Reset Cisco DNA Center's Maglev User Password

Contents

Introduction

This document describes how to unlock and/or reset the password for the Maglev user.

Background Information

In the case where the Maglev account is locked out, you cannot log in to unlock it. To unlock and/or reset the password for the Maglev user, you must mount an image to the Cisco IMC vKVM. This allows you to access the shell and reset the user and/or password.

Prerequisites

Requirements

- You need to download an ISO image for Ubuntu 16.04 or newer from https://ubuntu.com/download/desktop. We recommend 18.04 as it's the same version as the Cisco Catalyst Center.

- After the ISO has been downloaded to the local system you then need to mount the ISO to the Cisco Integrated Management Controller (CIMC) KVM.
- Once the ISO is mounted to the KVM you then need to boot from the ISO.
- Once you can access Ubuntu, mount the root and var directories to the system.
- After you have mounted the root and var directories, you can unlock and change the Maglev user account.
- Finally, you reboot the appliance, confirm you can login in with Maglev, and reset the password with the configuration wizard.

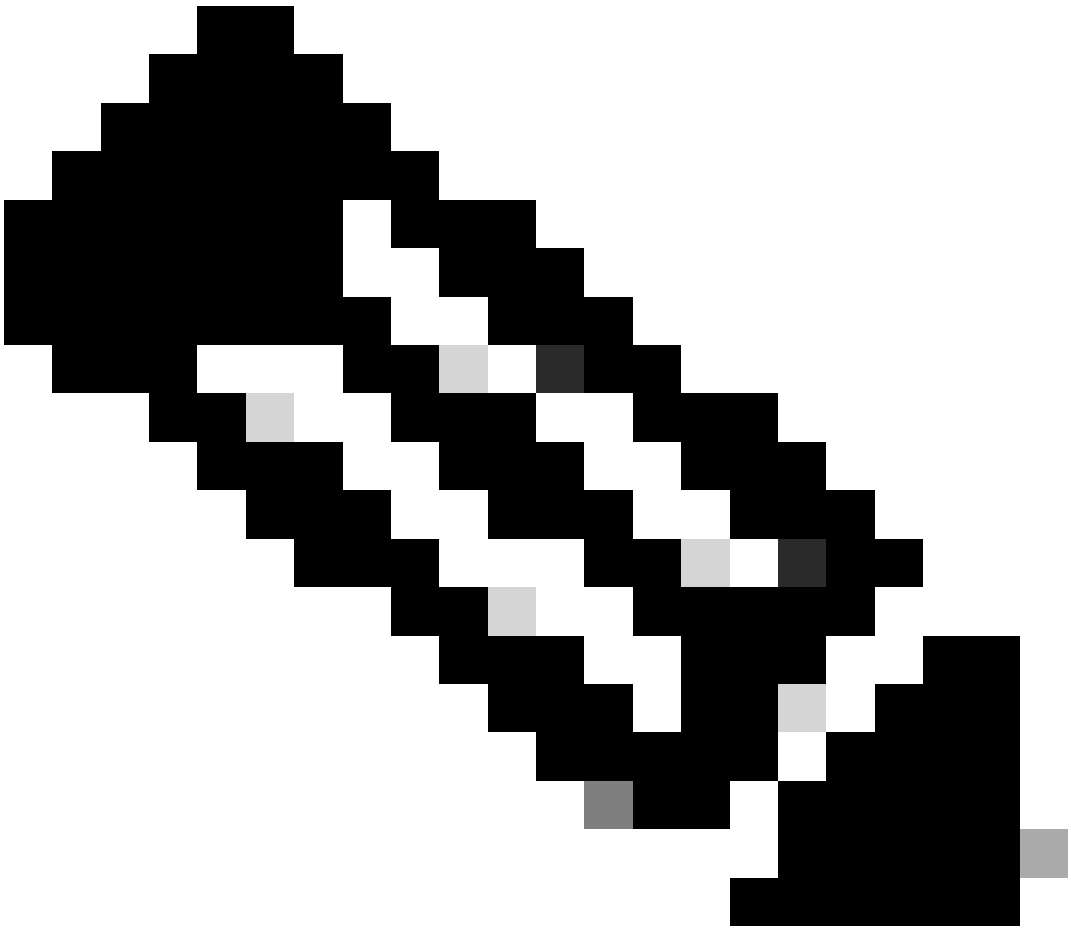
Components Used

This operation was run on Ubuntu 18.04 image; a different image produces different times and results.

It has been seen in some environments to take up to 2 hours to reach the Ubuntu desktop.

This operation is not restricted strictly to the Ubuntu desktop version. All that is required is access to the shell. Any Ubuntu image that provides shell access works for this operation.

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, ensure that you understand the potential impact of any command.



Note: you can use the same procedure in a DR environment. However, note these points:

***** Ensure that disaster recovery is in a PAUSED state before attempting any password recovery/reset methods *****

In a 1+1+1 DR deployment, the corresponding site is down while this process is completed.

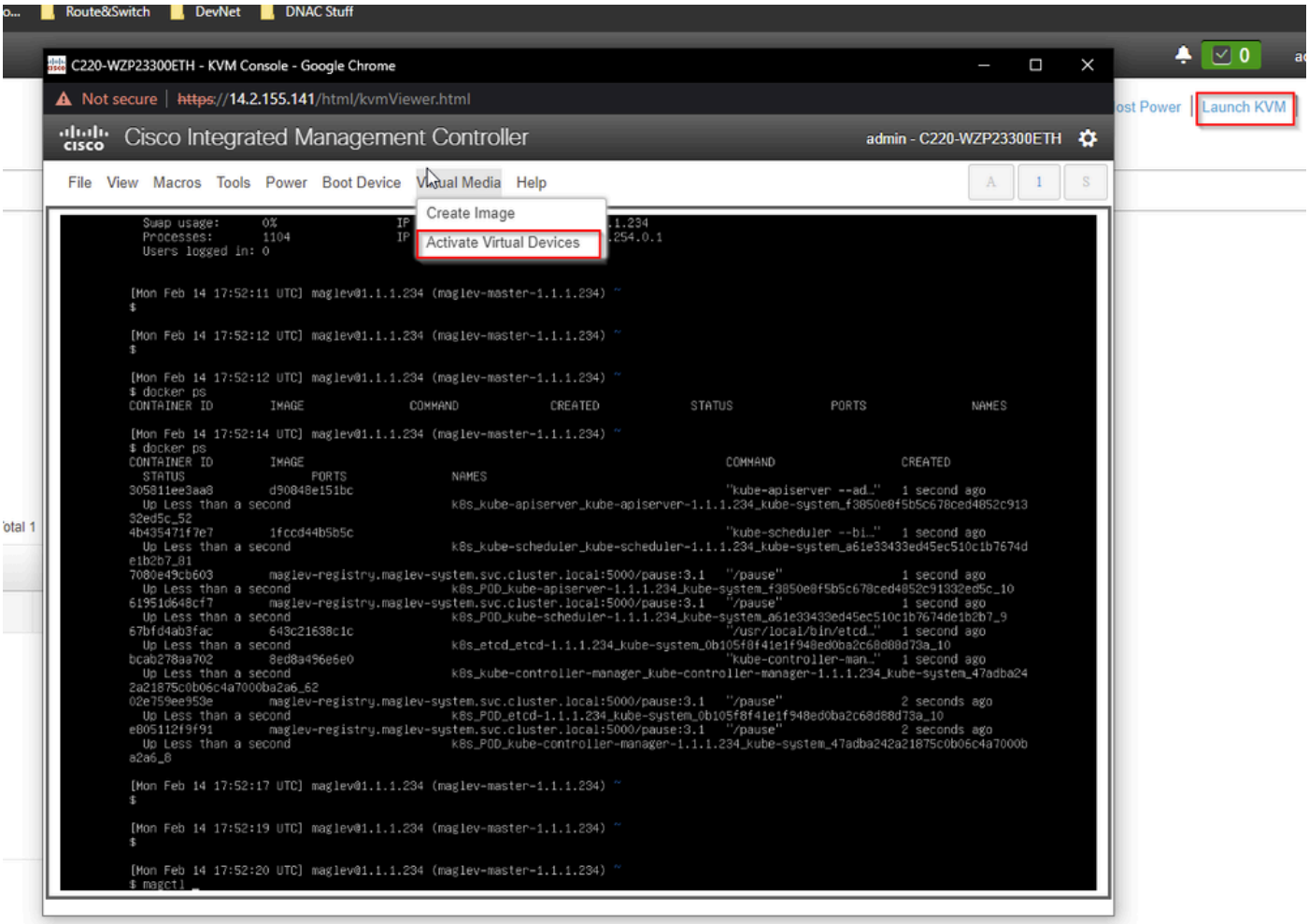
In a 3+3+3, If your passwords are to be updated on all three nodes, do it one node at a time to ensure that

