UCS Director Baremetal Agent Installation

The purpose to this document is to illustrate the steps to install the UCS Director Baremetal Agent (PXE Server) which can be used to write/use workflows that require a PXE Server such as the 'BMA + UCSM + MDS + NetApp Example' workflow located on the UCS Directors Communities site. This example workflow can be found at the following link: https://communities.cisco.com/docs/DOC-52546

Before you implement the Baremetal Agent, make sure your UCS Director is fully installed, functional and upgraded to 5.3. If this isn't the case, then you should upgrade before implementing the BMA and integrating with UCS Director. You cannot go directly to 5.3 so you must first install BMA 5.2 then upgrade to 5.3.

Useful Documents:

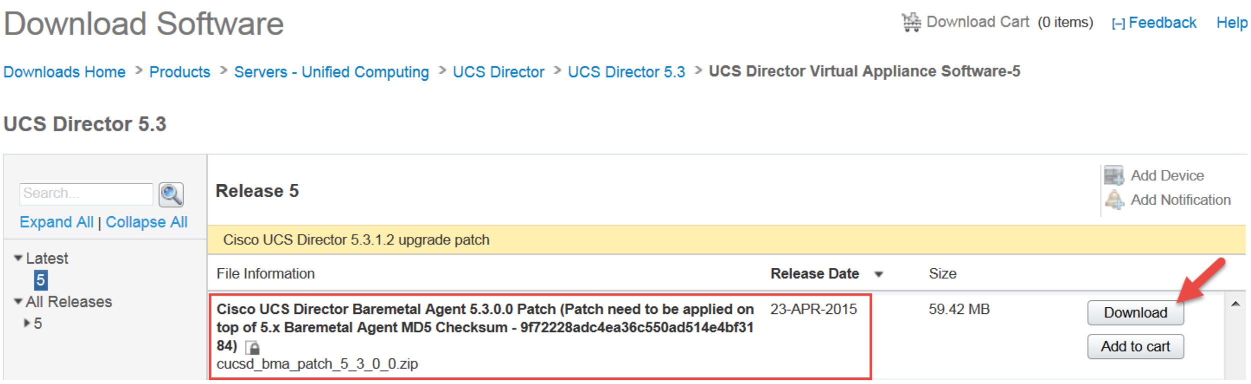
Cisco UCS Director Baremetal Agent Installation and Configuration Guide, Release 5.2

Cisco UCS Director Baremetal Agent Installation and Configuration Guide, Release 5.3

Table of Contents

1. Download Baremetal Agent 5.2 and Patch 5.3.0.0

Go to Cisco.com Downloads and navigate to UCS Director 5.3. Download the Cisco UCS Director Baremetal Agent Patch 5.3.0.0.



Download Software

Downloads Home > Products > Servers - Unified Computing > UCS Director > UCS Director 5.3 > UCS Director Virtual Appliance Software-5

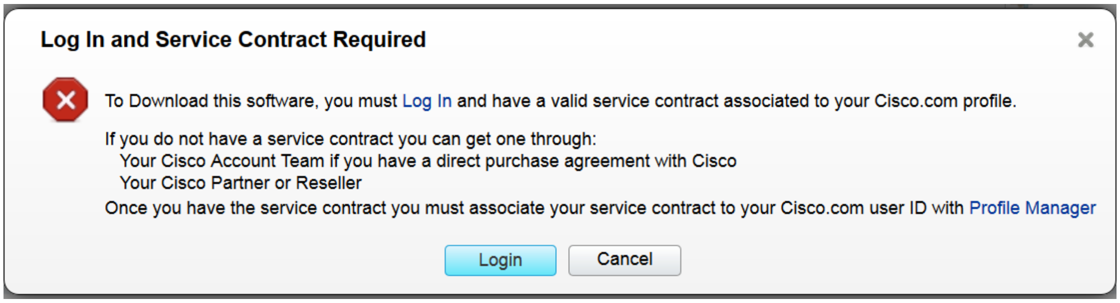
UCS Director 5.3

Release 5

Cisco UCS Director 5.3.1.2 upgrade patch

File Information	Release Date	Size
Cisco UCS Director Baremetal Agent 5.3.0.0 Patch (Patch need to be applied on top of 5.x Baremetal Agent MD5 Checksum - 9f72228adc4ea36c550ad514e4bf3184) cucsd_bma_patch_5_3_0_0.zip	23-APR-2015	59.42 MB

Login using your CCO account.



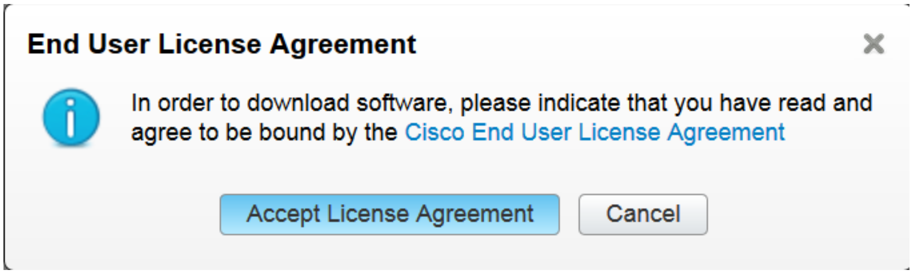
Log In and Service Contract Required

To Download this software, you must Log In and have a valid service contract associated to your Cisco.com profile.

If you do not have a service contract you can get one through:
Your Cisco Account Team if you have a direct purchase agreement with Cisco
Your Cisco Partner or Reseller

Once you have the service contract you must associate your service contract to your Cisco.com user ID with Profile Manager

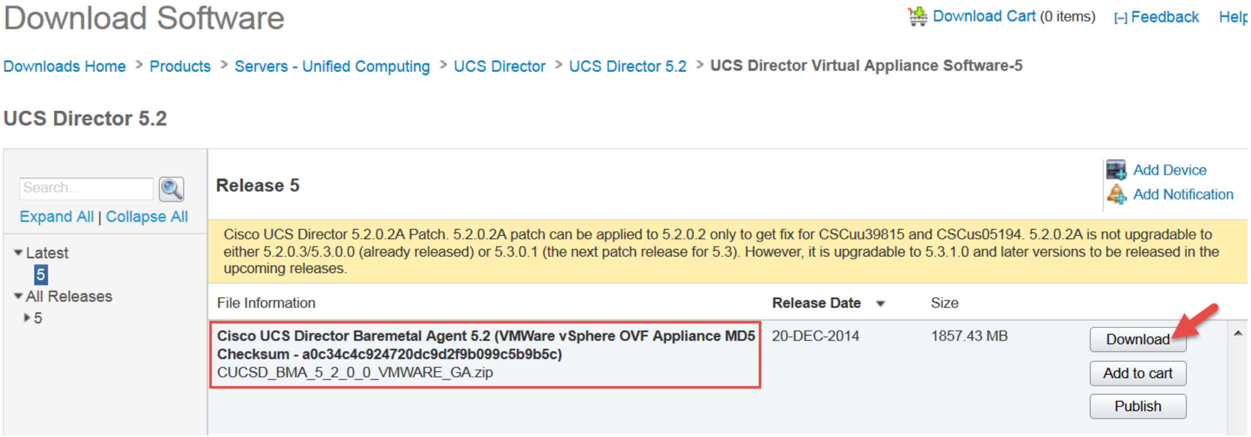
Accept the license agreement.



End User License Agreement

In order to download software, please indicate that you have read and agree to be bound by the Cisco End User License Agreement

Now, go back to the main UCS Director download page and select UCS Director 5.2. Download the Cisco UCS Director Baremetal Agent 5.2.



Download Software

Downloads Home > Products > Servers - Unified Computing > UCS Director > UCS Director 5.2 > UCS Director Virtual Appliance Software-5

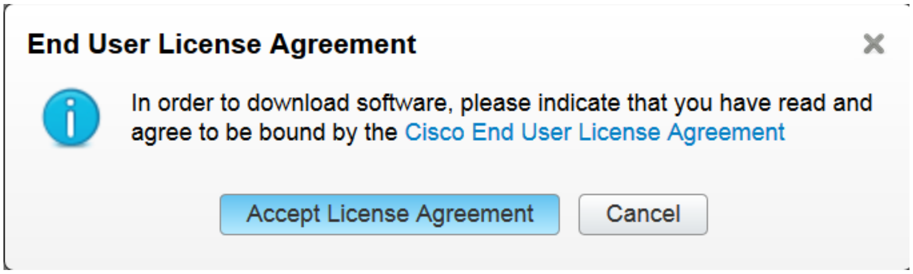
UCS Director 5.2

Release 5

Cisco UCS Director 5.2.0.2A Patch. 5.2.0.2A patch can be applied to 5.2.0.2 only to get fix for CSCuu39815 and CSCus05194. 5.2.0.2A is not upgradable to either 5.2.0.3/5.3.0.0 (already released) or 5.3.0.1 (the next patch release for 5.3). However, it is upgradable to 5.3.1.0 and later versions to be released in the upcoming releases.

File Information	Release Date	Size
Cisco UCS Director Baremetal Agent 5.2 (VMWare vSphere OVF Appliance MD5 Checksum - a0c34c4c924720dc9d2f9b099c5b9b5c) CUCSD_BMA_5_2_0_0_VMWARE_GA.zip	20-DEC-2014	1857.43 MB

Accept the license agreement.

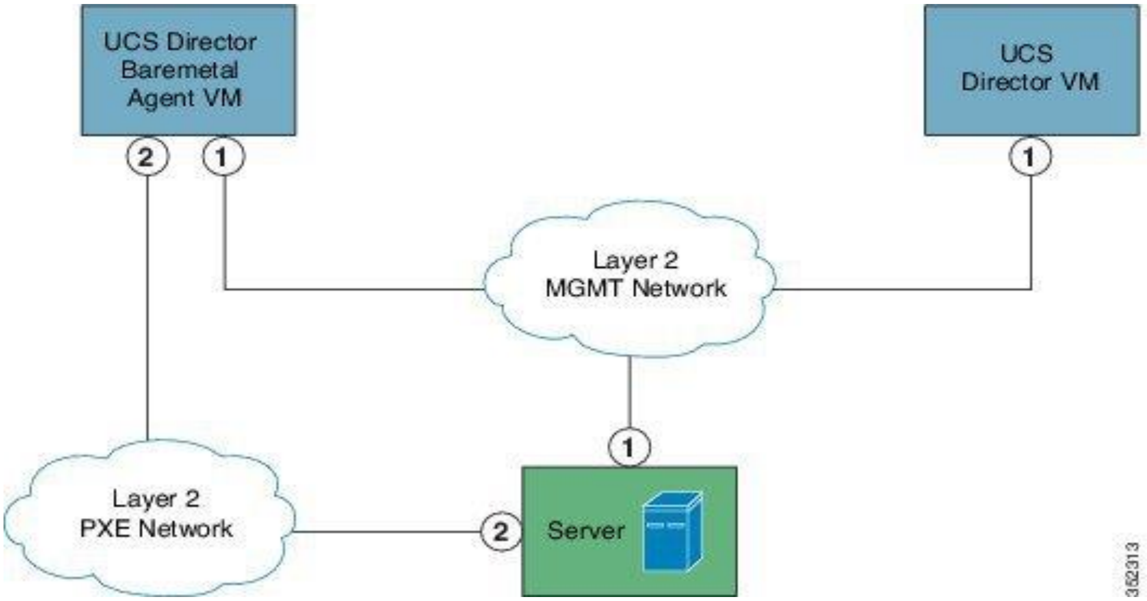


End User License Agreement

In order to download software, please indicate that you have read and agree to be bound by the Cisco End User License Agreement

2. PXE/Management Network setup

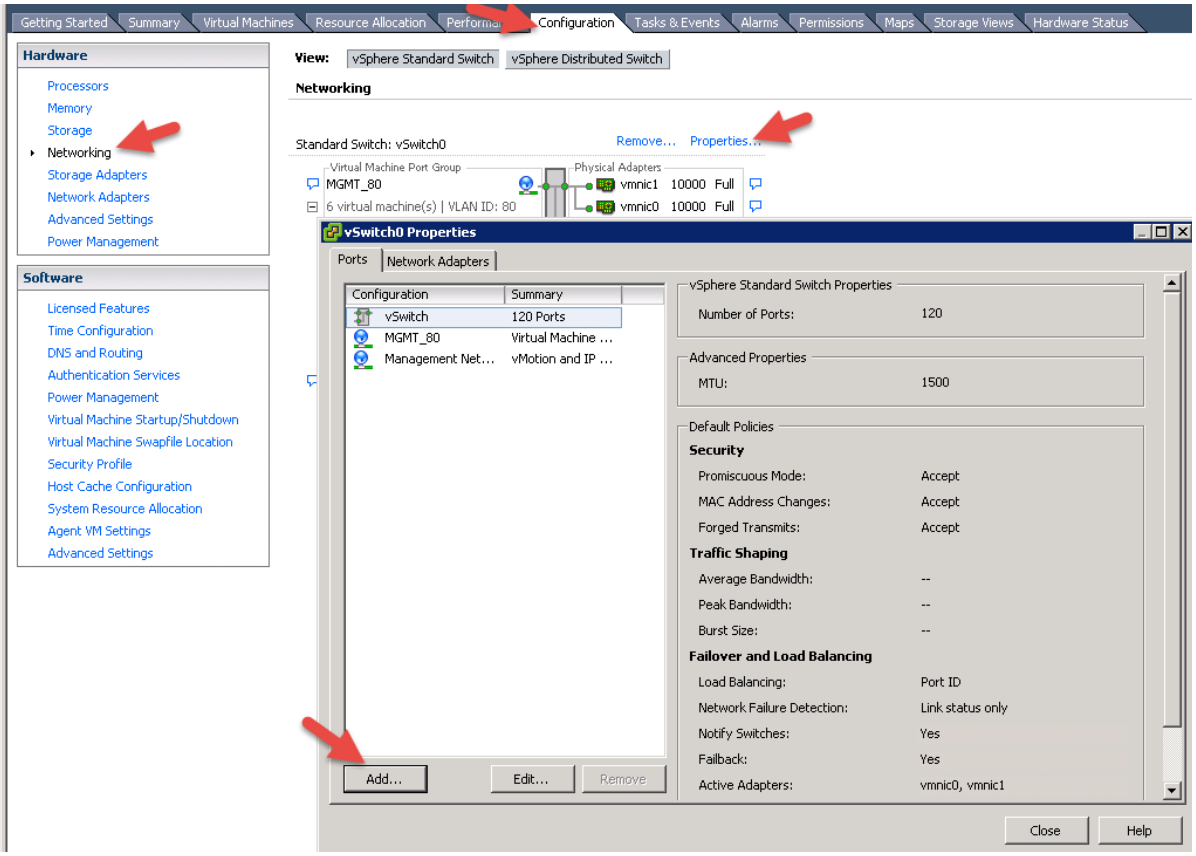
Determine if you want to use a Single or Separate Networks for Management and PXE. I have chosen to use Separate networks for PXE and Management so we need to configure PXE VLAN in vCenter and UCS.



2.1. Create PXE VLAN/Port Group in vCenter

Log into vCenter and create a Port-Group/VLAN for PXE on the host where UCS Director BMA will reside.

Select the ESXi host then do the following.



Standard Switch: vSwitch0

Virtual Machine Port Group
MGMT_80
6 virtual machine(s) | VLAN ID: 80

Physical Adapters
vmnic1 10000 Full
vmnic0 10000 Full

vSwitch0 Properties

Configuration	Summary
vSwitch	120 Ports
MGMT_80	Virtual Machine ...
Management Net...	vMotion and IP ...

vSphere Standard Switch Properties

Number of Ports: 120

Advanced Properties

MTU: 1500

Default Policies

Security

Promiscuous Mode: Accept

MAC Address Changes: Accept

Forged Transmits: Accept

Traffic Shaping

Average Bandwidth: --

Peak Bandwidth: --

Burst Size: --

Failover and Load Balancing

Load Balancing: Port ID

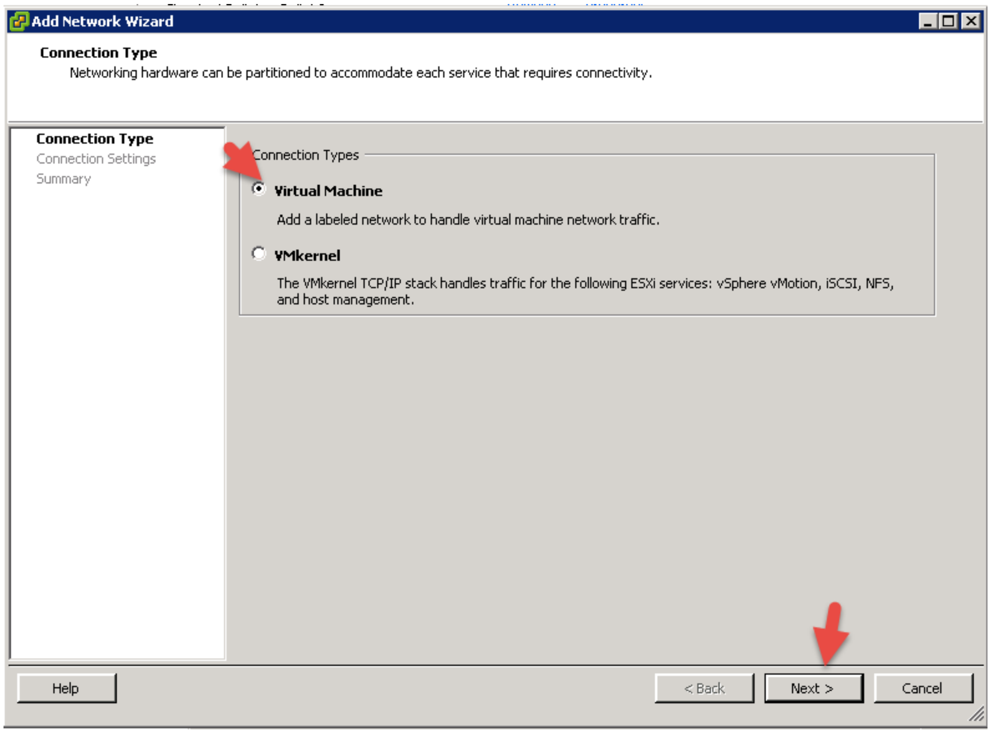
Network Failure Detection: Link status only

Notify Switches: Yes

Failback: Yes

Active Adapters: vmnic0, vmnic1

Select Virtual Machine and click Next.



Connection Type

Networking hardware can be partitioned to accommodate each service that requires connectivity.

Connection Types

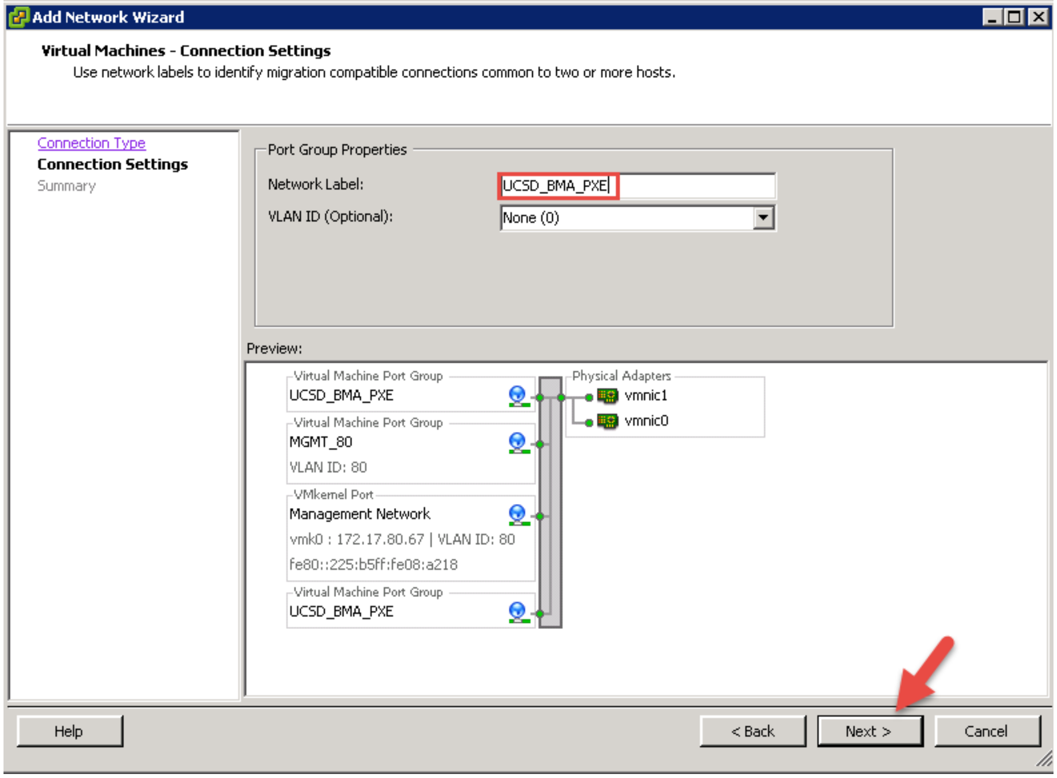
● **Virtual Machine**

Add a labeled network to handle virtual machine network traffic.

○ **VMkernel**

The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iSCSI, NFS, and host management.

Name the Port Group and leave VLAN default and click Next.



Add Network Wizard

Virtual Machines - Connection Settings

Use network labels to identify migration compatible connections common to two or more hosts.

- Connection Type
- **Connection Settings**
- Summary

Port Group Properties

Network Label: UCSD_BMA_PXE

VLAN ID (Optional): None (0)

Preview:

Virtual Machine Port Group
UCSD_BMA_PXE

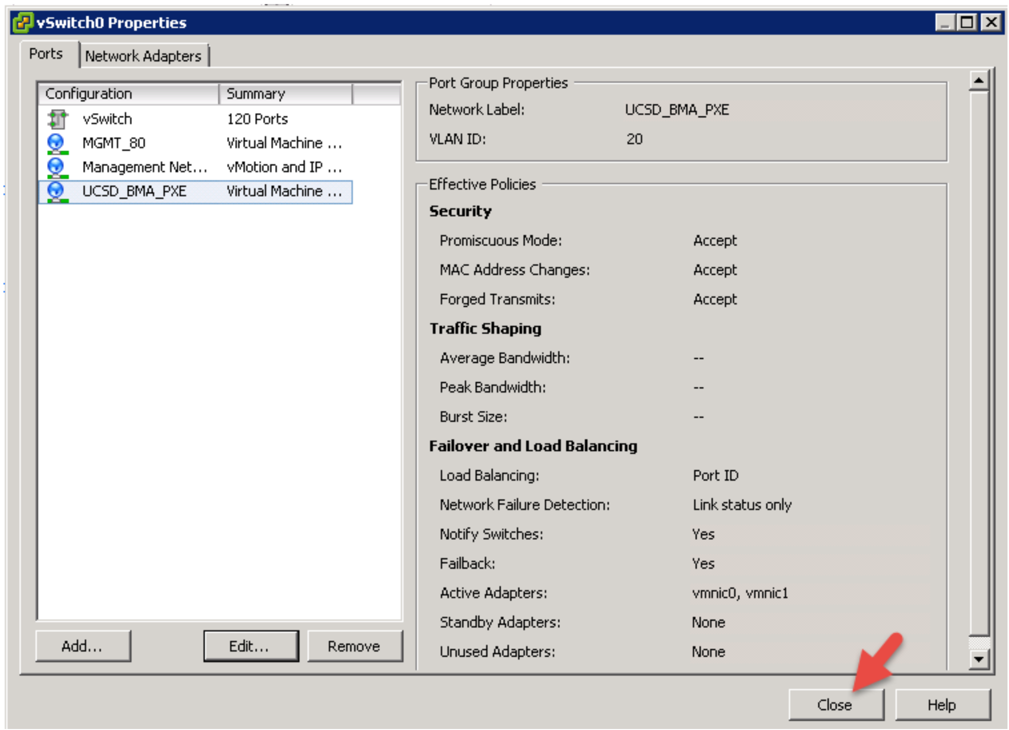
Virtual Machine Port Group
MGMT_80
VLAN ID: 80

VMkernel Port
Management Network
vmk0 : 172.17.80.67 | VLAN ID: 80
fe80::225:b5ff:fe08:a218

Virtual Machine Port Group
UCSD_BMA_PXE

Physical Adapters
vmnic1
vmnic0

Finally Click Close.



vSwitch0 Properties

Configuration	Summary
vSwitch	120 Ports
MGMT_80	Virtual Machine ...
Management Net...	vMotion and IP ...
UCSD_BMA_PXE	Virtual Machine ...

