

Reset Cisco DNA Center's Maglev User Password

Contents

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Step 1: Boot from Live CD](#)

[Step 2: Mount Required Partitions](#)

[Use Case 1: Unlock Maglev Account](#)

[Step 1: Verify that maglev user is unlocked](#)

[Step 2: Reset failed count](#)

[Use Case 2: Reset Maglev User Password](#)

[Step 1: Reset the Maglev user password](#)

[Step 2: Reboot normally to Cisco DNA Center environment](#)

[Step 3: Update Maglev User Password from Cisco DNA Center CLI](#)

[Step-by-Step Video Guide](#)

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.

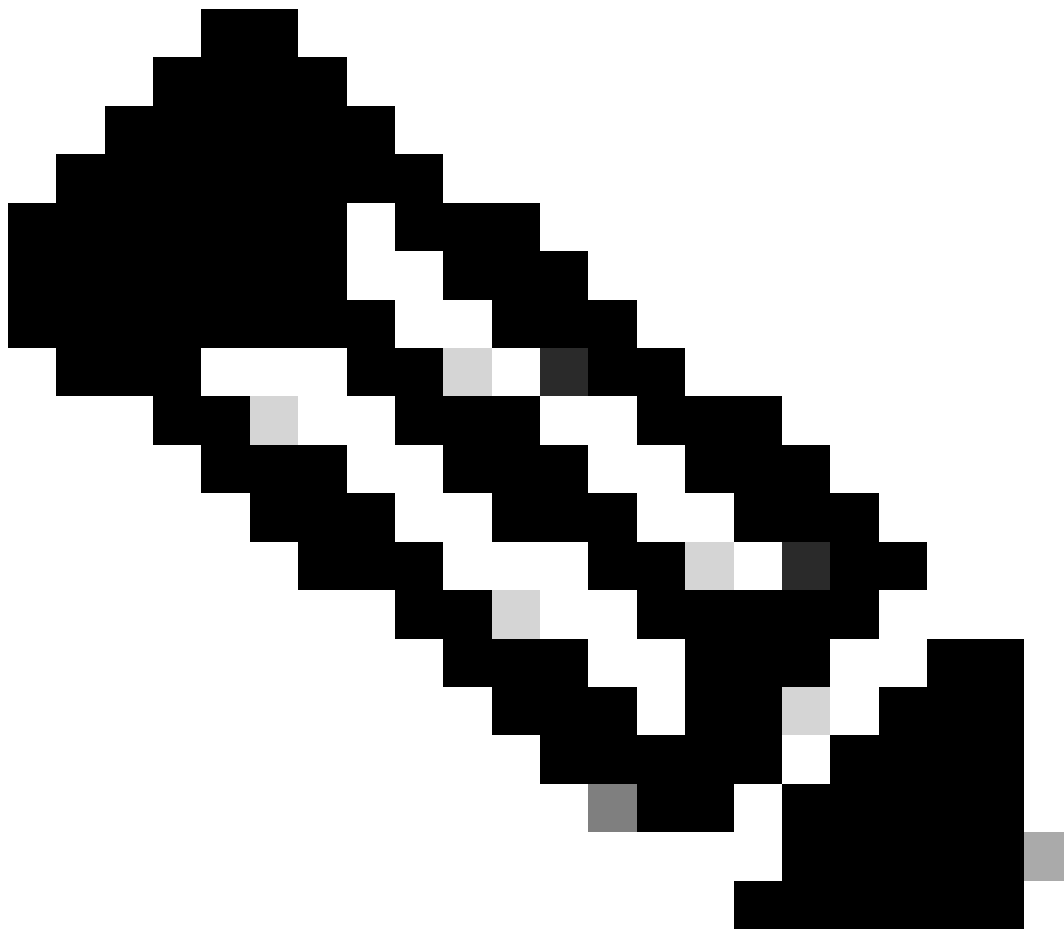
Components Used

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 *****

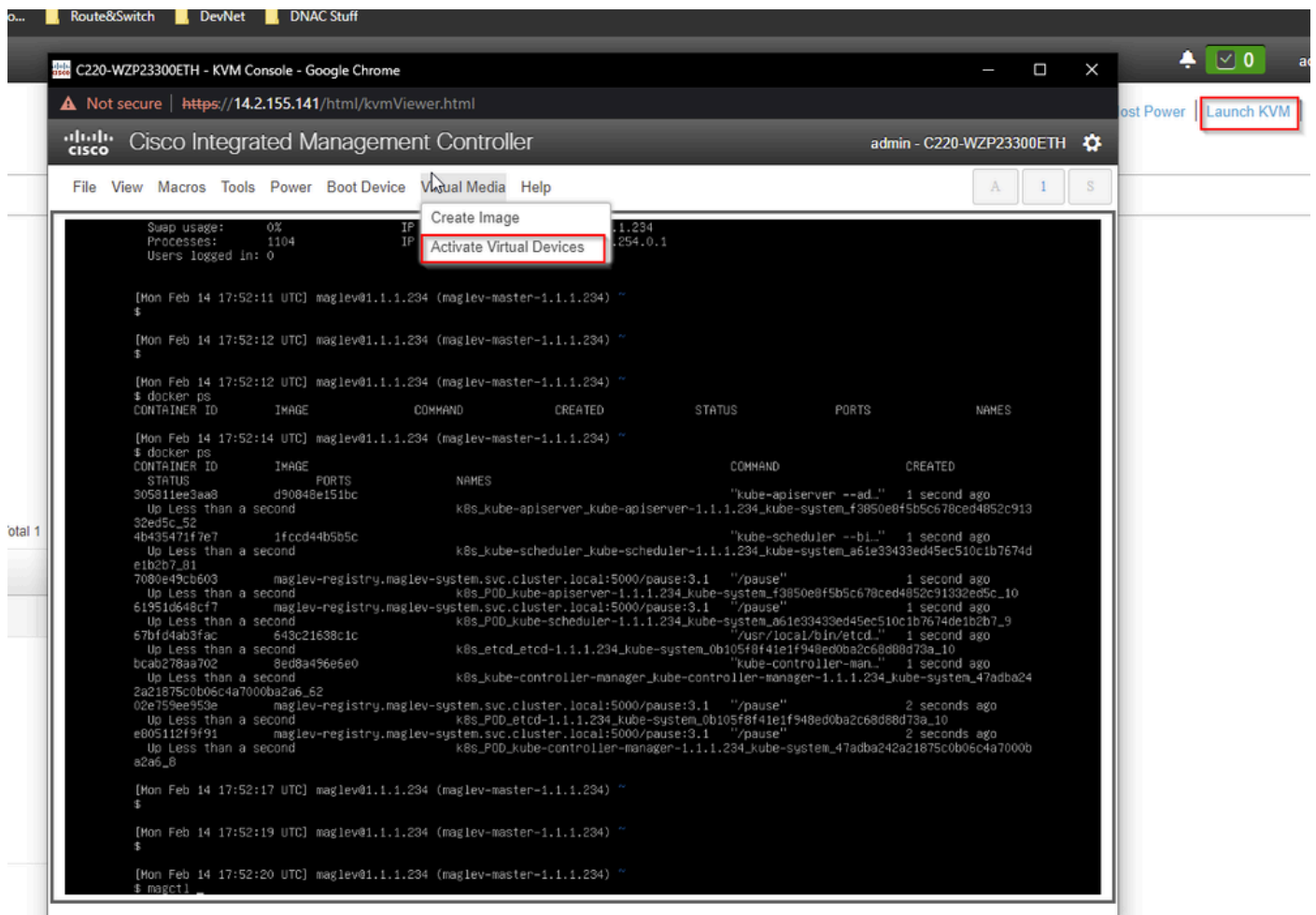
In a 1+1+1 DR deployment, the corresponding site is down while this process is completed.

