CSPC Collection Platform Software Installation and Configuration Guide

March 2024

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

CONTENTS

CHAPTER 1 **Introduction** 1-1

Introduction to CSPC Collection Platform Software 1-1

Who Should Use This Guide 1-1

Ordering Process 1-1

CHAPTER 2 **Installation and Configuration** 2-1

OVA Installation 2-1

Pre-requisites 2-1

Deploy CSPC OVA 2-1

Configure IPv4 address 2-8

Configure IPv6 Address 2-9

Configure the IP address directly on shell 2-10

Enable Default Account2-10

Set GRUB Password 2-11

TACACS Authentication 2-12

ESXi 7.0 Patch Installation 2-12

CSPC NAT OVA Installation 2-13

Prerequisites 2-13

CIMC Patch Installation 2-19

NOS Configurer 2-20

Installation Sequence For nos_configurer 2-20

Prime Infrastructure 2-21

Introduction

Introduction to CSPC Collection Platform Software

The Cisco Common Service Platform Collector (CSPC) is an SNMP-based tool that discovers and collects information from the Cisco devices installed on your network. The CSPC software provides an extensive collection mechanism to gather various aspects of customer device data. Information gathered by the collector is used by several Cisco Service offers, such as Smart Net Total Care, Partner Support Service, and Business Critical Services. The data is used to provide inventory reports, product alerts, configuration best practices, technical service coverage, lifecycle information, and many other detailed reports and analytics for both the hardware and operating system (OS) software.

This guide explains how to use install and configure CSPC Server. Refer to CSPC User Guide to use the application.

For program updates and important notes, refer to CSPC Release Notes and README documentation.

Who Should Use This Guide

This guide is written for Network and Security Administrators and Cisco Network Engineers and also for new users.

The user should have Administrative privileges on the machine to install CSPC.

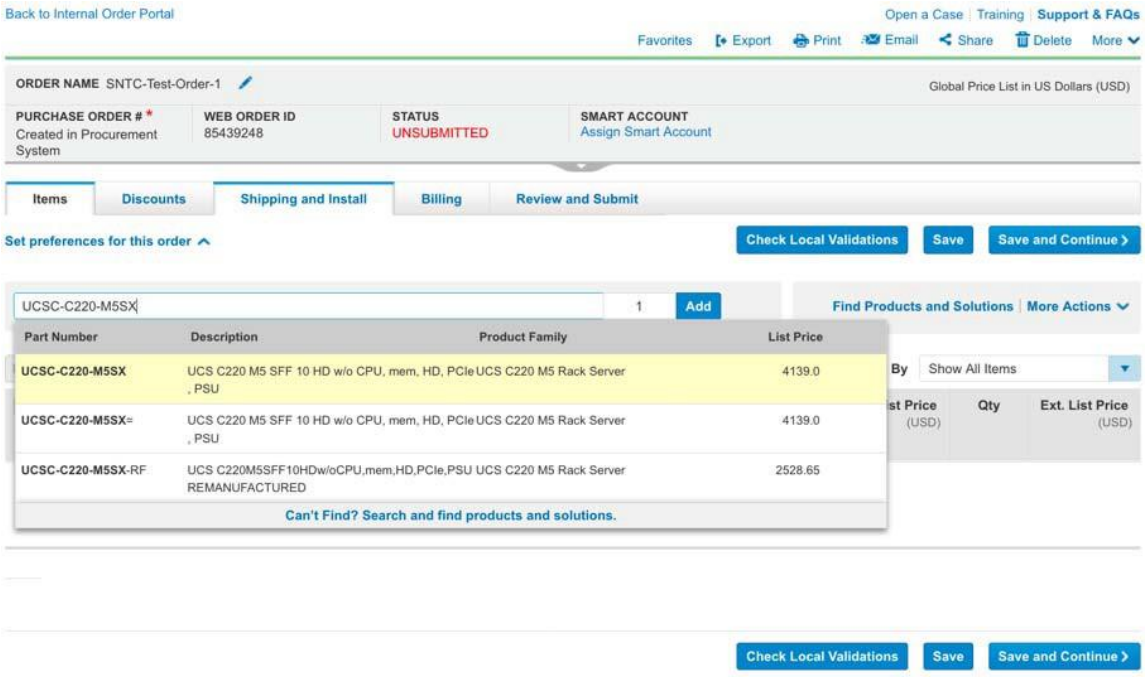
Ordering Process

To order a M5 hardware you need to do the following:

Step 1 Navigate to Cisco Commerce Website CCW and to learn how to using CCW navigate to Cisco_Commerce_User_Guide.pdf

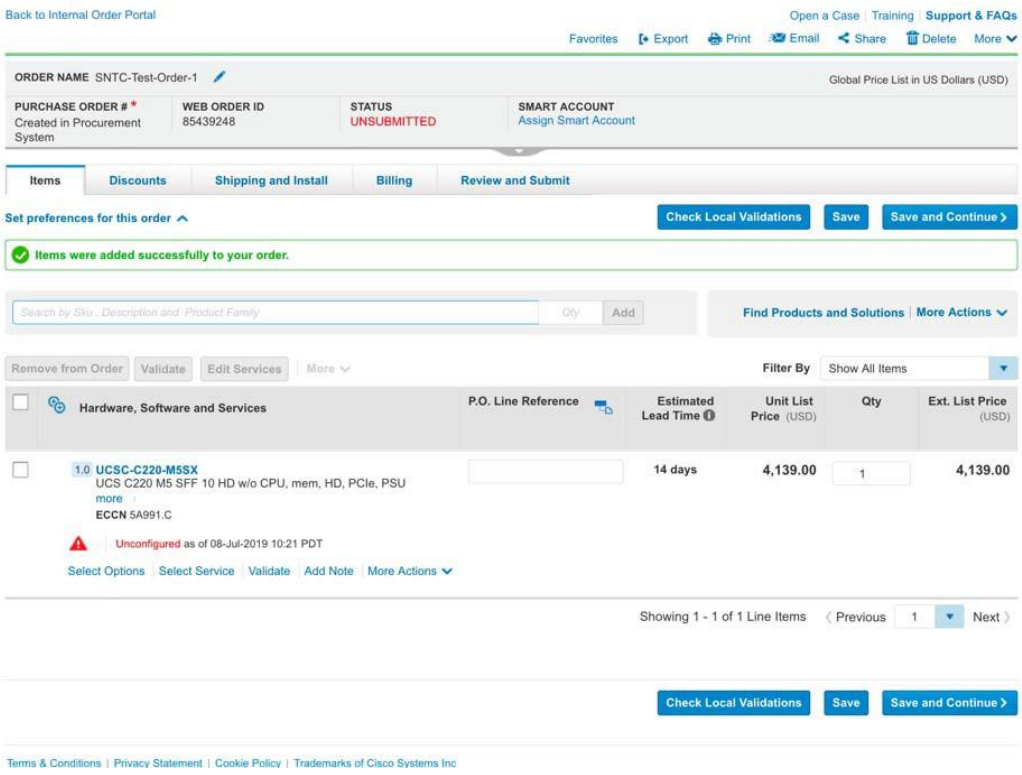
Step 2 Enter the chassis part number **UCSC-C220-M5SX** to search as shown below and select the exact part number from the list and then click **Add**

Figure 1-1 Search



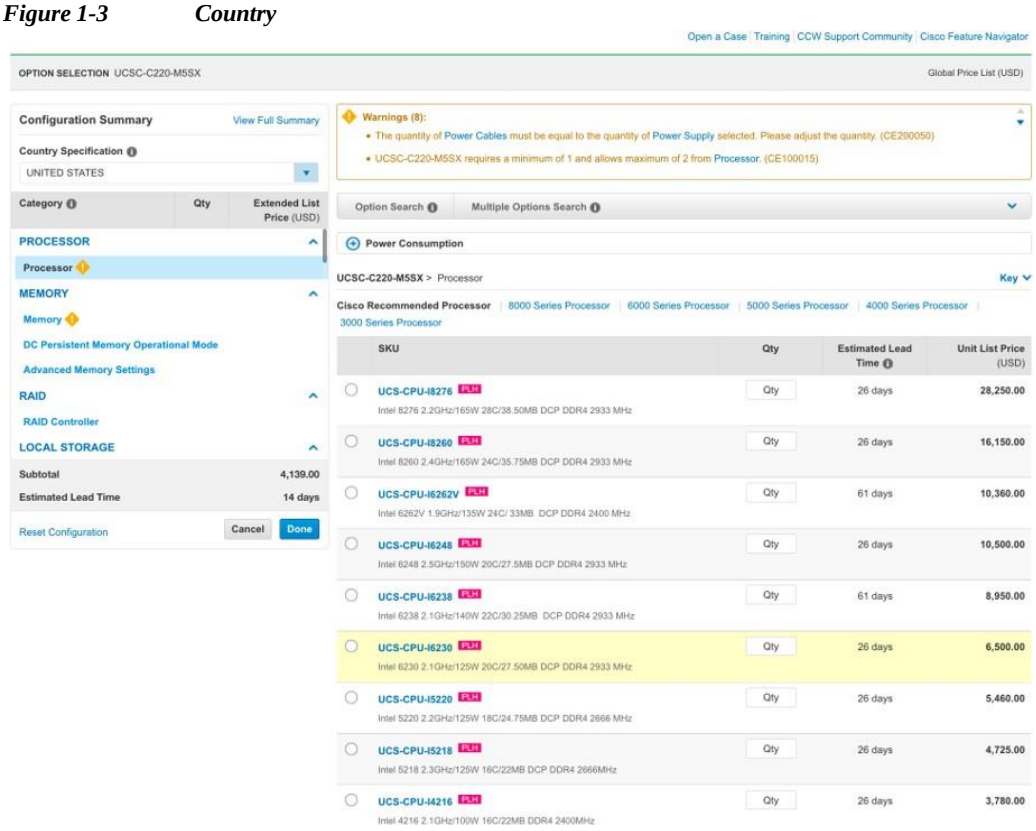
Step 3 Click **Select Options** link at the bottom of the page to select all the hardware components for the selected UCSC-C220M5SX chassis

