

UCS Director Multi-Node Deployment on VMware

The purpose of this document is to illustrate the steps to install UCS Director 5.4 in a Multi-Node deployment. Instead of a single standalone UCS Director Appliance, we will build a Primary Node, Inventory Database Node, Monitoring Database Node and one or more Service Nodes. A multi-node setup is used to increase scalability by offloading some of the system tasks such as inventory data collection tasks from the primary node to one or more service nodes.

Besides the basic Multi-Node installation, this document also provides steps for configuring other, optional but recommended, management options such as License Installation, Mail Setup, Self Service Policy, NTP, enable root access, change root password, change shelladmin password, change hostname, update hosts file, and changing the time zone. This document should take you to the point where you are ready to start configuring workflows.

Recommendations/Requirements

Best practices recommends to place the service nodes close to the physical and virtual infrastructure and associate the relevant system tasks to those service nodes to offload the work locally to the remote site. However, through testing on a real Nationwide deployment with real latencies, we discovered the performance was horrible in this architecture/design. At a minimum, it took twice the time to run system tasks such as Inventory data collection, than running the system task locally on the primary node or a service node that is local to the primary node. I suggest placing all of your service nodes in the same physical location as the Primary Node, Inventory Database Node, and Monitoring Database Nodes.

The Inventory and Monitoring Database Nodes require 50MB/s writes at 4k block size to the datastore in which these VMs will be installed on. The Primary and Service Nodes require 25MB/s writes at 4k block size to the datastore in which these VMs will reside on. The command to test these performance requirements are documented in the troubleshooting section of this document. At a minimum, you will need some high performance local SSDs to achieve these requirement.

Useful Documents

[Cisco UCS Director Multi-Node Installation and Configuration Guide, Release 5.4](#)

[Cisco UCS Director Installation on VMware vSphere, Release 5.4](#)

[Cisco UCS Director Administration Guide, Release 5.4](#)

[Cisco UCS Director Compatibility Matrix, Release 5.4](#)

[Cisco UCS Director Release Notes, Release 5.4](#)

Table of Contents

Table of Contents	2
1. Download UCS Director 5.4 software from Cisco.com	4
2. Create the Inventory Database Node	5
2.1. Create Inventory Database VM.....	5
2.2. Install/Update VMWare tools & VM Version.....	11
2.3. Configure Inventory Database	18
3. Create the Monitoring Database Node.....	23
3.1. Create Monitoring Database VM	23
3.2. Install/Update VMWare tools & VM Version.....	29
3.3. Configure Monitoring Database.....	36
4. Create the Primary Node	41
4.1. Create Primary Node VM	41
4.2. Install/Update VMWare tools & VM Version.....	47
4.3. Configure Primary Node.....	54
5. Create the Service Node	59
5.1. Create Service Node VM	59
5.2. Install/Update VMWare tools & VM Version.....	65
5.3. Configure Service Node.....	72
6. Add Physical, Virtual Accounts and Prerequisites.....	78
6.1. Configure Prerequisites.....	78
6.1.1. Add a Site	78
6.1.2. Hide the Default POD.....	79
6.1.3. Add a POD	80
6.2. Add Physical Accounts	81
6.2.1. Optional – Create UCSM Credential Policy	81
6.2.2. Add UCSM Account	82
6.2.3. Optional - Create NetApp Credential Policy	84
6.2.4. Add NetApp Account for Controller A	85
6.2.5. Add NetApp Account for Controller B.....	87
6.2.6. Optional - Create MDS Credential Policy	89
6.2.7. Add Fabric A MDS	90
6.2.8. Add Fabric B MDS.....	91
6.3. Add a Virtual Account for vCenter	92

- 6.3.1. Optional - Create vCenter Credential Policy 92
- 6.3.2. Add vCenter Virtual Account 93
- 7. System Tasks 95
 - 7.1. Create a Node Pool 95
 - 7.2. Create System Task Policy..... 97
 - 7.3. Create Service Node..... 98
 - 7.4. Assign System Policy to UCSM System Task 101
 - 7.5. Assign System Policy to NetApp Controller A System Task 104
 - 7.6. Assign System Policy to NetApp Controller B System Task..... 105
 - 7.7. Assign System Policy to vCenter System Task..... 106
- 8. Add Licenses to UCS Director 109
- 9. Mail Setup (Required) 111
- 10. Create Self Service Policy 112
- 11. Optional - Troubleshooting Service Node Connectivity..... 114
 - 11.1. IP Connectivity Troubleshooting..... 114
 - 11.2. Storage Performance Troubleshooting..... 116
 - 11.3. Determine if Service Node is UP and how long it took to come UP 116
 - 11.4. Verify if Task are taking longer than the Frequency configured..... 117
 - 11.5. Obtaining Logs from UCS Director 118

1. Download UCS Director 5.4 software from Cisco.com

Go to Cisco.com Downloads and navigate to UCS Director 5.4.

Download Software

Download Cart (0 items) [Feedback](#) [Help](#)

[Downloads Home](#) > [Products](#) > [Servers - Unified Computing](#) > [UCS Director](#) > [UCS Director 5.4](#) > [UCS Director Virtual Appliance Software-5](#)

UCS Director 5.4

Search...

[Expand All](#) | [Collapse All](#)

▼ Latest **5**

▼ All Releases

▶ 5

Release 5 [Add Device](#)
[Add Notification](#)

Cisco UCS Director 5.4 0.0 Cloupia Script Code Samples

File Information	Release Date	Size	
Cisco UCS Director 5.4 (VMWare vSphere OVF Appliance. MD5 Checksum - 5543 01a744551be95205c65004c81973) CUCSD_5_4_0_0_VMWARE_GA.zip	05-NOV-2015	4407.23 MB	Download Add to cart Publish

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](#)

[Login](#) [Cancel](#)

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](#)

[Accept License Agreement](#) [Cancel](#)

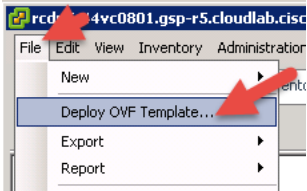
2. Create the Inventory Database Node

2.1. Create Inventory Database VM

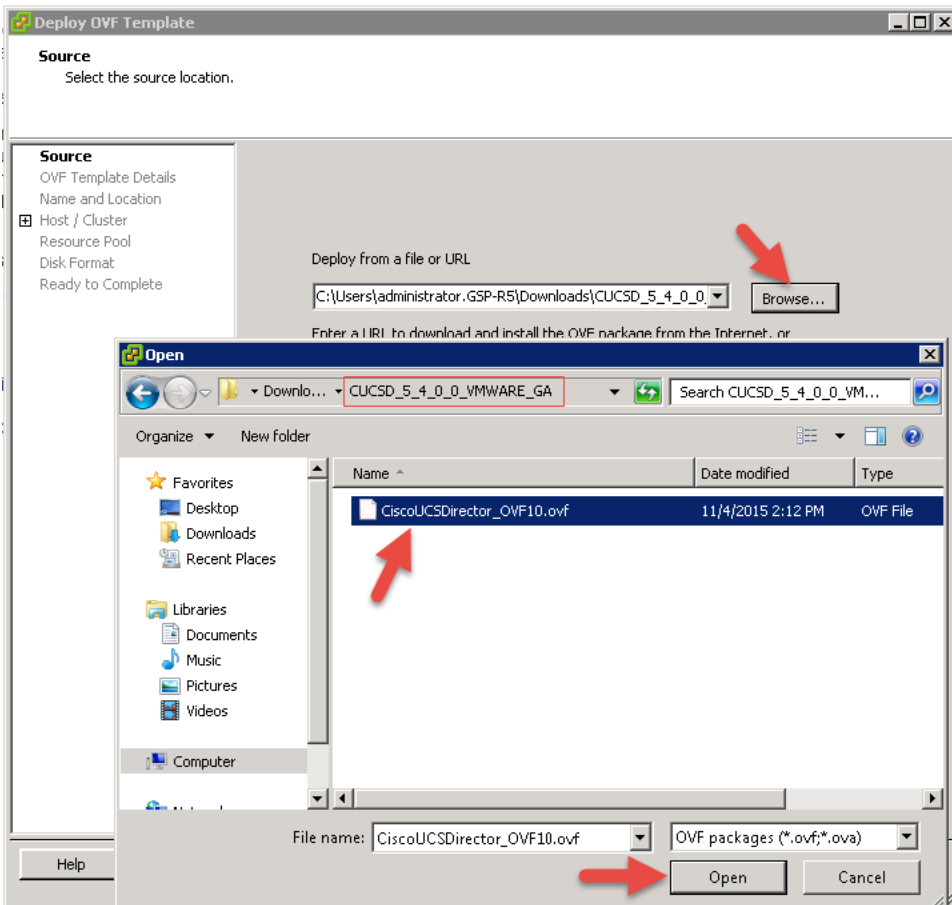
Extract/Unzip the “CUCSD_5_4_0_0_VMWARE_GA” file that was downloaded from Cisco.com to your local machine.

Note: The default windows or winzip may have an issue extracting the file and you may need to use a different extraction tool. I used 7-Zip to extract mine and can be found here: <http://7-zip.org/download.html>

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



Browse to the “CiscoUCSDirector_OVF10.ovf”, select it for deployment then click ‘Next’.



Verify details and click 'Next'.

The screenshot shows the 'Deploy OVF Template' window with the 'OVF Template Details' section selected. The window title is 'Deploy OVF Template'. Below the title bar, it says 'OVF Template Details' and 'Verify OVF template details.' The main content area is divided into a left sidebar and a main pane. The sidebar contains a tree view with the following items: Source, OVF Template Details (selected), End User License Agreement, Name and Location, Host / Cluster, Resource Pool, Disk Format, Properties, and Ready to Complete. The main pane displays the following details:

Product:	CUCSD-5.4.0.0
Version:	5.4.0.0
Vendor:	Cisco Systems
Publisher:	No certificate present
Download size:	4.3 GB
Size on disk:	7.6 GB (thin provisioned) 100.0 GB (thick provisioned)
Description:	Cisco UCS Director 5.4.0.0 (Emerald Bay)

Below the description, there is a note: 'Note: It is mandatory to reserve vCPU and Memory as recommended by Installation and Deployment guide.'

Accept the license agreement and click 'Next'.

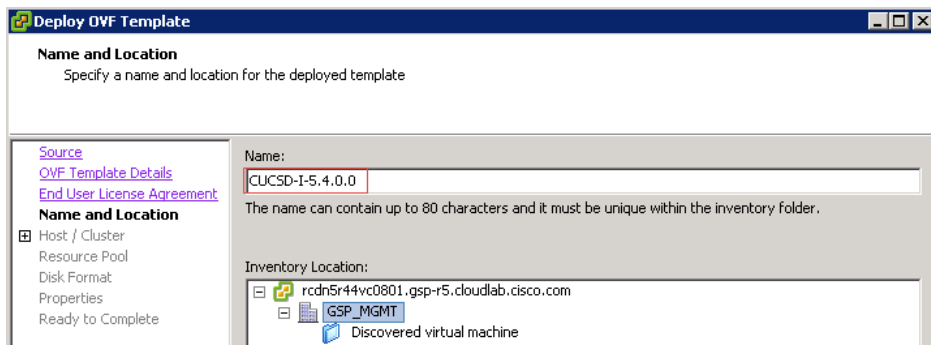
The screenshot shows the 'Deploy OVF Template' window with the 'End User License Agreement' section selected. The window title is 'Deploy OVF Template'. Below the title bar, it says 'End User License Agreement' and 'Accept the end user license agreements.' The main content area is divided into a left sidebar and a main pane. The sidebar contains a tree view with the following items: Source, OVF Template Details, End User License Agreement (selected), Name and Location, Storage, Disk Format, Network Mapping, Properties, and Ready to Complete. The main pane displays the following text:

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.

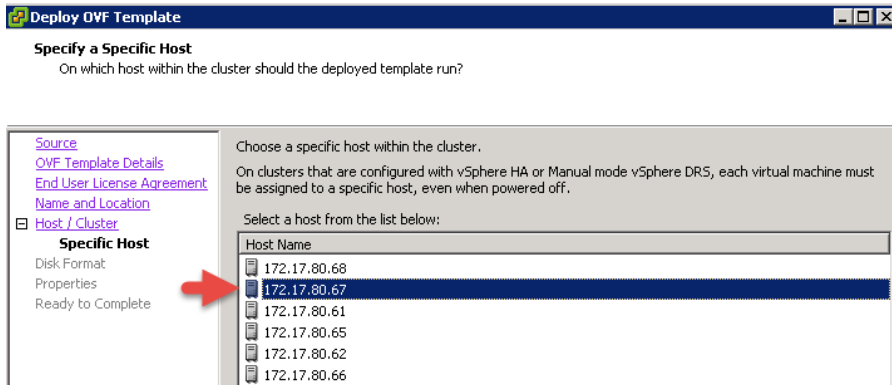
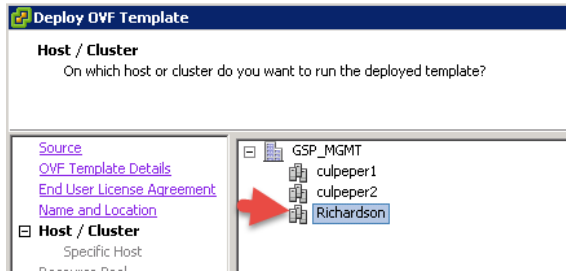
CISCO SYSTEMS, INC. OR ITS AFFILIATE LICENSING THE SOFTWARE ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS 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,

At the bottom of the main pane, there is an 'Accept' button with a red arrow pointing to it. Below the main pane, there are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button.

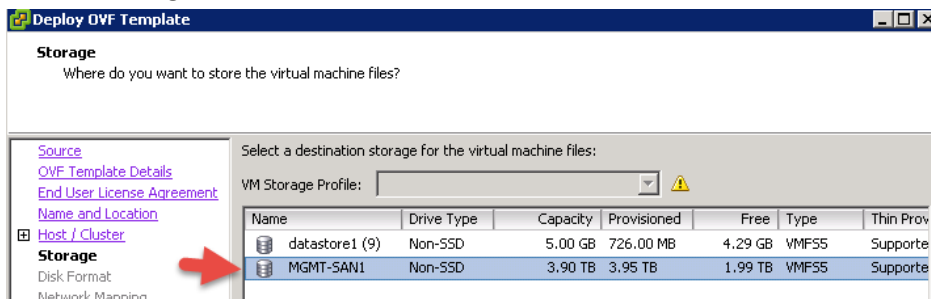
Name the VM and click 'Next'.



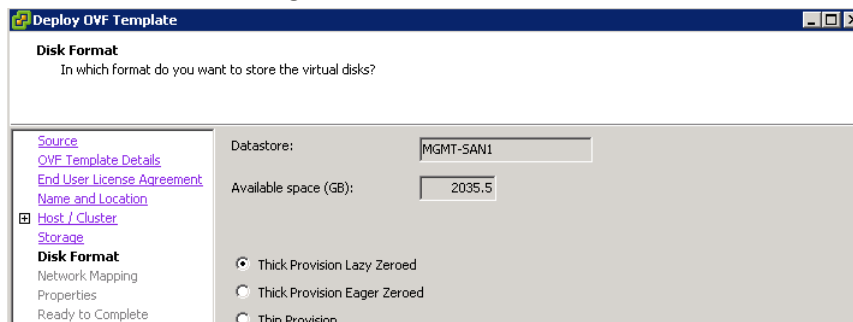
Select Cluster/Host to deploy this VM on and click 'Next'.



Select a storage location to install the VM and click 'Next'.



Leave the default settings for the Disk Format and click 'Next'.



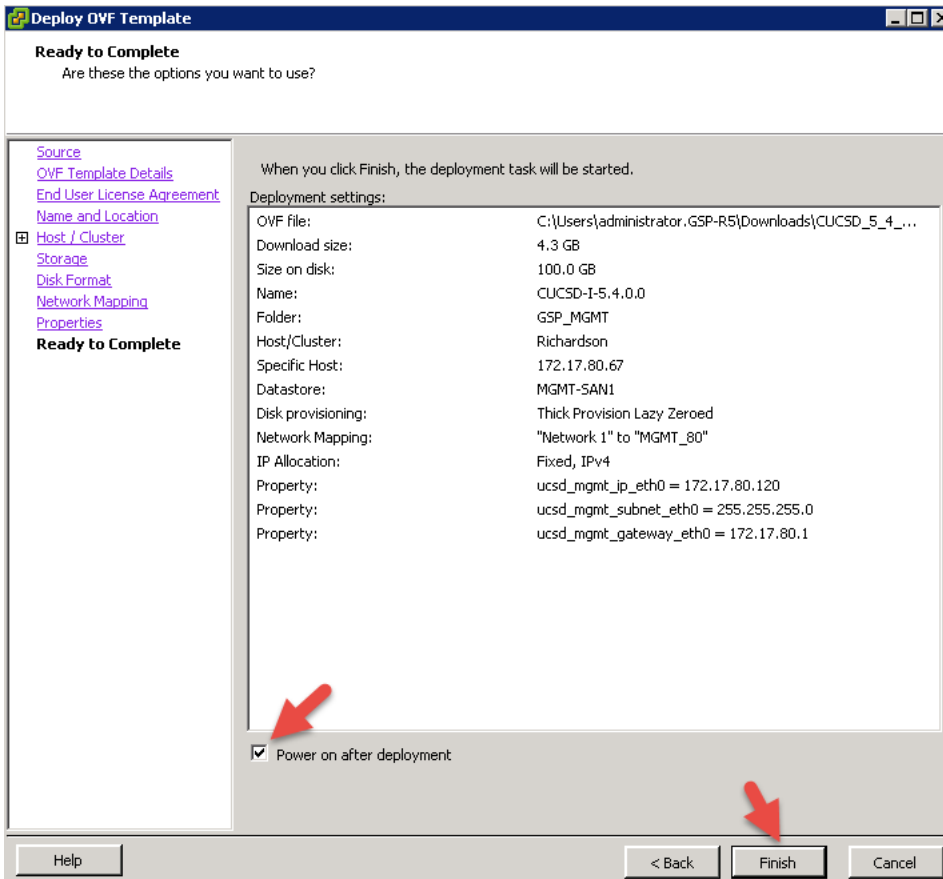
Select the Network to put this VM on and click 'Next'.

The screenshot shows the 'Deploy OVF Template' window with the 'Network Mapping' step selected. The title bar reads 'Deploy OVF Template'. Below the title bar, the text 'Network Mapping' is followed by the question 'What networks should the deployed template use?'. On the left, a navigation pane lists several options: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location', 'Host / Cluster' (which is selected and highlighted with a blue background), and 'Storage'. The main area contains the instruction 'Map the networks used in this OVF template to networks in your inventory'. Below this is a table with two columns: 'Source Networks' and 'Destination Networks'. The table contains one row with 'Network 1' in the 'Source Networks' column and 'MGMT_80' in the 'Destination Networks' column. Both 'Network 1' and 'MGMT_80' are enclosed in red rectangular boxes.

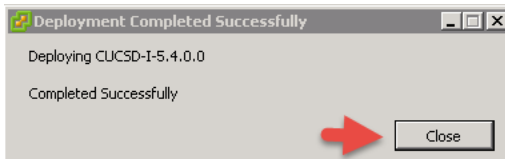
Enter a password for Root and Shelladmin Accounts, Management IP Address, Subnet Mask, Gateway and click 'Next'.

The screenshot shows the 'Deploy OVF Template' window with the 'Properties' step selected. The title bar reads 'Deploy OVF Template'. Below the title bar, the text 'Properties' is followed by the instruction 'Customize the software solution for this deployment.'. On the left, a navigation pane lists several options: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location', 'Host / Cluster', 'Storage', 'Disk Format', 'Network Mapping', 'Properties' (which is selected and highlighted with a blue background), and 'Ready to Complete'. The main area is titled 'Application' and contains several sections for configuration. Each section has a title and a description, followed by input fields. The 'Root Password' section has two fields: 'Enter password' and 'Confirm password', both containing '*****'. The 'Shelladmin Password' section has two fields: 'Enter password' and 'Confirm password', both containing '*****'. The 'Management IP Address' section has a description 'Enter Management IP Address for eth0. Set 0.0.0.0 to use DHCP' and a field containing '172 . 17 . 80 . 120'. The 'Management IP Subnet Mask' section has a description 'Enter Management IP Subnet Mask for eth0. Set 0.0.0.0 to use DHCP' and a field containing '255 . 255 . 255 . 0'. The 'Gateway IP Address' section has a description 'Gateway IP Address' and a field containing '172 . 17 . 80 . 1'. At the bottom of the window, there are three buttons: 'Help', '< Back', and 'Next >', and 'Cancel'. A red arrow points to the 'Next >' button.

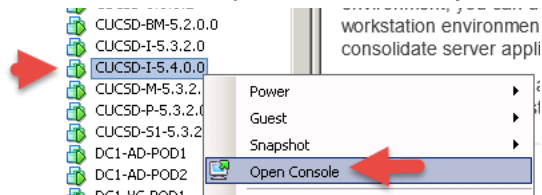
Select Power on after deployment and click **'Finish'**.



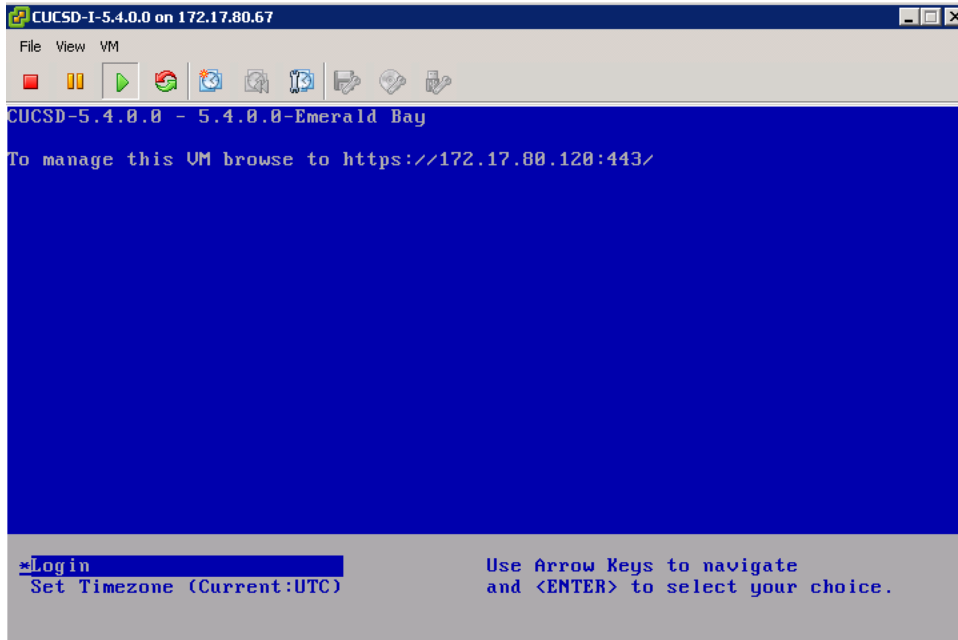
After deployment click **'Close'**.



Select the Inventory VM and select **'Open Console'**.

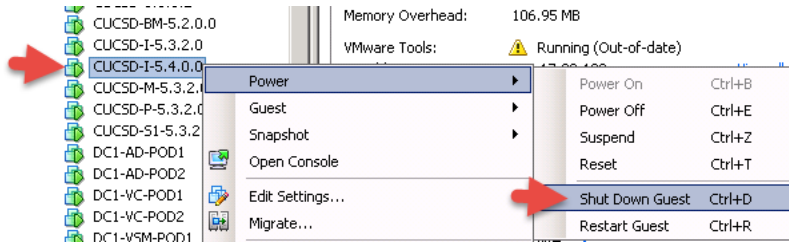


Monitor the console until the installation is complete and you will see a screen similar to the one below. The installation will take several minutes to complete so be patient.

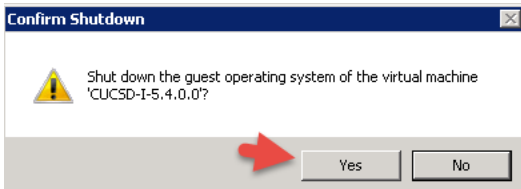


2.2. Install/Update VMWare tools & VM Version

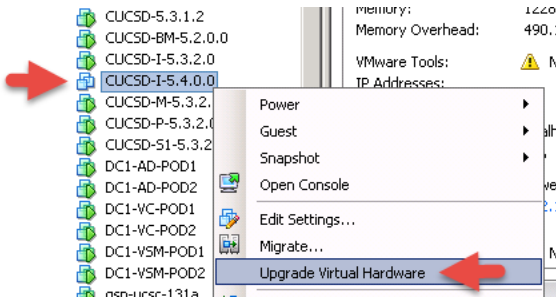
Navigate to the Inventory Database VM and select **'Shut Down Guest'**.



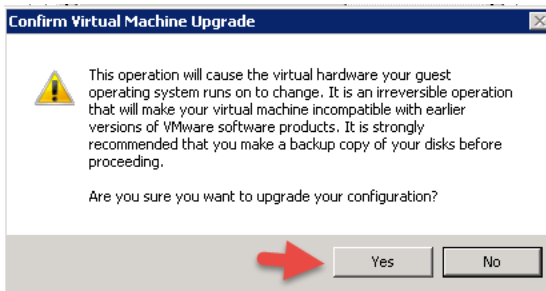
Select **'Yes'**.



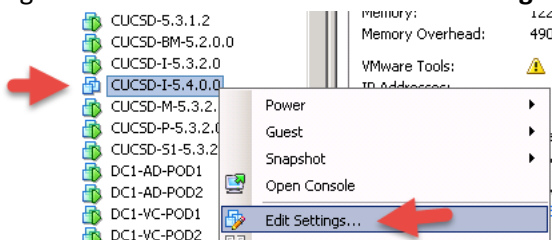
Wait for the VM to completely shut down then right click on the VM and select **'Upgrade Virtual Hardware'**.



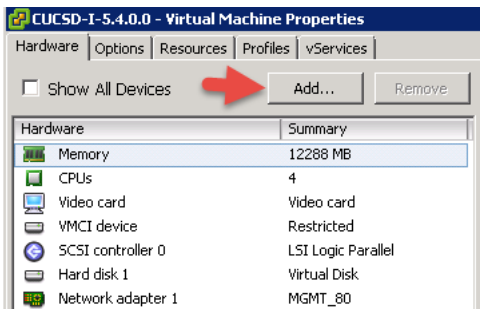
Select **'Yes'**.



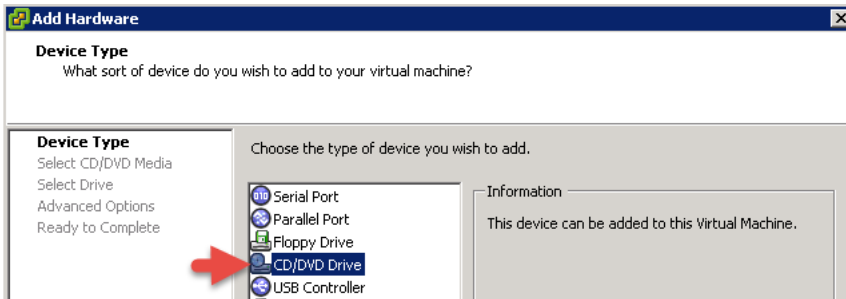
Right click on the VM and Select **'Edit Settings'**.



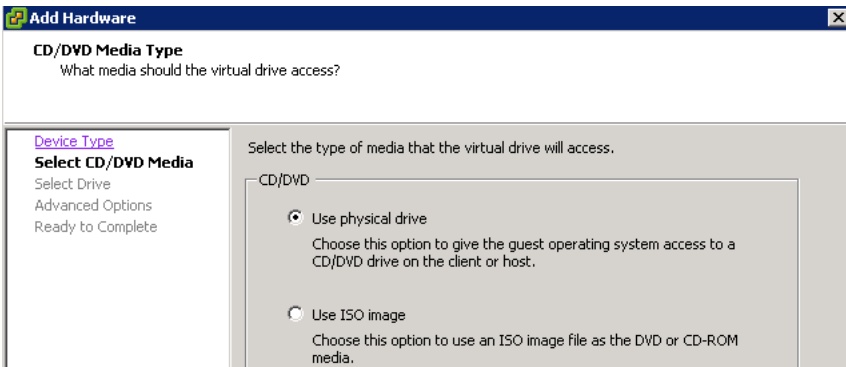
Click 'Add'.



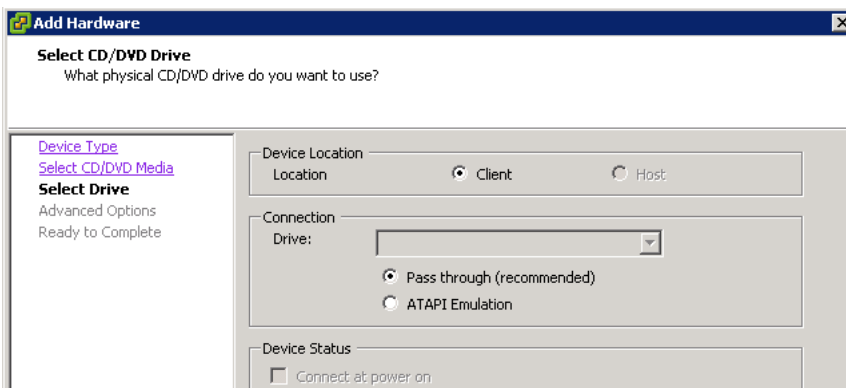
Select 'CD/DVD Drive' and click 'Next'.



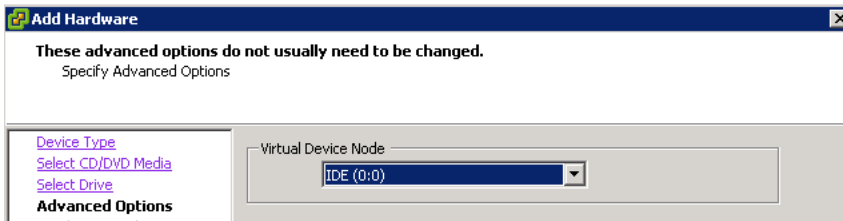
Leave default 'Use physical drive' and click 'Next'.



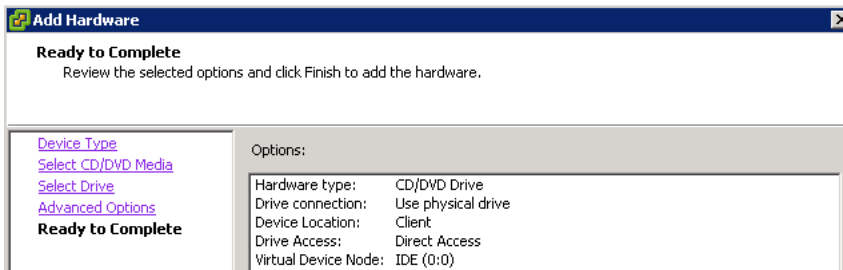
Leave default and click 'Next'.



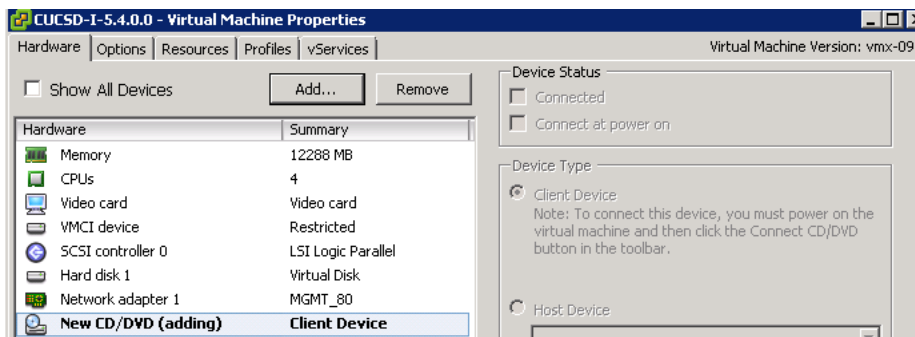
Leave default and click 'Next'.



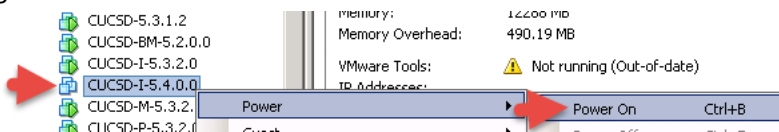
Review and click 'Finish'.



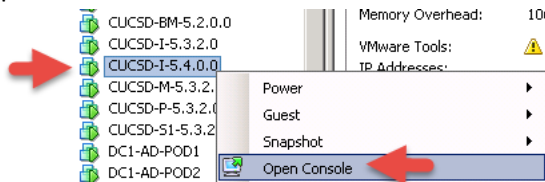
Review and click 'OK'.



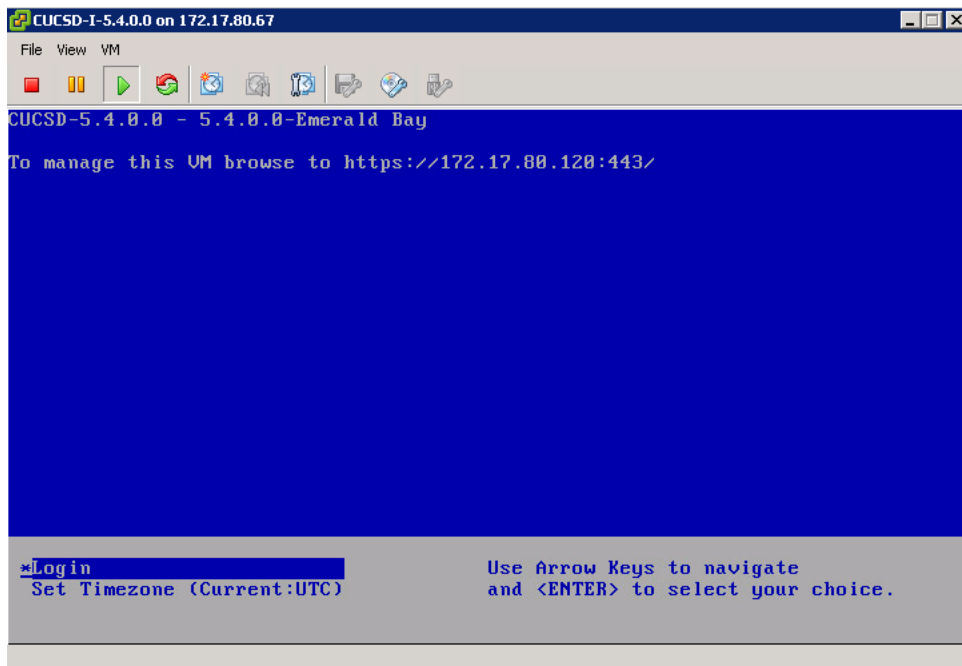
Right click on the VM and select 'Power On'.



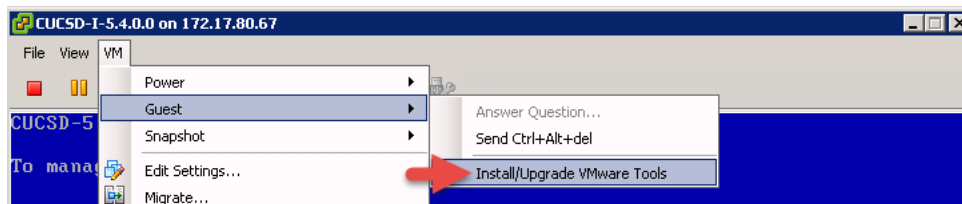
Open the VM Console to watch the VM Boot. Right click on the VM and select 'Open Console'.



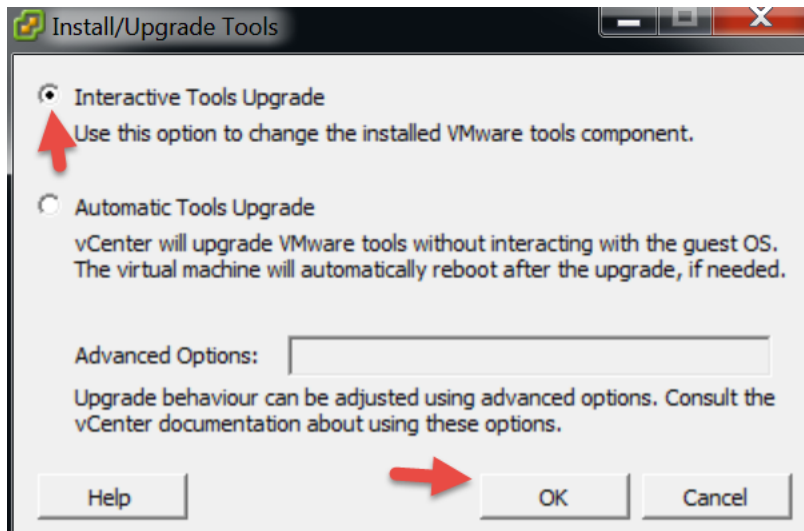
Once the VM is completely up, you should see the login screen similar to below.



From the console, select 'Install/Upgrade VMware Tools'.



Select 'Interactive Tools Upgrade' and click 'OK'.



SSH to the Inventory Database Node and login using the root account.

- Make a dir for cdrom: `'mkdir /mnt/cdrom'`
- Mount the cdrom: `'mount /dev/cdrom /mnt/cdrom'`
- Copy vmware install to /tmp: `'cp /mnt/cdrom/VMwareTools-5.0.0-<xxxx>.tar.gz /tmp/'` **Note:** tab out the VMware tools part so you don't have to figure out the correct name.
- Unzip the files in /tmp: `'tar xzf /tmp/VMwareTools-5.0.0-<xxxx>.tar.gz'` **Note:** tab out the VMware tools part so you don't have to figure out the correct name.
- Change directory: `'cd vmware-tools-distrib'`
- Run the install: `'./vmware-install.pl'`
- Accept all the defaults by Pressing Enter for all the options.

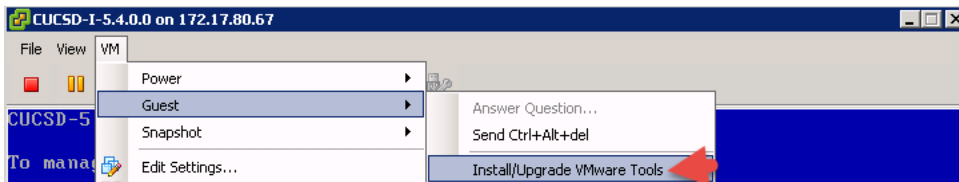
Note: You will probably get the following message.

VMware Tools cannot be installed, since they have already been installed using a package-based mechanism (rpm or deb) on this system. If you wish to continue, you must first remove the currently installed VMware Tools using the appropriate packaged-based mechanism, and then restart this installer
Execution aborted.

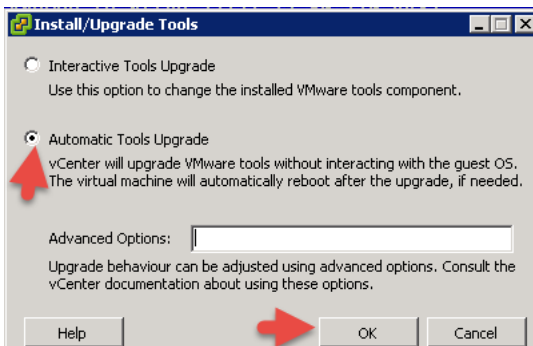
Found VMware Tools CDROM mounted at /mnt/cdrom. Ejecting device /dev/cdrom ... No eject (or equivalent) command could be located. Eject Failed: If possible manually eject the Tools installer from the guest cdrom mounted at /mnt/cdrom before canceling tools install on the host.

- If you get this message, we need to Delete the VMware tools directory: `'rm -rf /usr/lib/vmware-tools/'`
- Change directory: `'cd vmware-tools-distrib/'`
- Re-Run the install: `'./vmware-install.pl'`
- Enter **'Yes'** to the 'Would you like to remove the install DB?' You will probably get a Failure and Execution aborted.
- Re-Run the install: `'./vmware-install.pl'`
- Accept all the defaults by Pressing Enter for all the options.

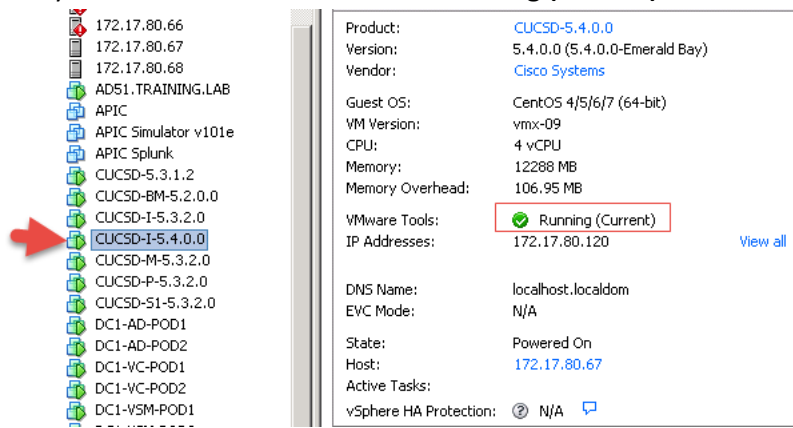
From the console, select **'Install/Upgrade VMware Tools'**.