Port Group Properties

Network Label: UCSD_BMA_PXE

VLAN ID: 20

Effective Policies

Security

Promiscuous Mode:	Accept
MAC Address Changes:	Accept
Forged Transmits:	Accept

Traffic Shaping

Average Bandwidth:	--
Peak Bandwidth:	--
Burst Size:	--

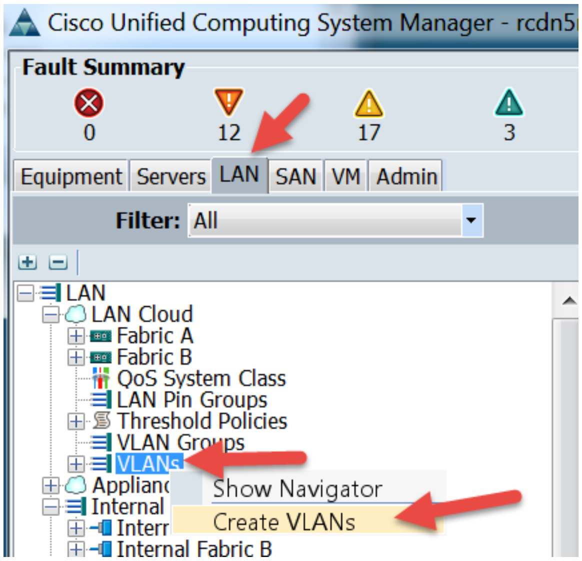
Failover and Load Balancing

Load Balancing:	Port ID
Network Failure Detection:	Link status only
Notify Switches:	Yes
Failback:	Yes
Active Adapters:	vmnic0, vmnic1
Standby Adapters:	None
Unused Adapters:	None

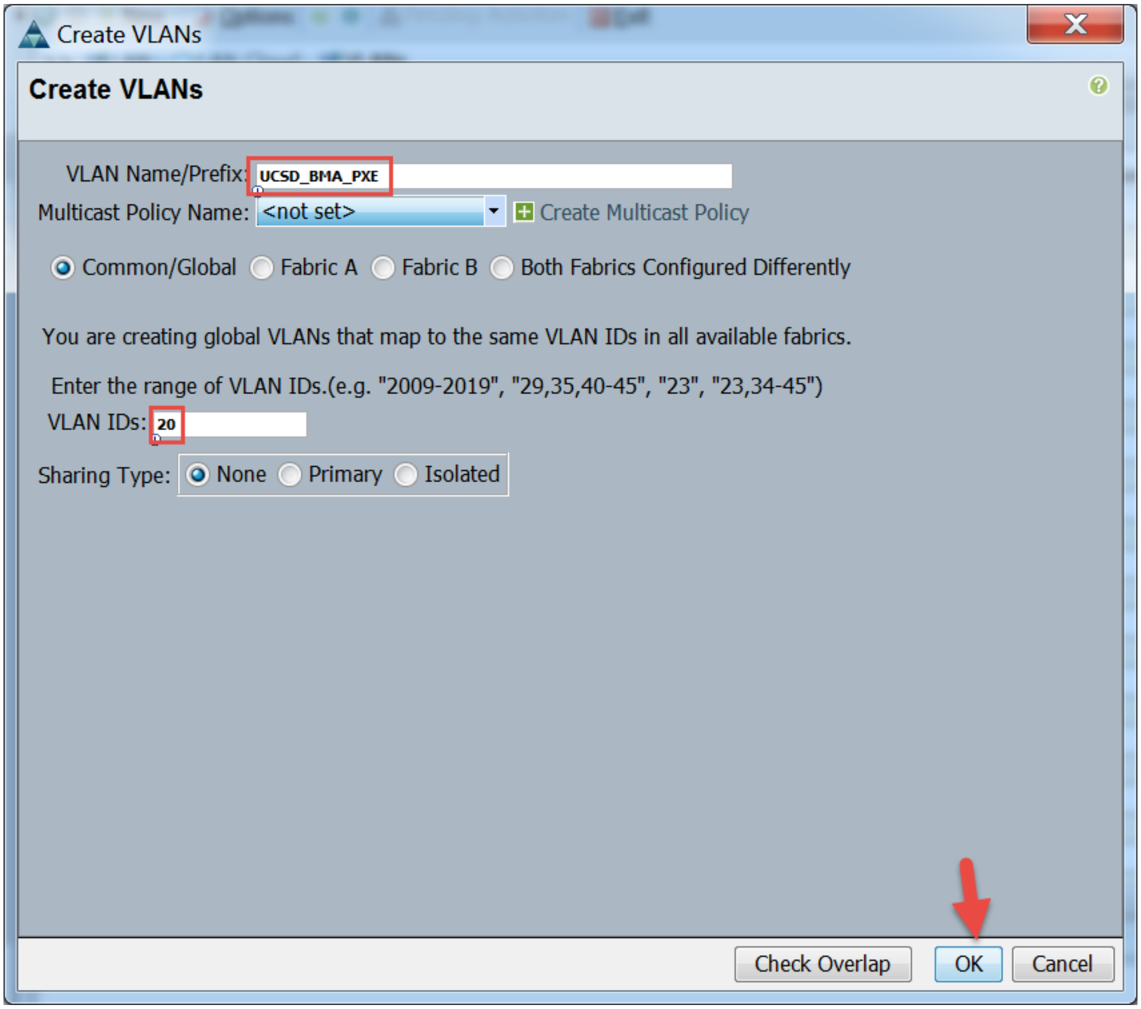
2.2. Create PXE VLAN in UCS Manager

Log into UCS Manager and Create the PXE VLAN.

Navigate as shown below and select Create VLAN.



Define the VLAN as follows.



Create VLANs

VLAN Name/Prefix: UCSD_BMA_PXE

Multicast Policy Name: <not set>

● Common/Global ○ Fabric A ○ Fabric B ○ Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.

Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

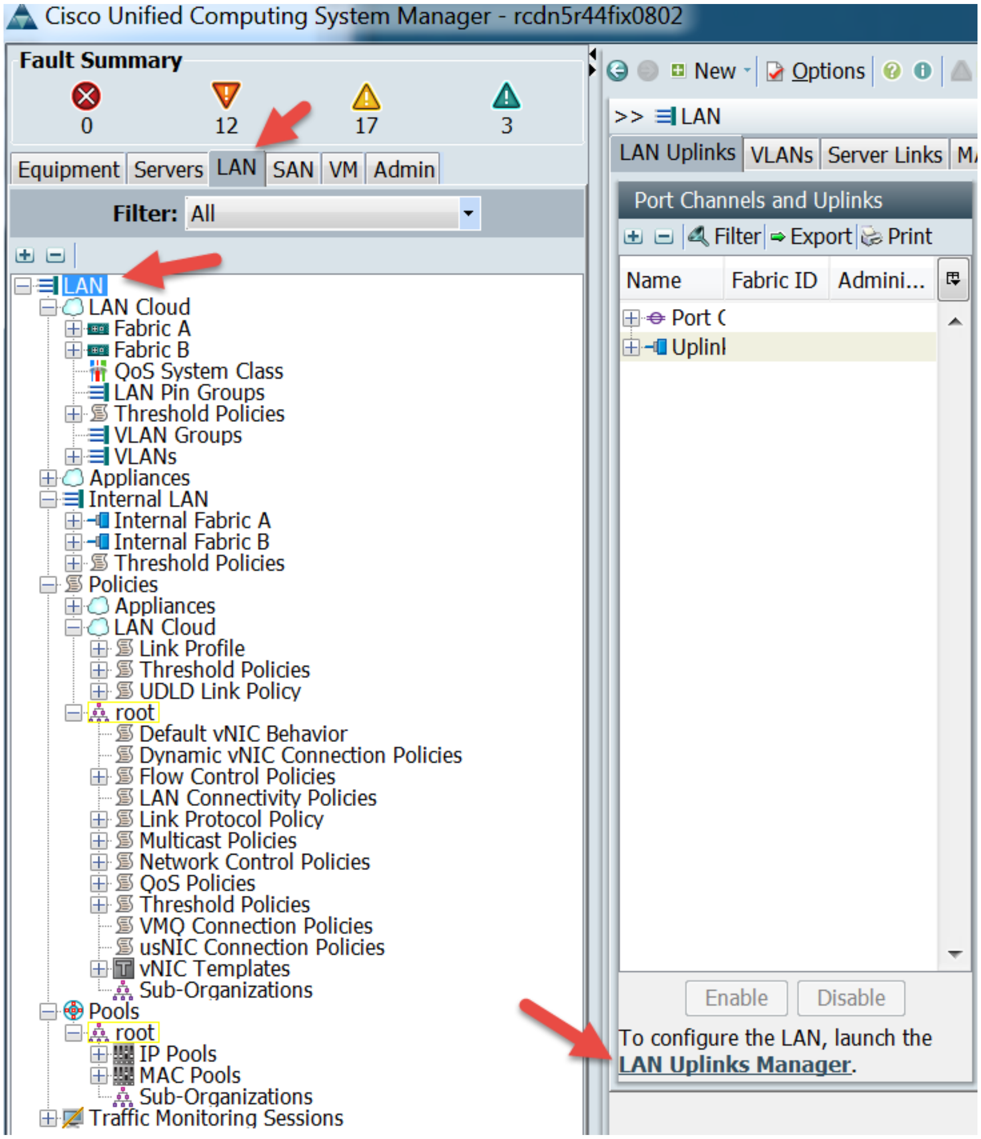
VLAN IDs: 20

Sharing Type: ● None ○ Primary ○ Isolated

2.3. Disjoint Layer-2 configuration PXE VLAN UCS Manager

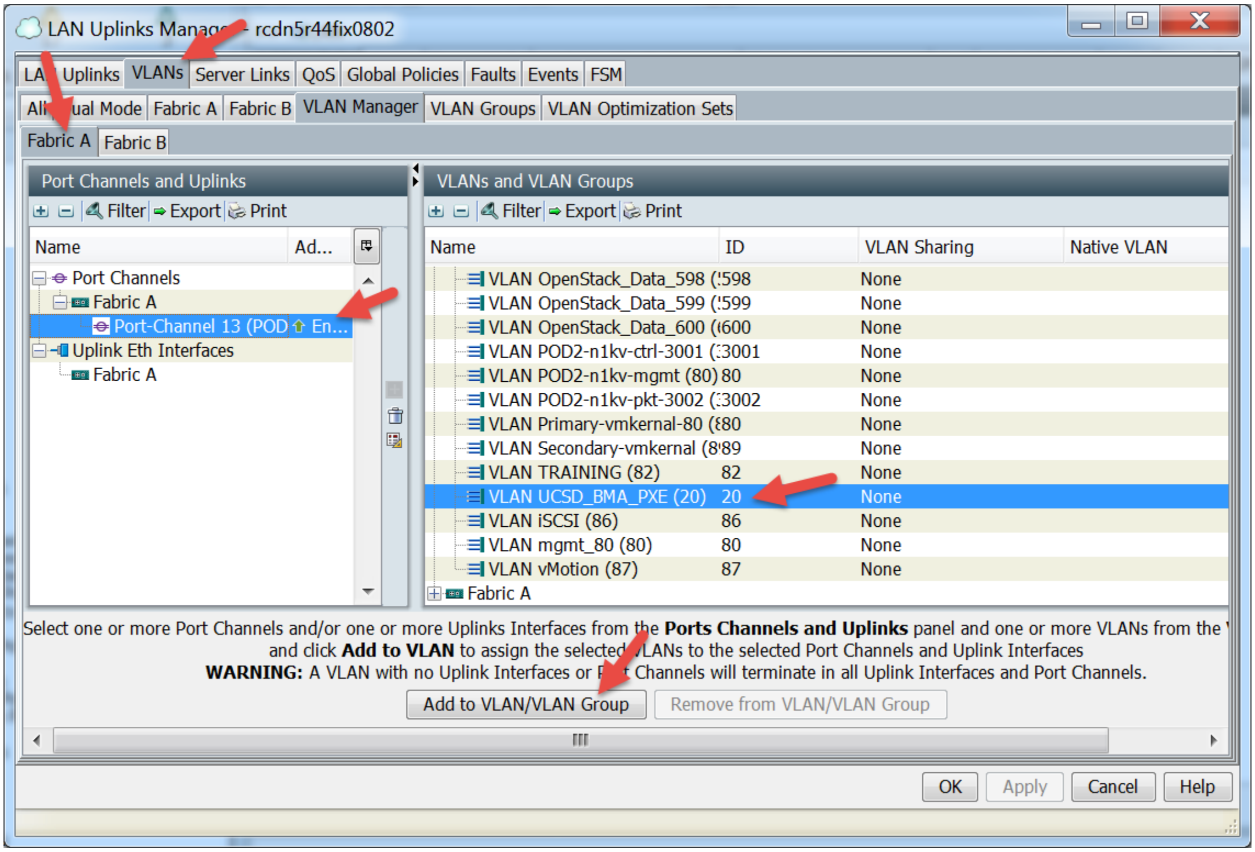
If you have Disjoint Layer 2 connectivity, ensure the PXE VLAN is only allowed on the correct uplinks.

Launch ‘LAN Uplinks Manager’



To configure the LAN, launch the **LAN Uplinks Manager**.

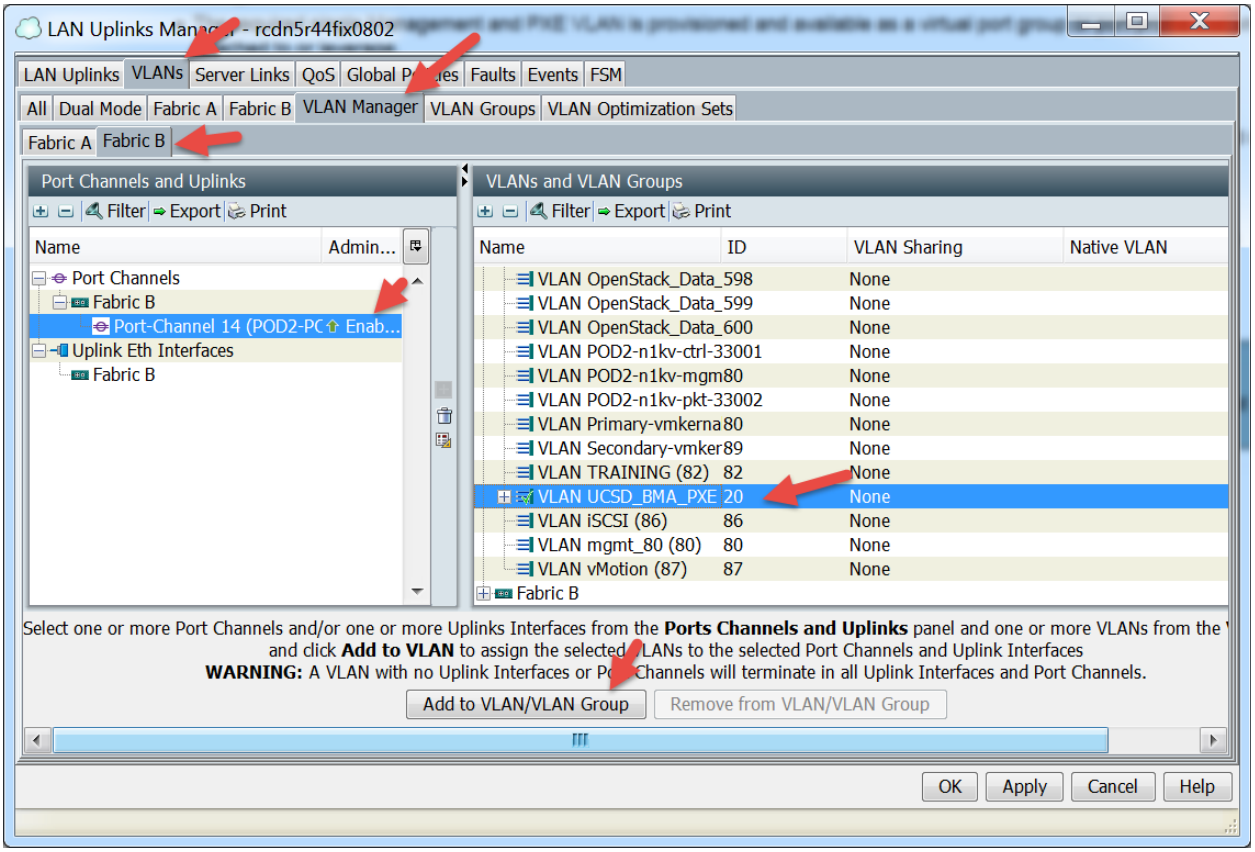
Add PXE VLAN to Fabric A Uplink Port-Channel.


LAN Uplinks Manager - rcdn5r44fix0802
LAN Uplinks | VLANs | Server Links | QoS | Global Policies | Faults | Events | FSM
All | Dual Mode | Fabric A | Fabric B | VLAN Manager | VLAN Groups | VLAN Optimization Sets
Fabric A | Fabric B
Port Channels and Uplinks
Filter | Export | Print
Name | Ad...
Port Channels
Fabric A
Port-Channel 13 (POD En...
Uplink Eth Interfaces
Fabric A
VLANs and VLAN Groups
Filter | Export | Print
Add to VLAN/VLAN Group
Remove from VLAN/VLAN Group
OK
Apply
Cancel
Help

Name	ID	VLAN Sharing	Native VLAN
VLAN OpenStack_Data_598 (598	598	None	
VLAN OpenStack_Data_599 (599	599	None	
VLAN OpenStack_Data_600 (600	600	None	
VLAN POD2-n1kv-ctrl-3001 (3001	3001	None	
VLAN POD2-n1kv-mgmt (80)	80	None	
VLAN POD2-n1kv-pkt-3002 (3002	3002	None	
VLAN Primary-vmkernal-80 (80	80	None	
VLAN Secondary-vmkernal (89	89	None	
VLAN TRAINING (82)	82	None	
VLAN UCSD_BMA_PXE (20)	20	None	
VLAN iSCSI (86)	86	None	
VLAN mgmt_80 (80)	80	None	
VLAN vMotion (87)	87	None	
Fabric A			

Select one or more Port Channels and/or one or more Uplinks Interfaces from the **Ports Channels and Uplinks** panel and one or more VLANs from the
and click **Add to VLAN** to assign the selected VLANs to the selected Port Channels and Uplink Interfaces
WARNING: A VLAN with no Uplink Interfaces or Port Channels will terminate in all Uplink Interfaces and Port Channels.

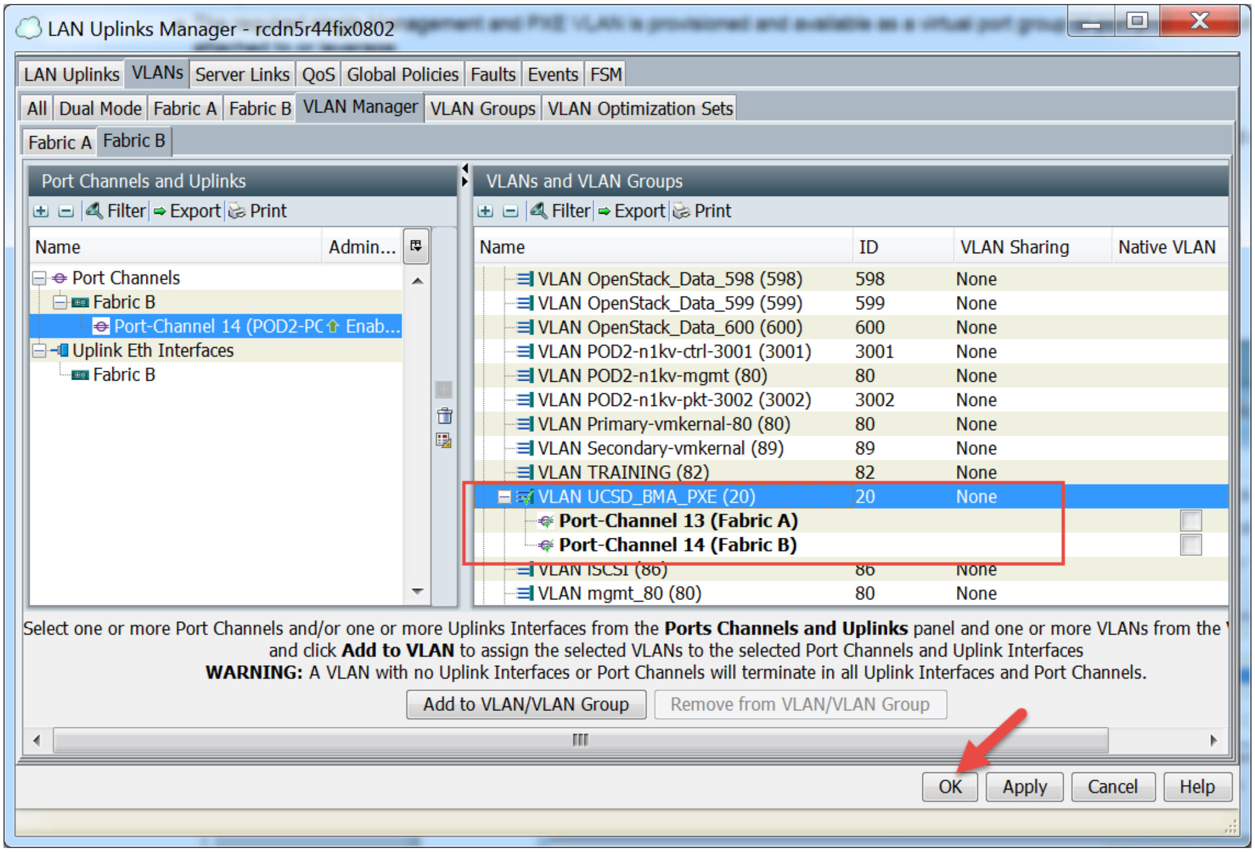
Add PXE VLAN to Fabric B Uplink Port-Channel.


LAN Uplinks Manager - rcdn5r44fix0802
LAN Uplinks | VLANs | Server Links | QoS | Global Policies | Faults | Events | FSM
All | Dual Mode | Fabric A | Fabric B | VLAN Manager | VLAN Groups | VLAN Optimization Sets
Fabric A | Fabric B
Port Channels and Uplinks
Filter | Export | Print
Name | Admin...
Port Channels
Fabric B
Port-Channel 14 (POD2-PC Enab...
Uplink Eth Interfaces
Fabric B
VLANs and VLAN Groups
Filter | Export | Print
Add to VLAN/VLAN Group
Remove from VLAN/VLAN Group
OK
Apply
Cancel
Help

Name	ID	VLAN Sharing	Native VLAN
VLAN OpenStack_Data_598		None	
VLAN OpenStack_Data_599		None	
VLAN OpenStack_Data_600		None	
VLAN POD2-n1kv-ctrl-3	3001	None	
VLAN POD2-n1kv-mgm	80	None	
VLAN POD2-n1kv-pkt-3	3002	None	
VLAN Primary-vmkerna	80	None	
VLAN Secondary-vmker	89	None	
VLAN TRAINING (82)	82	None	
VLAN UCSD_BMA_PXE	20	None	
VLAN iSCSI (86)	86	None	
VLAN mgmt_80 (80)	80	None	
VLAN vMotion (87)	87	None	
Fabric B			

Select one or more Port Channels and/or one or more Uplinks Interfaces from the **Ports Channels and Uplinks** panel and one or more VLANs from the
and click **Add to VLAN** to assign the selected VLANs to the selected Port Channels and Uplink Interfaces
WARNING: A VLAN with no Uplink Interfaces or Port Channels will terminate in all Uplink Interfaces and Port Channels.

