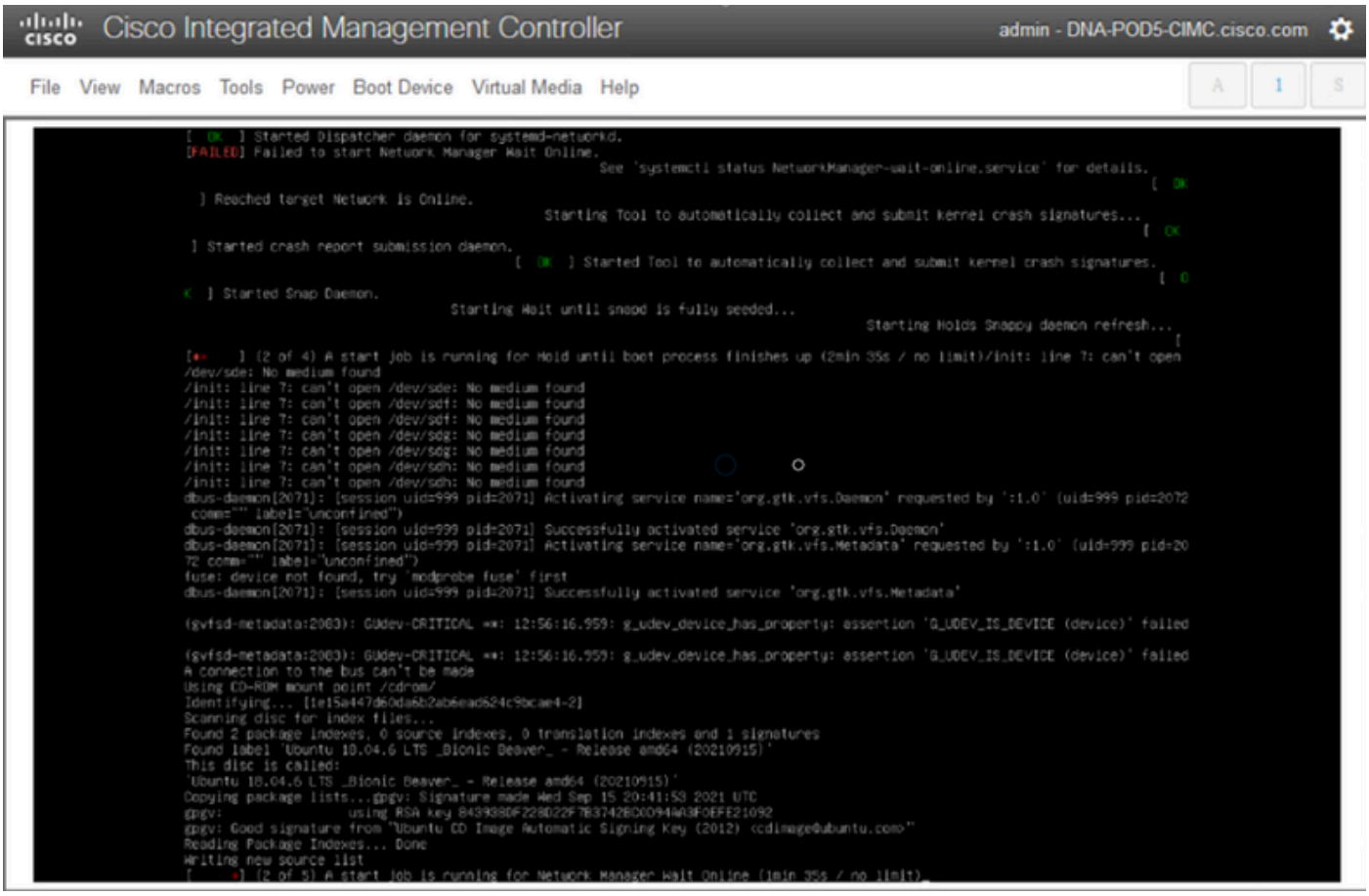
1.这是显示的第一个屏幕，它可能显示为空闲（等待下一个屏幕）。 在实验中，此屏幕会保留40秒。