Figure 1-2 Options



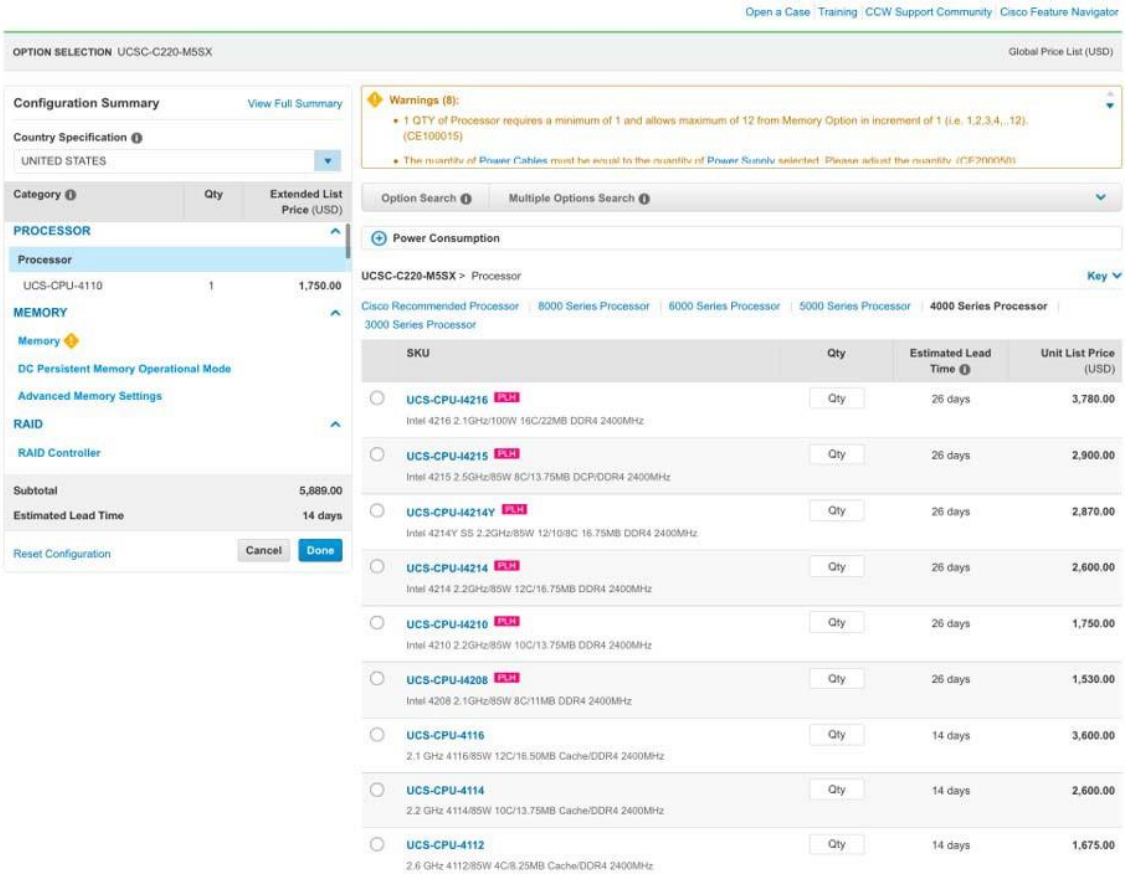
Step 4 After the **Select Options** link is selected, the following screen will be displayed. On LNP, select the **Country** where this M5 hardware will be installed. Although this is optional, it is recommended to select the correct country so that proper cabling that apply to the selected country will be applied

Figure 1-3 Country



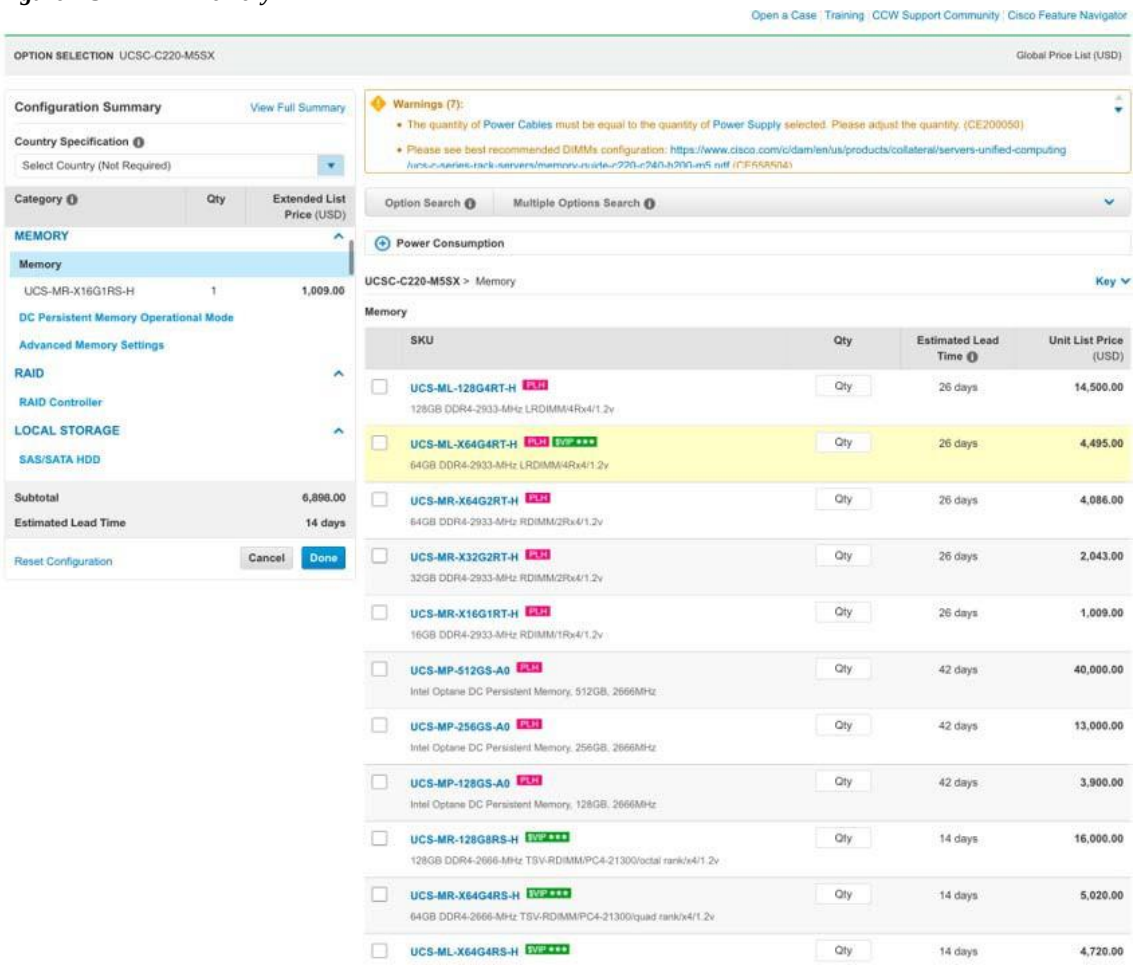
Step 5 On LNP click **Processor**, then from right side select the **UCS-CPU-4110** processor from the processor list as show below