Finally Click OK to apply configuration.


LAN Uplinks Manager - rcdn5r44fix0802
LAN Uplinks | VLANs | Server Links | QoS | Global Policies | Faults | Events | FSM
All | Dual Mode | Fabric A | Fabric B | VLAN Manager | VLAN Groups | VLAN Optimization Sets
Fabric A | Fabric B
Port Channels and Uplinks
Filter | Export | Print
VLANs and VLAN Groups
Filter | Export | Print

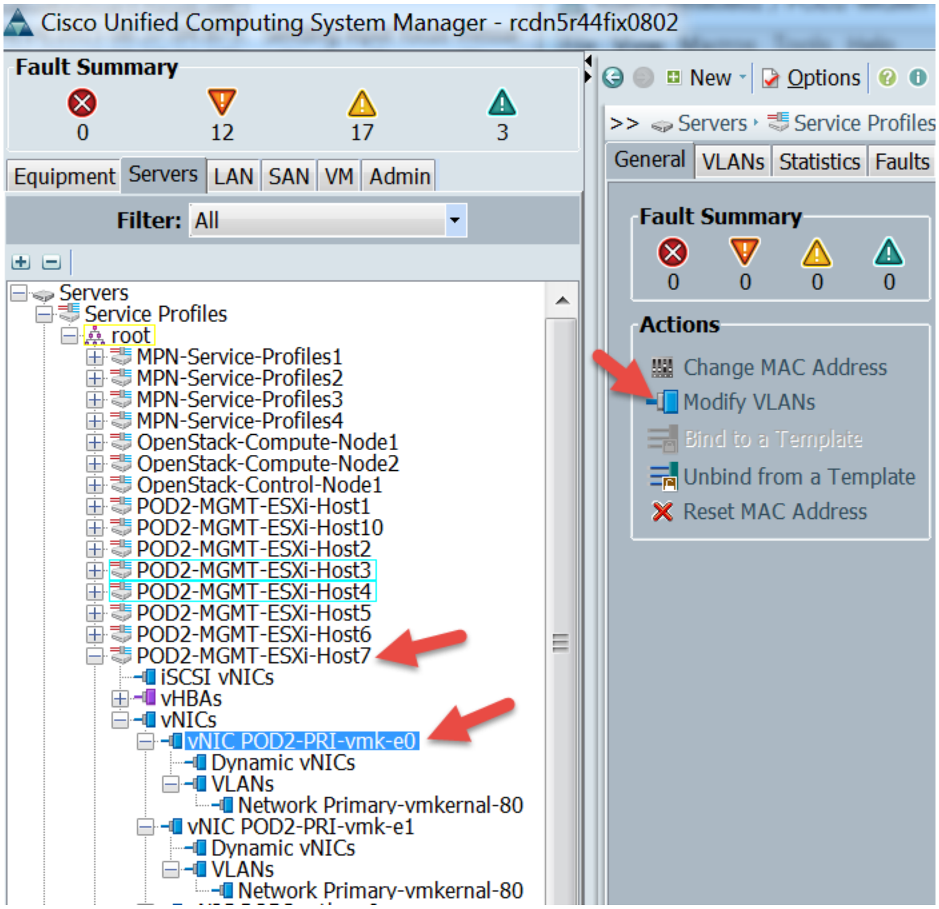
Name	Admin...
Port Channels	
Fabric B	
Port-Channel 14 (POD2-PC	Enab...
Uplink Eth Interfaces	
Fabric B	

Name	ID	VLAN Sharing	Native VLAN
VLAN OpenStack_Data_598 (598)	598	None	
VLAN OpenStack_Data_599 (599)	599	None	
VLAN OpenStack_Data_600 (600)	600	None	
VLAN POD2-n1kv-ctrl-3001 (3001)	3001	None	
VLAN POD2-n1kv-mgmt (80)	80	None	
VLAN POD2-n1kv-pkt-3002 (3002)	3002	None	
VLAN Primary-vmkernal-80 (80)	80	None	
VLAN Secondary-vmkernal (89)	89	None	
VLAN TRAINING (82)	82	None	
VLAN UCSD_BMA_PXE (20)	20	None	
Port-Channel 13 (Fabric A)			□
Port-Channel 14 (Fabric B)			□
VLAN ISCSI (86)	86	None	
VLAN mgmt_80 (80)	80	None	

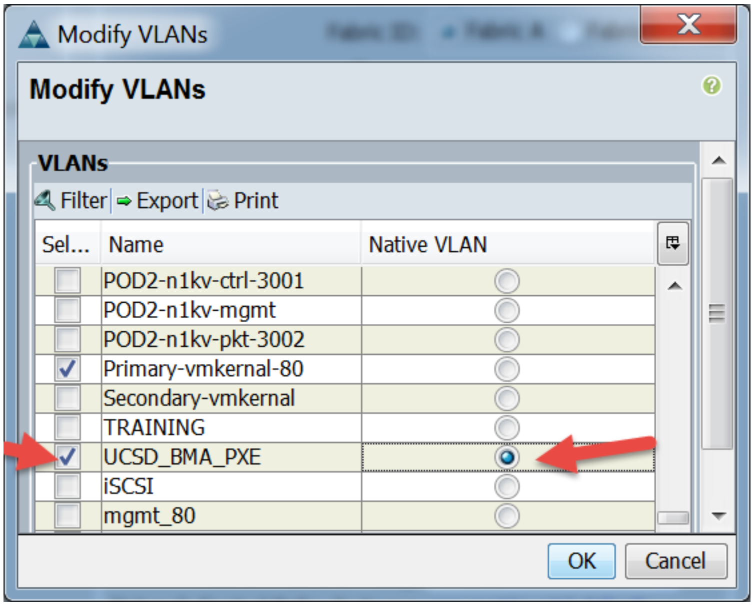
Select one or more Port Channels and/or one or more Uplinks Interfaces from the **Ports Channels and Uplinks** panel and one or more VLANs from the \
and click **Add to VLAN** to assign the selected VLANs to the selected Port Channels and Uplink Interfaces
WARNING: A VLAN with no Uplink Interfaces or Port Channels will terminate in all Uplink Interfaces and Port Channels.

2.4. Add PXE VLAN to Fabric A and Fabric B vNICs

Add the PXE VLAN to the Fabric A VNIC and select Native for this VLAN. This needs to be completed for the Service Profiles that host the BMA Agent. Select Modify VLANs.

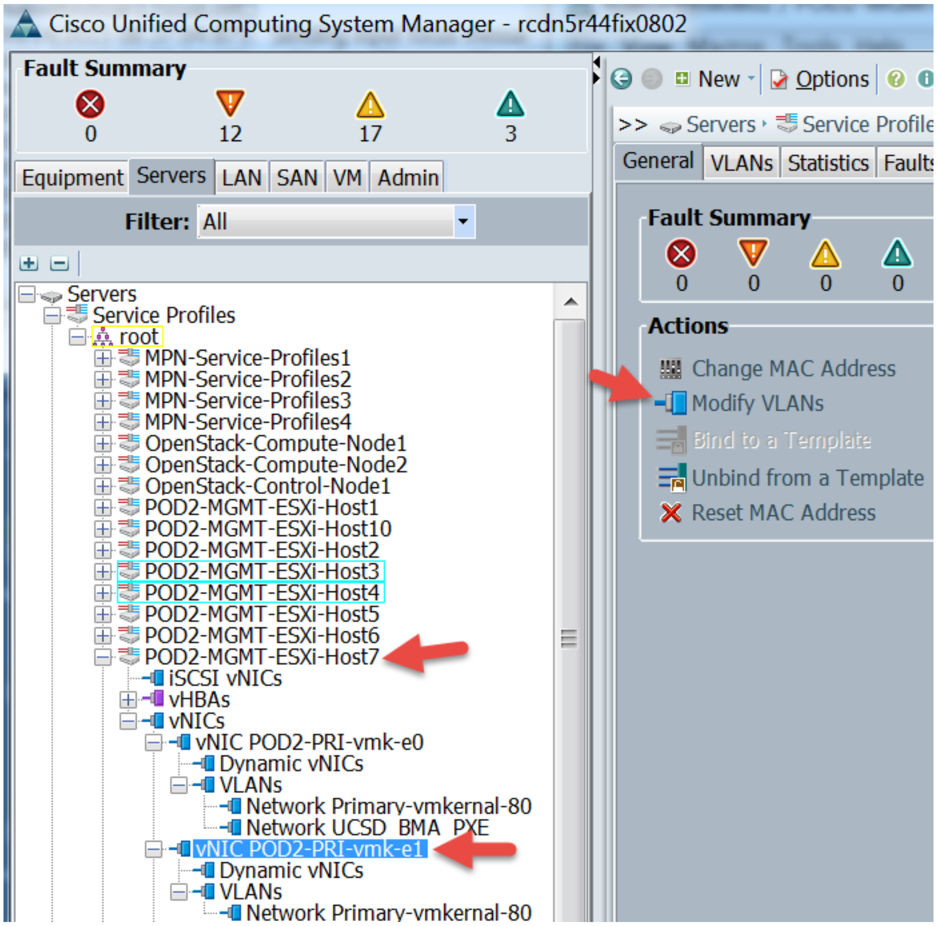


Select the PXE VLAN and Select Native and click OK.

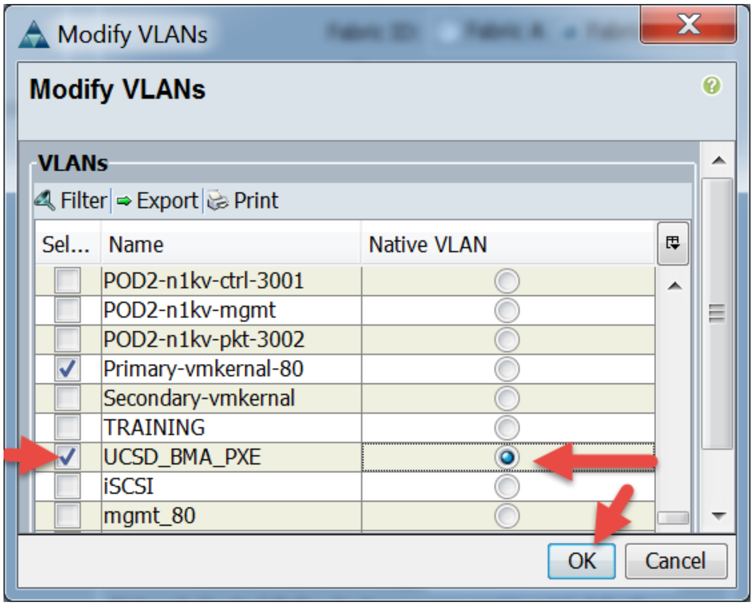


Sel...	Name	Native VLAN
☐	POD2-n1kv-ctrl-3001	○
☐	POD2-n1kv-mgmt	○
☐	POD2-n1kv-pkt-3002	○
☑	Primary-vmkernal-80	○
☐	Secondary-vmkernal	○
☐	TRAINING	○
☑	UCSD_BMA_PXE	●
☐	iSCSI	○
☐	mgmt_80	○

Now complete this for Fabric B.

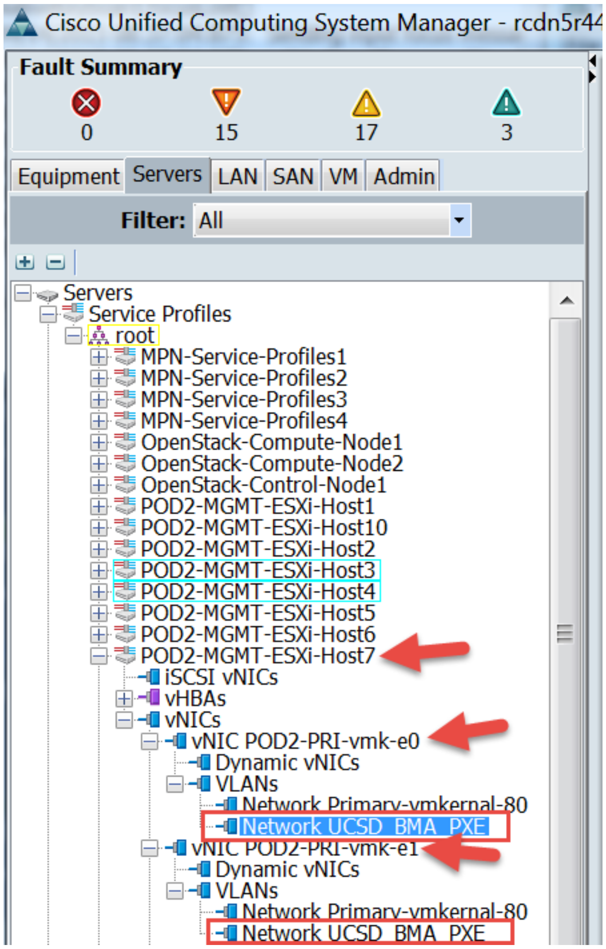


Select the PXE VLAN and Select Native VLAN then Click OK.



Sel...	Name	Native VLAN
□	POD2-n1kv-ctrl-3001	○
□	POD2-n1kv-mgmt	○
□	POD2-n1kv-pkt-3002	○
☑	Primary-vmkernal-80	○
□	Secondary-vmkernal	○
□	TRAINING	○
☑	UCSD_BMA_PXE	●
□	iSCSI	○
□	mgmt_80	○

Verify the PXE VLAN is configured on the service profile.



Cisco Unified Computing System Manager - rcdn5r44

Fault Summary

0	15	17	3

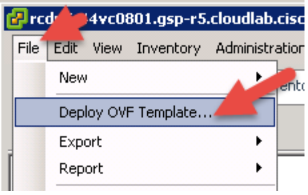
Filter: All

- Servers
  - Service Profiles
    - root
      - MPN-Service-Profiles1
      - MPN-Service-Profiles2
      - MPN-Service-Profiles3
      - MPN-Service-Profiles4
      - OpenStack-Compute-Node1
      - OpenStack-Compute-Node2
      - OpenStack-Control-Node1
      - POD2-MGMT-ESXi-Host1
      - POD2-MGMT-ESXi-Host10
      - POD2-MGMT-ESXi-Host2
      - POD2-MGMT-ESXi-Host3
      - POD2-MGMT-ESXi-Host4
      - POD2-MGMT-ESXi-Host5
      - POD2-MGMT-ESXi-Host6
      - POD2-MGMT-ESXi-Host7
        - iSCSI vNICs
        - vHBAs
        - vNICs
          - vNIC POD2-PRI-vmk-e0
            - Dynamic vNICs
            - VLANs
              - Network Primary-vmkernal-80
              - Network UCSD_BMA_PXE
          - vNIC POD2-PRI-vmk-e1
            - Dynamic vNICs
            - VLANs
              - Network Primary-vmkernal-80
              - Network UCSD_BMA_PXE

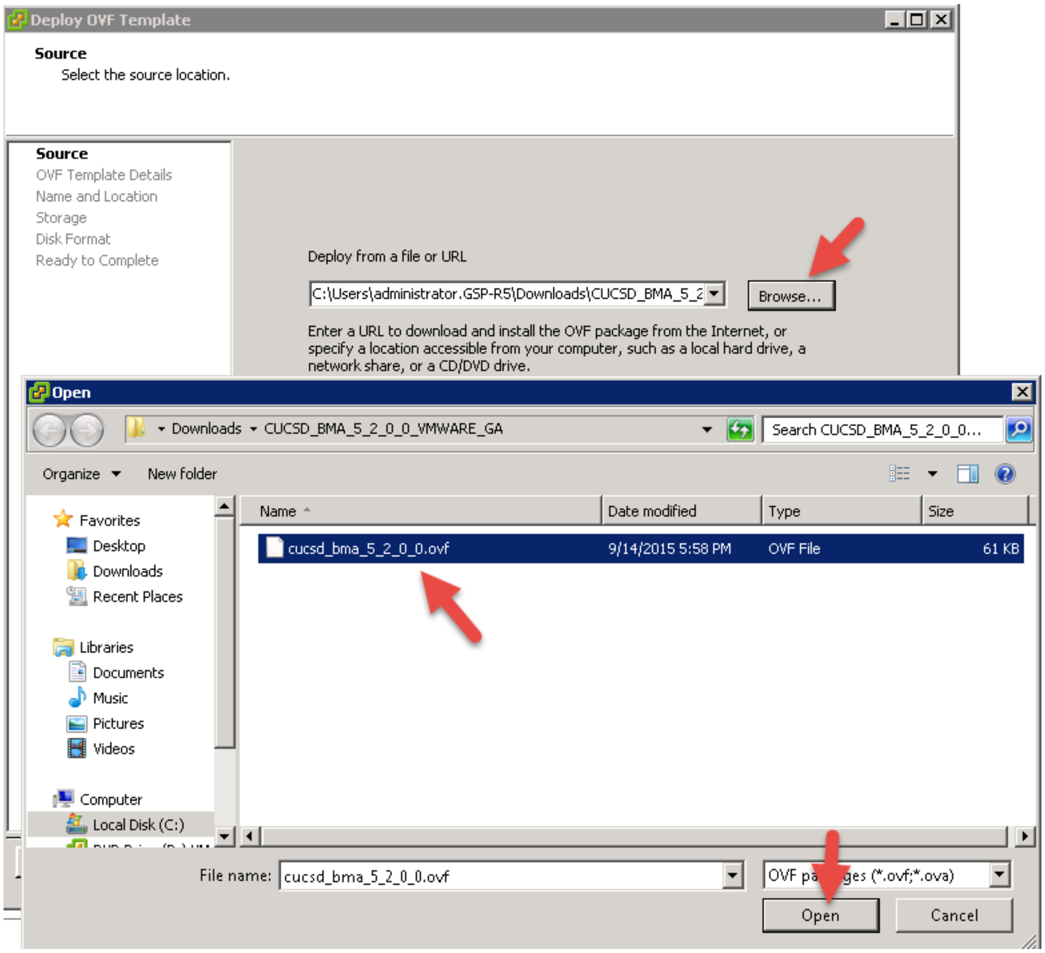
3. Deploy UCS Director BMA 5.2 OVF Template

Unzip the BMA 5.2 file that was downloaded from Cisco.com.

Log into vCenter and Select File -> Deploy OVF Template.



Browse for the BMA 5.2 OVF file, select it and Click Open. Click Next.



Select the source location.

Deploy from a file or URL: C:\Users\administrator.GSP-R5\Downloads\CUCSD_BMA_5_2

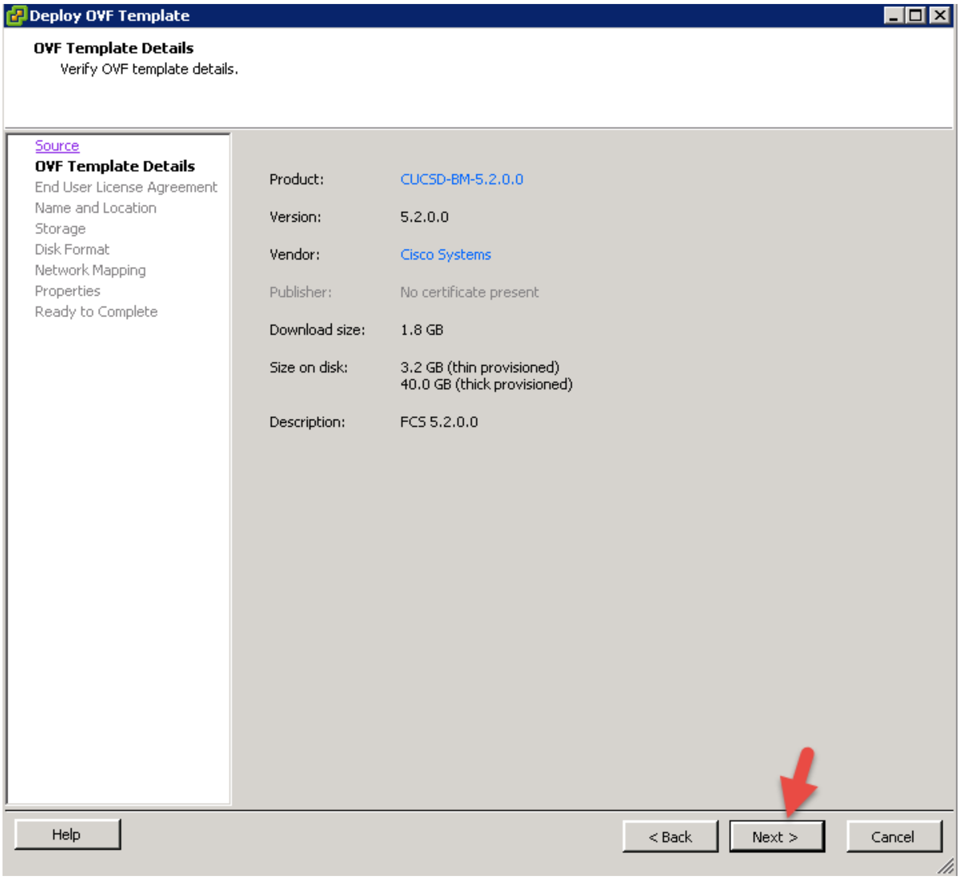
Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Name	Date modified	Type	Size
cucsd_bma_5_2_0_0.ovf	9/14/2015 5:58 PM	OVF File	61 KB

File name: cucsd_bma_5_2_0_0.ovf

OVF pa ges (*.ovf;*.ova)

Click Next.



OVF Template Details

Verify OVF template details.

Product: CUCSD-BM-5.2.0.0

Version: 5.2.0.0

Vendor: Cisco Systems

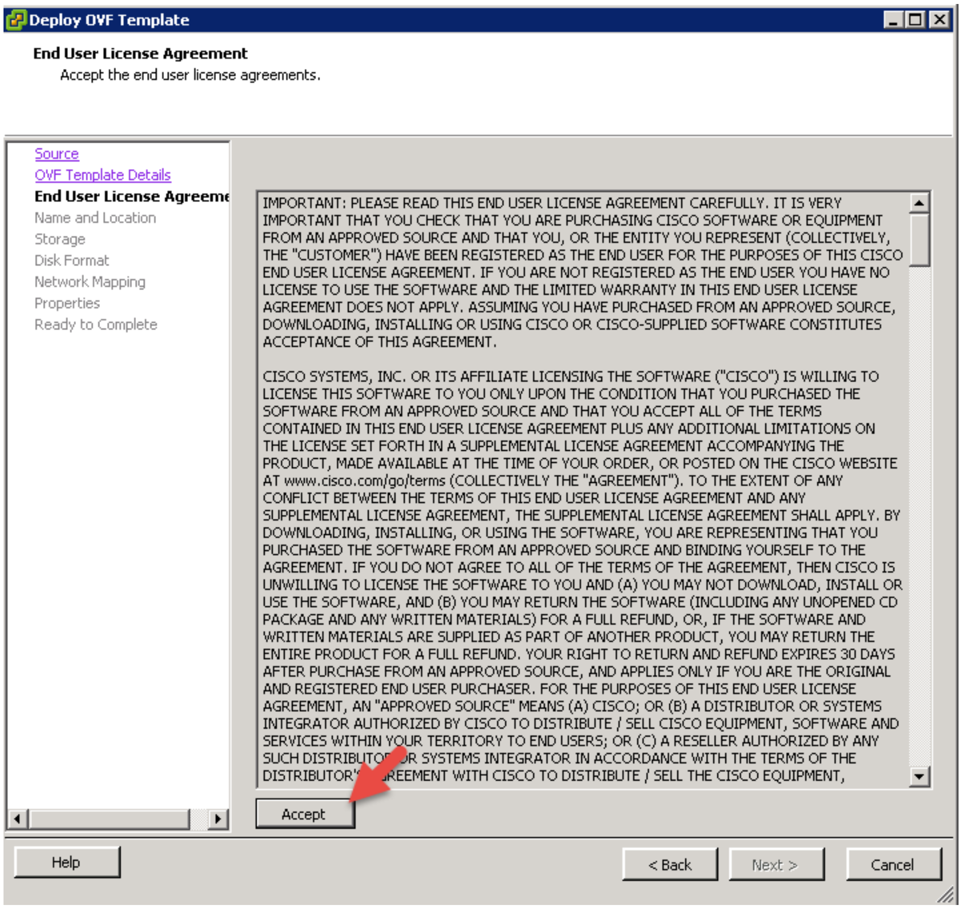
Publisher: No certificate present

Download size: 1.8 GB

Size on disk: 3.2 GB (thin provisioned)
40.0 GB (thick provisioned)

Description: FCS 5.2.0.0

Accept the license agreement and Click Next.