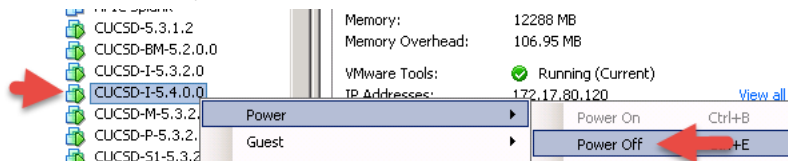
Select **'Automatic Tools Upgrade'** and click **'OK'**.



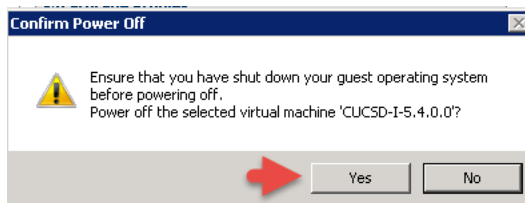
Verify Tools have been installed and **'Running (Current)'** as shown below.



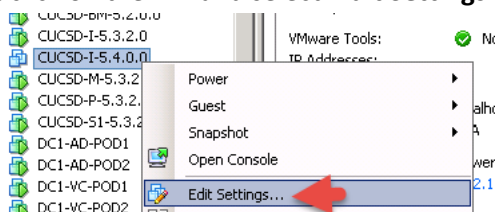
Power off the VM, **'Power Off'**.



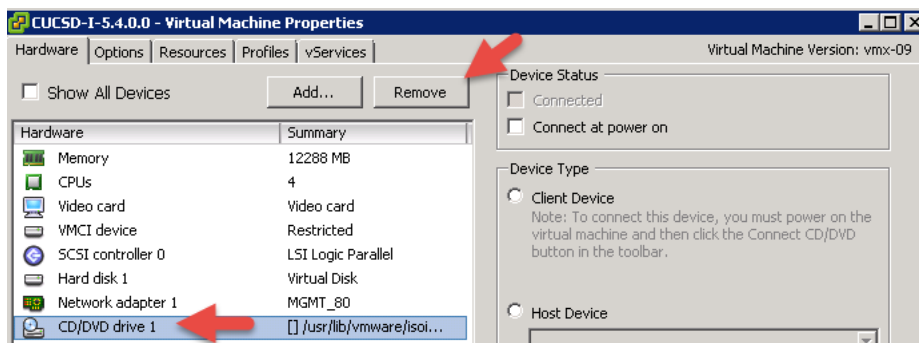
Select **'Yes'**.



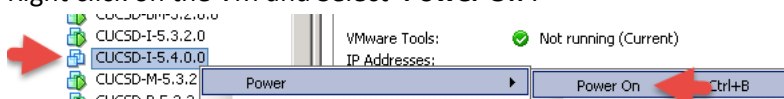
Right click on the VM and select **'Edit Settings'**.



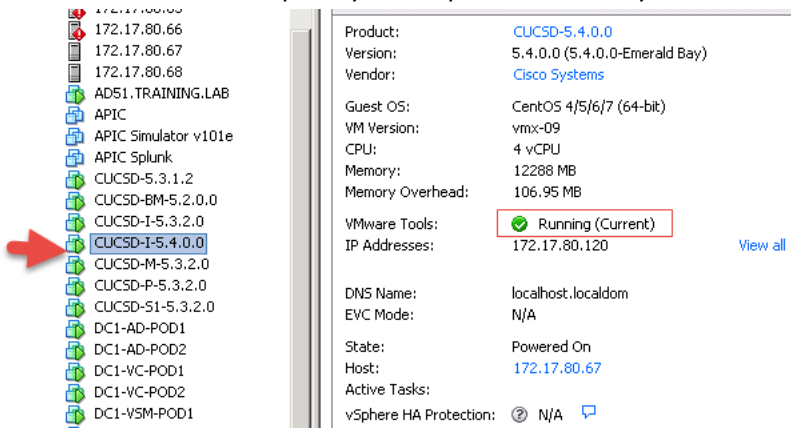
Select **'CD/DVD drive 1'**, click **'Remove'** and then click **'OK'**.



Right click on the VM and Select **'Power On'**.



Wait for the VM to completely boot up and then verify Tools have been installed and 'Running (Current)'.



The image shows a vSphere interface with a list of VMs on the left and a details pane on the right. A red arrow points to the VM 'CUCSD-I-5.4.0.0' in the list. The details pane for this VM shows the following information:

Product:	CUCSD-5.4.0.0
Version:	5.4.0.0 (5.4.0.0-Emerald Bay)
Vendor:	Cisco Systems
Guest OS:	CentOS 4/5/6/7 (64-bit)
VM Version:	vmx-09
CPU:	4 vCPU
Memory:	12288 MB
Memory Overhead:	106.95 MB
VMware Tools:	Running (Current)
IP Addresses:	172.17.80.120 View all
DNS Name:	localhost.localdom
EVC Mode:	N/A
State:	Powered On
Host:	172.17.80.67
Active Tasks:	
vSphere HA Protection:	N/A

2.3. Configure Inventory Database

SSH to the Inventory Database Node using the shelladmin account.

Configure NTP Server. From the Menu select 9 'Time Sync'. Replace the NTP IP Address with your NTP Server.

```
SELECT> 9
Time sync.....
System time is Fri Nov 6 02:19:24 UTC 2015
Hardware time is Fri 06 Nov 2015 02:19:25 AM UTC -0.656583 seconds
Do you want to sync systemtime [y/n]? y
System time reset to hardware clock
Do you want to sync to NTP [y/n]? y
Enter NTP server to sync time with: 173.37.102.254
ntpd (pid 1868) is running...
Shutting down ntpd: [ OK ]
6 Nov 02:19:42 ntpdate[3631]: adjust time server 173.37.102.254 offset 0.001981 sec
Synchronized time with NTP server '173.37.102.254'
Added NTP server '173.37.102.254' to /etc/ntp.conf
Starting ntpd: [ OK ]
synchronized to NTP server (173.37.102.254) at stratum 6
time correct to within 7940 ms
polling server every 64 s
Press return to continue ...
```

From the menu, choose (24) 'Configure Multi Node Setup (Advanced Deployment)' and press Enter.

- Enter '1' to configure the current node.
- Enter 'y' when asked if you want to configure multi node setup.
- Enter 'c' to Configure the node as Inventory DB.
- Enter 'y' when asked if you asked if you want to configure this node as an Inventory Database.
- Enter 'y' when asked about re-initializing the database.
- When prompted to logout, enter 'y' and press enter. Log back in as shelladmin by entering 'su shelladmin'

```
SELECT> 24
*****
This wizard helps to do Multi Node setup
*****
Configuration Options :
Current Node --> select '1'
Remote Node  --> select '2'
exit         --> select '3'

Please enter an option: 1
*****
Cisco UCS Director Multi Node Setup requires multiple instances of UCS Director OVF deployed with differen
t configurations. Following are the required configurations:

* UCS Director Primary Node (1 Instance) . This node also acts as a front end UI node
* UCS Director Service Node (1 or more instances ). Service node can be reconfigured as Primary Node when
necessary.
* UCS Director Inventory DB Node (1 Instance)
* UCS Director Monitoring DB Node (1 Instance)

Refer to UCS Director documentation for additional details on Multi Node Setup.
*****

This is a Standalone Node

Do you want to configure multi node setup [y/n]? y

Select a option from the menu below

a) Configure as Primary Node
b) Configure as Service Node
c) Configure as Inventory DB
d) Configure as Monitoring DB
x) Exit

Enter: [a/b/c/d/x]? c
Do you want to configure this node as Inventory Database [y/n]? y
Configuring Inventory DB
This will reinitialize database and you will lose all your data. Do you still want to continue? [y/n]? y
user selected 'y' reinitialize database
Checking DB status
Database (127.0.0.1)
-----
Status: UP
Client: localhost      Connections: 19

Stopping Services
Disabling UCS Director services at startup
Enabling Remote Database access to Primary Node and Service Node
Removing infra start/stop/status scripts
Re-initializing Database
Configured Inventory Database successfully
In order for changes to take effect logout and login back
Do you want to logout [y/n]? y
```

Verify the services for the inventory database are up and running, choose (2) '**Display Service Status**' and press Enter. You should see the lines in the red box below. **Note:** After you return to the shelladmin, the menu options change to those available for an inventory database node.

```
Cisco UCS Director Shell Menu
Inventory Database
Select a number from the menu below
1) Change ShellAdmin Password
2) Display Services Status
3) Stop Database
4) Start Database
5) Backup Database
6) Restore Database
7) Time Sync
8) Ping Hostname/IP Address
9) Configure Network Interface
10) Display Network Details
11) Enable Database for Cisco UCS Director Baremetal Agent
12) Add Cisco UCS Director Baremetal Agent Hostname/IP
13) Shutdown Appliance
14) Reboot Appliance
15) Manage Root Access
16) Login as Root
17) Apply Patch
18) Quit
SELECT> 2
Inventory database (127.0.0.1)
-----
Status: UP
Press return to continue ...
```

Edit the /etc/hosts file to update the name and IP address of the host. SSH to the Inventory Database Node using the root account.

- Edit the hosts file: '**vi /etc/hosts**'
- Go to the end of the line: '**shift + a**'
- Create a new line: press return
- enter your host details: example shown below
- when done: press '**esc**'
- enter '**:wq!**'
- Verify the hosts file has been saved: '**cat /etc/hosts**'

```
[root@localhost ~]# cat /etc/hosts
127.0.0.1 localhost.localdomain localhost localhost
172.17.80.120 CUCSD-I-5_4_0_0
172.17.80.121 CUCSD-M-5_4_0_0
172.17.80.122 CUCSD-S-5_4_0_0
172.17.80.119 CUCSD-P-5_4_0_0
::1 localhost.localdomain localhost localhost ip6-localhost ip6-loopback
[root@localhost ~]#
```

Edit the /etc/resolv.conf to update the DNS servers.

- Edit the resolv.conf file: '**vi /etc/resolv.conf**'
- press '**i**' for insert
- enter '**search localhost your domain name**', **Note:** Sometime search localhost is already there
- enter dns server ip address after nameserver, **Note:** if you have multiple DNS servers, enter on separate lines
- when done: press '**esc**'
- enter '**:wq!**'
- Example:

```
search localhost gsp-r5.cloudlab.cisco.com
nameserver 172.17.80.104
nameserver 8.8.8.8
nameserver 8.8.4.4
```

- Verify the changes: '**cat /etc/resolv.conf**'

```
[root@localhost ~]# cat /etc/resolv.conf
; generated by /sbin/dhclient-script
search localhost gsp-r5.cloudlab.cisco.com
nameserver 172.17.80.104
nameserver 8.8.8.8
nameserver 8.8.4.4
[root@localhost ~]#
```

Edit the hostname in /etc/sysconfig/network

- Edit the network config: `'vi /etc/sysconfig/network'`
- Move cursor to the beginning of localhost where it is on the l and enter `'cw'` (change word)
- Enter the Host name for the Inventory Database Node
- Enter your domain name
- when done: press `'esc'`
- enter `':wq!'`
- Verify changes were saved: `'cat /etc/sysconfig/network'`

```
[root@CUCSD-I-5_4_0_0 ~]# cat /etc/sysconfig/network
NETWORKING=yes
NETWORKING_IPV6=yes
HOSTNAME=CUCSD-I-5_4_0_0
DOMAINNAME=gsp-r5.cloudlab.cisco.com
[root@CUCSD-I-5_4_0_0 ~]#
```

Change the hostname.

```
[root@localhost ~]# hostname CUCSD-I-5_4_0_0
[root@localhost ~]# hostname
CUCSD-I-5_4_0_0
[root@localhost ~]#
```

Log out and log back into the Inventory Database and you will see the new hostname.

```
[root@CUCSD-I-5_4_0_0 ~]#
```

Verify NTP servers for Monitoring Database Node are configured and synced. SSH into Monitoring Database Node using root account.

- Create ntp user: `'useradd ntp'` **Note:** If the ntp user already exist, the system will let you know.
- Restart the ntpd services: `'service ntpd restart'`
- Verify configured NPT servers: `'ntpq -p'`
- The `'*'` next to the NTP server IP address indicates the Inventory Node is synced to the NTP server.

```
[root@CUCSD-I-5_4_0_0 ~]# useradd ntp
useradd: user 'ntp' already exists
[root@CUCSD-I-5_4_0_0 ~]# service ntpd restart
Shutting down ntpd: [ OK ]
Starting ntpd: [ OK ]
[root@CUCSD-I-5_4_0_0 ~]# ntpq -p
      remote           refid      st t when poll reach  delay  offset  jitter
-----
*173.17.112.254 LOCAL(1)      5 u   5   64   1   1.508  10.454  0.000
[root@CUCSD-I-5_4_0_0 ~]#
```

Optional: If you need to configure multiple NTP servers, you can do so by editing the ntp.conf file.

- Edit the ntp.conf file: **'vi /etc/ntp.conf'**
- cursor down to the **'server'** line
- press **'shit + a'** for insert and go to the end of the line
- press return to create a new line
- enter **'server your ip address'** of your NTP server IP address
- press **'esc'**, then enter **':wq!'** to quit and write the info
- Verify the config changes: **'cat /etc/ntp.conf'**

```
[root@CUCSD-I-5_4_0_0 ~]# cat /etc/ntp.conf
# For more information about this file, see the man pages
# ntp.conf(5), ntp_acc(5), ntp_auth(5), ntp_clock(5), ntp_misc(5), ntp_mon(5).

driftfile /var/lib/ntp/drift

# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery

# Permit all access over the loopback interface. This could
# be tightened as well, but to do so would effect some of
# the administrative functions.
restrict 127.0.0.1
restrict -6 ::1

# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

#broadcast 192.168.1.255 autokey          # broadcast server
#broadcastclient                          # broadcast client
#broadcast 224.0.1.1 autokey              # multicast server
#multicastclient 224.0.1.1                # multicast client
#manycastserver 239.255.254.254           # manycast server
#manycastclient 239.255.254.254 autokey   # manycast client

# Enable public key cryptography.
#crypto

includefile /etc/ntp/crypto/pw

# Key file containing the keys and key identifiers used when operating
# with symmetric key cryptography.
keys /etc/ntp/keys

# Specify the key identifiers which are trusted.
#trustedkey 4 8 42

# Specify the key identifier to use with the ntpdc utility.
#requestkey 8

# Specify the key identifier to use with the ntpq utility.
#controlkey 8

# Enable writing of statistics records.
#statistics clockstats cryptostats loopstats peerstats

server 173.37.202.254
[root@CUCSD-I-5_4_0_0 ~]# █
```

If you edited the ntp.conf file, you must restart the ntpd service and check the NTP synchronization. It may take a while but when the clock is synced with the NTP server there will be a **'*'** to the left of the IP address.

- Restart the ntpd services: **'service ntpd restart'**
- View the configured ntp servers and check for synchronization: **'ntpq -p'**

```
[root@CUCSD-I-5_4_0_0 ~]# service ntpd restart
Shutting down ntpd: [ OK ]
Starting ntpd: [ OK ]
[root@CUCSD-I-5_4_0_0 ~]# ntpq -p
      remote           refid      st t when poll reach  delay  offset  jitter
-----
*173.37.202.254 LOCAL(1)    5 u  50  64   1   1.484  3.461  0.000
[root@CUCSD-I-5_4_0_0 ~]# █
```

Change the time zone to the local timezone where the Primary Node, Inventory Database Service Nodes and the Monitoring Database reside. This will ensure the logs will match everywhere.

- Determine the current timezone: `'ls -l /etc/localtime'`
- Determine your timezone if your in America: `'ls /usr/share/zoneinfo/America/'`
- This deployment is in Dallas so I will choose `'Chicago'` for Central Standard Time.

```
[root@CUCSD-I-5_4_0_0 ~]# ls -l /etc/localtime
lrwxrwxrwx. 1 root root 27 Nov  4 19:23 /etc/localtime -> /usr/share/zoneinfo/Etc/UTC
[root@CUCSD-I-5_4_0_0 ~]# ls /usr/share/zoneinfo/America/
Adak          Campo_Grande  Eirunepe      Jamaica       Metlakatla   Port_of_Spain St_Lucia
Anchorage     Cancun        El_Salvador   Jujuy         Mexico_City  Porto_Velho   ST_Thomas
Anguilla      Caracas      Ensenada      Juneau        Miquelon     Puerto_Rico   ST_Vincent
Antigua      Catamarca    Fortaleza     Kentucky      Moncton      Rainy_River  Swift_Current
Araguaina    Cayenne      Fort_Wayne    Knox_IN       Monterrey    Rankin_Inlet  Tegucigalpa
Argentina    Cayman       Glace_Bay     Kralendijk    Montevideo   Recife       Thule
Aruba        Chicago       Godthab       La_Paz        Montreal     Regina        Thunder_Bay
Asuncion     Chihuahua    Goose_Bay     Lima          Montserrat   Resolute     Tijuana
Atikokan     Coral_Harbour Grand_Turk    Los_Angeles  Nassau       Rio_Branco   Toronto
Atka         Cordoba      Grenada       Louisville    New_York     Rosario      Tortola
Bahia        Costa_Rica   Guadeloupe   Lower_Princes Nipigon      Santa_Isabel Vancouver
Bahia_Banderas Creston      Guatemala    Maceio       Nome         Santarem     Virgin
Barbados     Cuiba       Guayaquil    Managua      Noronha      Santiago     Whitehorse
Belim        Curacao     Guyana       Manaois      North_Dakota Santo_Domingo Winnipeg
Belize       Danmarkshavn Halifax       Marigot      Ojinaga      Sao_Paulo    Yakutat
Blanc-Sablon Dawson      Havana       Martinique   Panama       Scoresbysund Yellowknife
Boa_Vista    Dawson_Creek Hermosillo    Matamoros    Pangnirtung  Shiprock
Bogota      Denver      Indiana      Mazatlan     Paramaribo   Sitka
Boise       Detroit     Indianapolis  Mendoza      Phoenix      St_Barthelemy
Buenos_Aires Dominica    Inuvik       Menominee    Port-au-Prince ST_Johns
Cambridge_Bay Edmonton  Iqaluit      Merida       Porto_Acre   St_Kitts
```

Change the timezone and verify. I have chosen the Central Time Zone for my location.

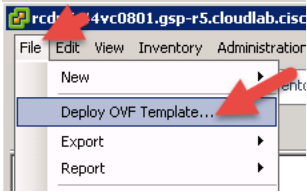
- Copy the localtime to new file named old.timezone: `'cp /etc/localtime /root/old.timezone'`
- Remove the localtime file: `'rm /etc/localtime'`
- When asked `'rm: remove symbolic link '/etc/localtime'?:'` enter `'y'` for yes
- Create the new localtime file: `'ln -s /usr/share/zoneinfo/America/Chicago /etc/localtime'`
- Verify the timzone is what you set it to: `'date'`
- Verify the link: `'ls -l /etc/localtime'`

```
[root@CUCSD-I-5_4_0_0 ~]# cp /etc/localtime /root/old.timezone
[root@CUCSD-I-5_4_0_0 ~]# rm /etc/localtime
rm: remove symbolic link '/etc/localtime'? y
[root@CUCSD-I-5_4_0_0 ~]# ln -s /usr/share/zoneinfo/America/Chicago /etc/localtime
[root@CUCSD-I-5_4_0_0 ~]# date
Thu Nov  5 21:49:37 CST 2015
[root@CUCSD-I-5_4_0_0 ~]# ls -l /etc/localtime
lrwxrwxrwx. 1 root root 35 Nov  5 21:49 /etc/localtime -> /usr/share/zoneinfo/America/Chicago
[root@CUCSD-I-5_4_0_0 ~]#
```

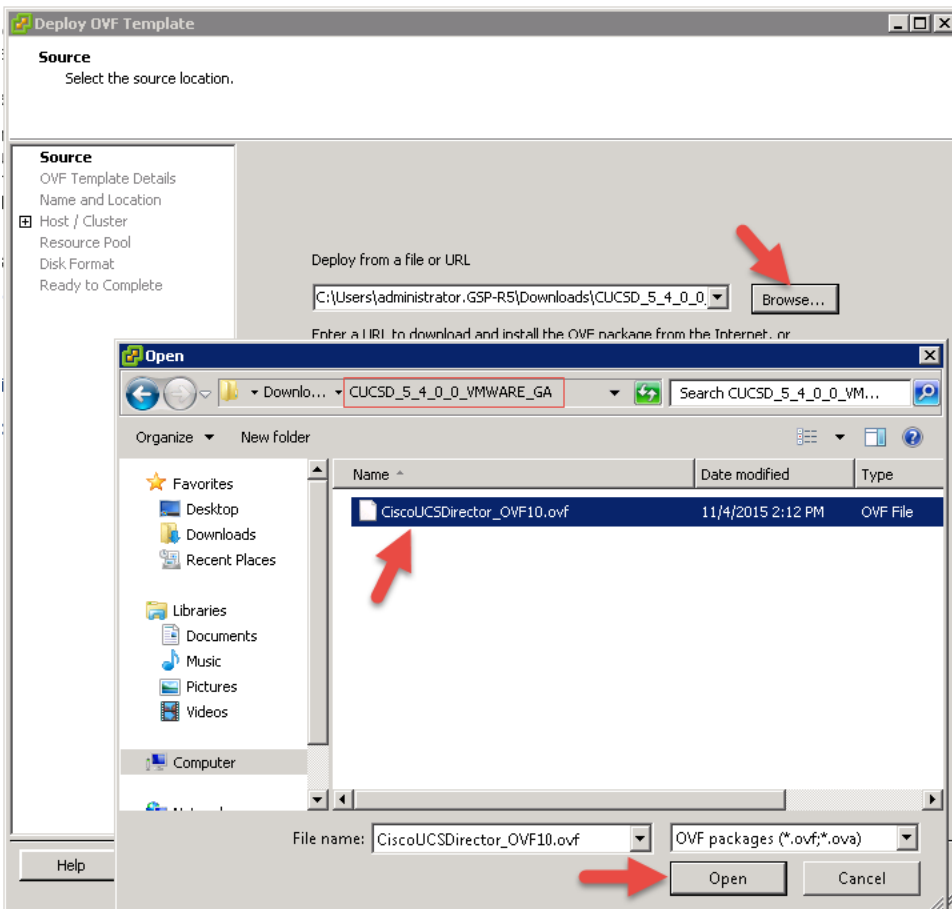
3. Create the Monitoring Database Node

3.1. Create Monitoring Database VM

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



Browse to the "CiscoUCSDirector_OVF10.ovf", select it for deployment then click 'Next'.



Verify details and click 'Next'.

The screenshot shows the 'Deploy OVF Template' window with the 'OVF Template Details' section active. The window title is 'Deploy OVF Template'. Below the title bar, it says 'OVF Template Details' and 'Verify OVF template details.' On the left, there is a navigation pane with the following items: Source, OVF Template Details (selected), End User License Agreement, Name and Location, Host / Cluster, Resource Pool, Disk Format, Properties, and Ready to Complete. The main area displays the following details:

Product:	CUCSD-5.4.0.0
Version:	5.4.0.0
Vendor:	Cisco Systems
Publisher:	No certificate present
Download size:	4.3 GB
Size on disk:	7.6 GB (thin provisioned) 100.0 GB (thick provisioned)
Description:	Cisco UCS Director 5.4.0.0 (Emerald Bay)

Below the table, there is a note: 'Note: It is mandatory to reserve vCPU and Memory as recommended by Installation and Deployment guide.'

Accept the license agreement and click 'Next'.

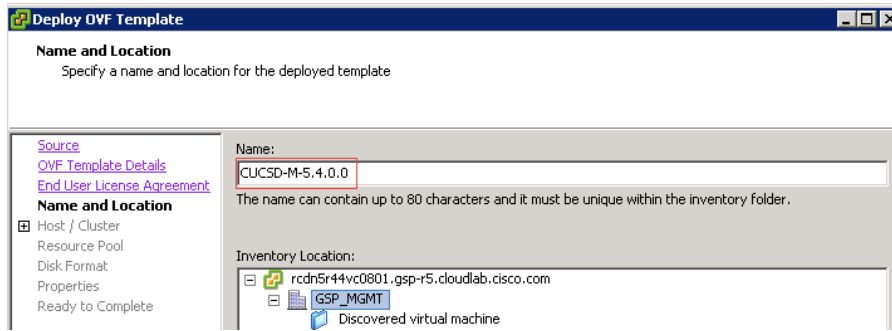
The screenshot shows the 'Deploy OVF Template' window with the 'End User License Agreement' section active. The window title is 'Deploy OVF Template'. Below the title bar, it says 'End User License Agreement' and 'Accept the end user license agreements.' On the left, there is a navigation pane with the following items: Source, OVF Template Details, End User License Agreement (selected), Name and Location, Storage, Disk Format, Network Mapping, Properties, and Ready to Complete. The main area displays the following text:

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.

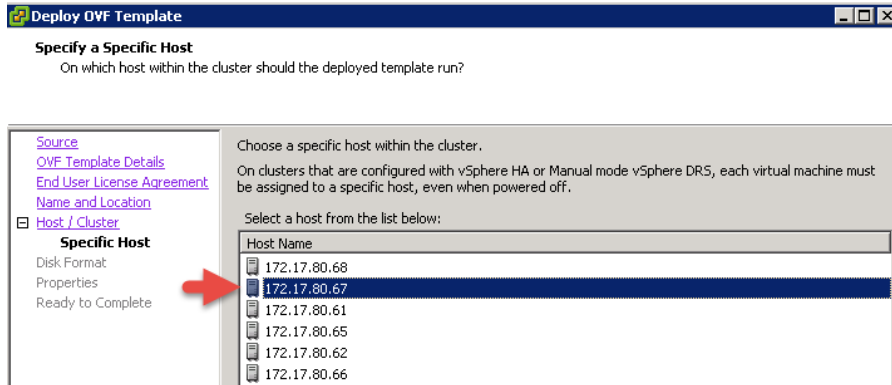
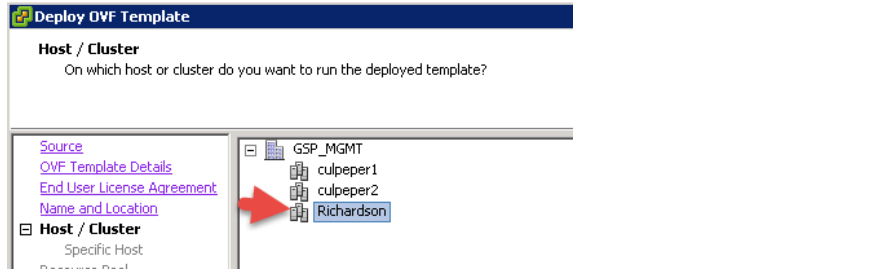
CISCO SYSTEMS, INC. OR ITS AFFILIATE LICENSING THE SOFTWARE ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS 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,

At the bottom of the text area, there is an 'Accept' button with a red arrow pointing to it. Below the text area, there are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button.

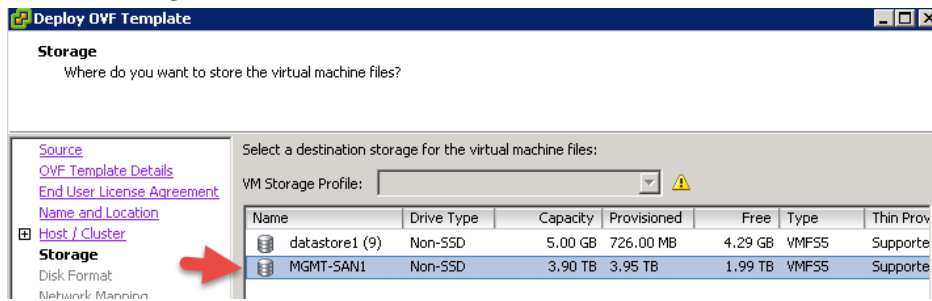
Name the VM and click 'Next'.



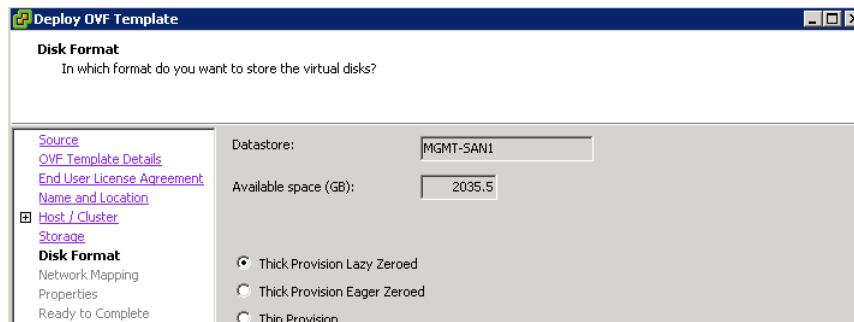
Select Cluster/Host to deploy this VM on and click 'Next'.



Select a storage location to install the VM and click 'Next'.



Leave the default settings for the Disk Format and click 'Next'.



Select the Network to put this VM on and click 'Next'.

The screenshot shows the 'Deploy OVF Template' window with the 'Network Mapping' step selected. The title bar reads 'Deploy OVF Template'. Below the title bar, the text 'Network Mapping' is followed by the question 'What networks should the deployed template use?'. On the left side, there is a navigation pane with links: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location', 'Host / Cluster' (which is selected and highlighted with a blue box), and 'Storage'. The main area contains the instruction 'Map the networks used in this OVF template to networks in your inventory'. Below this is a table with two columns: 'Source Networks' and 'Destination Networks'. The table has one row with 'Network 1' in the 'Source Networks' column and 'MGMT_80' in the 'Destination Networks' column. Both 'Network 1' and 'MGMT_80' are highlighted with a blue selection bar.

Source Networks	Destination Networks
Network 1	MGMT_80

Enter a password for Root and Shelladmin Accounts, Management IP Address, Subnet Mask, Gateway and click 'Next'.

The screenshot shows the 'Deploy OVF Template' window with the 'Properties' step selected. The title bar reads 'Deploy OVF Template'. Below the title bar, the text 'Properties' is followed by the instruction 'Customize the software solution for this deployment.'. On the left side, there is a navigation pane with links: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location', 'Host / Cluster', 'Storage', 'Disk Format', 'Network Mapping', and 'Properties' (which is selected and highlighted with a blue box). Below 'Properties' is the text 'Ready to Complete'. The main area is titled 'Application' and contains several sections for configuration. Each section has a title and a description, followed by input fields. The 'Root Password' section has 'Enter password' and 'Confirm password' fields, both containing '*****'. The 'Shelladmin Password' section has 'Enter password' and 'Confirm password' fields, both containing '*****'. The 'Management IP Address' section has a description 'Enter Management IP Address for eth0. Set 0.0.0.0 to use DHCP' and an input field containing '172 . 17 . 80 . 121'. The 'Management IP Subnet Mask' section has a description 'Enter Management IP Subnet Mask for eth0. Set 0.0.0.0 to use DHCP' and an input field containing '255 . 255 . 255 . 0'. The 'Gateway IP Address' section has a description 'Gateway IP Address' and an input field containing '172 . 17 . 80 . 1'. At the bottom of the window, there are three buttons: 'Help', '< Back', 'Next >', and 'Cancel'.

Application

Root Password
Root Password
Enter password: *****
Confirm password: *****

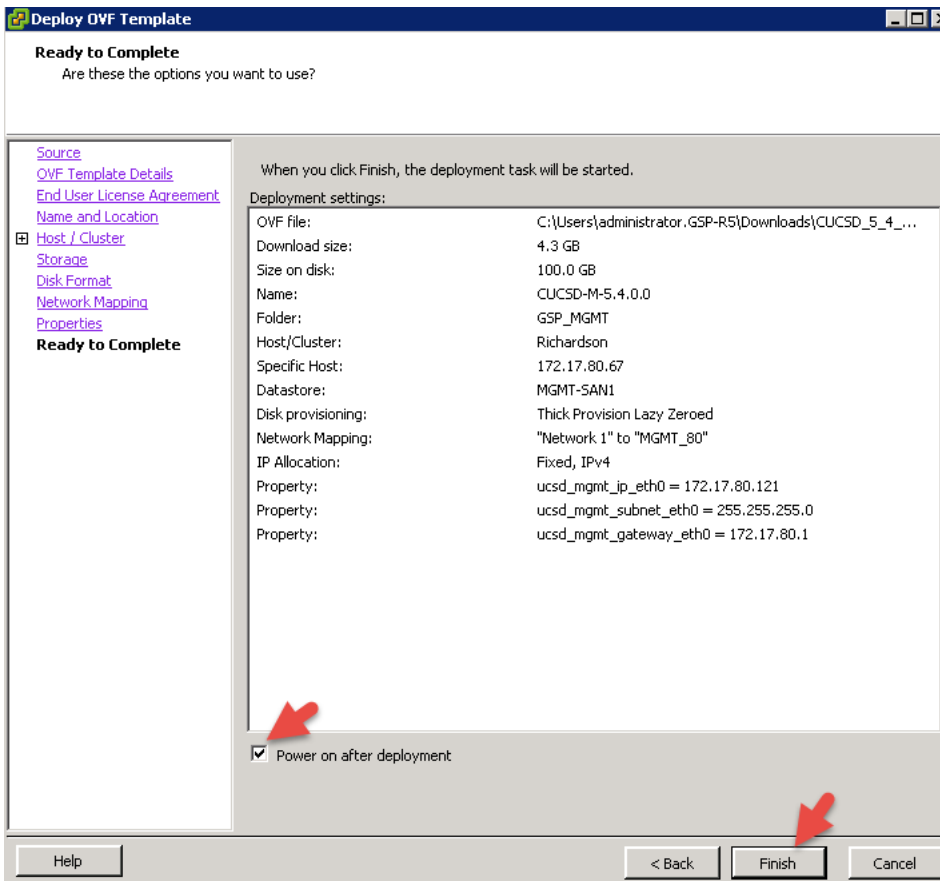
Shelladmin Password
Shelladmin Password
Enter password: *****
Confirm password: *****

Management IP Address
Enter Management IP Address for eth0. Set 0.0.0.0 to use DHCP
172 . 17 . 80 . 121

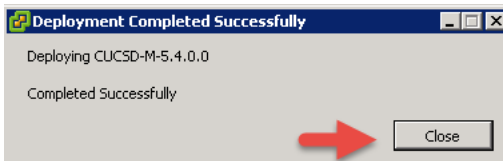
Management IP Subnet Mask
Enter Management IP Subnet Mask for eth0. Set 0.0.0.0 to use DHCP
255 . 255 . 255 . 0

Gateway IP Address
Gateway IP Address
172 . 17 . 80 . 1

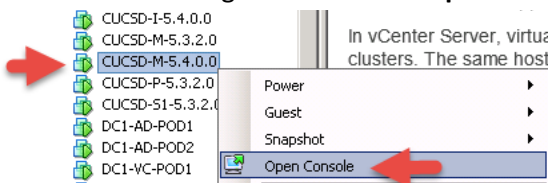
Select Power on after deployment and click **'Finish'**.



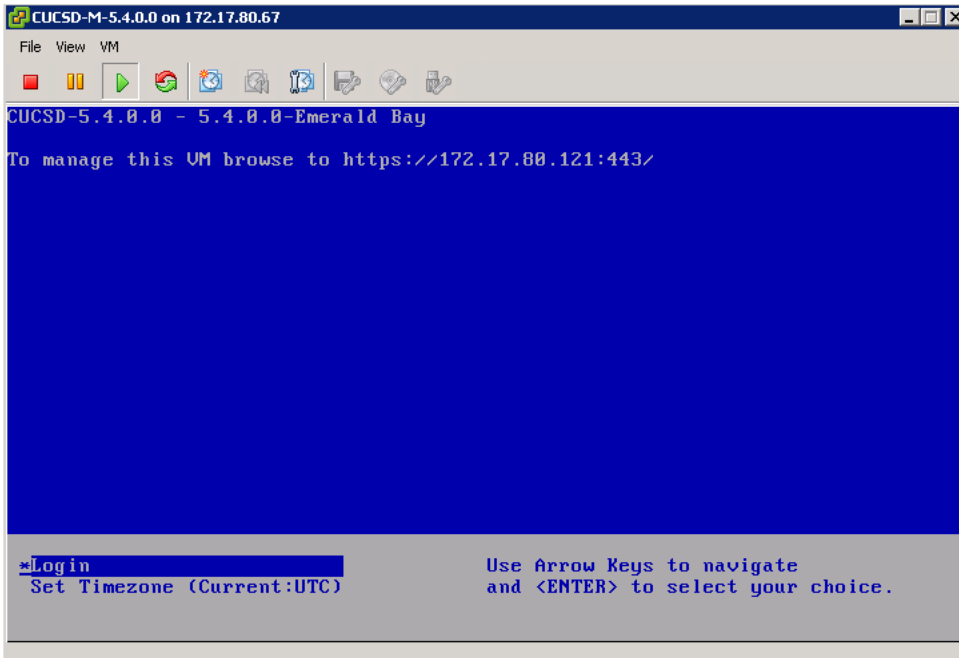
After deployment click **'Close'**.



Select the Monitoring VM and select **'Open Console'**.

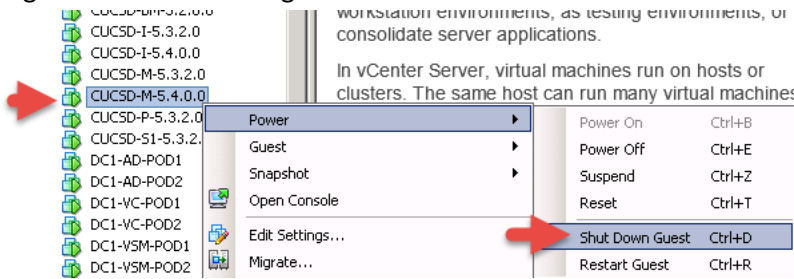


Monitor the console until the installation is complete and you will see a screen similar to the one below. The installation will take several minutes to complete so be patient.

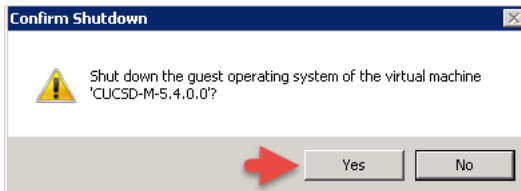


3.2. Install/Update VMWare tools & VM Version

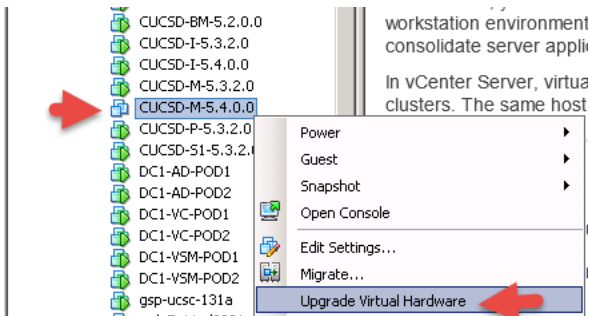
Navigate to the Monitoring Database VM and select **'Shut Down Guest'**.



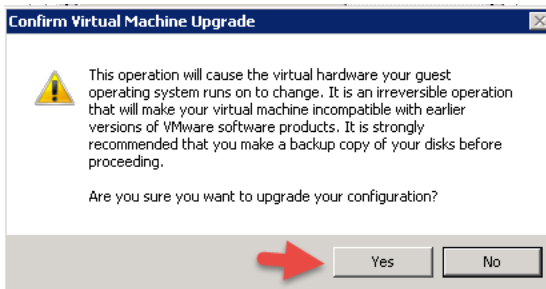
Select **'Yes'**.



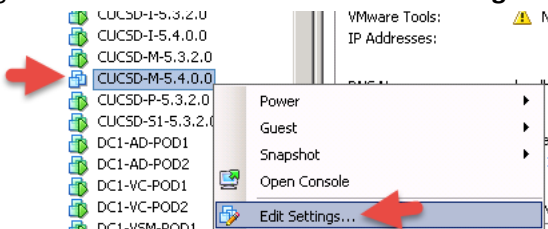
Wait for the VM to completely shut down then right click on the VM and select **'Upgrade Virtual Hardware'**.



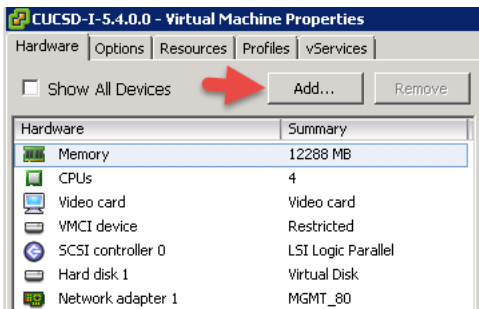
Select **'Yes'**.



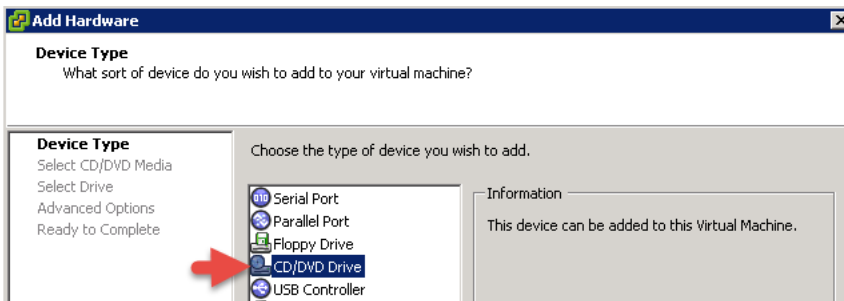
Right click on the VM and Select **'Edit Settings'**.