Figure 1-4 Processor



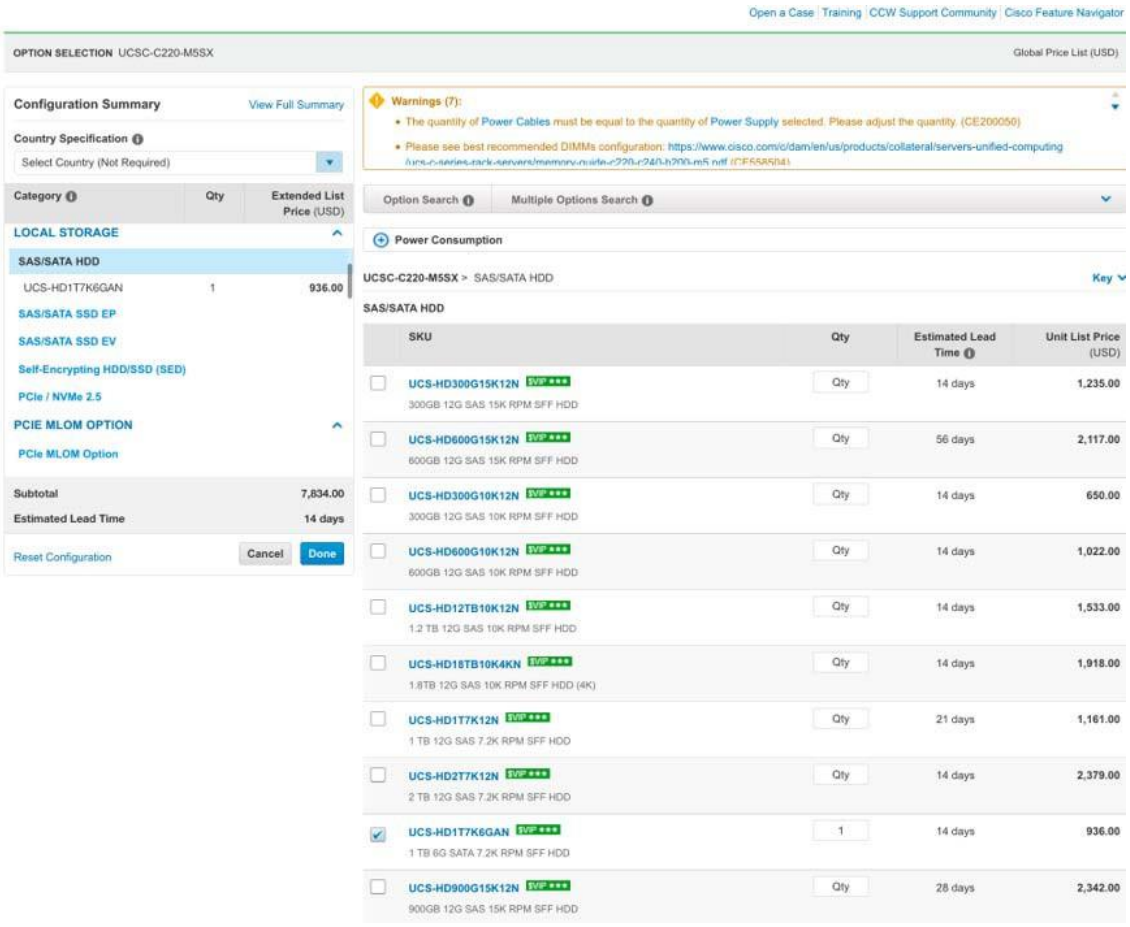
Step 6 ON LNP click the **Memory**, then from the right side select the **UCS-MR-X16G1RS-H** from the memory list as shown below

Figure 1-5 Memory



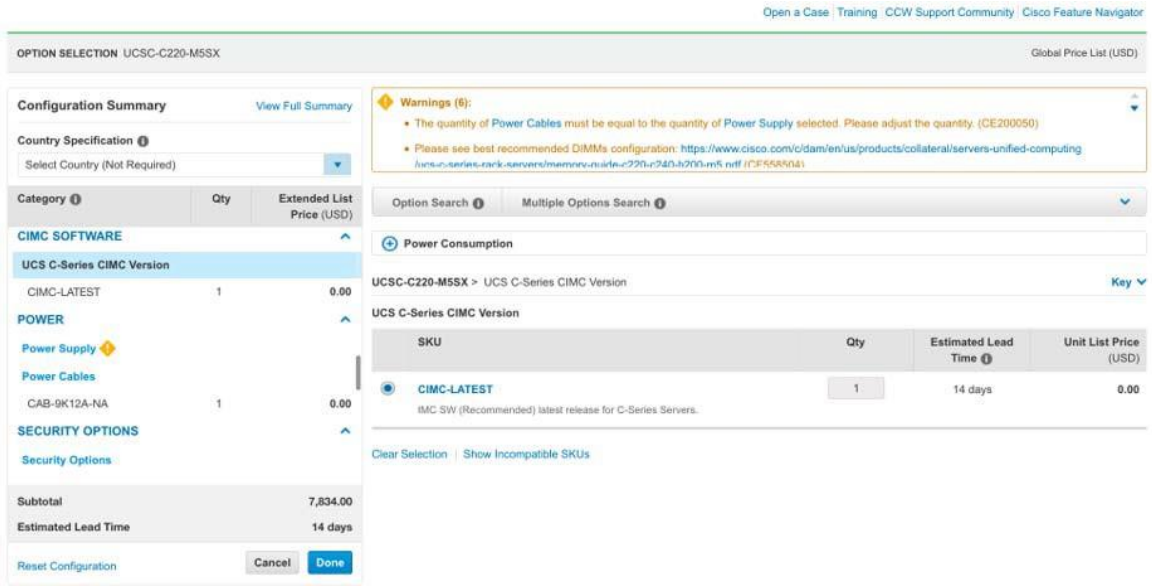
Step 7 On LNP click the **SAS/SATA HDD**, then from the right side select the **UCS-HD1T7K6GAN** from the SATA HDD list shown below

Figure 1-6 SAS/SATA HDD



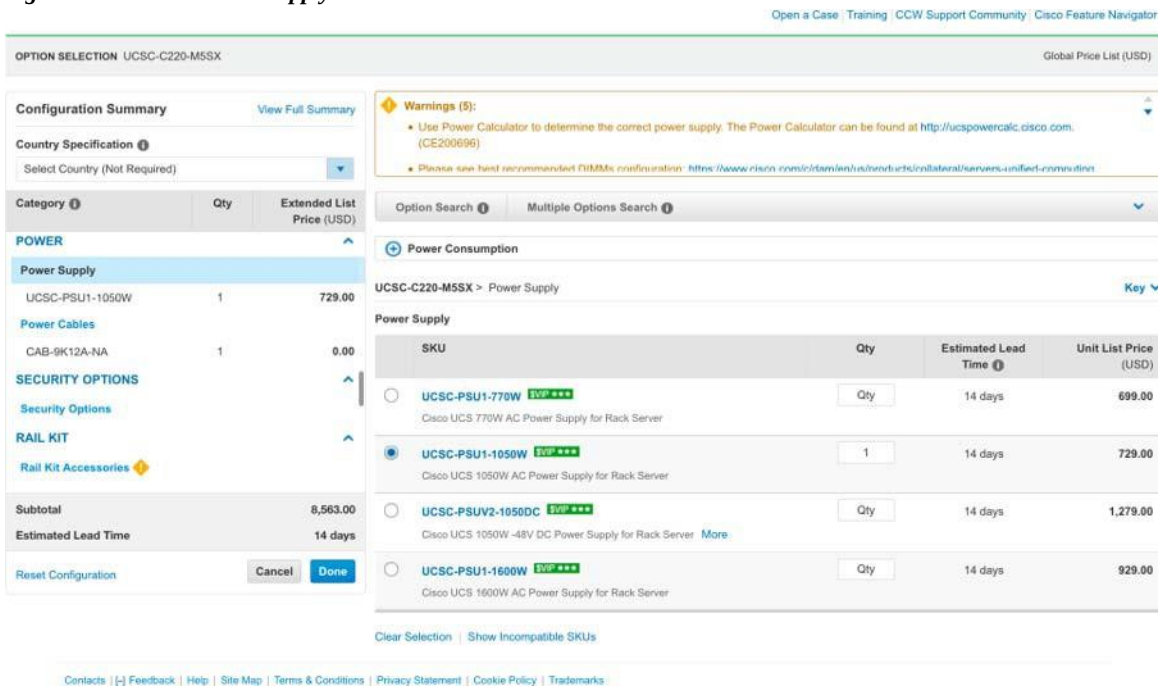
Step 8 On LNP click **UCS C-Series CIMC Version**, then from the right side select the **CIMC-Latest** from the CIMC version list as shown below

Figure 1-7 UCS C-Series CIMC



Step 9 On LNP click **Power Supply**, then from the right side select **UCSC-PSU1-1050W** as shown below