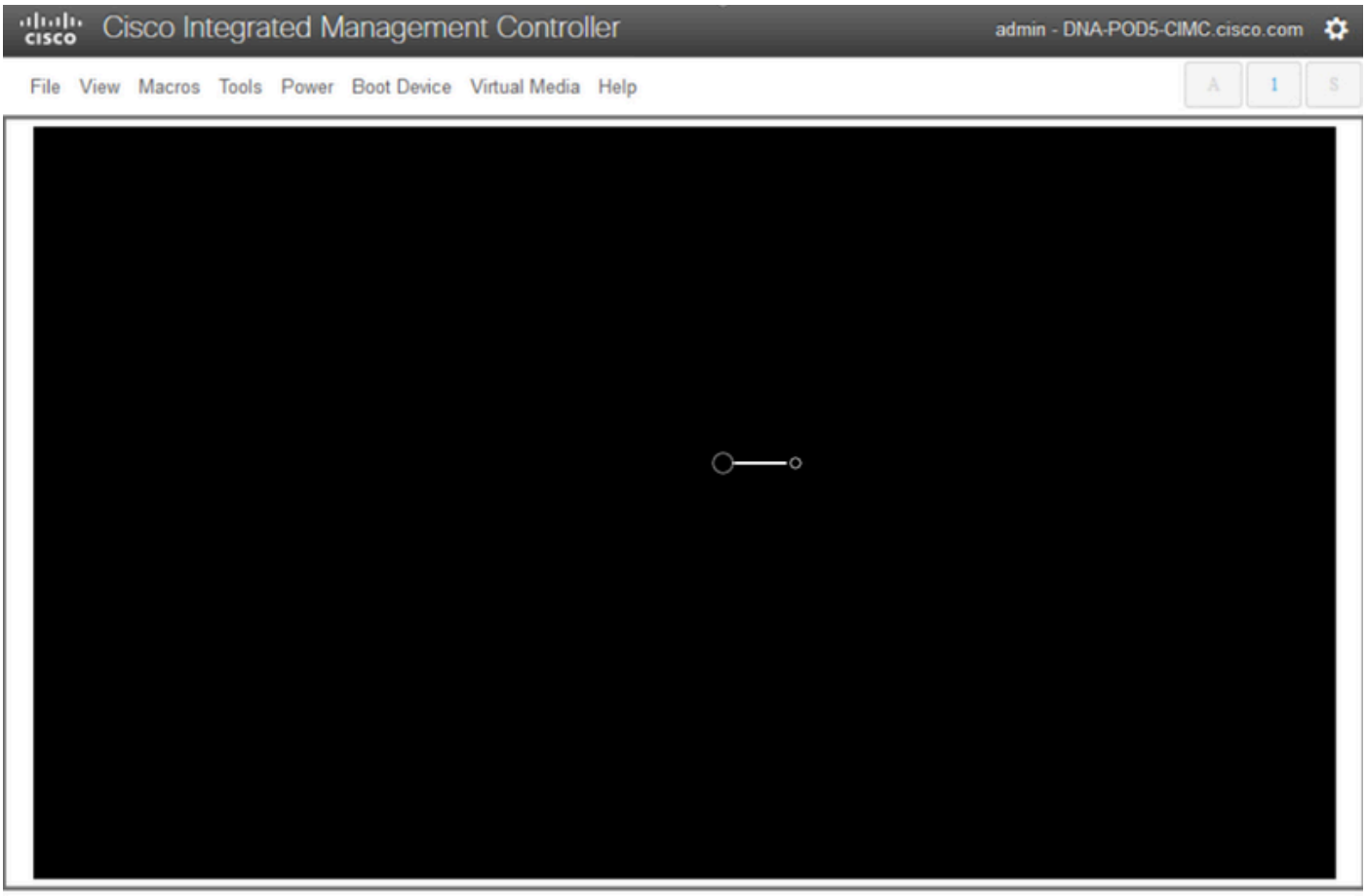
2.之后，屏幕完全变黑了大约30秒钟，然后出现Ubuntu加载屏幕。在实验中，此屏幕在继续操作之前会保留5分钟多一点，但部署时间会有所不同。