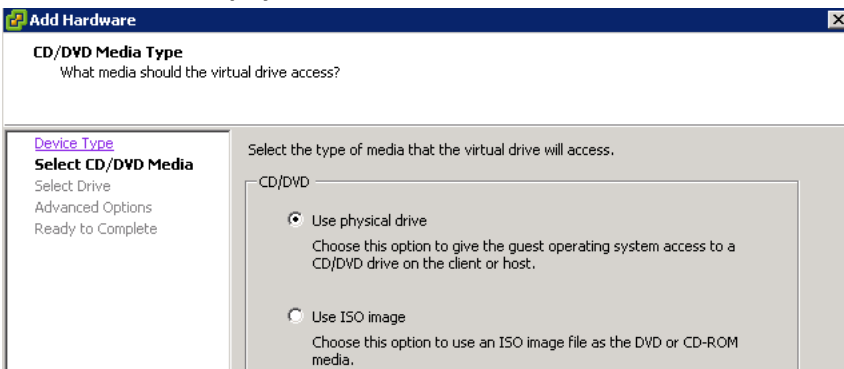
Click 'Add'.



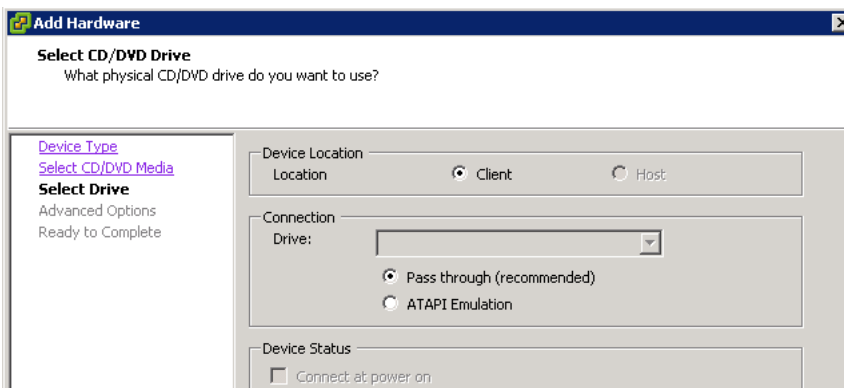
Select 'CD/DVD Drive' and click 'Next'.



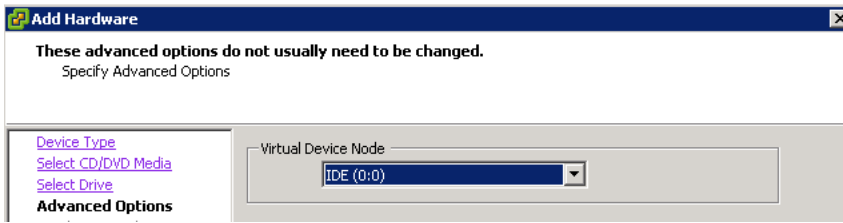
Leave default 'Use physical drive' and click 'Next'.



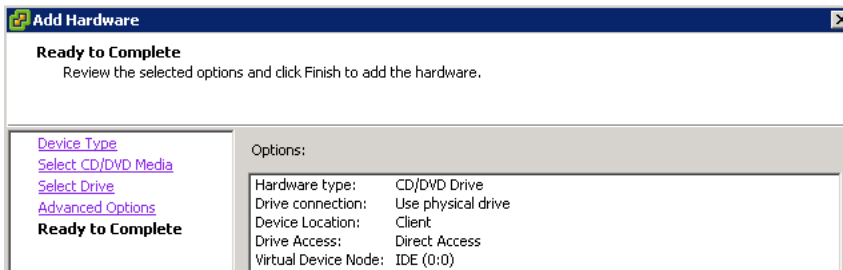
Leave default and click 'Next'.



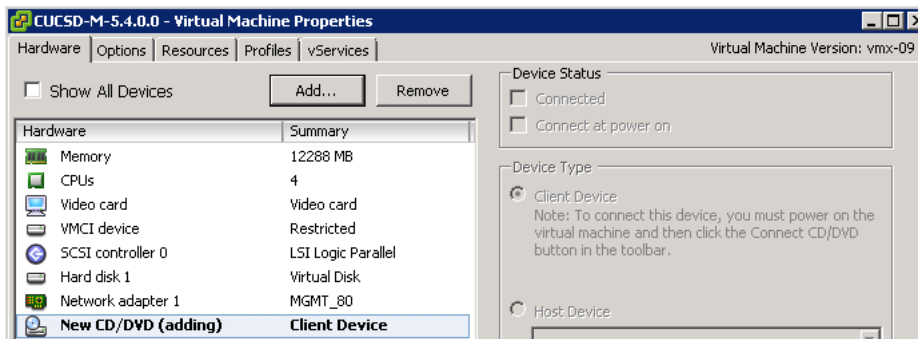
Leave default and click 'Next'.



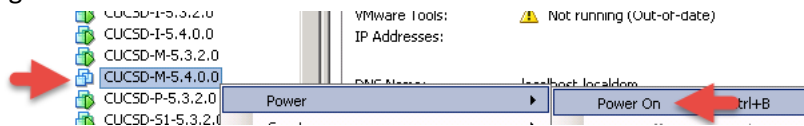
Review and click 'Finish'.



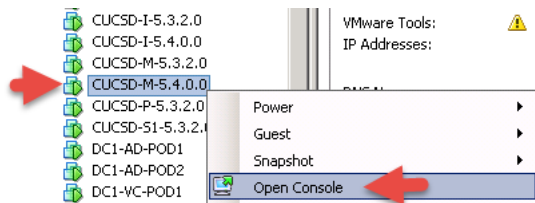
Review and click 'OK'.



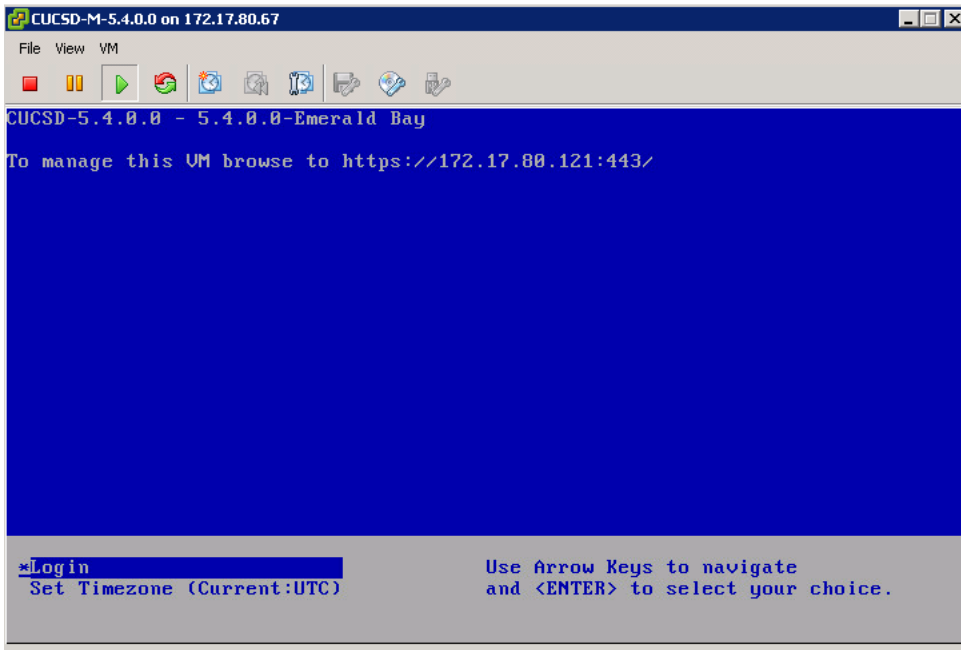
Right click on the VM and select 'Power On'.



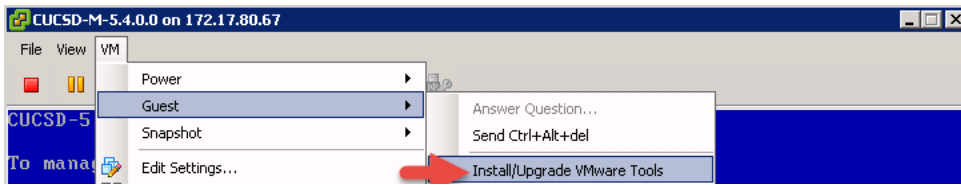
Open the VM Console to watch the VM Boot. Right click on the VM and select 'Open Console'.



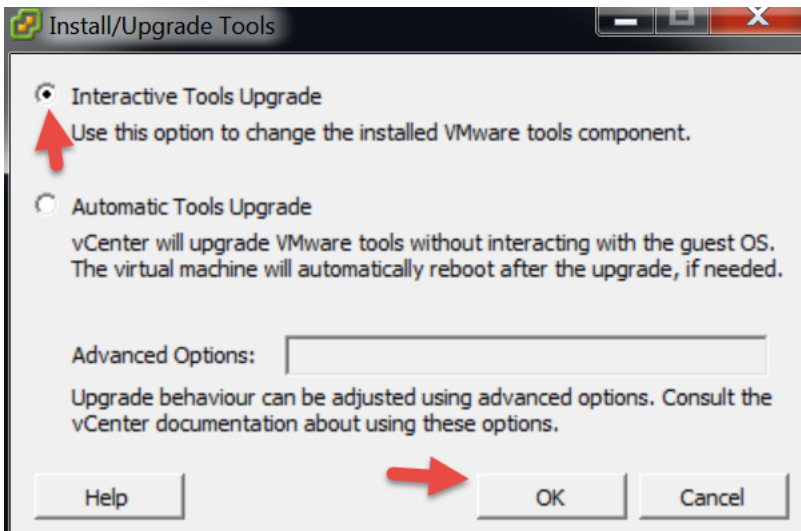
Once the VM is completely up, you should see the login screen similar to below.



From the console, select 'Install/Upgrade VMware Tools'.



Select 'Interactive Tools Upgrade' and click 'OK'.



SSH to the Monitoring Database Node and login using the root account.

- Make a dir for cdrom: `'mkdir /mnt/cdrom'`
- Mount the cdrom: `'mount /dev/cdrom /mnt/cdrom'`
- Copy vmware install to /tmp: `'cp /mnt/cdrom/VMwareTools-5.0.0-<xxxx>.tar.gz /tmp/'` **Note:** tab out the VMware tools part so you don't have to figure out the correct name.
- Unzip the files in /tmp: `'tar xzf /tmp/VMwareTools-5.0.0-<xxxx>.tar.gz'` **Note:** tab out the VMware tools part so you don't have to figure out the correct name.
- Change directory: `'cd vmware-tools-distrib'`
- Run the install: `'./vmware-install.pl'`
- Accept all the defaults by Pressing Enter for all the options.

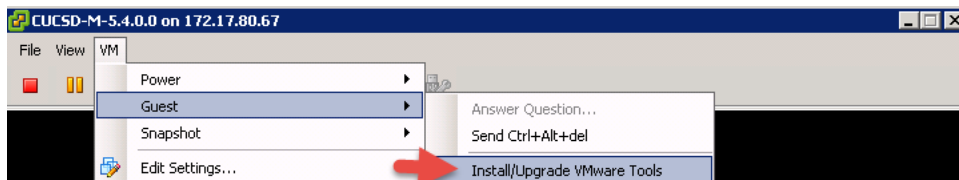
Note: You will probably get the following message.

VMware Tools cannot be installed, since they have already been installed using a package-based mechanism (rpm or deb) on this system. If you wish to continue, you must first remove the currently installed VMware Tools using the appropriate packaged-based mechanism, and then restart this installer
Execution aborted.

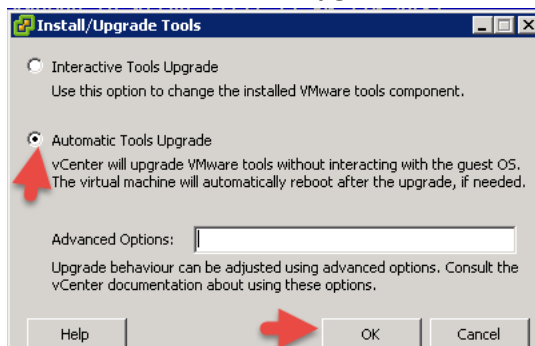
Found VMware Tools CDROM mounted at /mnt/cdrom. Ejecting device /dev/cdrom ... No eject (or equivalent) command could be located. Eject Failed: If possible manually eject the Tools installer from the guest cdrom mounted at /mnt/cdrom before canceling tools install on the host.

- If you get this message, we need to Delete the VMware tools directory: `'rm -rf /usr/lib/vmware-tools/'`
- Change directory: `'cd vmware-tools-distrib/'`
- Re-Run the install: `'./vmware-install.pl'`
- Enter **'Yes'** to the 'Would you like to remove the install DB?' You will probably get a Failure and Execution aborted.
- Re-Run the install: `'./vmware-install.pl'`
- Accept all the defaults by Pressing Enter for all the options.

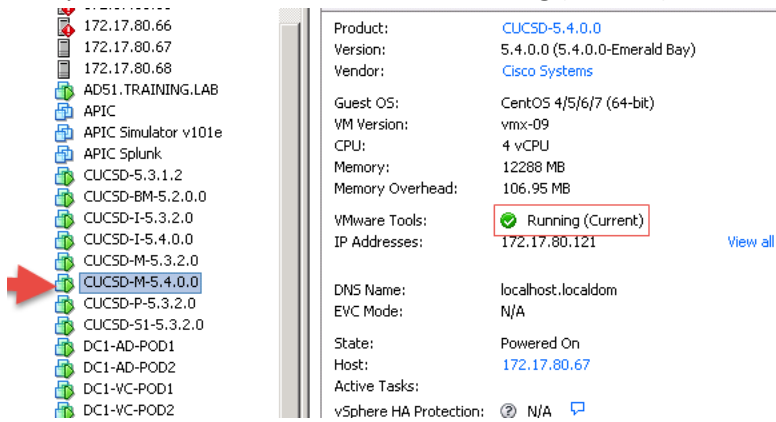
From the console, select **'Install/Upgrade VMware Tools'**.



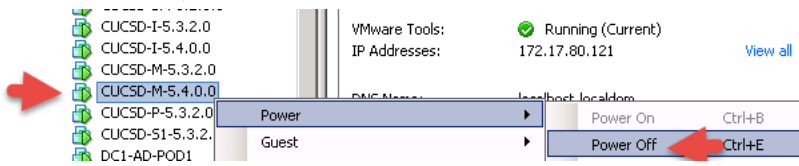
Select **'Automatic Tools Upgrade'** and click **'OK'**.



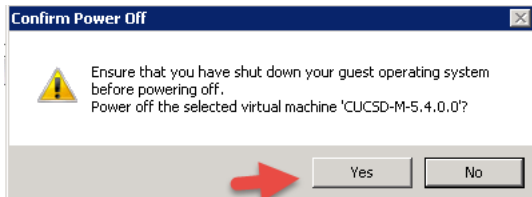
Verify Tools have been installed and 'Running (Current)' as shown below.



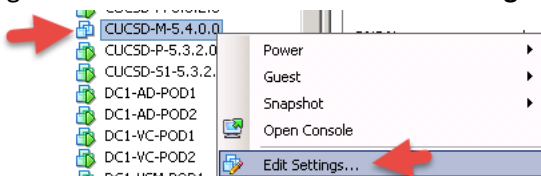
Power off the VM, 'Power Off'.



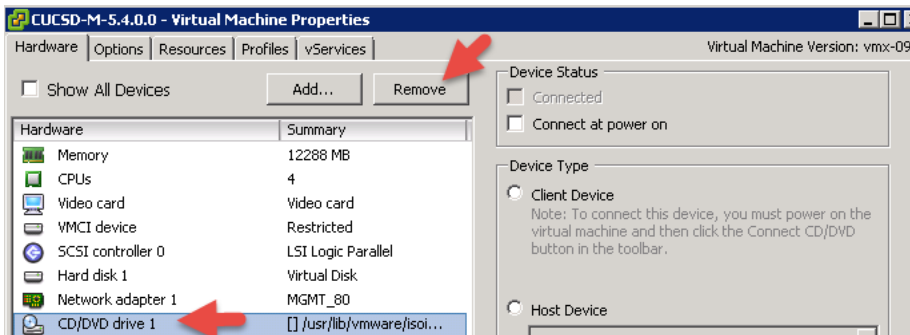
Select 'Yes'.



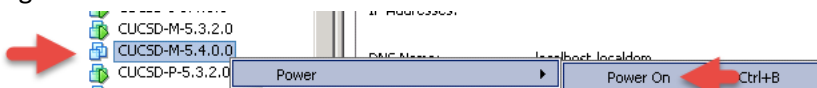
Right click on the VM and select 'Edit Settings'.



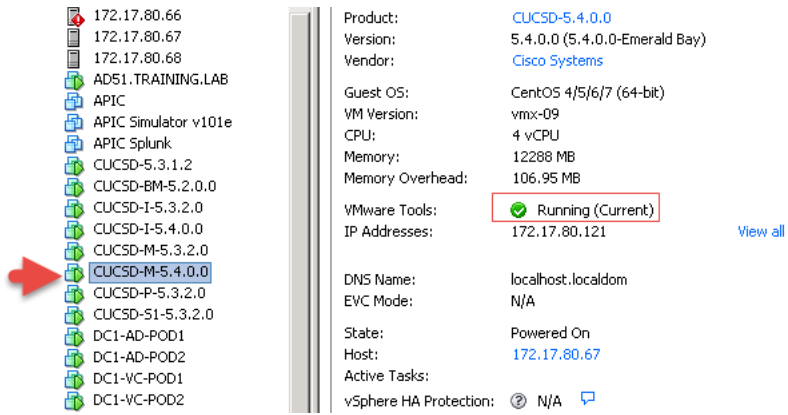
Select 'CD/DVD drive 1', click 'Remove' and then click 'OK'.






Right click on the VM and Select 'Power On'.



Wait for the VM to completely boot up and then verify Tools have been installed and 'Running (Current)'.



The screenshot shows a vSphere inventory list on the left and a details pane on the right. The VM 'CUCSD-M-5.4.0.0' is selected in the inventory list, indicated by a red arrow. The details pane shows the following information:

Product:	CUCSD-5.4.0.0
Version:	5.4.0.0 (5.4.0.0-Emerald Bay)
Vendor:	Cisco Systems
Guest OS:	CentOS 4/5/6/7 (64-bit)
VM Version:	vmx-09
CPU:	4 vCPU
Memory:	12288 MB
Memory Overhead:	106.95 MB
VMware Tools:	 Running (Current)
IP Addresses:	172.17.80.121 View all
DNS Name:	localhost.localdom
EVC Mode:	N/A
State:	Powered On
Host:	172.17.80.67
Active Tasks:	
vSphere HA Protection:	 N/A 

3.3. Configure Monitoring Database

SSH to the Monitoring Database Node using the shelladmin account.

Configure NTP Server. From the Menu select 9 'Time Sync'. Replace the NTP IP Address with your NTP Server.

```
SELECT> 9
Time sync.....
System time is Fri Nov 6 02:19:24 UTC 2015
Hardware time is Fri 06 Nov 2015 02:19:25 AM UTC -0.656583 seconds
Do you want to sync systemtime [y/n]? y
System time reset to hardware clock
Do you want to sync to NTP [y/n]? y
Enter NTP server to sync time with: 173.37.102.254
ntpd (pid 1868) is running...
Shutting down ntpd: [ OK ]
6 Nov 02:19:42 ntpdate[3631]: adjust time server 173.37.102.254 offset 0.001981 sec
Synchronized time with NTP server '173.37.102.254'
Added NTP server '173.37.102.254' to /etc/ntp.conf
Starting ntpd: [ OK ]
synchronized to NTP server (173.37.102.254) at stratum 6
time correct to within 7940 ms
polling server every 64 s
Press return to continue ...
```

From the menu, choose (24) 'Configure Multi Node Setup (Advanced Deployment)' and press Enter.

- Enter '1' to configure the current node.
- Enter 'y' when asked if you want to configure multi node setup.
- Enter 'd' to Configure the node as Monitoring DB.
- Enter 'y' when asked if you asked if you want to configure this node as Monitoring Database.
- Enter 'y' when asked about re-initializing the database.
- When prompted to logout, enter 'y' and press enter. Log back in as shelladmin by entering 'su shelladmin'

```
SELECT> 24
*****
This wizard helps to do Multi Node setup
*****
Configuration Options :
Current Node --> select '1'
Remote Node --> select '2'
exit --> select '3'

Please enter an option: 1
*****
Cisco UCS Director Multi Node Setup requires multiple instances of UCS Director oVf deployed with different configura
tions. Following are the required configurations:

* UCS Director Primary Node (1 Instance) . This node also acts as a front end UI node
* UCS Director Service Node (1 or more instances) . Service node can be reconfigured as Primary Node when necessary.
* UCS Director Inventory DB Node (1 Instance)
* UCS Director Monitoring DB Node (1 Instance)

Refer to UCS Director documentation for additional details on Multi Node Setup.
*****

This is a standalone Node
Do you want to configure multi node setup [y/n]? y

Select a option from the menu below

a) Configure as Primary Node
b) Configure as Service Node
c) Configure as Inventory DB
d) Configure as Monitoring DB
x) Exit

Enter: [a/b/c/d/x]? d
Do you want to configure this node as Monitoring Database [y/n]? y
Configuring Monitoring DB
This will reinitialize database and you will lose all your data. Do you still want to continue? [y/n]? y
user selected 'y' reinitialize database
Checking DB Status
Database (127.0.0.1)
-----
Status: UP
Client: localhost Connections: 17

Stopping Services
Disabling UCS Director services at startup
Enabling Remote Database access to Primary Node and Service Node
Removing infra start/stop/status scripts
Re-initializing Database
Configured Monitoring Database successfully
In order for changes to take effect logout and login back
Do you want to logout [y/n]? y
```

Verify the services for the Monitoring database are up and running, choose (2) **'Display Service Status'** and press Enter. You should see the lines in the red box below. **Note:** After you return to the shelladmin, the menu options change to those available for an Monitoring database node.

```
Cisco UCS Director Shell Menu
Monitoring Database
Select a number from the menu below
1) Change ShellAdmin Password
2) Display Services Status
3) Stop Database
4) Start Database
5) Backup Database
6) Restore Database
7) Time Sync
8) Ping Hostname/IP Address
9) Configure Network Interface
10) Display Network Details
11) Enable Database for Cisco UCS Director Baremetal Agent
12) Add Cisco UCS Director Baremetal Agent Hostname/IP
13) Shutdown Appliance
14) Reboot Appliance
15) Manage Root Access
16) Login as Root
17) Apply Patch
18) Quit
SELECT> 2
Monitoring database (127.0.0.1)
-----
Status: UP
Press return to continue ...
```

Edit the `/etc/hosts` file to update the name and IP address of the host. SSH to the Monitoring Database Node using the root account.

- Edit the hosts file: **'vi /etc/hosts'**
- Go to the end of the line: **'shift + a'**
- Create a new line: press return
- enter your host details: example shown below
- when done: press **'esc'**
- enter **':wq!'**
- Verify the hosts file has been saved: **'cat /etc/hosts'**

```
[root@localhost ~]# cat /etc/hosts
127.0.0.1 localhost.localdomain localhost localhost
172.17.80.120 CUCSD-I-5_4_0_0
172.17.80.121 CUCSD-M-5_4_0_0
172.17.80.122 CUCSD-S-5_4_0_0
172.17.80.119 CUCSD-P-5_4_0_0
::1 localhost.localdomain localhost localhost ip6-localhost ip6-loopback
[root@localhost ~]#
```

Edit the `/etc/resolv.conf` to update the DNS servers.

- Edit the resolv.conf file: **'vi /etc/resolv.conf'**
- press **'i'** for insert
- enter **'search localhost your domain name'**, **Note:** Sometime search localhost is already there
- enter dns server ip address after nameserver, **Note:** if you have multiple DNS servers, enter on separate lines
- when done: press **'esc'**
- enter **':wq!'**
- Example:

```
search localhost gsp-r5.cloudlab.cisco.com
nameserver 172.17.80.104
nameserver 8.8.8.8
nameserver 8.8.4.4
```

- Verify the changes: **'cat /etc/resolv.conf'**

```
[root@localhost ~]# cat /etc/resolv.conf
; generated by /sbin/dhclient-script
search localhost gsp-r5.cloudlab.cisco.com
nameserver 172.17.80.104
nameserver 8.8.8.8
nameserver 8.8.4.4
[root@localhost ~]#
```

Edit the hostname in /etc/sysconfig/network

- Edit the network config: `'vi /etc/sysconfig/network'`
- Move cursor to the beginning of localhost where it is on the l and enter `'cw'` (change word)
- Enter the Host name for the Monitoring Database Node
- Enter your domain name
- when done: press `'esc'`
- enter `':wq!'`
- Verify changes were saved: `'cat /etc/sysconfig/network'`

```
[root@localhost ~]# cat /etc/sysconfig/network
NETWORKING=yes
NETWORKING_IPV6=yes
HOSTNAME=CUCSD-M-5_4_0_0
DOMAINNAME=gsp-r5.cloudlab.cisco.com
[root@localhost ~]#
```

Change the hostname.

```
[root@localhost ~]# hostname CUCSD-M-5_4_0_0
[root@localhost ~]# hostname
CUCSD-M-5_4_0_0
[root@localhost ~]#
```

Log out and log back into the Monitoring Database and you will see the new hostname.

```
[root@CUCSD-M-5_4_0_0 ~]#
```

Verify NTP servers for Monitoring Database Node are configured and synced. SSH into Monitoring Database Node using root account.

- Create ntp user: `'useradd ntp'` **Note:** If the ntp user already exist, the system will let you know.
- Restart the ntpd services: `'service ntpd restart'`
- Verify configured NPT servers: `'ntpq -p'`
- The `'*'` next to the NTP server IP address indicates the Monitoring Node is synced to the NTP server.

```
[root@CUCSD-M-5_4_0_0 ~]# useradd ntp
useradd: user 'ntp' already exists
[root@CUCSD-M-5_4_0_0 ~]# service ntpd restart
Shutting down ntpd: [ OK ]
Starting ntpd: [ OK ]
[root@CUCSD-M-5_4_0_0 ~]# ntpq -p
=====
remote          refid          st t when poll reach  delay  offset  jitter
=====
*173.30.102.254 LOCAL(1)      5 u  6  64   1   1.445  2.928  0.000
[root@CUCSD-M-5_4_0_0 ~]#
```

Optional: If you need to configure multiple NTP servers you can do so by editing the ntp.conf file.

- Edit the ntp.conf file: **'vi /etc/ntp.conf'**
- cursor down to the **'server'** line
- press **'shit + a'** for insert and go to the end of the line
- press return to create a new line
- enter **'server your ip address'** of your NTP server IP address
- press **'esc'**, then enter **':wq!'** to quit and write the info
- Verify the config changes: **'cat /etc/ntp.conf'**

```
[root@CUCSD-M-5_4_0_0 ~]# cat /etc/ntp.conf
# For more information about this file, see the man pages
# ntp.conf(5), ntp_acc(5), ntp_auth(5), ntp_clock(5), ntp_misc(5), ntp_mon(5).

driftfile /var/lib/ntp/drift

# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery

# Permit all access over the loopback interface. This could
# be tightened as well, but to do so would effect some of
# the administrative functions.
restrict 127.0.0.1
restrict -6 ::1

# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

#broadcast 192.168.1.255 autokey          # broadcast server
#broadcastclient                          # broadcast client
#broadcast 224.0.1.1 autokey             # multicast server
#multicastclient 224.0.1.1               # multicast client
#manycastserver 239.255.254.254          # manycast server
#manycastclient 239.255.254.254 autokey  # manycast client

# Enable public key cryptography.
#crypto

includefile /etc/ntp/crypto/pw

# Key file containing the keys and key identifiers used when operating
# with symmetric key cryptography.
keys /etc/ntp/keys

# Specify the key identifiers which are trusted.
#trustedkey 4 8 42

# Specify the key identifier to use with the ntpdc utility.
#requestkey 8

# Specify the key identifier to use with the ntpq utility.
#controlkey 8

# Enable writing of statistics records.
#statistics clockstats cryptostats loopstats peerstats

server 173.57.132.254
[root@CUCSD-M-5_4_0_0 ~]# █
```

If you edited the ntp.conf file, you must restart the ntpd service and check the NTP synchronization. It may take a while but when the clock is synced with the NTP server there will be a **'*'** to the left of the IP address.

- Restart the ntpd services: **'service ntpd restart'**
- View the configured ntp servers and check for synchronization: **'ntpq -p'**

```
[root@CUCSD-M-5_4_0_0 ~]# service ntpd restart
Shutting down ntpd: [ OK ]
Starting ntpd: [ OK ]
[root@CUCSD-M-5_4_0_0 ~]# ntpq -p
      remote           refid      st t when poll reach  delay  offset  jitter
-----
*173.57.132.254 LOCAL(1)      5 u   6   64    1   1.445   2.928   0.000
[root@CUCSD-M-5_4_0_0 ~]#
```

Change the time zone to the local timezone where the Primary Node, Inventory Database Service Nodes and the Monitoring Database reside. This will ensure the logs will match everywhere.

- Determine the current timezone: `'ls -l /etc/localtime'`
- Determine your timezone if your in America: `'ls /usr/share/zoneinfo/America/'`
- This deployment is in Dallas so I will choose `'Chicago'` for Central Standard Time.

```
[root@CUCSD-M-5_4_0_0 ~]# ls -l /etc/localtime
lrwxrwxrwx. 1 root root 27 Nov  4 19:23 /etc/localtime -> /usr/share/zoneinfo/Etc/UTC
[root@CUCSD-M-5_4_0_0 ~]# ls /usr/share/zoneinfo/America/
Adak          Campo_Grande  Etropole      Jamaica      Metlakatla   Port_of_Spain St_Lucia
Anchorage     Cancun         El_Salvador  Jujuy        Mexico_City   Porto_Velho   St_Thomas
Anguilla      Caracas        Ensenada     Juneau       Miquelon     Puerto_Rico   St_Vincent
Antigua       Catamarca     Fortaleza    Kentucky     Moncton       Rainy_River   Swift_Current
Araguaina     Cayenne       Fort_Wayne    Knox_IN      Monterrey     Rankin_Inlet  Tegucigalpa
Argentina     Cayman        Glace_Bay    Kralendijk   Montevideo    Recife        Thule
Aruba         Chicago       Godthab      La_Paz       Montreal     Regina        Thunder_Bay
Asuncion      Chihuahua     Goose_Bay    Lima         Montserrat   Resolute      Tijuana
Atikokan      Coral_Harbour Grand_Turk    Los_Angeles  Nassau        Rio_Branco    Toronto
Atka          Cordoba       Grenada      Louisville   New_York      Rosario       Tortola
Bahia         Costa_Rica    Guadeloupe   Lower_Prices Nipigon       Santa_Isabel  Vancouver
Bahia_Banderas Creston        Guatemala    Maceio       Nome           Santarem      Virgin
Barbados      Cuiaba        Guayaquil    Managua      Noronha       Santiago      Whitehorse
Belem         Curacao       Guyana       Manaus       North_Dakota  Santo_Domingo Winnipeg
Belize        Darmarkshavn Halifax       Marigot      Ojinaga       Sao_Paulo     Yakutat
Blanc-Sablon Dawson         Havana       Martinique   Panama         Scoresbysund  Yellowknife
Boa_Vista     Dawson_Creek Hermosillo    Matamoros    Pangnirtung   Shiprock
Bogota        Denver        Indiana      Mazatlan     Paramaribo    Sitka
Boise         Detroit       Indianapolis Mendoza        Phoenix       St_Barthelemy
Buenos_Aires Dominica      Inuvik       Menominee    Port-au-Prince St_Johns
Cambridge_Bay Edmonton     Iqaluit      Merida       Porto_Acre    St_Kitts
```

Change the timezone and verify. I have chosen the Central Time Zone for my location.

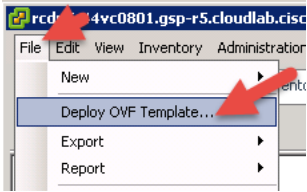
- Copy the localtime to new file named old.timezone: `'cp /etc/localtime /root/old.timezone'`
- Remove the localtime file: `'rm -f /etc/localtime'`
- Create the new localtime file: `'ln -s /usr/share/zoneinfo/America/Chicago /etc/localtime'`
- Verify the timzone is what you set it to: `'date'`
- Verify the link: `'ls -l /etc/localtime'`

```
[root@CUCSD-M-5_4_0_0 ~]# cp /etc/localtime /root/old.timezone
[root@CUCSD-M-5_4_0_0 ~]# rm -f /etc/localtime
[root@CUCSD-M-5_4_0_0 ~]# ln -s /usr/share/zoneinfo/America/Chicago /etc/localtime
[root@CUCSD-M-5_4_0_0 ~]# date
Fri Nov  6 10:11:50 CST 2015
[root@CUCSD-M-5_4_0_0 ~]# ls -l /etc/localtime
lrwxrwxrwx. 1 root root 35 Nov  6 10:11 /etc/localtime -> /usr/share/zoneinfo/America/Chicago
[root@CUCSD-M-5_4_0_0 ~]#
```

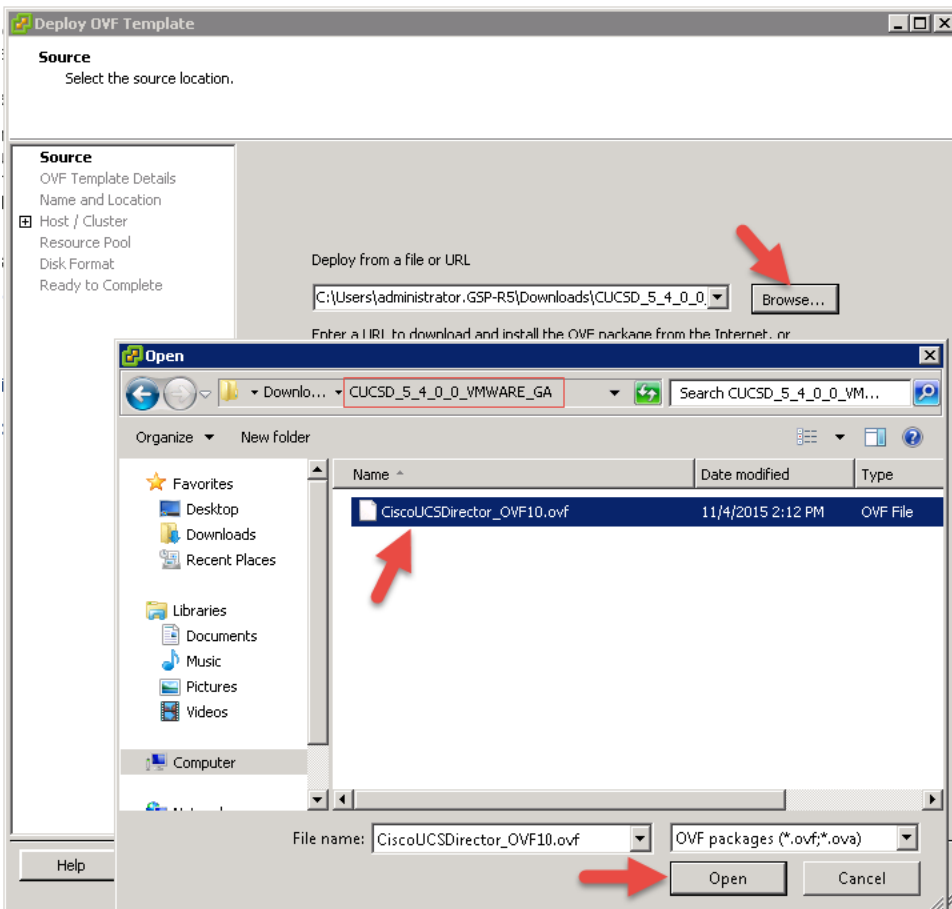

4. Create the Primary Node

4.1. Create Primary Node VM

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



Browse to the "CiscoUCSDirector_OVF10.ovf", select it for deployment then click 'Next'.



Verify details and click 'Next'.

The screenshot shows the 'Deploy OVF Template' window with the 'OVF Template Details' section active. The window title is 'Deploy OVF Template'. Below the title bar, it says 'OVF Template Details' and 'Verify OVF template details.' On the left, there is a navigation pane with the following items: 'Source', 'OVF Template Details' (selected), 'End User License Agreement', 'Name and Location', 'Host / Cluster', 'Resource Pool', 'Disk Format', 'Properties', and 'Ready to Complete'. The main area displays the following details:

Product:	CUCSD-5.4.0.0
Version:	5.4.0.0
Vendor:	Cisco Systems
Publisher:	No certificate present
Download size:	4.3 GB
Size on disk:	7.6 GB (thin provisioned) 100.0 GB (thick provisioned)
Description:	Cisco UCS Director 5.4.0.0 (Emerald Bay)

Below the table, there is a note: 'Note: It is mandatory to reserve vCPU and Memory as recommended by Installation and Deployment guide.'

Accept the license agreement and click 'Next'.

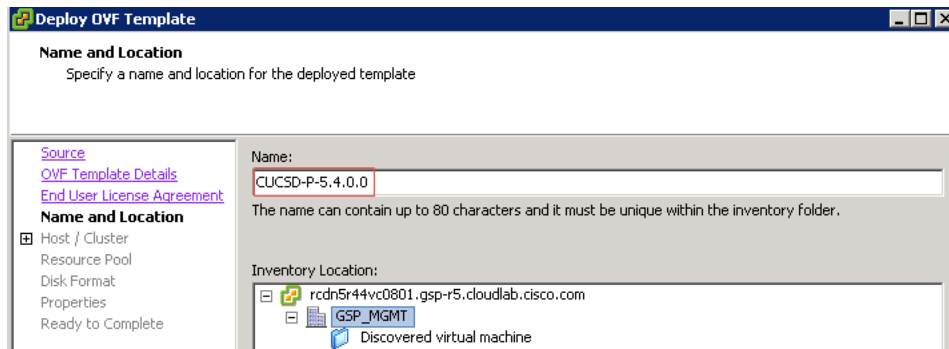
The screenshot shows the 'Deploy OVF Template' window with the 'End User License Agreement' section active. The window title is 'Deploy OVF Template'. Below the title bar, it says 'End User License Agreement' and 'Accept the end user license agreements.' On the left, there is a navigation pane with the following items: 'Source', 'OVF Template Details', 'End User License Agreement' (selected), 'Name and Location', 'Storage', 'Disk Format', 'Network Mapping', 'Properties', and 'Ready to Complete'. The main area displays the following text:

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.

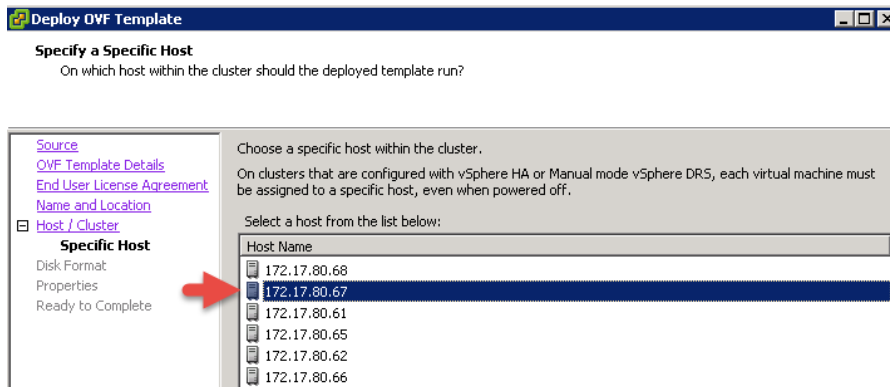
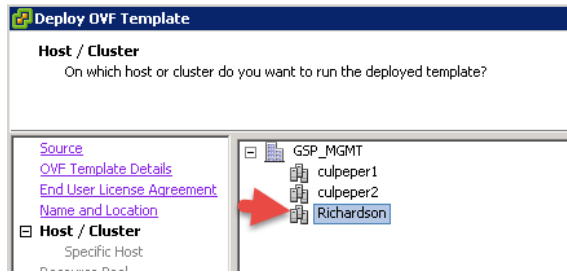
CISCO SYSTEMS, INC. OR ITS AFFILIATE LICENSING THE SOFTWARE ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS 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,

At the bottom of the text area, there is an 'Accept' button with a red arrow pointing to it. Below the text area, there are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button.

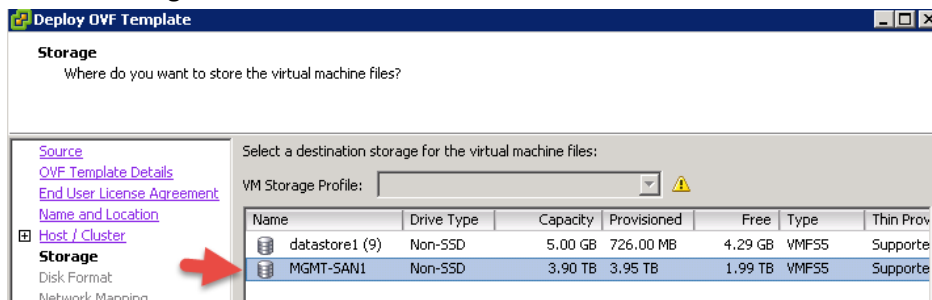
Name the VM and click 'Next'.