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

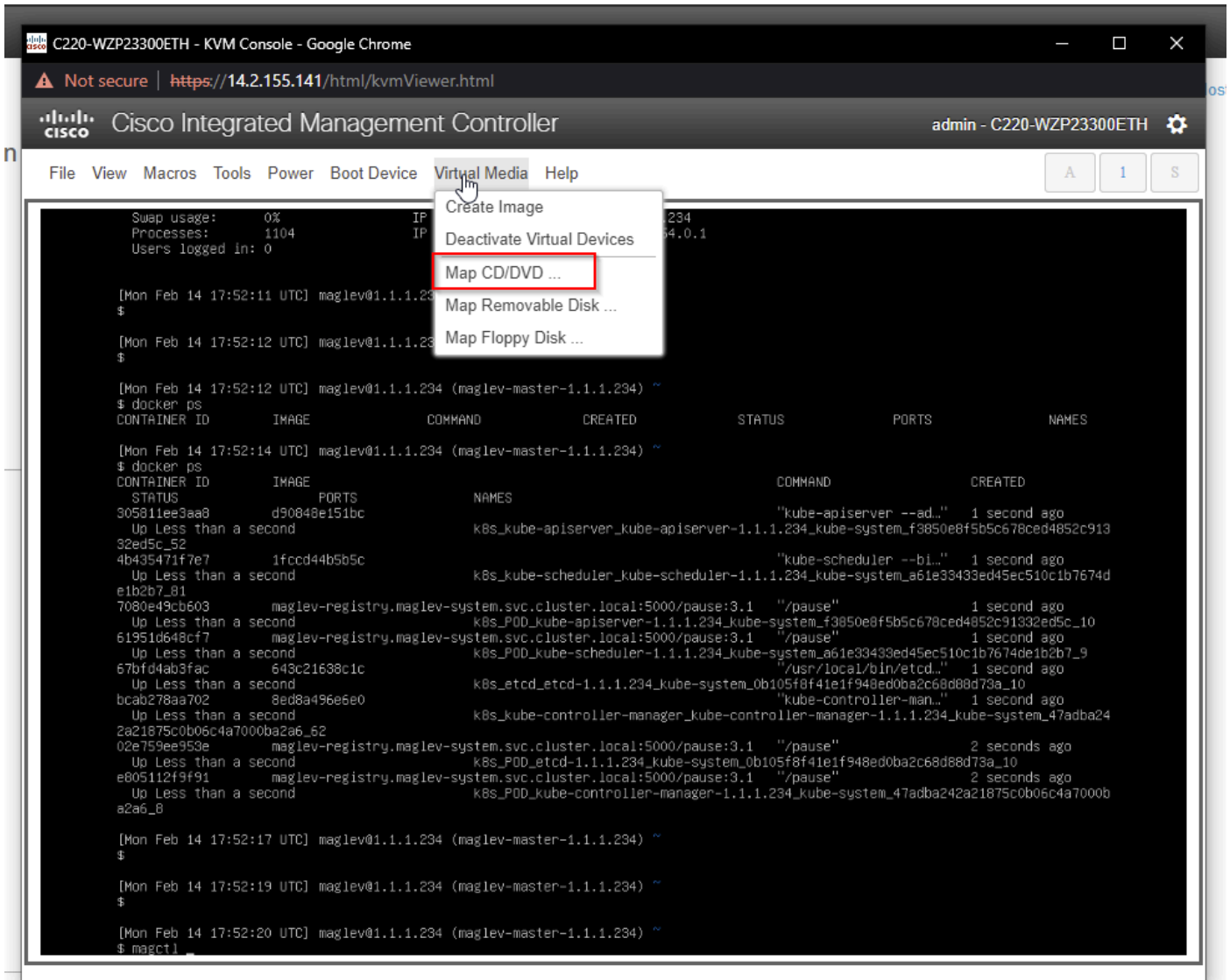
the two other nodes are available to avoid an unnecessary DR failover.

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.

C220-WZP23300ETH - KVM Console - Google Chrome

Not secure | https://14.2.155.141/html/kvmViewer.html

Cisco Integrated Management Controller admin - C220-WZP23300ETH

File View Macros Tools Power Boot Device Virtual Media Help

```
Swap usage: 0% IP address for cluster: 1.1.1.234
Processes: 1104 IP address for docker0: 169.254.0.1
Users logged in: 0
```

[Mon Feb 14 17:52:11 UTC] maglev@1.1.1.234 (maglev-master-1.1.1.234) ~
\$

[Mon Feb 14 17:52:12 UTC] maglev@1.1.1.234 (maglev-master-1.1.1.234) ~
\$

[Mon Feb 14 17:52:12 UTC] maglev@1.1.1.234 (maglev-master-1.1.1.234) ~
\$ docker ps

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
[Mon Feb 14 17:52:14 UTC] maglev@1.1.1.234 (maglev-master-1.1.1.234) ~						
\$ docker ps						
CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
305811ee3aa8	maglev-registry	"/pause"	1 second ago	Up Less than a second		maglev-registry
32ed5c_52	maglev-registry	"/pause"	1 second ago	Up Less than a second		maglev-registry
4b435471f7e7	maglev-registry	"/pause"	1 second ago	Up Less than a second		maglev-registry
e1b2b7_81	maglev-registry	"/pause"	1 second ago	Up Less than a second		maglev-registry
7080e49cb603	maglev-registry	"/pause"	1 second ago	Up Less than a second		maglev-registry
61951d648cf7	maglev-registry	"/pause"	1 second ago	Up Less than a second		maglev-registry
67bfd4ab3fac	643c21638c1c	"/usr/local/bin/etcd..."	1 second ago	Up Less than a second		etcd
bcab278aa702	8ed8a496e5e0	"/pause"	1 second ago	Up Less than a second		maglev-registry
2a21875c0b06c4a7000ba2a6_62	maglev-registry	"/pause"	1 second ago	Up Less than a second		maglev-registry
02e759ee953e	maglev-registry	"/pause"	1 second ago	Up Less than a second		maglev-registry
e805112f9f91	maglev-registry	"/pause"	1 second ago	Up Less than a second		maglev-registry
a2a6_8	maglev-registry	"/pause"	1 second ago	Up Less than a second		maglev-registry
[Mon Feb 14 17:52:17 UTC] maglev@1.1.1.234 (maglev-master-1.1.1.234) ~						
\$						
[Mon Feb 14 17:52:19 UTC] maglev@1.1.1.234 (maglev-master-1.1.1.234) ~						
\$						
[Mon Feb 14 17:52:20 UTC] maglev@1.1.1.234 (maglev-master-1.1.1.234) ~						
\$ magctl						

Virtual Media - CD/DVD

Image File : Browse

Read Only

Map Drive Cancel

Then browse for the Ubuntu image and then press the "Map Drive" button.