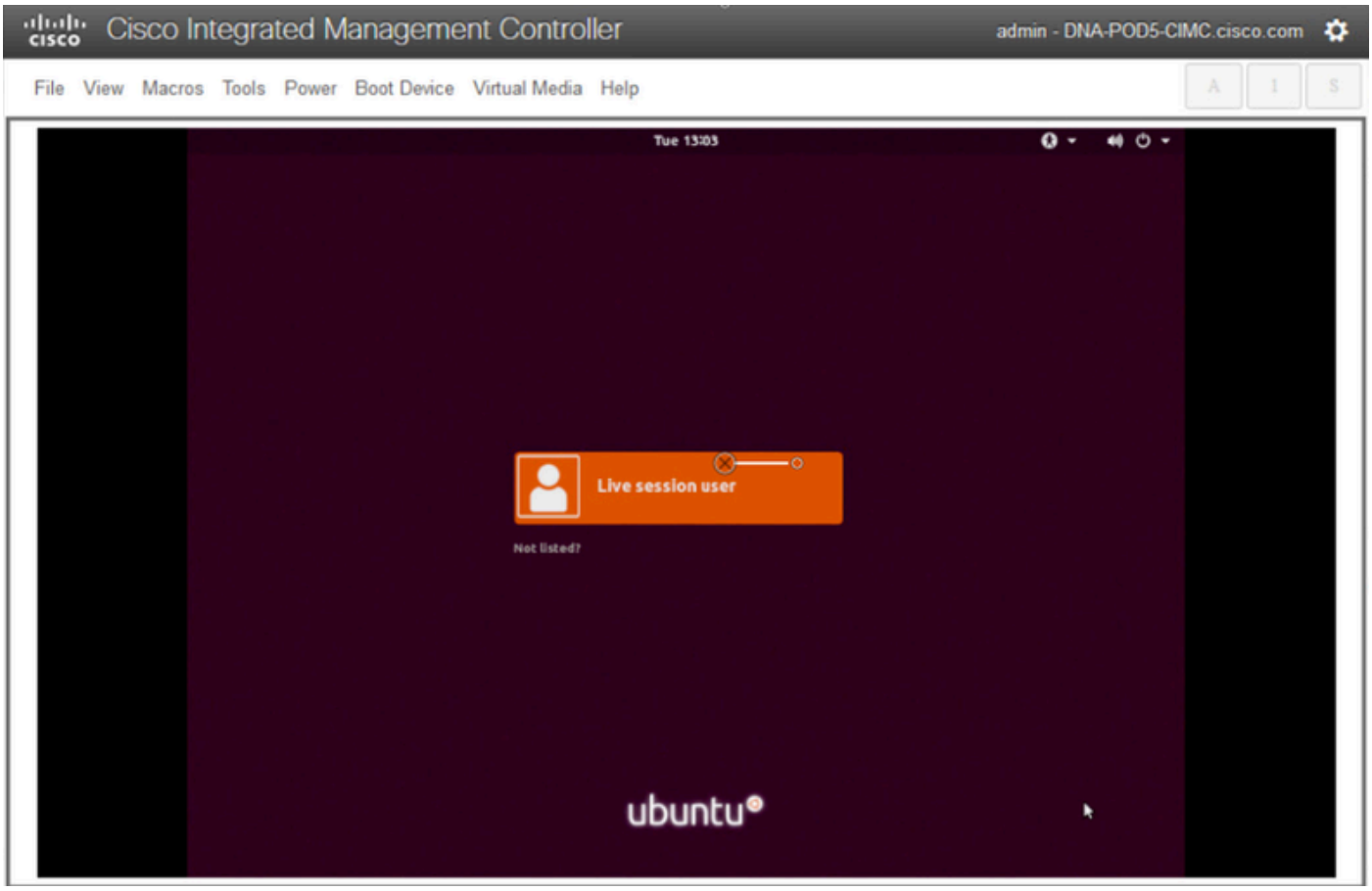
3.接下来，屏幕显示可能表明出现了问题，但这是预期结果。在实验中，此屏幕会保持2分钟后再继续。