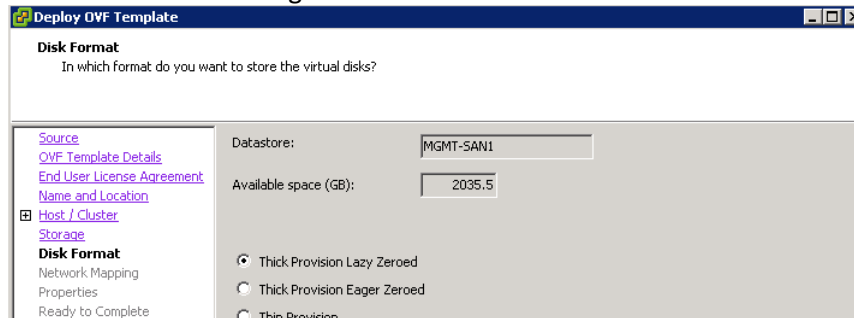
Select Cluster/Host to deploy this VM on and click 'Next'.



Select a storage location to install the VM and click 'Next'.



Leave the default settings for the Disk Format and click 'Next'.



Select the Network to put this VM on and click 'Next'.

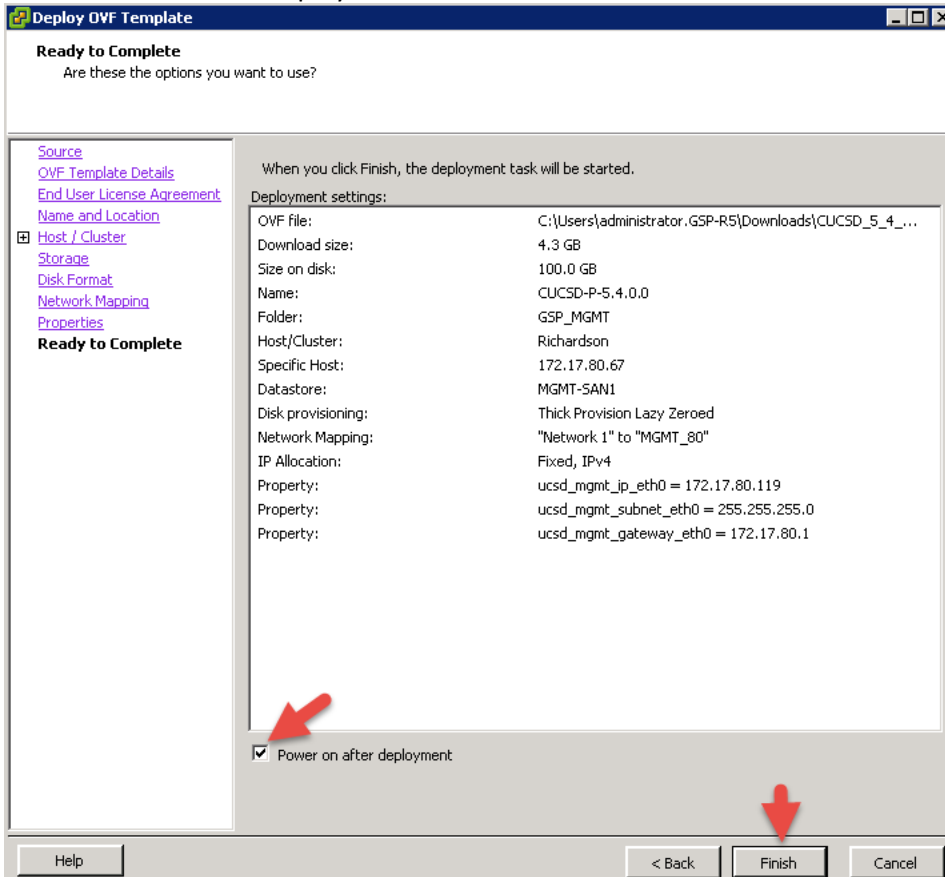
The screenshot shows the 'Deploy OVF Template' wizard at the 'Network Mapping' step. The title bar reads 'Deploy OVF Template'. Below the title bar, the text says 'Network Mapping' and 'What networks should the deployed template use?'. On the left, there is a navigation pane with links: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location', 'Host / Cluster' (selected), and 'Storage'. The main area contains the instruction 'Map the networks used in this OVF template to networks in your inventory' and a table with two columns: 'Source Networks' and 'Destination Networks'. The table has one row with 'Network 1' in the source column and 'MGMT_80' in the destination column.

Source Networks	Destination Networks
Network 1	MGMT_80

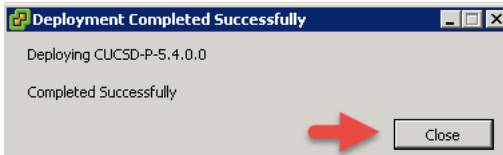
Enter a password for Root and Shelladmin Accounts, Management IP Address, Subnet Mask, Gateway and click 'Next'.

The screenshot shows the 'Deploy OVF Template' wizard at the 'Properties' step. The title bar reads 'Deploy OVF Template'. Below the title bar, the text says 'Properties' and 'Customize the software solution for this deployment.'. On the left, there is a navigation pane with links: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location', 'Host / Cluster' (selected), 'Storage', 'Disk Format', 'Network Mapping', and 'Properties'. The main area is titled 'Application' and contains several sections for configuration: 'Root Password' with 'Enter password' and 'Confirm password' fields (both containing '*****'); 'Shelladmin Password' with 'Enter password' and 'Confirm password' fields (both containing '*****'); 'Management IP Address' with a text input field containing '172 . 17 . 80 . 119' and the instruction 'Enter Management IP Address for eth0. Set 0.0.0.0 to use DHCP'; 'Management IP Subnet Mask' with a text input field containing '255 . 255 . 255 . 0' and the instruction 'Enter Management IP Subnet Mask for eth0. Set 0.0.0.0 to use DHCP'; and 'Gateway IP Address' with a text input field containing '172 . 17 . 80 . 1'. At the bottom, there are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

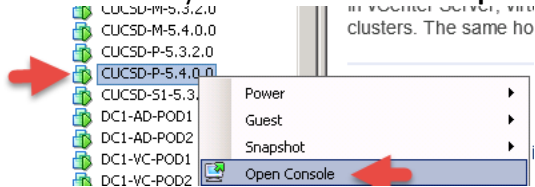
Select Power on after deployment and click **'Finish'**.



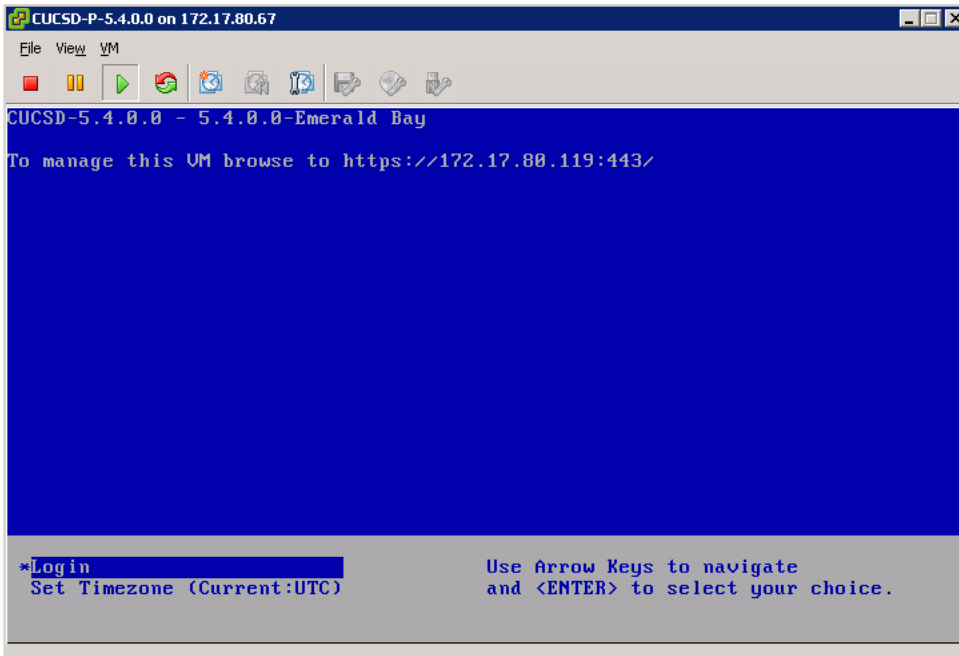
After deployment click **'Close'**.



Select the Primary Node VM and select **'Open Console'**.

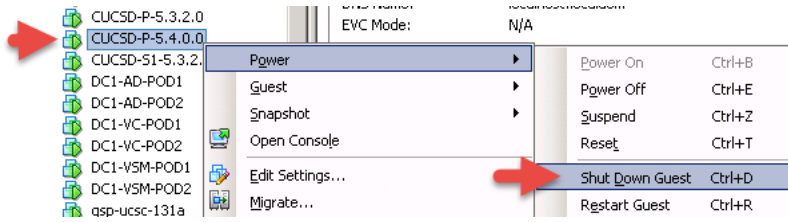


Monitor the console until the installation is complete and you will see a screen similar to the one below. The installation will take several minutes to complete so be patient.

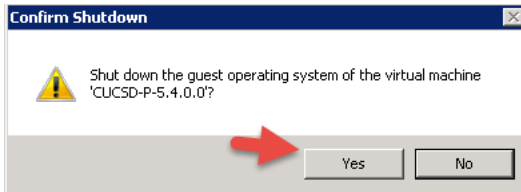


4.2. Install/Update VMWare tools & VM Version

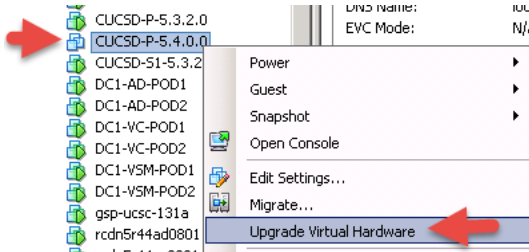
Navigate to the Primary Node VM and select **'Shut Down Guest'**.



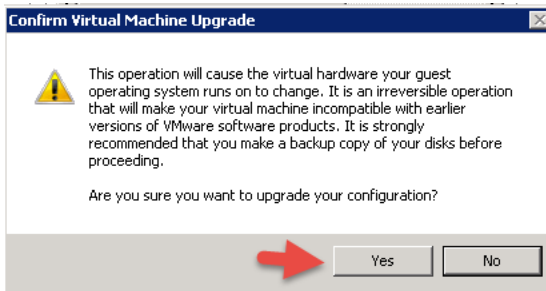
Select **'Yes'**.



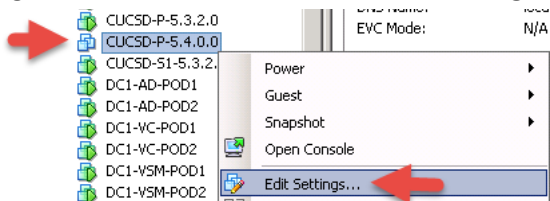
Wait for the VM to completely shut down then right click on the VM and select **'Upgrade Virtual Hardware'**.



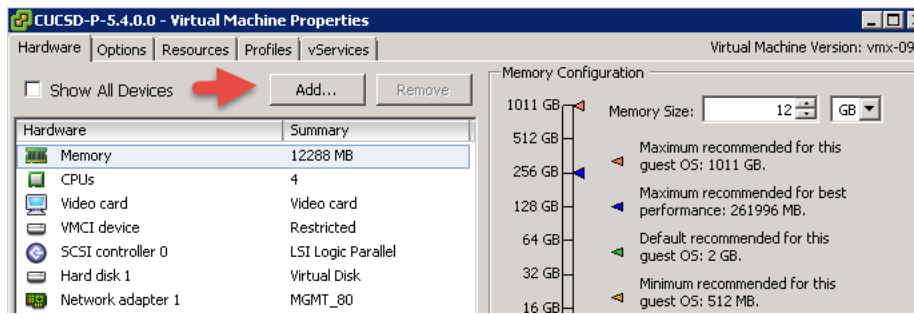
Select **'Yes'**.



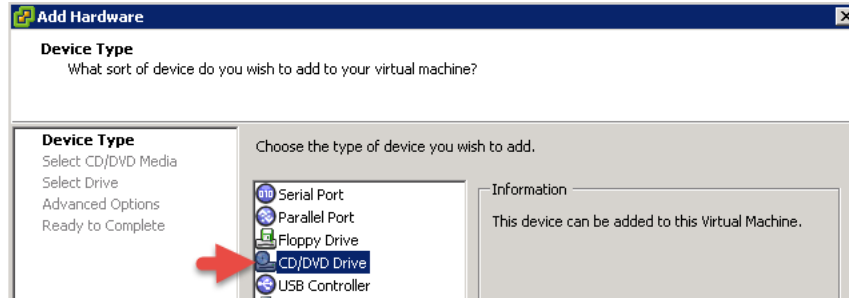
Right click on the VM and Select **'Edit Settings'**.



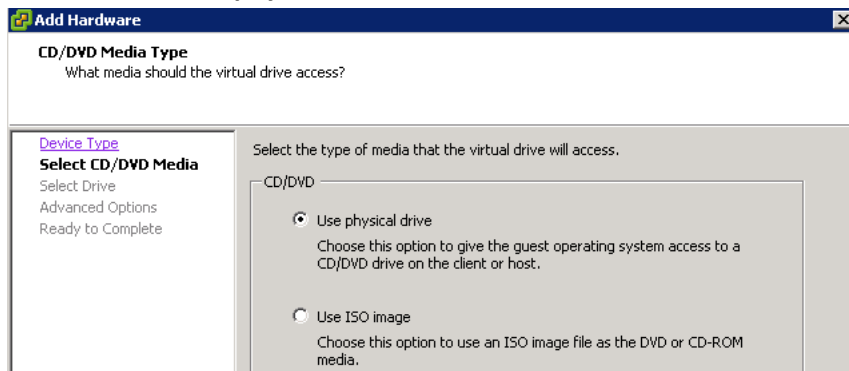
Click 'Add'.



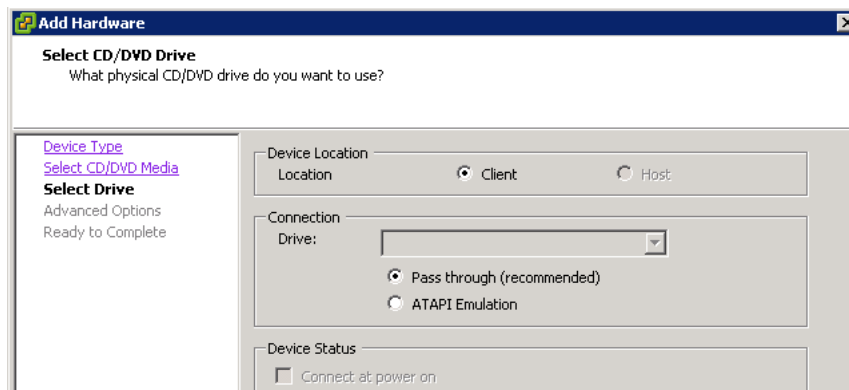
Select 'CD/DVD Drive' and click 'Next'.



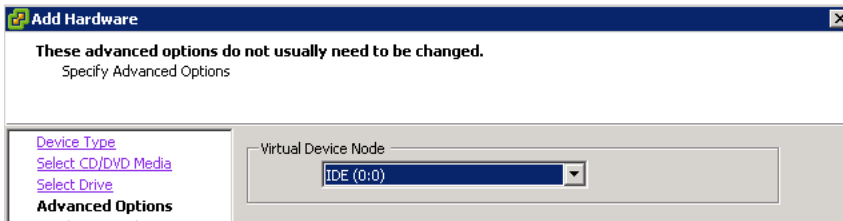
Leave default 'Use physical drive' and click 'Next'.



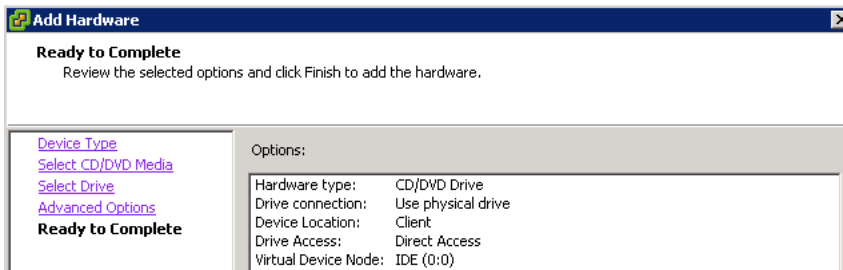
Leave default and click 'Next'.



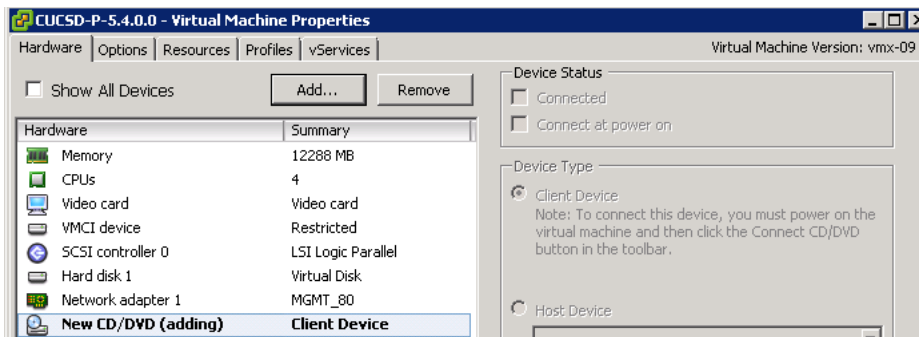
Leave default and click 'Next'.



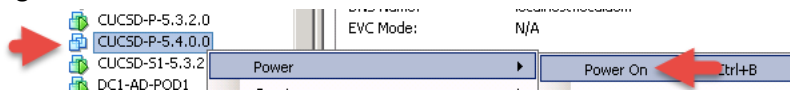
Review and click 'Finish'.



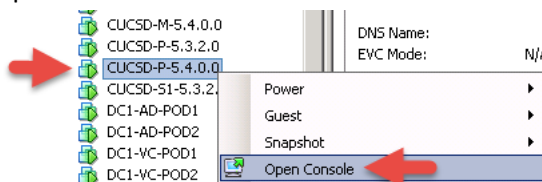
Review and click 'OK'.



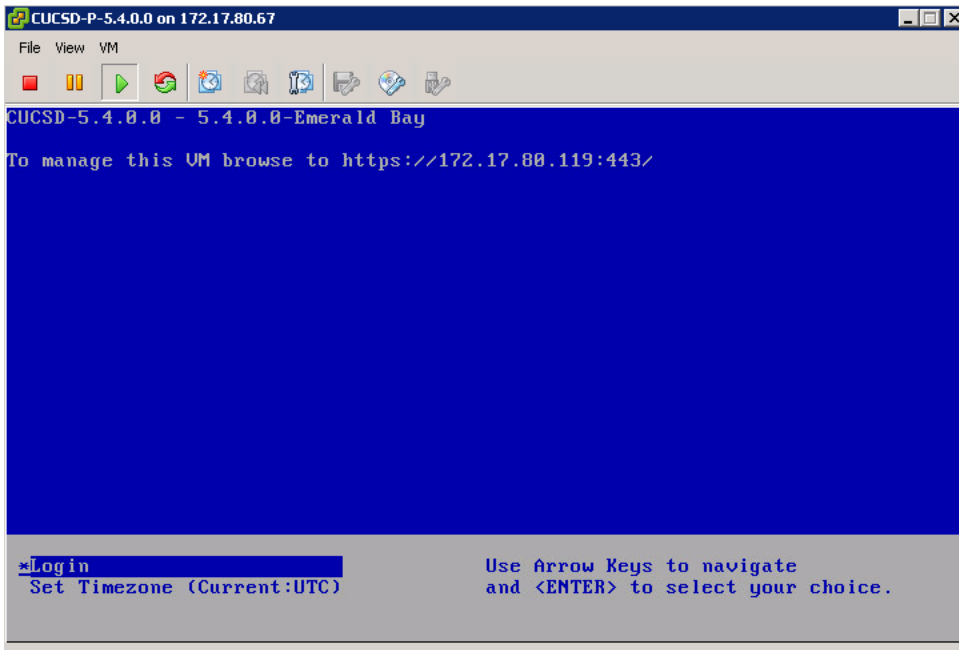
Right click on the VM and select 'Power On'.



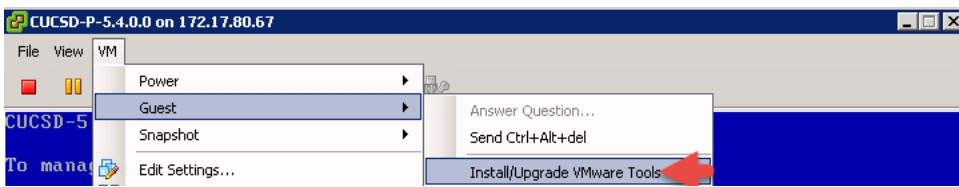
Open the VM Console to watch the VM Boot. Right click on the VM and select 'Open Console'.



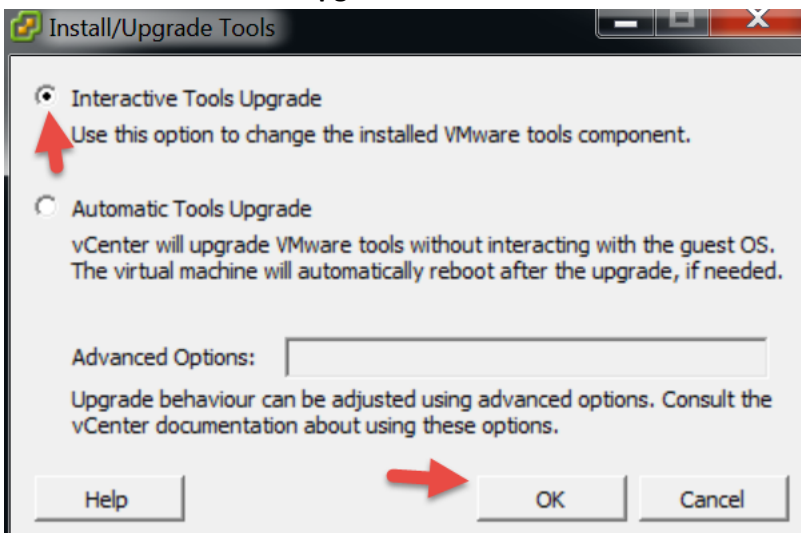
Once the VM is completely up, you should see the login screen similar to below.



From the console, select 'Install/Upgrade VMware Tools'.



Select 'Interactive Tools Upgrade' and click 'OK'.



SSH to the Primary Node and login using the root account.

- Make a dir for cdrom: `'mkdir /mnt/cdrom'`
- Mount the cdrom: `'mount /dev/cdrom /mnt/cdrom'`
- Copy vmware install to /tmp: `'cp /mnt/cdrom/VMwareTools-5.0.0-<xxxx>.tar.gz /tmp/'` **Note:** tab out the VMware tools part so you don't have to figure out the correct name.
- Unzip the files in /tmp: `'tar xzf /tmp/VMwareTools-5.0.0-<xxxx>.tar.gz'` **Note:** tab out the VMware tools part so you don't have to figure out the correct name.
- Change directory: `'cd vmware-tools-distrib'`
- Run the install: `'./vmware-install.pl'`
- Accept all the defaults by Pressing Enter for all the options.

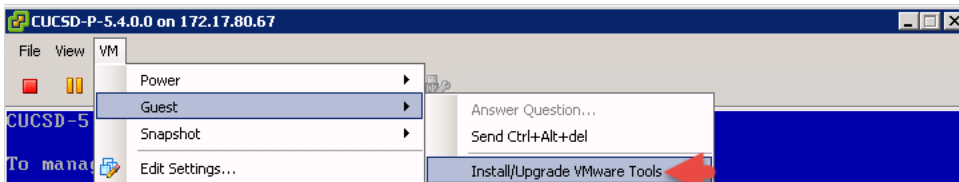
Note: You will probably get the following message.

VMware Tools cannot be installed, since they have already been installed using a package-based mechanism (rpm or deb) on this system. If you wish to continue, you must first remove the currently installed VMware Tools using the appropriate packaged-based mechanism, and then restart this installer
Execution aborted.

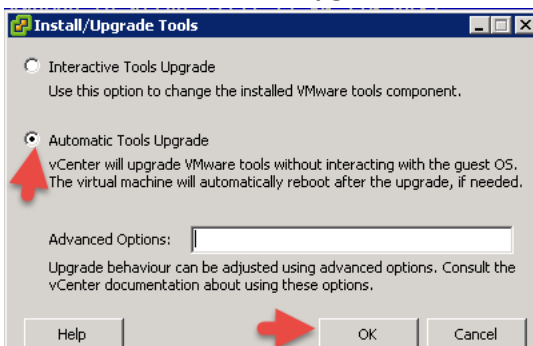
Found VMware Tools CDROM mounted at /mnt/cdrom. Ejecting device /dev/cdrom ... No eject (or equivalent) command could be located. Eject Failed: If possible manually eject the Tools installer from the guest cdrom mounted at /mnt/cdrom before canceling tools install on the host.

- If you get this message, we need to Delete the VMware tools directory: `'rm -rf /usr/lib/vmware-tools/'`
- Change directory: `'cd vmware-tools-distrib/'`
- Re-Run the install: `'./vmware-install.pl'`
- Enter **'Yes'** to the 'Would you like to remove the install DB?' You will probably get a Failure and Execution aborted.
- Re-Run the install: `'./vmware-install.pl'`
- Accept all the defaults by Pressing Enter for all the options.

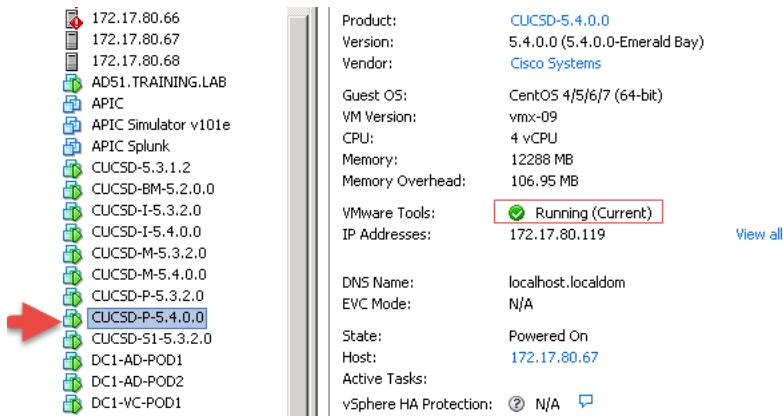
From the console, select **'Install/Upgrade VMware Tools'**.



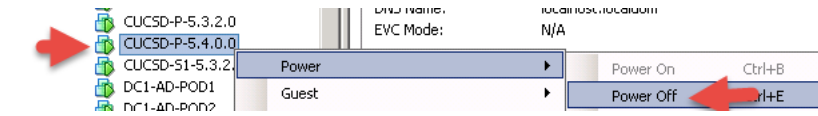
Select **'Automatic Tools Upgrade'** and click **'OK'**.



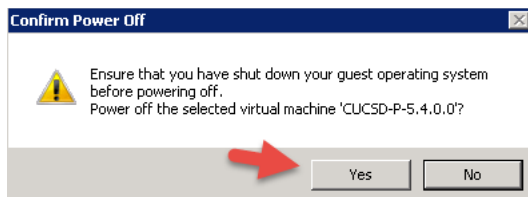
Verify Tools have been installed and **Running (Current)** as shown below.



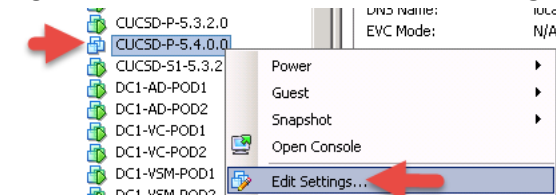
Power off the VM, **Power Off**.



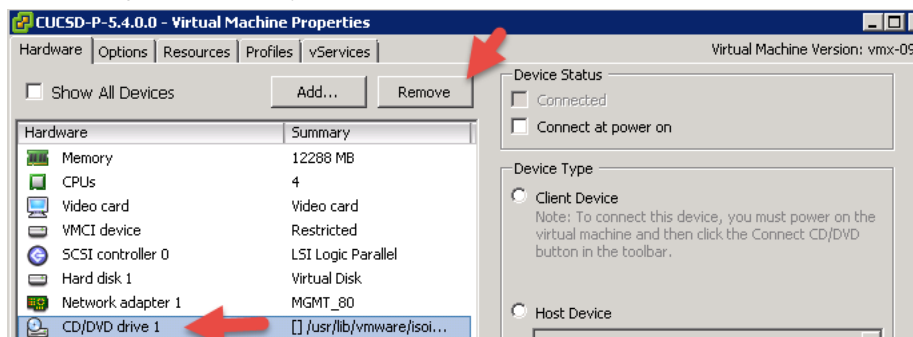
Select **Yes**.



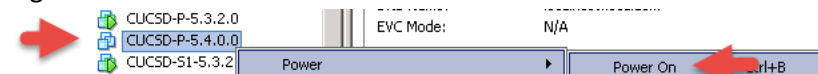
Right click on the VM and select **Edit Settings**.



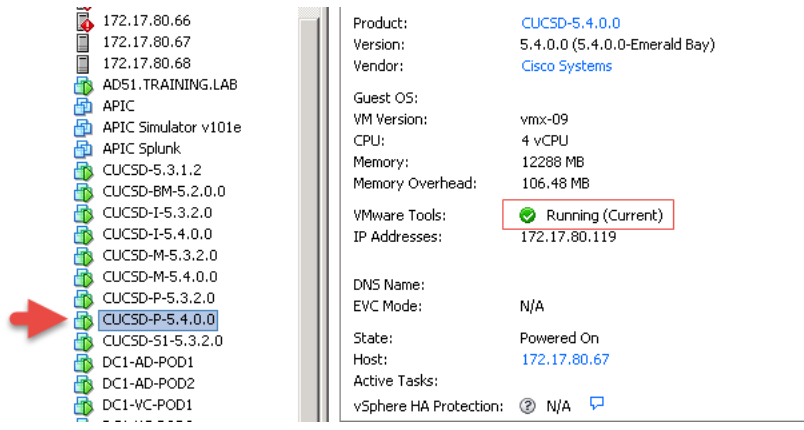
Select **CD/DVD drive 1**, click **Remove** and then click **OK**.



Right click on the VM and Select **Power On**.



Wait for the VM to completely boot up and then verify Tools have been installed and 'Running (Current)'.



The screenshot displays a vSphere interface with a VM inventory list on the left and a details pane on the right. A red arrow points to the VM 'CUCSD-P-5.4.0.0' in the inventory. The details pane for this VM shows the following information:

Product:	CUCSD-5.4.0.0
Version:	5.4.0.0 (5.4.0.0-Emerald Bay)
Vendor:	Cisco Systems
Guest OS:	
VM Version:	vmx-09
CPU:	4 vCPU
Memory:	12288 MB
Memory Overhead:	106.48 MB
VMware Tools:	Running (Current)
IP Addresses:	172.17.80.119
DNS Name:	
EVC Mode:	N/A
State:	Powered On
Host:	172.17.80.67
Active Tasks:	
vSphere HA Protection:	N/A

4.3. Configure Primary Node

SSH to the Primary Node using the shelladmin account.

Configure NTP Server. From the Menu select 9 'Time Sync'. Replace the NTP IP Address with your NTP Server.

```
SELECT> 9
Time Sync.....
System time is Fri Nov  6 02:19:24 UTC 2015
Hardware time is Fri 06 Nov 2015 02:19:25 AM UTC  -0.656583 seconds
Do you want to sync systemtime [y/n]? y
System time reset to hardware clock
Do you want to sync to NTP [y/n]? y
Enter NTP server to sync time with: 173.37.102.254
ntpd (pid 1868) is running...
shutting down ntpd: [ OK ]
 6 Nov 02:19:42 ntpdate[3631]: adjust time server 173.37.102.254 offset 0.001981 sec
synchronized time with NTP server '173.37.102.254'
Added NTP server '173.37.102.254' to /etc/ntp.conf
Starting ntpd: [ OK ]
synchronised to NTP server (173.37.102.254) at stratum 6
  time correct to within 7940 ms
  polling server every 64 s
Press return to continue ...
```

From the menu, choose (24) 'Configure Multi Node Setup (Advanced Deployment)' and press Enter.

- Enter '1' to configure the current node.
- Enter 'y' when asked if you want to configure multi node setup.
- Enter 'a' to Configure the node as Primary Node.
- Enter 'y' when asked if you want to configure this node as Primary Node.
- Enter 'a' when asked to select the IP version you want to configure.
- Enter 'Inventory DB IP' when asked to Provide the Inventory DB IP.
- Enter 'Monitoring DB IP' when asked to Provide the Monitoring DB IP.
- When prompted to logout, enter 'y' and press enter. Log back in as shelladmin by entering 'su shelladmin'

```
SELECT> 24
*****
This wizard helps to do Multi Node setup
*****
Configuration Options :
Current Node --> Select '1'
Remote Node  --> Select '2'
exit         --> Select '3'

Please enter an option: 1
*****
Cisco UCS Director Multi Node Setup requires multiple instances of UCS Director oVf deployed with different configurations. Following are the required configurations:

* UCS Director Primary Node (1 Instance) . This node also acts as a front end UI node
* UCS Director Service Node (1 or more instances ). Service node can be reconfigured as Primary Node when necessary.
* UCS Director Inventory DB Node (1 Instance)
* UCS Director Monitoring DB Node (1 Instance)

Refer to UCS Director documentation for additional details on Multi Node Setup.
*****

This is a standalone Node

Do you want to configure multi node setup [y/n]? y

Select a option from the menu below

a) Configure as Primary Node
b) Configure as Service Node
c) Configure as Inventory DB
d) Configure as Monitoring DB
x) Exit

Enter: [a/b/c/d/x]? a
Do you want to configure this node as Primary Node [y/n]? y
Configuring Primary Node
Stopping UCS Director Services
Select the IP version you want to configure [a) IPv4, b) IPv6] a/b : a
Provide Inventory DB IP:172.17.80.120
Provide Monitoring DB IP:172.17.80.121
Starting UCS Director Services
Checking MySQL database status... UP
Started service broker [PID=3530]
Started service controller [PID=3556]
Started service eventmgr [PID=3589]
Started service client [PID=3621]
Started service idaccessmgr [PID=3656]
Started service inframgr [PID=3700]
Started service tomcat [PID=3723]
Started service websock [PID=3778]
Configured Primary Node Successfully
In order for changes to take effect logout and login back
Do you want to logout [y/n]? y
```

Verify the services for the Primary Node are up and running, choose (2) 'Display Service Status' and press Enter. You should see the lines in the red box below. **Note:** After you return to the shelladmin, the menu options change to those available for a Primary node.

```
Cisco UCS Director Shell Menu
```

```
Primary Node
```

```
Select a number from the menu below
```

- 1) Change ShellAdmin Password
- 2) Display Services Status
- 3) Stop Services
- 4) Start Services
- 5) Time Sync
- 6) Ping Hostname/IP Address
- 7) Show Version
- 8) Generate Self-signed Certificate and Certificate Signing Request
- 9) Import CA/Self-signed Certificate
- 10) Configure Network Interface
- 11) Display Network Details
- 12) Add Cisco UCS Director Baremetal Agent Hostname/IP
- 13) Tail Inframgr Logs
- 14) Apply Patch
- 15) Shutdown Appliance
- 16) Reboot Appliance
- 17) Manage Root Access
- 18) Login as Root
- 19) Configure Multi Node Setup (Advanced Deployment)
- 20) Clean-up Patch Files
- 21) Collect logs from a Node
- 22) Backup Database
- 23) Quit

```
SELECT> 2
```

Service	Status	PID
broker	RUNNING	3530
controller	RUNNING	3556
eventmgr	RUNNING	3589
client	RUNNING	3621
idaccessmgr	RUNNING	3656
inframgr	RUNNING	3700
tomcat	RUNNING	3723
websock	RUNNING	3778

Node Type : primary
Inventory DB(172.17.80.120:3306) status : UP
Monitor DB(172.17.80.121:3306) status : UP
Press return to continue ...

Edit the /etc/hosts file to update the name and IP address of the host. SSH to the Primary Node using the root account.

- Edit the hosts file: 'vi /etc/hosts'
- Go to the end of the line: 'shift + a'
- Create a new line: press return
- enter your host details: example shown below
- when done: press 'esc'
- enter ':wq!'
- Verify the hosts file has been saved: 'cat /etc/hosts'

```
[root@localhost ~]# cat /etc/hosts
127.0.0.1 localhost.localdomain localhost localhost
172.17.80.120 CUCSD-I-5_4_0_0
172.17.80.121 CUCSD-M-5_4_0_0
172.17.80.122 CUCSD-S-5_4_0_0
172.17.80.119 CUCSD-P-5_4_0_0
:1 localhost.localdomain localhost localhost ip6-localhost ip6-loopback
[root@localhost ~]#
```

Edit the /etc/resolv.conf to update the DNS servers.

- Edit the resolv.conf file: `'vi /etc/resolv.conf'`
- press `'i'` for insert
- enter `'search localhost your domain name'`, **Note:** Sometime search localhost is already there
- enter dns server ip address after nameserver, **Note:** if you have multiple DNS servers, enter on separate lines
- when done: press `'esc'`
- enter `':wq!'`
- Example:

```
search localhost gsp-r5.cloudlab.cisco.com
nameserver 172.17.80.104
nameserver 8.8.8.8
nameserver 8.8.4.4
```

- Verify the changes: `'cat /etc/resolv.conf'`

```
[root@localhost ~]# cat /etc/resolv.conf
; generated by /sbin/dhclient-script
search localhost gsp-r5.cloudlab.cisco.com
nameserver 172.17.80.104
nameserver 8.8.8.8
nameserver 8.8.4.4
[root@localhost ~]# █
```

Edit the hostname in /etc/sysconfig/network

- Edit the network config: `'vi /etc/sysconfig/network'`
- Move cursor to the beginning of localhost where it is on the l and enter `'cw'` (change word)
- Enter the Host name for the Monitoring Database Node
- Enter your domain name
- when done: press `'esc'`
- enter `':wq!'`
- Verify changes were saved: `'cat /etc/sysconfig/network'`

```
[root@localhost ~]# cat /etc/sysconfig/network
NETWORKING=yes
NETWORKING_IPV6=yes
HOSTNAME=CUCSD-P-5_4_0_0
DOMAINNAME=gsp-r5.cloudlab.cisco.com
[root@localhost ~]# █
```

Change the hostname.

```
[root@localhost ~]# hostname CUCSD-P-5_4_0_0
[root@localhost ~]# hostname
CUCSD-P-5_4_0_0
[root@localhost ~]# █
```

Log out and log back into the Primary Node and you will see the new hostname.

```
[root@CUCSD-P-5_4_0_0 ~]#
```

Verify NTP servers for Primary Node are configured and synced. SSH into Primary Node using root account.

- Create ntp user: `'useradd ntp'` **Note:** If the ntp user already exist, the system will let you know.
- Restart the ntpd services: `'service ntpd restart'`
- Verify configured NPT servers: `'ntpq -p'`
- The `'*'` next to the NTP server IP address indicates the Primary Node is synced to the NTP server.

```
[root@CUCSD-P-5_4_0_0 ~]# useradd ntp
useradd: user 'ntp' already exists
[root@CUCSD-P-5_4_0_0 ~]# service ntpd restart
Shutting down ntpd: [ OK ]
Starting ntpd: [ OK ]
[root@CUCSD-P-5_4_0_0 ~]# ntpq -p
=====
remote          refid          st t when poll reach  delay  offset  jitter
=====
*173.30.172.254 LOCAL(1)      5 u   7   64    1   1.172  10.992  0.000
[root@CUCSD-P-5_4_0_0 ~]# █
```


Optional: If you need to configure multiple NTP servers you can do so by editing the ntp.conf file.

- Edit the ntp.conf file: **'vi /etc/ntp.conf'**
- cursor down to the **'server'** line
- press **'shit + a'** for insert and go to the end of the line
- press return to create a new line
- enter **'server your ip address'** of your NTP server IP address
- press **'esc'**, then enter **':wq!'** to quit and write the info
- Verify the config changes: **'cat /etc/ntp.conf'**

```
[root@CUCSD-P-5_4_0_0 ~]# cat /etc/ntp.conf
# For more information about this file, see the man pages
# ntp.conf(5), ntp_acc(5), ntp_auth(5), ntp_clock(5), ntp_misc(5), ntp_mon(5).

driftfile /var/lib/ntp/drift

# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery

# Permit all access over the loopback interface. This could
# be tightened as well, but to do so would effect some of
# the administrative functions.
restrict 127.0.0.1
restrict -6 ::1

# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

#broadcast 192.168.1.255 autokey          # broadcast server
#broadcastclient                          # broadcast client
#broadcast 224.0.1.1 autokey             # multicast server
#multicastclient 224.0.1.1               # multicast client
#manycastserver 239.255.254.254          # manycast server
#manycastclient 239.255.254.254 autokey  # manycast client

# Enable public key cryptography.
#crypto

includefile /etc/ntp/crypto/pw

# Key file containing the keys and key identifiers used when operating
# with symmetric key cryptography.
keys /etc/ntp/keys

# Specify the key identifiers which are trusted.
#trustedkey 4 8 42

# specify the key identifier to use with the ntpdc utility.
#requestkey 8

# specify the key identifier to use with the ntpq utility.
#controlkey 8

# Enable writing of statistics records.
#statistics clockstats cryptostats loopstats peerstats

server 173.202.222.254
[root@CUCSD-P-5_4_0_0 ~]#
```

If you edited the ntp.conf file, you must restart the ntpd service and check the NTP synchronization. It may take a while but when the clock is synced with the NTP server there will be a '*' to the left of the IP address.