Virtual Media - CD/DVD

Image File : Browse

Read Only

Map Drive Cancel

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

C220-WZP23300ETH - KVM Console - Google Chrome

Not secure | https://14.2.155.141/html/kvmViewer.html

Cisco Integrated Management Controller admin - C220-WZP23300ETH

File View Macros Tools **Power** Boot Device Virtual Media Help

- Power On System
- Power Off System
- Reset System (warm boot)**
- Power Cycle System (cold boot)

```
Swap usage:
Processes:
Users logged in:

[Mon Feb 14 17:52:12 UTC] maglev@1.1.1.234 (maglev-master-1.1.1.234) ~
$

[Mon Feb 14 17:52:12 UTC] maglev@1.1.1.234 (maglev-master-1.1.1.234) ~
$ docker ps
CONTAINER ID        IMAGE                                COMMAND                  CREATED             STATUS             PORTS             NAMES
[Mon Feb 14 17:52:14 UTC] maglev@1.1.1.234 (maglev-master-1.1.1.234) ~
$ docker ps
CONTAINER ID        IMAGE                                COMMAND                  CREATED             STATUS             PORTS             NAMES
STATUS            PORTS            NAMES
305811ee3aa8       d90848e151bc          "kube-apiserver --ad..." 1 second ago
Up Less than a second
32ed5c_52          k8s_kube-apiserver_kube-apiserver-1.1.1.234_kube-system_f3850e8f5b5c678ced4852c913
4b435471f7e7       1fccd44b5b5c          "kube-scheduler --bi..." 1 second ago
Up Less than a second
e1b2b7_81         k8s_kube-scheduler_kube-scheduler-1.1.1.234_kube-system_a61e33433ed45ec510c1b7674d
7080e49cb603       maglev-registry.maglev-system.svc.cluster.local:5000/pause:3.1 "/pause"                1 second ago
Up Less than a second
619510648cf7       maglev-registry.maglev-system.svc.cluster.local:5000/pause:3.1 "/pause"                1 second ago
Up Less than a second
67bfd4ab3fac       643c21638c1c          "usr/local/bin/etcd..." 1 second ago
Up Less than a second
bcab278aa702       8ed8a496e6e0          "kube-controller-man..." 1 second ago
Up Less than a second
2a21875c0b06c4a7000ba2a6_62
02e759ee953e       maglev-registry.maglev-system.svc.cluster.local:5000/pause:3.1 "/pause"                2 seconds ago
Up Less than a second
e805112f9f91       maglev-registry.maglev-system.svc.cluster.local:5000/pause:3.1 "/pause"                2 seconds ago
Up Less than a second
a2a6_8             k8s_POD_kube-controller-manager-1.1.1.234_kube-system_47adba242a21875c0b06c4a7000b

[Mon Feb 14 17:52:17 UTC] maglev@1.1.1.234 (maglev-master-1.1.1.234) ~
$

[Mon Feb 14 17:52:19 UTC] maglev@1.1.1.234 (maglev-master-1.1.1.234) ~
$

[Mon Feb 14 17:52:20 UTC] maglev@1.1.1.234 (maglev-master-1.1.1.234) ~
$ magctl
```

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



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 SNRAID 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

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

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

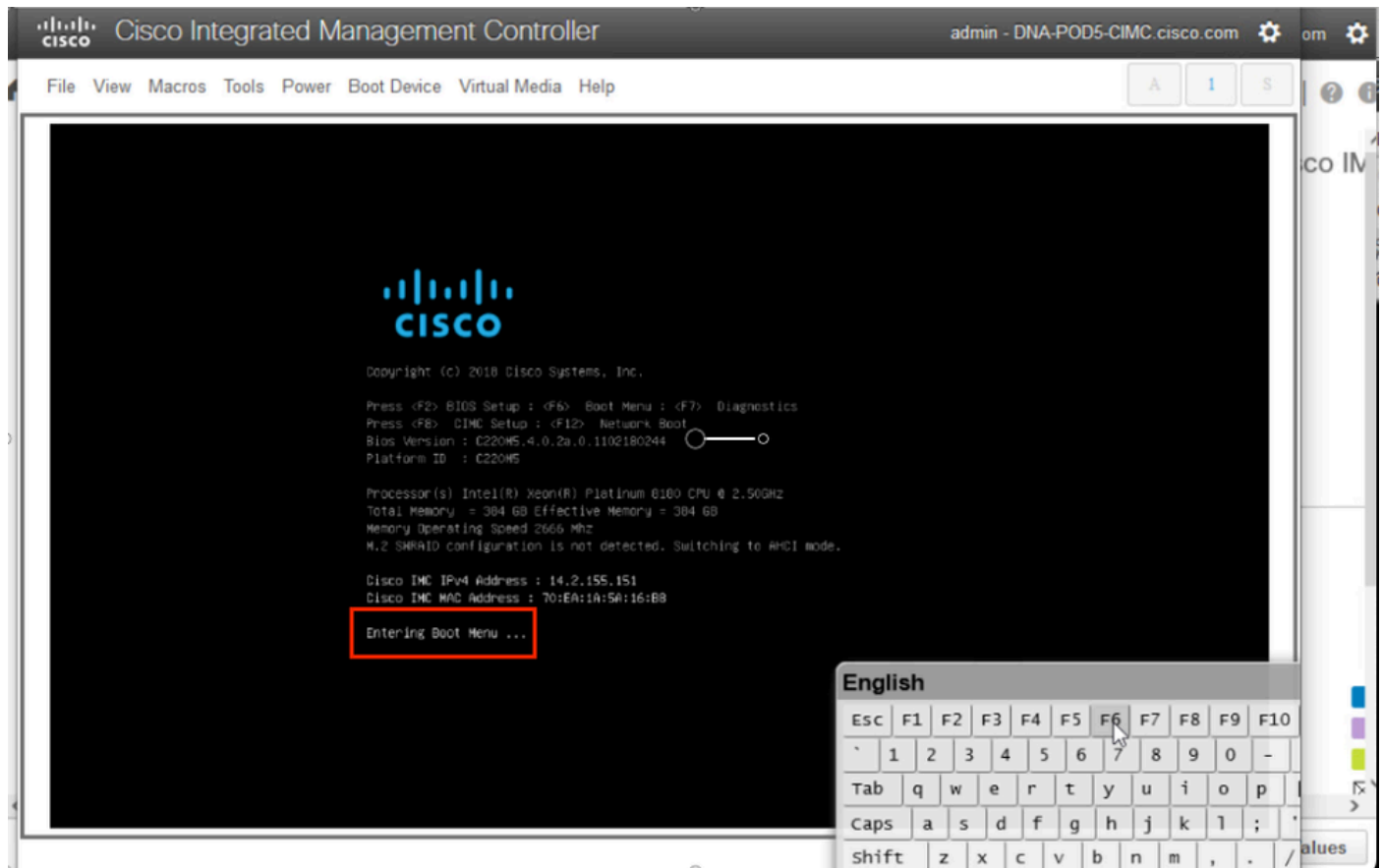
0 JBOD(s) found on the host adapter
3 Virtual Drive(s) found on the host adapter.

