Cisco Spaces: Connector OVA

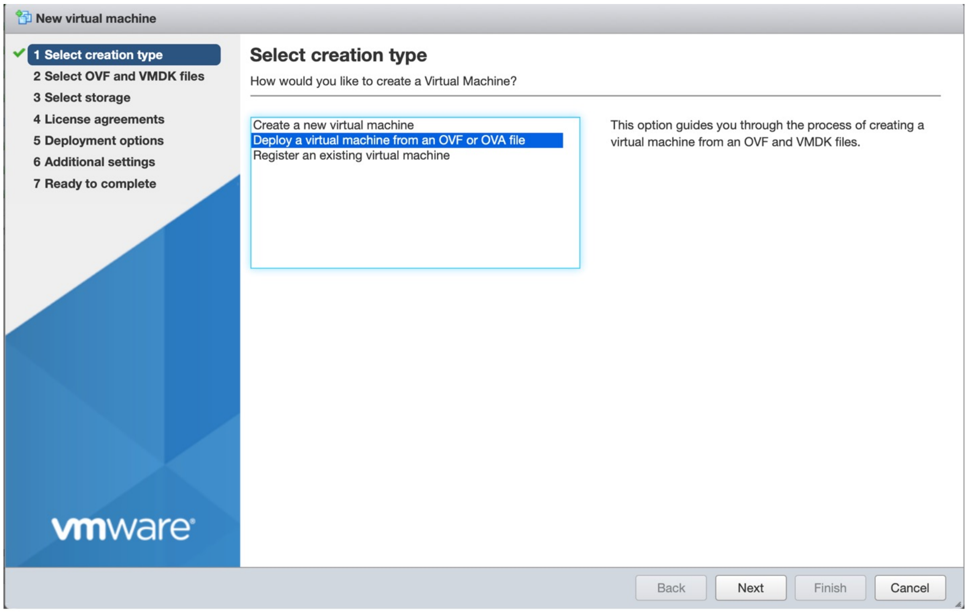
Downloading and Deploying the Cisco Spaces: Connector OVA (Single Interface)

This chapter provides information about how to download and deploy the Cisco Spaces: Connector and obtain the URL for the Connector GUI.

Step 1 Download Connector 2.3 from Cisco.com.

Step 2 Create a virtual machine in the ESXi server and deploy the downloaded Cisco Spaces: Connector OVA.

Step 3 In the **Select creation type** window, choose **Deploy a virtual machine from an OVF or OVA** file, and click **Next**.



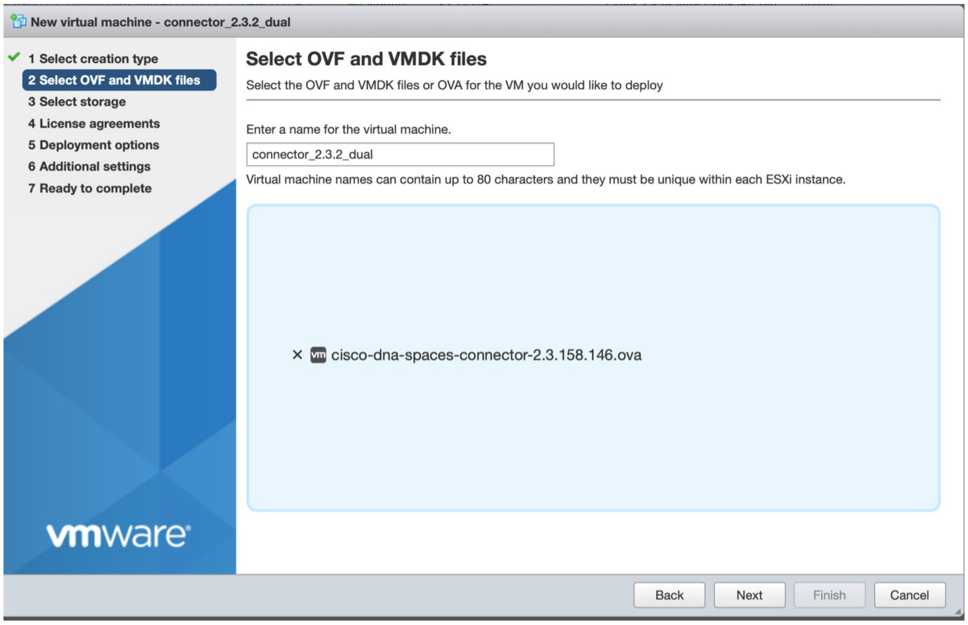
Select creation type

How would you like to create a Virtual Machine?

Create a new virtual machine
Deploy a virtual machine from an OVF or OVA file
Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

Step 4 In the **Select OVF and VMDK files** window, enter a name for the virtual machine. Click the blue area to either select files from the computer or drag and drop files. Click **Next**.



Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

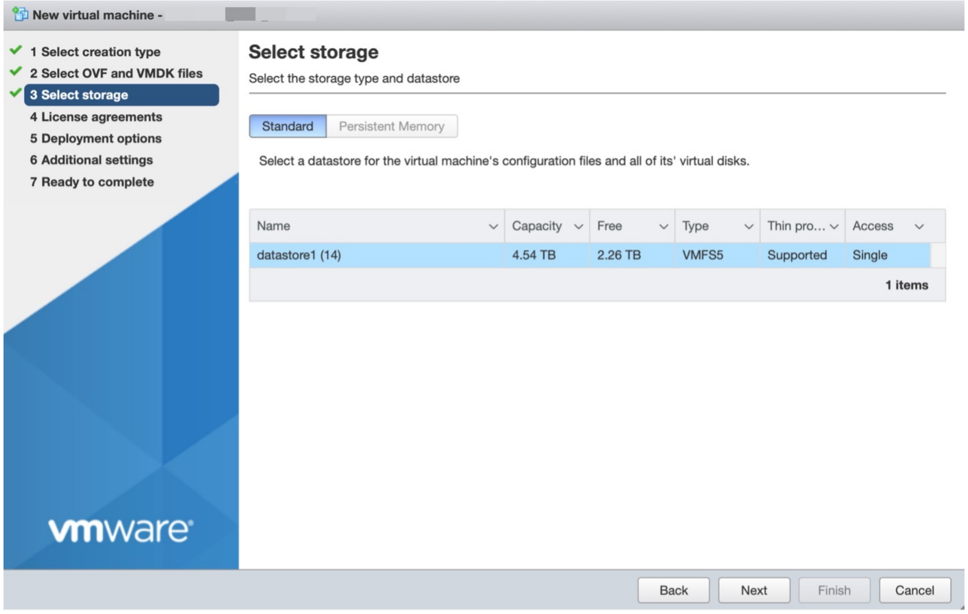
Enter a name for the virtual machine.

connector_2.3.2_dual

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× cisco-dna-spaces-connector-2.3.158.146.ova

Step 5 In the **Select storage** window, the **Standard** storage configuration is displayed. Click **Next**.



New virtual machine - [redacted]

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select storage

Select the storage type and datastore

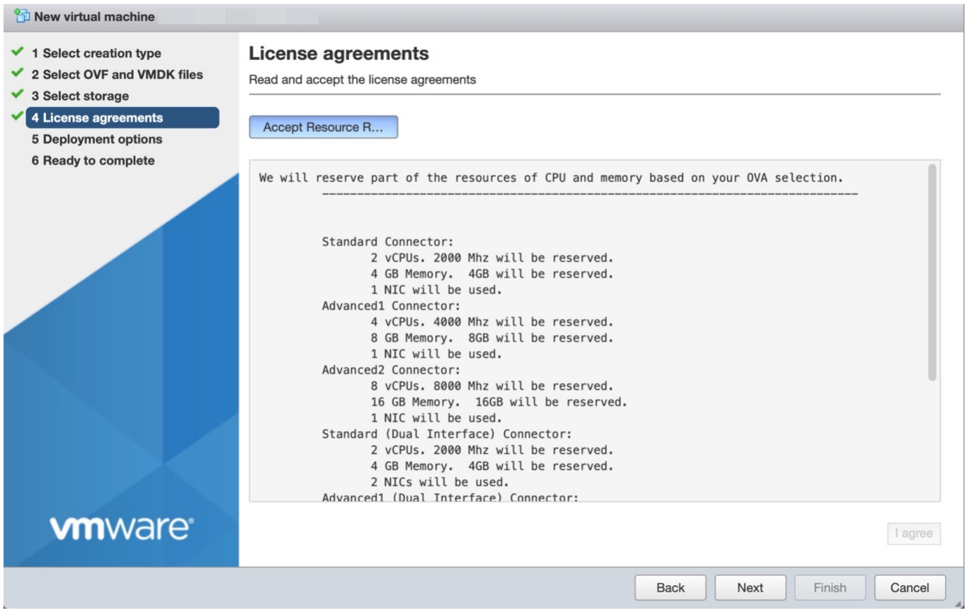
Standard | Persistent Memory

Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1 (14)	4.54 TB	2.26 TB	VMFS5	Supported	Single

1 items

Step 6 In the **License agreements** window, read the license agreement that is displayed and scroll to the end. Click **I Agree** and then click **Next**.



New virtual machine

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 License agreements
- 5 Deployment options
- 6 Ready to complete

License agreements

Read and accept the license agreements

Accept Resource R...

```
We will reserve part of the resources of CPU and memory based on your OVA selection.
         ----------------------------------------------------------------------------


         Standard Connector:
                2 vCPUs. 2000 Mhz will be reserved.
                4 GB Memory.  4GB will be reserved.
                1 NIC will be used.
         Advanced1 Connector:
                4 vCPUs. 4000 Mhz will be reserved.
                8 GB Memory.  8GB will be reserved.
                1 NIC will be used.
         Advanced2 Connector:
                8 vCPUs. 8000 Mhz will be reserved.
                16 GB Memory.  16GB will be reserved.
                1 NIC will be used.
         Standard (Dual Interface) Connector:
                2 vCPUs. 2000 Mhz will be reserved.
                4 GB Memory.  4GB will be reserved.
                2 NICs will be used.
         Advanced1 (Dual Interface) Connector:
```

Step 7 In the **Deployment Options** window, do the following:

a) In the **Network-mapping** field, enter the name of the network.