- Restart the ntpd services: **'service ntpd restart'**
- View the configured ntp servers and check for synchronization: **'ntpq -p'**

```
[root@CUCSD-P-5_4_0_0 ~]# service ntpd restart
Shutting down ntpd: [ OK ]
Starting ntpd: [ OK ]
[root@CUCSD-P-5_4_0_0 ~]# ntpq -p
      remote           refid      st t when poll reach  delay  offset  jitter
-----
*173.202.222.254 LOCAL(1)      5 u   5  64   1   1.162   9.541   0.000
[root@CUCSD-P-5_4_0_0 ~]#
```

Change the time zone to the local timezone where the Primary Node, Inventory Database Service Nodes and the Monitoring Database reside. This will ensure the logs will match everywhere.

- Determine the current timezone: `'ls -l /etc/localtime'`
- Determine your timezone if your in America: `'ls /usr/share/zoneinfo/America/'`
- This deployment is in Dallas so I will choose **'Chicago'** for Central Standard Time.

```
[root@CUCSD-P-5_4_0_0 ~]# ls -l /etc/localtime
lrwxrwxrwx. 1 root root 27 Nov  4 19:23 /etc/localtime -> /usr/share/zoneinfo/Etc/UTC
[root@CUCSD-P-5_4_0_0 ~]# ls /usr/share/zoneinfo/America/
Adak      Campo_Grande  Eirunepe      Jamaica      Metlakatla    Port_of_Spain  St_Lucia
Anchorage Cancun         El_Salvador   Jujuy        Mexico_City    Porto_Velho    St_Thomas
Anguilla  Caracas       Ensenada      Juneau       Miquelon      Puerto_Rico    St_Vincent
Antigua  Catamarca     Fortaleza     Kentucky     Moncton        Rainy_River    Swift_Current
Araguaina Cayenne       Fort_Wayne    Knox_IN      Monterrey      Rankin_Inlet   Tegucigalpa
Argentina Cayman        Glace_Bay     Kralendijk   Montevideo     Recife         Thule
Aruba    Chicago       Godthab      La_Paz       Montreal       Regina         Thunder_Bay
Asuncion Chihuahua     Goose_Bay    Lima         Montserrat     Resolute      Tijuana
Atikokan Coral_Harbour Grand_Turk   Los_Angeles  Nassau         Rio_Branco    Toronto
Atka     Cordoba       Grenada     Louisville   New_York       Rosario       Tortola
Bahia    Costa_Rica    Guadeloupe  Lower_Princes Nipigon        Santa_Isabel  Vancouver
Bahia_Banderas Creston       Guatemala   Maceio       Nome           Santarem     Virgin
Barbados Curacao      Guyana      Managua      Manaua        North_Dakota  Santo_Domingo Whitehorse
Belém    Danmarkshavn Halifax      Marigot      Manaribo     Ojinaga       Sao_Paulo     Yakutat
Belize  Dawson       Havana      Martinique   Matamoros    Panama        Scoresbysund  Yellowknife
Boa_Vista Dawson_Creek Hermosillo   Mazatlan     Matamoros    Pangnirtung   Shiprock
Bogota  Denver       Indiana     Mazatlan     Mendoza      Paramaribo    Sitka
Boise   Detroit      Indianapolis Mazatlan     Mendoza      Phoenix       St_Barthelemy
Buenos_Aires Dominica     Inuvik      Menominee    Port-au-Prince St_Johns
Cambridge_Bay Edmonton    Iqaluit     Merida       Porto_Acre    St_Kitts
```

Change the timezone and verify. I have chosen the Central Time Zone for my location.

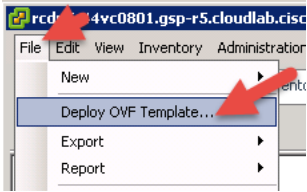
- Copy the localtime to new file named old.timezone: `'cp /etc/localtime /root/old.timezone'`
- Remove the localtime file: `'rm -f /etc/localtime'`
- Create the new localtime file: `'ln -s /usr/share/zoneinfo/America/Chicago /etc/localtime'`
- Verify the timzone is what you set it to: `'date'`
- Verify the link: `'ls -l /etc/localtime'`

```
[root@CUCSD-P-5_4_0_0 ~]# cp /etc/localtime /root/old.timezone
[root@CUCSD-P-5_4_0_0 ~]# rm -f /etc/localtime
[root@CUCSD-P-5_4_0_0 ~]# ln -s /usr/share/zoneinfo/America/Chicago /etc/localtime
[root@CUCSD-P-5_4_0_0 ~]# date
Fri Nov  6 11:38:59 CST 2015
[root@CUCSD-P-5_4_0_0 ~]# ls -l /etc/localtime
lrwxrwxrwx. 1 root root 35 Nov  6 11:38 /etc/localtime -> /usr/share/zoneinfo/America/Chicago
[root@CUCSD-P-5_4_0_0 ~]#
```

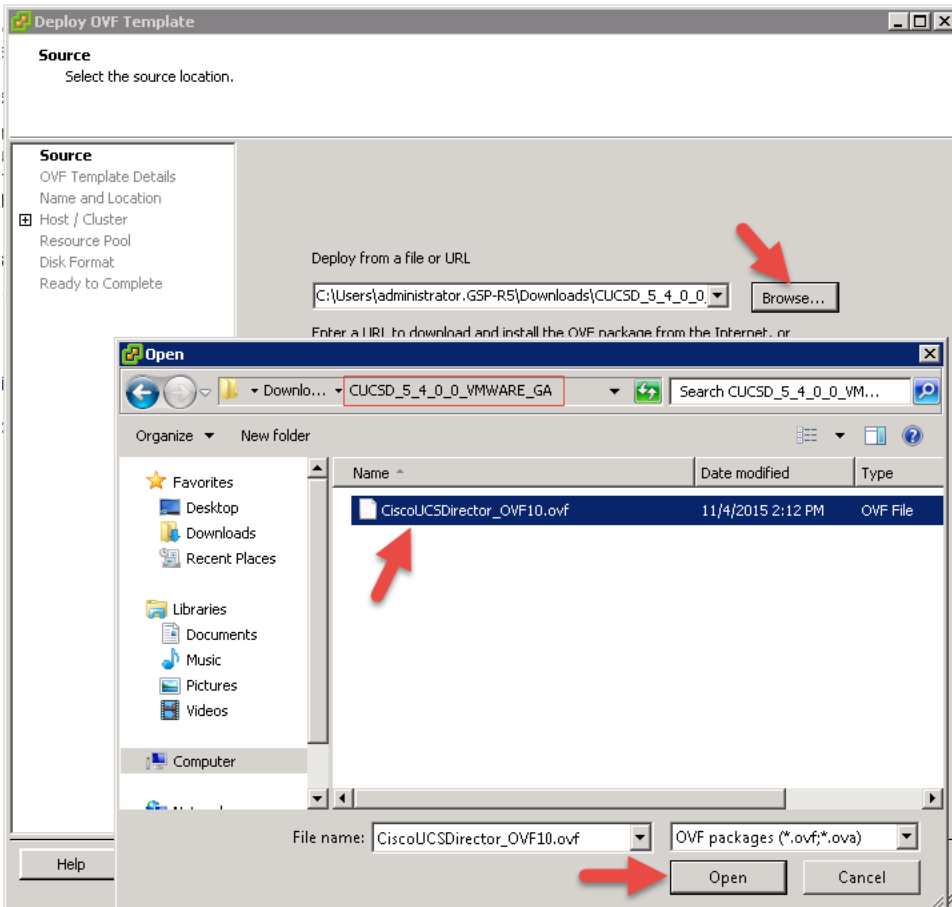
5. Create the Service Node

5.1. Create Service Node VM

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



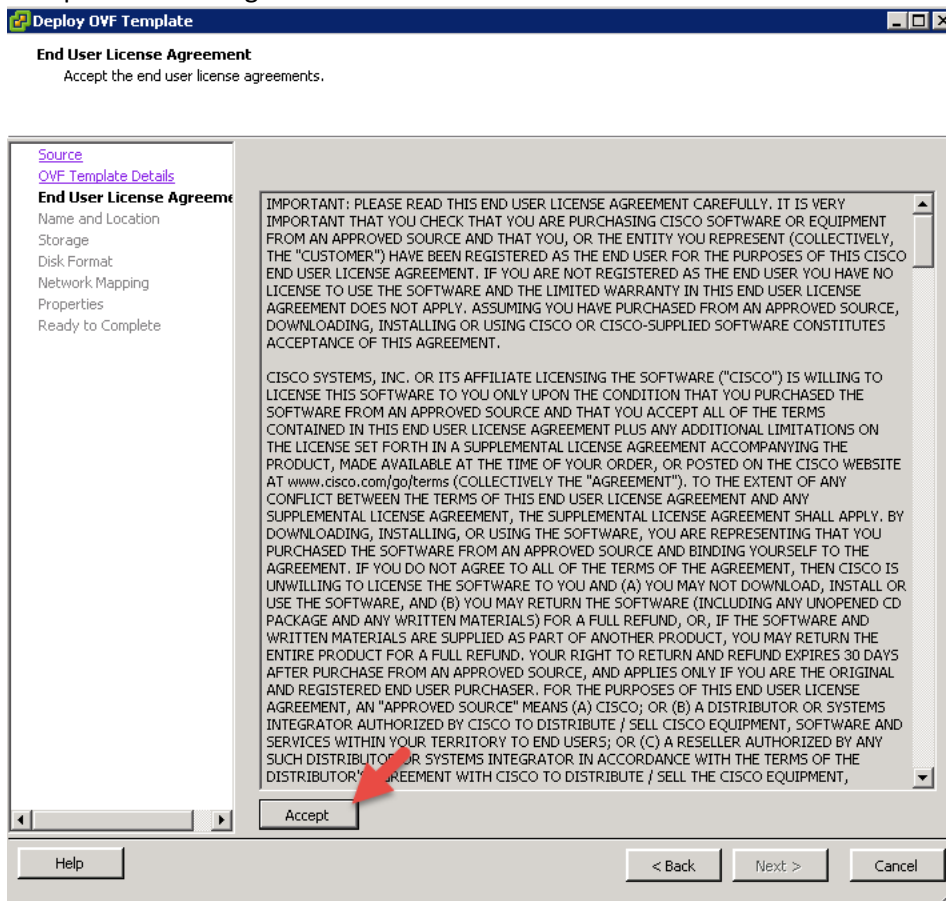
Browse to the "CiscoUCSDirector_OVF10.ovf", select it for deployment then click 'Next'.



Verify details and click 'Next'.



Accept the license agreement and click 'Next'.



Name the VM and click 'Next'.

Deploy OVF Template

Name and Location
Specify a name and location for the deployed template

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
Name and Location

Host / Cluster
Resource Pool
Disk Format
Properties
Ready to Complete

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

Inventory Location:
 rcdn5r44vc0801.gsp-r5.cloudlab.cisco.com
 GSP_MGMT
 Discovered virtual machine

Select Cluster/Host to deploy this VM on and click 'Next'.

Deploy OVF Template

Host / Cluster
On which host or cluster do you want to run the deployed template?

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)

Host / Cluster
Specific Host
Resource Pool

GSP_MGMT
 culpeper1
 culpeper2
 Richardson

Deploy OVF Template

Specify a Specific Host
On which host within the cluster should the deployed template run?

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)

Host / Cluster
Specific Host
Disk Format
Properties
Ready to Complete

Choose a specific host within the cluster.
On clusters that are configured with vSphere HA or Manual mode vSphere DRS, each virtual machine must be assigned to a specific host, even when powered off.

Select a host from the list below:

Host Name
172.17.80.68
172.17.80.67
172.17.80.61
172.17.80.65
172.17.80.62
172.17.80.66

Select a storage location to install the VM and click 'Next'.

Deploy OVF Template

Storage
Where do you want to store the virtual machine files?

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)

Host / Cluster
Storage
Disk Format
Network Mapping

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	VMFSS	Supporte
MGMT-SAN1	Non-SSD	3.90 TB	3.95 TB	1.99 TB	VMFSS	Supporte

Leave the default settings for the Disk Format and click 'Next'.

Deploy OVF Template

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

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)

Host / Cluster
Disk Format
Network Mapping
Properties
Ready to Complete

Datastore:

Available space (GB):

Thick Provision Lazy Zeroed
 Thick Provision Eager Zeroed
 Thin Provision

Select the Network to put this VM on and click 'Next'.

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

Navigation links: [Source](#), [OVF Template Details](#), [End User License Agreement](#), [Name and Location](#), [Host / Cluster](#), [Storage](#)

Enter a password for Root and Shelladmin Accounts, Management IP Address, Subnet Mask, Gateway and click 'Next'.

Deploy OVF Template

Properties
Customize the software solution for this deployment.

Navigation links: [Source](#), [OVF Template Details](#), [End User License Agreement](#), [Name and Location](#), [Host / Cluster](#), [Storage](#), [Disk Format](#), [Network Mapping](#), **Properties** (Ready to Complete)

Application

Root Password
Root Password
Enter password: [*****]
Confirm password: [*****]

Shelladmin Password
Shelladmin Password
Enter password: [*****]
Confirm password: [*****]

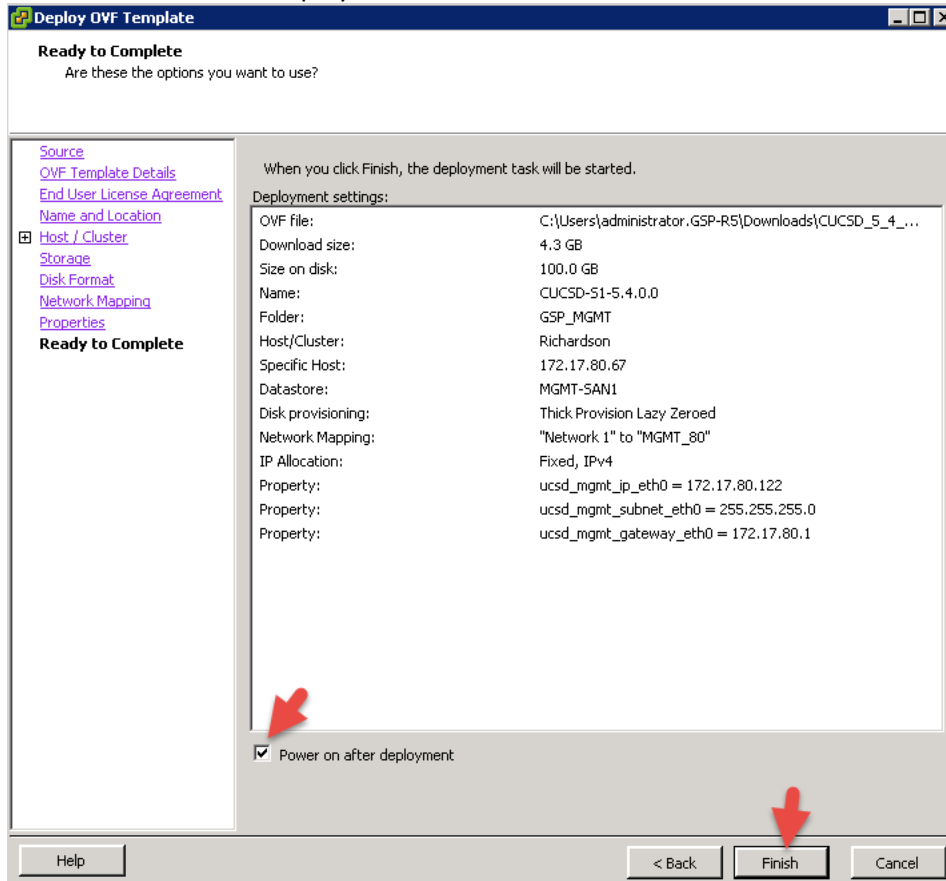
Management IP Address
Enter Management IP Address for eth0. Set 0.0.0.0 to use DHCP
[172 . 17 . 80 . 122]

Management IP Subnet Mask
Enter Management IP Subnet Mask for eth0. Set 0.0.0.0 to use DHCP
[255 . 255 . 255 . 0]

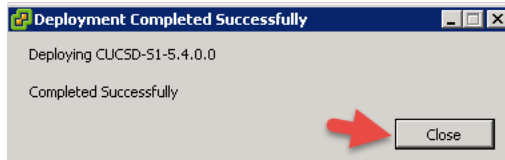
Gateway IP Address
Gateway IP Address
[172 . 17 . 80 . 1]

Buttons: Help, < Back, Next >, Cancel

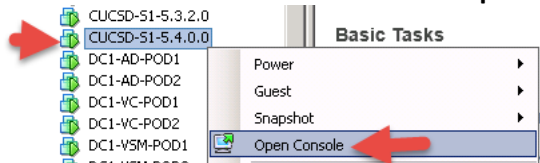
Select Power on after deployment and click **'Finish'**.



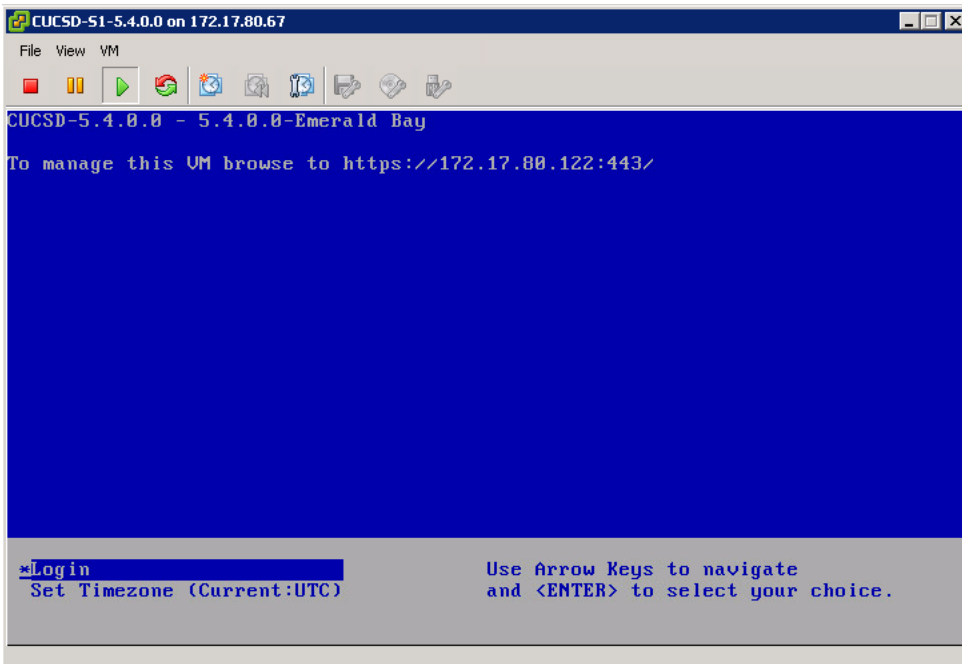
After deployment click **'Close'**.



Select the Service Node VM and select **'Open Console'**.

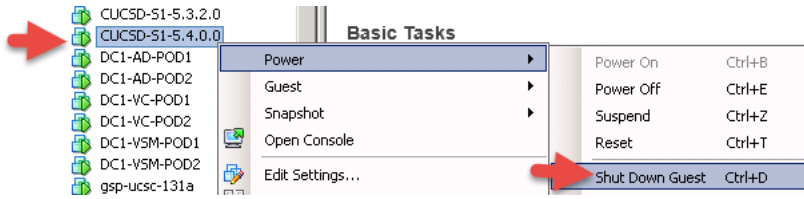


Monitor the console until the installation is complete and you will see a screen similar to the one below. The installation will take several minutes to complete so be patient.

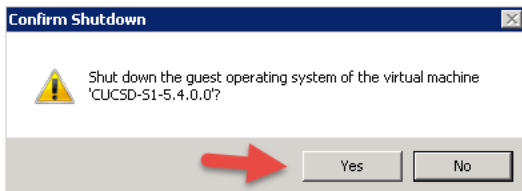


5.2. Install/Update VMWare tools & VM Version

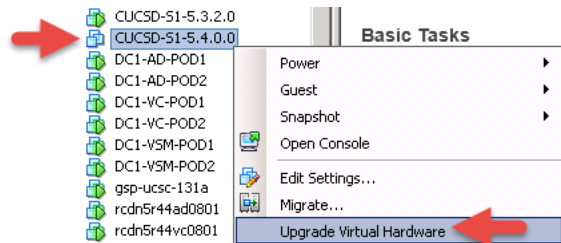
Navigate to the Service Node VM and select 'Shut Down Guest'.



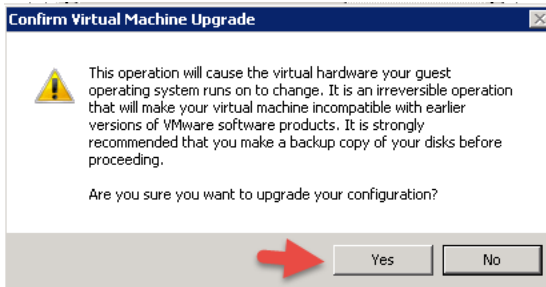
Select 'Yes'.



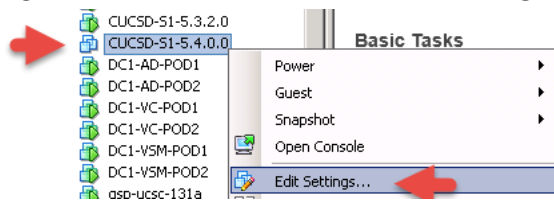
Wait for the VM to completely shut down then right click on the VM and select 'Upgrade Virtual Hardware'.



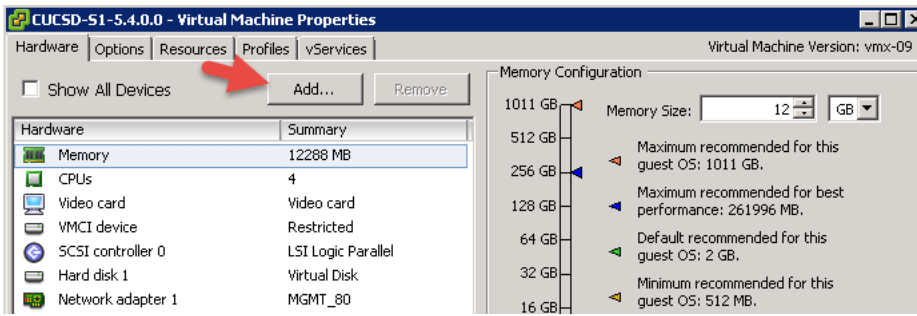
Select 'Yes'.



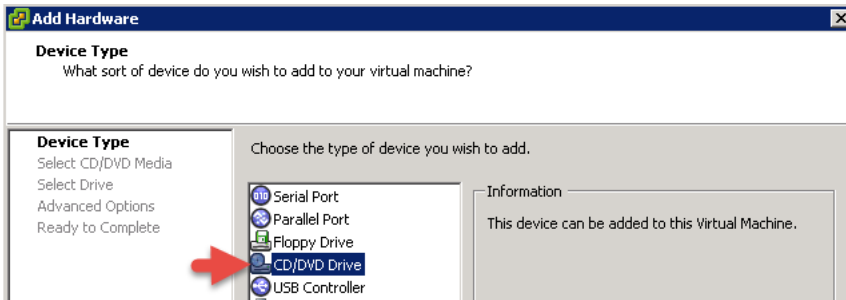
Right click on the VM and Select 'Edit Settings'.



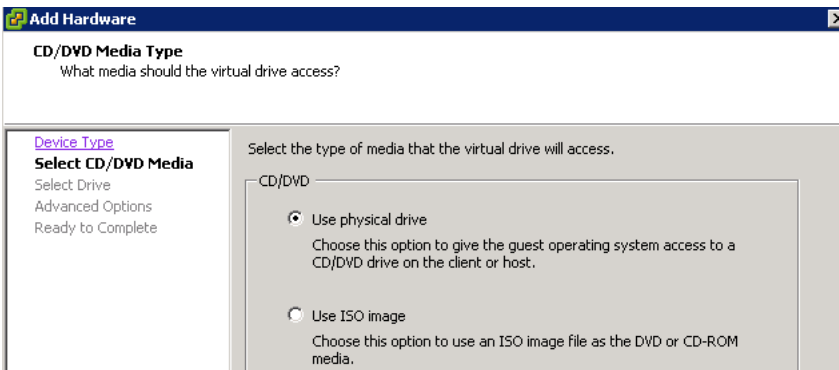
Click 'Add'.



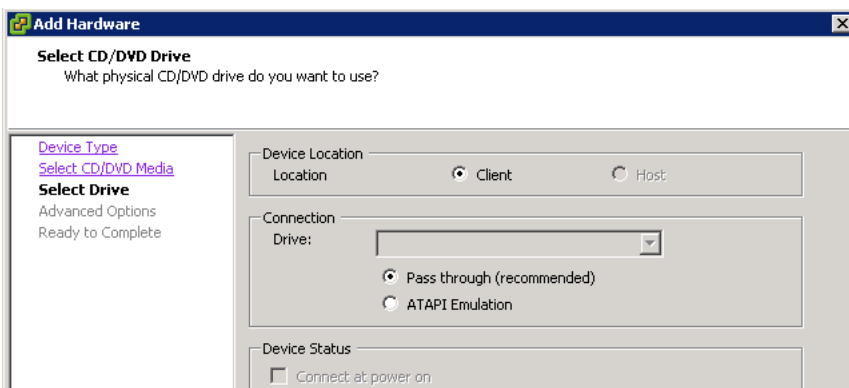
Select 'CD/DVD Drive' and click 'Next'.



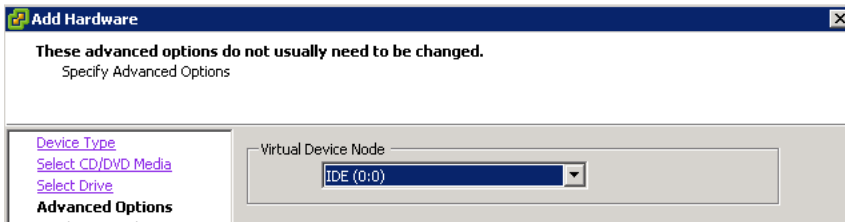
Leave default 'Use physical drive' and click 'Next'.



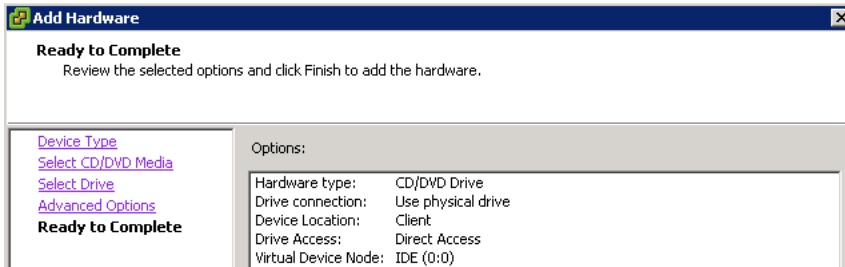
Leave default and click 'Next'.



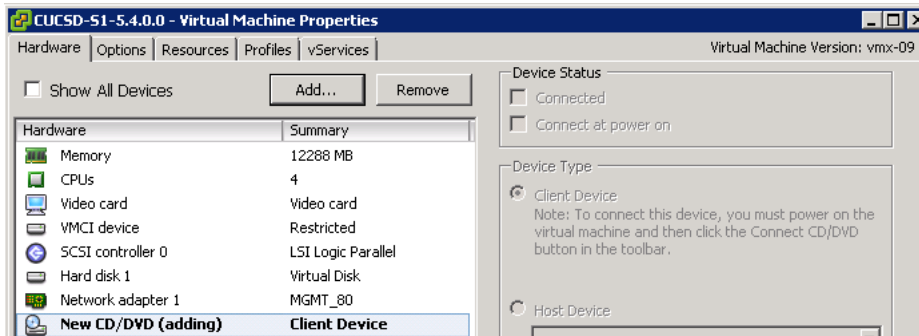
Leave default and click 'Next'.



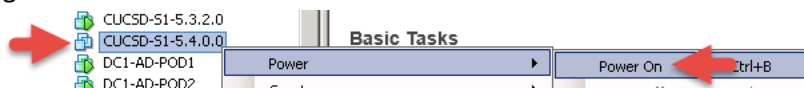
Review and click 'Finish'.



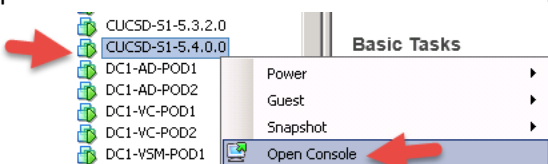
Review and click 'OK'.



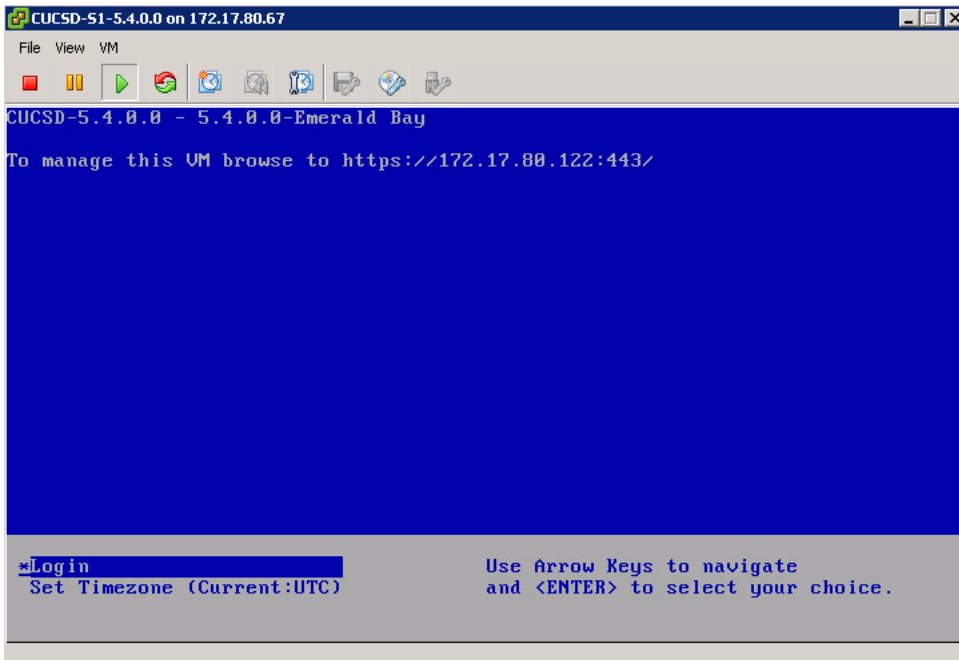
Right click on the VM and select 'Power On'.



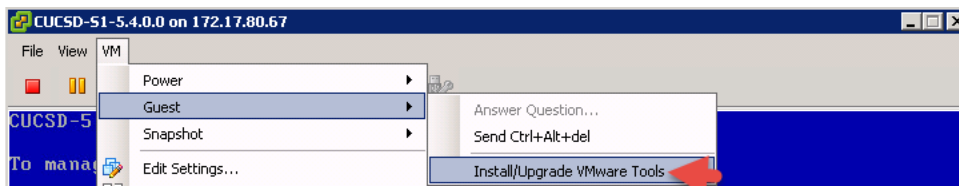
Open the VM Console to watch the VM Boot. Right click on the VM and select 'Open Console'.



Once the VM is completely up, you should see the login screen similar to below.



From the console, select 'Install/Upgrade VMware Tools'.



Select 'Interactive Tools Upgrade' and click 'OK'.



SSH to the Service Node and login using the root account.

- Make a dir for cdrom: `'mkdir /mnt/cdrom'`
- Mount the cdrom: `'mount /dev/cdrom /mnt/cdrom'`
- Copy vmware install to /tmp: `'cp /mnt/cdrom/VMwareTools-5.0.0-<xxxx>.tar.gz /tmp/'` **Note:** tab out the VMware tools part so you don't have to figure out the correct name.
- Unzip the files in /tmp: `'tar xzf /tmp/VMwareTools-5.0.0-<xxxx>.tar.gz'` **Note:** tab out the VMware tools part so you don't have to figure out the correct name.
- Change directory: `'cd vmware-tools-distrib'`
- Run the install: `'./vmware-install.pl'`
- Accept all the defaults by Pressing Enter for all the options.

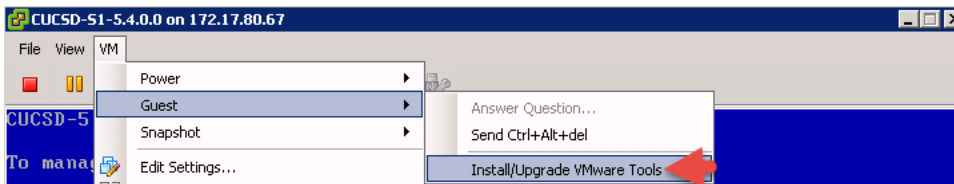
Note: You will probably get the following message.

VMware Tools cannot be installed, since they have already been installed using a package-based mechanism (rpm or deb) on this system. If you wish to continue, you must first remove the currently installed VMware Tools using the appropriate packaged-based mechanism, and then restart this installer
Execution aborted.

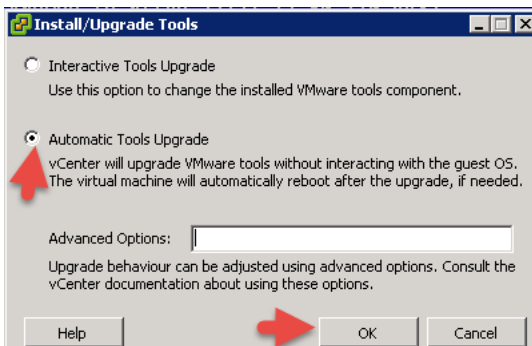
Found VMware Tools CDROM mounted at /mnt/cdrom. Ejecting device /dev/cdrom ... No eject (or equivalent) command could be located. Eject Failed: If possible manually eject the Tools installer from the guest cdrom mounted at /mnt/cdrom before canceling tools install on the host.

- If you get this message, we need to Delete the VMware tools directory: `'rm -rf /usr/lib/vmware-tools/'`
- Change directory: `'cd vmware-tools-distrib/'`
- Re-Run the install: `'./vmware-install.pl'`
- Enter **'Yes'** to the 'Would you like to remove the install DB?' You will probably get a Failure and Execution aborted.
- Re-Run the install: `'./vmware-install.pl'`
- Accept all the defaults by Pressing Enter for all the options.

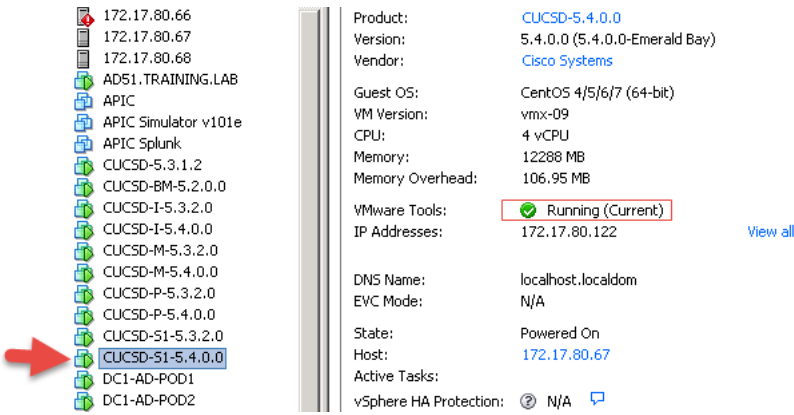
From the console, select **'Install/Upgrade VMware Tools'**.



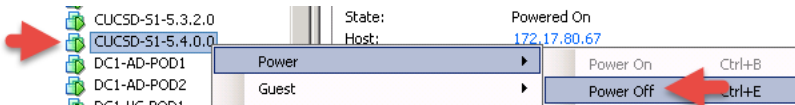
Select **'Automatic Tools Upgrade'** and click **'OK'**.



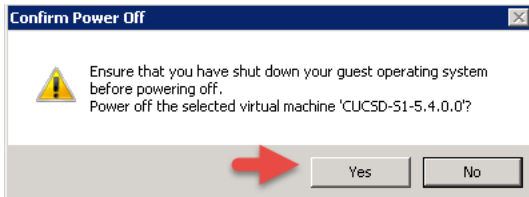
Verify Tools have been installed and **'Running (Current)'** as shown below.



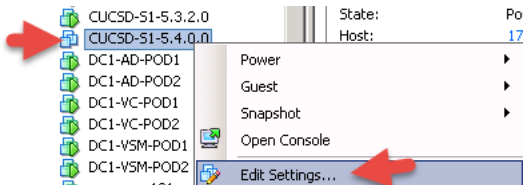
Power off the VM, **'Power Off'**.



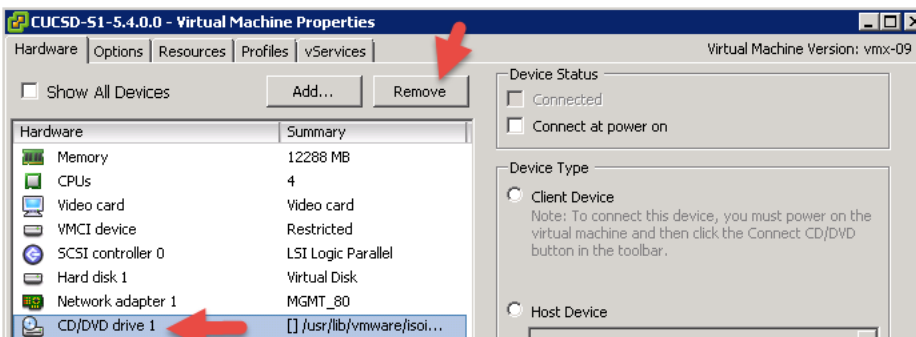
Select **'Yes'**.



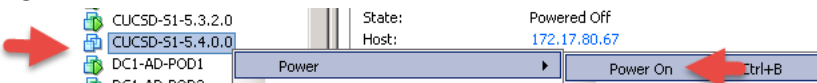
Right click on the VM and select **'Edit Settings'**.



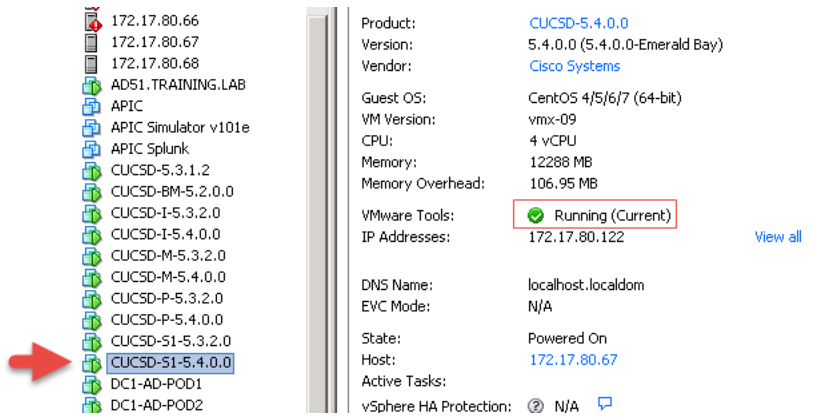
Select **'CD/DVD drive 1'**, click **'Remove'** and then click **'OK'**.



Right click on the VM and Select **'Power On'**.



Wait for the VM to completely boot up and then verify Tools have been installed and 'Running (Current)'.



The screenshot displays the VMware vSphere interface. On the left, a list of VMs is shown, with 'CUCSD-51-5.4.0.0' selected and highlighted in blue. A red arrow points to this entry. On the right, the details for the selected VM are displayed:

Product:	CUCSD-5.4.0.0
Version:	5.4.0.0 (5.4.0.0-Emerald Bay)
Vendor:	Cisco Systems
Guest OS:	CentOS 4/5/6/7 (64-bit)
VM Version:	vmx-09
CPU:	4 vCPU
Memory:	12288 MB
Memory Overhead:	106.95 MB
VMware Tools:	Running (Current)
IP Addresses:	172.17.80.122 View all
DNS Name:	localhost.localdom
EVC Mode:	N/A
State:	Powered On
Host:	172.17.80.67
Active Tasks:	
vSphere HA Protection:	Ⓜ N/A

5.3. Configure Service Node

SSH to the Service Node using the shelladmin account.

Configure NTP Server. From the Menu select 9 'Time Sync'. Replace the NTP IP Address with your NTP Server.

```
SELECT> 9
Time Sync.....
System time is Fri Nov 6 02:19:24 UTC 2015
Hardware time is Fri 06 Nov 2015 02:19:25 AM UTC -0.656583 seconds
Do you want to sync systemtime [y/n]? y
System time reset to hardware clock
Do you want to sync to NTP [y/n]? y
Enter NTP server to sync time with: 173.37.102.254
ntpd (pid 1868) is running...
shutting down ntpd: [ OK ]
6 Nov 02:19:42 ntpdate[3631]: adjust time server 173.37.102.254 offset 0.001981 sec
synchronized time with NTP server '173.37.102.254'
Added NTP server '173.37.102.254' to /etc/ntp.conf
Starting ntpd: [ OK ]
synchronised to NTP server (173.37.102.254) at stratum 6
time correct to within 7940 ms
polling server every 64 s
Press return to continue ...
```

From the menu, choose (24) 'Configure Multi Node Setup (Advanced Deployment)' and press Enter.