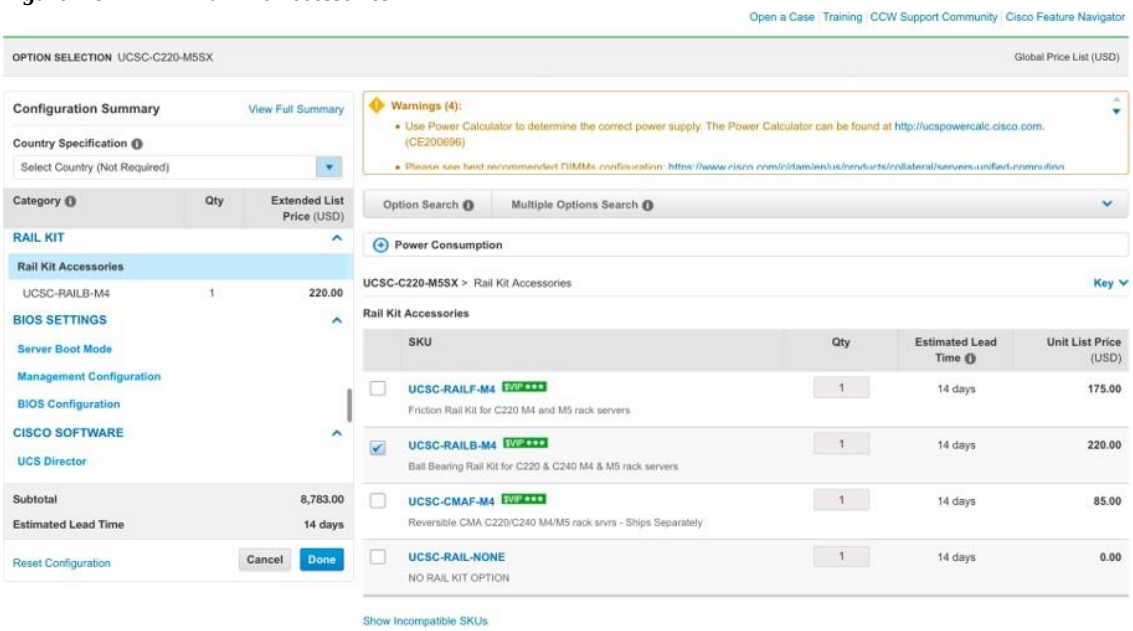
Figure 1-8 Power Supply



Note Once the power supply type is selected, the system automatically adds the correct power cable and in this example the product part number for the corresponding cable is CAB-9K12A-NA.

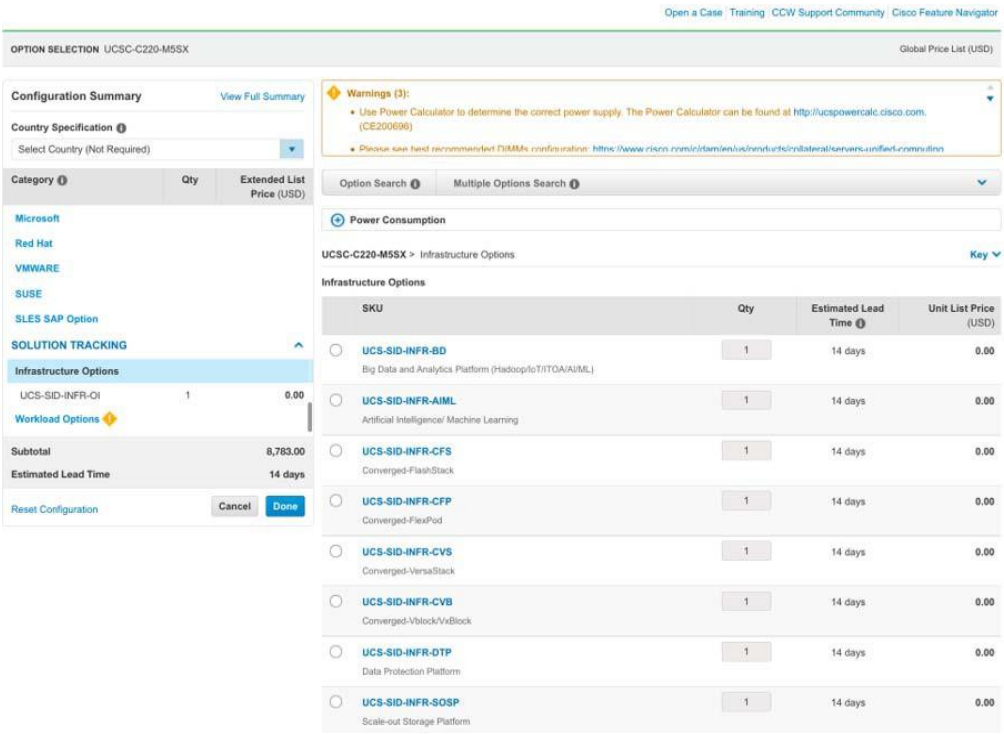
Step 10 On LNP click the **Rail Kit Accessories**, then from the right side select **UCSC-RAILB-M4** from the Rail Kit Accessories list as shown below

Figure 1-9 Rail Kit Accessories



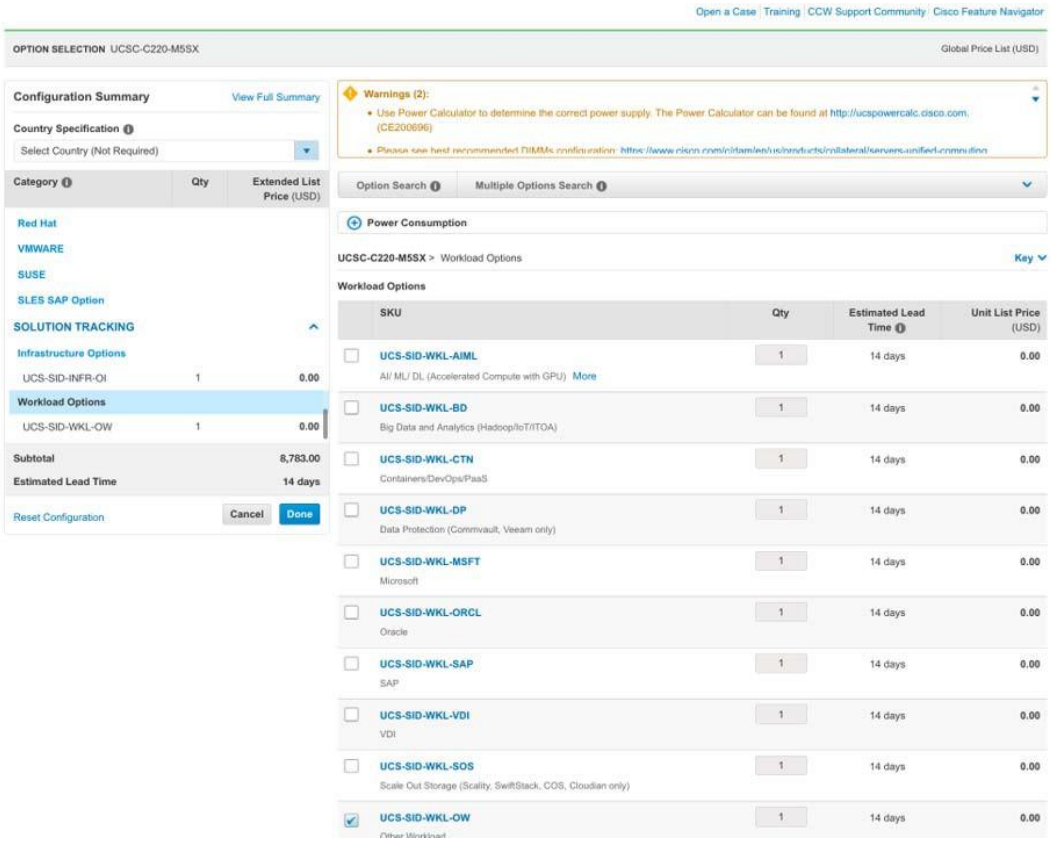
Step 11 On LNP click **Infrastructure Options**, then from the right side select **UCS-SID-INFR-OI** from the Infrastructure Options list as shown below

Figure 1-10 Infrastructure Options



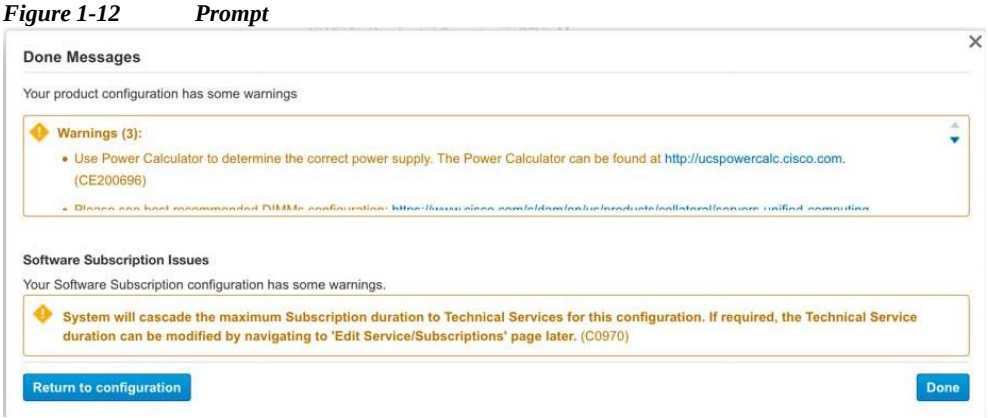
Step 12 On LNP click **Workload Options**, then from the right side select **UCS-SID-WKL-OW** from the Workload Options list as shown below