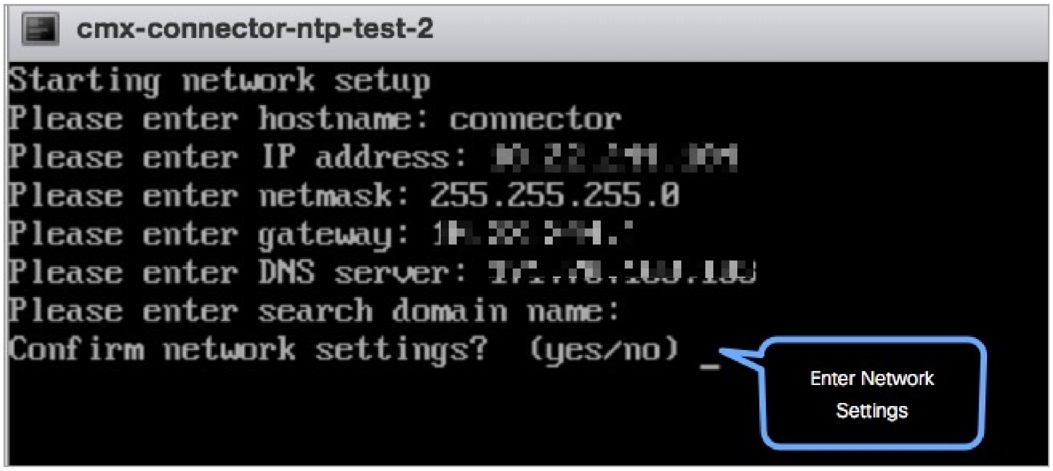
b) From the **Deployment type** drop-down list, choose one of the following, and click **Next**:

- **Standard**
- **Advanced1**
- **Advanced2**

Step 8 Review the configurations and click **Finish**.

Step 9 Log in to the terminal and enter the default username **root** and default password **cisco**.

Step 10 Enter the network settings by specifying parameters such as IP address, hostname, and so on, that you want to configure on the Cisco Spaces: Connector.



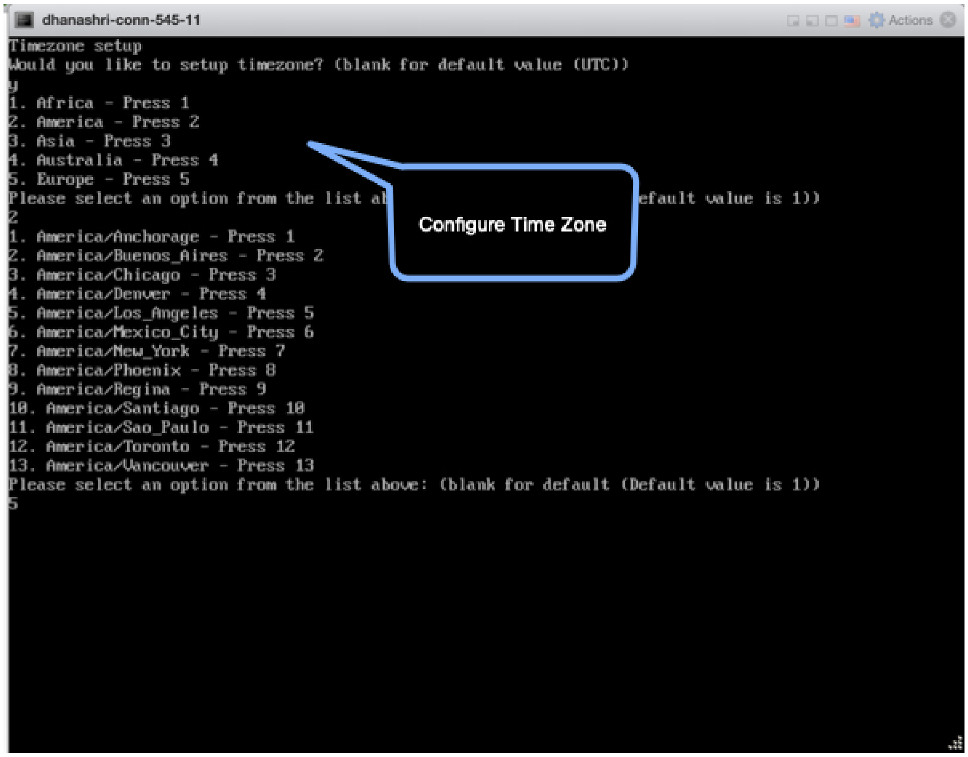
cmx-connector-ntp-test-2

```
Starting network setup
Please enter hostname: connector
Please enter IP address: [redacted]
Please enter netmask: 255.255.255.0
Please enter gateway: [redacted]
Please enter DNS server: [redacted]
Please enter search domain name:
Confirm network settings? (yes/no) _
```

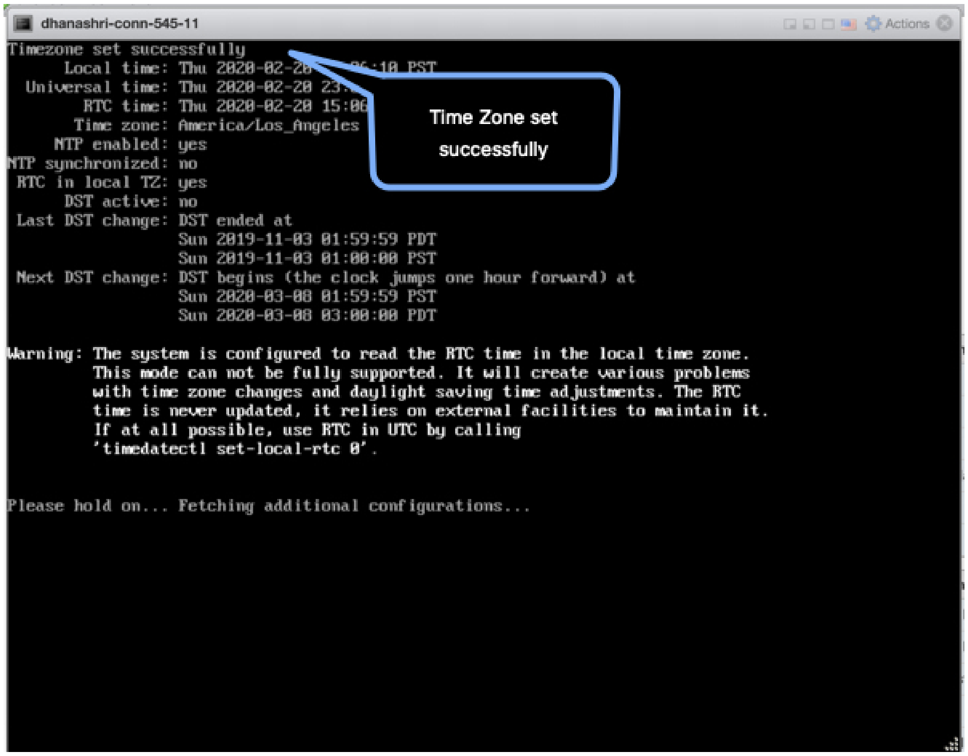
Note Because this configuration screen times out in 60 seconds, ensure that you provide the input on time to avoid reconfiguration.

You can add multiple DNS server as a comma separated list in this step. Once the task is complete and the Cisco Spaces: Connector is deployed, you can login to the Connector CLI, and run the **connectorctl networkconfig** command to add more DNS servers or edit the existing list.

Step 11 Enter the time zone.



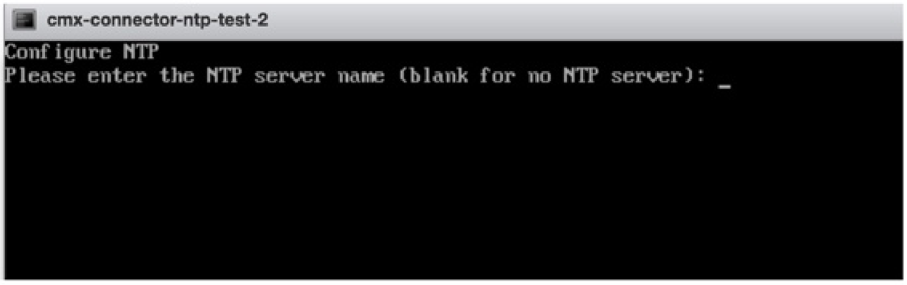
```
Timezone setup
Would you like to setup timezone? (blank for default value (UTC))
y
1. Africa - Press 1
2. America - Press 2
3. Asia - Press 3
4. Australia - Press 4
5. Europe - Press 5
Please select an option from the list al                        efault value is 1))
2
1. America/Anchorage - Press 1
2. America/Buenos_Aires - Press 2
3. America/Chicago - Press 3
4. America/Denver - Press 4
5. America/Los_Angeles - Press 5
6. America/Mexico_City - Press 6
7. America/New_York - Press 7
8. America/Phoenix - Press 8
9. America/Regina - Press 9
10. America/Santiago - Press 10
11. America/Sao_Paulo - Press 11
12. America/Toronto - Press 12
13. America/Vancouver - Press 13
Please select an option from the list above: (blank for default (Default value is 1))
5
```



```
Timezone set successfully
      Local time: Thu 2020-02-2      6:10 PST
  Universal time: Thu 2020-02-20 23:
        RTC time: Thu 2020-02-20 15:06
       Time zone: America/Los_Angeles
     NTP enabled: yes
NTP synchronized: no
 RTC in local TZ: yes
      DST active: no
 Last DST change: DST ended at
                  Sun 2019-11-03 01:59:59 PDT
                  Sun 2019-11-03 01:00:00 PST
 Next DST change: DST begins (the clock jumps one hour forward) at
                  Sun 2020-03-08 01:59:59 PST
                  Sun 2020-03-08 03:00:00 PDT

Warning: The system is configured to read the RTC time in the local time zone.
         This mode can not be fully supported. It will create various problems
         with time zone changes and daylight saving time adjustments. The RTC
         time is never updated, it relies on external facilities to maintain it.
         If at all possible, use RTC in UTC by calling
         'timedatectl set-local-rtc 0'.


Please hold on... Fetching additional configurations...
```

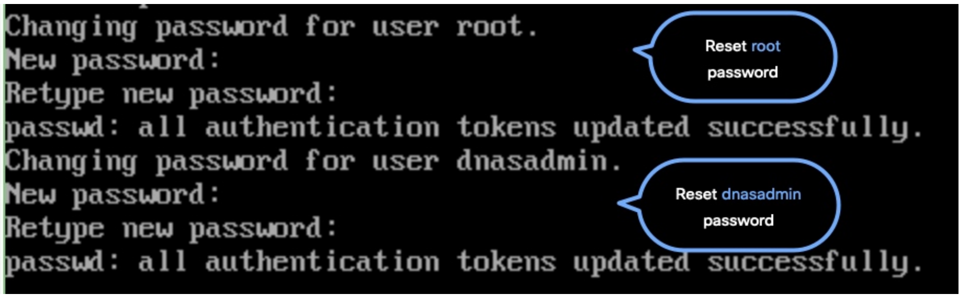
Step 12 Enter the Network Time Protocol (NTP) server name to synchronize the system time with the NTP server's or leave it blank if you do not want to configure an NTP server.