---

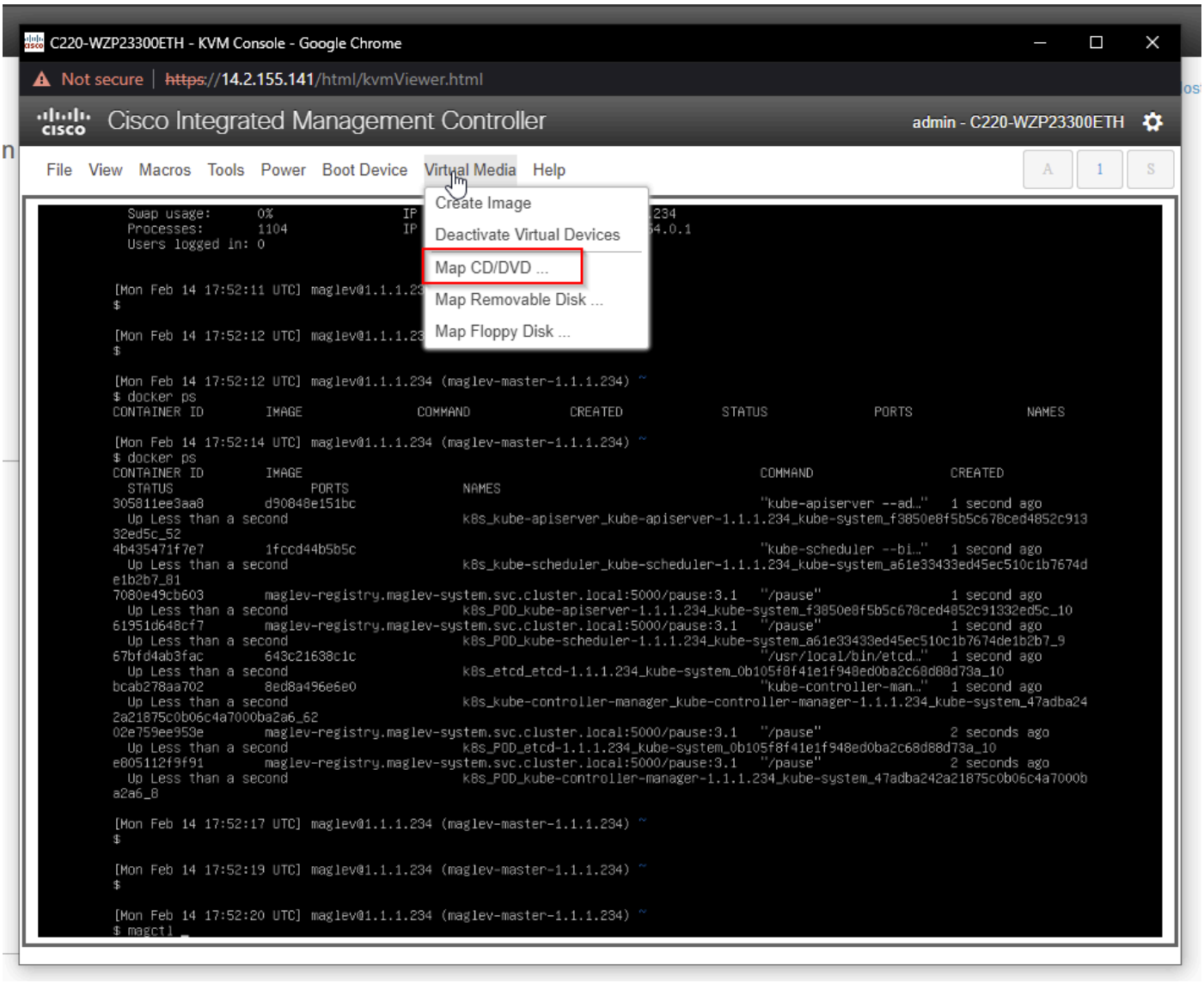
the two other nodes are available to avoid an unnecessary DR failover.

Step 1: Boot from Live CD

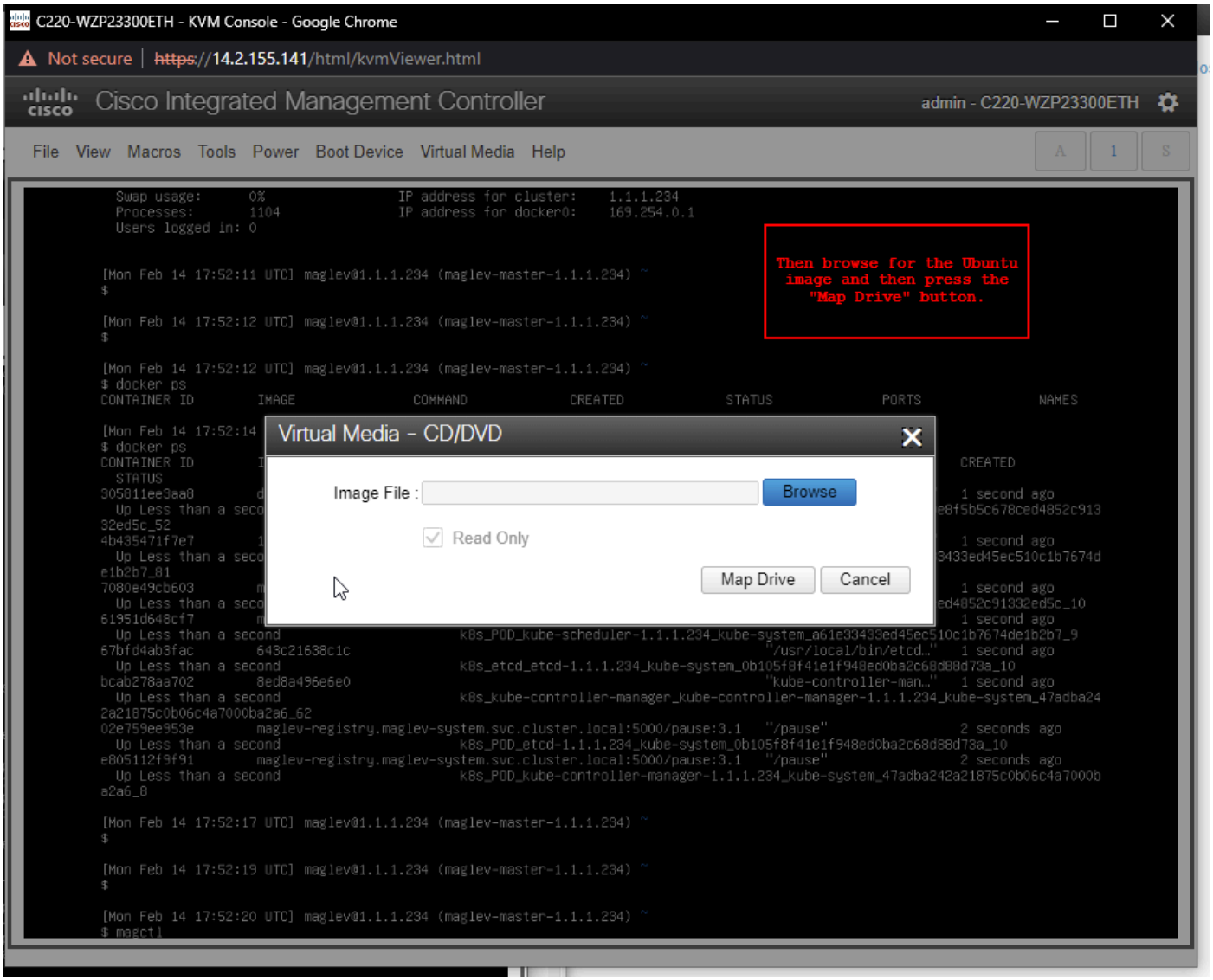
Log in to the Cisco IMC GUI, choose **Launch KVM** and then choose **Virtual Media > Activate Devices**.

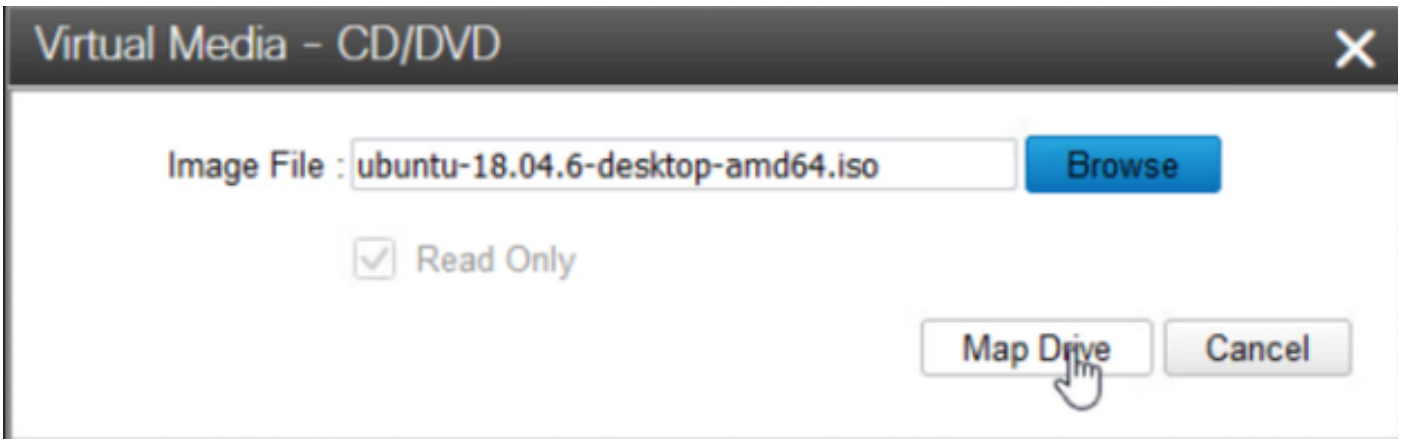


Next, choose **Map CD/DVD**.