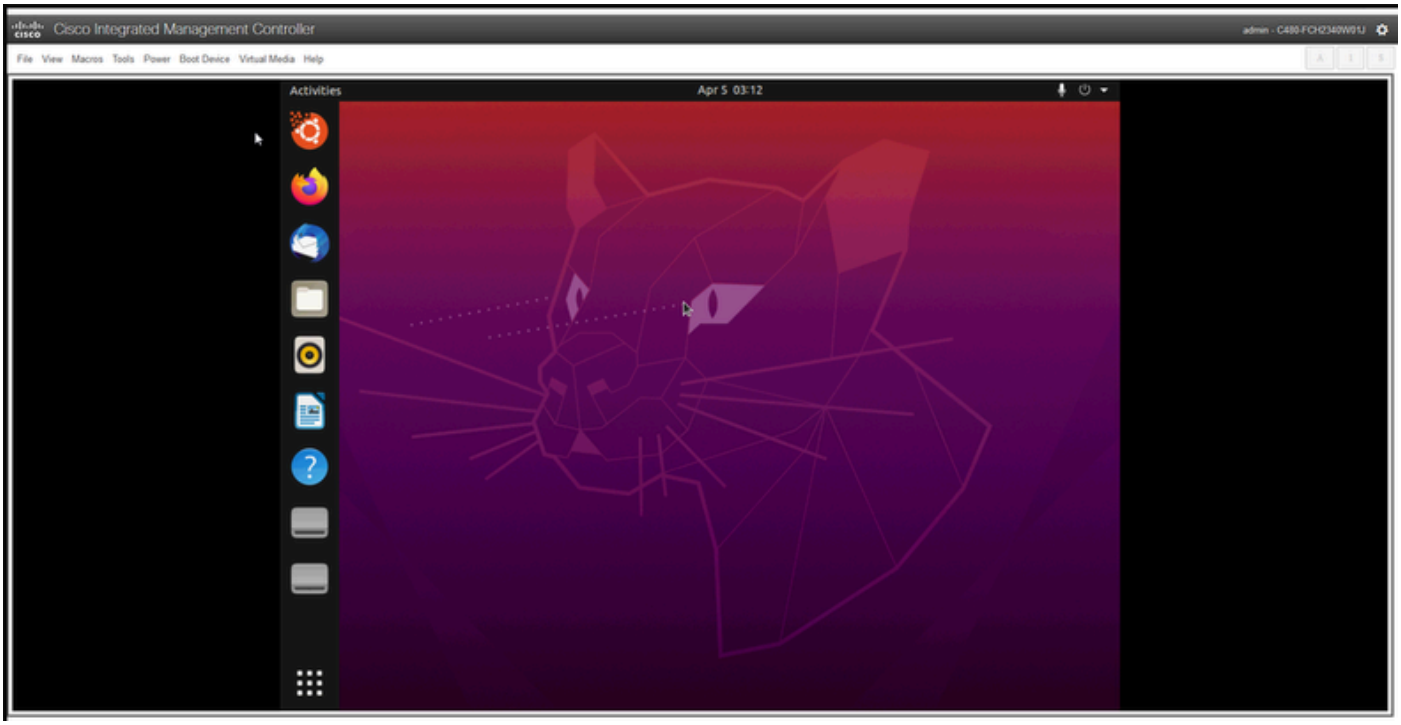
4.屏幕返回黑色屏幕约3分钟，上一屏幕再次闪烁几分钟，然后再次返回黑色屏幕约2分钟。



5.接下来，系统将显示选择Live会话用户的选项。如果出现try Ubuntu desktop选项，请选择该选项。选择此用户以继续。



6.选择用户后，屏幕再次变黑，然后显示Ubuntu桌面。



在某些环境中，最多可能需要两个小时才能达到此点。

步骤 2b：安装所需分区

一旦可以访问Ubuntu桌面GUI环境，请打开终端应用程序并执行这些步骤。

在此过程稍后进入chroot环境后，您可以确定需要执行哪些恢复操作：

- 如果/etc/shadow在maglev的密码散列之前显示感叹号(!)，则帐户将被锁定且必须解锁。
- 如果帐户未锁定但登录仍被拒绝，请重置磁悬浮的失败登录计数器。
- 如果必须设置新密码，请重置maglev密码，然后在重新启动后运行sudo maglev-config update。