0 JBOD(s) handled by BIOS
3 Virtual Drive(s) handled by BIOS.
Press <Ctrl><R> to Run MegaRAID Configuration Utility

English

Esc	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
`	1	2	3	4	5	6	7	8	9	0
Tab	q	w	e	r	t	y	u	i	o	p
Caps	a	s	d	f	g	h	j	k	l	;
shift	z	x	c	v	b	n	m	,	.	/

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.

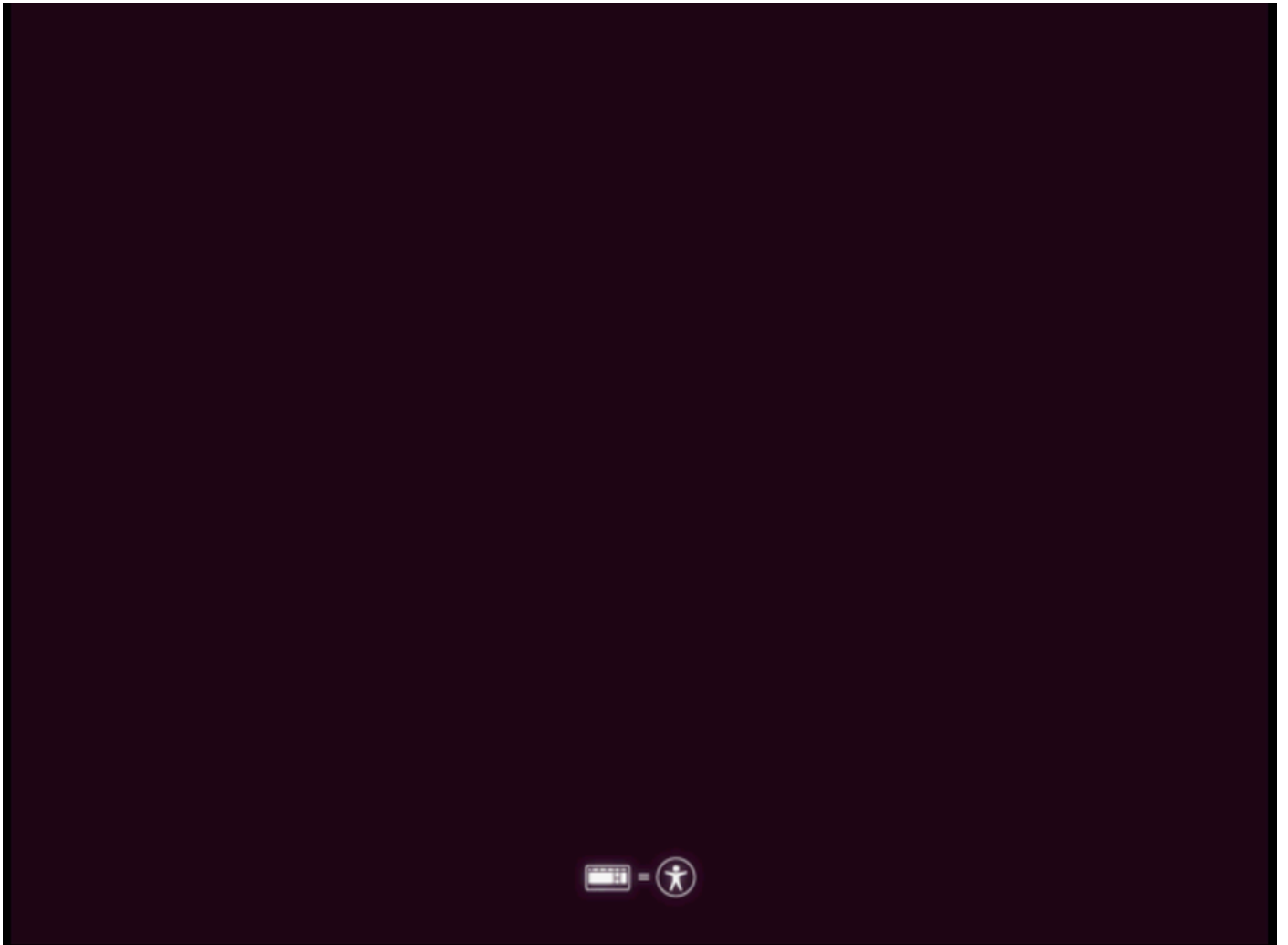
Please select boot device:

(Bus 33 Dev 00)PCI RAID Adapter
CiscoVD Hypervisor
SanDisk
UEFI: Built-in EFI Shell
IBA XE (X550) Slot 3500 v2413
IBA XE (X550) Slot 3501 v2413
Cisco vKVM-Mapped vDVD1.24
Cisco vKVM-Mapped vHDD1.24
Cisco vKVM-Mapped vFDD1.24
Cisco CIMC-Mapped vDVD1.24
Cisco CIMC-Mapped vHDD1.24
Cisco Flexutil DVD 1 1.24