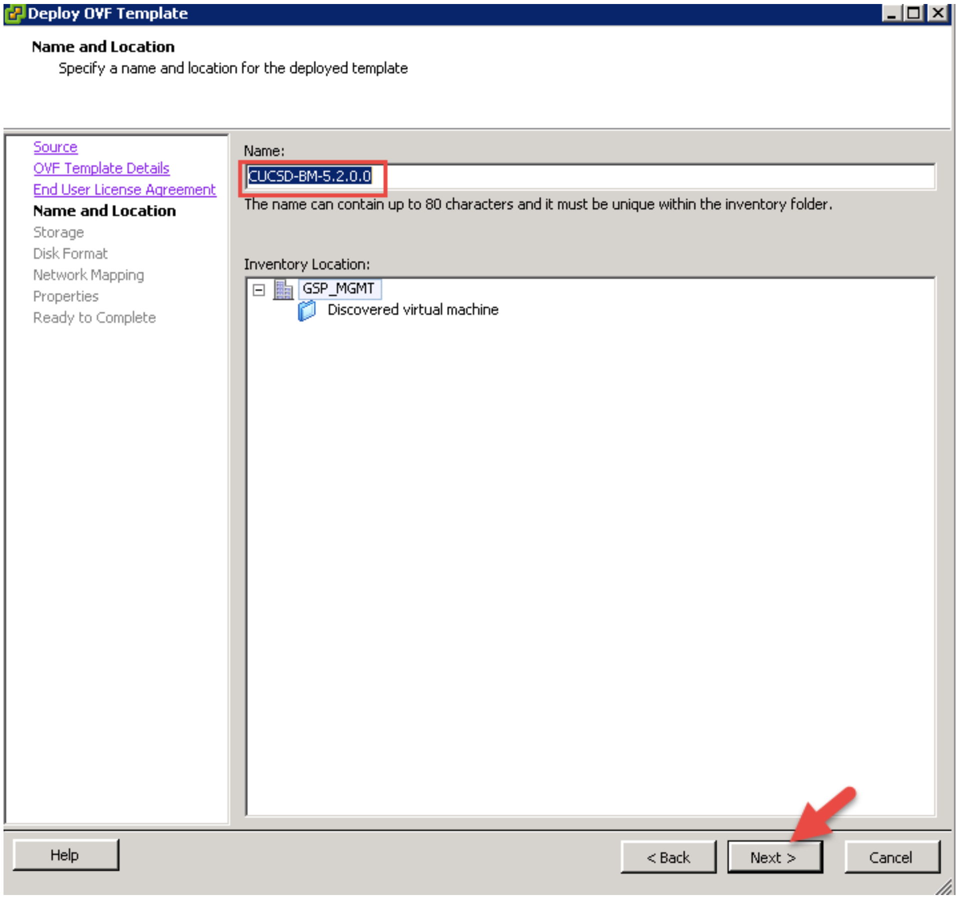


End User License Agreement

Accept the end user license agreements.

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS AFFILIATE LICENSING THE SOFTWARE ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT, MADE AVAILABLE AT THE TIME OF YOUR ORDER, OR POSTED ON THE CISCO WEBSITE AT www.cisco.com/go/terms (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE REPRESENTING THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND BINDING YOURSELF TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM AN APPROVED SOURCE, AND APPLIES ONLY IF YOU ARE THE ORIGINAL AND REGISTERED END USER PURCHASER. FOR THE PURPOSES OF THIS END USER LICENSE AGREEMENT, AN "APPROVED SOURCE" MEANS (A) CISCO; OR (B) A DISTRIBUTOR OR SYSTEMS INTEGRATOR AUTHORIZED BY CISCO TO DISTRIBUTE / SELL CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS; OR (C) A RESELLER AUTHORIZED BY ANY SUCH DISTRIBUTOR OR SYSTEMS INTEGRATOR IN ACCORDANCE WITH THE TERMS OF THE DISTRIBUTOR'S AGREEMENT WITH CISCO TO DISTRIBUTE / SELL THE CISCO EQUIPMENT, Name the BMA VM and Click Next.



Name and Location

Specify a name and location for the deployed template

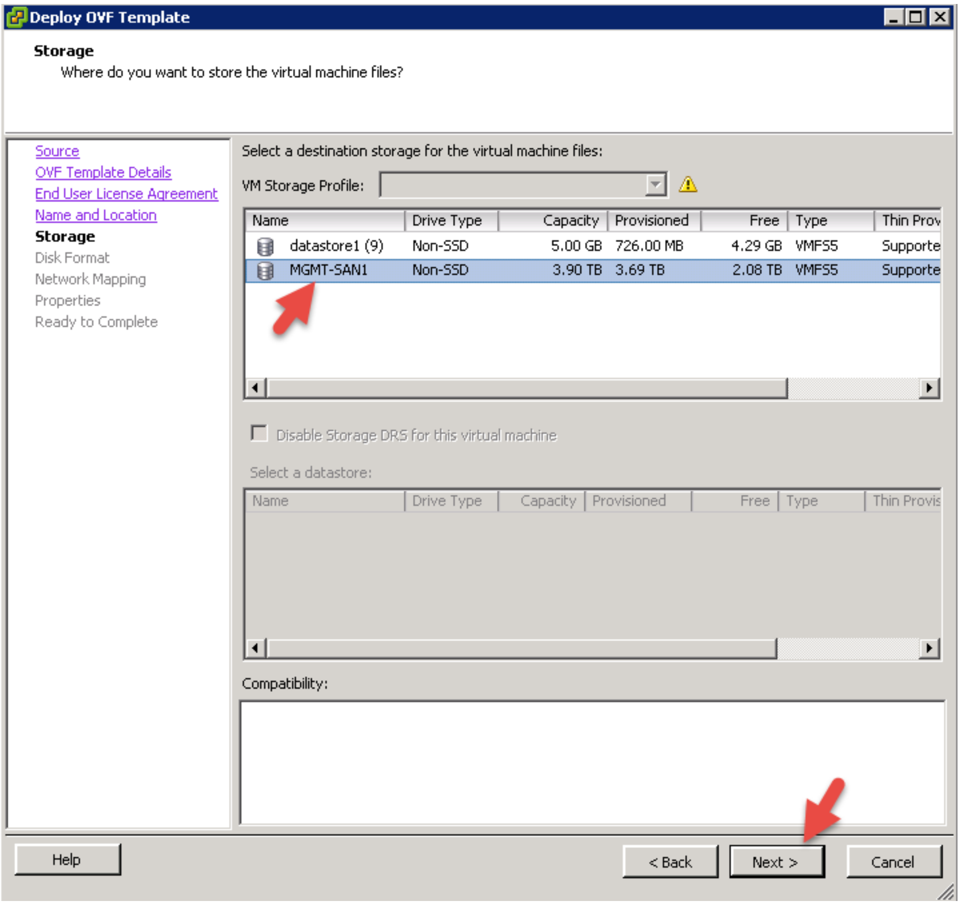
Name: CUCSD-BM-5.2.0.0

The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location:

- GSP_MGMT
  - Discovered virtual machine

Select the Storage location to install the VM and click Next.



Storage

Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

VM Storage Profile:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Prov
datastore1 (9)	Non-SSD	5.00 GB	726.00 MB	4.29 GB	VMFS5	Supporte
MGMT-SAN1	Non-SSD	3.90 TB	3.69 TB	2.08 TB	VMFS5	Supporte

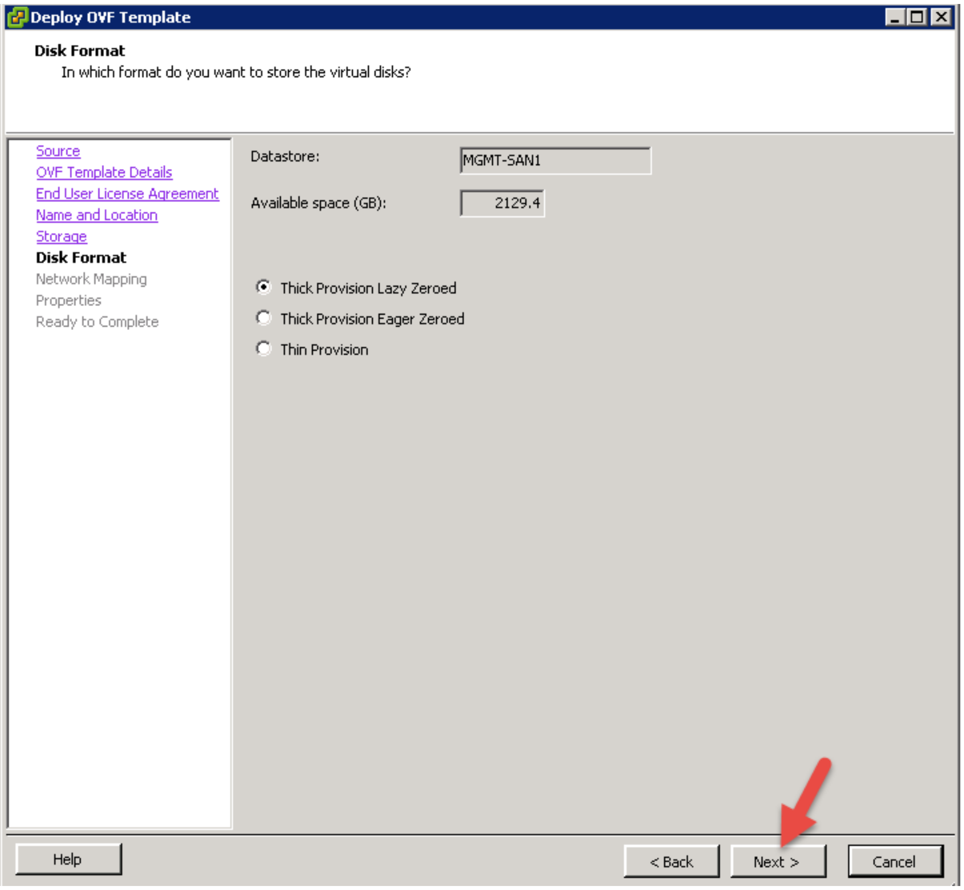
□ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provis

Compatibility:

Leave default and Click Next. Recommended to keep 'Thick Provision Lazy Zeroed'.



Deploy OVF Template

Disk Format

In which format do you want to store the virtual disks?

Datastore: MGMT-SAN1

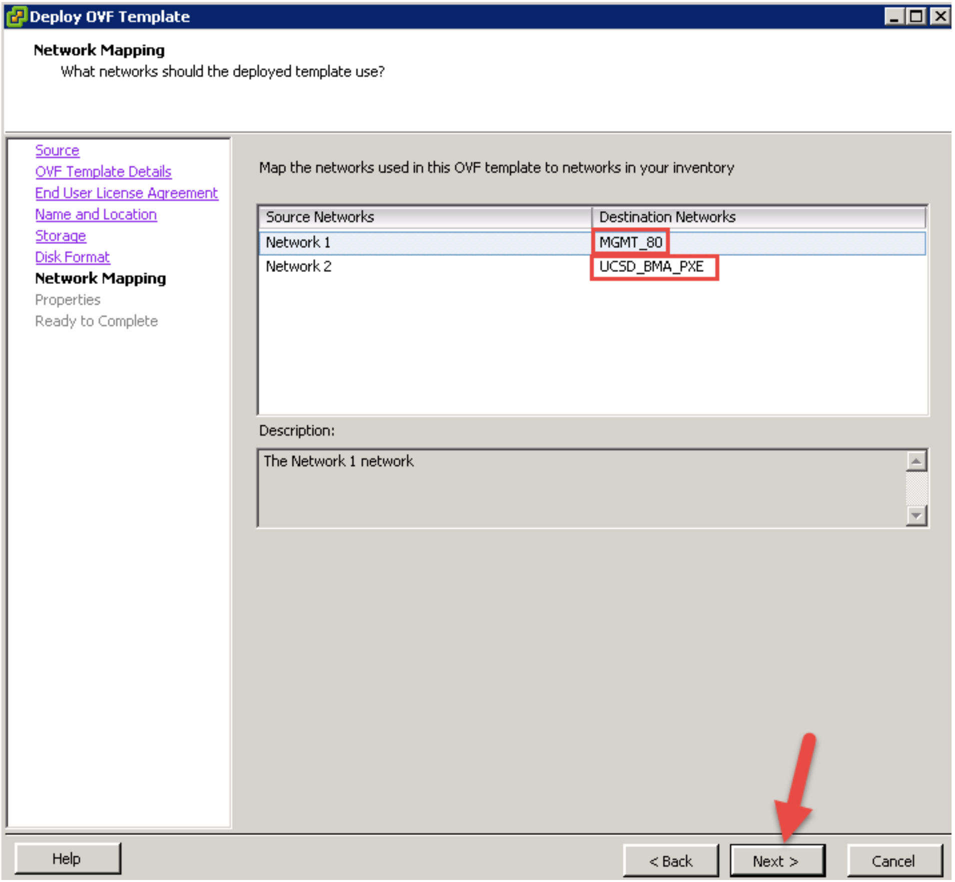
Available space (GB): 2129.4

● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

Select your management Network for Network 1 and the PXE Network for Network 2.



Deploy OVF Template

Network Mapping

What networks should the deployed template use?

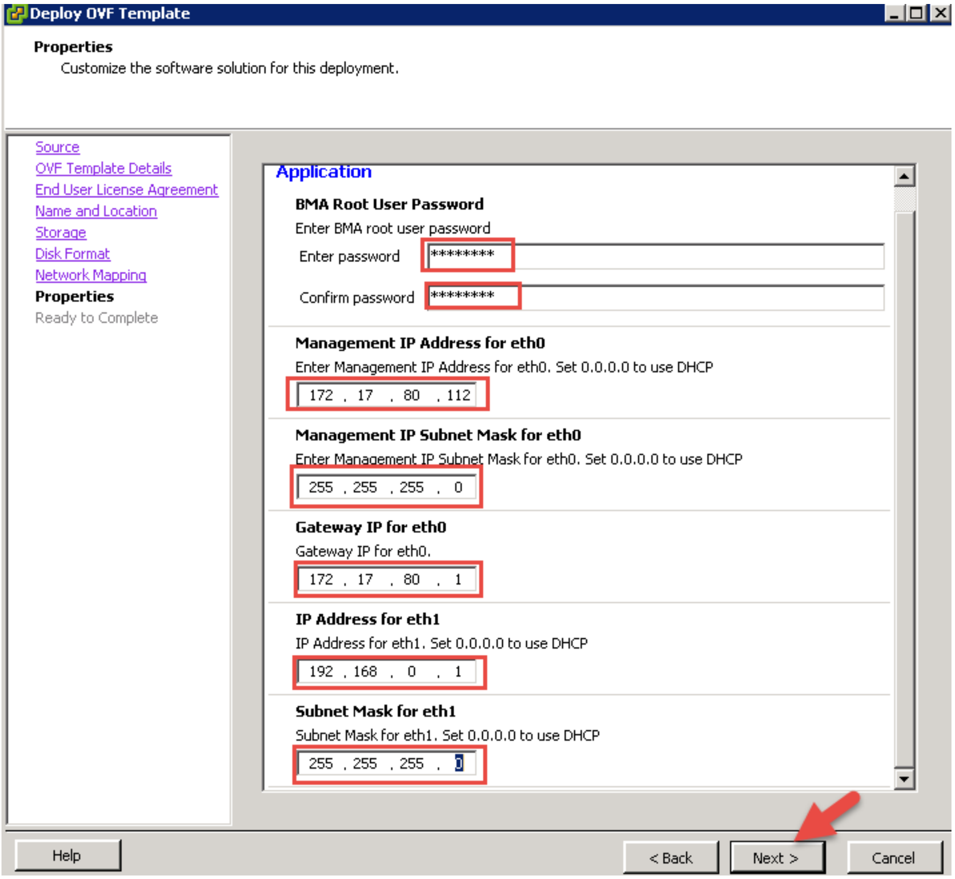
Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
Network 1	MGMT_80
Network 2	UCSD_BMA_PXE

Description:

The Network 1 network

Configure a password and IP Addresses, Masks and Gateway as shown below then Click Next.



Deploy OVF Template

Properties

Customize the software solution for this deployment.

Application

BMA Root User Password

Enter BMA root user password

Enter password ********

Confirm password ********

Management IP Address for eth0

Enter Management IP Address for eth0. Set 0.0.0.0 to use DHCP

172 . 17 . 80 . 112

Management IP Subnet Mask for eth0

Enter Management IP Subnet Mask for eth0. Set 0.0.0.0 to use DHCP

255 . 255 . 255 . 0

Gateway IP for eth0

Gateway IP for eth0.

172 . 17 . 80 . 1

IP Address for eth1

IP Address for eth1. Set 0.0.0.0 to use DHCP

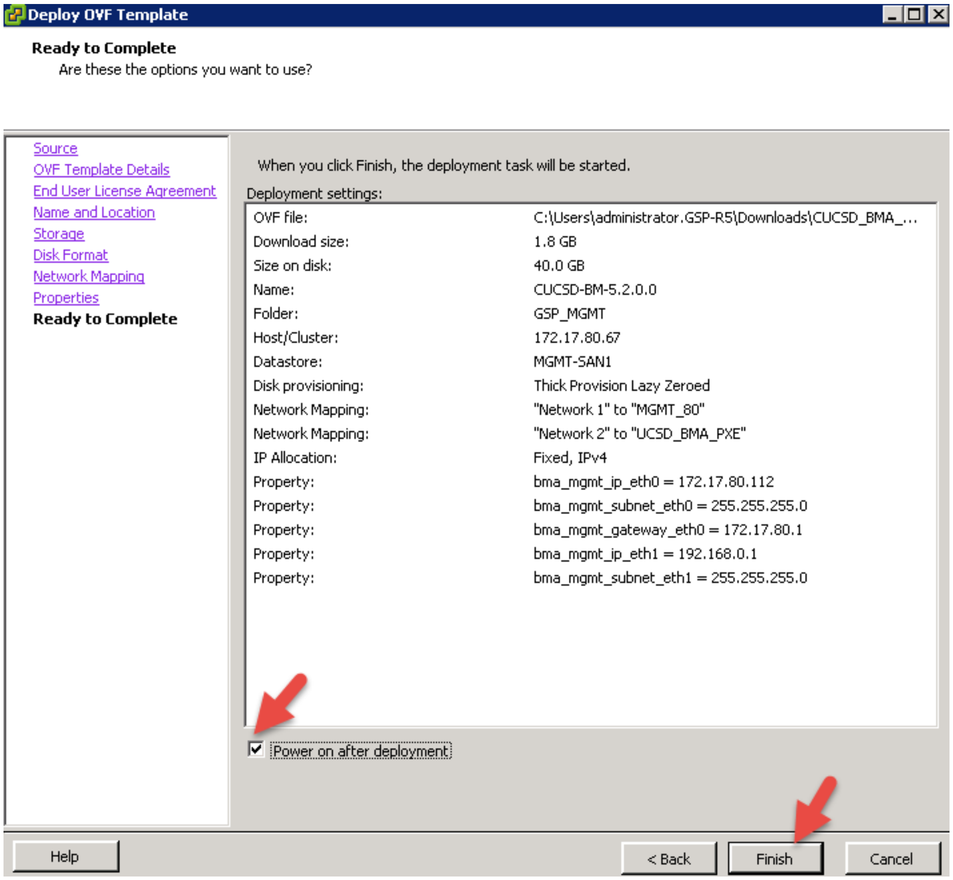
192 . 168 . 0 . 1

Subnet Mask for eth1

Subnet Mask for eth1. Set 0.0.0.0 to use DHCP

255 . 255 . 255 . 0

Review the settings and check the ‘Power on after deployment’ box and click Finish.



Deploy OVF Template

Ready to Complete

Are these the options you want to use?

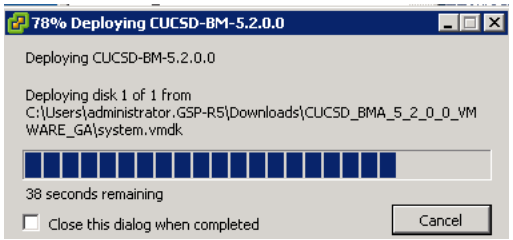
When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Users\administrator.GSP-R5\Downloads\CUCSD_BMA_...
Download size:	1.8 GB
Size on disk:	40.0 GB
Name:	CUCSD-BM-5.2.0.0
Folder:	GSP_MGMT
Host/Cluster:	172.17.80.67
Datastore:	MGMT-SAN1
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"Network 1" to "MGMT_80"
Network Mapping:	"Network 2" to "UCSD_BMA_PXE"
IP Allocation:	Fixed, IPv4
Property:	bma_mgmt_ip_eth0 = 172.17.80.112
Property:	bma_mgmt_subnet_eth0 = 255.255.255.0
Property:	bma_mgmt_gateway_eth0 = 172.17.80.1
Property:	bma_mgmt_ip_eth1 = 192.168.0.1
Property:	bma_mgmt_subnet_eth1 = 255.255.255.0

☑ Power on after deployment

Monitor the BMA VM Deployment.



78% Deploying CUCSD-BM-5.2.0.0

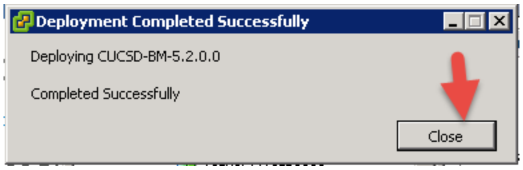
Deploying CUCSD-BM-5.2.0.0

Deploying disk 1 of 1 from C:\Users\administrator.GSP-R5\Downloads\CUCSD_BMA_5_2_0_0_VMWARE_GA\system.vmdk

38 seconds remaining

□ Close this dialog when completed

Upon completion, click Close.