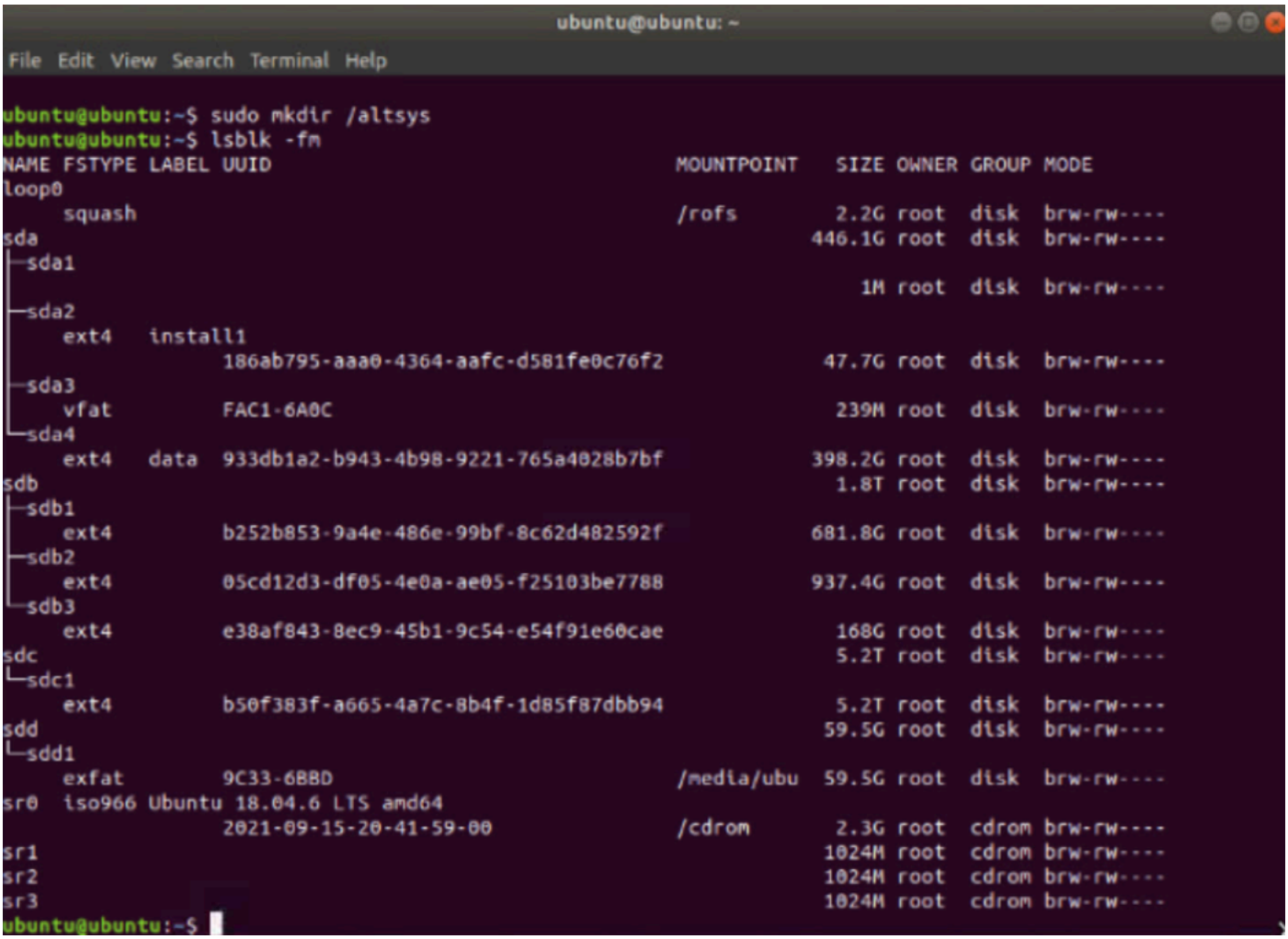
1. 创建临时装载点。
2. 将根分区和var分区装载到系统。
3. 将伪文件系统装载到临时装载点。