Figure 1: Enter NTP Setting



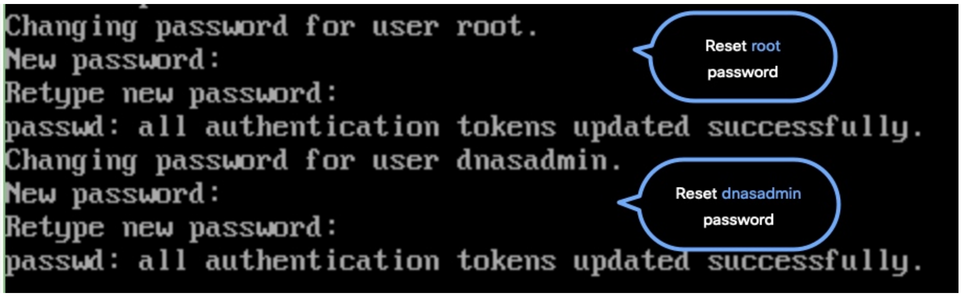
```
Configure NTP
Please enter the NTP server name (blank for no NTP server): _
```

Step 13 Set a new password for the **root** user.



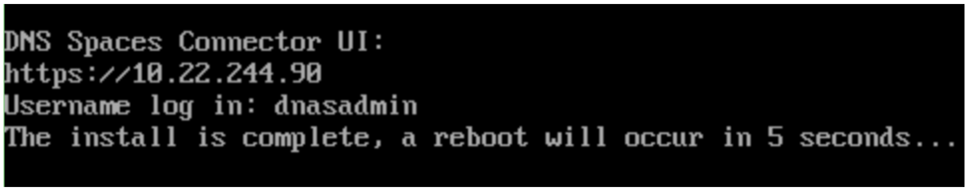
```
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Changing password for user dnasadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Step 14 Set a new password for the **dnasadmin** user, which is user with administrative privileges.



```
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Changing password for user dnasadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Step 15 Copy and save the URL before the automatic reboot. You can use this URL later to open the Cisco Spaces: Connector GUI.



```
DNS Spaces Connector UI:
https://10.22.244.90
Username log in: dnasadmin
The install is complete, a reboot will occur in 5 seconds...
```

What to do next

.

The root user is disabled and is used only for advanced troubleshooting by Cisco Support Team.

Downloading and Deploying the Cisco Spaces: Connector OVA (Dual Interface)

Starting with Connector 2.3.2, you can use the dual-interface deployment of the Connector in network deployments which require the Connector to connect to two separate networks.

One of these networks is usually a private network connecting most of your devices. The other network is external facing and hence can connect to the cloud-hosted Cisco Spaces.

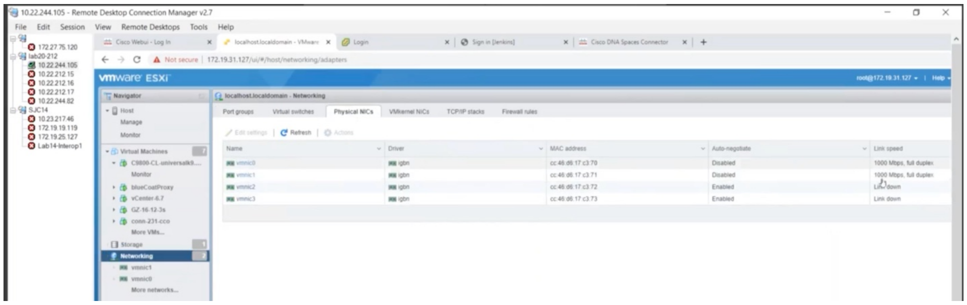
This deployment is recommended when most of the devices that are managed by the Connector are on private or internal networks.

Note We recommend that you connect the controller to a private network because this configuration allows the Connector to connect to the controller using SSH connections.

Before you begin

Ensure that the Cisco Unified Computing System (Cisco UCS) device where you install the Open Virtualization Appliance (OVA) is connected to two separate networks. In this network configuration, the Cisco UCS device is configured with two physical network interface cards (NICs). Each NIC is connected to a switch. In this way, the Cisco UCS device is connected to two networks.

Figure 2: Two Physical Interfaces

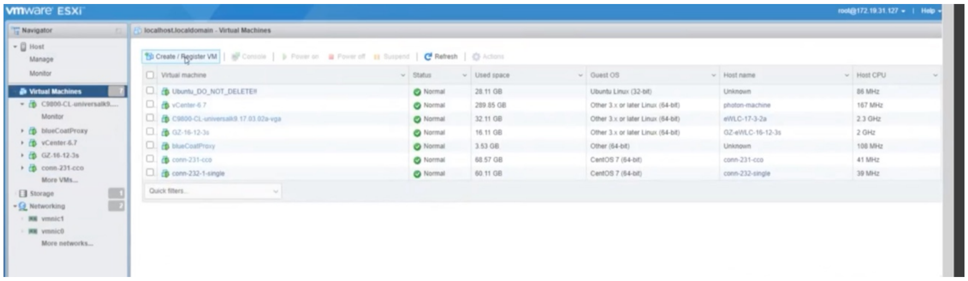


172.19.31.127/ui/#/host/networking/adapters

localhost.localdomain - Networking

Name	Driver	MAC address	Auto-negotiate	Link speed
vmnic0	igbn	cc:46:d6:17:c3:70	Disabled	1000 Mbps, full duplex
vmnic1	igbn	cc:46:d6:17:c3:71	Disabled	1000 Mbps, full duplex
vmnic2	igbn	cc:46:d6:17:c3:72	Enabled	Link down
vmnic3	igbn	cc:46:d6:17:c3:73	Enabled	Link down

Figure 3: Two Separate Networks



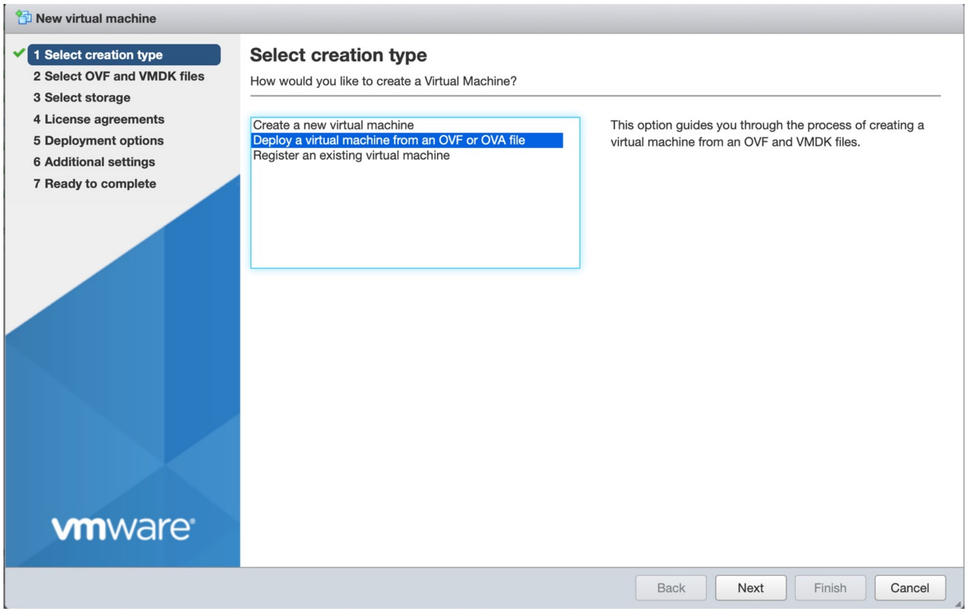
localhost.localdomain - Virtual Machines

Virtual machine	Status	Used space	Guest OS	Host name	Host CPU
Ubuntu_DO_NOT_DELETE!!	Normal	28.11 GB	Ubuntu Linux (32-bit)	Unknown	86 MHz
vCenter-6.7	Normal	289.85 GB	Other 3.x or later Linux (64-bit)	photon-machine	167 MHz
C9800-CL-universalk9.17.03.02a-vga	Normal	32.11 GB	Other 3.x or later Linux (64-bit)	eWLC-17-3-2a	2.3 GHz
GZ-16-12-3s	Normal	16.11 GB	Other 3.x or later Linux (64-bit)	GZ-eWLC-16-12-3s	2 GHz
blueCoatProxy	Normal	3.53 GB	Other (64-bit)	Unknown	108 MHz
conn-231-cco	Normal	68.57 GB	CentOS 7 (64-bit)	conn-231-cco	41 MHz
conn-232-1-single	Normal	60.11 GB	CentOS 7 (64-bit)	conn-232-single	39 MHz

Step 1 Download Connector 2.3 from Cisco.com.

Step 2 Create a virtual machine in the ESXi server and deploy the downloaded Cisco Spaces: Connector OVA.

Step 3 In the **Select creation type** window, choose **Deploy a virtual machine from an OVF or OVA** file, and click **Next**.



New virtual machine

1 Select creation type
2 Select OVF and VMDK files
3 Select storage
4 License agreements
5 Deployment options
6 Additional settings
7 Ready to complete

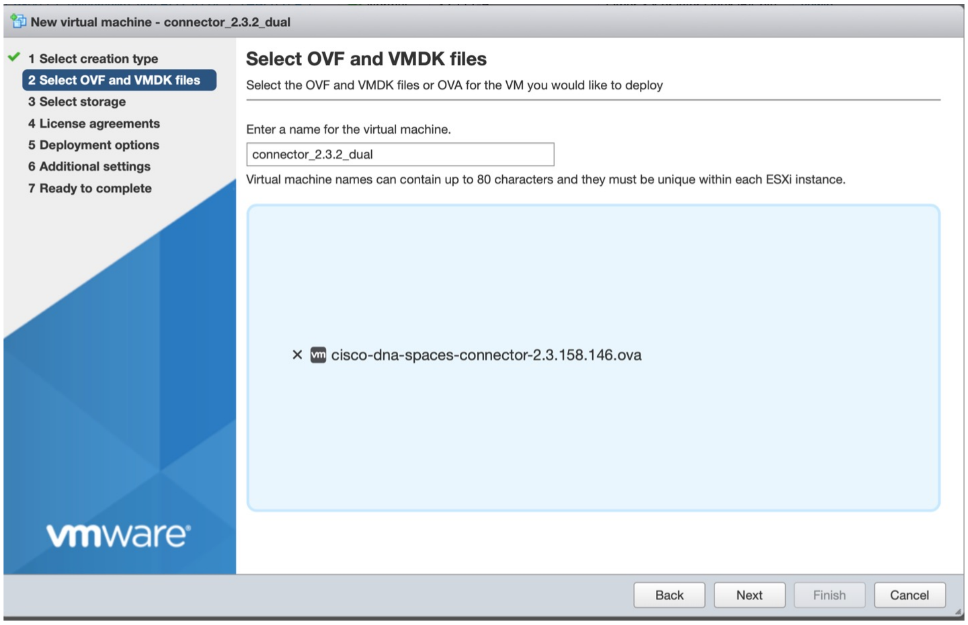
Select creation type

How would you like to create a Virtual Machine?

Create a new virtual machine
Deploy a virtual machine from an OVF or OVA file
Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

Step 4 In the **Select OVF and VMDK files** window, enter a name for the virtual machine. Click the blue area to either select files from the computer or drag and drop files. Click **Next**.