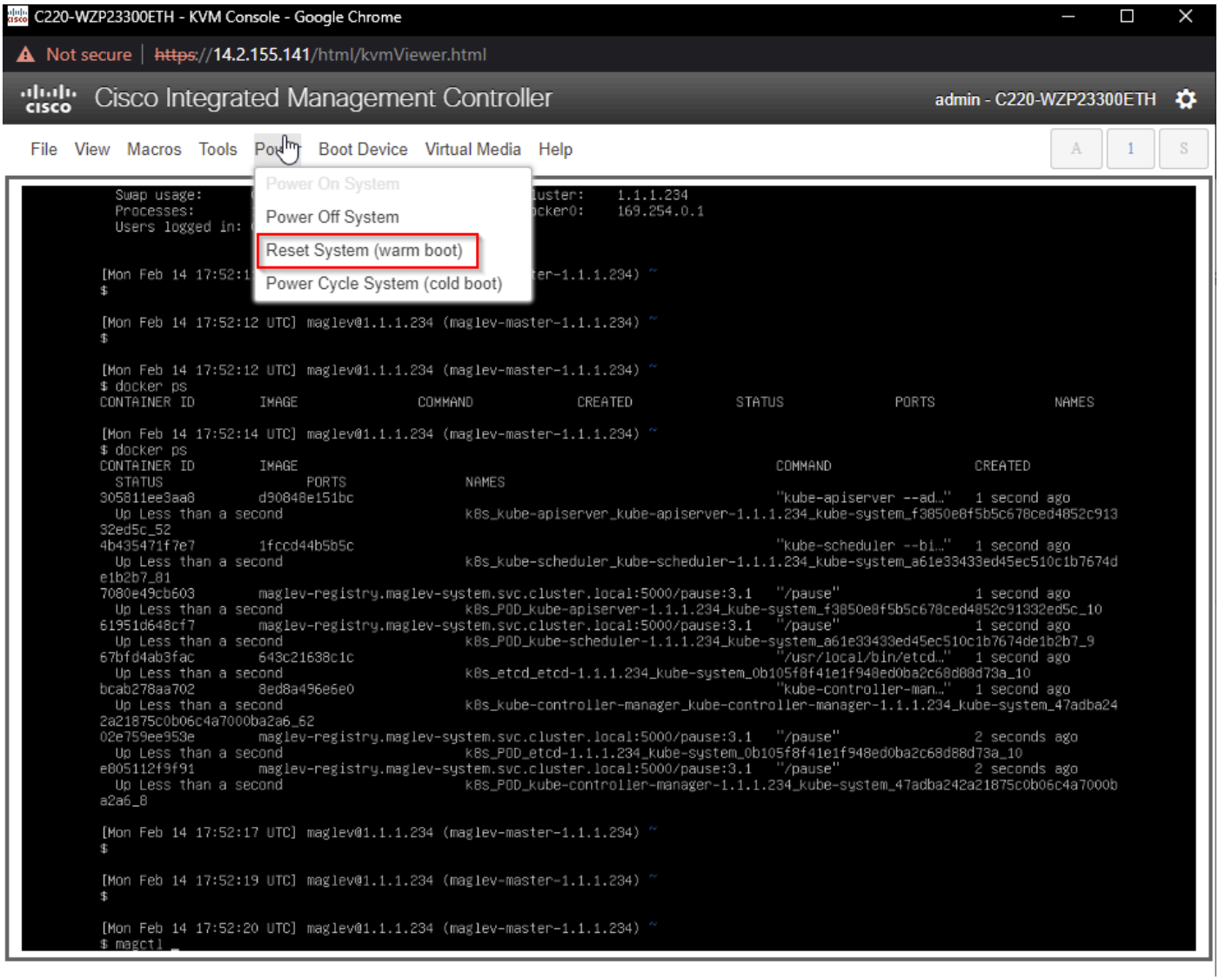


After that choose **Browse** and then select the Ubuntu ISO image you downloaded to your local system. After you have selected the Ubuntu image, choose the **Map Drive** button.

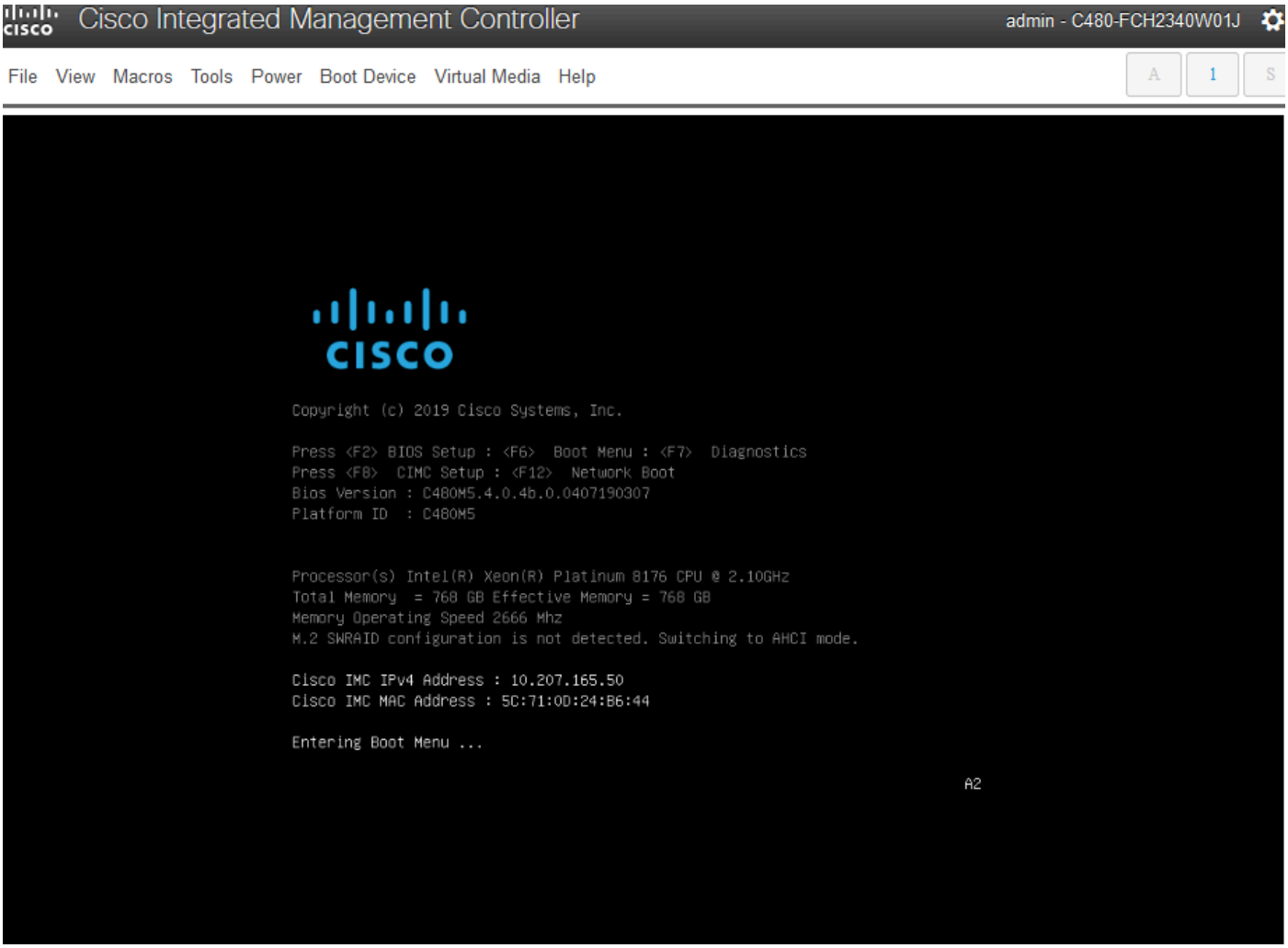




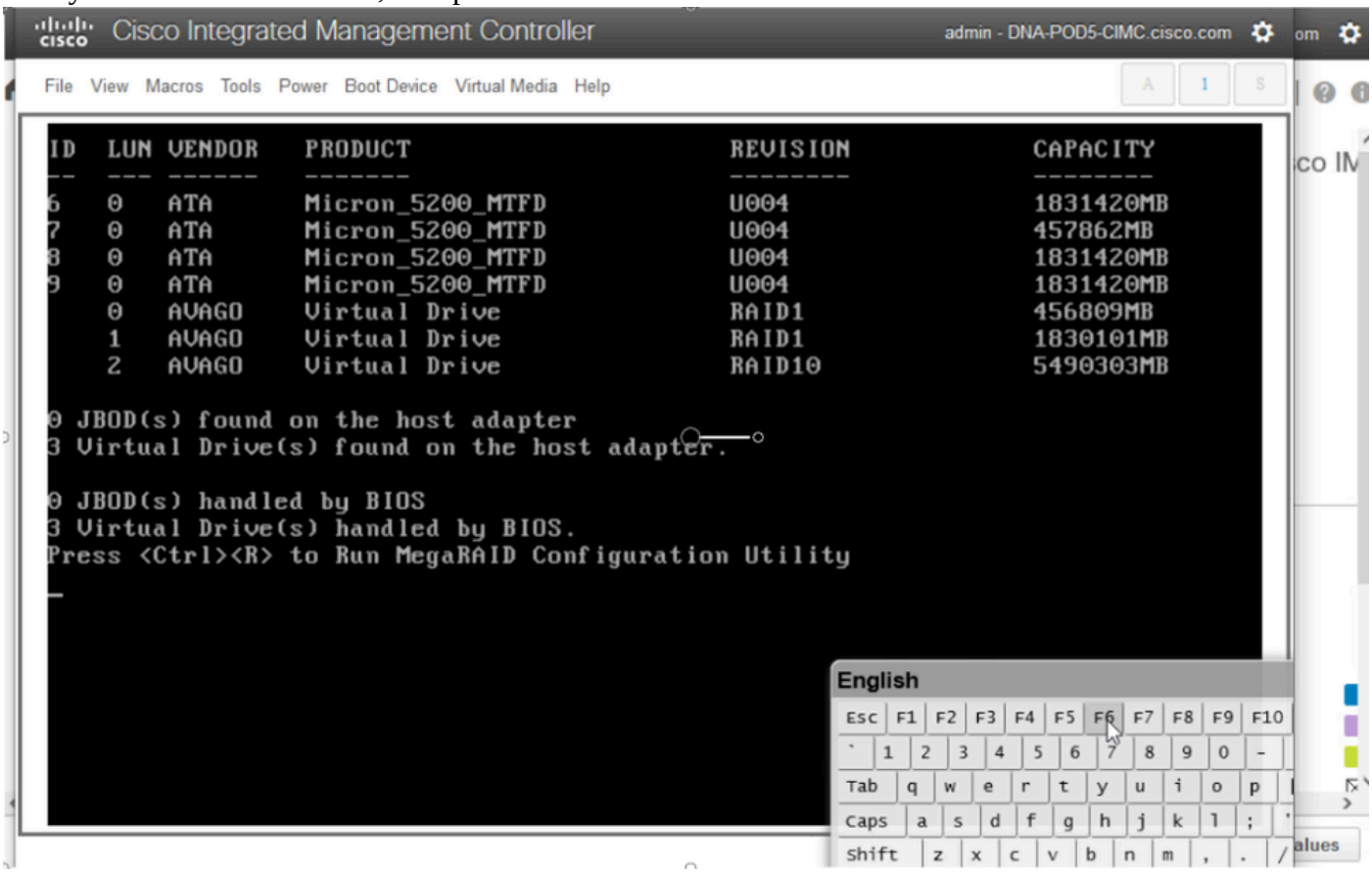
Next power cycle the appliance with **Power > Reset System (warm boot).**