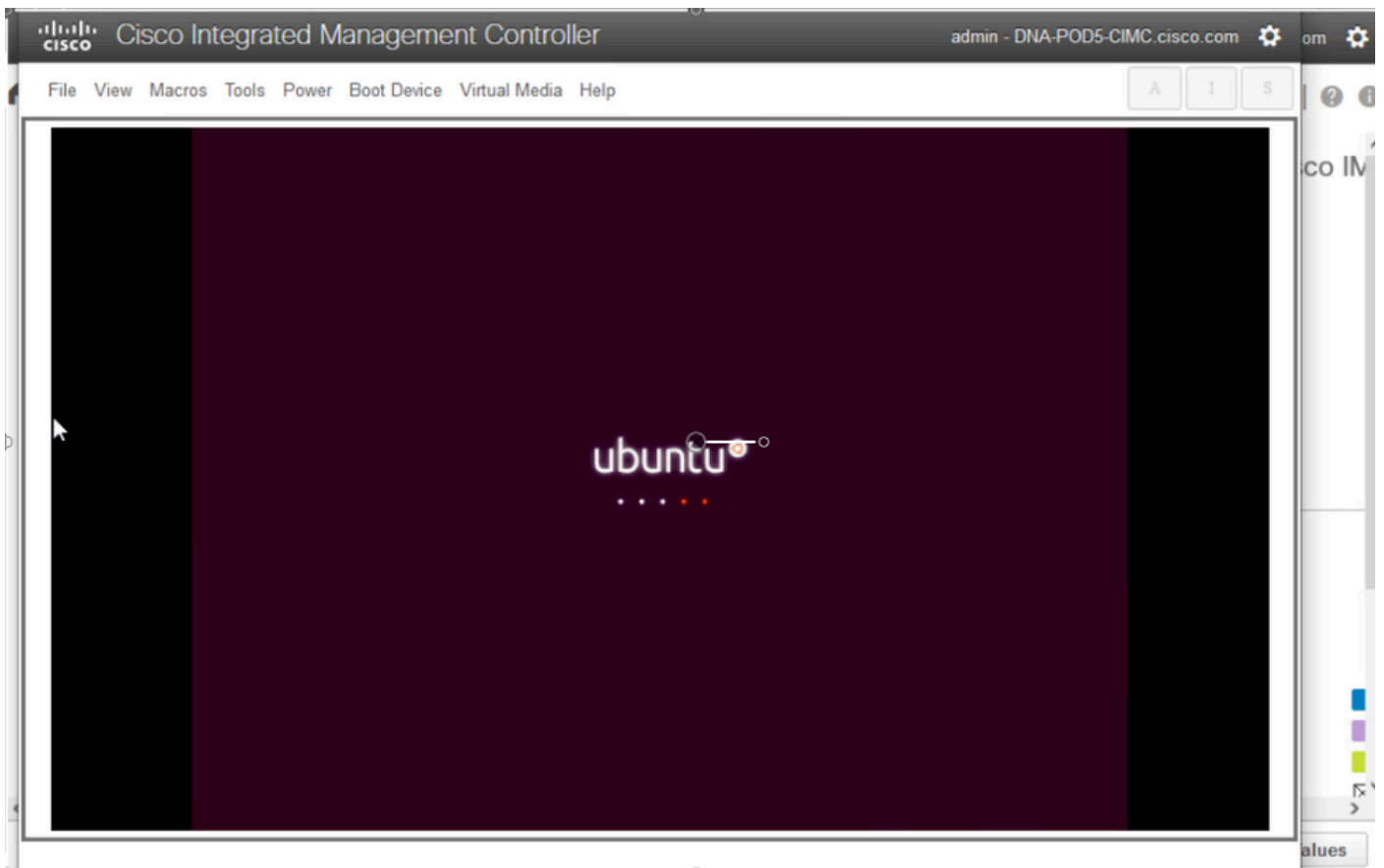
↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults

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

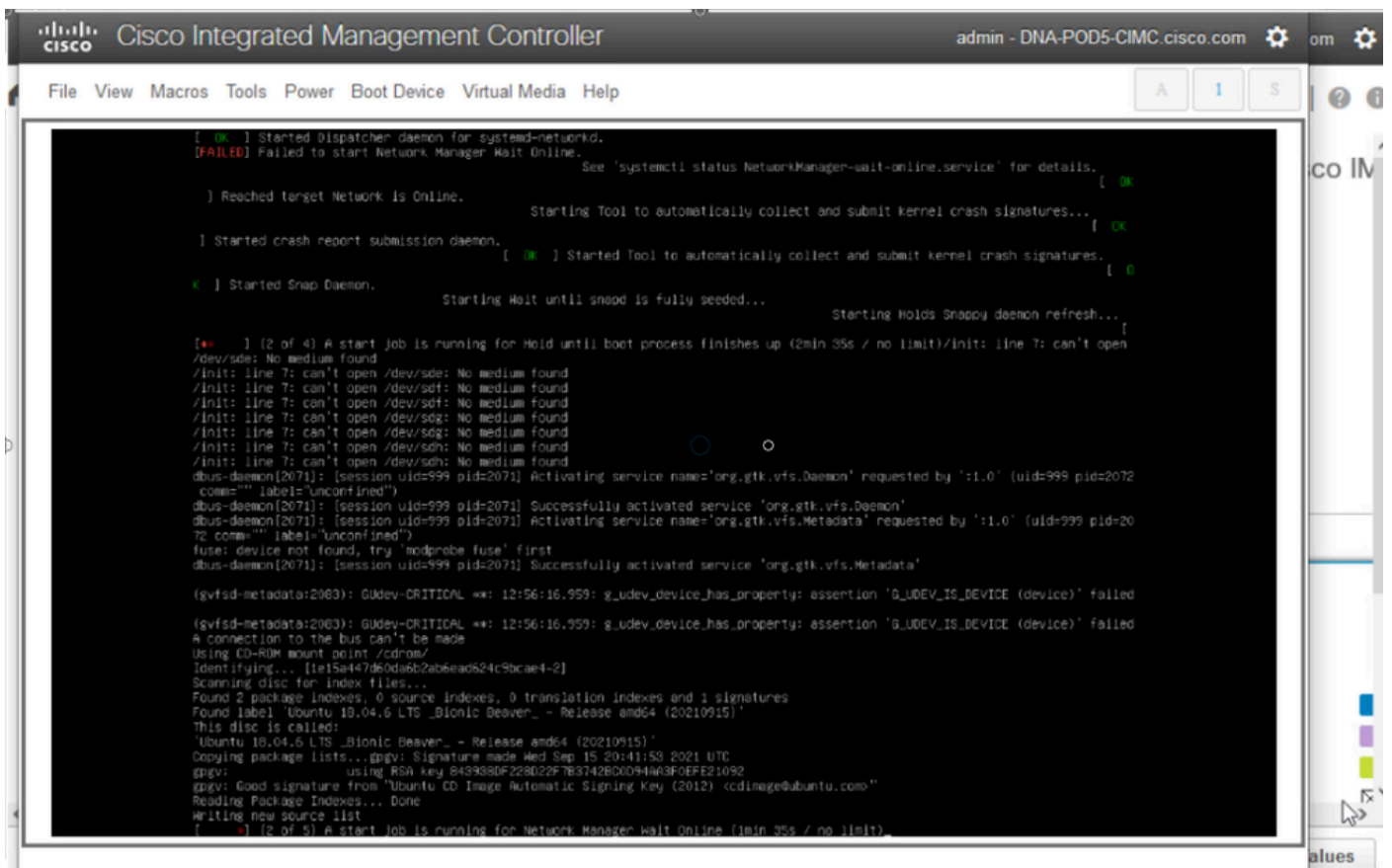
This is the first screen we're presented with. It may not look like anything's happening but just wait. In the lab we're on this screen for 40 seconds



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.