- Enter '1' to configure the current node.
- Enter 'y' when asked if you want to configure multi node setup.
- Enter 'b' to Configure the node as Service Node.
- Enter 'y' when asked if you asked if you want to configure this node as Service Node.
- Enter 'a' when asked to select the IP version you want to configure.
- Enter 'Inventory DB IP' when asked to Provide the Inventory DB IP.
- Enter 'Monitoring DB IP' when asked to Provide the Monitoring DB IP.
- When prompted to logout, enter 'y' and press enter. Log back in as shelladmin by entering 'su shelladmin'

```
SELECT> 24
*****
This wizard helps to do Multi Node setup
*****
Configuration Options :
Current Node --> Select '1'
Remote Node --> Select '2'
exit --> Select '3'

Please enter an option: 1
*****
Cisco UCS Director Multi Node Setup requires multiple instances of UCS Director OVF deployed with different configurations. Following are the required configurations:

* UCS Director Primary Node (1 Instance) . This node also acts as a front end UI node
* UCS Director Service Node (1 or more instances) . Service node can be reconfigured as Primary Node when necessary.
* UCS Director Inventory DB Node (1 Instance)
* UCS Director Monitoring DB Node (1 Instance)

Refer to UCS Director documentation for additional details on Multi Node Setup.
*****

This is a standalone Node

Do you want to configure multi node setup [y/n]? y

Select a option from the menu below

a) Configure as Primary Node
b) Configure as Service Node
c) Configure as Inventory DB
d) Configure as Monitoring DB
x) Exit

Enter: [a/b/c/d/x]? b
Do you want to configure this node as service Node [y/n]? y
Configuring Service Node
Stopping UCS Director Services
Select the IP version you want to configure [a] IPv4, b) IPv6] a/b : a
Provide Inventory DB IP:172.17.80.120
Provide Monitoring DB IP:172.17.80.121
Starting UCS Director services
Checking MySQL database status.... UP
Started service broker [PID=3910]
Started service controller [PID=3936]
Started service eventmgr [PID=3969]
Started service client [PID=4001]
Started service idaccessmgr [PID=4036]
Started service inframgr [PID=4080]
Started service tomcat [PID=4106]
Started service websock [PID=4161]
Configured Service Node Successfully
In order for changes to take effect logout and login back
Do you want to logout [y/n]? y
```


Verify the services for the Service Node are up and running, choose (2) '**Display Service Status**' and press Enter. You should see the lines in the red box below. **Note:** After you return to the shelladmin, the menu options change to those available for a Service node.

```

Cisco UCS Director Shell Menu

service Node

Select a number from the menu below

1) Change ShellAdmin Password
2) Display Services Status
3) Stop Services
4) Start Services
5) Time Sync
6) Ping Hostname/IP Address
7) Show Version
8) Generate Self-Signed Certificate and Certificate Signing Request
9) Import CA/Self-Signed Certificate
10) Configure Network Interface
11) Display Network Details
12) Add Cisco UCS Director Baremetal Agent Hostname/IP
13) Tail Inframgr Logs
14) Apply Patch
15) Shutdown Appliance
16) Reboot Appliance
17) Manage Root Access
18) Login as Root
19) Configure Multi Node Setup (Advanced Deployment)
20) Clean-up Patch Files
21) Collect logs from a Node
22) Quit

```

```

SELECT> 2

```

Service	Status	PID
broker	RUNNING	3910
controller	RUNNING	3936
eventmgr	RUNNING	3969
client	RUNNING	4001
idaccessmgr	RUNNING	4036
inframgr	RUNNING	4080
tomcat	RUNNING	4106
websock	RUNNING	4161

```

Node Type : service
Inventory DB( 172.17.80.120:3306 ) status      : UP
Monitor DB( 172.17.80.121:3306 ) status : UP
Press return to continue ...

```

Edit the /etc/hosts file to update the name and IP address of the host. SSH to the Service Node using the root account.

- Edit the hosts file: '**vi /etc/hosts**'
- Go to the end of the line: '**shift + a**'
- Create a new line: press return
- enter your host details: example shown below
- when done: press '**esc**'
- enter '**:wq!**'
- Verify the hosts file has been saved: '**cat /etc/hosts**'

```

[root@localhost ~]# cat /etc/hosts
127.0.0.1 localhost.localdomain localhost localhost
172.17.80.120 CUCSD-I-5_4_0_0
172.17.80.121 CUCSD-M-5_4_0_0
172.17.80.122 CUCSD-S-5_4_0_0
172.17.80.119 CUCSD-P-5_4_0_0
::1 localhost.localdomain localhost localhost ip6-localhost ip6-loopback
[root@localhost ~]#

```

Edit the /etc/resolv.conf to update the DNS servers.

- Edit the resolv.conf file: **'vi /etc/resolv.conf'**
- press **'i'** for insert
- enter **'search localhost your domain name'**, **Note:** Sometime search localhost is already there
- enter dns server ip address after nameserver, **Note:** if you have multiple DNS servers, enter on separate lines
- when done: press **'esc'**
- enter **':wq!'**
- Example:

```
search localhost gsp-r5.cloudlab.cisco.com
nameserver 172.17.80.104
nameserver 8.8.8.8
nameserver 8.8.4.4
```

- Verify the changes: **'cat /etc/resolv.conf'**

```
[root@localhost ~]# cat /etc/resolv.conf
; generated by /sbin/dhclient-script
search localhost gsp-r5.cloudlab.cisco.com
nameserver 172.17.80.104
nameserver 8.8.8.8
nameserver 8.8.4.4
[root@localhost ~]# █
```

Edit the hostname in /etc/sysconfig/network

- Edit the network config: **'vi /etc/sysconfig/network'**
- Move cursor to the beginning of localhost where it is on the l and enter **'cw'** (change word)
- Enter the Host name for the Monitoring Database Node
- Enter your domain name
- when done: press **'esc'**
- enter **':wq!'**
- Verify changes were saved: **'cat /etc/sysconfig/network'**

```
[root@localhost ~]# cat /etc/sysconfig/network
NETWORKING=yes
NETWORKING_IPV6=yes
HOSTNAME=CUCSD-S-5_4_0_0
DOMAINNAME=gsp-r5.cloudlab.cisco.com
[root@localhost ~]# █
```

Change the hostname.

```
[root@localhost ~]# hostname CUCSD-S-5_4_0_0
[root@localhost ~]# hostname
CUCSD-S-5_4_0_0
[root@localhost ~]# █
```

Log out and log back into the Service Node and you will see the new hostname.

```
[root@CUCSD-S-5_4_0_0 ~]# █
```

Verify NTP servers for Service Node are configured and synced. SSH into Primary Node using root account.

- Create ntp user: **'useradd ntp'** **Note:** If the ntp user already exist, the system will let you know.
- Restart the ntpd services: **'service ntpd restart'**
- Verify configured NPT servers: **'ntpq -p'**
- The **'*'** next to the NTP server IP address indicates the Service Node is synced to the NTP server.

```
[root@CUCSD-S-5_4_0_0 ~]# useradd ntp
useradd: user 'ntp' already exists
[root@CUCSD-S-5_4_0_0 ~]# service ntpd restart
shutting down ntpd: [ OK ]
starting ntpd: [ OK ]
[root@CUCSD-S-5_4_0_0 ~]# ntpq -p
-----
remote           refid           st t when poll reach  delay  offset jitter
-----
*173.39.1.2.254 LOCAL(1)
                    5 u   6  64   1   1.158  2.722  0.000
[root@CUCSD-S-5_4_0_0 ~]#
```

Optional: If you need to configure multiple NTP servers you can do so by editing the ntp.conf file.

- Edit the ntp.conf file: `'vi /etc/ntp.conf'`
- cursor down to the `'server'` line
- press `'shit + a'` for insert and go to the end of the line
- press return to create a new line
- enter `'server your ip address'` of your NTP server IP address
- press `'esc'`, then enter `':wq!'` to quit and write the info
- Verify the config changes: `'cat /etc/ntp.conf'`

```
[root@CUCSD-S-5_4_0_0 ~]# cat /etc/ntp.conf
# For more information about this file, see the man pages
# ntp.conf(5), ntp_acc(5), ntp_auth(5), ntp_clock(5), ntp_misc(5), ntp_mon(5).

driftfile /var/lib/ntp/drift

# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery

# Permit all access over the loopback interface. This could
# be tightened as well, but to do so would effect some of
# the administrative functions.
restrict 127.0.0.1
restrict -6 ::1

# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

#broadcast 192.168.1.255 autokey          # broadcast server
#broadcastclient                          # broadcast client
#broadcast 224.0.1.1 autokey             # multicast server
#multicastclient 224.0.1.1               # multicast client
#manycastserver 239.255.254.254          # manycast server
#manycastclient 239.255.254.254 autokey  # manycast client

# Enable public key cryptography.
#crypto

includefile /etc/ntp/crypto/pw

# Key file containing the keys and key identifiers used when operating
# with symmetric key cryptography.
keys /etc/ntp/keys

# Specify the key identifiers which are trusted.
#trustedkey 4 8 42

# Specify the key identifier to use with the ntpdc utility.
#requestkey 8

# Specify the key identifier to use with the ntpq utility.
#controlkey 8

# Enable writing of statistics records.
#statistics clockstats cryptostats loopstats peerstats

server 173.100.254
[root@CUCSD-S-5_4_0_0 ~]#
```

If you edited the ntp.conf file, you must restart the ntpd service and check the NTP synchronization. It may take a while but when the clock is synced with the NTP server there will be a `'*'` to the left of the IP address.

- Restart the ntpd services: `'service ntpd restart'`
- View the configured ntp servers and check for synchronization: `'ntpq -p'`

```
[root@CUCSD-S-5_4_0_0 ~]# service ntpd restart
Shutting down ntpd: [ OK ]
Starting ntpd: [ OK ]
[root@CUCSD-S-5_4_0_0 ~]# ntpq -p
      remote           refid      st t when poll reach  delay  offset  jitter
-----
*173.100.254 LOCAL(1)      5 u   2   64    1   1.376   3.853   0.000
[root@CUCSD-S-5_4_0_0 ~]#
```

Change the time zone to the local timezone where the Primary Node, Inventory Database Service Nodes and the Monitoring Database reside. This will ensure the logs will match everywhere.

- Determine the current timezone: `'ls -l /etc/localtime'`
- Determine your timezone if your in America: `'ls /usr/share/zoneinfo/America/'`
- This deployment is in Dallas so I will choose `'Chicago'` for Central Standard Time.

```
[root@CUCSD-S-5_4_0_0 ~]# ls -l /etc/localtime
lrwxrwxrwx. 1 root root 27 Nov  4 19:23 /etc/localtime -> /usr/share/zoneinfo/Etc/UTC
[root@CUCSD-S-5_4_0_0 ~]# ls /usr/share/zoneinfo/America/
Adak          Campo_Grande  Eirunepe      Jamaica       Metlakatla    Port_of_Spain  St_Lucia
Anchorage     Cancun         El_Salvador   Jujuy         Mexico_City   Porto_Velho    St_Thomas
Anguilla      Caracas       Ensenada      Juneau        Miquelon     Puerto_Rico    St_Vincent
Antigua       Catamarca     Fortaleza     Kentucky      Moncton       Rainy_River    Swift_Current
Araguaina     Cayenne       Fort_Wayne    Knox_IN       Monterrey     Rankin_Inlet   Tegucigalpa
Argentina     Cayman        Glace_Bay     Kralendijk    Montevideo    Recife         Thule
Aruba         Chicago        Godthab       La_Paz        Montreal      Regina         Thunder_Bay
Asuncion      Chihuahua     Goose_Bay     Lima          Montserrat    Resolute       Tijuana
Atikokan     Coral_Harbour Grand_Turk    Los_Angeles   Nassau        Rio_Branco     Toronto
Atka          Cordoba       Grenada       Louisville    New_York       Rosario        Tortola
Bahia         Costa_Rica    Guadeloupe   Lower_Princes Nipigon       Santa_Isabel   Vancouver
Bahia_Banderas Creston        Guatemala     Maceio        Nome           Santarem       Virgin
Barbados      Cuiaba        Guayaquil     Managua       Noronha        Santiago       Whitehorse
Belem         Curacao       Guyana        Manaua        North_Dakota   Santo_Domingo  Winnipeg
Belize        Danmarkshavn  Halifax       Marigot       Ojinaga        Sao_Paulo      Yakutat
Blanc-Sablon Dawson        Havana        Martinique    Panama          Scoresbyund    Yellowknife
Boa_Vista     Dawson_Creek Hermosillo    Matamoros     Pangnirtung    Shiprock
Bogota        Denver        Indiana       Mazatlan      Paramaribo     Sitka
Boise         Detroit       Indianapolis   Mendoza        Phoenix        St_Barthelemy
Buenos_Aires Dominica      Inuvik        Menominee     Port-au-Prince St_Johns
Cambridge_Bay Edmonton     Iqaluit       Merida        Porto_Acre     St_Kitts
```

Change the timezone and verify. I have chosen the Central Time Zone for my location.

- Copy the localtime to new file named old.timezone: `'cp /etc/localtime /root/old.timezone'`
- Remove the localtime file: `'rm -f /etc/localtime'`
- Create the new localtime file: `'ln -s /usr/share/zoneinfo/America/Chicago /etc/localtime'`
- Verify the timzone is what you set it to: `'date'`
- Verify the link: `'ls -l /etc/localtime'`

```
[root@CUCSD-S-5_4_0_0 ~]# cp /etc/localtime /root/old.timezone
[root@CUCSD-S-5_4_0_0 ~]# rm -f /etc/localtime
[root@CUCSD-S-5_4_0_0 ~]# ln -s /usr/share/zoneinfo/America/Chicago /etc/localtime
[root@CUCSD-S-5_4_0_0 ~]# date
Fri Nov  6 15:36:28 CST 2015
[root@CUCSD-S-5_4_0_0 ~]# ls -l /etc/localtime
lrwxrwxrwx. 1 root root 35 Nov  6 15:36 /etc/localtime -> /usr/share/zoneinfo/America/Chicago
[root@CUCSD-S-5_4_0_0 ~]#
```

Verify the Service Node is completely up before moving on to the next section. Do not move on until you see the **“Ready to send announcement”** in the **‘logfile.txt’**. From the Service Node CLI do the following:

- Use the vi editor to access the logfile.txt: **‘vi /opt/infra/inframgr/logfile.txt’**
- Go to the end/bottom of the log file: enter **‘shift + g’**
- Look for **‘Ready to send announcement’** starting from the bottom: enter **‘?Ready to send announcement’**

```
2015-10-18 23:32:35,184 [pool-1-thread-24] INFO userAPIAgentConnectivityCheck(RemoteScheduleTaskAPI.java:480) - inside rem
onnectivity check
~
?Ready to send announcement
```

- Press enter/return

```
2015-10-13 15:09:08,682 [AS-Inframgr:A130BA99DB] INFO run(AnnouncementSender.java:35) - Ready to send announcements
```

- Type **‘:q!’** to exit vi editor

Optional: Determine how long it took for the Service Node to come up. From the Service Node CLI do the following:

- Use the vi editor to access the logfile.txt: **‘vi /opt/infra/inframgr/logfile.txt’**
- Go to the end/bottom of the log file: enter **‘shift + g’**
- Look for **‘Choosing MySQL DB’** starting from the bottom: enter **‘?Choosing MySQL DB’**

```
2015-10-18 23:47:33,101 [pool-1-thread-27] INFO userAPIAgentConnectivityCheck(RemoteScheduleTaskAPI.java:480) - inside rem
onnectivity check
~
?Choosing MySQL DB
```

- Press enter/return

```
2015-10-13 15:03:50,467 [main] INFO init(DB.java:81) - Choosing MySQL DB
```

- Type **‘:q!’** to exit vi editor

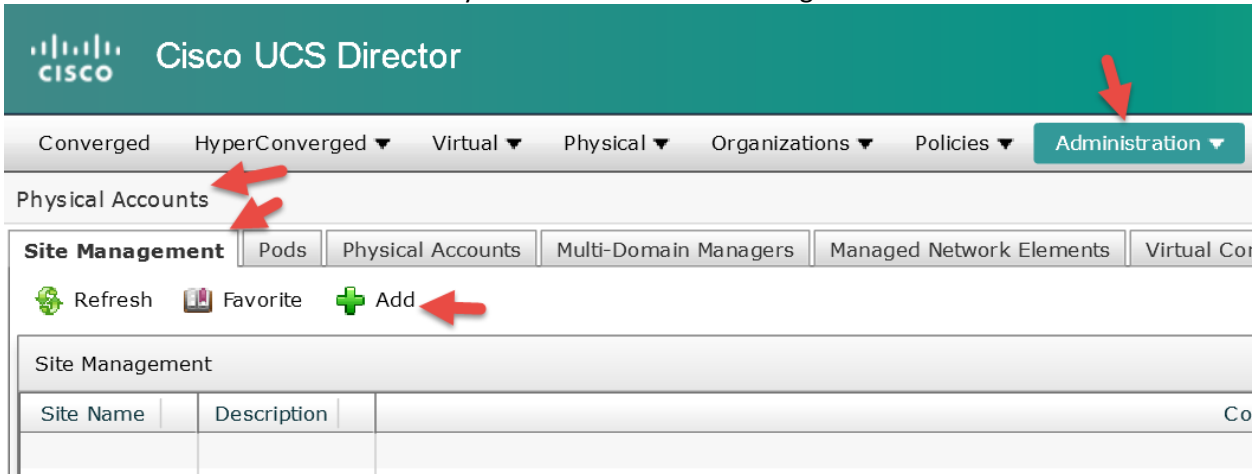
Using the time from **‘Choosing MySQL DB’** of **15:03** subtract it from the time **‘Ready to send announcement’** of **15:09** and the result is the time it took for the Node to come completely up.

6. Add Physical, Virtual Accounts and Prerequisites

6.1. Configure Prerequisites

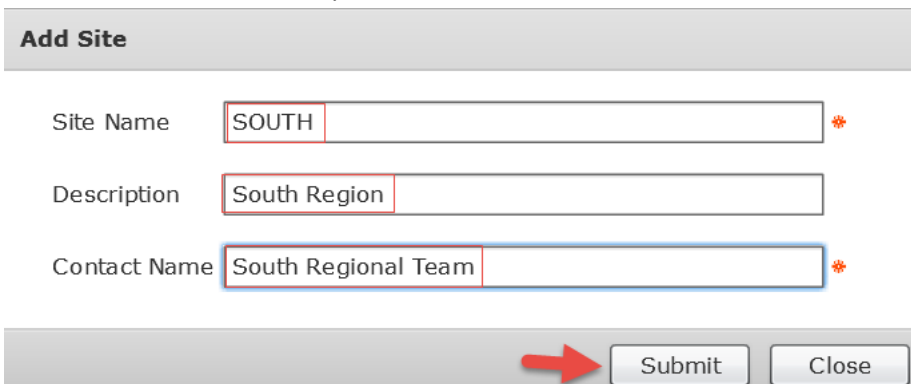
6.1.1. Add a Site

Add a Site. Go to Administration -> Physical Accounts -> Site Management -> select 'Add'.



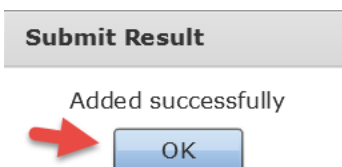
The screenshot shows the Cisco UCS Director web interface. At the top, there is a green header with the Cisco logo and the text "Cisco UCS Director". Below the header is a navigation bar with several tabs: "Converged", "HyperConverged", "Virtual", "Physical", "Organizations", "Policies", and "Administration". The "Administration" tab is selected and highlighted in green. Below the navigation bar, there is a "Physical Accounts" section. Underneath, there are several sub-sections: "Site Management", "Pods", "Physical Accounts", "Multi-Domain Managers", "Managed Network Elements", and "Virtual Cor". The "Site Management" sub-section is active. In this sub-section, there are three buttons: "Refresh", "Favorite", and "Add". The "Add" button is highlighted with a red arrow. Below the buttons, there is a table with the following columns: "Site Name", "Description", and "Co".

Enter the Site Name, Description, Contact Name and click 'Submit'.



The screenshot shows the "Add Site" form. It has three input fields: "Site Name" with the value "SOUTH", "Description" with the value "South Region", and "Contact Name" with the value "South Regional Team". Each input field has a red asterisk icon to its right, indicating a required field. Below the input fields, there are two buttons: "Submit" and "Close". A red arrow points to the "Submit" button.

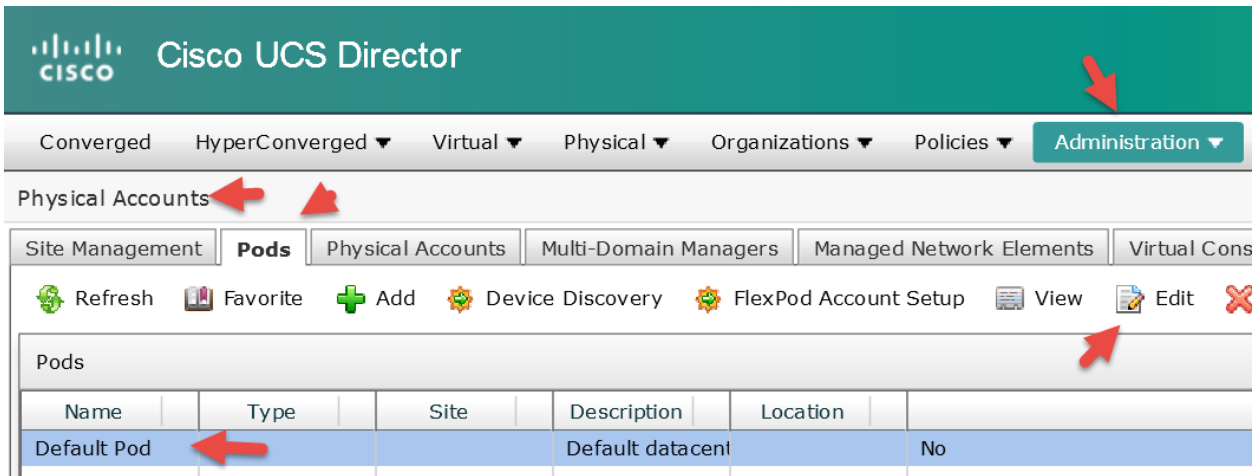
Click 'OK'.



The screenshot shows the "Submit Result" dialog box. It has a title bar that says "Submit Result". Below the title bar, there is a message that says "Added successfully". Below the message, there is a blue button with the text "OK". A red arrow points to the "OK" button.

6.1.2. Hide the Default POD

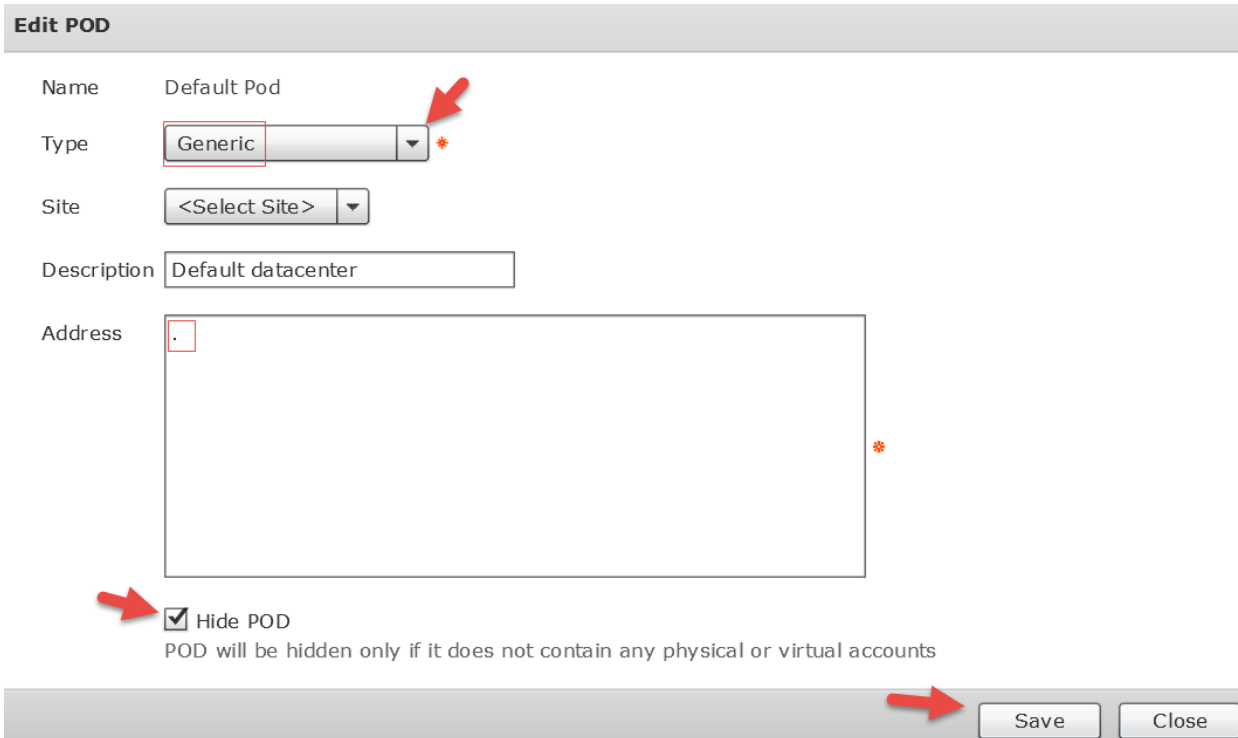
Hide the Default Pod from the Converged View. Go to Administration -> Physical Accounts -> Pods -> select Default Pod -> select 'Edit'.



The screenshot shows the Cisco UCS Director interface. At the top, the 'Administration' menu is highlighted with a red arrow. Below it, the 'Physical Accounts' section is selected, and the 'Pods' tab is active. A table of Pods is displayed with the following columns: Name, Type, Site, Description, Location, and an empty column. The 'Default Pod' is highlighted in blue, with a red arrow pointing to its 'Type' field.

Name	Type	Site	Description	Location	
Default Pod			Default datacent		No


Using the drop down, select 'Generic' for the 'Type' field, add enter a '.' or a real address in the 'Address' field, select the 'Hide POD' check box and then click 'Save'.



The 'Edit POD' form is shown with the following fields and actions:

- Name: Default Pod
- Type: A dropdown menu with 'Generic' selected and a red arrow pointing to it.
- Site: A dropdown menu with '<Select Site>' selected.
- Description: Default datacenter
- Address: A text area containing a single period '.' and a red asterisk icon to its right.
- Hide POD: A checked checkbox with a red arrow pointing to it. Below it, the text reads: 'POD will be hidden only if it does not contain any physical or virtual accounts'.
- Save and Close buttons: A red arrow points to the 'Save' button.

Click 'OK'.



The 'Submit Result' dialog box displays the message: 'POD modified successfully.' Below the message is an 'OK' button with a red arrow pointing to it.

6.1.3. Add a POD

Add a POD. Go to Administration -> Physical Accounts -> Pods -> select 'Add'.

The screenshot shows the Cisco UCS Director interface. At the top, the 'Administration' menu is highlighted with a red arrow. Below it, the 'Physical Accounts' menu is selected, and the 'Pods' sub-menu is active. The 'Add' button, represented by a green plus sign, is highlighted with a red arrow. Below the navigation, there are icons for Refresh, Favorite, Add, Device Discovery, and FlexPod Account Setup. A table titled 'Pods' is visible, with columns for Name, Type, Site, Description, Location, and an empty column. The first row shows 'Default Pod' with 'Generic' as the type, 'Default datacent' as the site, and 'No' as the location.

Enter a Name, select 'Generic' for the Type, select the site you created, enter a description, enter an address and click 'Add'.

The 'Add POD' form contains the following fields and options:

- Name:** Text input field containing 'RCDN5-LAB' with a red asterisk indicating a required field.
- Type:** Dropdown menu with 'Generic' selected and a red asterisk.
- Site:** Dropdown menu with 'SOUTH' selected.
- Description:** Text input field containing 'Richardson 5 LAB'.
- Address:** Large text area containing 'Richardson Texas' with a red asterisk.
- Hide POD**
POD will be hidden only if it does not contain any physical or virtual accounts

At the bottom right, there are 'Add' and 'Close' buttons, with a red arrow pointing to the 'Add' button.

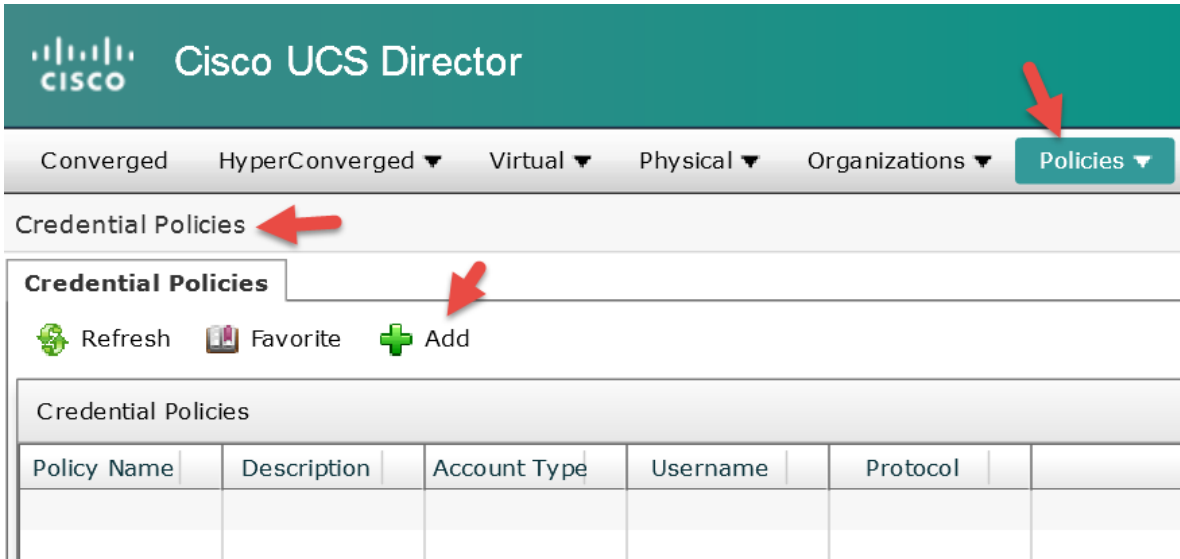
Click 'OK'.

The 'Submit Result' dialog box displays the message 'POD added successfully.' and an 'OK' button, which is highlighted with a red arrow.

6.2. Add Physical Accounts

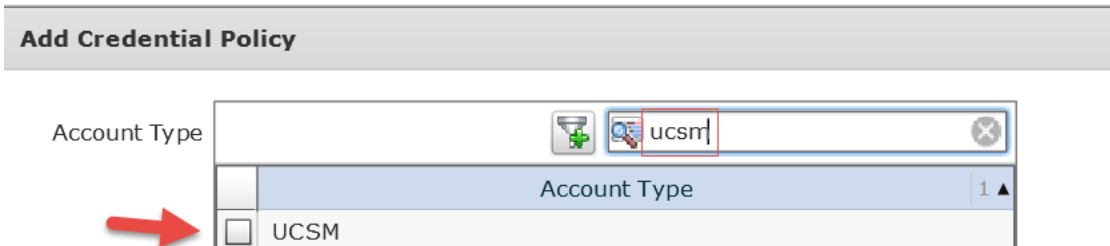
6.2.1. Optional – Create UCSM Credential Policy

Create UCSM Credentials Policy. Go to Policies -> Physical Infrastructure Policies -> Credential Policies -> select 'Add'.



The screenshot shows the Cisco UCS Director interface. At the top, there is a navigation bar with the Cisco logo and the text "Cisco UCS Director". Below this, there is a secondary navigation bar with tabs for "Converged", "HyperConverged", "Virtual", "Physical", "Organizations", and "Policies". The "Policies" tab is selected, and a red arrow points to it. Below the navigation bar, there is a section titled "Credential Policies" with a red arrow pointing to the title. Underneath, there are three buttons: "Refresh", "Favorite", and "Add". A red arrow points to the "Add" button. Below the buttons, there is a table with the following columns: "Policy Name", "Description", "Account Type", "Username", and "Protocol". The table is currently empty.

Enter UCSM in the filter on the right then select the 'UCSM' check box.



The screenshot shows the "Add Credential Policy" dialog box. At the top, there is a section titled "Add Credential Policy". Below this, there is a search bar for "Account Type" with the text "ucsm" entered. A red arrow points to the search bar. Below the search bar, there is a list of account types. The first item is "UCSM" with an unchecked checkbox next to it. A red arrow points to the checkbox. The list also shows "Account Type" with a count of "1" and an upward arrow.

Enter a Policy Name, Optional Description, Username, Password and click 'Submit'.

Add Credential Policy

Account Type	UCSM
Policy Name	<input type="text" value="UCSM Credential Policy"/>
Description	<input type="text" value="UCSM Credential Policy"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>
Protocol	<input type="text" value="https"/>
Port	<input type="text" value="443"/>
Authentication Type	<input type="text" value="Locally Authenticated"/>
Server Management	<input type="text" value="All Servers"/>

Click 'OK'.

Submit Result

Added entry successfully

6.2.2. Add UCSM Account

Add a UCSM Account. Go to Administration -> Physical Accounts -> Physical Accounts -> select 'Add'.

Cisco UCS Director

Converged HyperConverged Virtual Physical Organizations Policies Administration

Physical Accounts

Site Management Pods Physical Accounts Multi-Domain Managers Managed Network Elements Virtual Cor

Refresh Favorite Add Device Discovery

Account Nam	Account Type	Connection S	Pod	Contact	Location	Server / Filer

Drop down and select the POD, 'Computing' Category, 'UCSM' Account Type and click 'Submit'.

Add Account

Pod *

Category *

Account Type *

Enter an Account Name, Server Address, select the 'Use Credential Policy' check box, drop down and select the UCSM Credential Policy created in the previous section and click 'Add'.

Add Account

Pod *

Category *

Account Type *

Account Name *

Server Address *

Use Credential Policy

Credential Policy *

Description

Contact Email

Location

Service Provider

Click 'OK'.

Submit Result

Account added successfully.

6.2.3. Optional - Create NetApp Credential Policy

Create NetApp Credentials Policy. Go to Policies -> Physical Infrastructure Policies -> Credential Policies -> select 'Add'.

The screenshot shows the Cisco UCS Director interface. At the top, there is a navigation bar with the following items: Converged, HyperConverged, Virtual, Physical, Organizations, and Policies. A red arrow points to the 'Policies' dropdown menu. Below this, the 'Credential Policies' section is highlighted with a red arrow. Underneath, there are three buttons: Refresh, Favorite, and Add. A red arrow points to the 'Add' button. Below the buttons is a table with the following columns: Policy Name, Description, Account Type, Username, Protocol, and an empty column. The table is currently empty.

Enter 'NetApp Ontap' in the filter on the right then select the 'NetApp ONTAP' check box.

The screenshot shows the 'Add Credential Policy' dialog box. It has a search bar for 'Account Type' with a filter icon and a search icon. The search bar contains the text 'NetApp Ontap'. Below the search bar is a list of results. The first result is 'Account Type' with a count of '1' and an upward arrow. Below this is a checkbox labeled 'NetApp ONTAP'. A red arrow points to this checkbox.

Enter a Policy Name, Optional Description, Username, Password and click 'Submit'.

Modify Credential Policy

Account Type NetApp ONTAP

Policy Name NetApp Credential Policy

Description

Username *

Password *

Protocol *

Port *

Click 'OK'.

Submit Result

Added entry successfully

6.2.4. Add NetApp Account for Controller A

Add NetApp Controller-A Account. Go to Administration -> Physical Accounts -> Physical Accounts -> select 'Add'.

Cisco UCS Director

Converged HyperConverged Virtual Physical Organizations Policies Administration

Physical Accounts

Site Management Pods **Physical Accounts** Multi-Domain Managers Managed Network Elements Virtual Cor

Refresh Favorite Add Device Discovery

Account Nam	Account Type	Connection S	Pod	Contact	Location	Server / Filer

Drop down and select the POD, 'Storage' Category, 'NetApp ONTAP' Account Type and click 'Submit'.

Add Account

Pod *

Category *

Account Type *

Enter an Account Name, Server Address, select the 'Use Credential Policy' check box, drop down and select the NetApp Credential Policy created in the previous section and click 'Add'.

Add Account

Pod *

Category *

Account Type *

Account Name *

Server Address *

Use Credential Policy

Credential Policy *

Description

Contact Email

Location

Service Provider

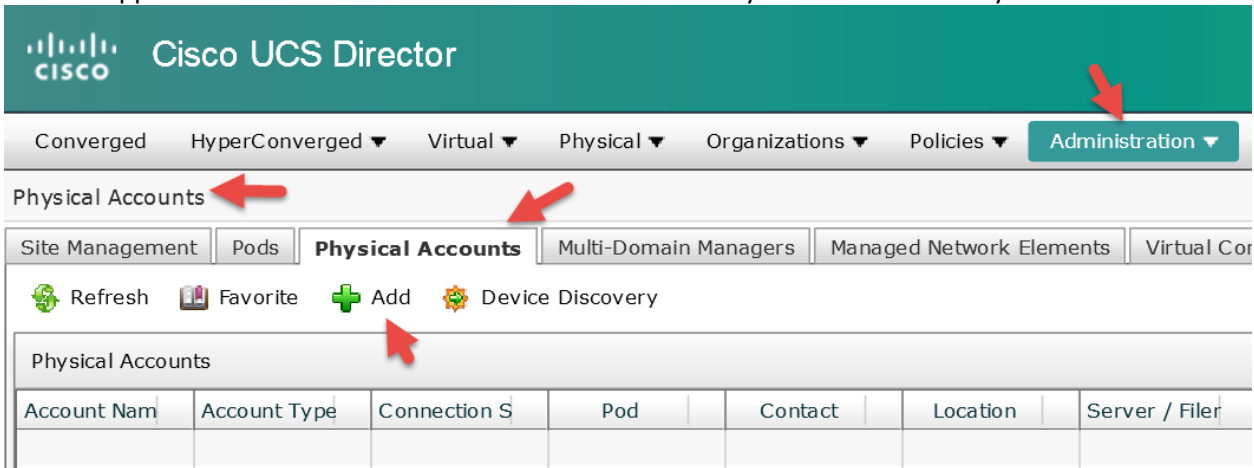
Click 'OK'.

Submit Result

Account added successfully.

6.2.5. Add NetApp Account for Controller B

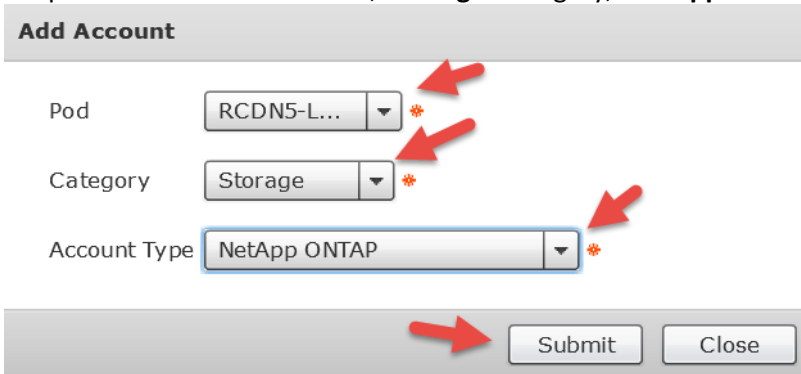
Add NetApp Controller-B Account. Go to Administration -> Physical Accounts -> Physical Accounts -> select 'Add'.



The screenshot shows the Cisco UCS Director Administration interface. The top navigation bar includes 'Administration' with a dropdown arrow. Below it, the 'Physical Accounts' section is selected, indicated by a red arrow. The 'Add' button is highlighted with a red arrow. The table below shows columns for Account Name, Account Type, Connection S, Pod, Contact, Location, and Server / File.

Account Nam	Account Type	Connection S	Pod	Contact	Location	Server / File

Drop down and select the POD, 'Storage' Category, 'NetApp ONTAP' Account Type and click 'Submit'.



The 'Add Account' form shows three dropdown menus: 'Pod' (RCDN5-L...), 'Category' (Storage), and 'Account Type' (NetApp ONTAP). Red arrows point to each dropdown and the 'Submit' button.

Pod: RCDN5-L... *

Category: Storage *

Account Type: NetApp ONTAP *

Submit Close

Enter an Account Name, Server Address, select the 'Use Credential Policy' check box, drop down and select the NetApp Credential Policy created in the previous section and click 'Add'.

Add Account

Pod *



Category *

Account Type *

Account Name *

Server Address *

Use Credential Policy

Credential Policy   *

Description

Contact Email

Location

Service Provider



Click 'OK'.

Submit Result

Account added successfully.



6.2.6. Optional - Create MDS Credential Policy

Create MDS Credentials Policy. Go to Policies -> Physical Infrastructure Policies -> Credential Policies -> select 'Add'.