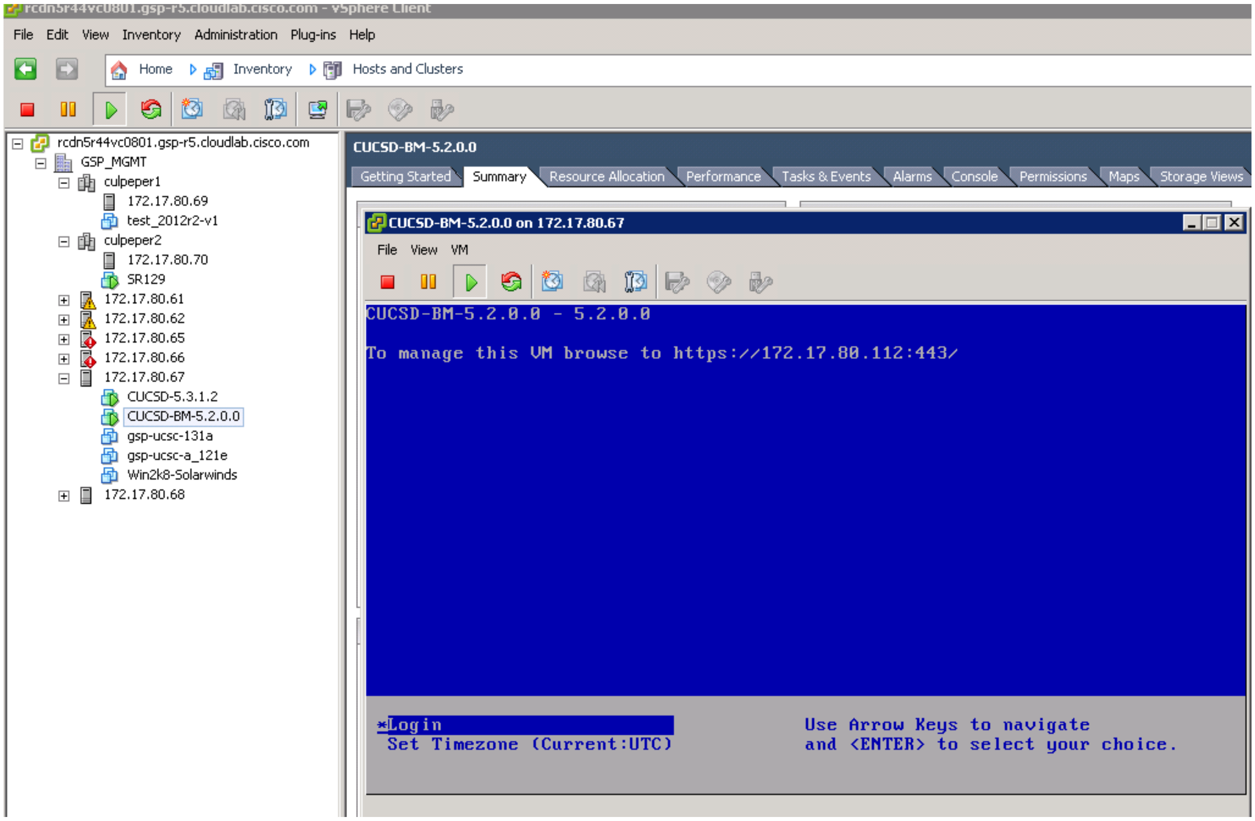


Deployment Completed Successfully

Deploying CUCSD-BM-5.2.0.0

Completed Successfully

Open the Console of the BMA VM and wait until you get the following screen to determine the VM is complete and has booted all the way up.



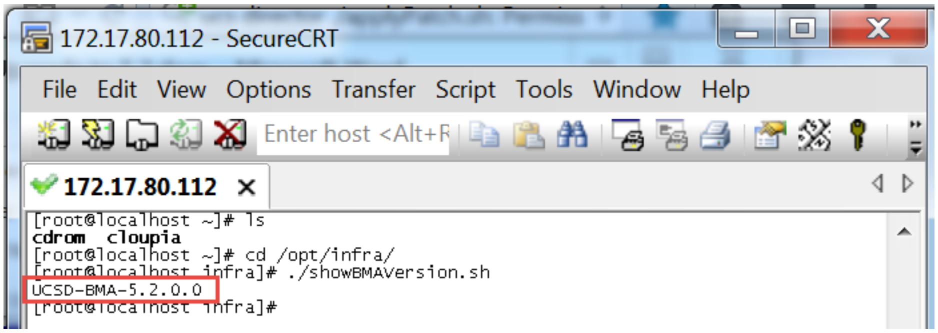
```
CUCSD-BM-5.2.0.0 - 5.2.0.0

To manage this VM browse to https://172.17.80.112:443/



 *Login                                 Use Arrow Keys to navigate
  Set Timezone (Current:UTC)            and <ENTER> to select your choice.
```

Verify connectivity by using SSH to access the BMA VM. Run the following commands to see the current version.



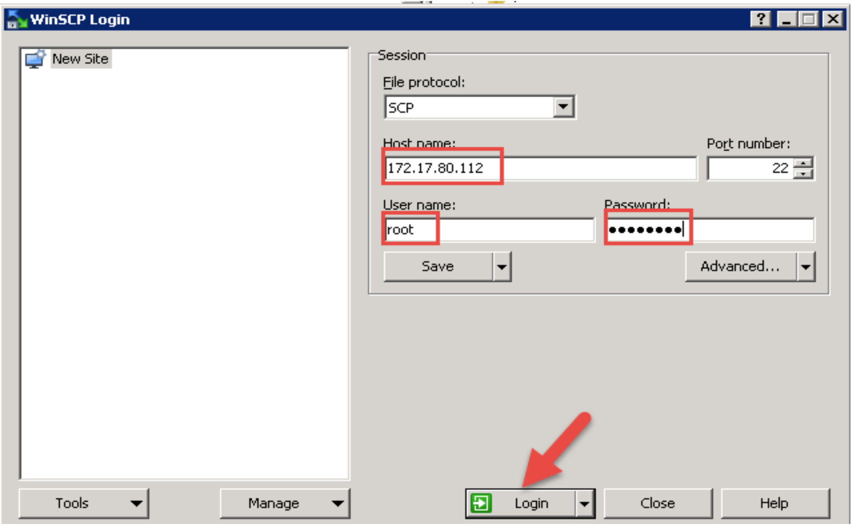
172.17.80.112 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R
172.17.80.112

```
[root@localhost ~]# ls
cdrom  cloupia
[root@localhost ~]# cd /opt/infra/
[root@localhost infra]# ./showBMAVersion.sh
UCSD-BMA-5.2.0.0
[root@localhost infra]#
```

4. Upgrade UCS Director BMA from 5.2 to 5.3

I recommend unzipping the 5.3 patch file on your local machine before uploading it to the BMA Server. You can use WinSCP or FileZilla to transfer the files to the BMA Server.

Using WinSCP, Enter the IP of the BMA Server and the username and password and click Login.



File protocol: SCP

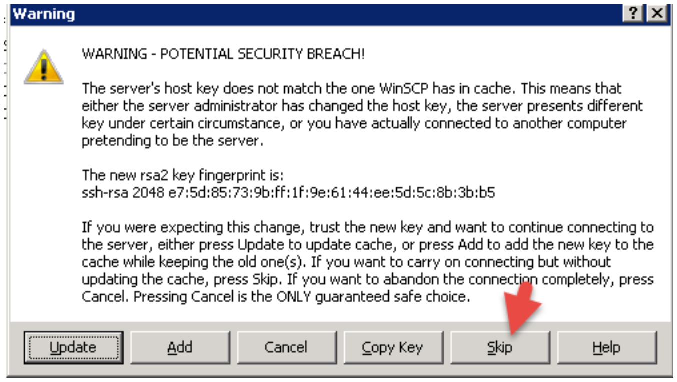
Host name: 172.17.80.112

Port number: 22

User name: root

Password: ••••••••

If prompted by this security alert, I selected skip.



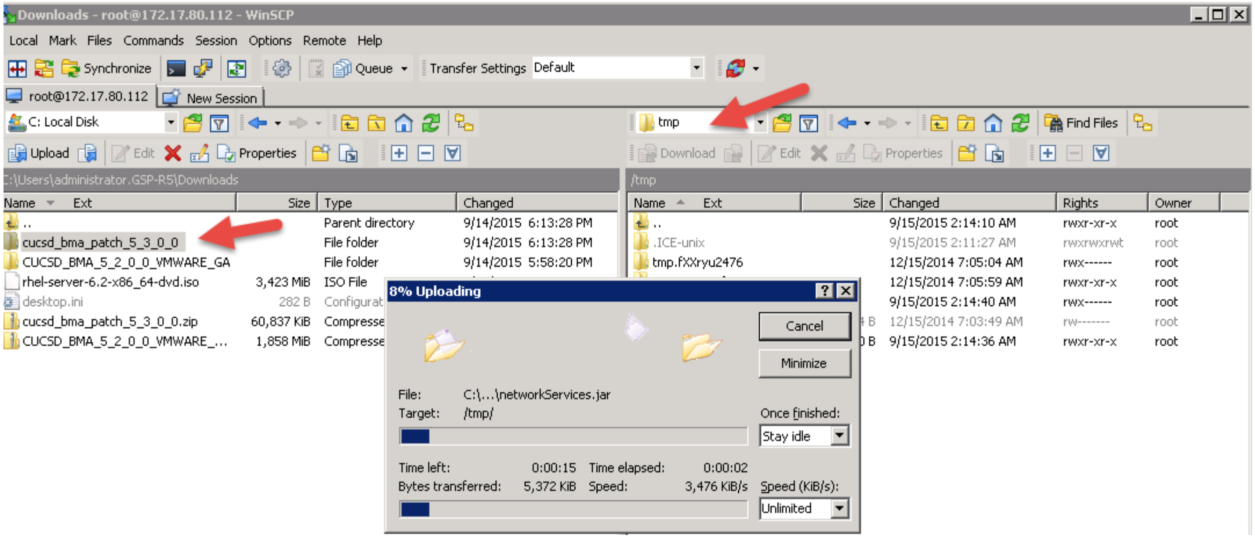
WARNING - POTENTIAL SECURITY BREACH!

The server's host key does not match the one WinSCP has in cache. This means that either the server administrator has changed the host key, the server presents different key under certain circumstance, or you have actually connected to another computer pretending to be the server.

The new rsa2 key fingerprint is:
ssh-rsa 2048 e7:5d:85:73:9b:ff:1f:9e:61:44:ee:5d:5c:8b:3b:b5

If you were expecting this change, trust the new key and want to continue connecting to the server, either press Update to update cache, or press Add to add the new key to the cache while keeping the old one(s). If you want to carry on connecting but without updating the cache, press Skip. If you want to abandon the connection completely, press Cancel. Pressing Cancel is the ONLY guaranteed safe choice.

Browse to the location where the patch is located on the left and navigate to the tmp folder on the right then drag the patch folder to the right to transfer the files to the BMA Server.



C:\Users\administrator.GSP-R5\Downloads

Name	Ext	Size	Type	Changed
..			Parent directory	9/14/2015 6:13:28 PM
cucsd_bma_patch_5_3_0_0			File folder	9/14/2015 6:13:28 PM
CUCSD_BMA_5_2_0_0_VMWARE_GA			File folder	9/14/2015 5:58:20 PM
rhel-server-6.2-x86_64-dvd.iso		3,423 MiB	ISO File	
desktop.ini		282 B	Configurat	
cucsd_bma_patch_5_3_0_0.zip		60,837 KiB	Compresse	
CUCSD_BMA_5_2_0_0_VMWARE_...		1,858 MiB	Compresse	

/tmp

Name	Ext	Size	Changed	Rights	Owner
..			9/15/2015 2:14:10 AM	rwxr-xr-x	root
.ICE-unix			9/15/2015 2:11:27 AM	rwxrwxrwt	root
tmp.fXXryu2476			12/15/2014 7:05:04 AM	rwx------	root
			12/15/2014 7:05:59 AM	rwxr-xr-x	root
			9/15/2015 2:14:40 AM	rwx------	root
		4 B	12/15/2014 7:03:49 AM	rw-------	root
		0 B	9/15/2015 2:14:36 AM	rwxr-xr-x	root

File: C:\...\networkServices.jar

Target: /tmp/

Once finished: Stay idle

Time left: 0:00:15

Time elapsed: 0:00:02

Bytes transferred: 5,372 KiB

Speed: 3,476 KiB/s

Speed (KiB/s): Unlimited

Once the files have been uploaded, log into the BMA appliance via SSH and change directory to tmp folder (or the folder you uploaded to). Run the command to apply the patch. Note: You will probably get permissions denied when trying to patch and you will have to chmod it to give yourself permissions to run the patch upgrade.

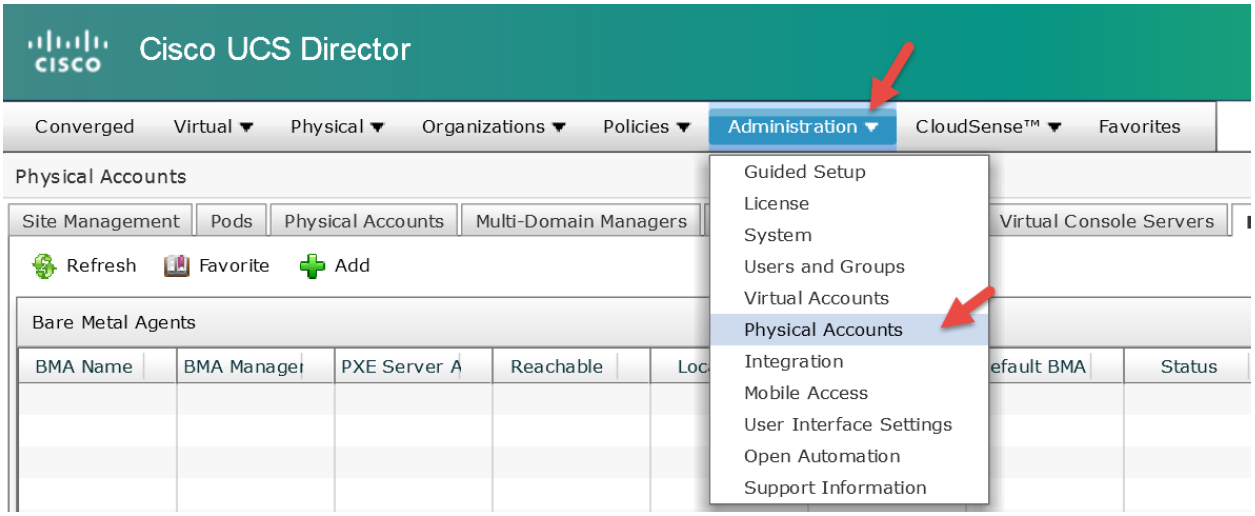
```
[root@localhost /]# cd tmp/
 [root@localhost tmp]# ls
cucsd_bma_patch_5_3_0_0  tmp.fXXryu2476  vmware-root
sfcbLocalSocket         vmware-config0
[root@localhost tmp]#
[root@localhost tmp]# cd cucsd_bma_patch_5_3_0_0/
 [root@localhost cucsd_bma_patch_5_3_0_0]# ls
ucsd_bma_patch_5_3_0_0
[root@localhost cucsd_bma_patch_5_3_0_0]# cd ucsd_bma_patch_5_3_0_0/
[root@localhost tmp]#
[root@localhost ucsd_bma_patch_5_3_0_0]# ls
ESXi5.5-VSAN  applyPatch.sh  isoExtractor.sh  networkServices.jar  storcliExtractor.sh  ucsd-bma-prod-info.json
[root@localhost ucsd_bma_patch_5_3_0_0]#
 [root@localhost ucsd_bma_patch_5_3_0_0]# ./applyPatch.sh
-bash: ./applyPatch.sh: Permission denied
[root@localhost ucsd_bma_patch_5_3_0_0]#
 [root@localhost ucsd_bma_patch_5_3_0_0]# ls -al
total 60920
drwxr-xr-x 3 root root     4096 Sep 15 02:27 .
drwxr-xr-x 3 root root     4096 Sep 15 02:27 ..
drwxr-xr-x 2 root root     4096 Sep 15 02:27 ESXi5.5-VSAN
-rw-r--r-- 1 root root     1414 Sep 14 23:13 applyPatch.sh
-rw-r--r-- 1 root root     6844 Sep 14 23:13 isoExtractor.sh
-rw-r--r-- 1 root root 62281019 Sep 14 23:13 networkServices.jar
-rw-r--r-- 1 root root     1096 Sep 14 23:13 storcliExtractor.sh
-rw-r--r-- 1 root root      348 Sep 14 23:13 ucsd-bma-prod-info.json
[root@localhost ucsd_bma_patch_5_3_0_0]#
 [root@localhost ucsd_bma_patch_5_3_0_0]# chmod 777 applyPatch.sh
[root@localhost ucsd_bma_patch_5_3_0_0]#
 [root@localhost ucsd_bma_patch_5_3_0_0]# ./applyPatch.sh
Current BMA version is UCSD-BMA-5.2.0.0
Taking file backup before upgrade
Taking Backup of Templates
Taking Backup of isoExtractor script
Copying NetworkServices jar.....
Copying ESXi5.5-VSAN templates....
Copying latest isoExtractor script....
Copying storcliExtractor.sh script....
Copying Latest Version details.....
Applied the patch successfully
[root@localhost ucsd_bma_patch_5_3_0_0]#
```

Navigate to /opt/infra and run the showBMAVersion scipt to verify you are not on the new version.

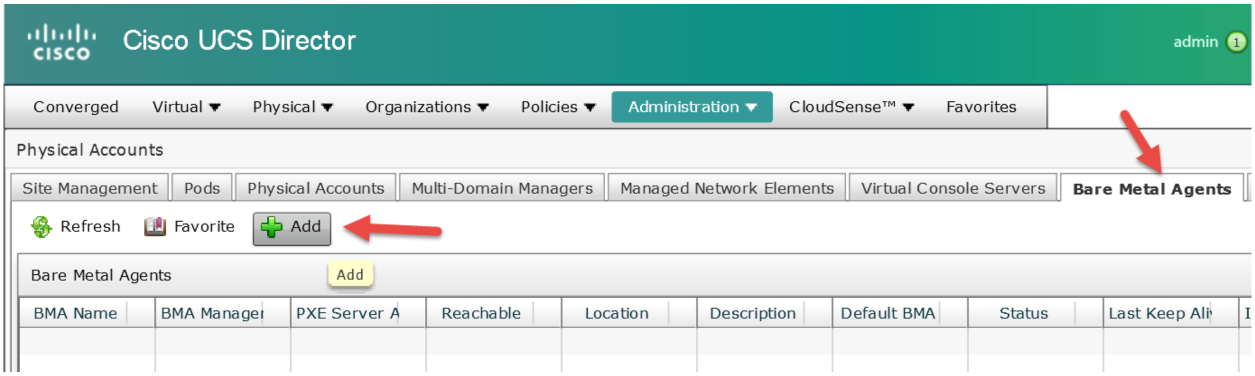
```
[root@localhost ucsd_bma_patch_5_3_0_0]# cd /opt/infra/
[root@localhost infra]# ls
addBMAAccount.sh   configureInterface.sh  networkServices              startInfraAll.sh
broker             controller             run.sh.template              statusInfra.sh
configure.sh       infraenv.sh            service.properties.template  stopInfraAll.sh
configureBmaID.sh  isoExtractor.sh        showBMAVersion.sh            ucsd-bma-prod-info.json
[root@localhost infra]# ./showBMAVersion.sh
UCSD-BMA-5.3.0.0
[root@localhost infra]#
```

5. Integrate UCS Director with Baremetal Agent Server

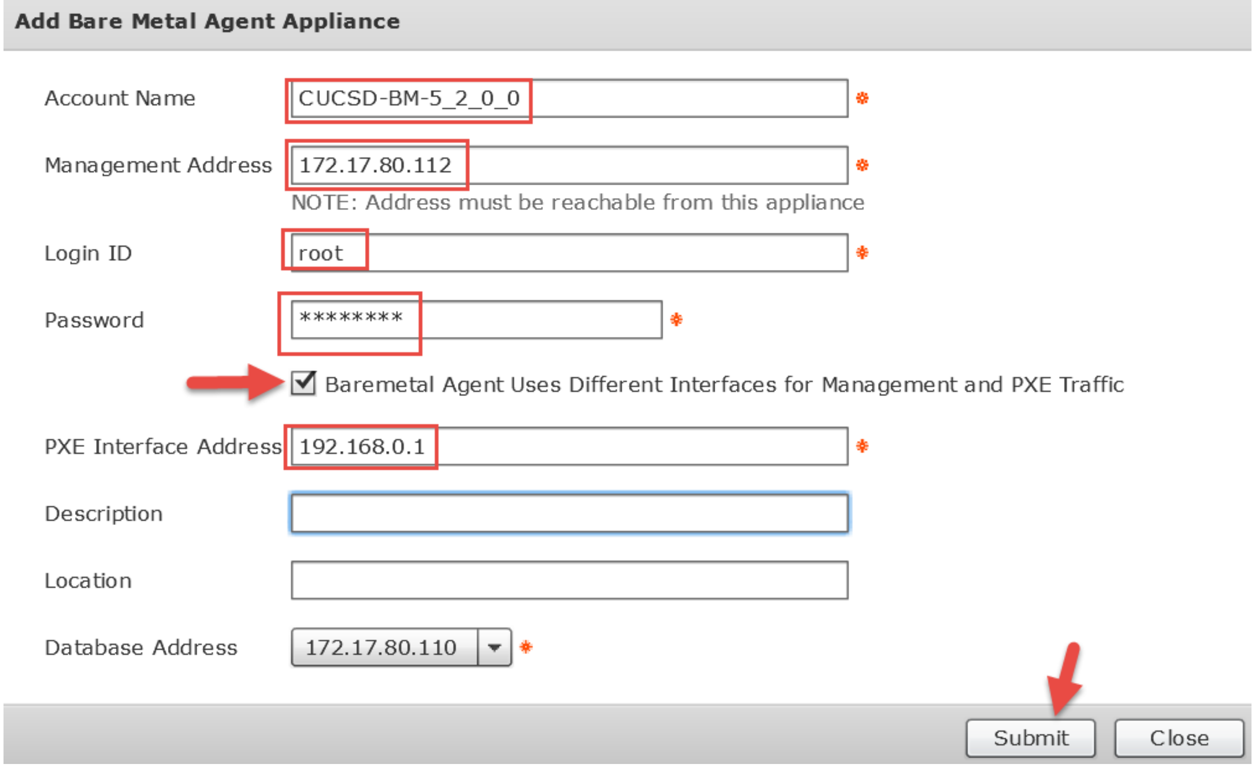
Log into UCS Director and navigate to Physical Accounts.



Select Baremetal Agents and Click Add.



Enter the name of your Baremetal appliance as the account name, select the checkbox for 'Baremetal Agent uses Different interfaces for management and PXE Traffic' and this will provide separate address boxes for the two IPs. Enter all other pertinent info as shown below and click Submit.



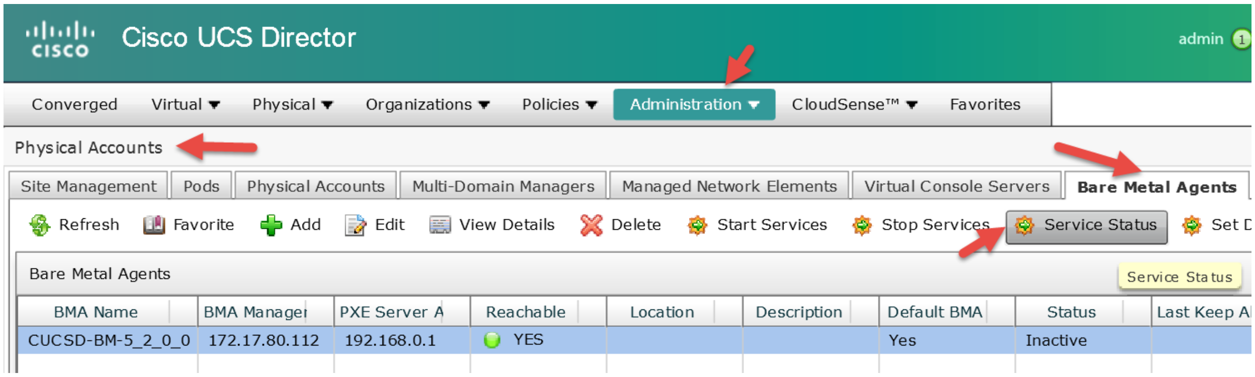
Add Bare Metal Agent Appliance

Account Name	CUCSD-BM-5_2_0_0 *
Management Address	172.17.80.112 * NOTE: Address must be reachable from this appliance
Login ID	root *
Password	******** *
	☑ Baremetal Agent Uses Different Interfaces for Management and PXE Traffic
PXE Interface Address	192.168.0.1 *
Description	
Location	
Database Address	172.17.80.110 *

You'll get a pop-up to say Request saved successfully. Click ok. Next you'll see that the Baremetal agent has been registered and ensure it is reachable from UCS Director.