Figure 1-11 Workload Option



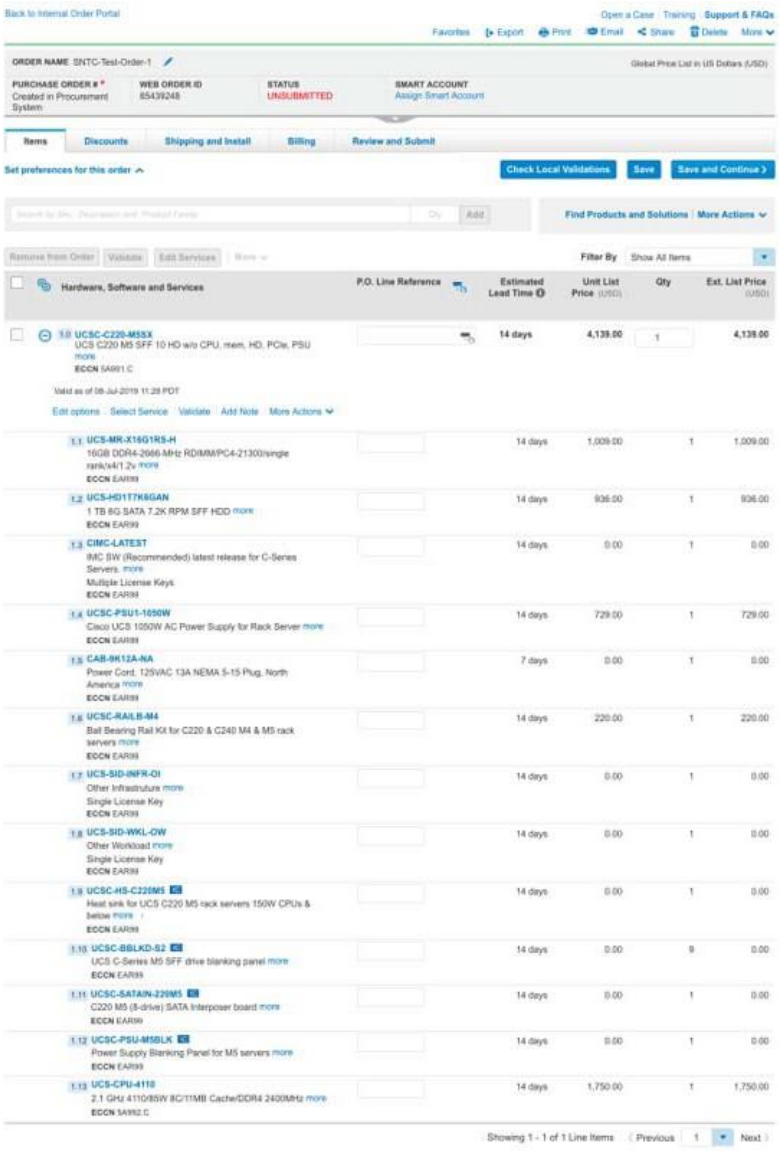
Step 13 A prompt appears, click **Done**

Figure 1-12 Prompt



In the main screen, if you expand the + sign for the USCS-C220-M5SX chassis the entire components will be expanded, and you will see the following configurations for your M5.

Figure 1-13 M5 Configuration



Note These remaining items will be automatically added based on the configuration:
UCS-HS-C220M5
UCSC-BBLKD-S2
UCSC-SATAIN-220M5
UCSC-PSU-M5BLK

Installation and Configuration

CSPC Server image comes with a preloaded application that consists of server software, database, and all the necessary tools.

Important Note: Before you begin

On Installation: If 2.11 installation shows direct login prompt instead of asking for setting admin password then reboot the server once.

Post reboot, it will land on the setting admin password prompt.

OVA Installation

This section describes detailed installation procedures for different installation stages.

Prerequisites

- *xxx.ova* file form the download center
- CSPC static IP address, default gateway IP address and subnet mask. This is recommended only if DHCP is not enabled

Deploy CSPC OVA

This section describes the steps to deploy CSPC OVA using VMWare vSphere Client:

Step 1 Get the xxx.ova file either to a web server or local file system where vSphere client is available

Step 2 Launch vSphere client and login using credentials with the privilege to deploy an OVA file

Step 3 Use vSphere client and select the ESXi host or IP address that manages CSPC virtual machine

Step 5 There are two ways to select the OVF file to deploy:

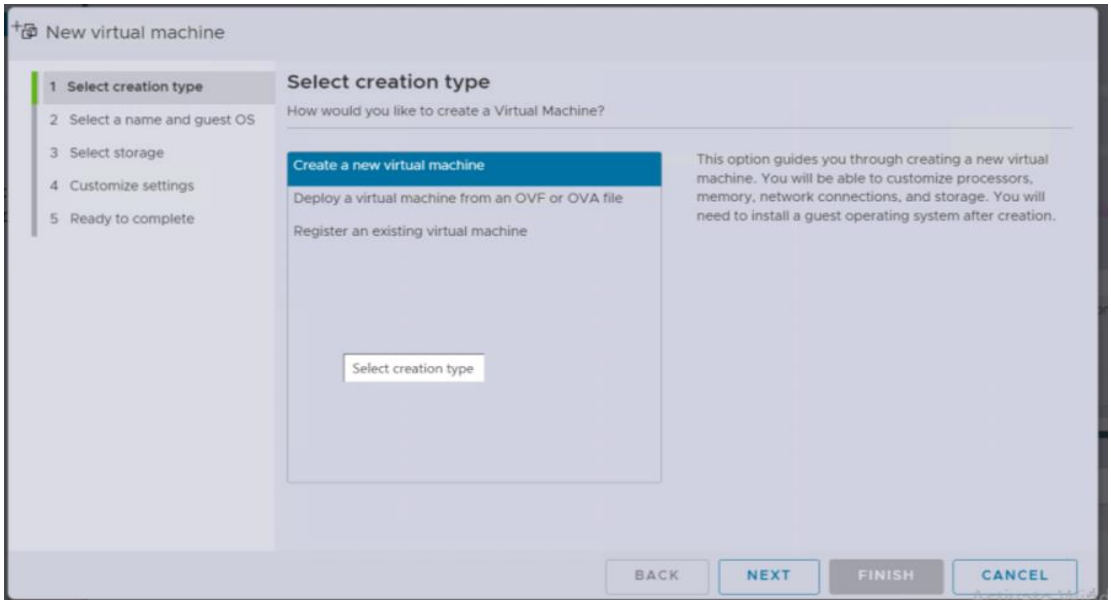
- Select the OVF file residing on local or a remote web server using web browser. If this option is

selected, type the URL for the file *xxx.ova*, then click **Next**

- Select the OVF file residing locally using the file explorer. If this option is selected, click **Browse…**and navigate the file explorer to locate the file *xxx.ova*, then click **Next**

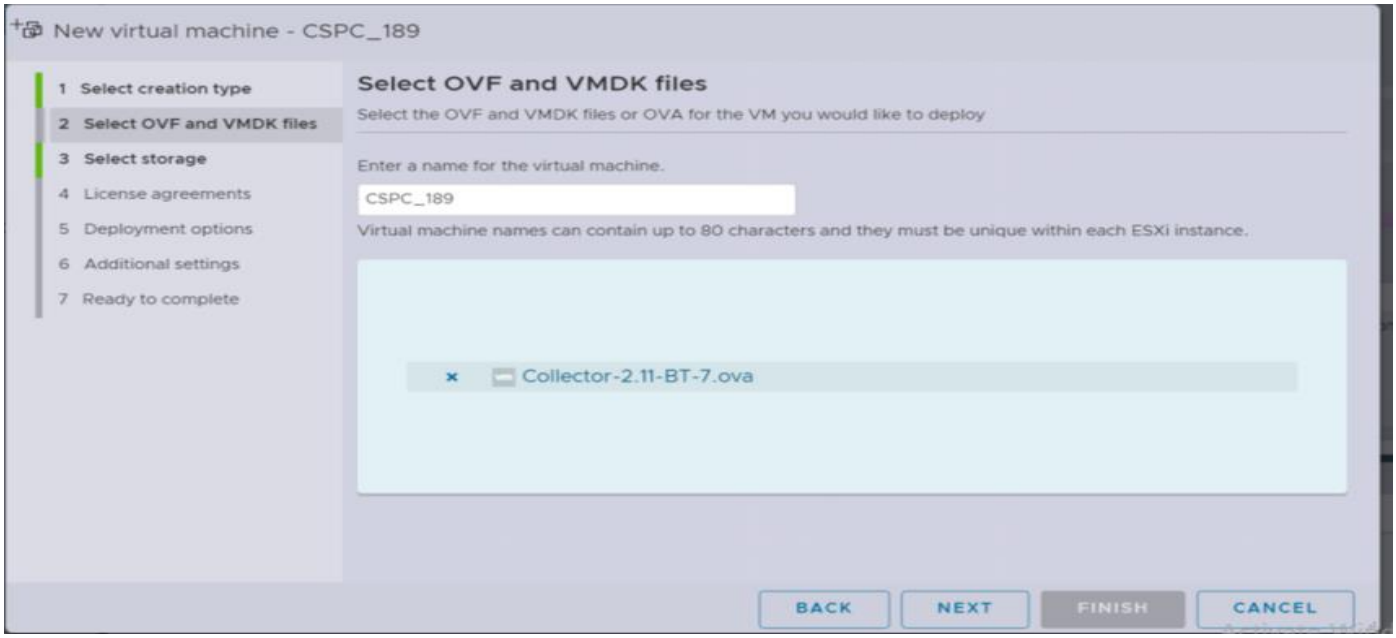
Note All the screens below are just for illustration and not actual ones.