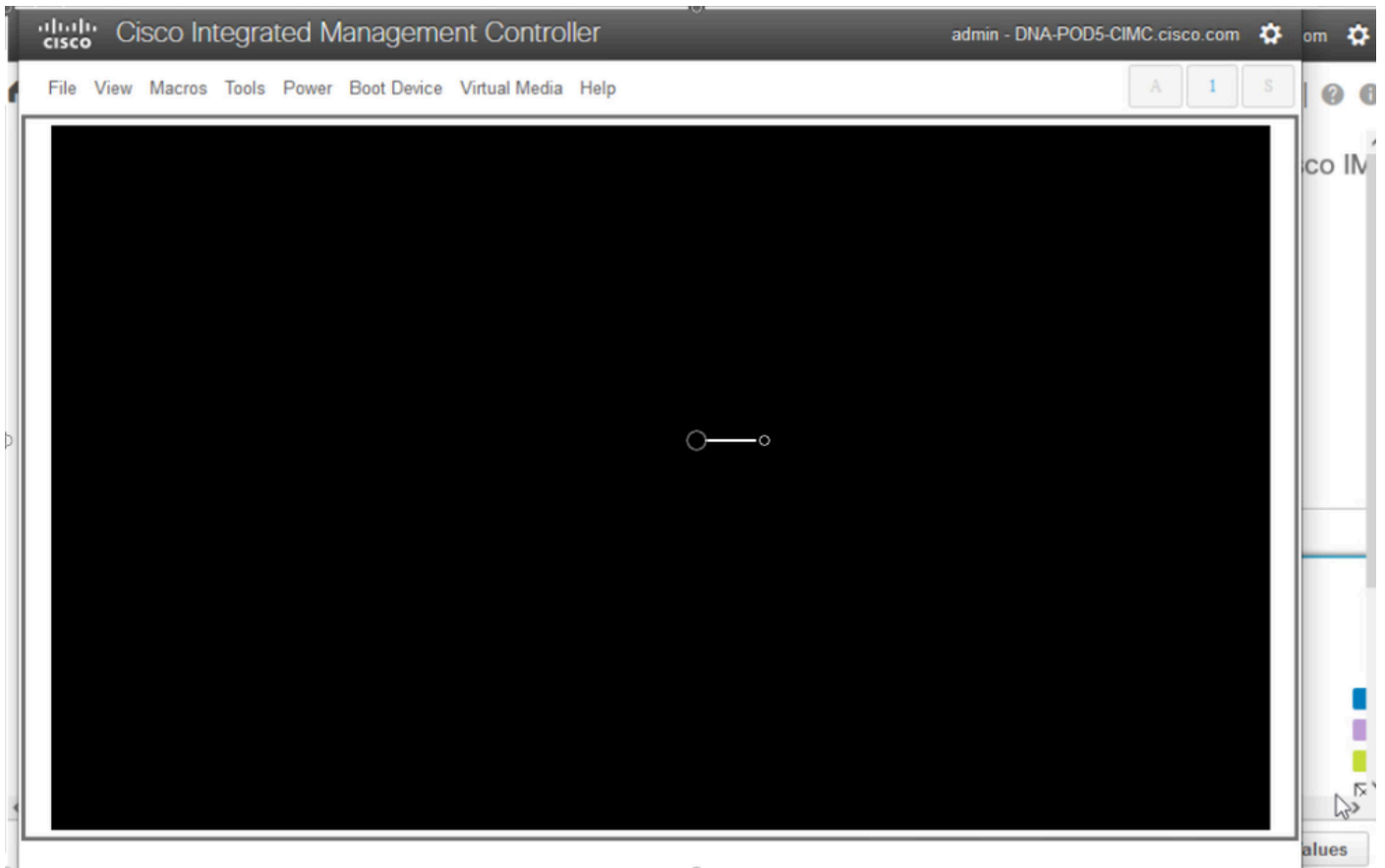


Next, we're presented with a screen that may look like something went wrong, but this is expected. In the lab, this screen stayed up for 2 minutes before proceeding

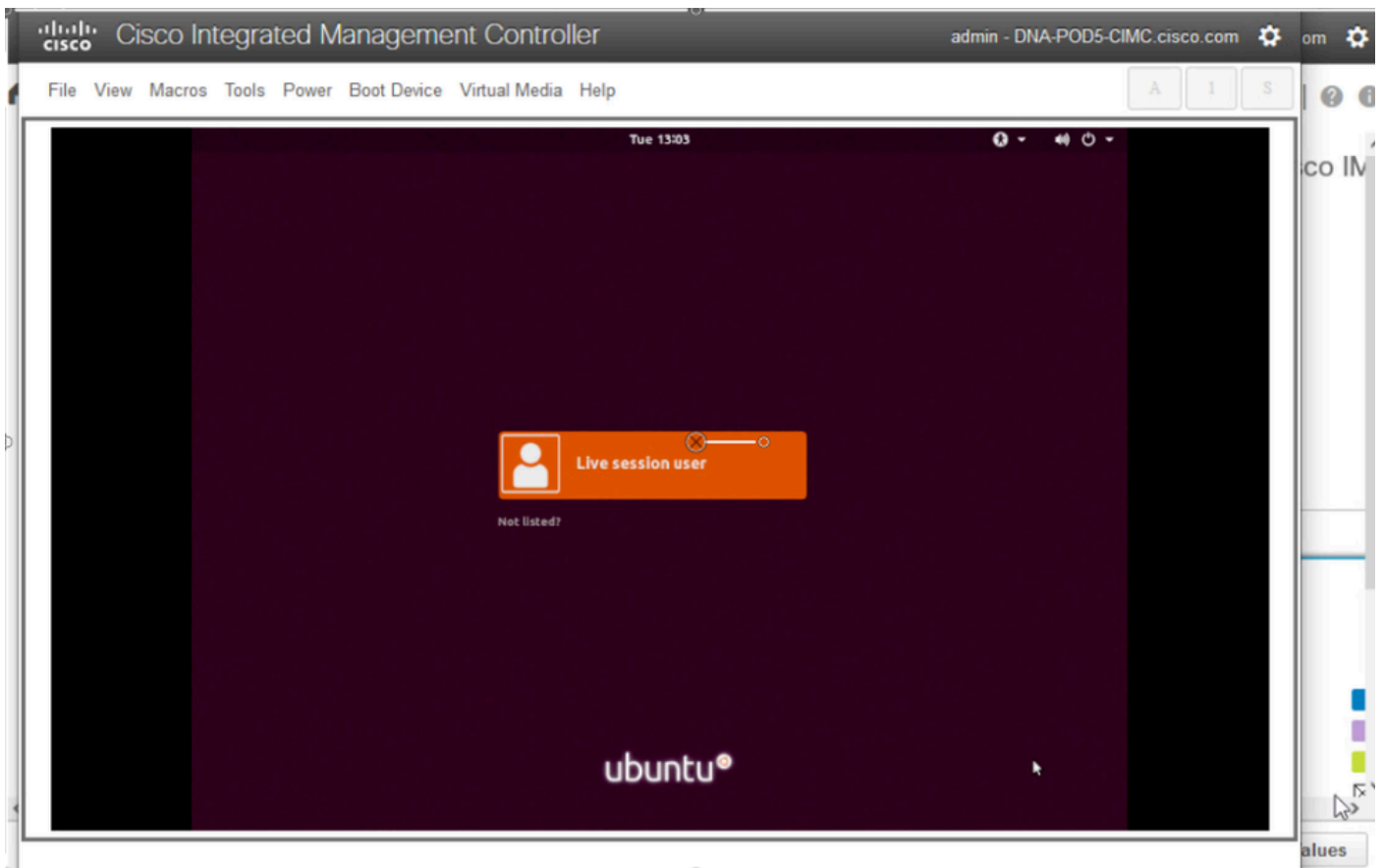


The screen returned to a black screen for about 3 minutes, the above screen flashed again for a few minutes,