首先通过运行以下命令创建临时装载点：

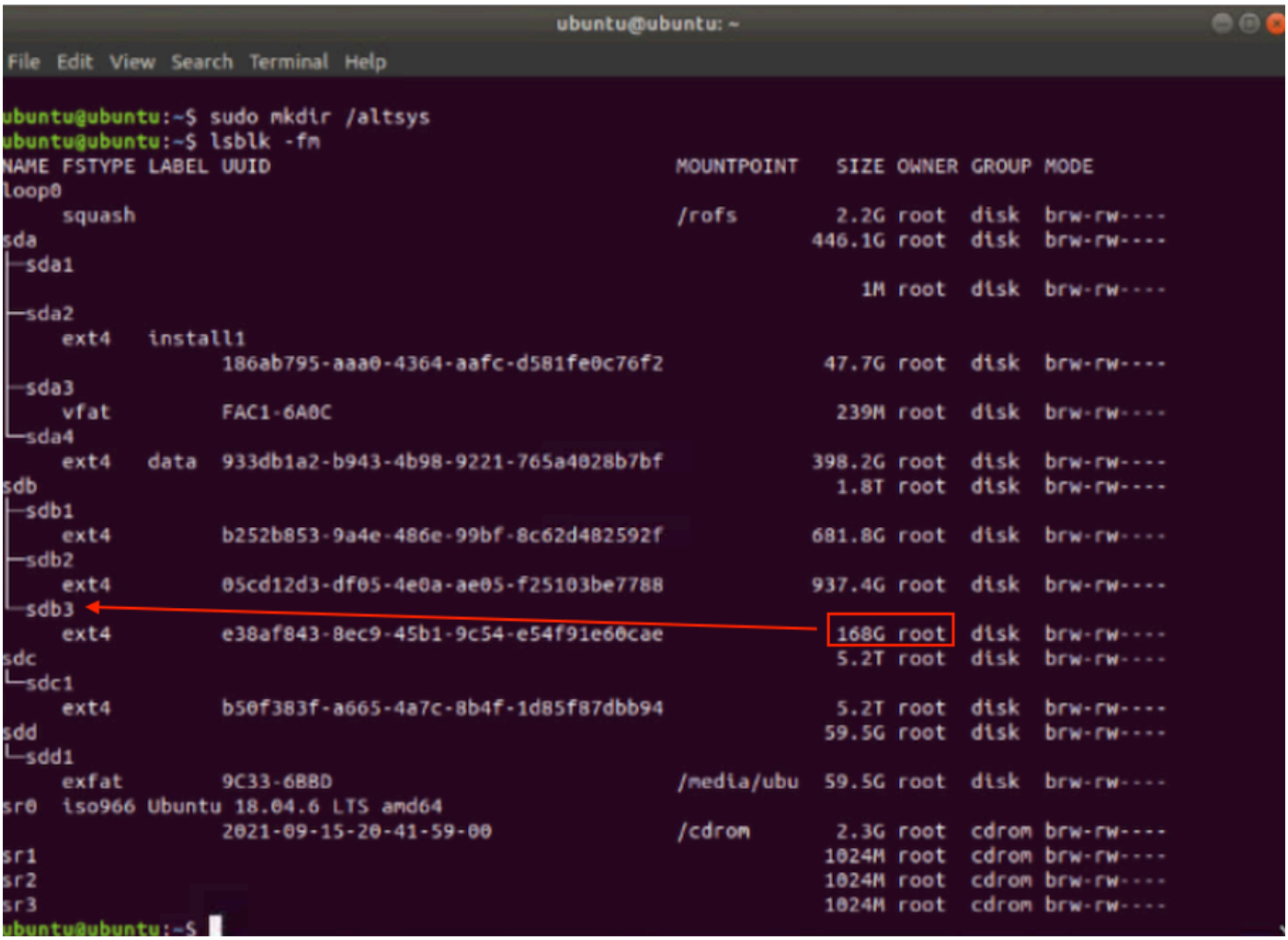
<#root>

```
sudo mkdir /altsys
```

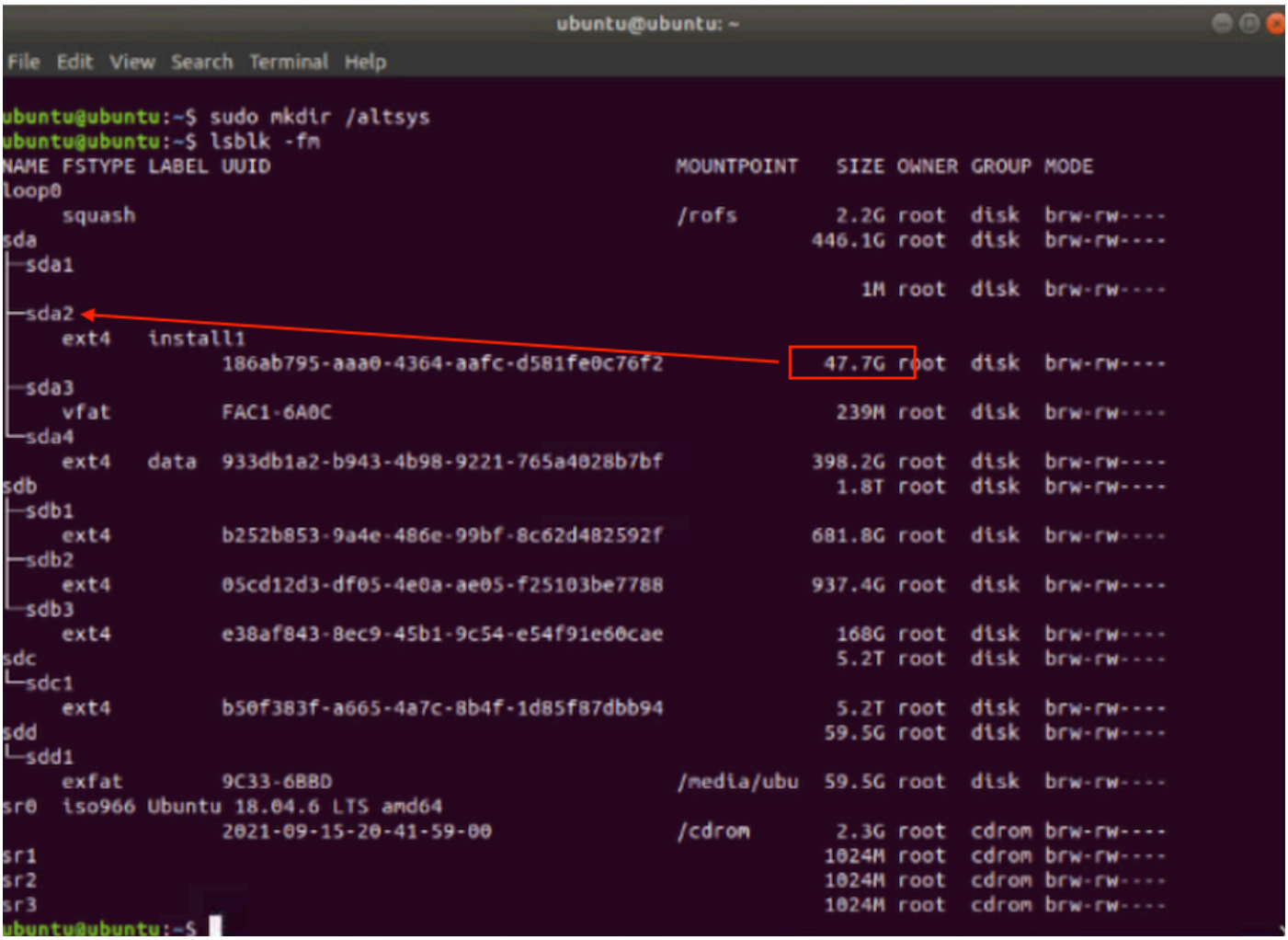
接下来，查找要装载的根分区和可变分区。运行lsblk -fm命令以标识（根）和/var的分区。记下下一步中为mount命令标识的分区。