New virtual machine - connector_2.3.2_dual

1 Select creation type
2 Select OVF and VMDK files
3 Select storage
4 License agreements
5 Deployment options
6 Additional settings
7 Ready to complete

Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

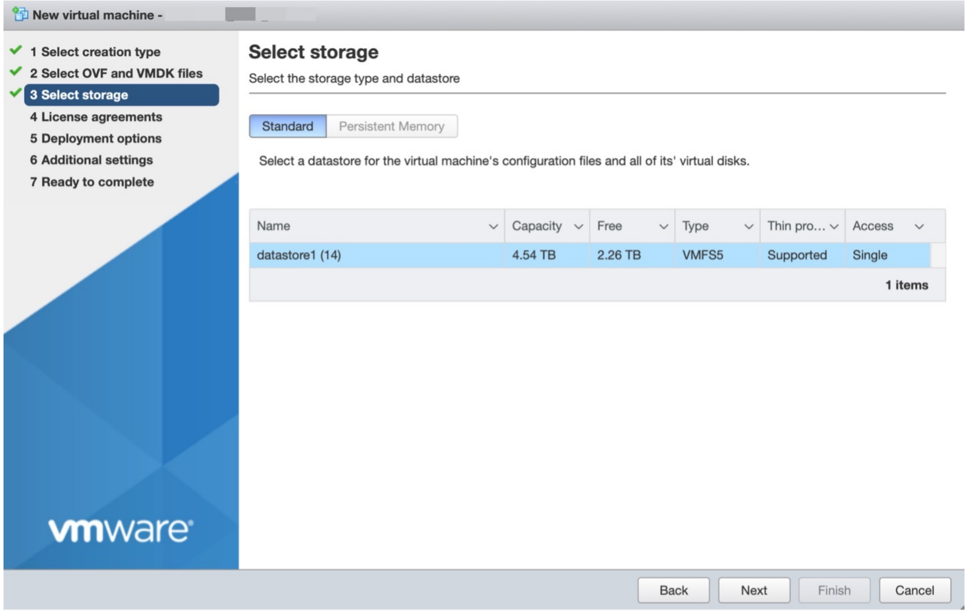
Enter a name for the virtual machine.

connector_2.3.2_dual

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× cisco-dna-spaces-connector-2.3.158.146.ova

Step 5 In the **Select storage** window, the **Standard** storage configuration is displayed. Click **Next**.



Select storage

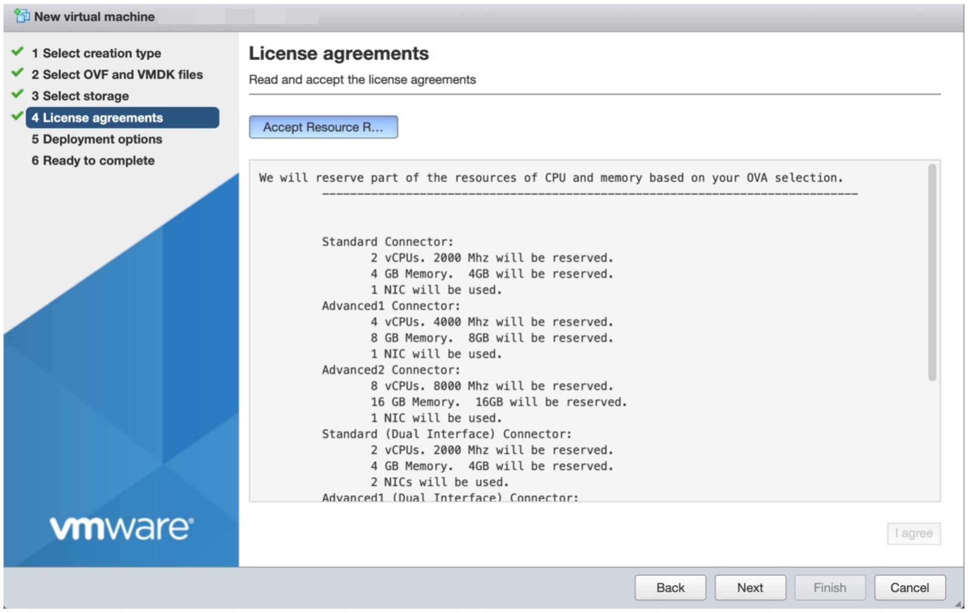
Select the storage type and datastore

Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1 (14)	4.54 TB	2.26 TB	VMFS5	Supported	Single

1 items

Step 6 In the **License agreements** window, read the license agreement that is displayed and scroll to the end. Click **I Agree** and then click **Next**.



License agreements

Read and accept the license agreements

```
We will reserve part of the resources of CPU and memory based on your OVA selection.
         ------------------------------------------------------------------------------


         Standard Connector:
                2 vCPUs. 2000 Mhz will be reserved.
                4 GB Memory.  4GB will be reserved.
                1 NIC will be used.
         Advanced1 Connector:
                4 vCPUs. 4000 Mhz will be reserved.
                8 GB Memory.  8GB will be reserved.
                1 NIC will be used.
         Advanced2 Connector:
                8 vCPUs. 8000 Mhz will be reserved.
                16 GB Memory.  16GB will be reserved.
                1 NIC will be used.
         Standard (Dual Interface) Connector:
                2 vCPUs. 2000 Mhz will be reserved.
                4 GB Memory.  4GB will be reserved.
                2 NICs will be used.
         Advanced1 (Dual Interface) Connector:
```

Step 7 In the **Deployment options** window, do the following:

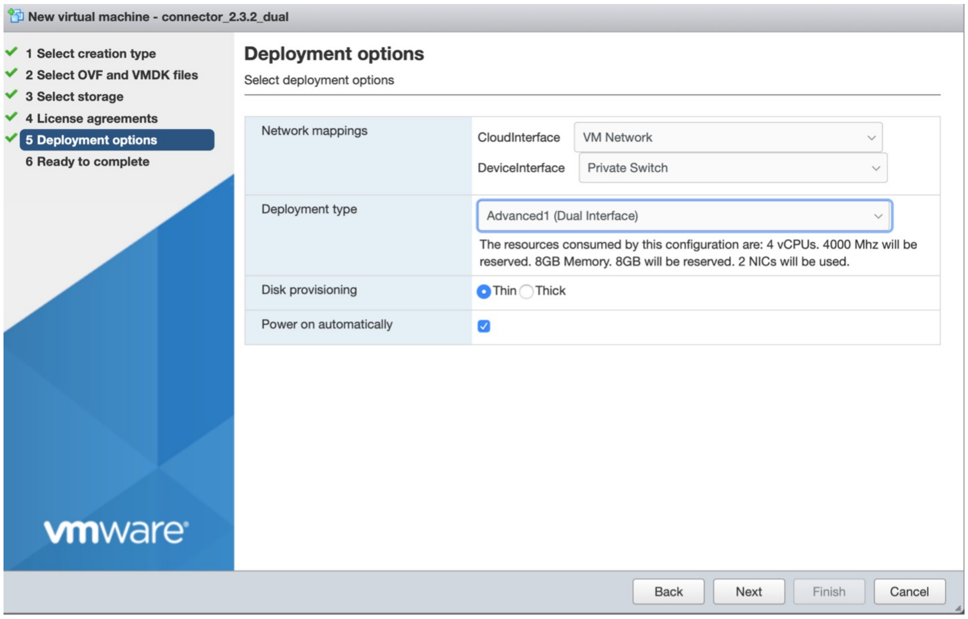
a) In the **CloudInterface** field, enter the name of the external-facing network.

b) In the **DeviceInterface** field, enter the name of the private network.

c) From the **Deployment type** drop-down list, choose one of the following deployment types, and lick **Next**.

- **Standard (Dual Interface)**
- **Advanced1 (Dual Interface)**
- **Advanced2 (Dual Interface)**

Figure 4: Entering the External-Facing and Private Network's Names



New virtual machine - connector_2.3.2_dual

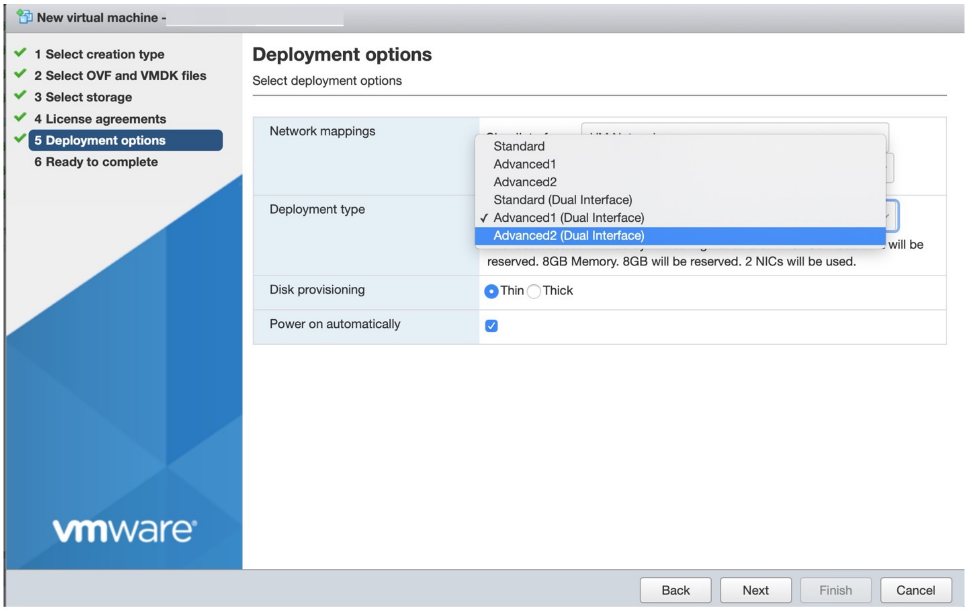
- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 License agreements
- ✓ 5 Deployment options
- 6 Ready to complete

Deployment options

Select deployment options

Network mappings	CloudInterface: VM Network DeviceInterface: Private Switch
Deployment type	Advanced1 (Dual Interface) The resources consumed by this configuration are: 4 vCPUs. 4000 Mhz will be reserved. 8GB Memory. 8GB will be reserved. 2 NICs will be used.
Disk provisioning	● Thin ○ Thick
Power on automatically	☑

Figure 5: Choosing the Deployment Type



New virtual machine -

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 License agreements
- ✓ 5 Deployment options
- 6 Ready to complete

Deployment options

Select deployment options

Network mappings	
Deployment type	will be reserved. 8GB Memory. 8GB will be reserved. 2 NICs will be used.
Disk provisioning	● Thin ○ Thick
Power on automatically	☑

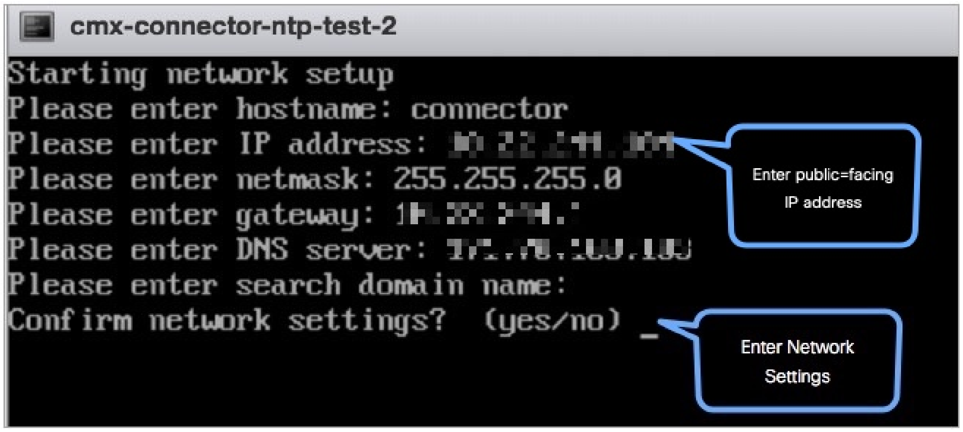
Standard
Advanced1
Advanced2
Standard (Dual Interface)
✓ Advanced1 (Dual Interface)
Advanced2 (Dual Interface)
vmware
Back
Next
Finish
Cancel

Step 8 Review the configurations and click **Finish**.