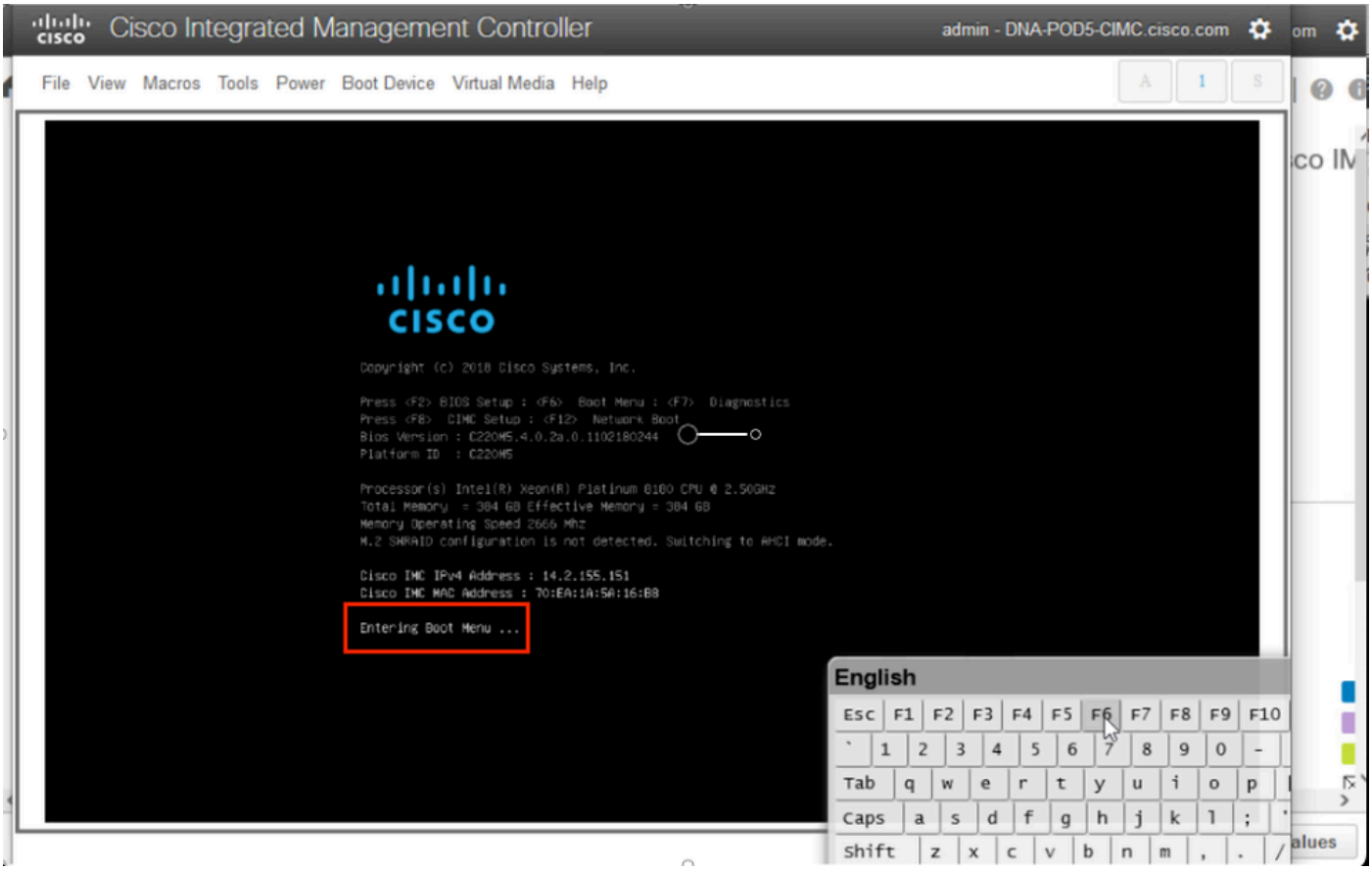
After the system has rebooted, press **F6** when the Cisco logo appears.



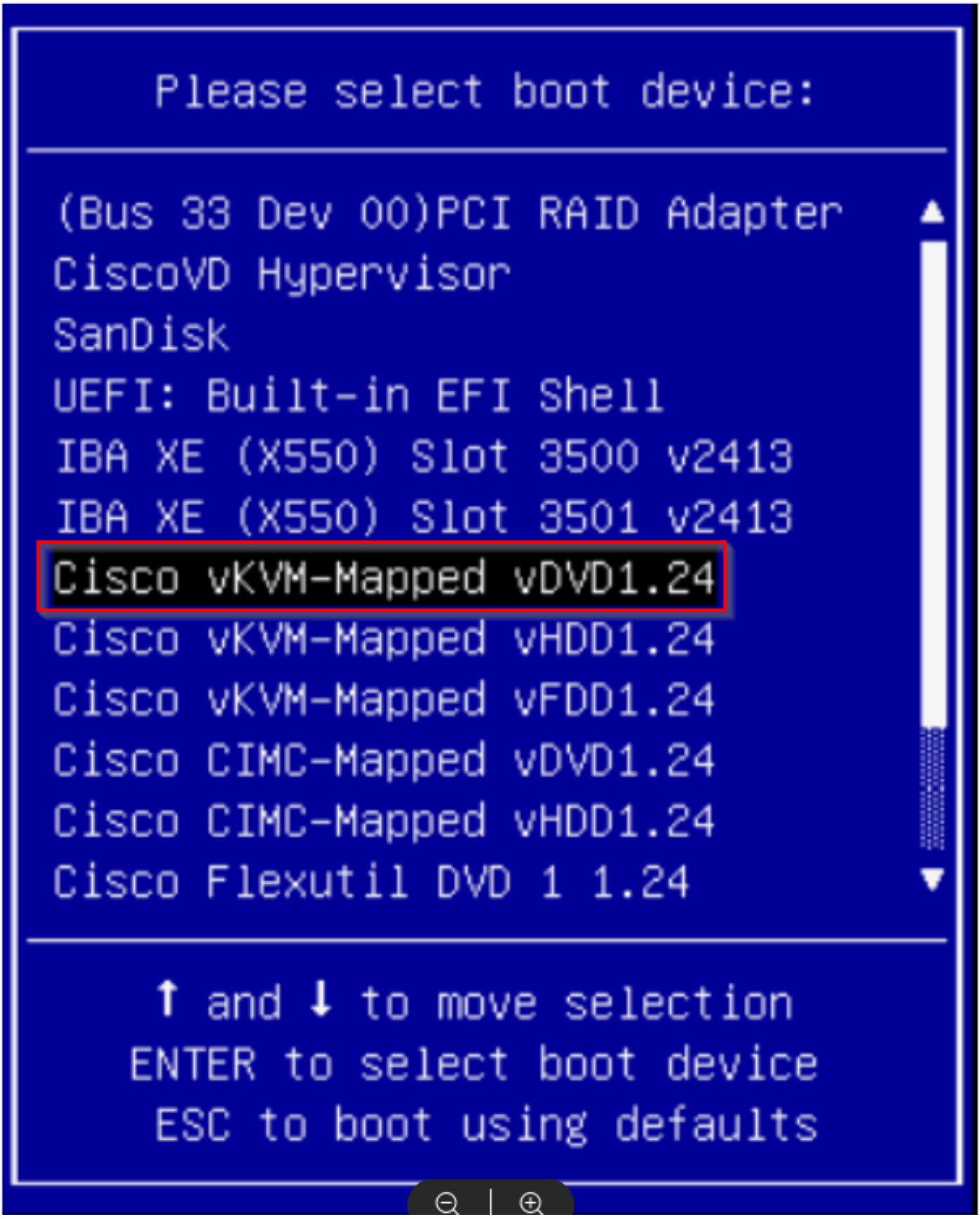
It may look like it didn't work, as it proceeds to a screen that looks similar to this one:



But a second screen will appear and we can see that it's entering the boot menu. If we forgot to press **F6** on the first Cisco screen, we can press it here