Figure 2-1 Select creation type



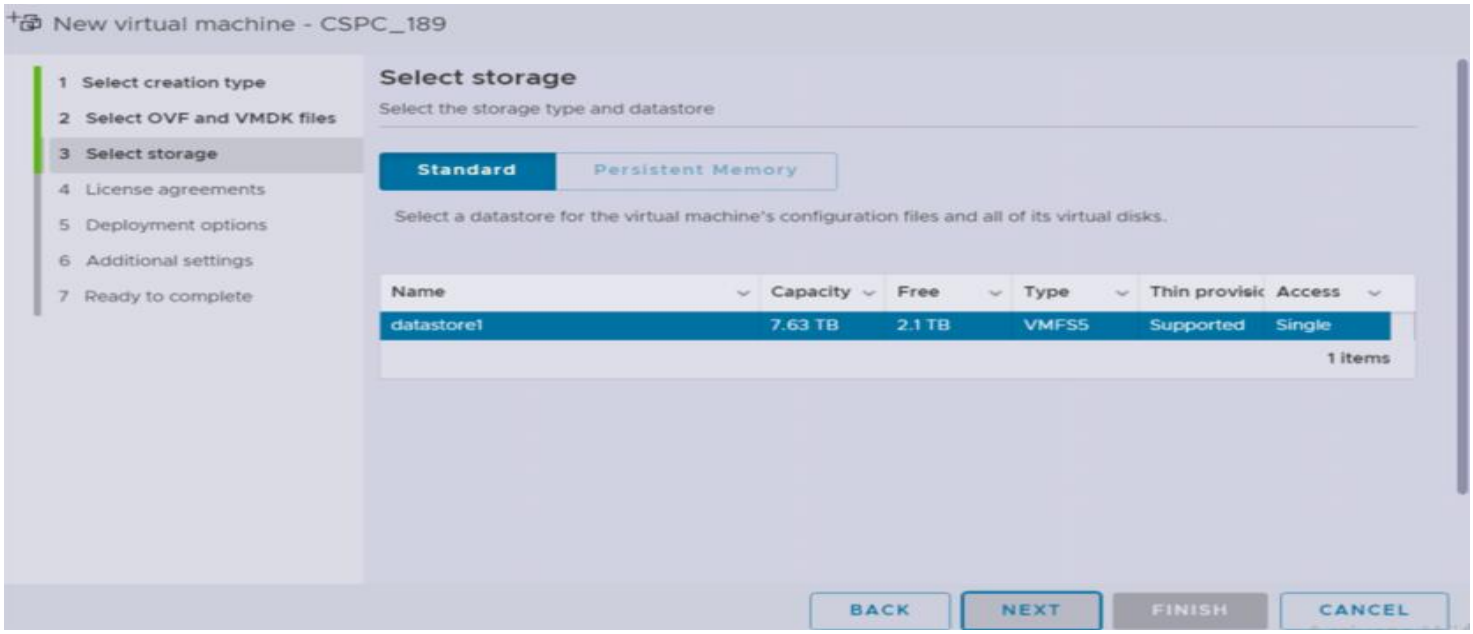
Step 6 click **Next** to proceed

Figure 2-2 Select OVF and VMDK files



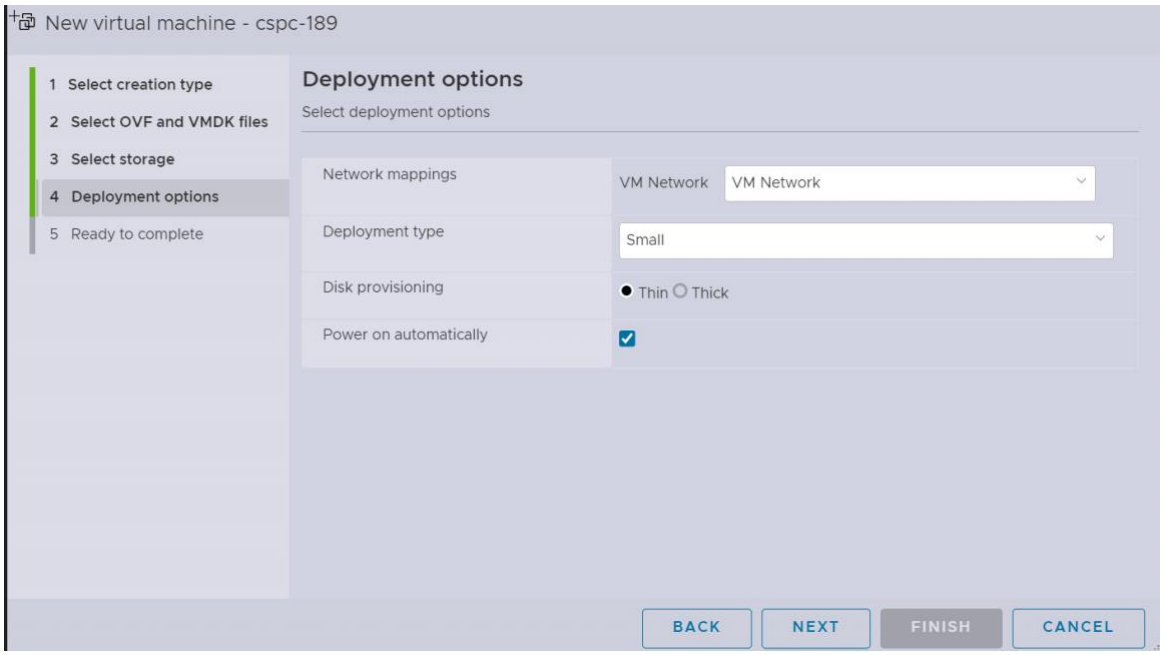
Step 7 Click **Next** to proceed.

Figure 2-3 Select storage



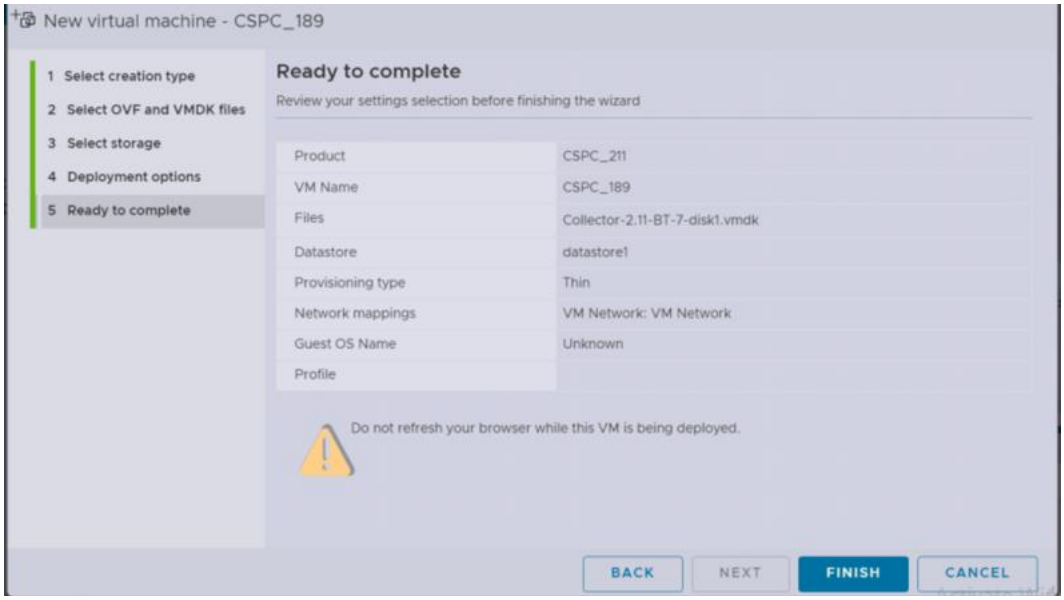
Step 8 *Select VM Network And Click* **Next** *to proceed*

Figure 2-4 Deployment options



Step 9 *Click Finish*

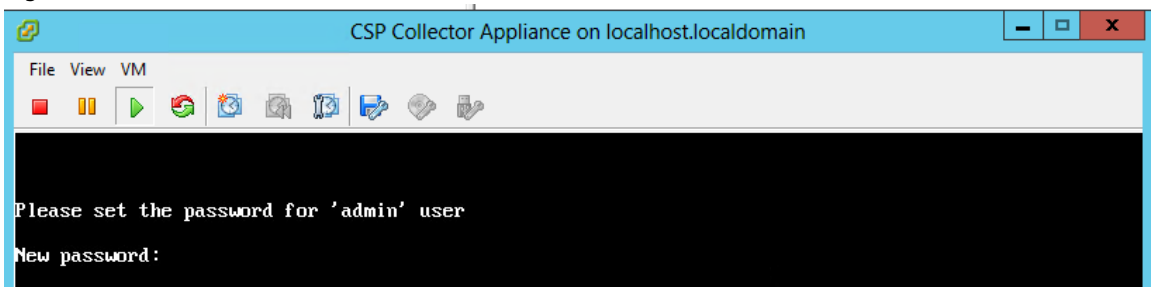
Figure 2-5 Ready to complete



After Successful installation of CSPC OVA, you have to configure IP address.