Step 9 Log in to the terminal and enter the default username **root** and default password **cisco**.

Step 10 Configure the network settings for the external-facing network first, by specifying the parameters such as IP address, hostname, and so on.

Figure 6: Enter the Network Settings of External-Facing Network

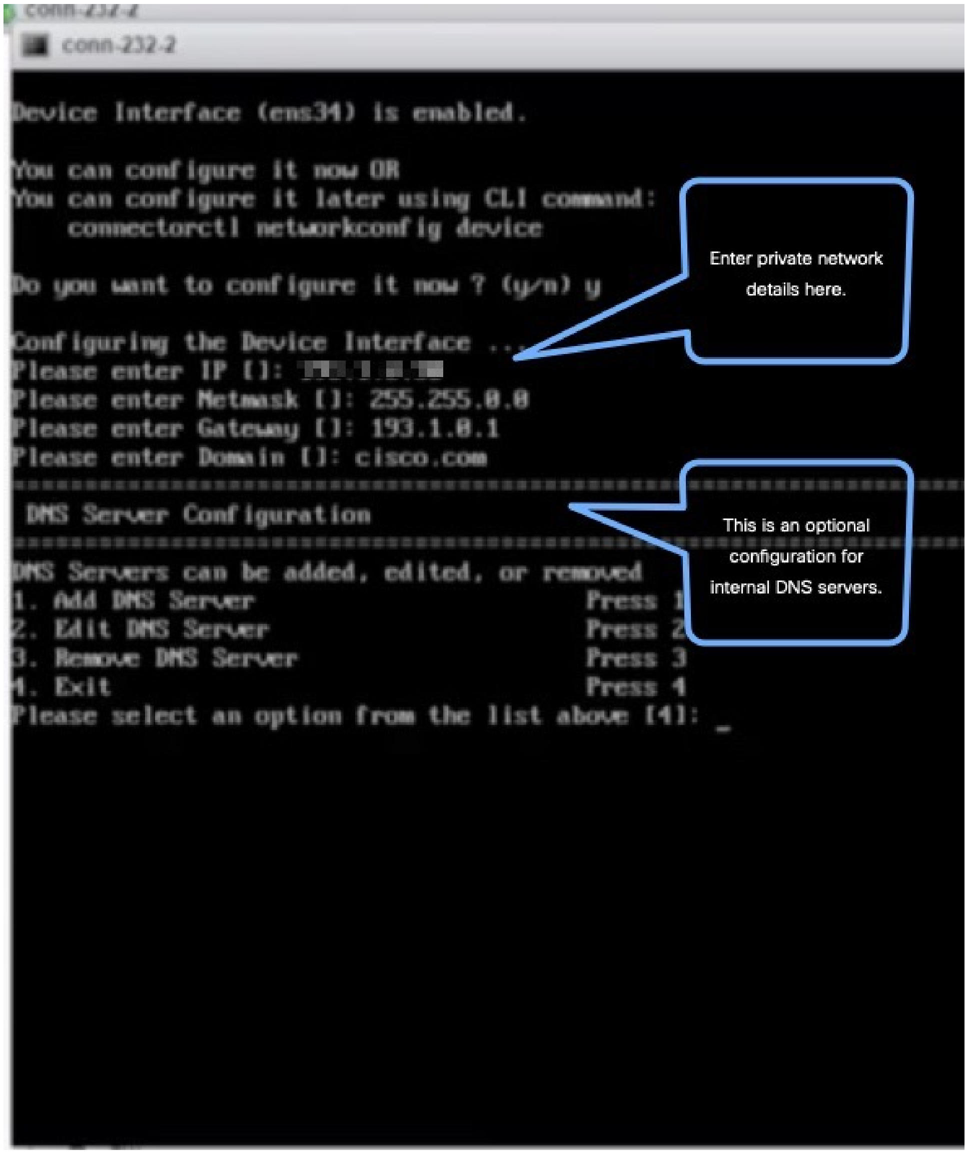


```
Starting network setup
Please enter hostname: connector
Please enter IP address: [redacted]
Please enter netmask: 255.255.255.0
Please enter gateway: [redacted]
Please enter DNS server: [redacted]
Please enter search domain name:
Confirm network settings?  (yes/no) _
```

Note As this configuration screen times out in 60 seconds, ensure you provide the input in time to avoid reconfiguring.

Step 11 Configure the network settings for the private network by specifying the parameters such as IP address, hostname, and so on.

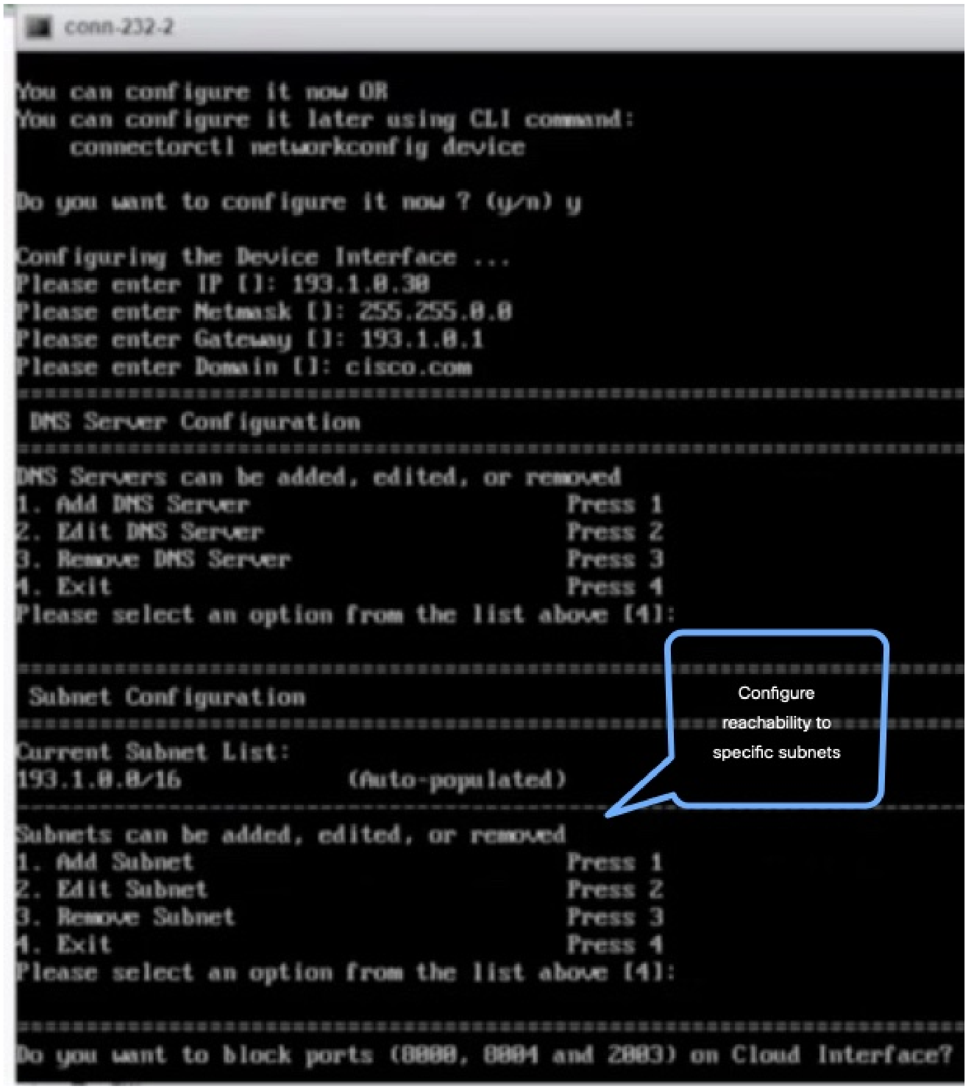
Figure 7: Enter the Network Settings of Private Network



conn-232-2
Enter private network details here.
This is an optional configuration for internal DNS servers.

```
Device Interface (ens34) is enabled.

You can configure it now OR
You can configure it later using CLI command:
    connectorctl networkconfig device

Do you want to configure it now ? (y/n) y

Configuring the Device Interface ...
Please enter IP []: [redacted]
Please enter Netmask []: 255.255.0.0
Please enter Gateway []: 193.1.0.1
Please enter Domain []: cisco.com
=================================================================
 DNS Server Configuration
=================================================================
DNS Servers can be added, edited, or removed
1. Add DNS Server                          Press 1
2. Edit DNS Server                         Press 2
3. Remove DNS Server                       Press 3
4. Exit                                    Press 4
Please select an option from the list above [4]: _
```