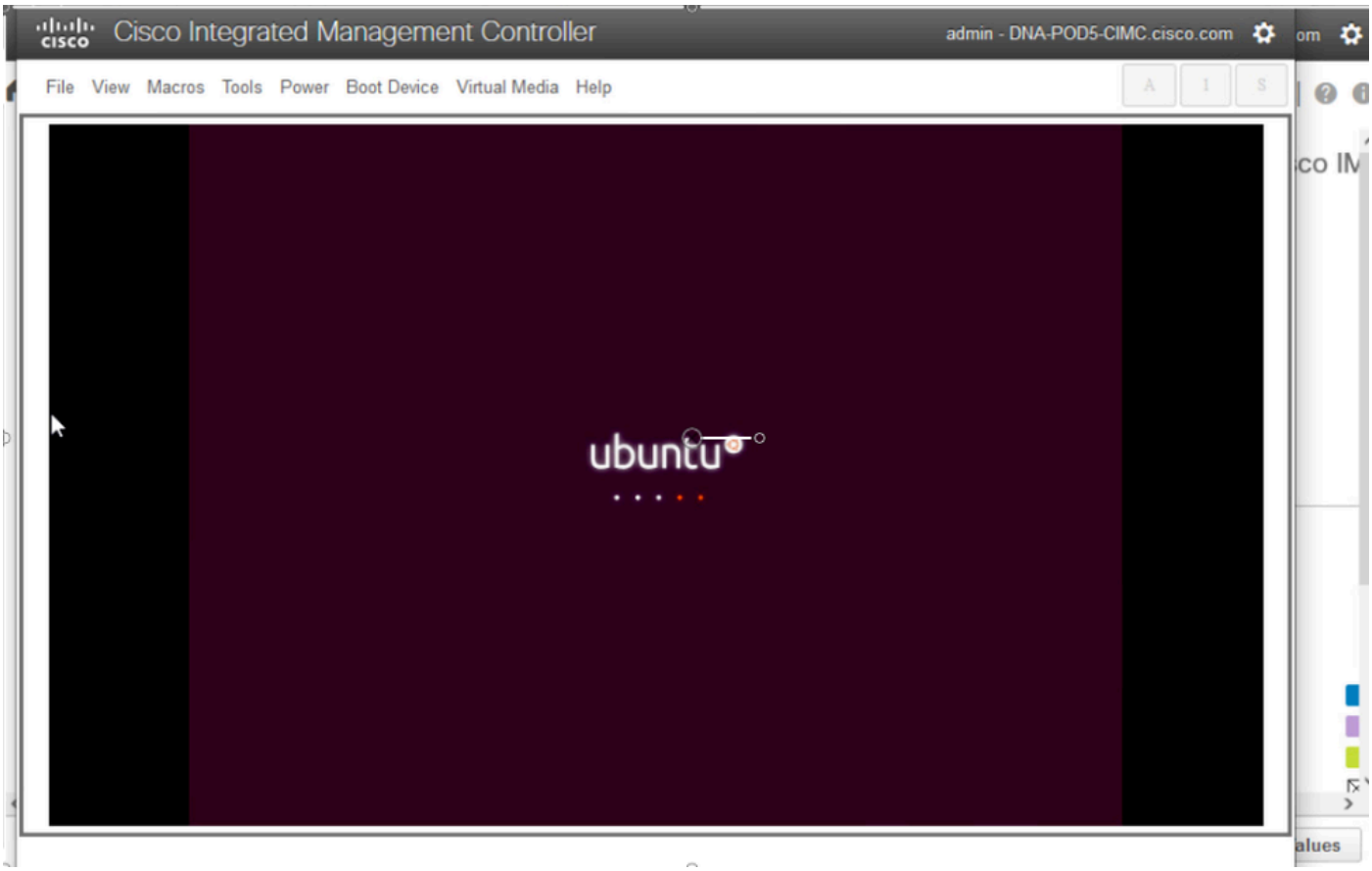
When the boot menu pops up, choose the option that says **Cisco vKVM-Mapped vDVD1.24**. This causes the appliance to boot from the mapped Ubuntu image selected earlier.



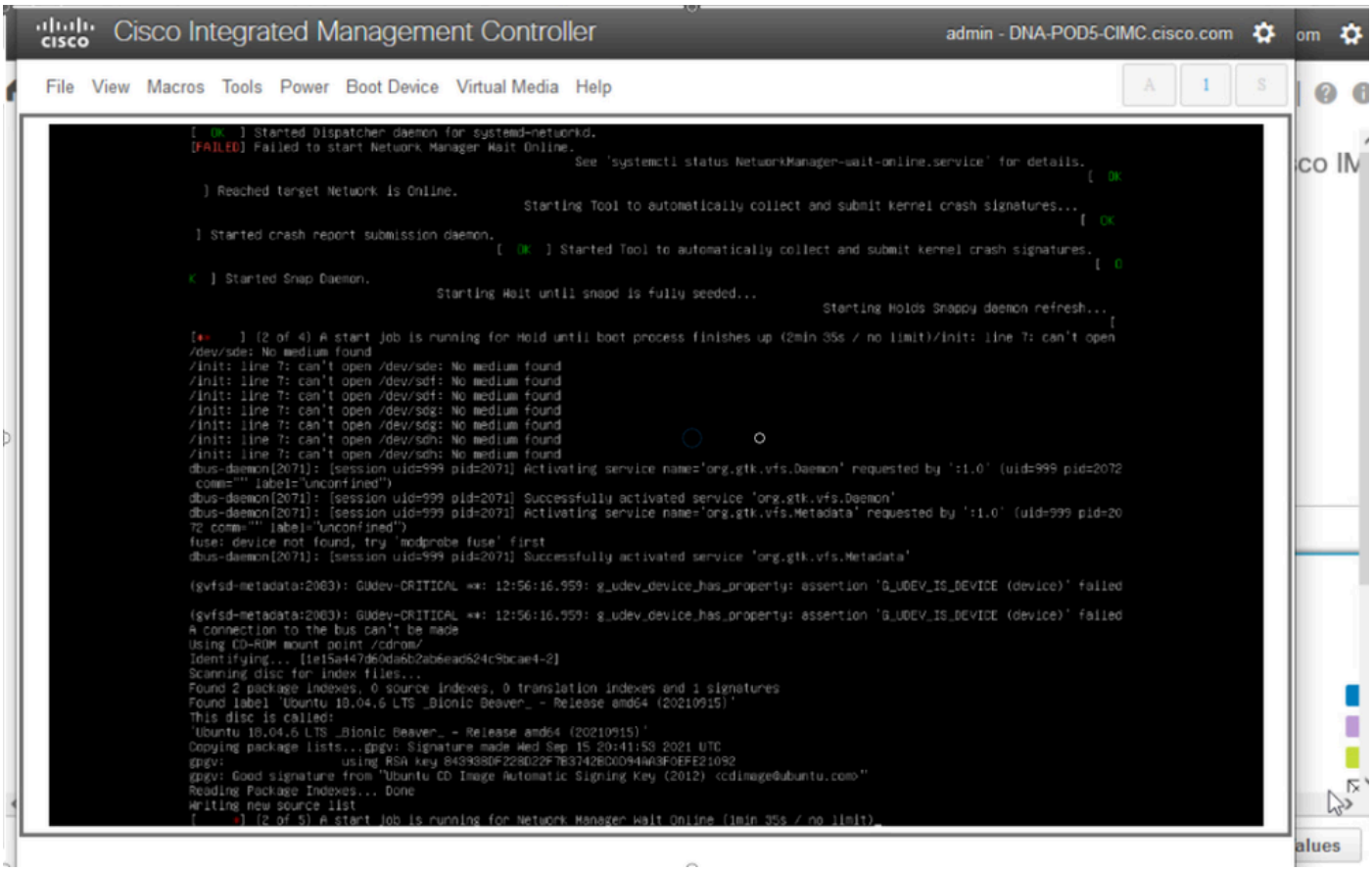
***** NOTE: The screen shots illustrate how long it takes to reach the Ubuntu desktop. *****

This is the first screen we're presented with. It may not look like anything's happening but just wait. In the lab we're on this screen for 40 seconds

After that, the screen turned completely black for about 30 seconds before we're presented with an Ubuntu loading screen. We were on this screen for a little over 5 minutes before it moved on, but times may vary from deployment to deployment.