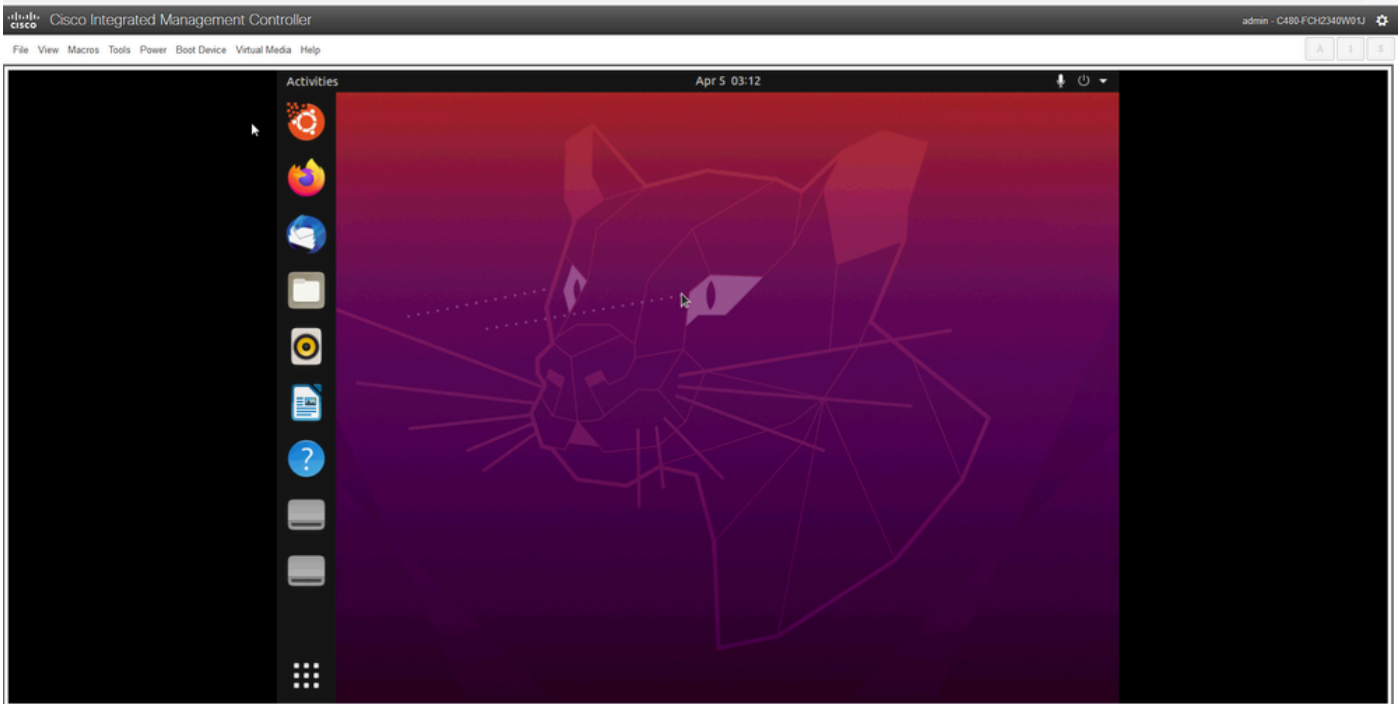
and then returned to the black screen for another two minutes.



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 select this user to continue.



Once we select the user, the screen goes black again before we're presented 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

```
ubuntu@ubuntu: ~
File Edit View Search Terminal Help

ubuntu@ubuntu:~$ sudo mkdir /altsys
ubuntu@ubuntu:~$ lsblk -fm
NAME FSTYPE LABEL UUID                                MOUNTPOINT  SIZE OWNER  GROUP  MODE
loop0
  squash
sda
  sda1
  sda2
  sda3 ext4 install1
    186ab795-aaa0-4364-aafc-d581fe0c76f2
  sda4 vfat FAC1-6A0C
  sdb1 ext4 data
    933db1a2-b943-4b98-9221-765a4028b7bf
  sdb2 ext4
    b252b853-9a4e-486e-99bf-8c62d482592f
  sdb3 ext4
    05cd12d3-df05-4e0a-ae05-f25103be7788
  sdb4 ext4
    e38af843-8ec9-45b1-9c54-e54f91e60cae
sdc
  sdc1 ext4
    b50f383f-a665-4a7c-8b4f-1d85f87dbb94
sdd
  sdd1 exfat
    9C33-688D
    /media/ubu 59.5G root  disk  brw-rw----
sr0 iso966 Ubuntu 18.04.6 LTS amd64
    2021-09-15-20-41-59-00
    /cdrom 2.3G root  cdrom brw-rw----
sr1
    1024M root  cdrom brw-rw----
sr2
    1024M root  cdrom brw-rw----
sr3
    1024M root  cdrom brw-rw----
ubuntu@ubuntu:~$
```

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

```
ubuntu@ubuntu: ~  
File Edit View Search Terminal Help  
ubuntu@ubuntu:~$ sudo mkdir /altsys  
ubuntu@ubuntu:~$ lsblk -fm  
NAME FSTYPE LABEL UUID MOUNTPOINT SIZE OWNER GROUP MODE  
loop0  
  squash /rofs 2.2G root disk brw-rw----  
sda  
├─sda1 446.1G root disk brw-rw----  
│ 1M root disk brw-rw----  
├─sda2 47.7G root disk brw-rw----  
│ ext4 install1 186ab795-aaa0-4364-aafc-d581fe0c76f2  
├─sda3 239M root disk brw-rw----  
│ vfat FAC1-6A0C  
├─sda4 398.2G root disk brw-rw----  
│ ext4 data 933db1a2-b943-4b98-9221-765a4028b7bf  
sdb 1.8T root disk brw-rw----  
├─sdb1 681.8G root disk brw-rw----  
│ ext4 b252b853-9a4e-486e-99bf-8c62d482592f  
├─sdb2 937.4G root disk brw-rw----  
│ ext4 05cd12d3-df05-4e0a-ae05-f25103be7788  
├─sdb3 168G root disk brw-rw----  
│ ext4 e38af843-8ec9-45b1-9c54-e54f91e60cae  
sdc 5.2T root disk brw-rw----  
├─sdc1 5.2T root disk brw-rw----  
│ ext4 b50f383f-a665-4a7c-8b4f-1d85f87dbb94  
sdd 59.5G root disk brw-rw----  
├─sdd1 59.5G root disk brw-rw----  
│ exfat 9C33-68BD /media/ubu  
sr0 iso966 Ubuntu 18.04.6 LTS amd64 /cdrom 2.3G root cdrom brw-rw----  
  2021-09-15-20-41-59-00  
sr1 1024M root cdrom brw-rw----  
sr2 1024M root cdrom brw-rw----  
sr3 1024M root cdrom brw-rw----  
ubuntu@ubuntu:~$
```