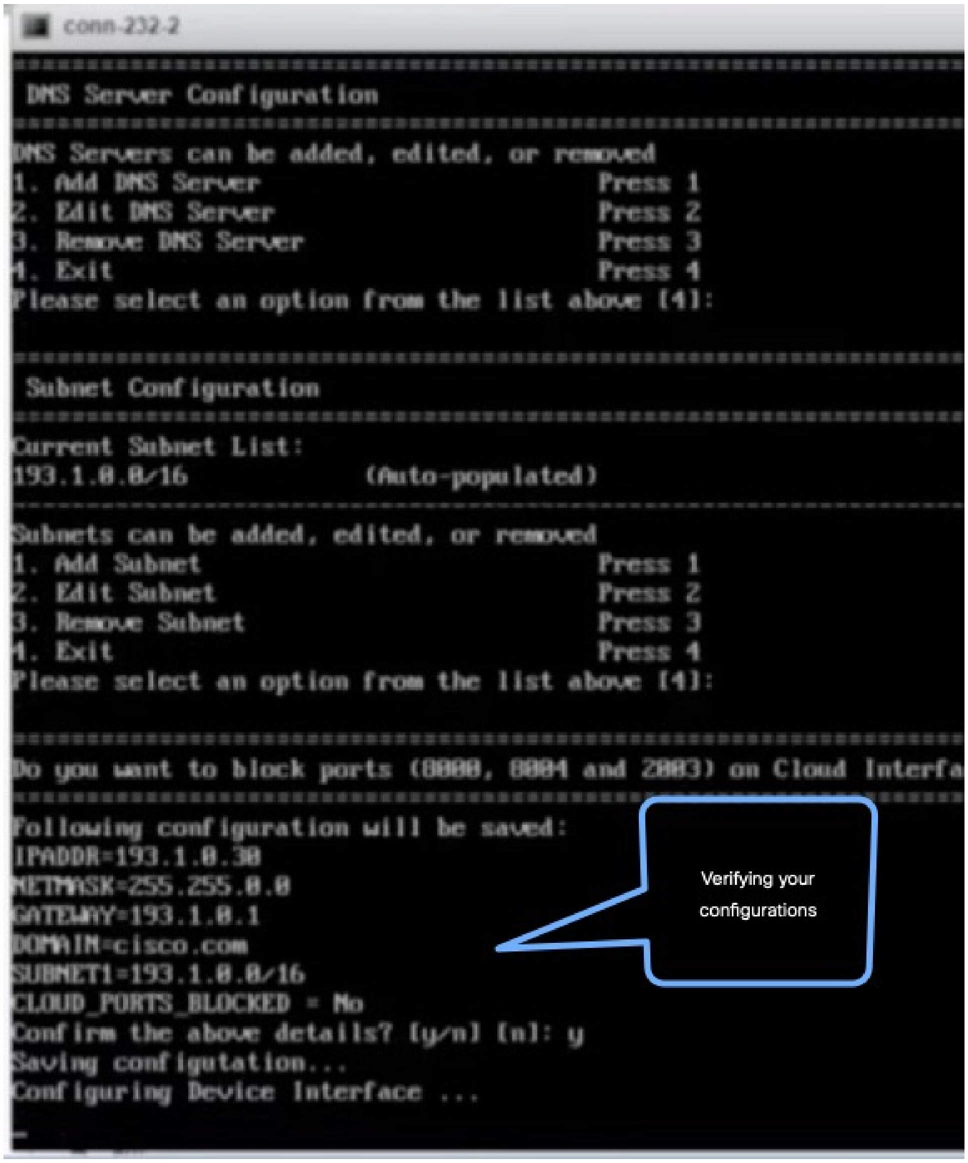
Step 12 Configure subnets that the Connector can reach.



```
You can configure it now OR
You can configure it later using CLI command:
    connectorctl networkconfig device

Do you want to configure it now ? (y/n) y

Configuring the Device Interface ...
Please enter IP []: 193.1.0.30
Please enter Netmask []: 255.255.0.0
Please enter Gateway []: 193.1.0.1
Please enter Domain []: cisco.com
======================================================================
 DNS Server Configuration
======================================================================
DNS Servers can be added, edited, or removed
1. Add DNS Server                        Press 1
2. Edit DNS Server                       Press 2
3. Remove DNS Server                     Press 3
4. Exit                                  Press 4
Please select an option from the list above [4]:

======================================================================
 Subnet Configuration
======================================================================
Current Subnet List:
193.1.0.0/16            (Auto-populated)
----------------------------------------------------------------------
Subnets can be added, edited, or removed
1. Add Subnet                            Press 1
2. Edit Subnet                           Press 2
3. Remove Subnet                         Press 3
4. Exit                                  Press 4
Please select an option from the list above [4]:

======================================================================
Do you want to block ports (8000, 8004 and 2003) on Cloud Interface?
```

Configure reachability to specific subnets

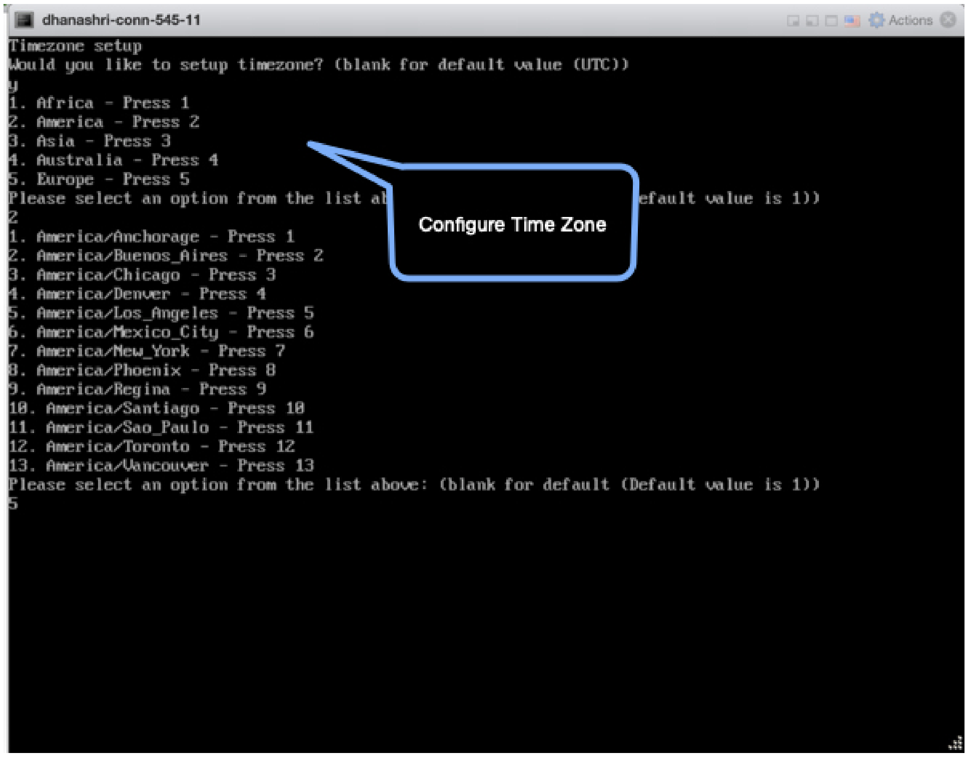
You can observe as the configurations and network reachability are verified.



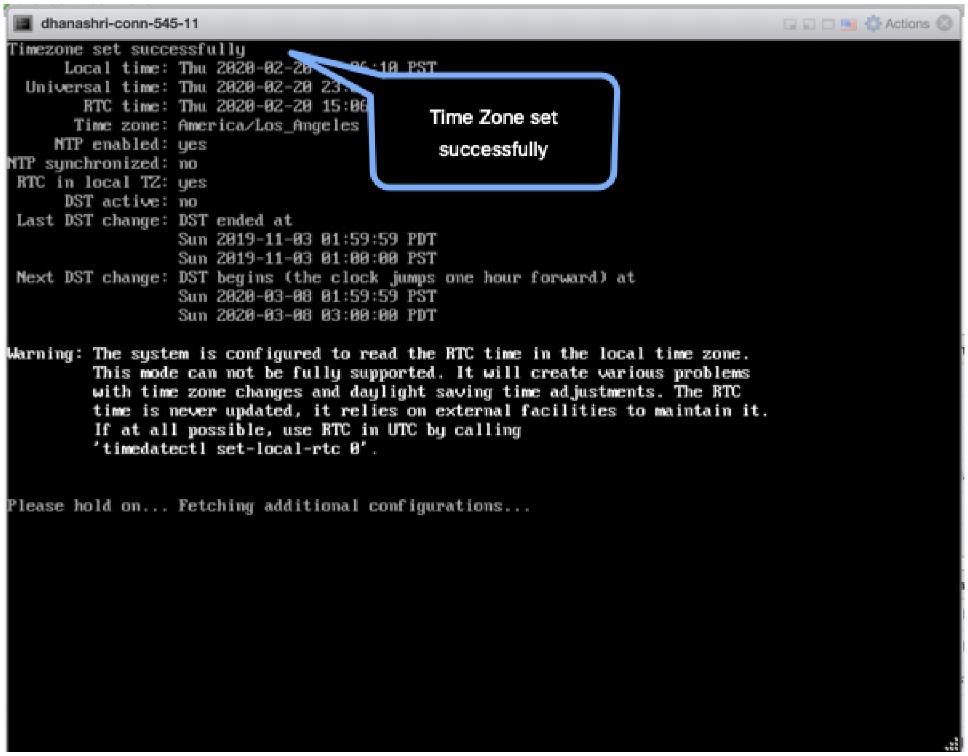
```
================================================================================
 DNS Server Configuration
================================================================================
DNS Servers can be added, edited, or removed
1. Add DNS Server                        Press 1
2. Edit DNS Server                       Press 2
3. Remove DNS Server                     Press 3
4. Exit                                  Press 4
Please select an option from the list above [4]:

================================================================================
 Subnet Configuration
================================================================================
Current Subnet List:
193.1.0.0/16            (Auto-populated)
--------------------------------------------------------------------------------
Subnets can be added, edited, or removed
1. Add Subnet                            Press 1
2. Edit Subnet                           Press 2
3. Remove Subnet                         Press 3
4. Exit                                  Press 4
Please select an option from the list above [4]:

================================================================================
Do you want to block ports (8000, 8004 and 2003) on Cloud Interfa
================================================================================
Following configuration will be saved:
IPADDR=193.1.0.30
NETMASK=255.255.0.0
GATEWAY=193.1.0.1
DOMAIN=cisco.com
SUBNET1=193.1.0.0/16
CLOUD_PORTS_BLOCKED = No
Confirm the above details? [y/n] [n]: y
Saving configutation...
Configuring Device Interface ...
_
```

Verifying your configurations

Step 13 Enter the time zone.