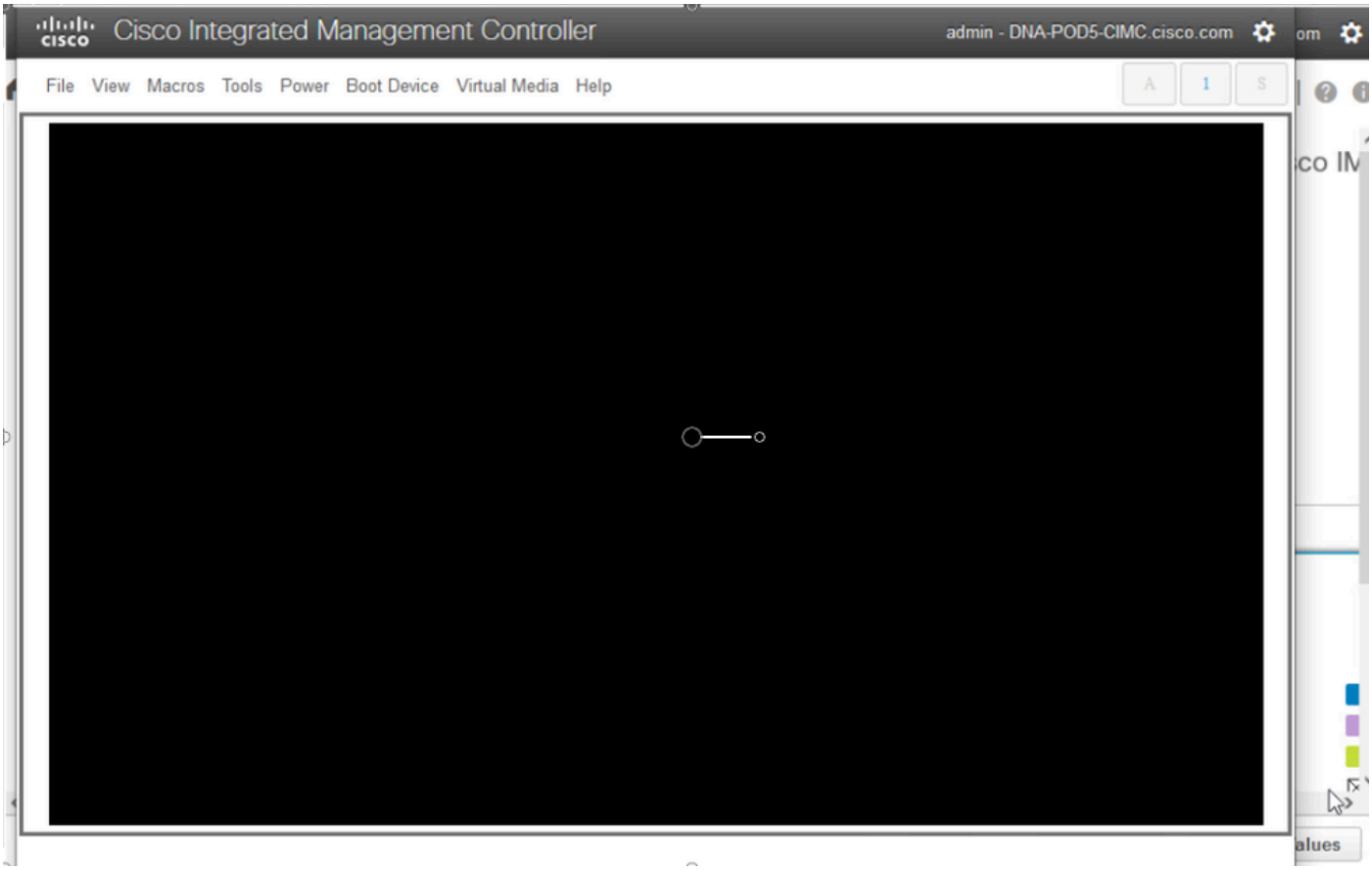


Next, we're presented with a screen that may look like something went wrong, but this is expected. In the lab, this screen stayed up for 2 minutes before proceeding

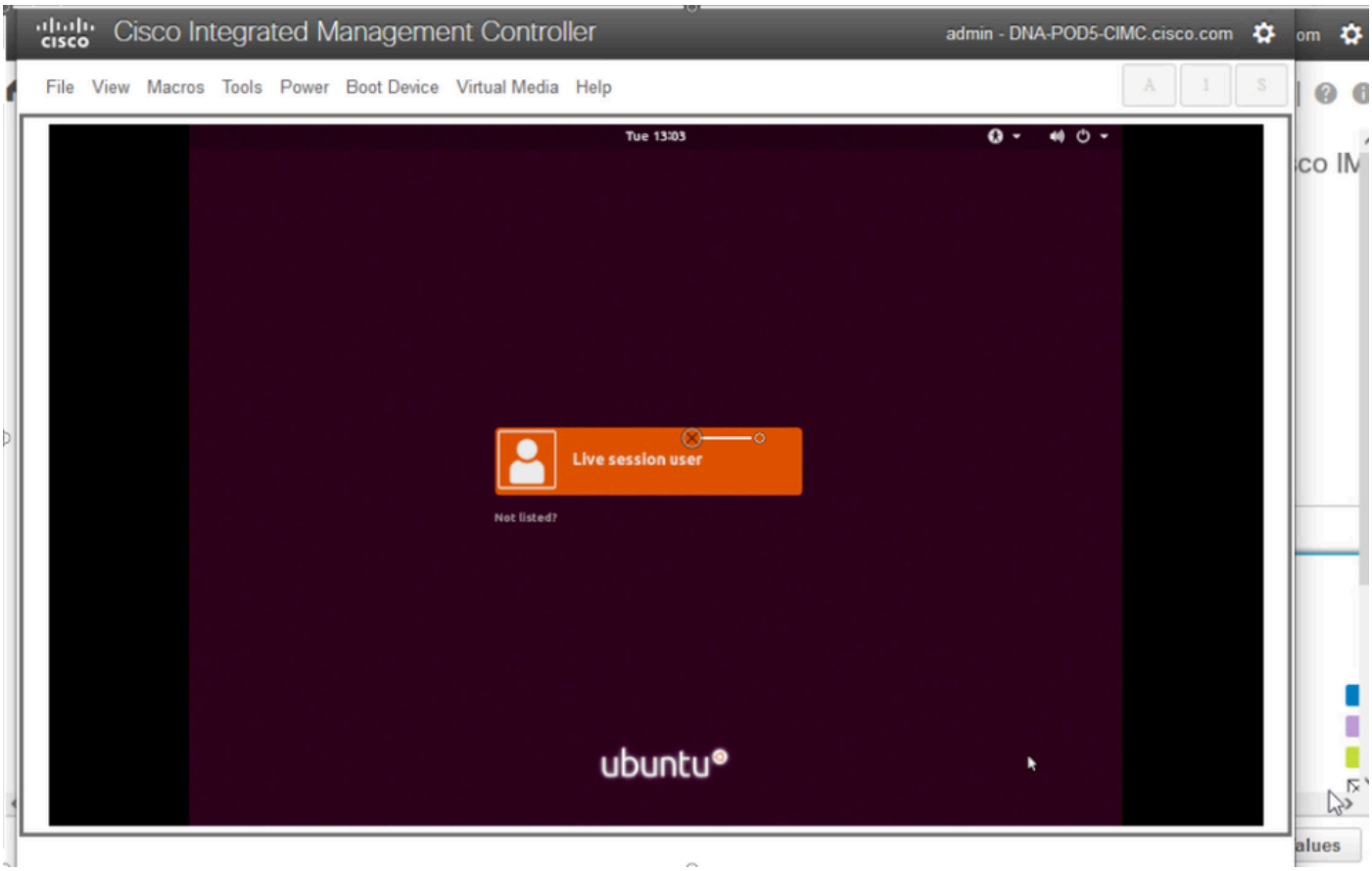


The screen returned to a black screen for about 3 minutes, the above screen flashed again for a few minutes,

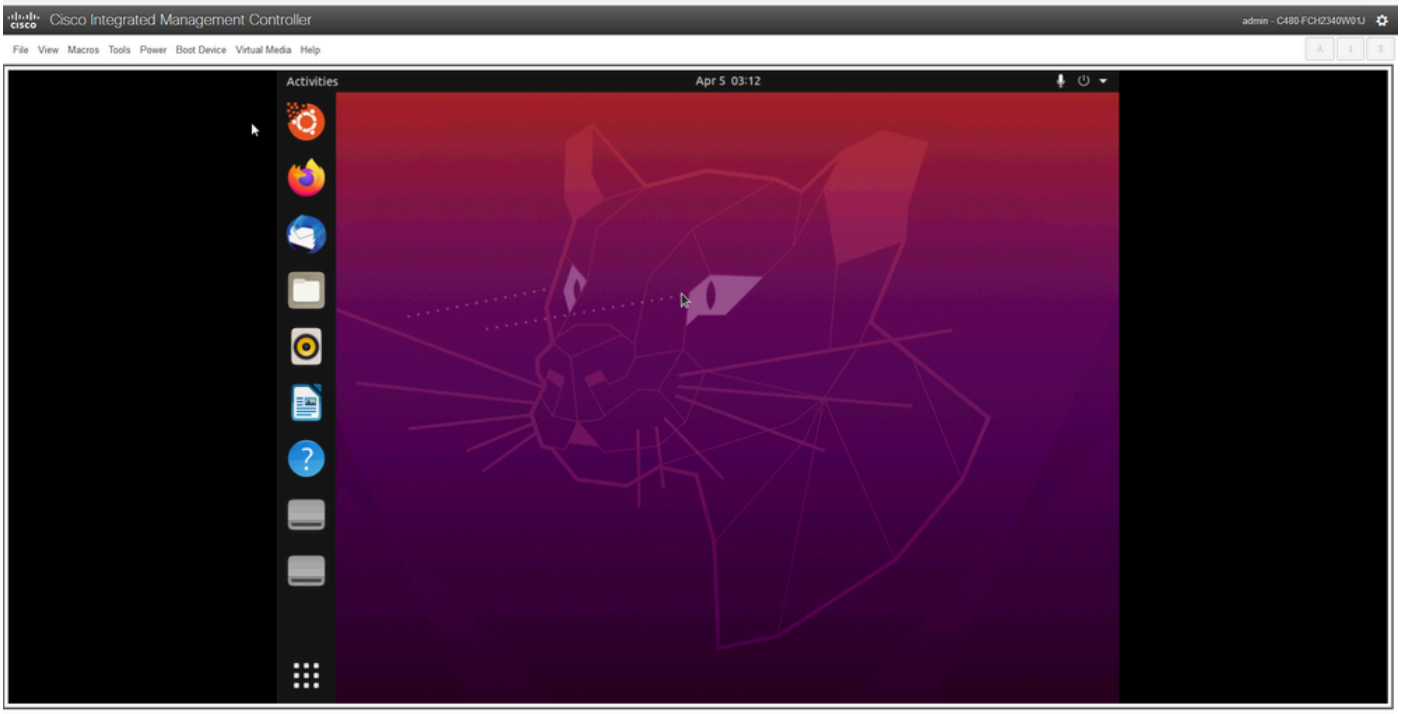
and then returned to the black screen for another two minutes.



Next we're presented with the option to select a Live session user. If we're presented with the option to 'try Ubuntu desktop', choose that option. We welect this user to continue.



Once we select the user, the screen goes black again before we're rpesented with the Ubuntu desktop.