Step 1 Click on the new installed CSPC OVA

Figure 2-11 Set Admin Password



You will be prompted to enter your password. First enter the password and confirm the password.

Note Be sure to save this password in a secure, accessible location. The Admin password is needed to access the Admin Shell (CLI).

If 2.11 startup job(/etc/rc.d/rc.local) is running for more than 20 mins then try pressing Alt+F1 through Alt+F6 to shift to alternate virtual terminals and you may see one of them waiting for with the admin password prompt. (if so, enter password).

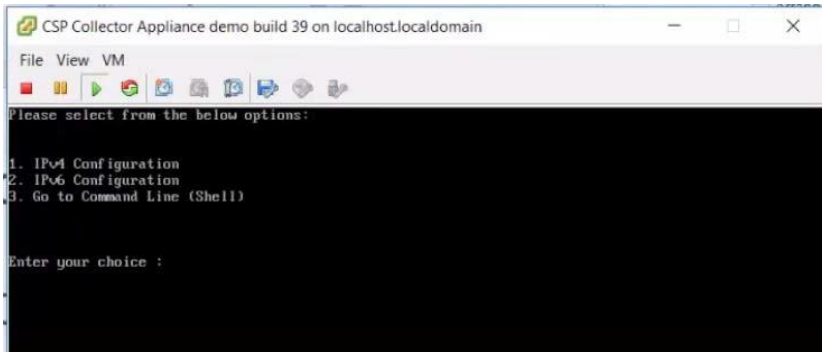
Once you enter your password, you will be able to configure the IP from the menu or in the command shell prompt.

No matter which method you use to configure the IP address, be sure to connect to the admin shell to initialize the collector login and root users.

Step 2 Select one of the options

Chapter 2 Installation and Configuration
OVA Installation

Figure 2-12 Main Menu

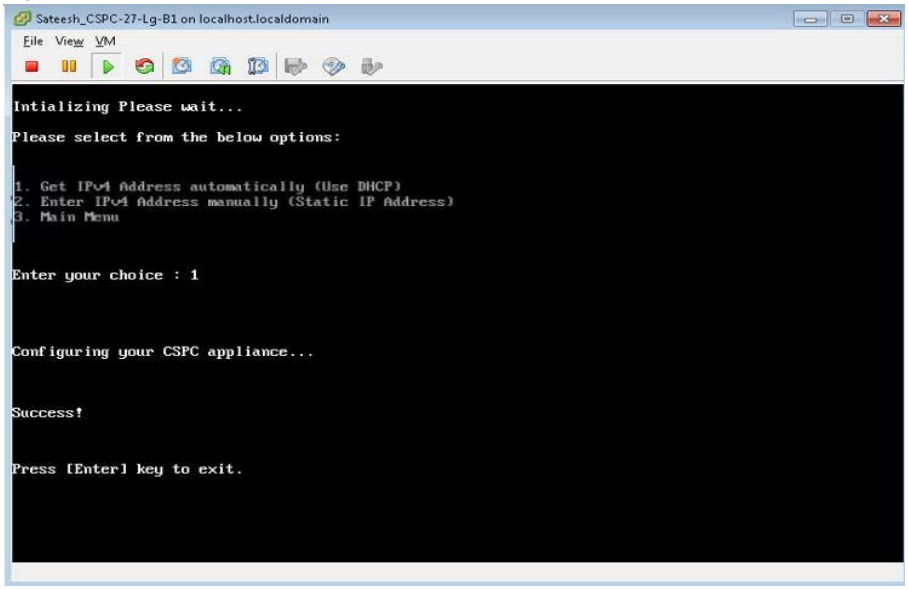


Configure IPv4 address

Step 1 Select **1** to configure IPv4 address

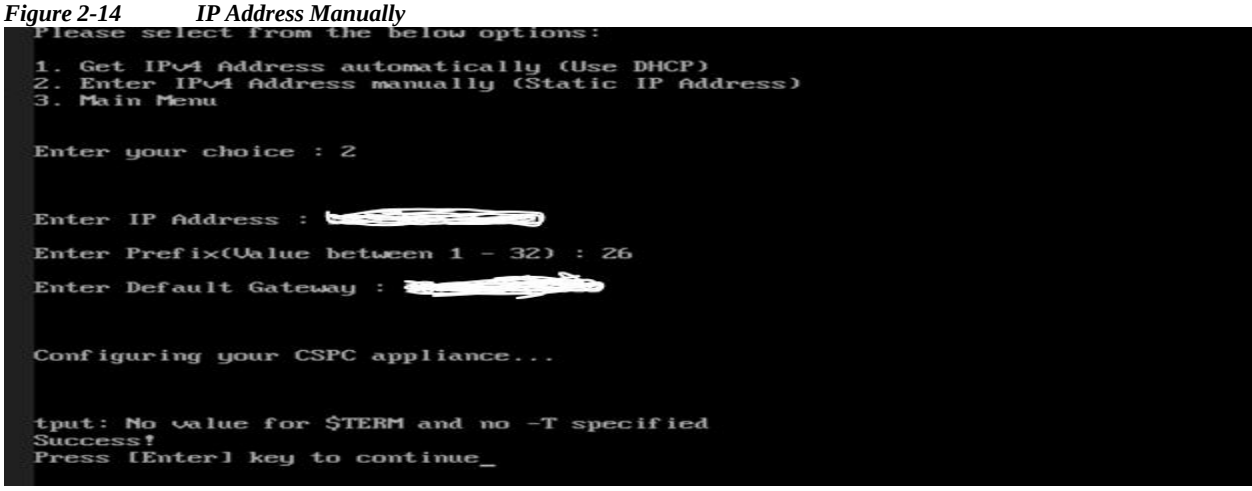
- Select the any one option:
  - Select **1** to fetch IP address automatically

Figure 2-13 DHCP

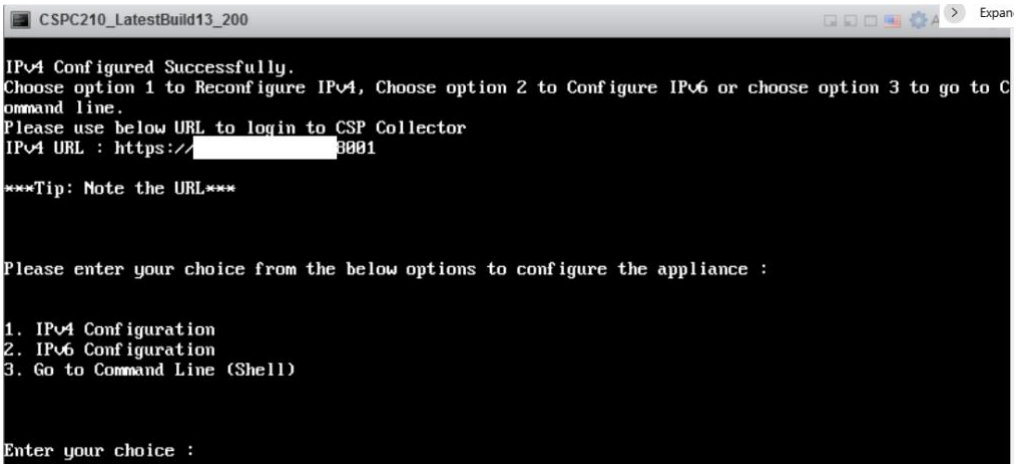


  - Select **2** to enter the IP Address manually

Figure 2-14 IP Address Manually



– Select **3** to go back to main menu



Choose option 1 to reconfigure IPv4 address, choose option 2 to reconfigure IPv6 address or choose option 3 to go to command line.