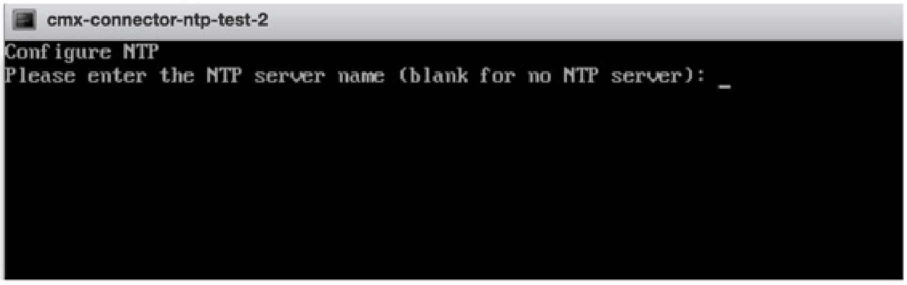
```
Timezone setup
Would you like to setup timezone? (blank for default value (UTC))
y
1. Africa - Press 1
2. America - Press 2
3. Asia - Press 3
4. Australia - Press 4
5. Europe - Press 5
Please select an option from the list al                         efault value is 1))
2
1. America/Anchorage - Press 1
2. America/Buenos_Aires - Press 2
3. America/Chicago - Press 3
4. America/Denver - Press 4
5. America/Los_Angeles - Press 5
6. America/Mexico_City - Press 6
7. America/New_York - Press 7
8. America/Phoenix - Press 8
9. America/Regina - Press 9
10. America/Santiago - Press 10
11. America/Sao_Paulo - Press 11
12. America/Toronto - Press 12
13. America/Vancouver - Press 13
Please select an option from the list above: (blank for default (Default value is 1))
5
```



```
Timezone set successfully
      Local time: Thu 2020-02-20     06:10 PST
  Universal time: Thu 2020-02-20 23:
        RTC time: Thu 2020-02-20 15:06
       Time zone: America/Los_Angeles
     NTP enabled: yes
NTP synchronized: no
 RTC in local TZ: yes
      DST active: no
 Last DST change: DST ended at
                  Sun 2019-11-03 01:59:59 PDT
                  Sun 2019-11-03 01:00:00 PST
 Next DST change: DST begins (the clock jumps one hour forward) at
                  Sun 2020-03-08 01:59:59 PST
                  Sun 2020-03-08 03:00:00 PDT

Warning: The system is configured to read the RTC time in the local time zone.
         This mode can not be fully supported. It will create various problems
         with time zone changes and daylight saving time adjustments. The RTC
         time is never updated, it relies on external facilities to maintain it.
         If at all possible, use RTC in UTC by calling
         'timedatectl set-local-rtc 0'.


Please hold on... Fetching additional configurations...
```

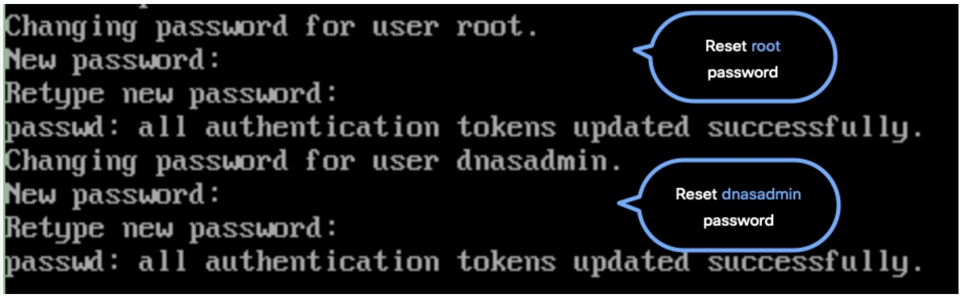
Step 14 Enter the Network Time Protocol (NTP) server name to synchronize the system time with the NTP server's or leave it blank if you do not want to configure an NTP server.

Figure 8: Enter NTP Setting



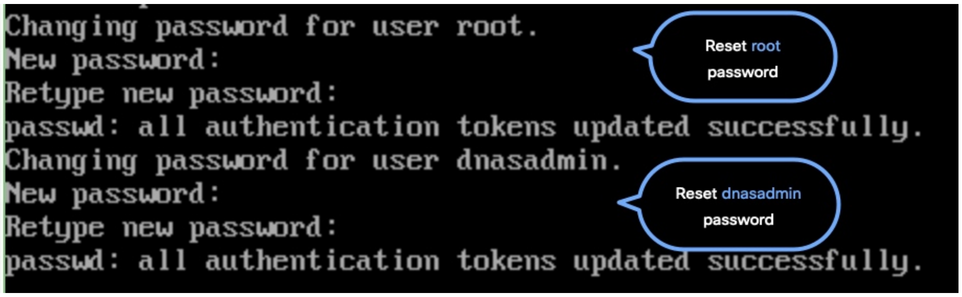
```
cmx-connector-ntp-test-2
Configure NTP
Please enter the NTP server name (blank for no NTP server): _
```

Step 15 Set a new password for the **root** user.



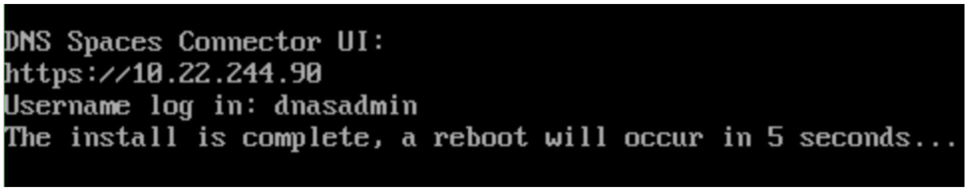
```
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Changing password for user dnasadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Step 16 Set a new password for the **dnasadmin** user, which is user with administrative privileges.



```
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Changing password for user dnasadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

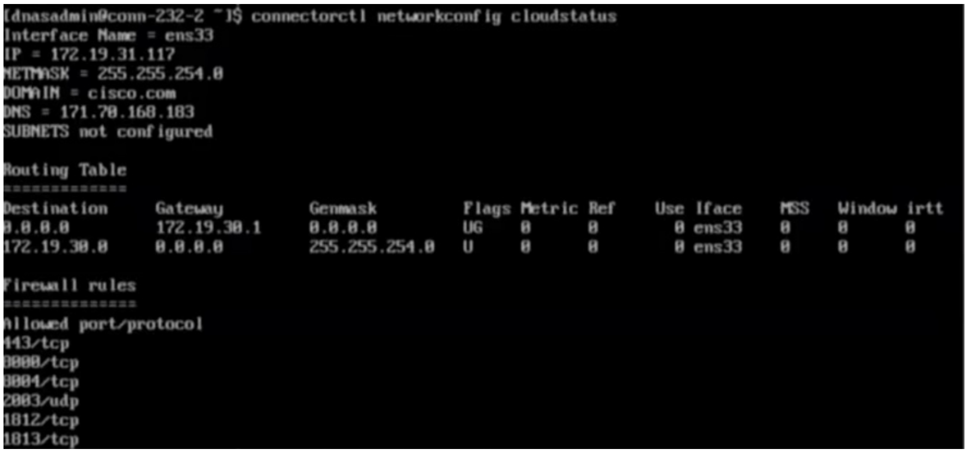
Step 17 Copy and save the URL before the automatic reboot. You can use this URL later to open the Cisco Spaces: Connector GUI.



```
DNS Spaces Connector UI:
https://10.22.244.90
Username log in: dnasadmin
The install is complete, a reboot will occur in 5 seconds...
```

Step 18 Verify the network Settings of external-facing network using the **connectorctl networkconfig cloudstatus** command.

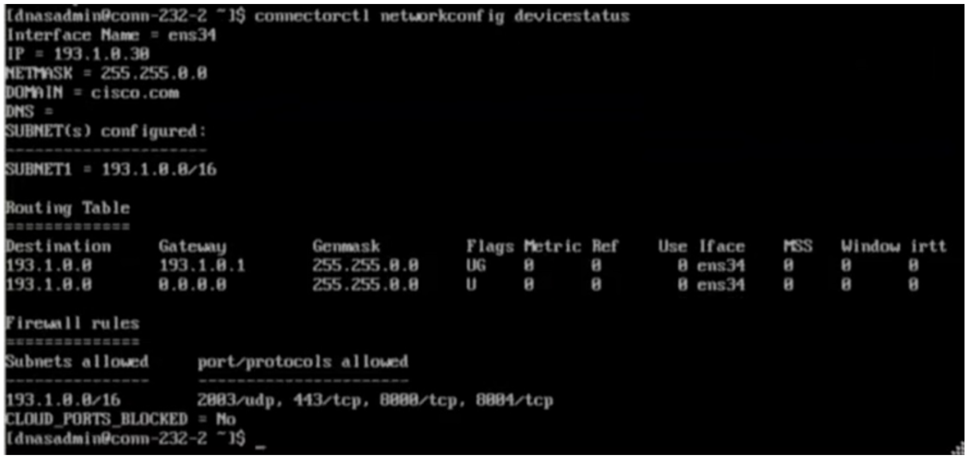
Figure 9: Enter the Network Settings of Private Network



```
[dnasadmin@conn-232-2 ~]$ connectorctl networkconfig cloudstatus
Interface Name = ens33
IP = 172.19.31.117
NETMASK = 255.255.254.0
DOMAIN = cisco.com
DNS = 171.70.168.183
SUBNETS not configured

Routing Table
=============
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface    MSS   Window irtt
0.0.0.0         172.19.30.1     0.0.0.0         UG    0      0        0 ens33    0     0      0
172.19.30.0     0.0.0.0         255.255.254.0   U     0      0        0 ens33    0     0      0

Firewall rules
==============
Allowed port/protocol
443/tcp
8000/tcp
8004/tcp
2003/udp
1812/tcp
1813/tcp
```

Step 19 Verify the network settings of private network using the **connectorctl networkconfig devicestatus** command.

Figure 10: Enter the Network Settings of Private Network



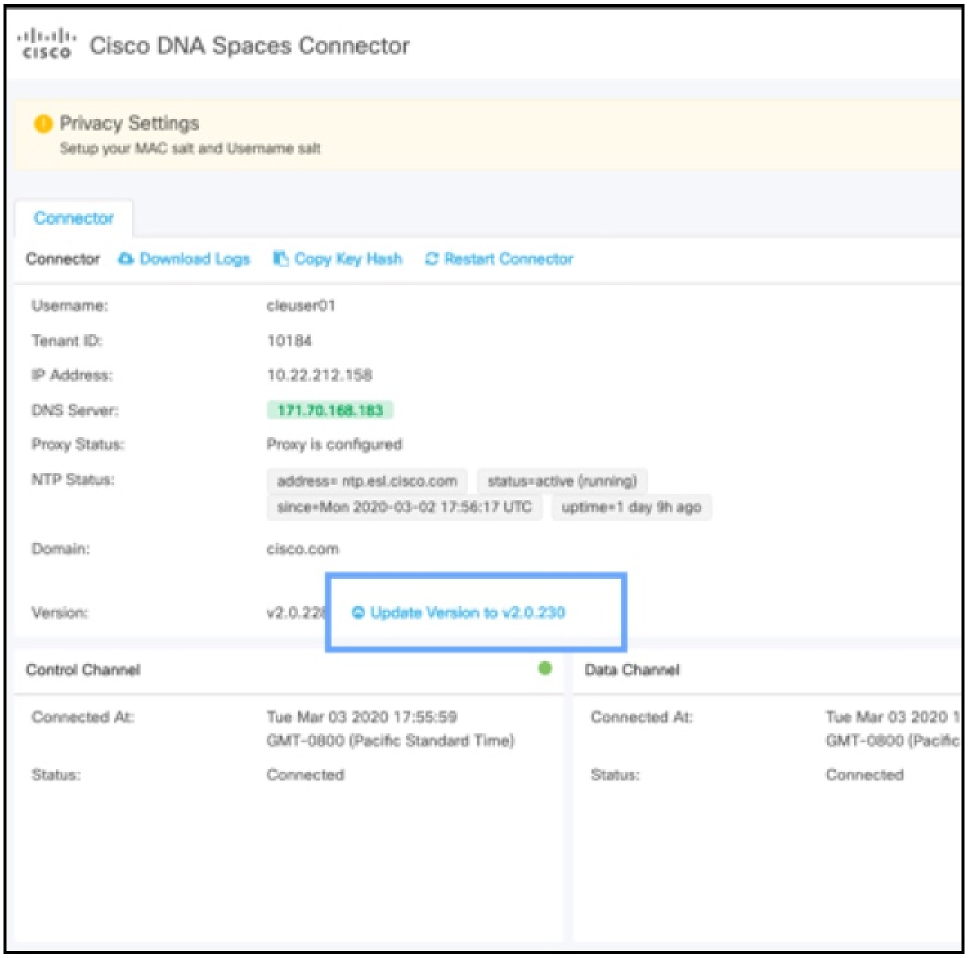
```
[dnasadmin@conn-232-2 ~]$ connectorctl networkconfig devicestatus
Interface Name = ens34
IP = 193.1.0.30
NETMASK = 255.255.0.0
DOMAIN = cisco.com
DNS =
SUBNET(s) configured:
----------------------
SUBNET1 = 193.1.0.0/16

Routing Table
=============
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface    MSS   Window irtt
193.1.0.0       193.1.0.1       255.255.0.0     UG    0      0        0 ens34    0     0      0
193.1.0.0       0.0.0.0         255.255.0.0     U     0      0        0 ens34    0     0      0

Firewall rules
==============
Subnets allowed     port/protocols allowed
---------------     ----------------------
193.1.0.0/16        2003/udp, 443/tcp, 8000/tcp, 8004/tcp
CLOUD_PORTS_BLOCKED = No
[dnasadmin@conn-232-2 ~]$ _
```