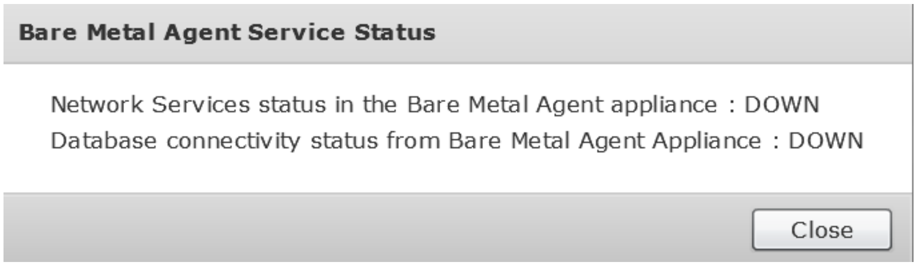
6. Configure DHCP on the BMA

From the Baremetal Agents tab in UCS Director, verify the Services are stopped by checking the Service Status.



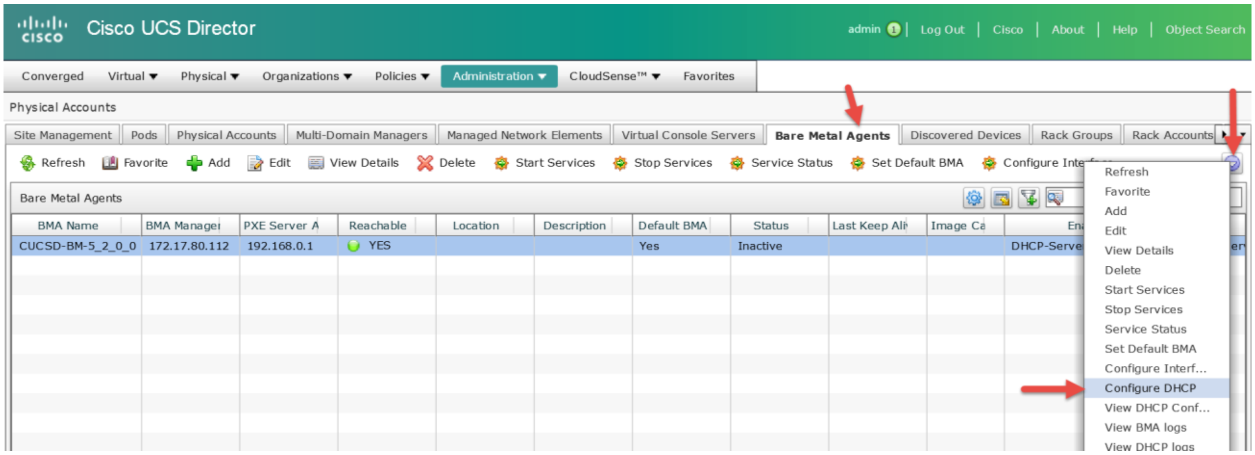
BMA Name	BMA Manager	PXE Server A	Reachable	Location	Description	Default BMA	Status	Last Keep A
CUCSD-BM-5_2_0_0	172.17.80.112	192.168.0.1	YES			Yes	Inactive	

Services should show Down as follows.



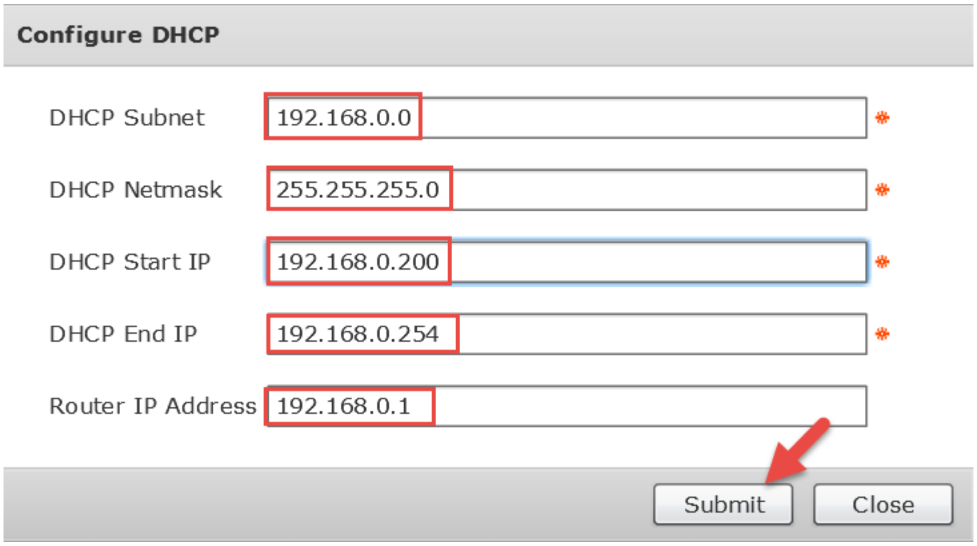
Network Services status in the Bare Metal Agent appliance : DOWN
Database connectivity status from Bare Metal Agent Appliance : DOWN

Select Configure DHCP. You may have to click the little down arrow to the right to see the Configure DHCP option.



BMA Name	BMA Manager	PXE Server A	Reachable	Location	Description	Default BMA	Status	Last Keep Ali	Image Ca	Ena	
CUCSD-BM-5_2_0_0	172.17.80.112	192.168.0.1	YES			Yes	Inactive			DHCP-Serve	er

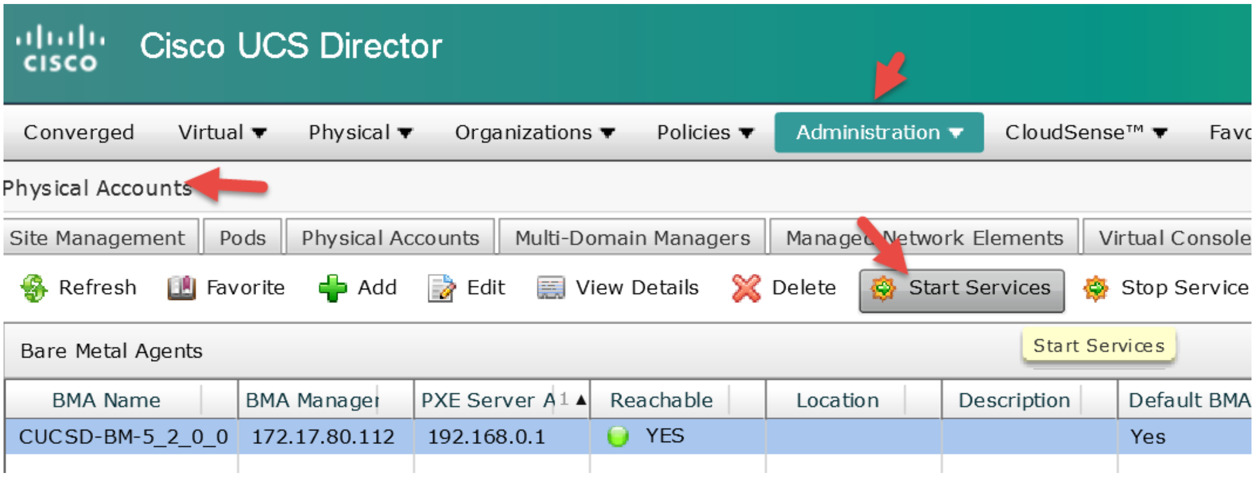
Configure the DHCP IP Addresses and click Submit.



Configure DHCP

DHCP Subnet	192.168.0.0 *
DHCP Netmask	255.255.255.0 *
DHCP Start IP	192.168.0.200 *
DHCP End IP	192.168.0.254 *
Router IP Address	192.168.0.1

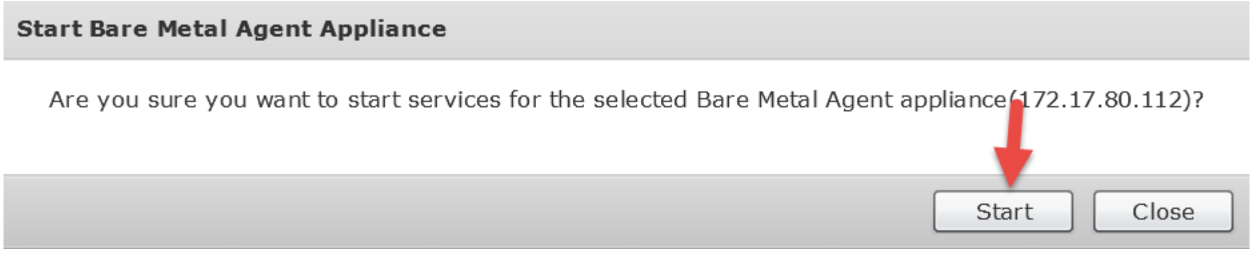
Click Start Services.



Bare Metal Agents

BMA Name	BMA Manager	PXE Server A	Reachable	Location	Description	Default BMA
CUCSD-BM-5_2_0_0	172.17.80.112	192.168.0.1	● YES			Yes

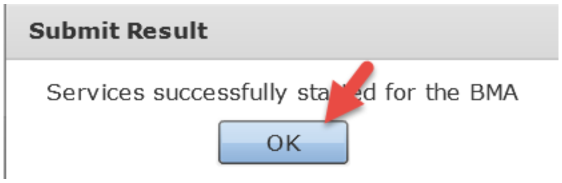
Click Start.



Start Bare Metal Agent Appliance

Are you sure you want to start services for the selected Bare Metal Agent appliance(172.17.80.112)?

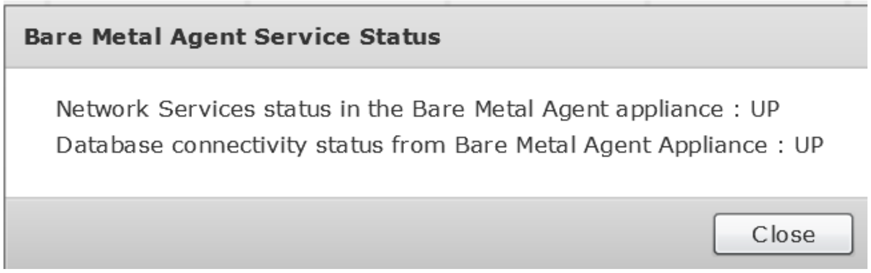
Click OK.



Submit Result

Services successfully started for the BMA

Check the Service Status again.



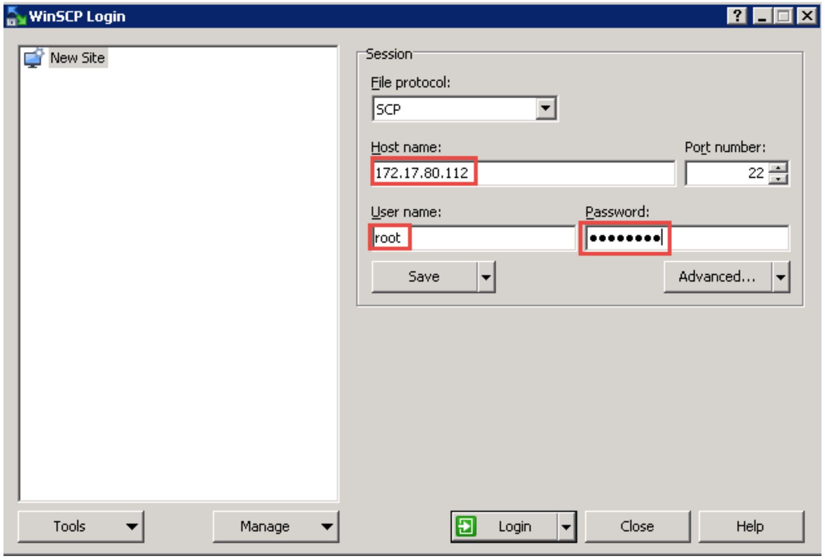
Bare Metal Agent Service Status

Network Services status in the Bare Metal Agent appliance : UP
Database connectivity status from Bare Metal Agent Appliance : UP

7. Upload Images

Here we will upload ISO images to the BMA appliance to be used for PXEboot deployments. You will need copies of the ISOs you plan on putting on the BMA appliance. You can upload the ISO images using WinSCP.

Connect to BMA Server using WinSCP.



Session

File protocol: SCP

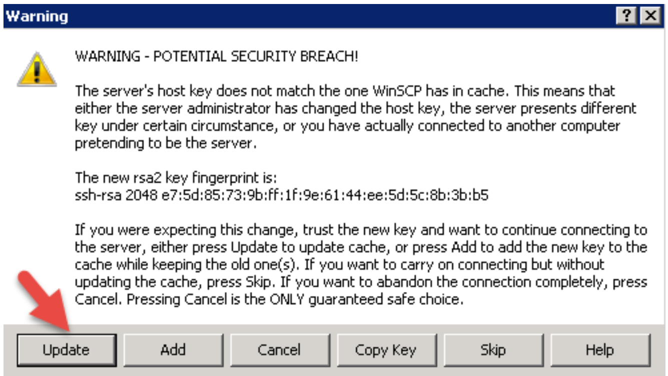
Host name: 172.17.80.112

Port number: 22

User name: root

Password: ●●●●●●●●

Select Update or Skip for this security worning.



Warning

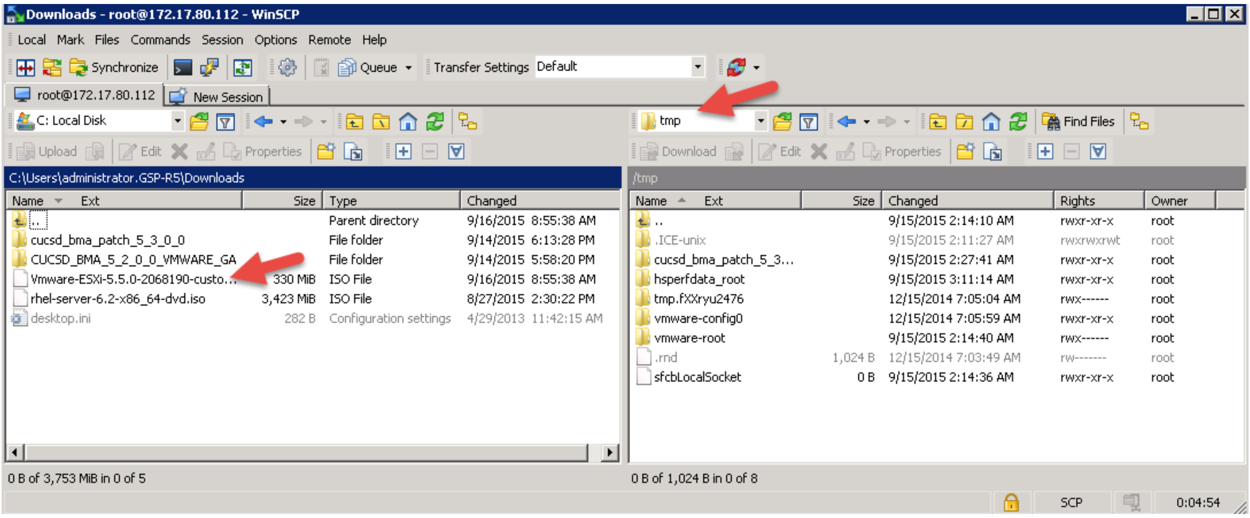
WARNING - POTENTIAL SECURITY BREACH!

The server's host key does not match the one WinSCP has in cache. This means that either the server administrator has changed the host key, the server presents different key under certain circumstance, or you have actually connected to another computer pretending to be the server.

The new rsa2 key fingerprint is:
ssh-rsa 2048 e7:5d:85:73:9b:ff:1f:9e:61:44:ee:5d:5c:8b:3b:b5

If you were expecting this change, trust the new key and want to continue connecting to the server, either press Update to update cache, or press Add to add the new key to the cache while keeping the old one(s). If you want to carry on connecting but without updating the cache, press Skip. If you want to abandon the connection completely, press Cancel. Pressing Cancel is the ONLY guaranteed safe choice.

On the left browse to your ISO and on the right, browse to the tmp folder as this is where we will place the ISO file. In this example, we are using the Custom Cisco ESXi 5.5 Update 2 image.



C:\Users\administrator.GSP-R5\Downloads

Name	Ext	Size	Type	Changed
..			Parent directory	9/16/2015 8:55:38 AM
cucsd_bma_patch_5_3_0_0			File folder	9/14/2015 6:13:28 PM
CUCSD_BMA_5_2_0_0_VMWARE_GA			File folder	9/14/2015 5:58:20 PM
Vmware-ESXi-5.5.0-2068190-custo...		330 MiB	ISO File	9/16/2015 8:55:38 AM
rhel-server-6.2-x86_64-dvd.iso		3,423 MiB	ISO File	8/27/2015 2:30:22 PM
desktop.ini		282 B	Configuration settings	4/29/2013 11:42:15 AM

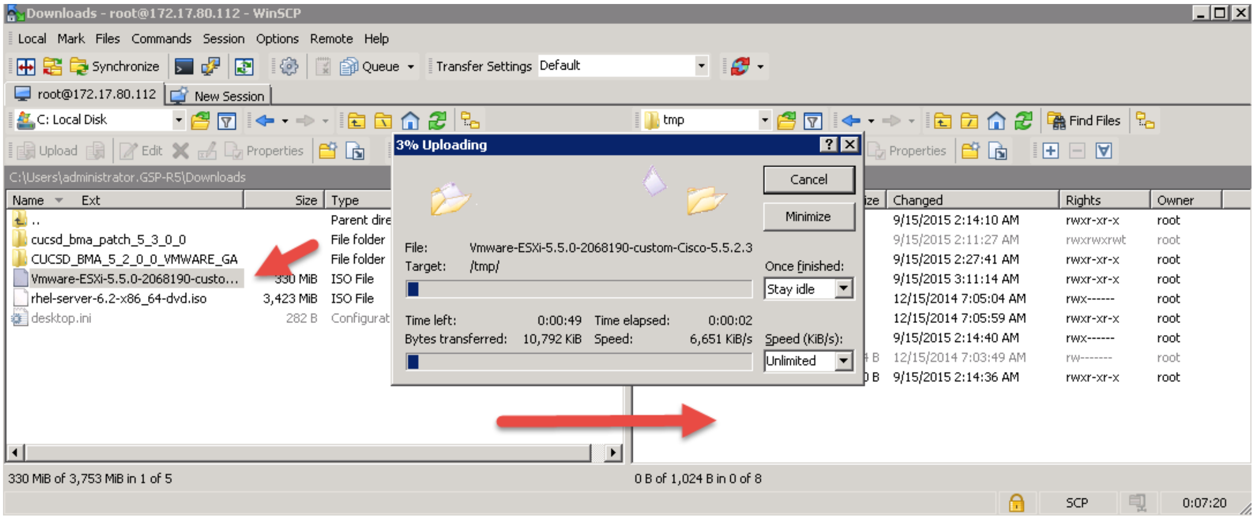
0 B of 3,753 MiB in 0 of 5

/tmp

Name	Ext	Size	Changed	Rights	Owner
..			9/15/2015 2:14:10 AM	rwxr-xr-x	root
.ICE-unix			9/15/2015 2:11:27 AM	rwxrwxrwt	root
cucsd_bma_patch_5_3...			9/15/2015 2:27:41 AM	rwxr-xr-x	root
hsperfdata_root			9/15/2015 3:11:14 AM	rwxr-xr-x	root
tmp.fXXryu2476			12/15/2014 7:05:04 AM	rwx------	root
vmware-config0			12/15/2014 7:05:59 AM	rwxr-xr-x	root
vmware-root			9/15/2015 2:14:40 AM	rwx------	root
.rnd		1,024 B	12/15/2014 7:03:49 AM	rw-------	root
sfcbLocalSocket		0 B	9/15/2015 2:14:36 AM	rwxr-xr-x	root

0 B of 1,024 B in 0 of 8

Select the ISO on the left and drag it to the tmp directory on the right.



Downloads - root@172.17.80.112 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
root@172.17.80.112
New Session
C: Local Disk
tmp
Find Files
Upload
Edit
Properties
Properties
Cancel
Minimize

C:\Users\administrator.GSP-R5\Downloads

Name	Ext	Size	Type
..			Parent dire
cucsd_bma_patch_5_3_0_0			File folder
CUCSD_BMA_5_2_0_0_VMWARE_GA			File folder
Vmware-ESXi-5.5.0-2068190-custo…		330 MiB	ISO File
rhel-server-6.2-x86_64-dvd.iso		3,423 MiB	ISO File
desktop.ini		282 B	Configurat

ize	Changed	Rights	Owner
	9/15/2015 2:14:10 AM	rwxr-xr-x	root
	9/15/2015 2:11:27 AM	rwxrwxrwt	root
	9/15/2015 2:27:41 AM	rwxr-xr-x	root
	9/15/2015 3:11:14 AM	rwxr-xr-x	root
	12/15/2014 7:05:04 AM	rwx------	root
	12/15/2014 7:05:59 AM	rwxr-xr-x	root
	9/15/2015 2:14:40 AM	rwx------	root
# B	12/15/2014 7:03:49 AM	rw-------	root
0 B	9/15/2015 2:14:36 AM	rwxr-xr-x	root

3% Uploading

File: Vmware-ESXi-5.5.0-2068190-custom-Cisco-5.5.2.3
Target: /tmp/

Once finished: Stay idle

Time left: 0:00:49 Time elapsed: 0:00:02
Bytes transferred: 10,792 KiB Speed: 6,651 KiB/s

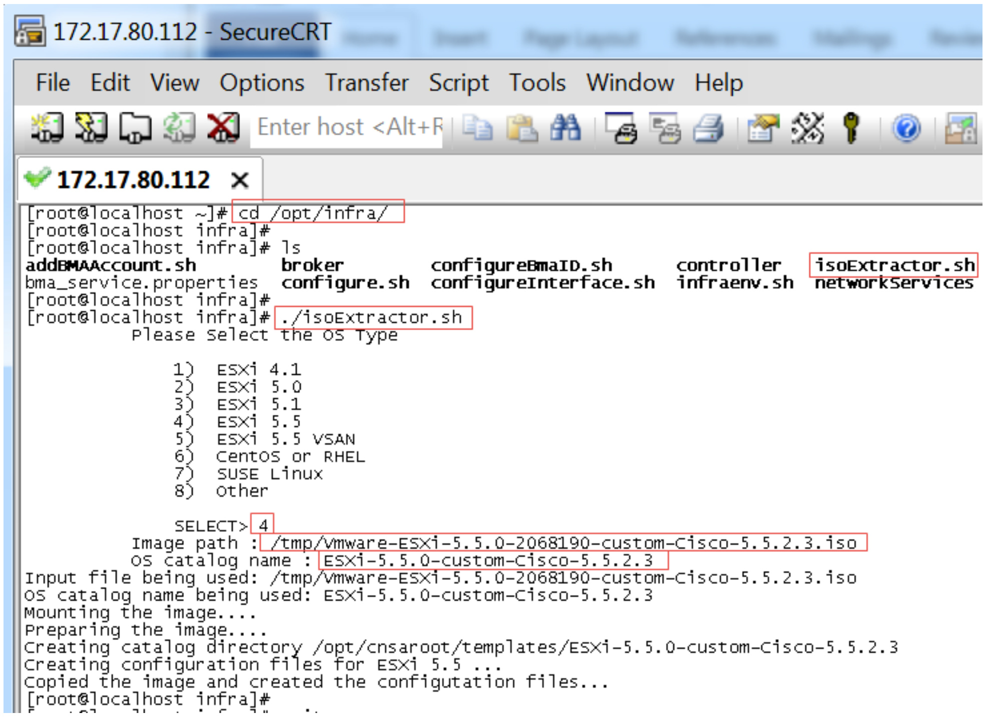
Speed (KiB/s): Unlimited

330 MiB of 3,753 MiB in 1 of 5

0 B of 1,024 B in 0 of 8

SCP 0:07:20

Once the images have been uploaded, SSH to the BMA appliance and cd to /opt/infra directory and run the isoExtractor.sh script. This will extract the ISO to the local machine. If you have multiple ISOs uploaded, you can extract them all before continuing. You will need to enter the image location and catalog name for the extracted files.