***** REMINDER: It has been seen in some environments to take up to 2 hours to get to this point *****

Step 2: Mount Required Partitions

Once you have access to the Ubuntu desktop GUI environment you need to open the terminal application and perform these steps

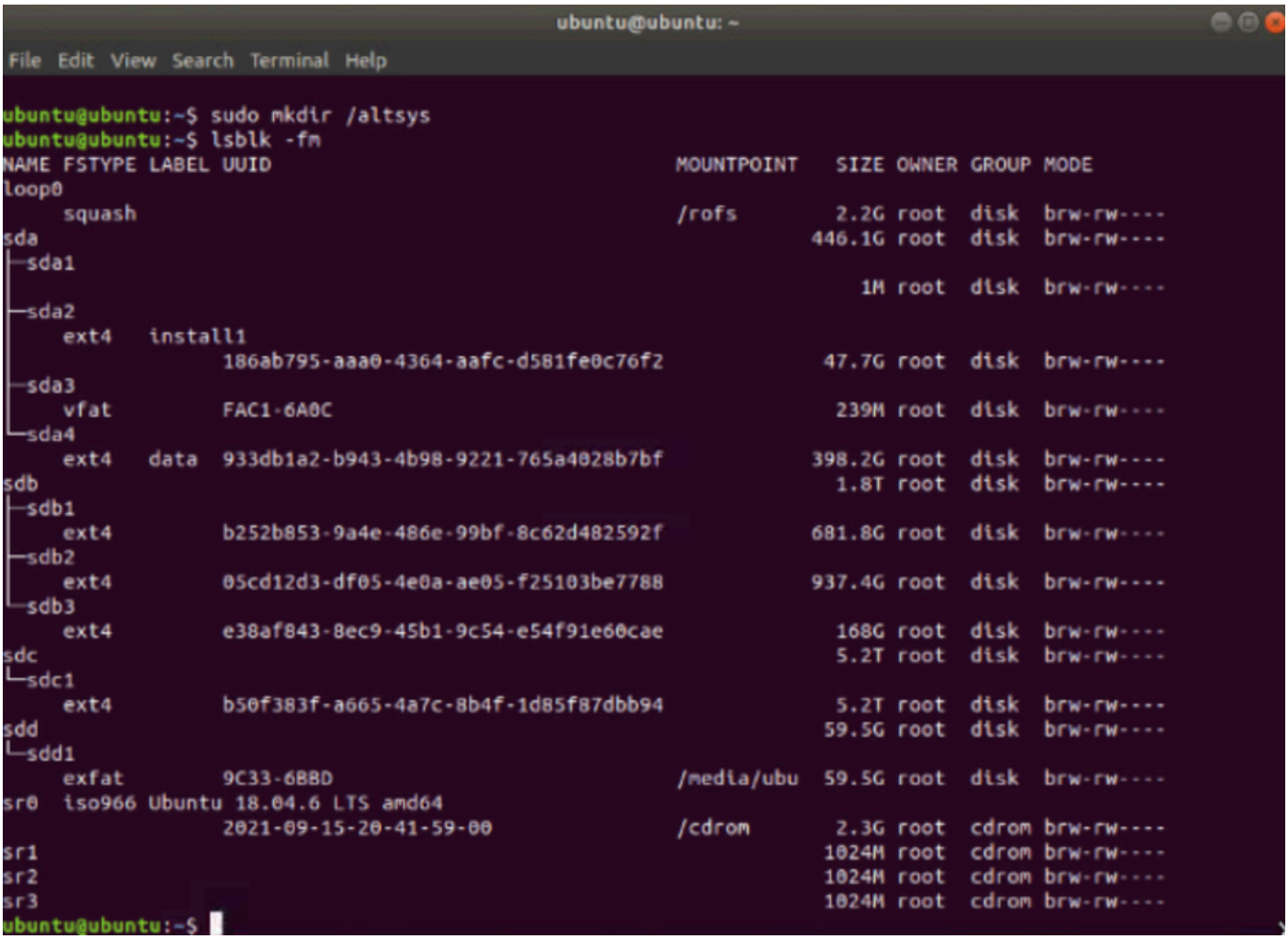
- Create a temporary mount point.
- Mount the root and var partitions to the system.
- Mount the pseudo filesystems to the temporary mount point.

First create the temporary mount point with the command:

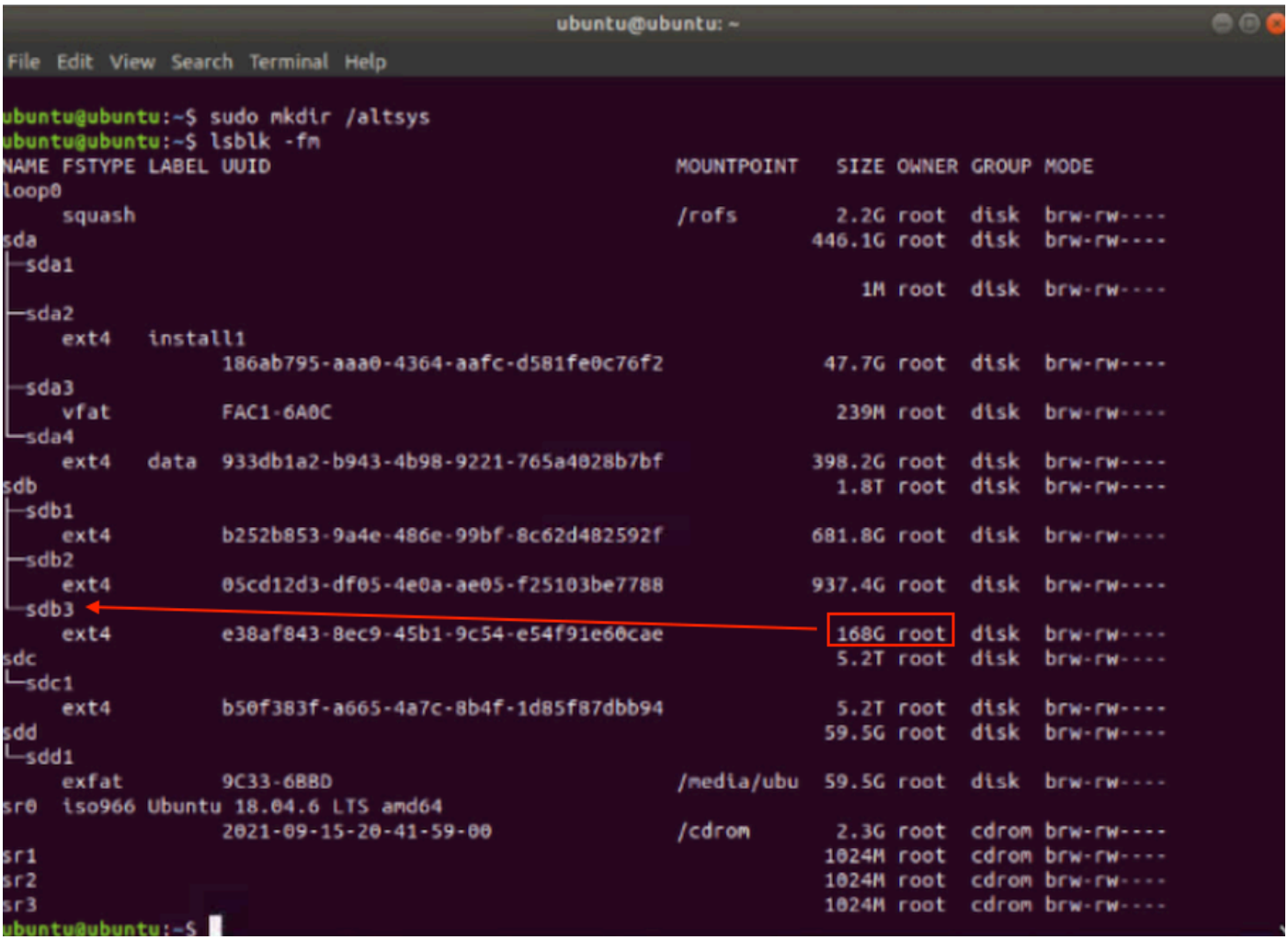
<#root>

```
sudo mkdir /altsys
```

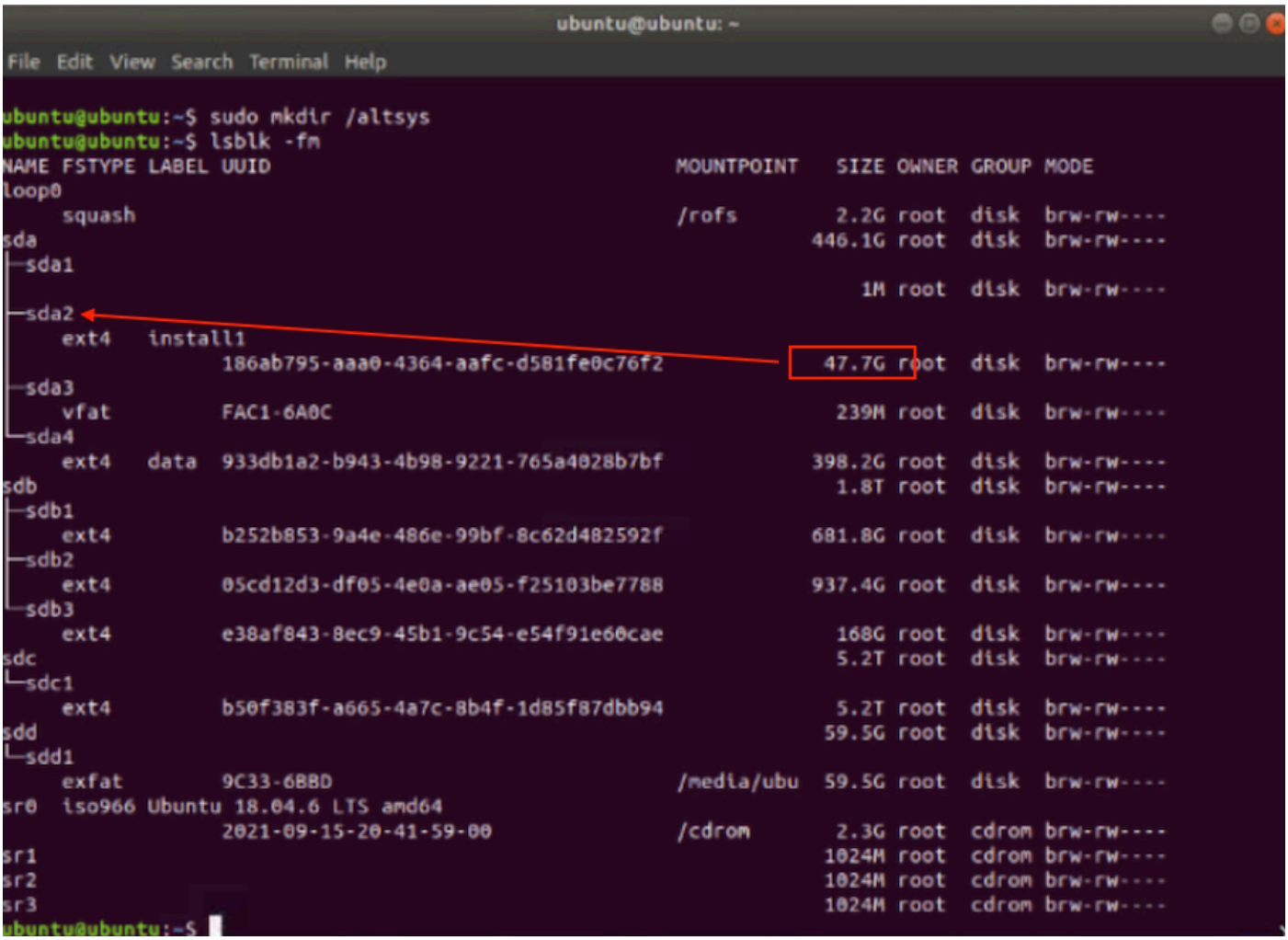
Next, we need to find the root and var partitions to mount. We can use the **lsblk -fm** command to find the partition to mount for **"/"** (root) and **"/var".** Make note of the partition we've identified for the mount commands in the next step



For **/var**, look for a **9.5G** or **168G** partition. We can see in this case it is **sdb3**



For the / (root), look for the **28.66G** or **47.7G** partition. In this example, it is **sda2**



Once you have identified the var and root partitions mount them:

<#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
```

Once root and var have been mounted, mount the psuedo filesystems:

<#root>

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

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

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

The last step before you change the password or unlock the Maglev account is to change to the temporary mount environment:

<#root>

sudo chroot /altsys

Use Case 1: Unlock Maglev Account

Step 1: Verify that maglev user is unlocked

<#root>

grep maglev /etc/shadow

<#root>

maglev:

!

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

Check if there is an exclamation mark in front of the password hash or not. If there is, that indicates the account is locked. Type in the command to unlock the user:

Unlock the maglev user with the command:

<#root>

usermod -U maglev

Step 2: Reset failed count

If the user does not have an escalation mark in front of the hash in the **/etc/shadow** file, then the login failure limit has been exceeded. Please use these steps to reset failed login attempts.

Find the failed login attempts for the maglev user:

<#root>

$

sudo pam_tally2 -u maglev

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

As shown here, the login attempts are larger than the default 6 attempts. This denies that user the ability to log in until the failure count drops to less than six (6). You can reset the login failure count with the command:

<#root>

sudo pam_tally2 -r -u maglev

You can confirm that the counter has been reset:

<#root>

sudo pam_tally2 -u maglev

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

Use Case 2: Reset Maglev User Password

Step 1: Reset the Maglev user password

<#root>

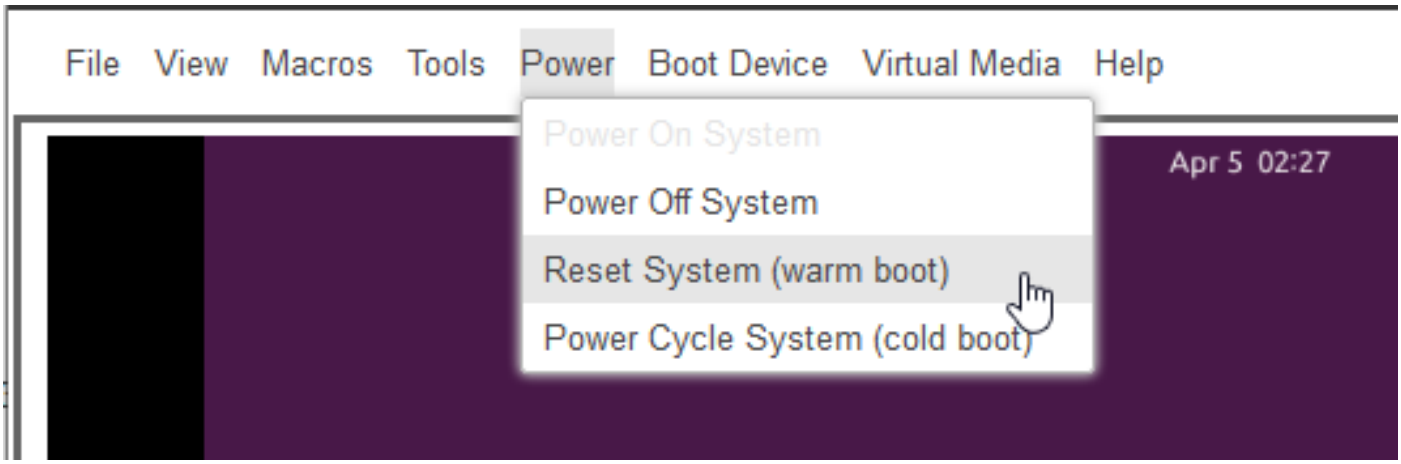
#

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
```

Step 2: Reboot normally to Cisco DNA Center environment

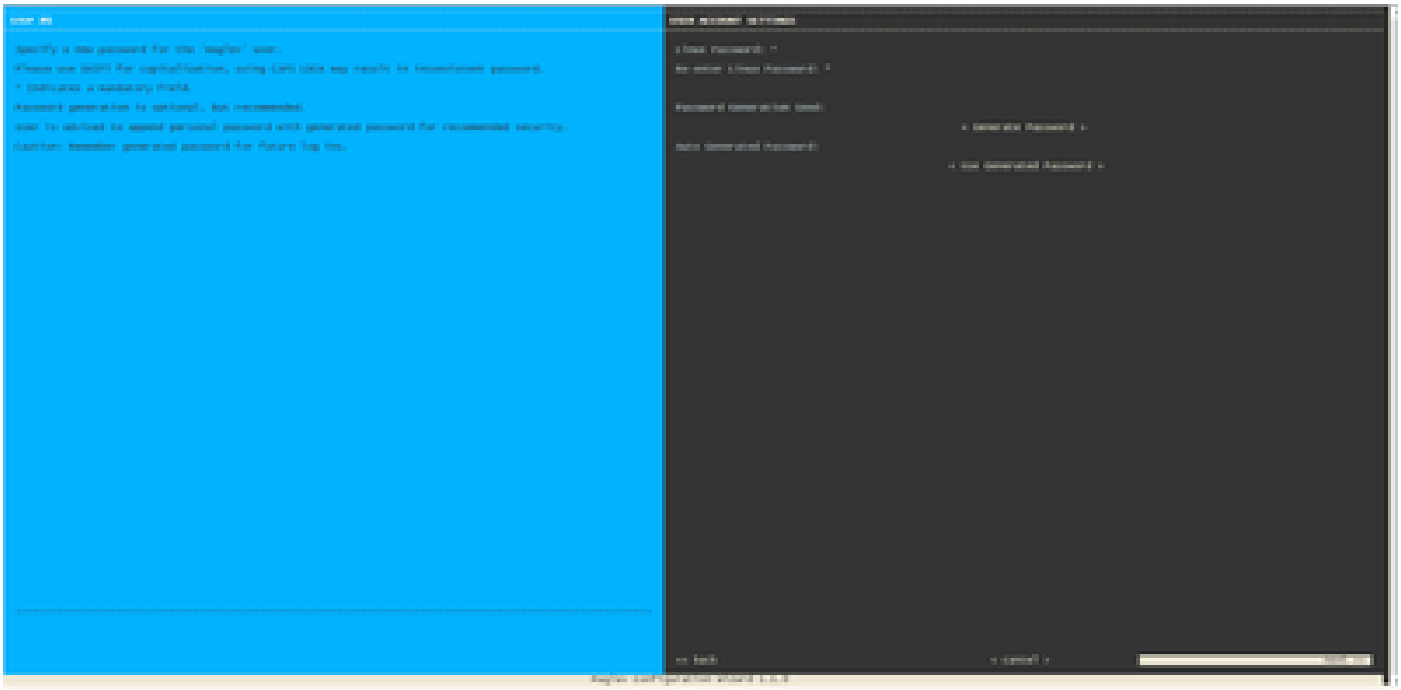
Click on **Power** in the KVM window and then **Reset System (warm boot)**. This causes the system to reboot and boot with the RAID controller so that the Cisco DNA Center software boots up.



Step 3: Update Maglev User Password from Cisco DNA Center CLI

Once the Cisco DNA Center software boots and you have access to the CLI, you need to change the Maglev password with the command **sudo maglev-config update**. This step is required to ensure that the change takes affect across the whole system.

Once the config wizard has been launched, you need to navigate completely through the wizard to screen that allows us to set the Maglev password in step 6.



Once the password has been set for both fields **Linux Password** and **Re-enter Linux Password**, choose **next** and complete the wizard. When the wizard finishes the configuration push, the password is successfully changed. You can create a new SSH session or enter in the command **sudo -i** in the CLI to test that the password has been changed.

Step-by-Step Video Guide

Please use the link below to access the step-by-step video created for this workflow.