对于/var，查找9.5G或168G分区；在本例中为sdb3。



对于/根分区，请查找28.66G或47.7G分区。在本例中，它是sda2。



确定var和根分区后，请将其装入：

<#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
```

挂载root和var后，装载伪文件系统：

<#root>

sudo mount --bind /proc /altsys/proc

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

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

更改密码或解锁磁悬浮账户之前的最后一步是更改为临时安装环境：

<#root>

```
sudo chroot /altsys
```

步骤 3：选择恢复操作（解锁帐户或重置密码）

运行sudo chroot /altsys后，请使用以下工作流程之一：

- 解锁帐户:使用步骤3a和步骤3b。
- 重置密码:使用步骤3c到步骤3e。

步骤 3a：检查磁悬浮帐户是否已锁定

<#root>

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

<#root>

```
maglev:

!

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

检查密码哈希前面是否有感叹号。如果存在，则该帐户被锁定。运行此命令可解锁用户：

<#root>

```
usermod -U maglev
```

步骤 3b：重置失败计数

如果用户在/etc/shadow文件中的密码哈希前面没有感叹号(!)，则已超过登录失败限制。使用以下步骤重置失败的登录尝试。

1.查找磁悬浮用户的失败登录尝试：

<#root>

$

sudo pam_tally2 -u maglev

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

2.在本示例中，失败的登录尝试超出了默认限制6。这可以阻止用户登录，直到失败计数重置或降到6以下。可以通过运行以下命令重置登录失败计数：

<#root>

sudo pam_tally2 -r -u maglev