Upgrade the Cisco Spaces: Connector Docker

You can upgrade the Connector docker to the latest version from the Connector GUI. Note that the upgrade link appears only if a new upgrade image is available.

Note This procedure does not upgrade the Connector OVA.

Figure 11: Docker Upgrade Link on the Connector



Cisco DNA Spaces Connector

Privacy Settings
Setup your MAC salt and Username salt

Username:	cleuser01
Tenant ID:	10184
IP Address:	10.22.212.158
DNS Server:	171.70.168.183
Proxy Status:	Proxy is configured

NTP Status:	address= ntp.esl.cisco.com
	status=active (running)
	since=Mon 2020-03-02 17:56:17 UTC
	uptime=1 day 9h ago

Domain:	cisco.com
Version:	v2.0.228 Update Version to v2.0.230

Control Channel

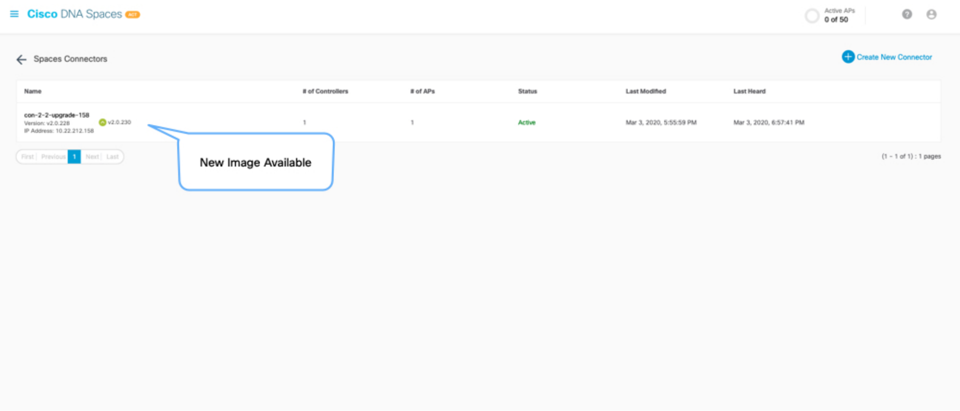
Connected At:	Tue Mar 03 2020 17:55:59 GMT-0800 (Pacific Standard Time)
Status:	Connected

Data Channel

Connected At:	Tue Mar 03 2020 1 GMT-0800 (Pacific
Status:	Connected

You can also upgrade the Connector docker to the latest version from the Cisco Spaces dashboard. The upgrade link appears only if a new upgrade image is available.

Figure 12: Docker Upgrade Link Appears Only if New Image is Available



Name	# of Controllers	# of APs	Status	Last Modified	Last Heard
con-2-2-upgrade-158 Version: v2.0.228 IP Address: 10.22.212.158 v2.0.230	1	1	Active	Mar 3, 2020, 5:55:59 PM	Mar 3, 2020, 6:57:41 PM

Upgrade Path

The following table is best viewed in the HTML format. Here is a description of the contents of the table.

- **Release Number**: Lists the identifying number of the release.
- **Platforms**: Lists the platforms (OVA, VHDX, AMI) on which this release can be installed or the corresponding installation file name.
- **Upgrade to This Release**: Lists the releases to which you can upgrade the release mentioned in the **Release Number** column.
- **Upgrade File**: Lists the *.connector* upgrade files you can use to upgrade to the release mentioned in the **Upgrade to This Release** column.

Table 1: Upgrade Path for Active Releases

Release Number	Platforms	Upgrade to This Release	Upgrade File
2.3.4	cisco-dna-spaces-connector-2.3.507.ova	N.A	N.A
	cisco-dna-spaces-connector-2.3.507.vhdx		
2.3.3	cisco-dna-spaces-connector-2.3.497.ova	2.3.4	cisco-dna-spaces-connector-2.3.507.connector
2.3.2	cisco-dna-spaces-connector-2.3.495.ova	2.3.3	cisco-dna-spaces-connector-2.3.497.connector
	cisco-dna-spaces-connector-2.3.496.vhdx		
2.3.1	cisco-dna-spaces-connector-2.3.478.ova	2.3.2	cisco-dna-spaces-connector-2.3.495.connector
	cisco-dna-spaces-connector-2.3.478.vhdx		
2.3	cisco-dna-spaces-connector-2.3.462.ova	2.3.1	cisco-dna-spaces-connector-2.3.478.connector
2.2	cisco-dna-spaces-connector-2.2.295.ova	2.3	cisco-dna-spaces-connector-2.3.462.connector

Note All release versions prior to 2.2 are deferred. We recommend that you deploy the latest OVA to get all the latest updates.

Table 2: Upgrade Path for AMI Releases

Release Number	Platforms	Upgrade to This Release	Upgrade File
2.3.4	AMI	N.A	N.A
2.3.3	AMI	2.3.4	cisco-dna-spaces-connector-ami-2.3.507.connector

Upgrading the Connector OVA

The following procedure shows you how to upgrade the Cisco Spaces: Connector OVA.

Step 1 Download Connector 2.3 from Cisco.com.

Step 2 Copy the downloaded file on to the machine hosting the Connector.

Step 3 Log in to the Connector command line.

Step 4 Use the **connectorctl upgrade** <<*upgrade_file_name*>> command to start the OVA upgrade process.

```
(cmxadminPcon-2-3-upg-87 -]S connectorctl upgrade cisco-dna-spaces-connector-2.3.494.connector
Machine will restart automatically after upgrade. Do you still want to continue? [yes / noj [yesj:
yes
Before upgrade, OVA version:2.2.295
New image exists.
Backing up current version of the image and db ...
Preparing for upgrade ...
umount: /mnt/cmx: not mounted
mount: /dev/loop0 is write-protected, mounting read-only
Starting pip repo
Starting upgrade ...
Warning: RPMDB altered outside of yum.
Error: No matching Packages to list
000000000000000000000000000000 IMPORTANT 000000*00000000000000000000*0000a«000
We are changing username from 'cmxadmin' to 'dnasadmin*
We will be performing following tasks now.
1. Create new user 'dnasadmin'
2. You will need to set up password for 'dnasadmin'
3. We will move over all files/folders from /home/cmxadmin to /ho®e/dnasadmin
4. Delete 'cmxadnin* user.

After the reboot, REMEMBER to login using dnasadmin credentials.
0000000000000000000000000000000000000000000000000000000000000000000000000000800


Please press ENTER to continue...
```

The **dnasadmin** user is now created.

Step 5 Set a password for the newly created **dnasadmin** user when prompted.

```
Please press ENTER to continue...
New user dnasadmin created.
Set password for user dnasadmin
Changing password for user dnasadmin.
New password:

Retype new password:

passwd: all authentication tokens updated successfully.
Start cleanup ...
Error response from daemon: No such container:
c9408eelb68f2acdel436622c4eeddf742dcd53a2619faa30c01aadcld8bd88e
```

Step 6 Wait a few seconds for the upgrade to complete.

```
Error response from daemon: No such container: c9408ee1b68f2acde1436622c4eeddf742dcd53a2

Upgrade successful.
After upgrade, OVA version : 2.3.494

System will reboot in 5 seconds...
```

Step 7 Once the upgrade is completed, log in to the connector as the **dnasadmin** user.

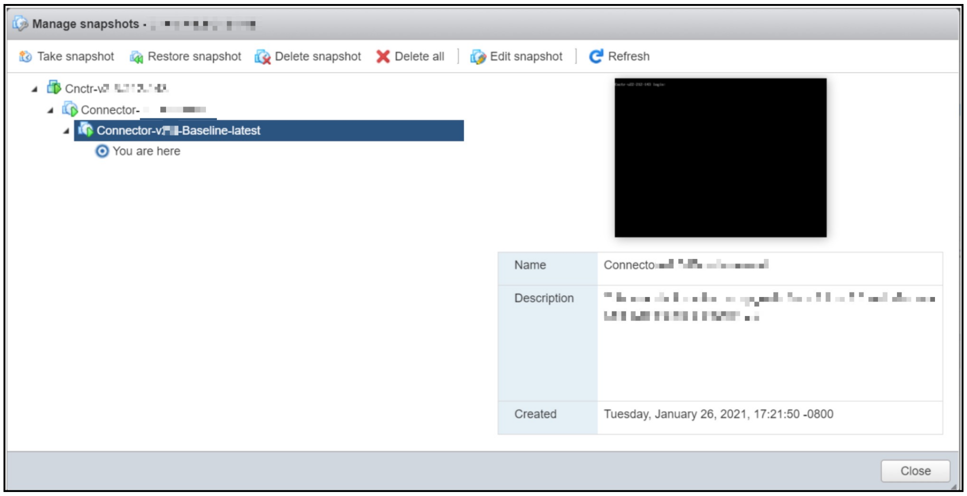
- Verify if the Connector is running in the same state as it was running before the upgrade.
- With CSCvr74830, you can ignore the two known errors that are displayed during upgrade.

Using Snapshots for Backup

You can use the snapshot of a deployed Connector OVA for backing up your Connector. Ensure that the following prerequisites in place:

- Connector is deployed.
- All the services are started.
- Connector is added to Cisco Spaces.

Figure 13: Backing Up Using a Snapshot



Name: Connecto[redacted]

Description: [redacted]

Created: Tuesday, January 26, 2021, 17:21:50 -0800

Note Proxies are not carried over during a snapshot restore. You have to reconfigure proxies.