The screenshot shows the Cisco UCS Director interface. At the top, there is a navigation bar with tabs for Converged, HyperConverged, Virtual, Physical, Organizations, and Policies. A red arrow points to the Policies tab. Below the navigation bar, the breadcrumb path is Credential Policies. A red arrow points to the Credential Policies link. Below the breadcrumb, there are icons for Refresh, Favorite, and Add. A red arrow points to the Add icon. Below the icons, there is a table with the following columns: Policy Name, Description, Account Type, Username, Protocol, and an empty column. The table is currently empty.

Enter 'Cisco Nexus OS' in the filter on the right then select the 'Cisco Nexus OS' check box.

The screenshot shows the 'Add Credential Policy' dialog box. The Account Type field is set to Cisco Nexus OS. A red arrow points to the search filter on the right, which contains the text 'Cisco Nexus OS'. Below the search filter, there is a table with the following columns: Account Type and a checkbox. The table contains one entry: Cisco Nexus OS with a checked checkbox. A red arrow points to the checkbox.

Enter a Policy Name, Optional Description, Username, Password and click 'Submit'.

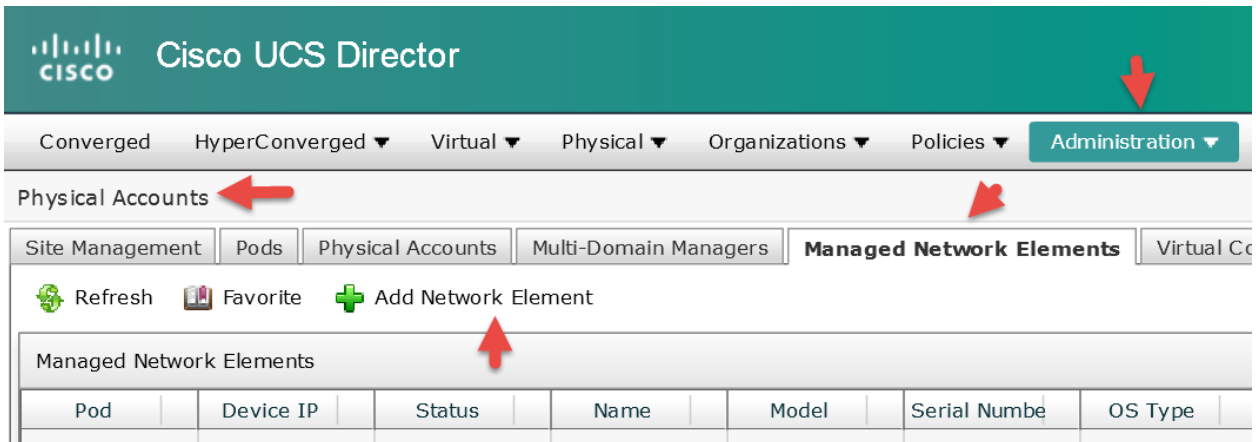
The screenshot shows the 'Add Credential Policy' dialog box. The Account Type is set to Cisco Nexus OS. The form fields are: Policy Name (MDS Credential Policy), Description (MDS Credential Policy), Username (admin), Password (*****), Protocol (ssh), and Port (22). A red arrow points to the Submit button.

Click 'OK'.

The screenshot shows the 'Submit Result' dialog box. The message is 'Added entry successfully'. A red arrow points to the OK button.

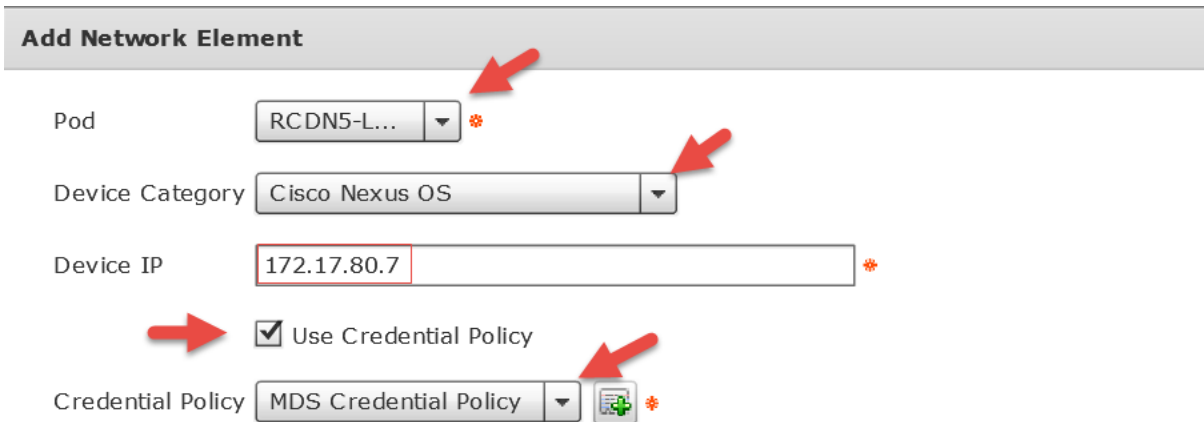
6.2.7. Add Fabric A MDS

Add Fabric A MDS Account. Go to Administration -> Physical Accounts -> Managed Network Elements -> select 'Add Network Element'.



The screenshot shows the Cisco UCS Director interface. The top navigation bar includes 'Administration' with a dropdown arrow. Below it, the 'Physical Accounts' section is active, with a sub-tab for 'Managed Network Elements'. The 'Add Network Element' button is highlighted with a red arrow. Below the button is a table with columns: Pod, Device IP, Status, Name, Model, Serial Number, and OS Type.

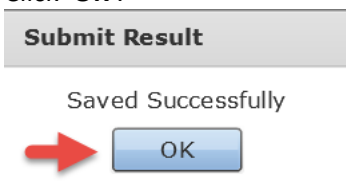
Drop down and select the POD, 'Cisco Nexus OS' Device Category, Enter the IP Address of the MDS Fabric A switch, select the 'Use Credential Policy' check box, drop down and select the MDS Credential Policy created in the previous section and click 'Submit'.



The 'Add Network Element' form contains the following fields and actions:

- Pod:** A dropdown menu with 'RCDN5-L...' selected.
- Device Category:** A dropdown menu with 'Cisco Nexus OS' selected.
- Device IP:** A text input field containing '172.17.80.7'.
- Use Credential Policy:** A checked checkbox.
- Credential Policy:** A dropdown menu with 'MDS Credential Policy' selected.

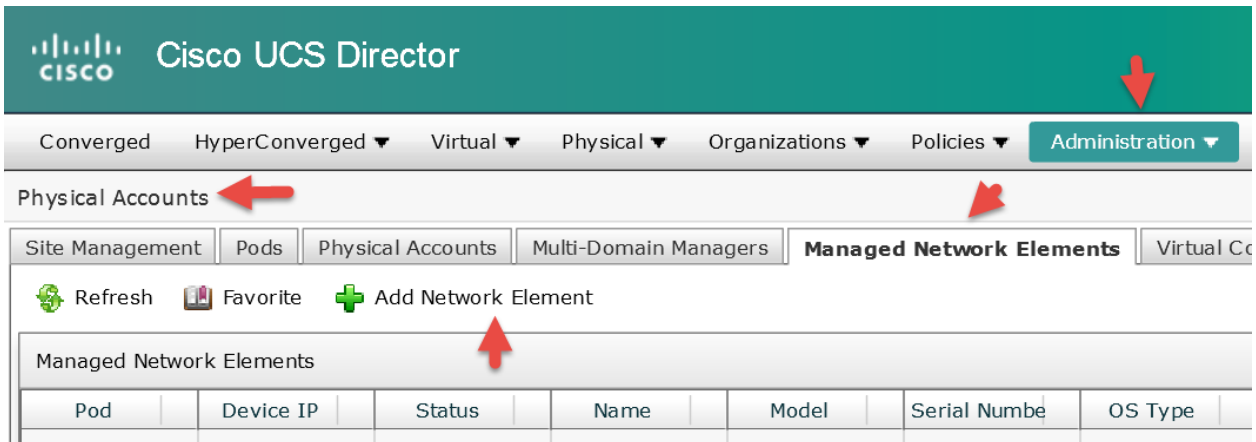
Click 'OK'.



The 'Submit Result' dialog box displays the message 'Saved Successfully' and an 'OK' button.

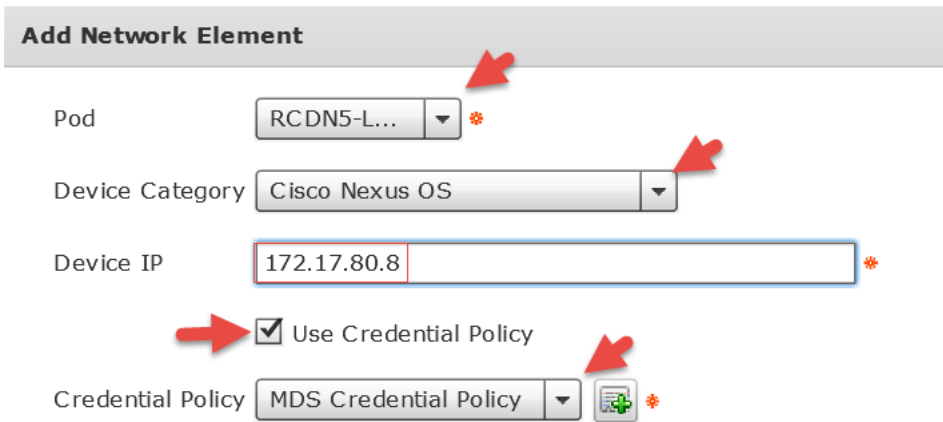
6.2.8. Add Fabric B MDS

Add Fabric B MDS Account. Go to Administration -> Physical Accounts -> Managed Network Elements -> select 'Add Network Element'.



The screenshot shows the Cisco UCS Director Administration interface. The top navigation bar includes 'Administration' with a dropdown arrow. Below it, the 'Physical Accounts' tab is selected, and the 'Managed Network Elements' sub-tab is active. The 'Add Network Element' button is highlighted with a red arrow. Below the button is a table with columns: Pod, Device IP, Status, Name, Model, Serial Number, and OS Type.

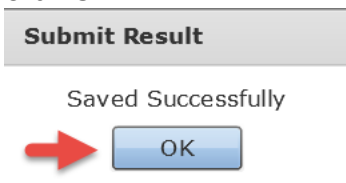
Drop down and select the POD, 'Cisco Nexus OS' Device Category, Enter the IP Address of the MDS Fabric B switch, select the 'Use Credential Policy' check box, drop down and select the MDS Credential Policy created in the previous section and click 'Submit'.



The 'Add Network Element' form is shown with the following fields and values:

- Pod: RCDN5-L... (dropdown menu)
- Device Category: Cisco Nexus OS (dropdown menu)
- Device IP: 172.17.80.8 (text input)
- Use Credential Policy: (checkbox)
- Credential Policy: MDS Credential Policy (dropdown menu)

Click 'OK'.

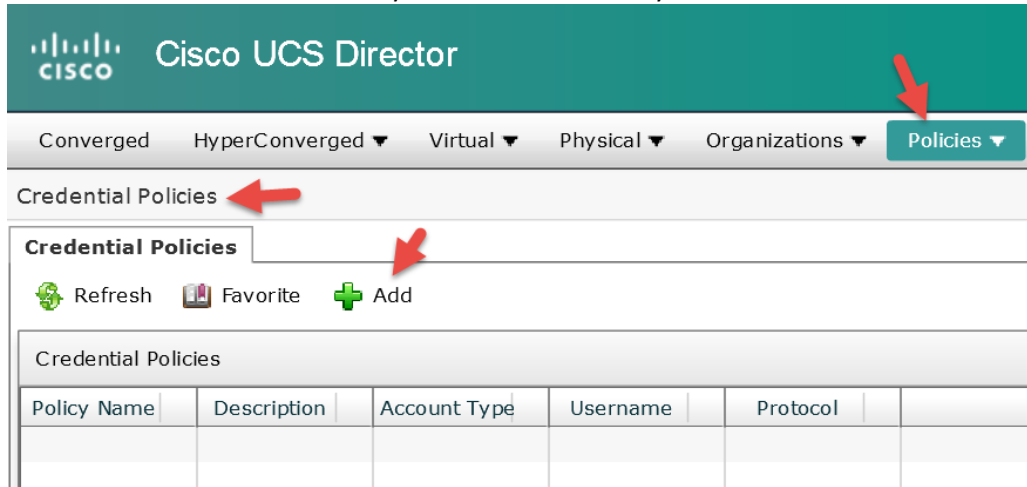


The 'Submit Result' dialog box displays the message 'Saved Successfully' and an 'OK' button.

6.3. Add a Virtual Account for vCenter

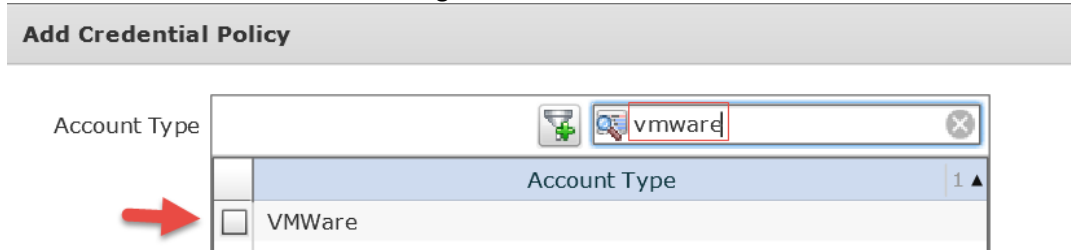
6.3.1. Optional - Create vCenter Credential Policy

Create vCenter Credentials Policy. Go to Policies -> Physical Infrastructure Policies -> Credential Policies -> select 'Add'.



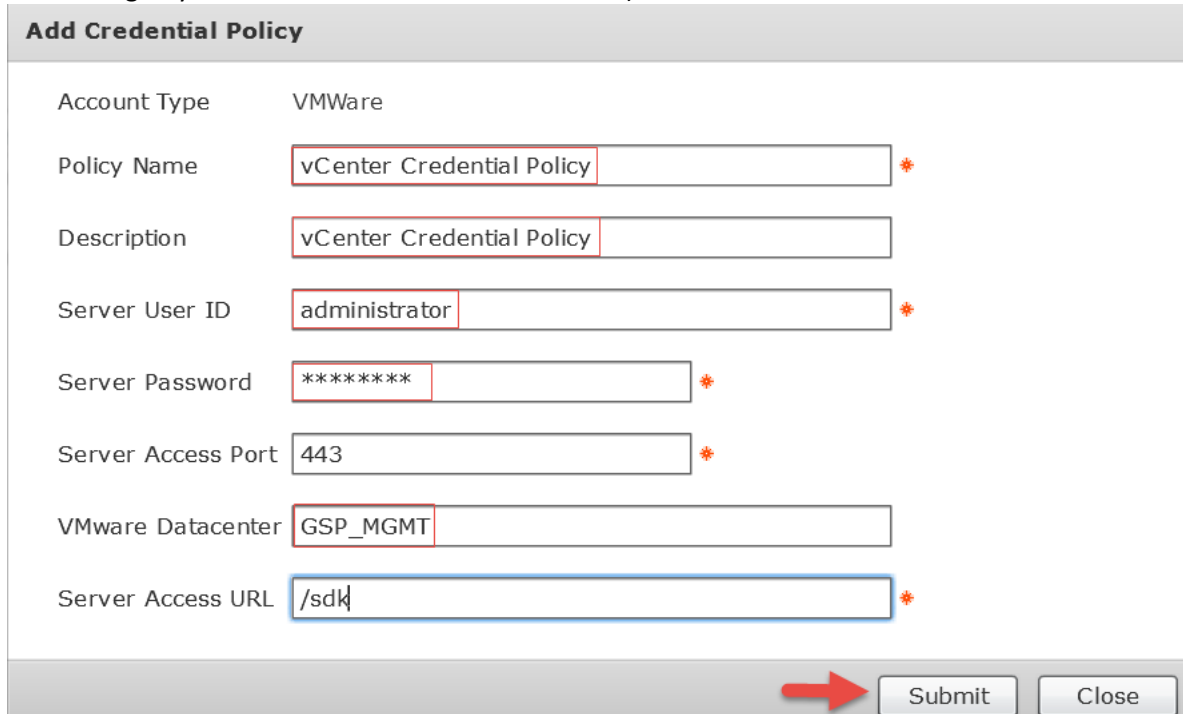
The screenshot shows the Cisco UCS Director interface. At the top, there is a navigation bar with tabs for Converged, HyperConverged, Virtual, Physical, Organizations, and Policies. A red arrow points to the Policies tab. Below the navigation bar, there is a breadcrumb trail: Credential Policies. A red arrow points to the Credential Policies link. Below the breadcrumb trail, there are three buttons: Refresh, Favorite, and Add. A red arrow points to the Add button. Below the buttons, there is a table with the following columns: Policy Name, Description, Account Type, Username, Protocol, and an empty column. The table is currently empty.

Enter 'vmware' in the filter on the right then select the 'VMWare' check box.



The screenshot shows the 'Add Credential Policy' dialog box. The Account Type field is selected, and a search filter 'vmware' is applied. The search results show a single entry: VMWare, with a checkbox next to it. A red arrow points to the checkbox.

Enter a Policy Name, Optional Description, Server User ID, Server Password, Optional VMware Datacenter (If you are connecting to your vCenter at the Data Center Level) and click 'Submit'.



The screenshot shows the 'Add Credential Policy' dialog box with the following fields filled out:

- Account Type: VMWare
- Policy Name: vCenter Credential Policy *
- Description: vCenter Credential Policy
- Server User ID: administrator *
- Server Password: ***** *
- Server Access Port: 443 *
- VMware Datacenter: GSP_MGMT
- Server Access URL: /sdk *

At the bottom right, there are two buttons: Submit and Close. A red arrow points to the Submit button.

Click 'OK'.

Submit Result

Added entry successfully



6.3.2. Add vCenter Virtual Account

Add vCenter Virtual Account. Go to Administration -> Virtual Accounts -> Virtual Accounts -> select 'Add'.

The screenshot shows the Cisco UCS Director interface. At the top, there's a green header with the Cisco logo and "Cisco UCS Director". Below it is a navigation bar with tabs: "Converged", "HyperConverged", "Virtual", "Physical", "Organizations", "Policies", and "Administration". The "Administration" tab is selected. Under "Administration", there's a "Virtual Accounts" link. Below that, there's a "Virtual Accounts" section with tabs for "Virtual Accounts", "Plugins", and "PowerShell Agents". The "Virtual Accounts" tab is active. There are icons for "Refresh", "Favorite", and "Add". The "Add" icon is highlighted with a red arrow. Below the icons is a table with columns: "Cloud Name", "Account Type", "Connection S", "Pod", "Contact", "Location", and "Server".

Cloud Name	Account Type	Connection S	Pod	Contact	Location	Server
------------	--------------	--------------	-----	---------	----------	--------

Drop down and select 'VMWare' for Cloud Type.

The screenshot shows the "Add Cloud" dialog box. It has a "Cloud Type" dropdown menu. The dropdown is open, showing a list of options: "Select Cloud Type", "AWS-EC2", "VMware", "RackSpace-Cloud", "Tier3-Cloud", and "Hyper-V". The "VMware" option is highlighted with a red box and a red arrow. There is a "Close" button on the right side of the dialog.

Cloud Type: Select Cloud Type

- Select Cloud Type
- AWS-EC2
- VMware
- RackSpace-Cloud
- Tier3-Cloud
- Hyper-V

Close

Enter a Cloud Name, Server Address, select the 'Use Credential Policy' check box, drop down and select the vCenter Credential Policy created in the previous section, drop down and select the POD to place this Virtual Account in and click 'Add'.


Add Cloud

Cloud Type *

Cloud Name *

Server Address *

Use Credential Policy

Credential Policy * 

Enable SRM

Use SSO

Description

Contact Email

Location

Pod *

Service Provider

Click 'OK'.

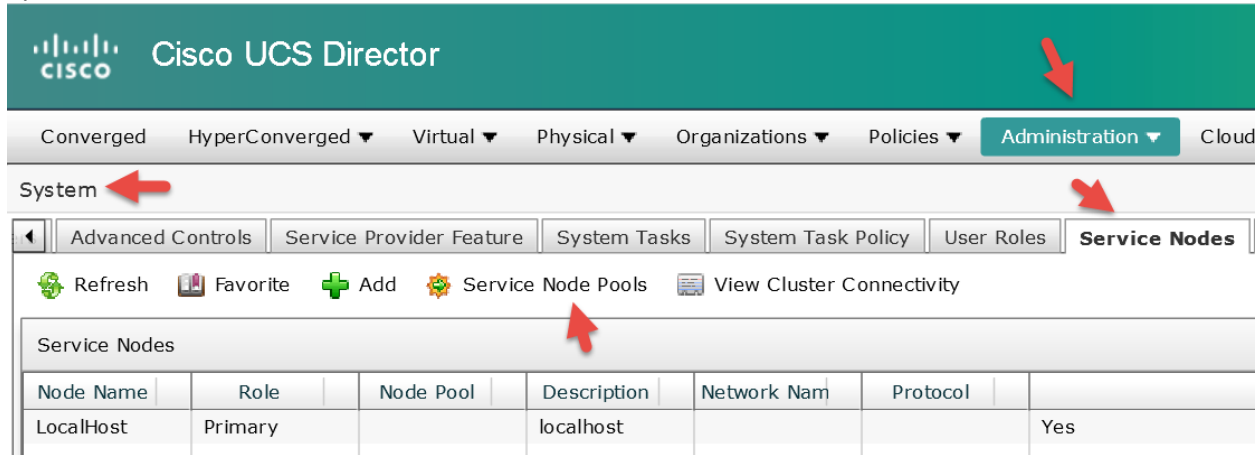
Submit Result

Cloud added successfully.

7. System Tasks

7.1. Create a Node Pool

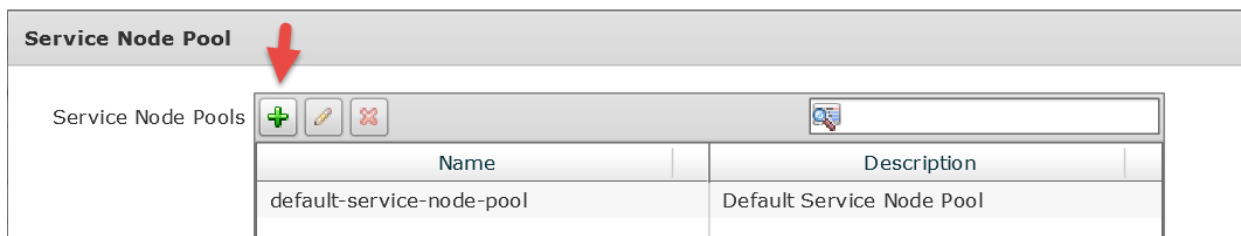
Create a Service Node Pool. Log into UCS Director GUI using the Primary Node IP address and go to Administration -> System -> Service Nodes -> select 'Service Node Pools'.



The screenshot shows the Cisco UCS Director interface. The top navigation bar includes 'Administration' and 'System'. The 'System' menu is expanded, showing 'Service Nodes' as the selected option. Below this, the 'Service Node Pools' tab is active, displaying a table with one entry: 'LocalHost' with a 'Primary' role and 'localhost' as the network name.

Node Name	Role	Node Pool	Description	Network Name	Protocol	
LocalHost	Primary		localhost			Yes

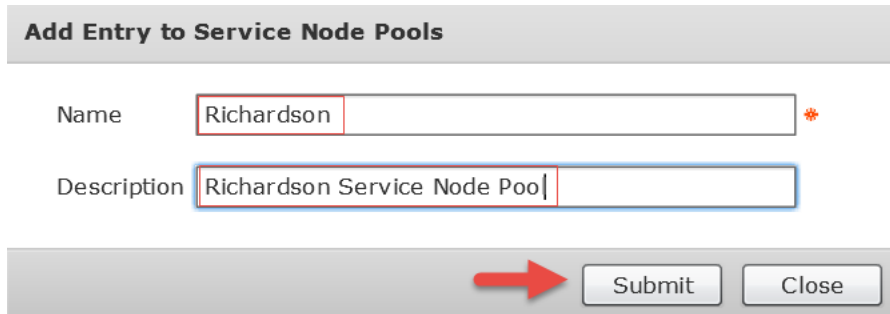
Click '+' to add a new Service Node Pool.



The 'Service Node Pool' dialog box is shown. It has a table with one entry: 'default-service-node-pool' with the description 'Default Service Node Pool'. A red arrow points to the '+' icon in the top left corner of the dialog.

Name	Description
default-service-node-pool	Default Service Node Pool

Enter a Name and Description for the Service Profile Pool and click 'Submit'.



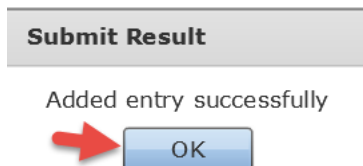
The 'Add Entry to Service Node Pools' form is shown. It has two input fields: 'Name' with the value 'Richardson' and 'Description' with the value 'Richardson Service Node Poo'. A red arrow points to the 'Submit' button.

Add Entry to Service Node Pools

Name:

Description:

Click 'OK'.



The 'Submit Result' dialog box is shown. It contains the message 'Added entry successfully' and an 'OK' button. A red arrow points to the 'OK' button.

Submit Result

Added entry successfully

Review and click 'Close'.

Service Node Pool

Service Node Pools

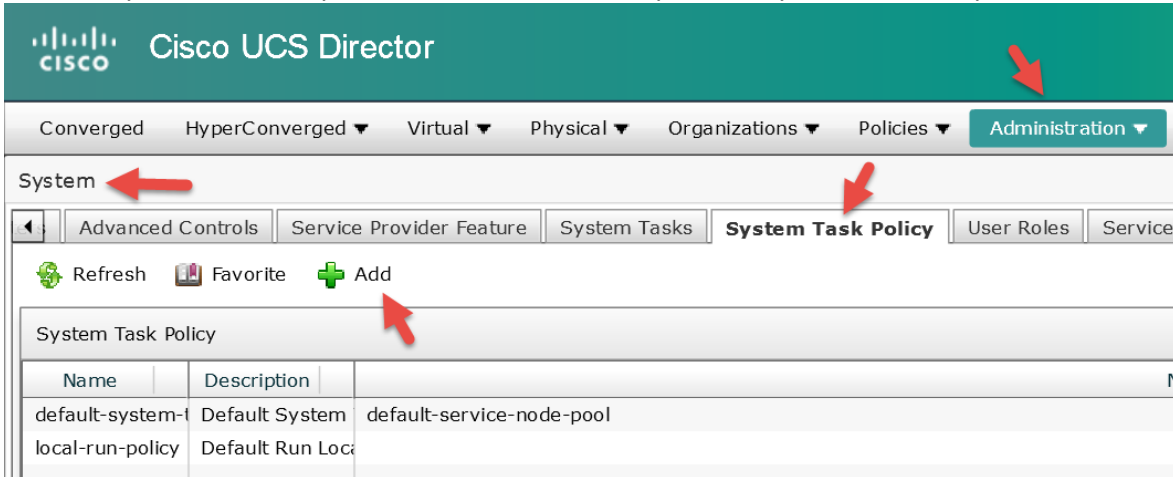
Name	Description
default-service-node-pool	Default Service Node Pool
Richardson	Richardson Service Node Pool

Total 2 items



7.2. Create System Task Policy

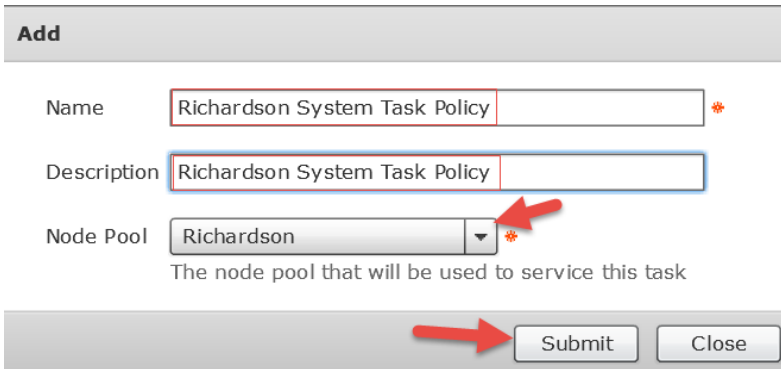
Create a System Task Policy. Go to Administration -> System -> System Task Policy -> select 'Add'.



The screenshot shows the Cisco UCS Director Administration interface. The top navigation bar includes 'Administration' with a dropdown arrow. Below it, the 'System' section is selected, and the 'System Task Policy' tab is active. A table lists existing policies:

Name	Description	
default-system-t	Default System	default-service-node-pool
local-run-policy	Default Run Loc	

Enter a System Task Policy Name and description, drop down and select the Node Pool we previously created and click 'Submit'.

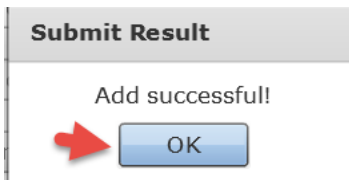


The 'Add' form contains the following fields:

- Name: Richardson System Task Policy *
- Description: Richardson System Task Policy
- Node Pool: Richardson *

The Node Pool dropdown is accompanied by the text: "The node pool that will be used to service this task". At the bottom, there are 'Submit' and 'Close' buttons.

Click 'OK'.



The 'Submit Result' dialog box displays the message "Add successful!" and an 'OK' button.

7.3. Create Service Node

Add the Service Node. Go to Administration -> System -> Service Nodes -> select 'Add'.

The screenshot shows the Cisco UCS Director Administration interface. The top navigation bar includes 'Administration', 'System', and 'Service Nodes'. A red arrow points to the 'Administration' menu. Below it, another red arrow points to the 'System' menu. A third red arrow points to the 'Add' button in the 'Service Nodes' section. A table below shows the existing 'LocalHost' service node.

Node Name	Role	Node Pool	Description	Network Name	Protocol	
LocalHost	Primary		localhost			Yes

Enter a Node Name, select the Service Node Pool you previously created, DNS Name and Protocol then click 'Submit'.

Service Node

Node Name: *

Role: Service

Service Node Pool:
 Select a Service Node Pool to associate this Service node with

DNS Name: *
 DNS Name or IP/IPv6 Address of the Service Node

Description:

Protocol:

Port: *

UserName:
 This user's API Key is used to authenticate with the Service Node

Click 'OK'.

Submit Result

Added successfully

Test Service Node Connectivity. Go to Administration -> System -> Service Nodes -> select the Service Node -> select 'Test Connectivity'.

Cisco UCS Director Administration

System

Advanced Controls | Service Provider Feature | System Tasks | System Task Policy | User Roles | **Service Nodes** | Email Templates

Refresh | Favorite | Add | Service Node Pools | View Cluster Connectivity | Edit | Delete | **Test Connectivity**

Node Name	Role	Node Pool	Description	Network Nam	Protocol	
LocalHost	Primary		localhost			Yes
CUCSD-S1-5_4	Service	Richardson		172.17.80.122	https	Not Verified

Click 'Close'.

Test Connectivity

Connection Successful

Close

Click 'Refresh' and verify the Reachability is 'Yes'.

Cisco UCS Director Administration

System

Advanced Controls | Service Provider Feature | System Tasks | System Task Policy | User Roles | **Service Nodes**

Refresh | Favorite | Add | Service Node Pools | View Cluster Connectivity

Node Name	Role	Node Pool	Description	Network Nam	Protocol	
LocalHost	Primary		localhost			Yes
CUCSD-S1-5_4	Service	Richardson		172.17.80.122	https	Yes

Verify Service Node is in sync with UCS Director. Go to Administration -> System -> select 'System Information'.

Cisco UCS Director Administration

System

System Information | Mail Setup | System Parameters | Infrastructure System Parameters | Advanced Controls | Service Provider Feature | System Tasks | System Ta

Refresh

Primary Node		Service Node(s)		DB Node(s)	
Name	CUCSD-P-5_4_0_0	Reachable	1	Inventory(172.17.80.120)	Ok
IP Address	172.17.80.119	Non Reachable	0	Monitoring(172.17.80.121)	Ok
Up Time	0 Day (s) 20 hour (s) 17 Min				
System Time	November 07,2015 13:41:11				
Total Service Nodes	1				

Verify UCS Director is fully integrated with the Service Node(s), Inventory Database Node and the Monitoring Database Node. Go to Administration -> System -> select 'System Information'.

The screenshot shows the Cisco UCS Director Administration interface. The top navigation bar includes 'Administration' and 'System' menus. The 'System Information' tab is active, displaying a table of node status information. Red arrows point to the 'Administration' menu, the 'System' menu, and the 'Refresh' button.

Primary Node		Service Node(s)		DB Node(s)	
Name	CUCSD-P-5_4_0_0	Reachable	1	Inventory(172.17.80.120)	Ok
IP Address	172.17.80.119	Non Reachable	0	Monitoring(172.17.80.121)	Ok
Up Time	0 Day (s) 20 hour (s) 17 Min				
System Time	November 07,2015 13:41:17				
Total Service Nodes	1				

7.4. Assign System Policy to UCSM System Task

Assign Richardson System Policy to UCSM System Task. Go to Administration -> System -> Service Tasks -> expand 'Cisco UCS Tasks' -> right click on 'Virtual SAN Ready Node Qualification Task – UCSM_MGMT' and select 'Manage Task'.

The screenshot shows the Cisco UCS Director Administration interface. The breadcrumb navigation is Administration > System > Service Tasks > System Tasks. The 'System Tasks' tab is active, and the 'Cisco UCS Tasks' folder is expanded. The 'Virtual SAN Ready Node Qualification Task - UCSM_MGMT' is selected, and the context menu is open, with 'Manage Task' highlighted.

Label	Description	Enabled	Freq
UCS Monthly Historical DataPurge Task	Deletes historical	Enabled	24
UCS Fault Record Purge Task	Deletes fault rec	Enabled	12
UCS Event Record Purge Task	Deletes event re	Enabled	12
Deleted UCSAccount CleanUp Task	Deletes all data	Enabled	4 h
UCS Daily Historical DataPurge Task	Deletes historical	Enabled	4 h
UCS Event Subscription Task	Subscribe the ev	Enabled	4 h
Virtual SAN Ready Node Qualification Task - UCSM_MGMT	Collects Virtual	Enabled	1 h
UCS Inventory Collector - UCSM_MGMT			
UCS Historical Data Aggregator Task			
UCS Monitoring DataCollector Task - UCSM_MGMT			
UCS Server Transition State Manager			

Drop down and select the 'Richardson System Task Policy' and click 'Submit'.

Manage Task (Virtual SAN Ready Node Qualification Task - UCSM_MGMT)

Task Execution:

System Task Policy:

Hours:

Minutes:

Click 'OK'.

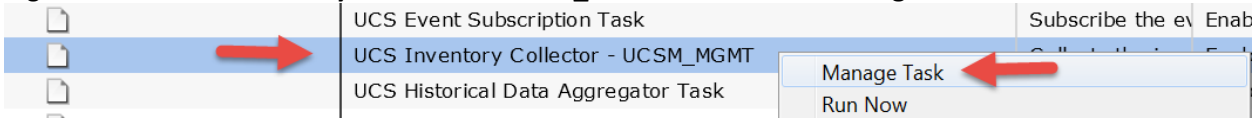
Submit Result

Task details updated successfully

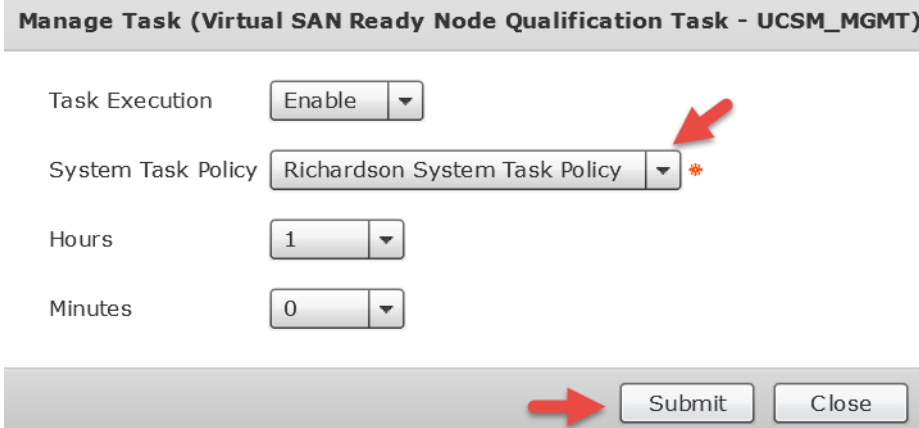
Run the 'Virtual SAN Ready Node Qualification Task – UCSM_MGMT' task.

UCS Event Subscription Task	Subscribe the ev	Enabled	4 h
Virtual SAN Ready Node Qualification Task - UCSM_MGMT	Collects Virtual	Enabled	1 h
UCS Inventory Collector - UCSM_MGMT			
UCS Historical Data Aggregator Task			

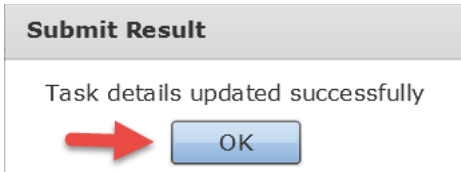
Right click on 'UCS Inventory Collector – UCSM_MGMT' and select 'Manage Task'.



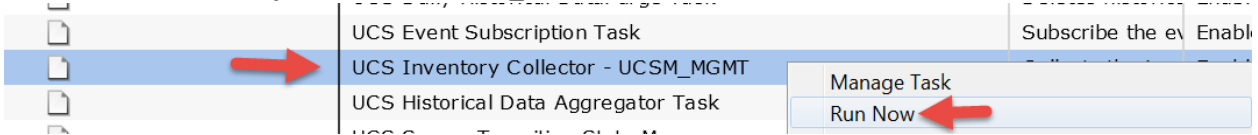
Drop down and select the 'Richardson System Task Policy' and click 'Submit'.



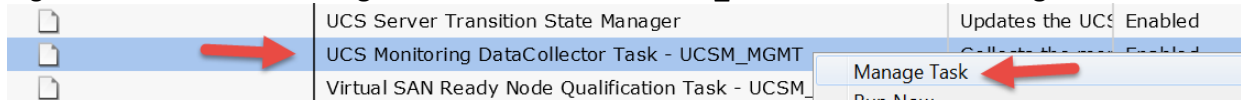
Click 'OK'.



Run the 'UCS Inventory Collector – UCSM_MGMT' task.



Right click on 'UCS Monitoring DataCollector Task – UCSM_MGMT' and select 'Manage Task'.



Drop down and select the 'Richardson System Task Policy' and click 'Submit'.

Manage Task (UCS Monitoring DataCollector Task - UCSM_MGMT)

Task Execution

System Task Policy

Hours

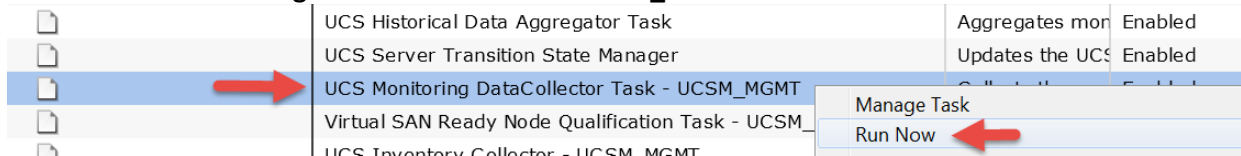
Minutes

Click 'OK'.

Submit Result

Task details updated successfully

Run the 'UCS Monitoring DataCollector Task – UCSM_MGMT' task.



Click 'Submit'

Run Now

Are you sure you want to run task 'UcsMonitoringDataCollectorTask:UCSM_MGMT' now?

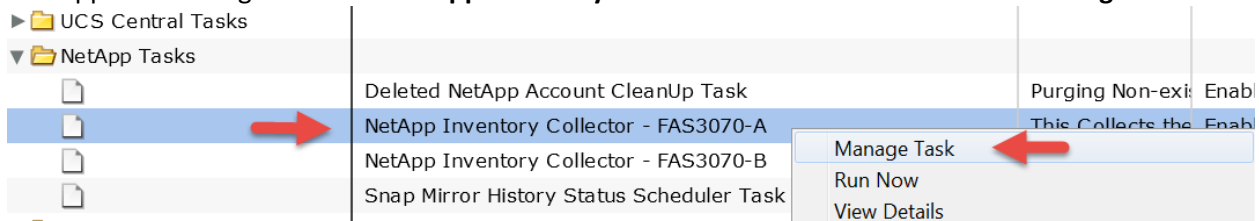
Click 'OK'.