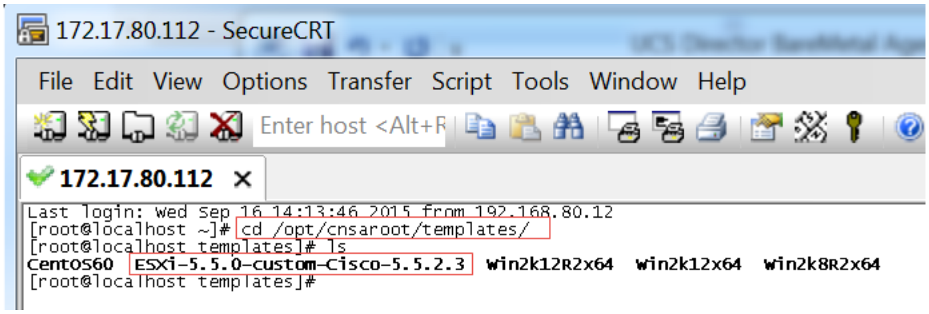

172.17.80.112 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R
172.17.80.112

```
[root@localhost ~]# cd /opt/infra/
[root@localhost infra]#
[root@localhost infra]# ls
addBMAAccount.sh        broker        configureBmaID.sh       controller    isoExtractor.sh
bma_service.properties  configure.sh  configureInterface.sh   infraenv.sh   networkServices
[root@localhost infra]#
[root@localhost infra]# ./isoExtractor.sh
          Please Select the OS Type

              1)  ESXi 4.1
              2)  ESXi 5.0
              3)  ESXi 5.1
              4)  ESXi 5.5
              5)  ESXi 5.5 VSAN
              6)  CentOS or RHEL
              7)  SUSE Linux
              8)  Other

              SELECT> 4
          Image path : /tmp/Vmware-ESXi-5.5.0-2068190-custom-Cisco-5.5.2.3.iso
          OS catalog name : ESXi-5.5.0-custom-Cisco-5.5.2.3
Input file being used: /tmp/Vmware-ESXi-5.5.0-2068190-custom-Cisco-5.5.2.3.iso
OS catalog name being used: ESXi-5.5.0-custom-Cisco-5.5.2.3
Mounting the image....
Preparing the image....
Creating catalog directory /opt/cnsaroot/templates/ESXi-5.5.0-custom-Cisco-5.5.2.3
Creating configuration files for ESXi 5.5 ...
Copied the image and created the configutation files...
[root@localhost infra]#
```

Verify the image is available in the catalog location.


172.17.80.112 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R
172.17.80.112

```
Last login: Wed Sep 16 14:13:46 2015 from 192.168.80.12
[root@localhost ~]# cd /opt/cnsaroot/templates/
[root@localhost templates]# ls
CentOS60  ESXi-5.5.0-custom-Cisco-5.5.2.3  Win2k12R2x64  Win2k12x64  Win2k8R2x64
[root@localhost templates]#
```

Verify the image shows up in UCS Director. Administrator -> Physical Accounts -> Bare Metal Agents -> CUSCD-BM-5_2_0_0.

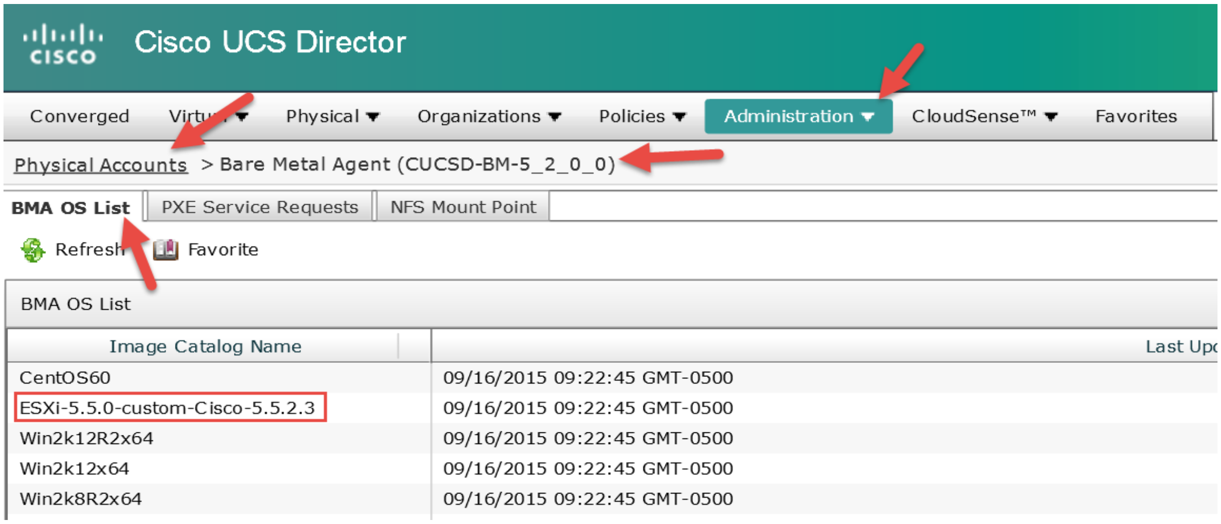
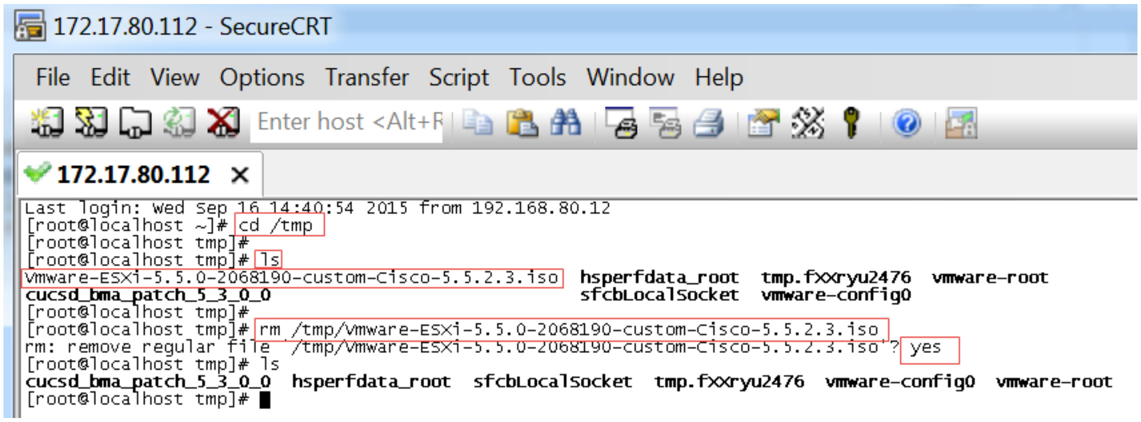


Image Catalog Name	Last Upc
CentOS60	09/16/2015 09:22:45 GMT-0500
ESXi-5.5.0-custom-Cisco-5.5.2.3	09/16/2015 09:22:45 GMT-0500
Win2k12R2x64	09/16/2015 09:22:45 GMT-0500
Win2k12x64	09/16/2015 09:22:45 GMT-0500
Win2k8R2x64	09/16/2015 09:22:45 GMT-0500

Clean up the BMA by removing the ISO that we put in tmp directory.



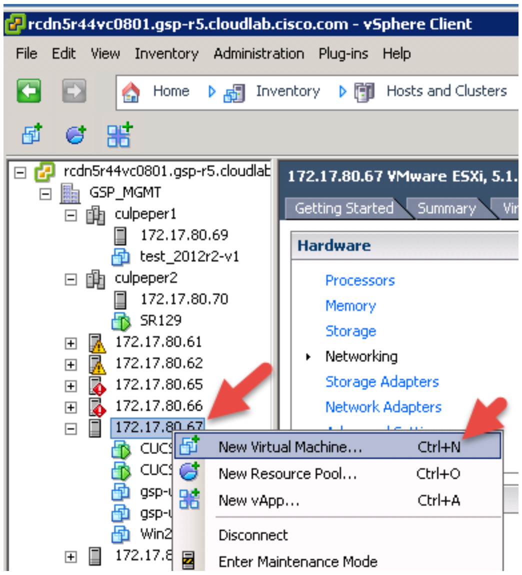
172.17.80.112 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R
172.17.80.112

```
Last login: Wed Sep 16 14:40:54 2015 from 192.168.80.12
[root@localhost ~]# cd /tmp
[root@localhost tmp]#
[root@localhost tmp]# ls
Vmware-ESXi-5.5.0-2068190-custom-Cisco-5.5.2.3.iso  hsperfdata_root  tmp.fXXryu2476  vmware-root
cucsd_bma_patch_5_3_0_0                              sfcbLocalSocket  vmware-config0
[root@localhost tmp]#
[root@localhost tmp]# rm /tmp/Vmware-ESXi-5.5.0-2068190-custom-Cisco-5.5.2.3.iso
rm: remove regular file `/tmp/Vmware-ESXi-5.5.0-2068190-custom-Cisco-5.5.2.3.iso'? yes
[root@localhost tmp]# ls
cucsd_bma_patch_5_3_0_0  hsperfdata_root  sfcbLocalSocket  tmp.fXXryu2476  vmware-config0  vmware-root
[root@localhost tmp]# █
```

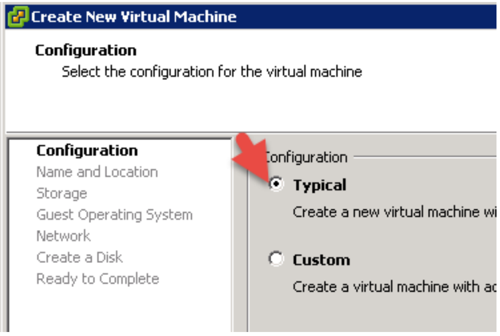
8. Basic functionality BMA Test/Validation

Before moving on to build a complete workflow to provision a Baremetal server, it is highly recommended to test functionality of the BMA using a basic VM. This will confirm that your network is configured correctly, DHCP is functioning correctly and the UCS Director is integrated with BMA. **Note**: DHCP for BMA was previously configured so we don't need to complete that step.

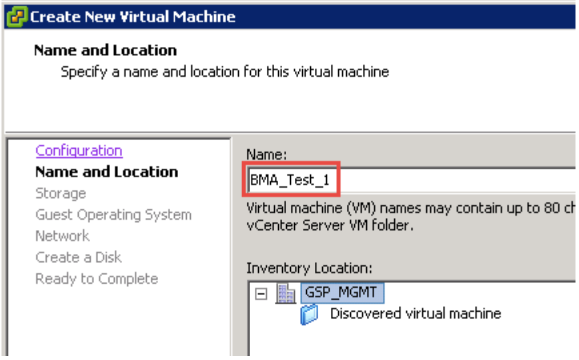
Create Generic VM. Select New Virtual Machine.



Leave default set to Typical and click Next.



Define any name for the VM and click Next.



Create New Virtual Machine

Name and Location

Specify a name and location for this virtual machine

Configuration
Name and Location
Storage
Guest Operating System
Network
Create a Disk
Ready to Complete

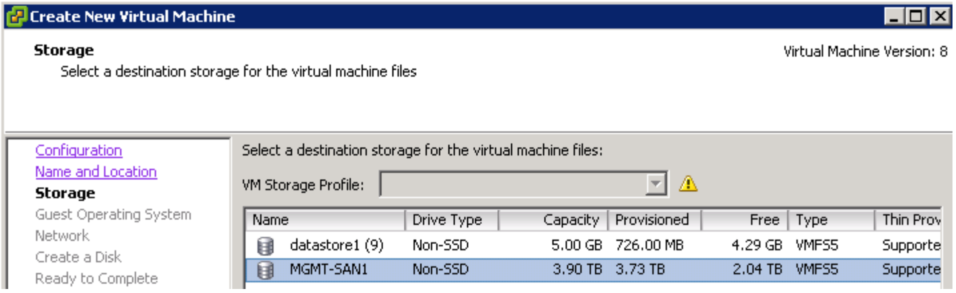
Name: BMA_Test_1

Virtual machine (VM) names may contain up to 80 ch
vCenter Server VM folder.

Inventory Location:

⊟ GSP_MGMT
Discovered virtual machine

Select the location to install your VM.



Create New Virtual Machine

Storage

Select a destination storage for the virtual machine files

Virtual Machine Version: 8

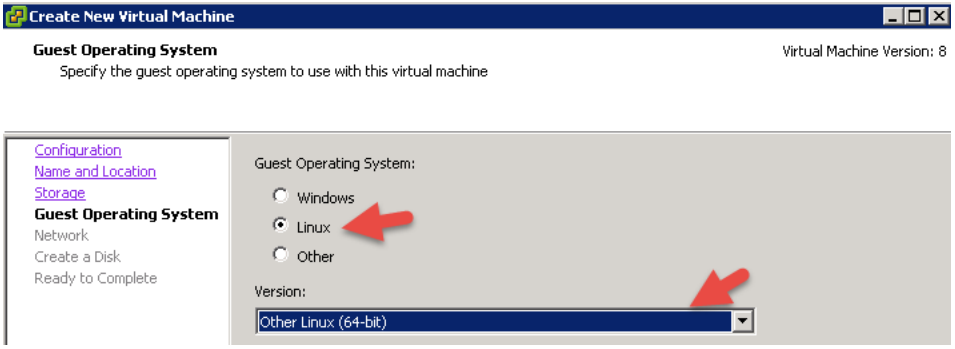
Configuration
Name and Location
Storage
Guest Operating System
Network
Create a Disk
Ready to Complete

Select a destination storage for the virtual machine files:

VM Storage Profile:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Prov
datastore1 (9)	Non-SSD	5.00 GB	726.00 MB	4.29 GB	VMFS5	Supporte
MGMT-SAN1	Non-SSD	3.90 TB	3.73 TB	2.04 TB	VMFS5	Supporte

These parameters really don’t matter for this test so you can leave it default or select something else like I have done here and click Next.



Create New Virtual Machine

Guest Operating System

Specify the guest operating system to use with this virtual machine

Virtual Machine Version: 8

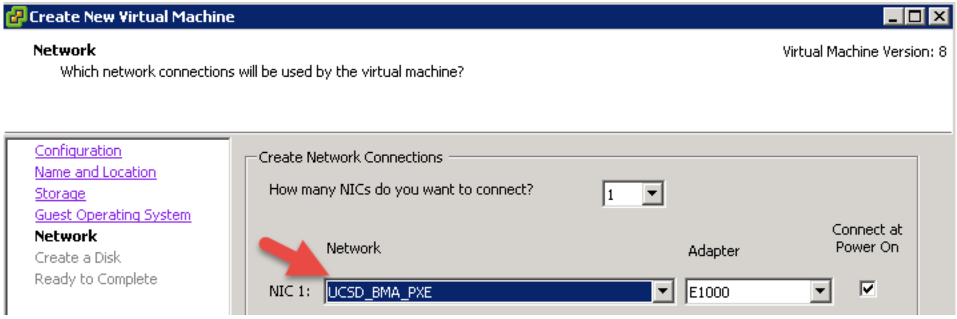
Configuration
Name and Location
Storage
Guest Operating System
Network
Create a Disk
Ready to Complete

Guest Operating System:

○ Windows
● Linux
○ Other

Version: Other Linux (64-bit)

Select the PXE network we defined earlier. **Note**: This VM should be deployed on an ESXi host that has the PXE Port-Group.



Create New Virtual Machine

Network

Which network connections will be used by the virtual machine?

Virtual Machine Version: 8

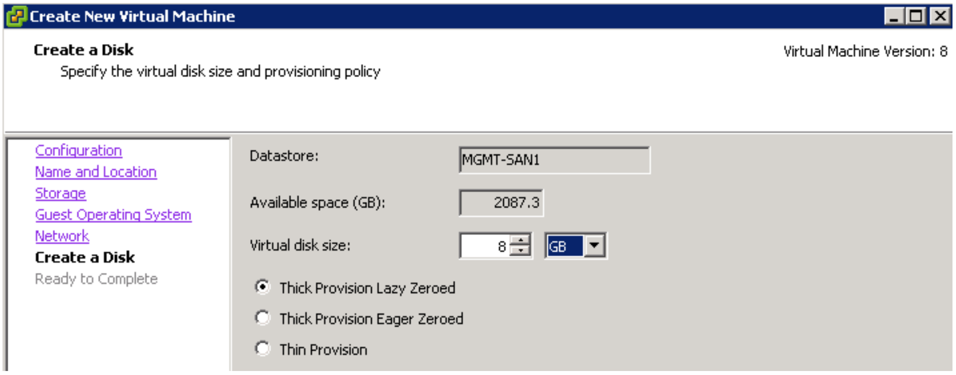
Configuration
Name and Location
Storage
Guest Operating System
Network
Create a Disk
Ready to Complete

Create Network Connections

How many NICs do you want to connect? 1

	Network	Adapter	Connect at Power On
NIC 1:	UCSD_BMA_PXE	E1000	☑

These parameters aren’t important for this test so you can leave default and click Next.



Create New Virtual Machine

Create a Disk
Specify the virtual disk size and provisioning policy

Virtual Machine Version: 8

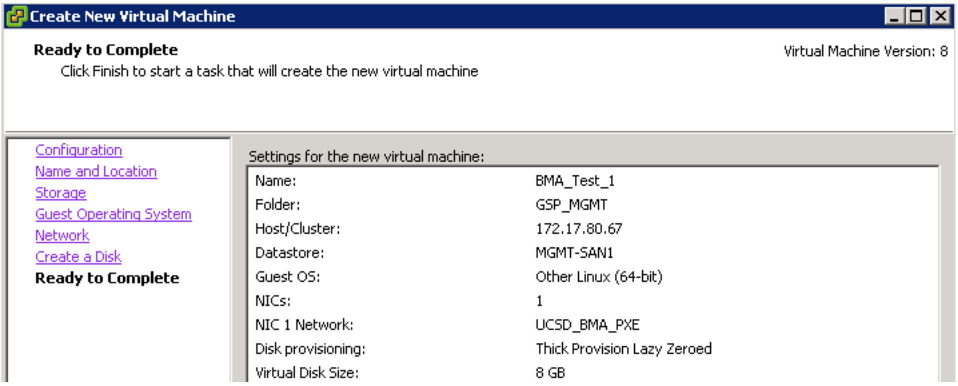
Datastore: MGMT-SAN1

Available space (GB): 2087.3

Virtual disk size: 8 GB

● Thick Provision Lazy Zeroed
○ Thick Provision Eager Zeroed
○ Thin Provision

Verify settings and click Finish.



Create New Virtual Machine

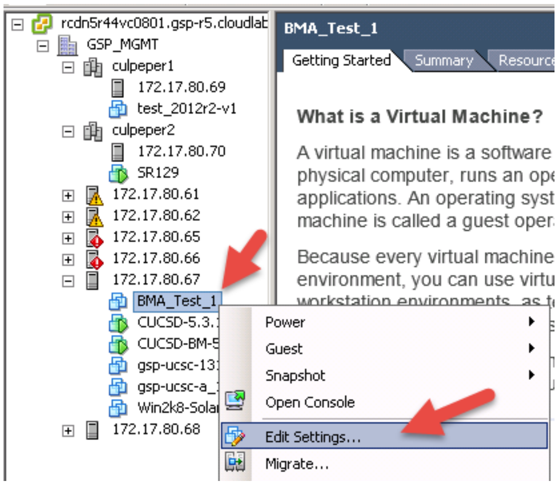
Ready to Complete
Click Finish to start a task that will create the new virtual machine

Virtual Machine Version: 8

Settings for the new virtual machine:

Name:	BMA_Test_1
Folder:	GSP_MGMT
Host/Cluster:	172.17.80.67
Datastore:	MGMT-SAN1
Guest OS:	Other Linux (64-bit)
NICs:	1
NIC 1 Network:	UCSD_BMA_PXE
Disk provisioning:	Thick Provision Lazy Zeroed
Virtual Disk Size:	8 GB

We need to find the MAC address for the VM to setup the PXE for the VM on BMA. To do so, select Edit Settings for the VM.

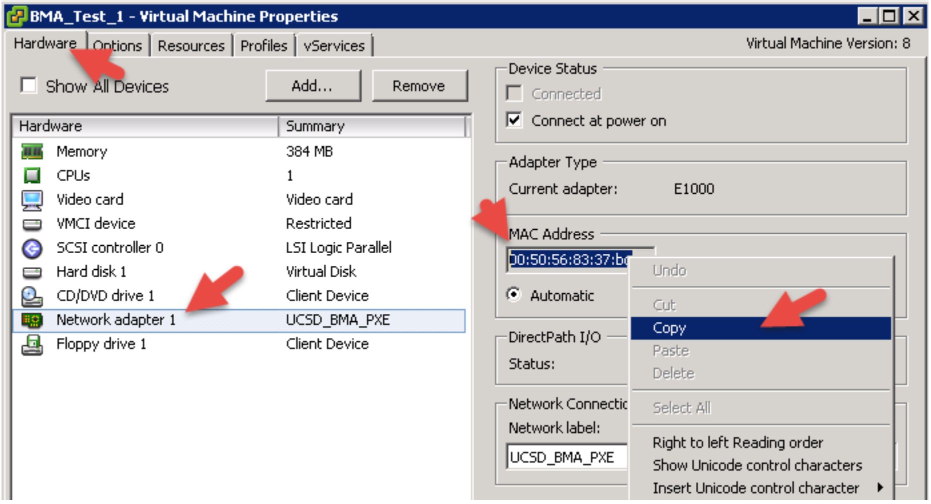


What is a Virtual Machine?

A virtual machine is a software
physical computer, runs an ope
applications. An operating syst
machine is called a guest oper

Because every virtual machine
environment, you can use virtu
workstation environments, as t

Copy the MAC Address.