3.计数器可以确认为重置：

<#root>

sudo pam_tally2 -u maglev

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

步骤3c:重置Maglev用户密码

<#root>

#

passwd maglev

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

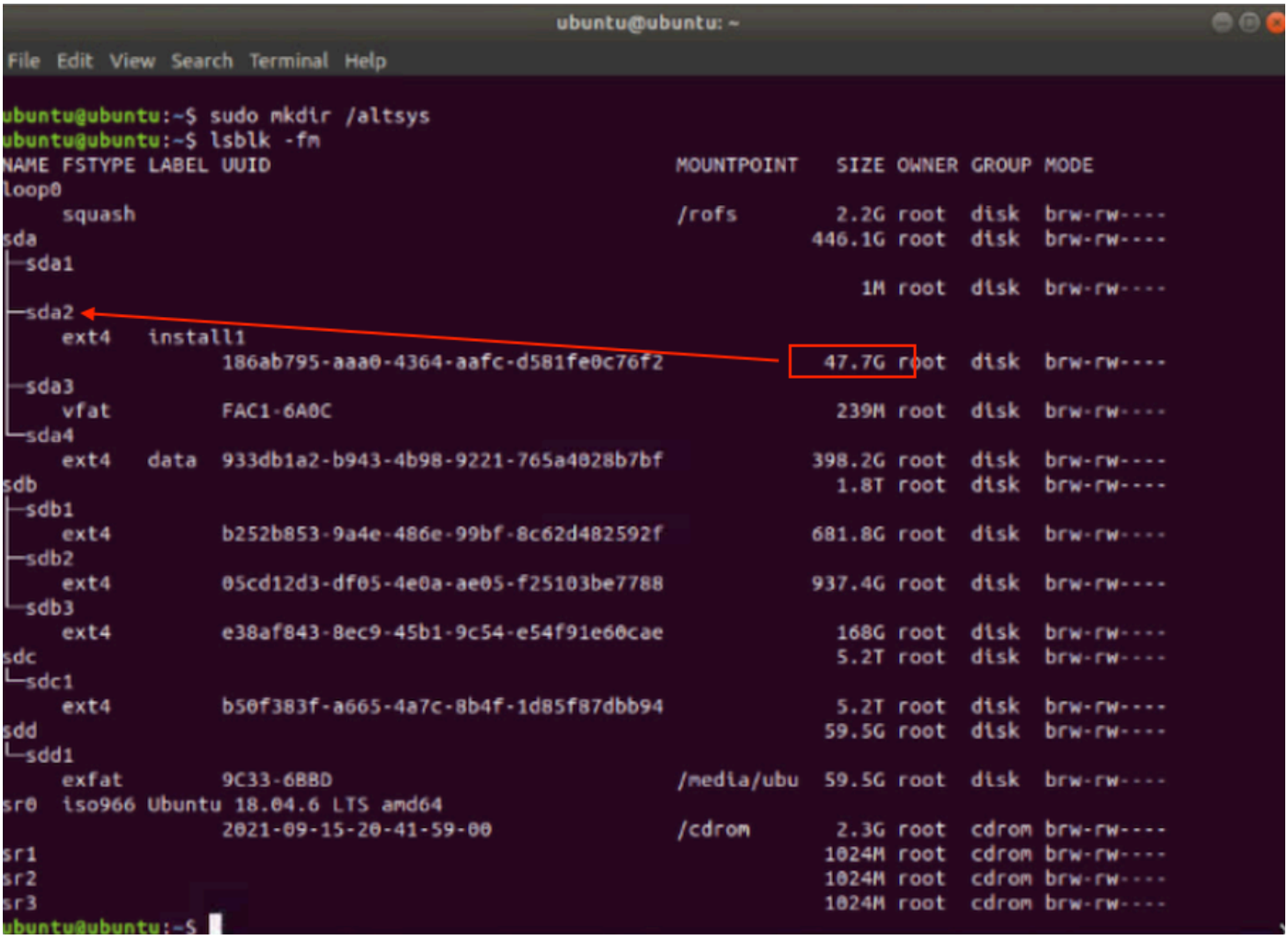
Retype new UNIX password:  #Re-enter the same password previously applied

Password has been already used.

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

步骤3d:正常重启到Cisco Catalyst Center环境

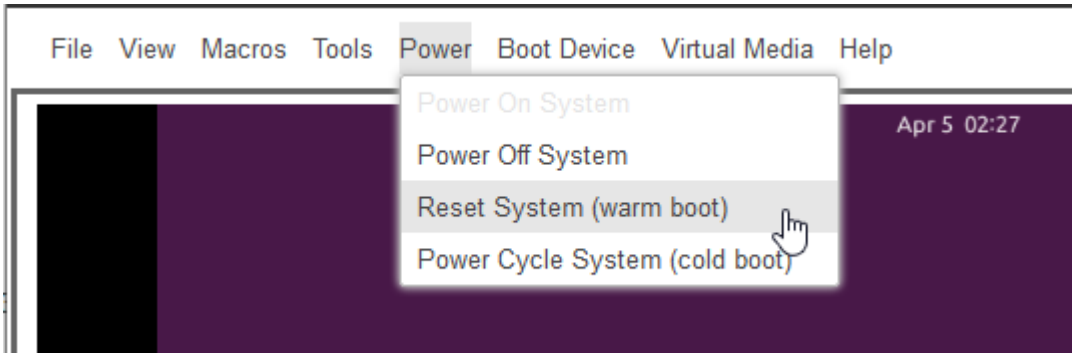
1.在KVM窗口中单击Power，然后单击Reset System（热启动）。 系统重新启动并从RAID控制器启动Cisco Catalyst Center软件。



步骤3e:从Cisco Catalyst Center CLI更新Maglev用户密码

1.一旦Cisco Catalyst Center软件启动且可以访问CLI，请运行sudo maglev-config update命令更改磁悬浮密码。此步骤可确保更改在整个系统中生效。

2.启动配置向导后，通过向导导航至允许在第6步中设置磁悬浮密码的屏幕。



3.在Linux密码和重新输入Linux密码字段中输入密码后，选择下一步并完成向导。向导完成配置推送后，密码已成功更改。创建新的SSH会话或在CLI中运行sudo -i命令以确保密码已更改。

原因

当磁悬浮账户被锁定时，用户无法登录以解除锁定。要解锁和/或重置Maglev用户的密码，需要将映像安装到Cisco IMC vKVM。这提供对外壳的访问权限并允许重置用户帐户和/或密码。

相关内容

分步视频指南

- 磁悬浮用户密码重置工作流程

思科提供的映像。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。