Submit Result

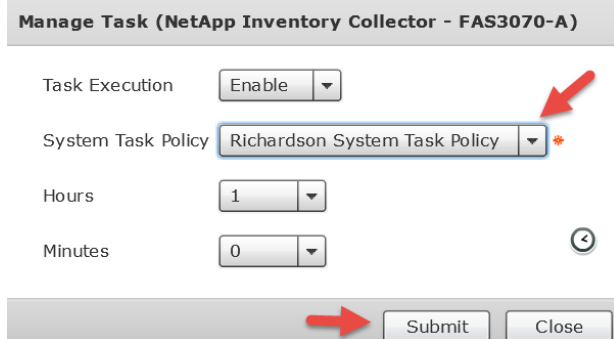
Task is scheduled to run immediately

7.5. Assign System Policy to NetApp Controller A System Task

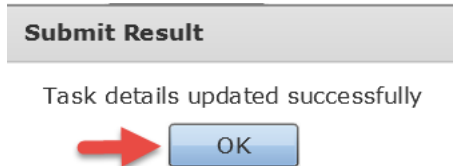
Assign Richardson System Policy to NetApp System Task. Go to Administration -> System -> Service Tasks -> expand 'NetApp Tasks' -> right click on 'NetApp Inventory Collector – FAS3070-A' and select 'Manage Task'.



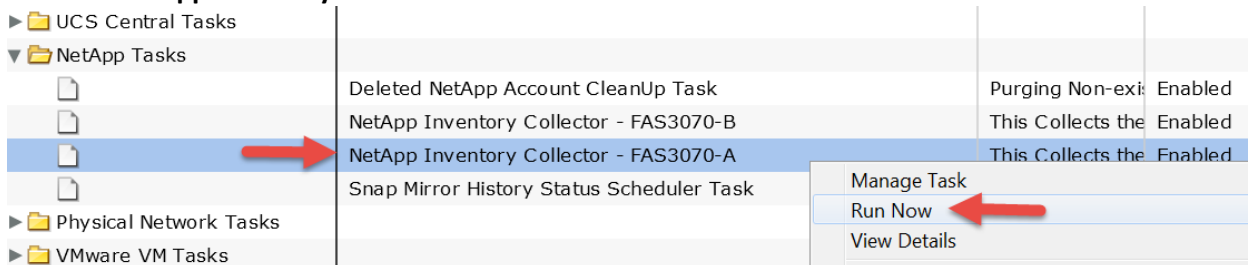
Drop down and select the 'Richardson System Task Policy' and click 'Submit'.



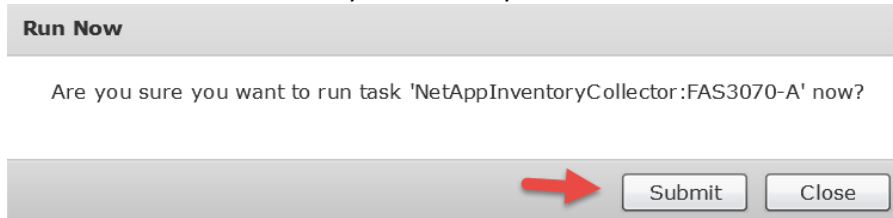
Click 'OK'.



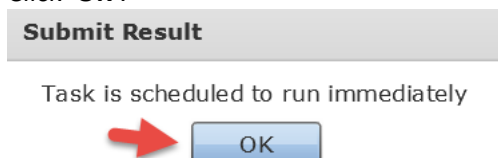
Run the 'NetApp Inventory Collector – FAS3070-A' task.



Click 'Submit' when asked if you are sure you want to run the task now.

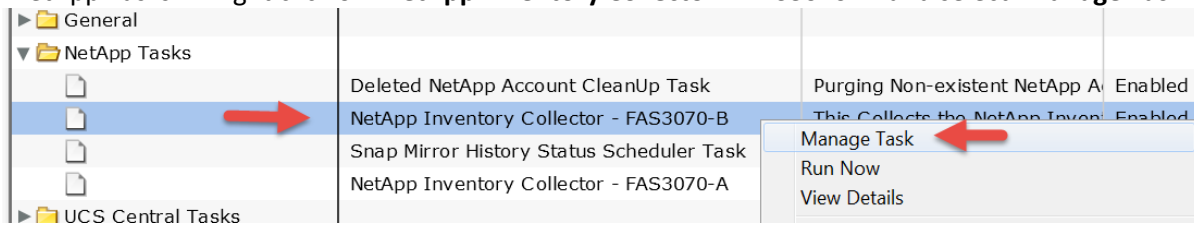


Click 'OK'.



7.6. Assign System Policy to NetApp Controller B System Task

Assign Richardson System Policy to NetApp System Task. Go to Administration -> System -> Service Tasks -> expand 'NetApp Tasks' -> right click on 'NetApp Inventory Collector – FAS3070-B' and select 'Manage Task'.



Drop down and select the 'Richardson System Task Policy' and click 'Submit'.

Manage Task (NetApp Inventory Collector - FAS3070-B)

Task Execution:

System Task Policy:

Hours:

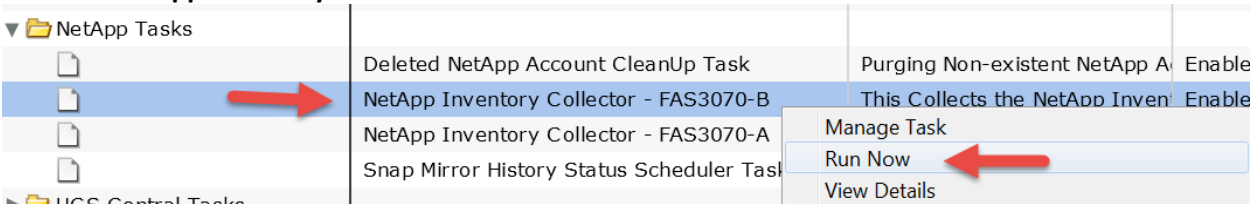
Minutes:

Click 'OK'.

Submit Result

Task details updated successfully

Run the 'NetApp Inventory Collector – FAS3070-B' task.



Click 'Submit' when asked if you are sure you want to run the task now.

Run Now

Are you sure you want to run task 'NetAppInventoryCollector:FAS3070-B' now?

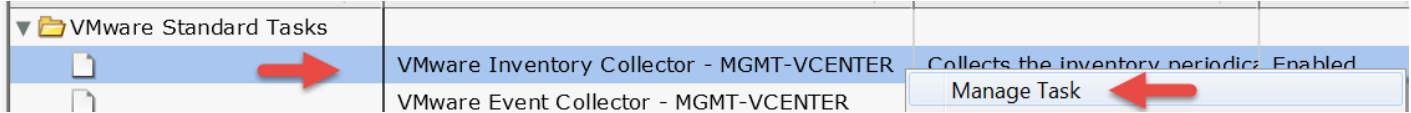
Click 'OK'.

Submit Result

Task is scheduled to run immediately

7.7. Assign System Policy to vCenter System Task

Assign Richardson System Policy to VMware System Task. Go to Administration -> System -> Service Tasks -> expand 'VMware Standard Tasks' -> right click on 'VMware Inventory Collector – MGMT-VCENTER' and select 'Manage Task'.



Drop down and select the 'Richardson System Task Policy' and click 'Submit'.

Manage Task (VMware Inventory Collector - MGMT-VCENTE...

Task Execution: Enable

System Task Policy: Richardson System Task Policy *

Hours: 1

Minutes: 0

Submit Close

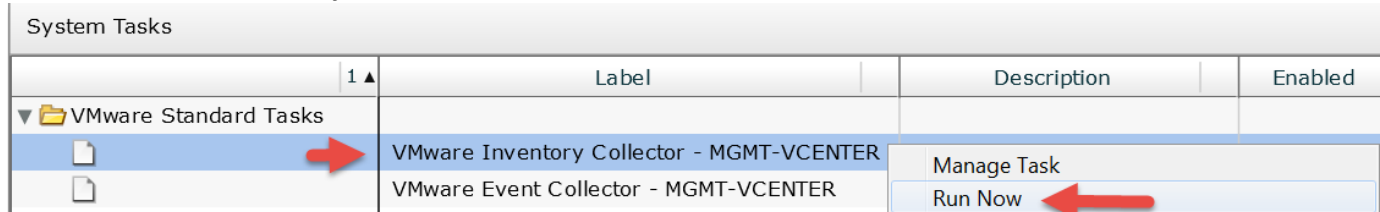
Click 'OK'.

Submit Result

Task details updated successfully

OK

Run the 'VMware Inventory Collector – MGMT-VCENTER' task.



Click 'Submit' when asked if you are sure you want to run the task now.

Run Now

Are you sure you want to run task 'VMwareInventoryCollector:MGMT-VCENTER' now?

Submit Close

Click 'OK'.

Submit Result

Task is scheduled to run immediately

OK

Go to Administration -> System -> Service Tasks -> expand 'VMware Standard Tasks' -> right click on 'VMware Event Collector – MGMT-VCENTER' and select 'Manage Task'.

▼ VMware Standard Tasks			
VMware Inventory Collector - MGMT-VCENTER	Collects the inventory periodically	Enabled	
VMware Event Collector - MGMT-VCENTER	Collects the events periodically	Enabled	Manage Task
▼ Virtualization Tasks			

Drop down and select the 'Richardson System Task Policy' and click 'Submit'.

Manage Task (VMware Event Collector - MGMT-VCENTER)

Task Execution

System Task Policy

Hours

Minutes

Click 'OK'.

Submit Result

Task details updated successfully

Run the 'VMware Event Collector – MGMT-VCENTER' task.

▼ VMware Standard Tasks			
VMware Inventory Collector - MGMT-VCENTER	Collects the inventory periodically	Enabled	
VMware Event Collector - MGMT-VCENTER	Collects the events periodically	Enabled	Run Now
▼ Virtualization Tasks			
Performance Data Collector - MGMT-VCENTER			

Click 'Submit' when asked if you are sure you want to run the task now.

Run Now

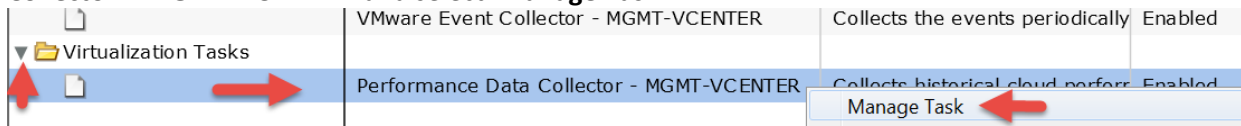
Are you sure you want to run task 'VMwareEventCollector:MGMT-VCENTER' now?

Click 'OK'.

Submit Result

Task is scheduled to run immediately

Go to Administration -> System -> Service Tasks -> expand 'Virtualization Tasks' -> right click on 'Performance Data Collector – MGMT-VCENTER' and select 'Manage Task'.



Drop down and select the 'Richardson System Task Policy' and click 'Submit'.

Manage Task (Performance Data Collector - MGMT-VCENTER)

Task Execution

System Task Policy

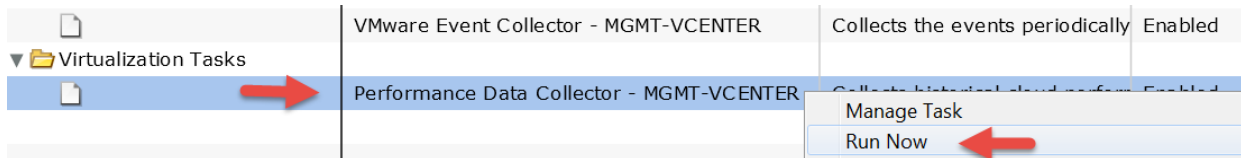
Minutes

Click 'OK'.

Submit Result

Task details updated successfully

Run the 'Performance Data Collector – MGMT-VCENTER' task.



Click 'Submit' when asked if you are sure you want to run the task now.

Run Now

Are you sure you want to run task 'perfDataCollector:MGMT-VCENTER' now?

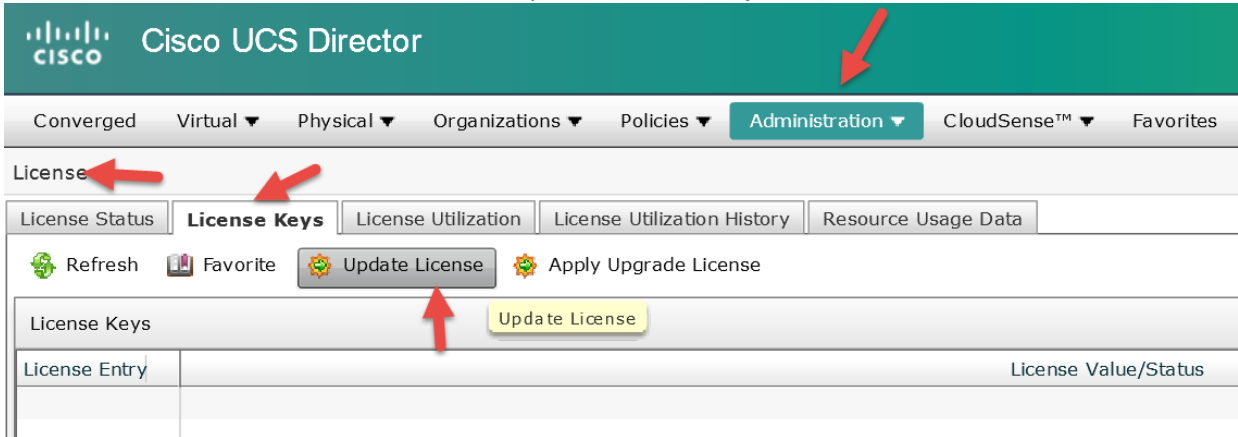
Click 'OK'.

Submit Result

Task is scheduled to run immediately

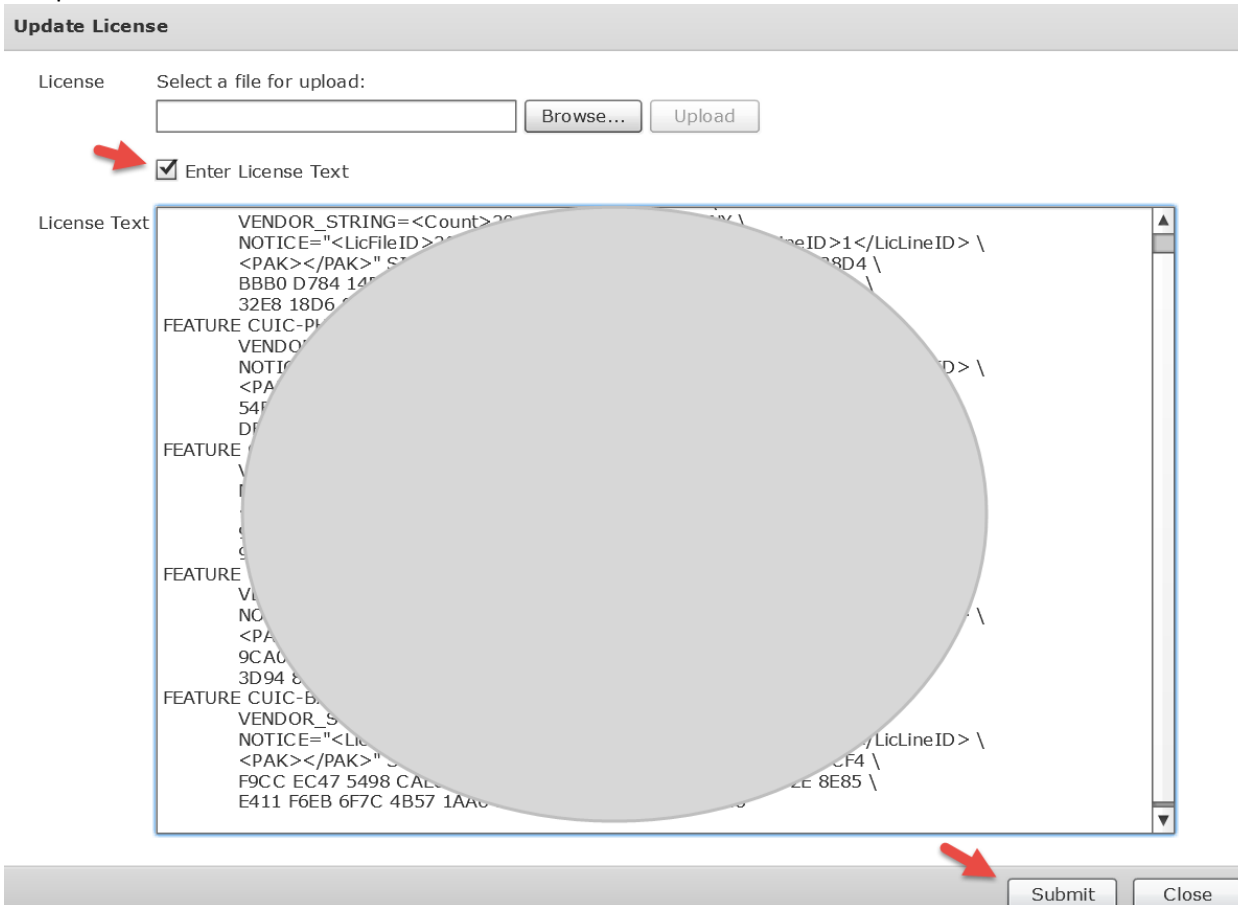
8. Add Licenses to UCS Director

Go to Administrator -> License -> License Keys -> and select 'Update License'.



The screenshot shows the Cisco UCS Director web interface. At the top, the navigation bar includes 'Administration' and 'License'. The 'License' menu is expanded, and 'License Keys' is selected. Below this, there are tabs for 'License Status', 'License Keys', 'License Utilization', 'License Utilization History', and 'Resource Usage Data'. The 'License Keys' tab is active, showing a table with columns for 'License Entry' and 'License Value/Status'. A red arrow points to the 'Update License' button in the top navigation bar, and another red arrow points to the 'Update License' button in the table header.

You have the option to browse to the license file or Enter License Text. To enter the license text, simply copy the license and paste it into the screen then click 'Submit'.



The screenshot shows the 'Update License' dialog box. It has a 'License' section with a text input field and 'Browse...' and 'Upload' buttons. Below this, the 'Enter License Text' checkbox is checked. A large text area contains the license text, which is partially obscured by a large grey circle. At the bottom right, there are 'Submit' and 'Close' buttons. A red arrow points to the 'Submit' button.

```
VENDOR_STRING=<Count>20
NOTICE="<LicFileID>20
<PAK></PAK>"
BBB0 D784 14
32E8 18D6
FEATURE CUIC-PH
VENDOR
NOTICE="<LicFileID>
<PAK></PAK>"
54F
DF
FEATURE
V
9CAU
3D94 8
FEATURE CUIC-B
VENDOR_S
NOTICE="<LicFileID>
<PAK></PAK>"
F9CC EC47 5498 CAL
E411 F6EB 6F7C 4B57 1AA0
```

Verify License Utilization.

Cisco UCS Director

Converged Virtual Physical Organizations Policies **Administration** CloudSense™ Favorites

License License Status License Keys **License Utilization** License Utilization History Resource Usage Data

Refresh Favorite Update License Run License Audit

License	Licensed Lim	Available	Used	Status	
Production Base	1		1	✔ Licensed	
Physical Servers	100	100	0	✔ Licensed	Licensed Limit =Physical BM Server(=0) + Small/Medium POD servers are not counted i
Storage Control	120	120	0	✔ Licensed	Licensed Limit = Actual Licensed(=20) + Small/Medium POD storage controllers are n
Network Devices	120	120	0	✔ Licensed	Licensed Limit = Actual Licensed(=20) + Small/Medium POD network devices are not
Other Devices	105	105	0	✔ Licensed	Licensed Limit = Actual Licensed(=5) + Small/Medium POD storage controllers are n
Big Data Nodes	0	0	0	⚠ Not License	Available = Actual Licensed(=0) - Used(=0)
Small Pod	0	0	0	⚠ Not License	Available = Actual Licensed(=0) - Used(=0) -
Medium Pod	0	0	0	⚠ Not License	Available = Actual Licensed(=0) - Used(=0) -
Small Pod Enter	0	0	0	⚠ Not License	
Medium Pod Ent	0	0	0	⚠ Not License	
Server VMs	5000	5000	0	✔ Licensed	Licensed Limit = Physical Server License Cou Available = Licensed Physical Servers(=100)

9. Mail Setup (Required)

Go to Administrator -> System -> select 'Mail Setup'. Enter the 'Outgoing Email Server (SMTP)', 'Outgoing SMTP Port', 'Outgoing Email Sender Email Address', 'UCSD Server IP Address' and click 'Save'.

Cisco UCS Director

Converged Virtual Physical Organizations Policies Administration

System

System Information **Mail Setup** System Parameters Infrastructure System Parameters

Outgoing Email Server (SMTP) 72.142.112.100 *

Outgoing SMTP Port 25 *

Outgoing SMTP User

Outgoing SMTP Password

Outgoing Email Sender Email Address no-reply@cisco.com *

UCSD Server IP Address 172.17.80.113 *

Send Test Email

Save

Add 'User Contact Email' for admin account. Go to Administration -> User and Groups -> Login Users -> select admin -> click 'Edit'. Enter the 'User Contact Email' and click 'Save'.

Cisco UCS Director

Converged Virtual Physical Organizations Policies Administration CloudSense™

Users and Groups

User Groups **Login Users** Current Online Users

Refresh Favorite Add View

Login Name	First Name	Last Name	Access
admin			
infraUser			

Edit User

User Role System Admin *

Login Name admin

User Contact Email efarfan@cisco.com *

First Name

Last Name

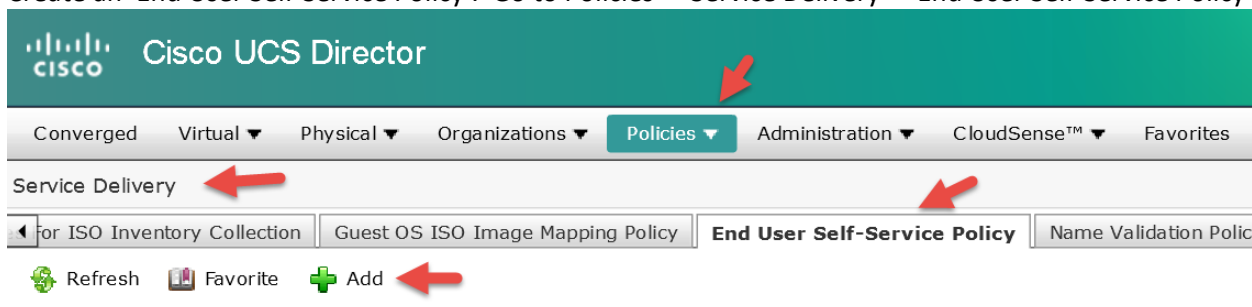
Phone

10. Create Self Service Policy

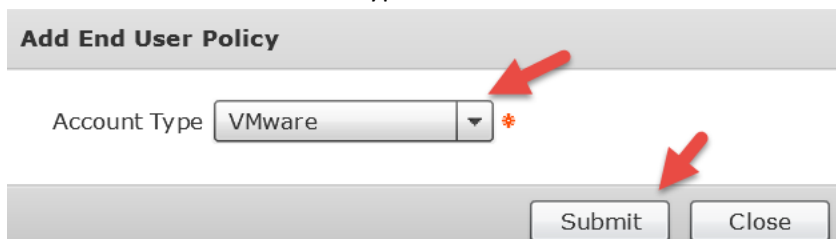
An End User Self-Service Policy controls the actions or tasks that a user can perform on a vDC. The starting point for creating this policy is to specify an Account Type, for example VMware. After you specify an account type, you can continue with creating the policy. After you create the policy, you must assign the policy to a vDC that is created with the same account type. For example, if you have created an end user policy for VMware, then you can specify this policy when you create a VMware vDC. You cannot view or assign policies that have been created for other account types.

Assigning a policy to a vDC is the only method through which you can control the tasks that a user can perform on the vDC. In prior versions, you enabled or disabled tasks on a vDC while creating it. If you have upgraded to the current release, those previously set permissions and options are automatically grouped as an end user policy, with the name of the vDC, and assigned to the vDC.

Create an 'End User Self-Service Policy'. Go to Policies -> Service Delivery -> End User Self-Service Policy -> click 'Add'.



Select 'VMware' for Account Type and click 'Submit'.



Name the Policy and Select all options.

End User Policy

Policy Name

All Buttons *

Policy Description

End User Self-Service Options

- VM Power Management
 - Power ON
 - Power OFF
 - Suspend
 - Standby
 - Reset
 - Reboot
 - Shutdown Guest
- VM Resizing
 - Resize VM
- VM Snapshot Management
 - Create Snapshot
 - Revert Snapshot
 - Mark Golden Snapshot
 - Delete Snapshot
 - Delete All Snapshots
- VM Deletion Management
 - Delete VM
- VM Disk Management
 - Create VM Disk
 - VM Disk Resize
 - Delete VM Disk
- VM Network Management
 - Add vNICs
 - Delete vNICs
 - VM Resync
- VM Lease Expiry
 - Configure Lease Time
- VM Console Management
 - Launch VM Client
 - Configure VNC
 - Test VNC
 - Enable/Disable VMRC Console
- VM Clone and Template Management
 - Clone
 - Clone VM as Image
 - Convert VM as Image
 - Move VM To VDC
 - Assign VMs To VDC
- VM ISO Management
 - Mount ISO Image As CD/DVD Drive

11. Optional - Troubleshooting Service Node Connectivity

11.1. IP Connectivity Troubleshooting

Ping the Service Node from the Primary Node. If you are using the fully qualified domain name instead of an IP address for the Service Node configuration then you should test a ping to it instead of the IP Address. If it doesn't resolve the name you should verify your hosts files on all nodes and your DNS server. You could also change the Service Node configuration to use the IP Address.

```
[root@CUCSD_Primary ~]# ping 172.17.80.116
PING 172.17.80.116 (172.17.80.116) 56(84) bytes of data.
64 bytes from 172.17.80.116: icmp_seq=1 ttl=64 time=0.269 ms
64 bytes from 172.17.80.116: icmp_seq=2 ttl=64 time=0.257 ms
64 bytes from 172.17.80.116: icmp_seq=3 ttl=64 time=0.258 ms

--- 172.17.80.116 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.257/0.261/0.269/0.014 ms
[root@CUCSD_Primary ~]#
```

Tail the logfile.txt file on the Primary Node and then test connectivity to the Service Node.

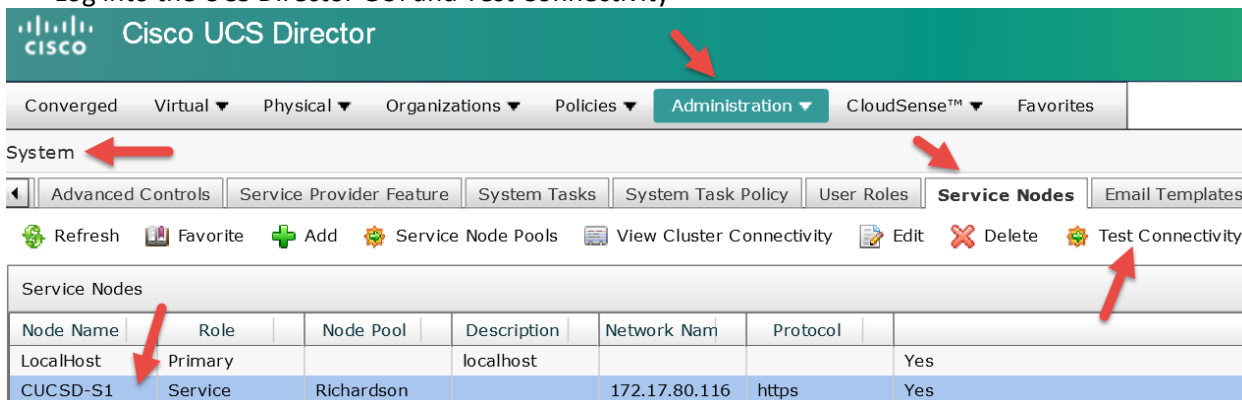
- SSH to the Primary node using the root account
- **'tail -f /opt/infra/inframgr/logfile.txt'**

```
[root@CUCSD_Primary ~]# tail -f /opt/infra/inframgr/logfile.txt
2015-09-19 02:12:10,369 [pool-35-thread-27] INFO getBestAgent(AgentAllocator.java:109) - Node pool default-service
2015-09-19 02:12:10,372 [pool-35-thread-27] INFO getBestAgent(SystemTaskExecutor.java:317) - No Agent available f
VMwareEventCollector:MGMT-VCENTER
2015-09-19 02:12:10,373 [pool-35-thread-27] INFO updateStatus(SystemTaskStatusProvider.java:181) - Task: task.VMw
lector:MGMT-VCENTER changed state to OK
2015-09-19 02:12:10,380 [pool-35-thread-27] INFO executeLocally(SystemTaskExecutor.java:142) - Executing task loc
eEventCollector:MGMT-VCENTER
2015-09-19 02:12:10,380 [pool-35-thread-27] INFO getClusterLeaf(ClusterPersistenceUtil.java:81) - Leaf name Local
2015-09-19 02:12:10,385 [pool-35-thread-27] INFO updateStatus(SystemTaskStatusProvider.java:181) - Task: task.VMw
lector:MGMT-VCENTER changed state to In Progress
2015-09-19 02:12:10,391 [pool-35-thread-27] INFO executeLocally(SystemTaskExecutor.java:158) - Start executing ta
wareEventCollector:MGMT-VCENTER status=OK lastExecuted=1442627820648
```

- Launch a second SSH session to the Primary Node
- Test the connection to the Service Node: **'telnet 172.17.80.116 443'**
- If your output shows connected as show below then the connection was successful
- **Note:** The 443 at the end of the telnet command is port number 443 for https

```
[root@CUCSD_Primary ~]# telnet 172.17.80.116 443
Trying 172.17.80.116...
Connected to 172.17.80.116.
Escape character is '^['.
```

- Monitor the logging in the other session to see if you see any signs for the connection failing.
- Log into the UCS Director GUI and Test Connectivity



Monitor the logging on the Primary Node to see if you see any signs for the connection failing.

SSH to the Primary node and issue **'telnet 172.17.80.116 443'** to initiate a connection to the Service Node and quickly move to the next step. You only have 30 seconds or so to see the connection. Longer than that, you will need to run the telnet command again to re-establish the session.

```
[root@CUCSD_Primary ~]# telnet 172.17.80.116 443
Trying 172.17.80.116...
Connected to 172.17.80.116.
Escape character is '^['.
```

Run the following command on the Service Node: **'netstat -n | grep 172.17.80.113'**. The output in the screen shot below shows ESTABLISHED which is a good sign the connectivity is working properly.

```
[root@CUCSD_Service1 ~]# netstat -n | grep 172.17.80.113
tcp        0      0 :::ffff:172.17.80.116:443  :::ffff:172.17.80.113:49379  ESTABLISHED
[root@CUCSD_Service1 ~]#
```

11.2. Storage Performance Troubleshooting

Verify the connection performance to the datastore using the following command. **'25MB/s'** is the recommended minimum performance for the Primary and Service Nodes and **'50MB/s'** for the Inventory and Monitoring Database Nodes but it's not uncommon to get speeds as low as 4.0 MB/s. If possible, use a storage array that will get you to the optimal performance. It may take a few minutes to process this command before you see the output.

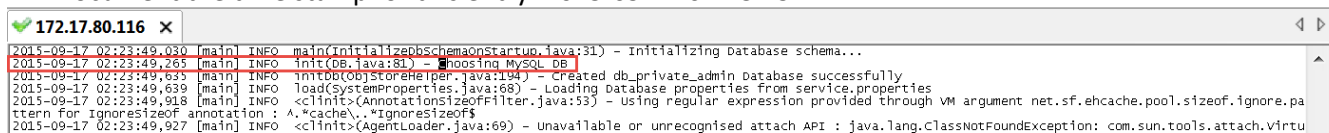
- Command: **'dd if=/dev/zero of=/tmp/test1 bs=4096 count=262144 oflag=direct'**

```
[root@CUCSD_Service1 ~]# dd if=/dev/zero of=/tmp/test1 bs=4096 count=262144 oflag=direct
262144+0 records in
262144+0 records out
1073741824 bytes (1.1 GB) copied, 252.307 seconds, 4.3 MB/s
[root@CUCSD_Service1 ~]#
```

11.3. Determine if Service Node is UP and how long it took to come UP

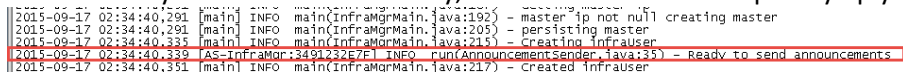
Determine if the Service Node is completely up.

- Change Directory to inframgr: **'cd /opt/infra/inframgr/'**
- You can look at the logfile: **'tail -f logfile.txt'**
- Exit the logfile: enter **'quit'**
- Open the logfile with vi so you can search it: **'vi logfile.txt'**
- Search the logfile for **'Choosing MySQL DB'**: enter **'G'** to go to the end of the logfile then enter **'?Choosing'** to find the last instance of Choosing in the logfile, press return
- Document the time stamp for this entry: 2015-09-17 02:23:49



```
172.17.80.116 x
2015-09-17 02:23:49,030 [main] INFO main(InitializeSchemaOnStartup.java:31) - Initializing database schema...
2015-09-17 02:23:49,265 [main] INFO init(DB.java:81) - Choosing MySQL DB
2015-09-17 02:23:49,635 [main] INFO initDB(ObjStoreHelper.java:134) - Created db_private_admin database successfully
2015-09-17 02:23:49,639 [main] INFO load(SystemProperties.java:68) - Loading Database properties from service.properties
2015-09-17 02:23:49,918 [main] INFO <clinit>(AnnotationsSizeOfFilter.java:53) - Using regular expression provided through VM argument net.sf.ehcache.pool.sizeof.ignore.pattern For IgnoreSizeOf annotation : A.*cache\..*IgnoreSizeOf$
2015-09-17 02:23:49,927 [main] INFO <clinit>(AgentLoader.java:69) - Unavailable or unrecognized attach API : java.lang.ClassNotFoundException: com.sun.tools.attach.VirtualMachine
```

- Search the logfile for **'Ready to send announcements'**: enter **'G'** to go to the end of the logfile then enter **'?Ready'** to find the last instance of Ready in the logfile, press return
- Document the time stamp for this entry: 2015-09-17 02:34:40
- **Note:** If you do not see this entry, then the node isn't completely up yet. Wait until you see this entry.



```
2015-09-17 02:34:40,291 [main] INFO main(InframgrMain.java:192) - master ip not null creating master
2015-09-17 02:34:40,291 [main] INFO main(InframgrMain.java:205) - persisting master
2015-09-17 02:34:40,335 [main] INFO main(InframgrMain.java:215) - Creating infrauser
2015-09-17 02:34:40,339 [AS-InfraMgr:3491232E7F1] INFO run(AnnouncementSender.java:35) - Ready to send announcements
2015-09-17 02:34:40,351 [main] INFO main(InframgrMain.java:217) - Created infrauser
```

- The difference between **'Choosing MySQL DB'** and **'Ready to send announcements'** is the time it took for the node to come up. In this case, it took approximately 11 minutes.
- Exit vi without saving: enter **'quit'**

11.4. Verify if Task are taking longer than the Frequency configured

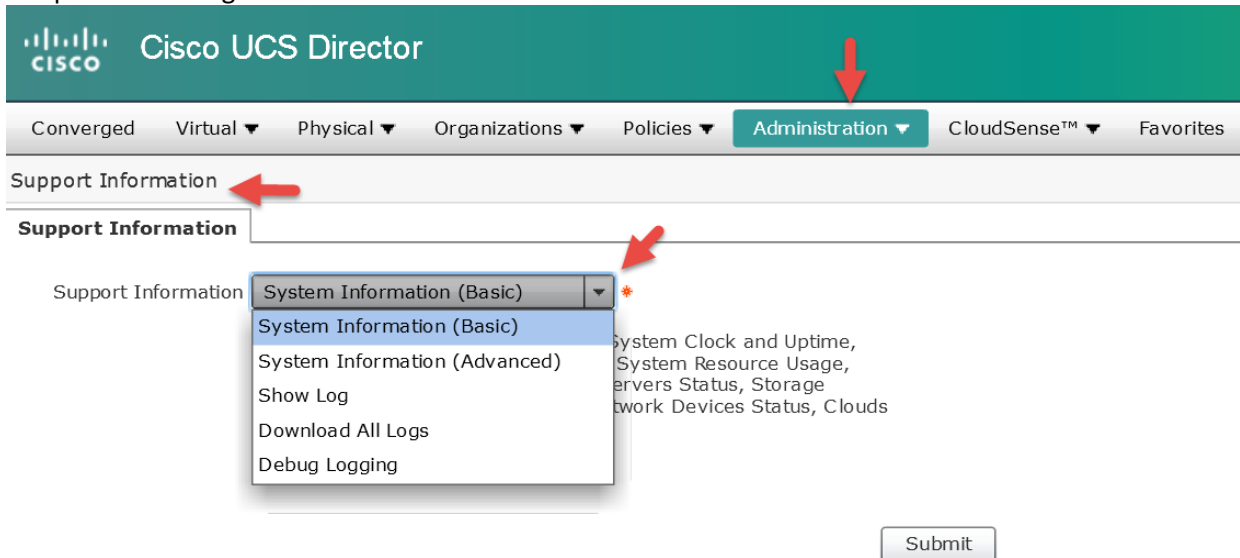
Verify the task does not take longer to complete than the frequency of the task. In this case the 'VMware Inventory Collector – MGMT-VCENTER' took 21 seconds to complete and the frequency is 1 hour so this is not a problem. If the task took longer than the frequency, this would be a problem.

The screenshot shows the Cisco UCS Director interface. The top navigation bar includes 'Converged', 'Virtual', 'Physical', 'Organizations', 'Policies', 'Administration', 'CloudSense™', and 'Favorites'. The 'Administration' menu is highlighted with a red arrow. Below the navigation bar, the 'System' section is visible, with 'System Tasks' selected. The 'System Tasks' table is shown with columns: Label, Enable, Frequency, Executor, Execution N1, Execution Duration, Start Time, and Last Executed Time. The 'VMware Inventory Collector - MGMT-VCENTER' task is highlighted with a red arrow. Its execution duration is '0 minutes 21 seconds', and its start and last executed times are '10/06/2015 19:49:59' and '10/06/2015 19:50:21' respectively, both highlighted with red boxes.

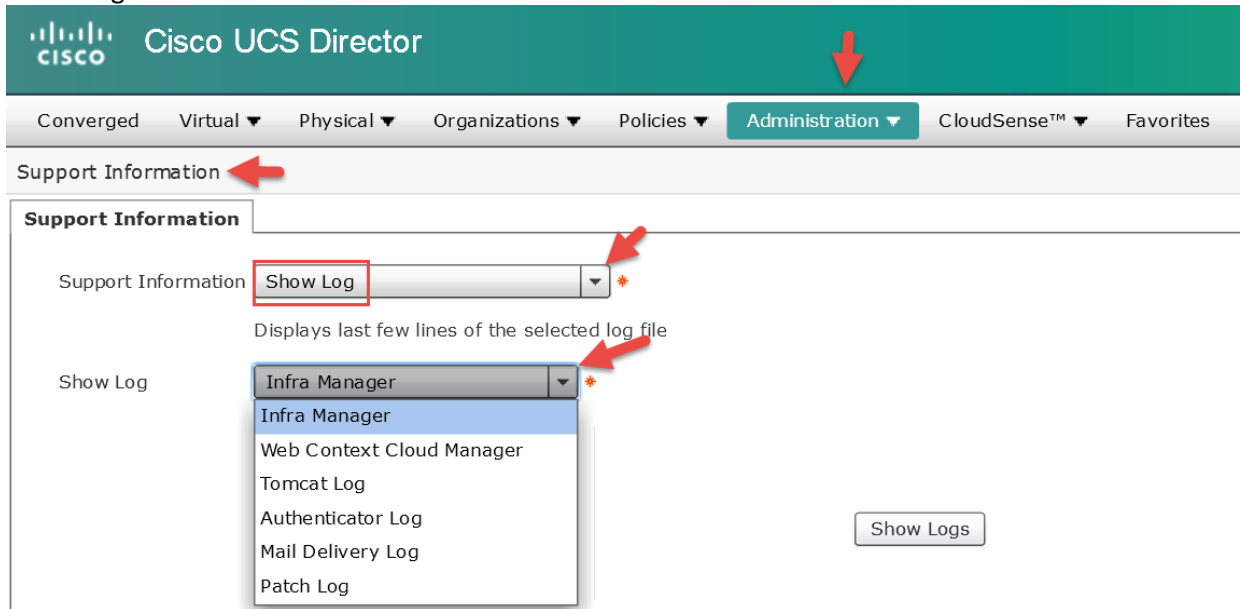
Label	Enable	Frequency	Executor	Execution N1	Execution Duration	Start Time	Last Executed Time
VMware Inventory Collector - MGMT-VCENTER	Enabled	1 hour	CUCSD-S1	172.17.80.116 OK	0 minutes 21 seconds	10/06/2015 19:49:59	10/06/2015 19:50:21
VMware Event Collector - MGMT-VCENTER	Enabled	15 minutes	CUCSD-S1	172.17.80.116 OK	0 minutes 0 seconds	10/06/2015 19:49:49	10/06/2015 19:49:50

11.5. Obtaining Logs from UCS Director

If you need to view or download the logs from UCS Director, you can find them here. Administration -> 'Support Information' and select the logs you want to see or download. If you open a TAC case, they will most likely request you to upload these logs to the TAC Case.



Useful logs to view from the GUI.



Last resort: Reboot the Primary Node and see if this fixes the connectivity issue between the Primary Node and the Services Node. If that doesn't fix the issue, then reboot the Service Node. You can reboot these Nodes via root account using the reboot command or shelladmin account and select the menu item to reboot appliance.

If all else fails, Open a TAC Case ;-)