BMA_Test_1 - Virtual Machine Properties

Hardware	Summary
Memory	384 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
CD/DVD drive 1	Client Device
Network adapter 1	UCSD_BMA_PXE
Floppy drive 1	Client Device

Device Status
□ Connected
☑ Connect at power on

Adapter Type
Current adapter: E1000

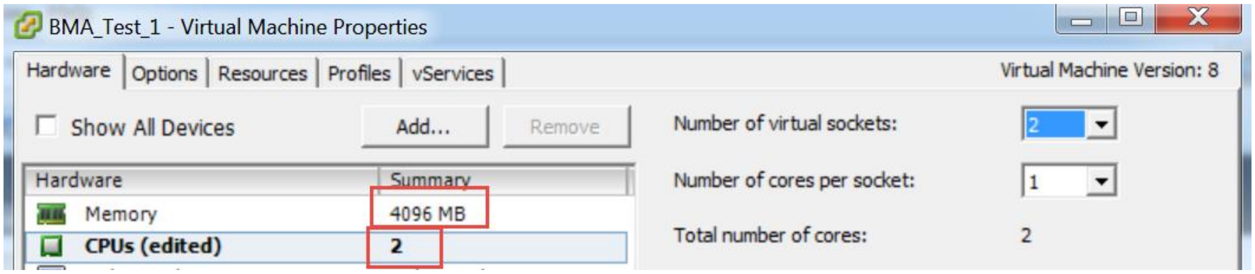
MAC Address
00:50:56:83:37:bc
● Automatic

DirectPath I/O
Status:

Network Connectic
Network label:
UCSD_BMA_PXE

Undo
Cut
Copy
Paste
Delete
Select All
Right to left Reading order
Show Unicode control characters
Insert Unicode control character

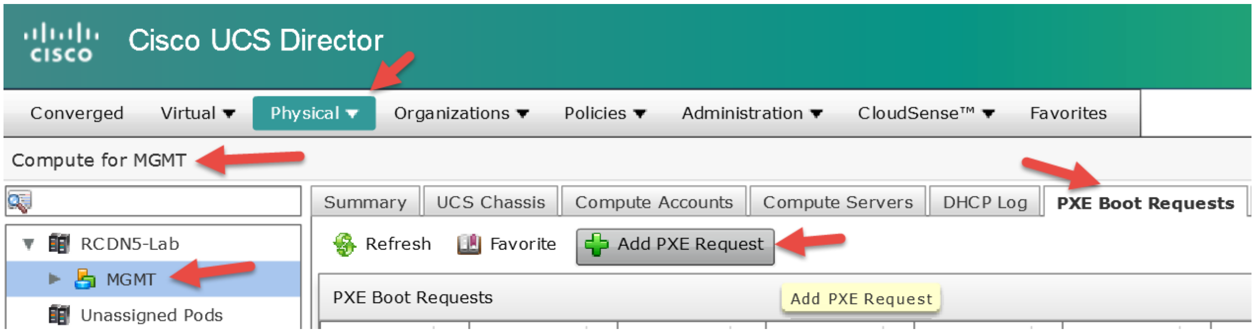
Optional: If you want to see ESXi finish the install at the end of this test, you will need to set a password that meets VMwares password complexity policy, add a Second CPU and add more memory than the default 384MB. The password that we are referring to here is in the PXE Boot Request in UCS Director.


BMA_Test_1 - Virtual Machine Properties

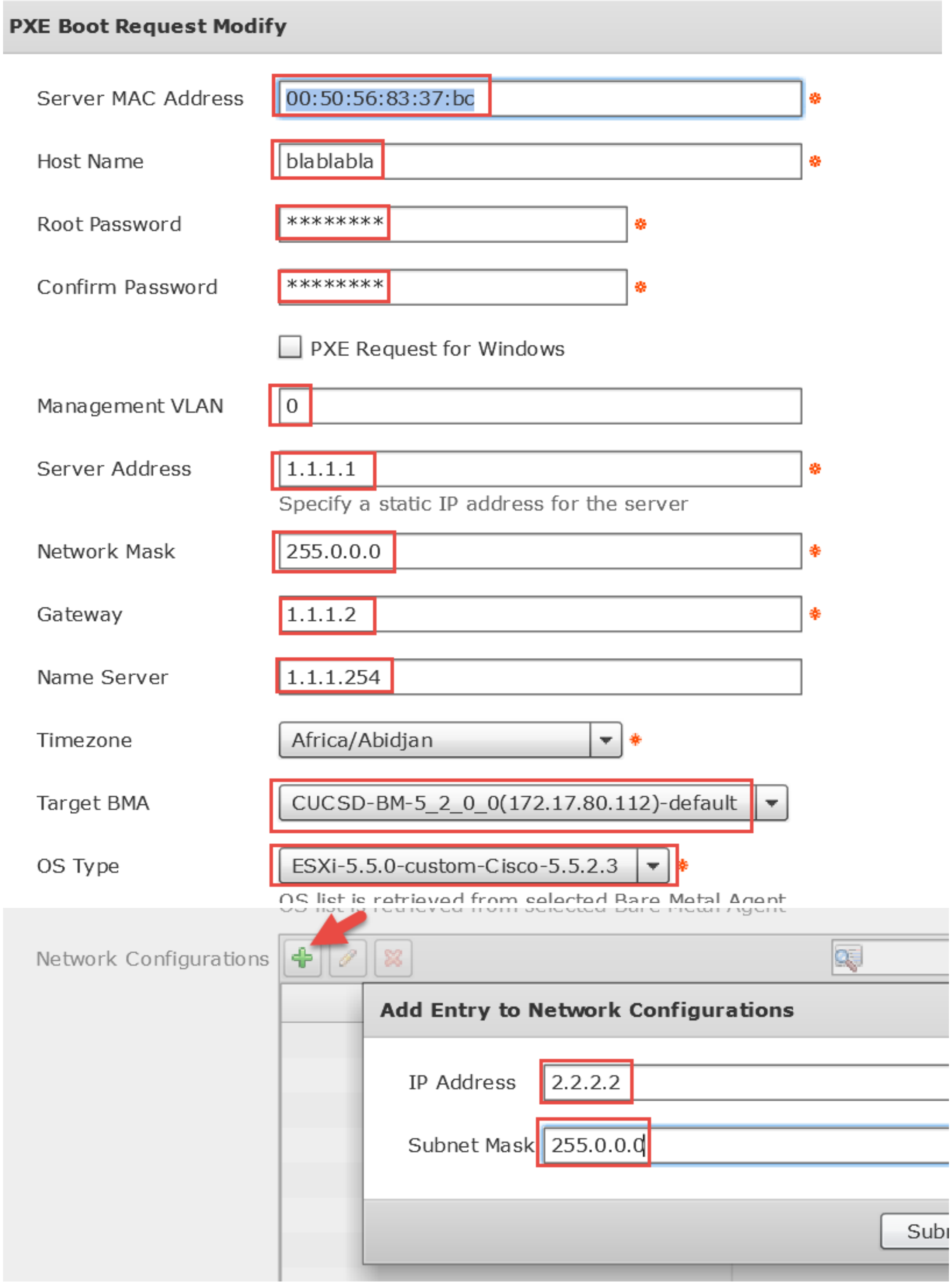
Hardware	Summary
Memory	4096 MB
CPUs (edited)	2

Number of virtual sockets: 2
Number of cores per socket: 1
Total number of cores: 2

Now that the VM has been created and the MAC address has been copied, we need to log into UCS Director and go to Physical -> Compute -> Select your Compute -> PXE Boot Request -> Add PXE Request.



Fill in the PXE Boot Request as follows. **Note**: The most important data here is the Server MAC Address of the VM, and the OS Type. All other fields aren't important and can be filled in with bogus information. Click Submit on the IP field and then Submit again when done.



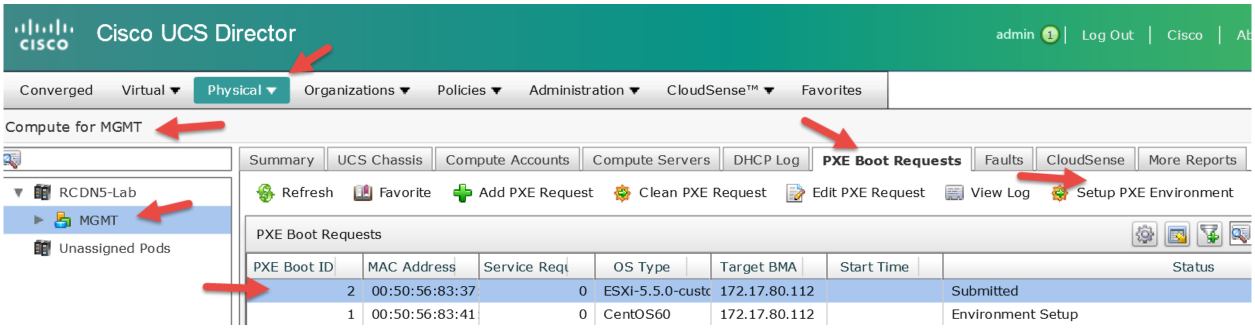
PXE Boot Request Modify

Server MAC Address	00:50:56:83:37:bc *
Host Name	blablabla *
Root Password	******** *
Confirm Password	******** *
	□ PXE Request for Windows
Management VLAN	0
Server Address	1.1.1.1 * Specify a static IP address for the server
Network Mask	255.0.0.0 *
Gateway	1.1.1.2 *
Name Server	1.1.1.254
Timezone	Africa/Abidjan *
Target BMA	CUCSD-BM-5_2_0_0(172.17.80.112)-default
OS Type	ESXi-5.5.0-custom-Cisco-5.5.2.3 * OS list is retrieved from selected Bare Metal Agent
Network Configurations	

Add Entry to Network Configurations

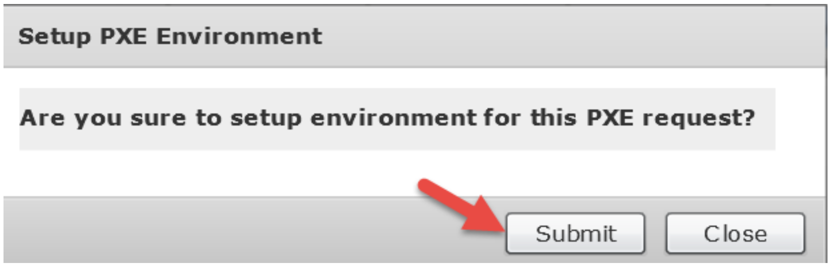
IP Address	2.2.2.2
Subnet Mask	255.0.0.0

Setup PXE Environment.



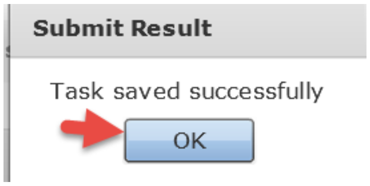
PXE Boot ID	MAC Address	Service Requ	OS Type	Target BMA	Start Time	Status
2	00:50:56:83:37	0	ESXi-5.5.0-custc	172.17.80.112		Submitted
1	00:50:56:83:41	0	CentOS60	172.17.80.112		Environment Setup

Select Submit to confirm the PXE Environment Setup.


Setup PXE Environment

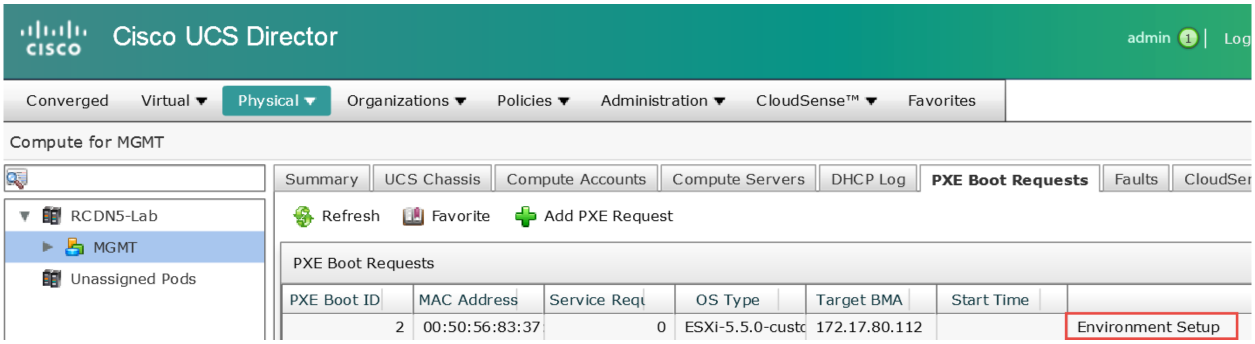
Are you sure to setup environment for this PXE request?

Click OK.


Submit Result

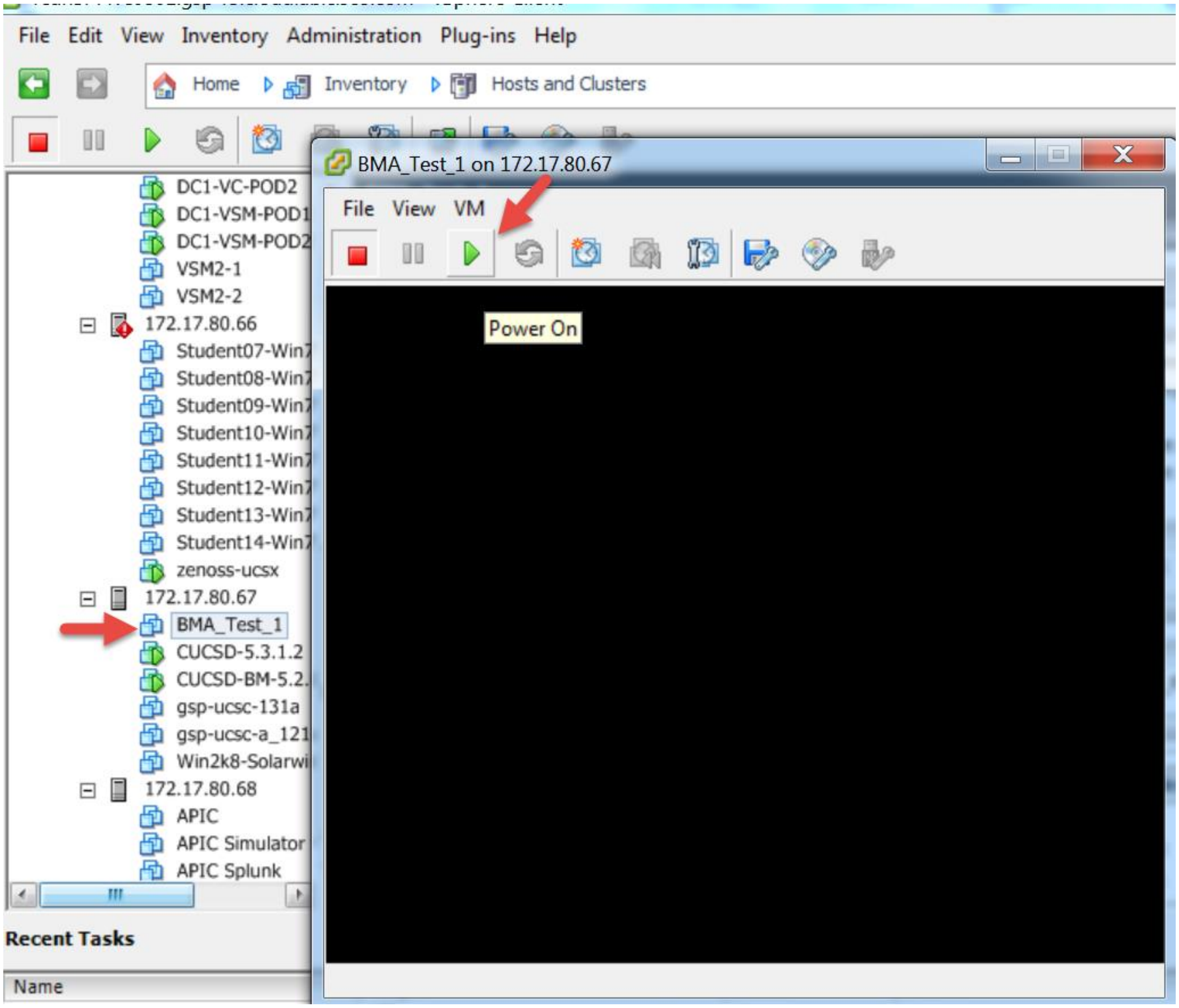
Task saved successfully

Verify Status changes to Environment Setup.

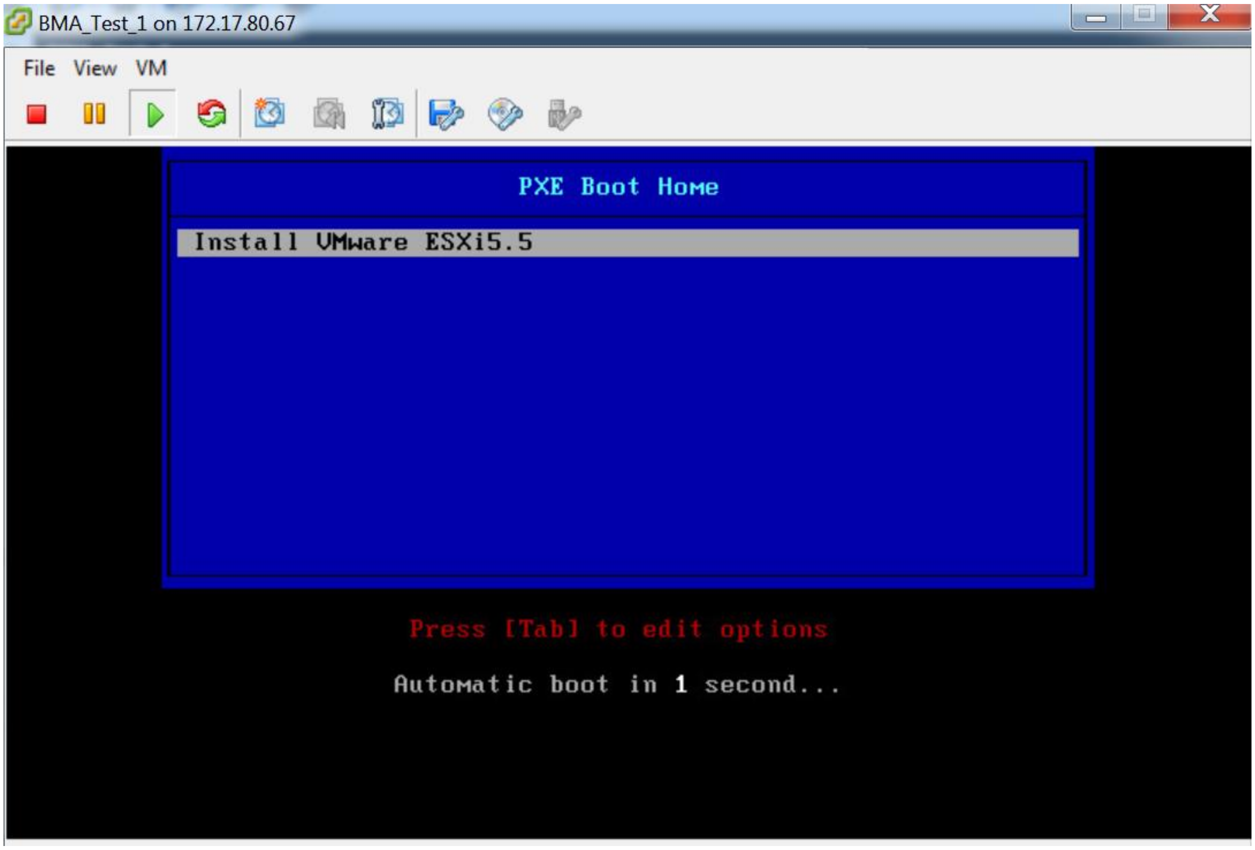


PXE Boot ID	MAC Address	Service Requ	OS Type	Target BMA	Start Time	
2	00:50:56:83:37	0	ESXi-5.5.0-custc	172.17.80.112		Environment Setup

Now go back to vCenter and Open the Console of the BMA test VM and Click Power ON.



Watch the Console to see if the VM Boots from the ISO. As you can see below the VM is booting from ESXi 5.5 ISO. This verifies everything is working as expected. We are done with the testing. We don't need to verify full install of VMware ESXi 5.5 as all we care about is it is booting from PXE Server. You can now power off the VM and delete it. You can also clean up UCS Director by deleting the PXE Boot Request for this MAC Address.

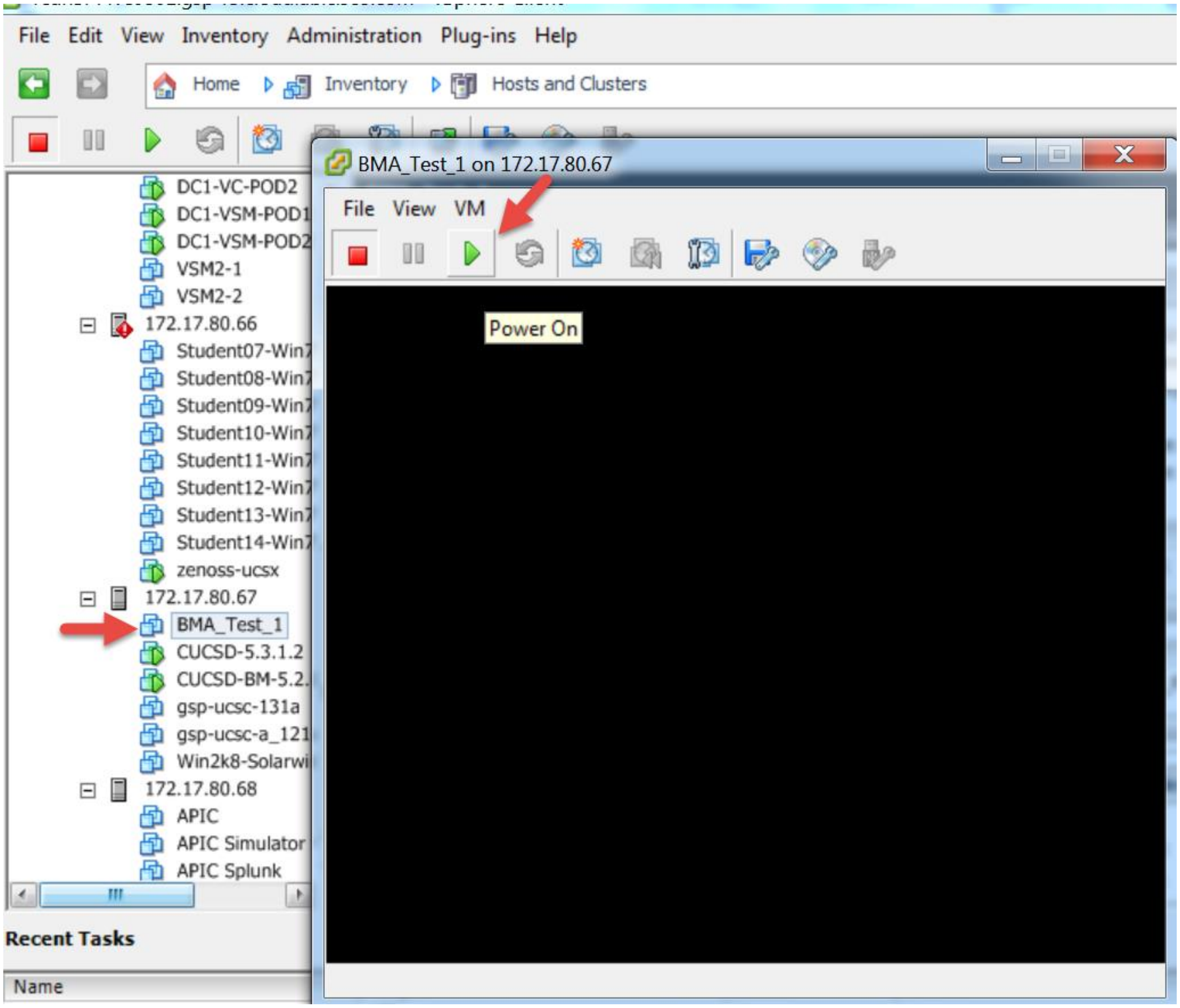


PXE Boot Home

Install VMware ESXi5.5

Press [Tab] to edit options

Automatic boot in 1 second...


File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Hosts and Clusters
DC1-VC-POD2
DC1-VSM-POD1
DC1-VSM-POD2
VSM2-1
VSM2-2
172.17.80.66
Student07-Win7
Student08-Win7
Student09-Win7
Student10-Win7
Student11-Win7
Student12-Win7
Student13-Win7
Student14-Win7
zenoss-ucsx
172.17.80.67
BMA_Test_1
CUCSD-5.3.1.2
CUCSD-BM-5.2.
gsp-ucsc-131a
gsp-ucsc-a_121
Win2k8-Solarwi
172.17.80.68
APIC
APIC Simulator
APIC Splunk
Recent Tasks
Name
BMA_Test_1 on 172.17.80.67
File View VM
Power On