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

```
ubuntu@ubuntu: ~
File Edit View Search Terminal Help

ubuntu@ubuntu:~$ sudo mkdir /altsys
ubuntu@ubuntu:~$ lsblk -fm
NAME FSTYPE LABEL UUID                                MOUNTPOINT  SIZE OWNER  GROUP  MODE
loop0
  squash
sda
  sda1
  sda2
    ext4  install1
      186ab795-aaa0-4364-aafc-d581fe0c76f2  47.7G root  disk  brw-rw----
  sda3
    vfat  FAC1-6A0C  239M root  disk  brw-rw----
  sda4
    ext4  data  933db1a2-b943-4b98-9221-765a4028b7bf  398.2G root  disk  brw-rw----
sdb
  sdb1
    ext4
  sdb2
    ext4
  sdb3
    ext4
sdc
  sdc1
    ext4
sdd
  sdd1
    exfat
sr0  iso966 Ubuntu 18.04.6 LTS amd64
    2021-09-15-20-41-59-00  /cdrom  2.3G root  cdrom  brw-rw----
sr1
sr2
sr3
```

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$6jvRGoDihpcsr8X1$RUFs.Lb.2Abbgv0DfJsw4b2EnpSwiNU1wJ6NQIjEnv0tT5Svz4ePHZa4f0eUvLH17VAFca46f2nHxqMWORY
```

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

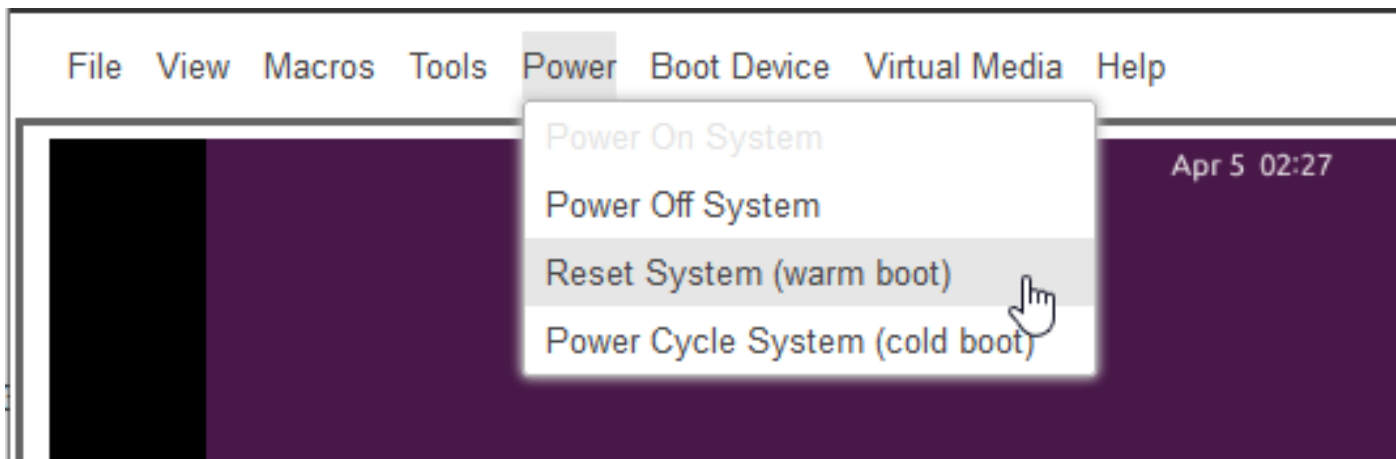
Retype new UNIX password: #Re-enter the same password previously applied

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

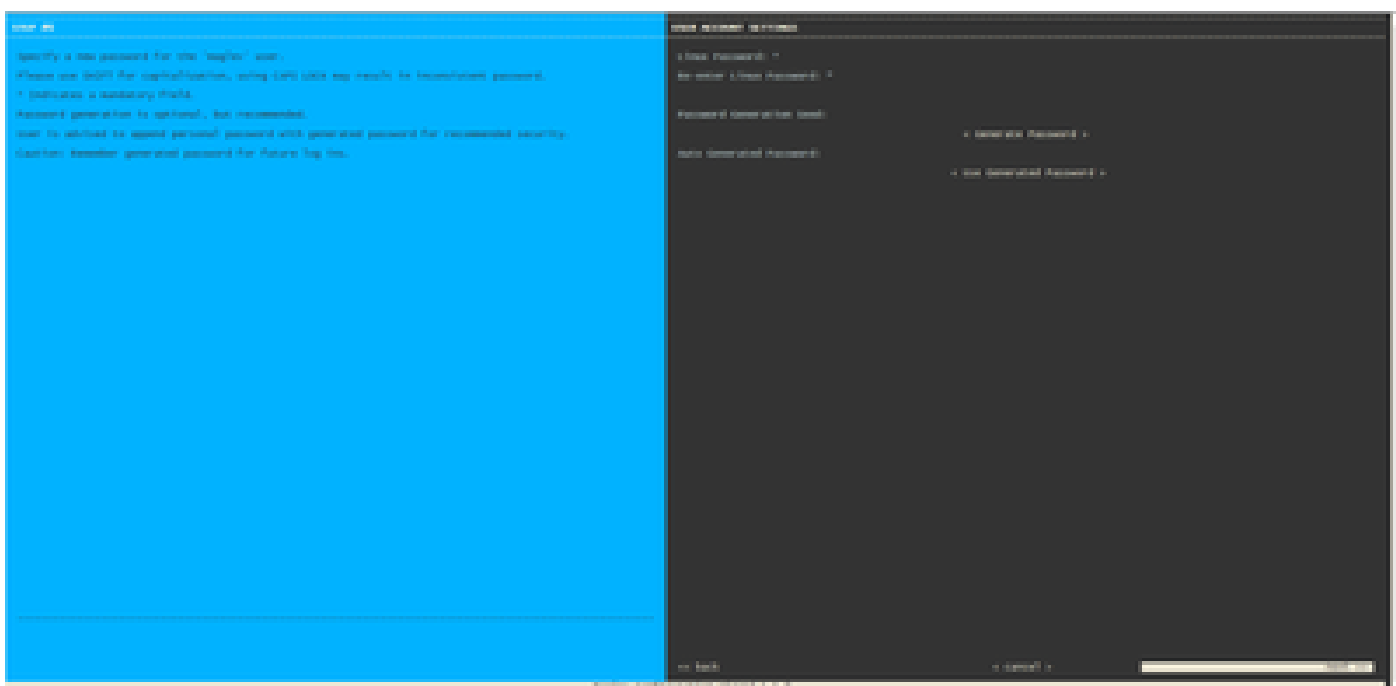
Click on **Power** in the KVM window and then **Reset System (warm boot)**. This causes the system to reboot and boot with the RAID controller so that the Cisco DNA Center software boots up.



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.