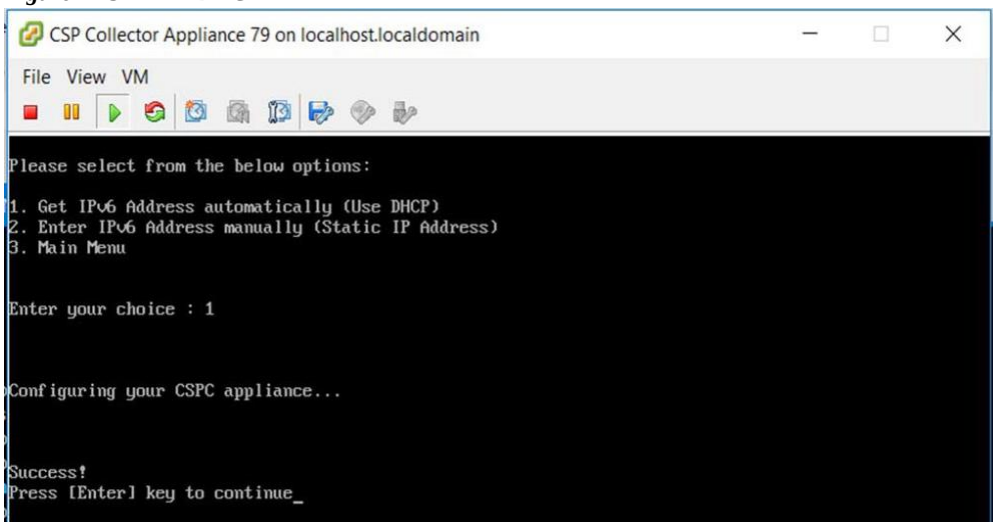
After selecting option 3, ssl certificate will be generated during installation instead of static certificates

Configure IPv6 Address

Step 2 Select 2 to configure IPv6 address

- Select any one option:
  - Select **1** to fetch IP address automatically

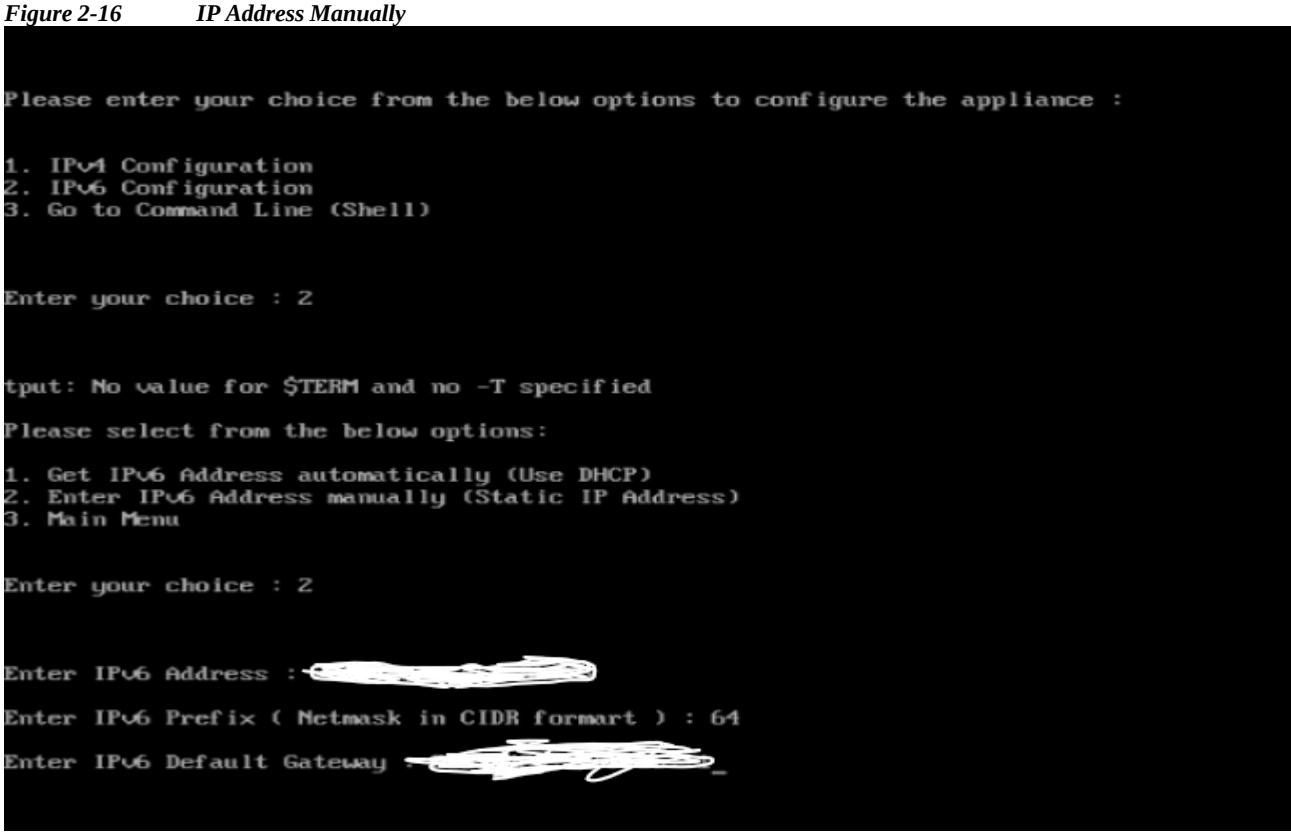
Figure 2-15 DHCP



  - Select **2** to enter the IP Address manually

Chapter 2 Installation and Configuration
OVA Installation

Figure 2-16 IP Address Manually



– Select **3** to go back to main menu.

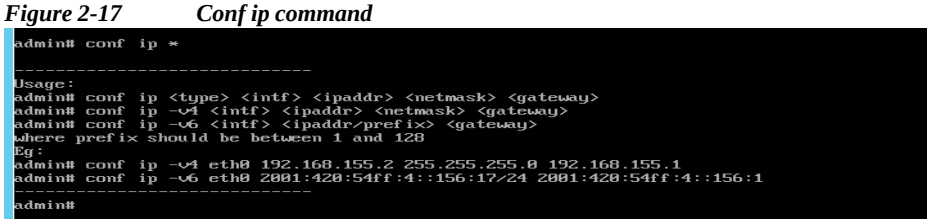
Configure the IP address directly on shell

Step 1 Select **3** to view Command line (Shell)

Note Only admin users can configure IP. Before configuring IP switch over as an admin user

Step 2 Enter the command `Conf ip -v4 eth0` or `Conf ip -v6 eth0` and enter IP Address, Subnet mask, and gateway as show in the figure

Figure 2-17 Conf ip command



Confirm your IP address settings

```
# show ip
```

Enable Default Account

To initially set or reset the password use the below command:

Step 1 Enable the Linux user login "collectorlogin"

```
# pwdreset collectorlogin 90
```

This generates a password for the username "collectorlogin."

Step 2 Enable the Linux root login

```
# pwdreset root 90
```

This generates a password for the username " root".

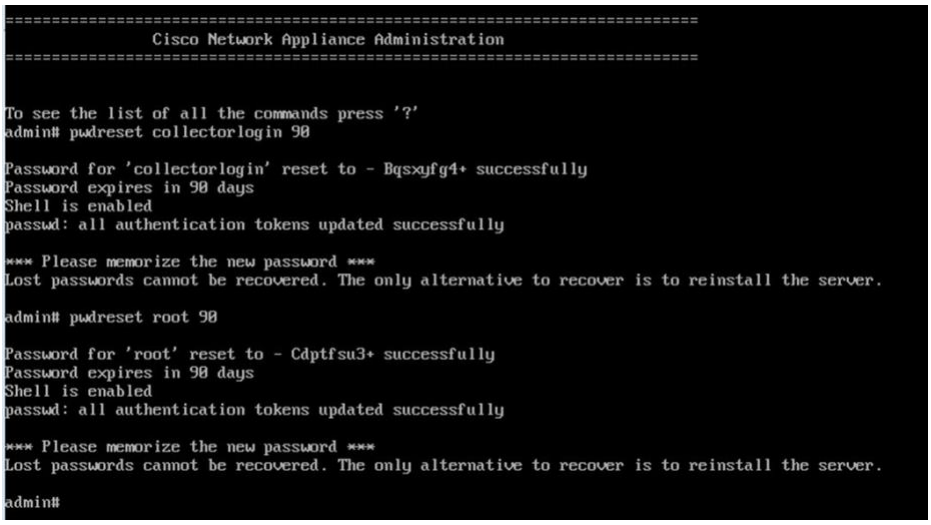
To connect to root first connect to the collectorlogin prompt and then use the command `su root`

```
$ su root
```

Note

- Be sure to save both the collectorlogin and root passwords in a secure, accessible location!
- You are not allowed to connect directly to root, attempts to connect directly to the user root will cause a lock on that account!

Figure 2-18 Password set/reset



Note

- You can now connect to the server using SSH or through a browser at address https://<IP Address of the Collector>:8001
- There are additional commands on the admin shell. To display them just do the following: # ?
- Even though IPV4 is configured, login banner message shows the URL with default IPV6 address in some cases, but you should be able to login via configured IPV4 address. If you want to remove IPV6 address from login banner message then comment the following line from */etc/NetworkManager/system-connections/<**interfacename**>.nmconnection* file.

  #[ipv6]

  #addr-gen-mode=default

  #method=auto

Set GRUB Password

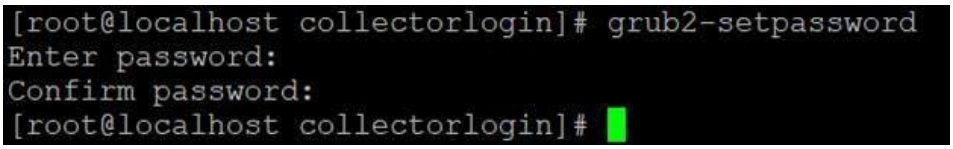
Step 1 Login as a root user

Step 2 Execute the command `grub2-setpassword`

Step 5 Provide the password and make sure you save this password

Note Save the grub password in a secure and accessible location for future use. Password recovery and other troubleshooting is not possible without grub password.

Figure 2-19 GRUB Password



TACACS Authentication

To enable TACACS authentication for collector CLI login as root user, perform the following:

Step 1 `vi /etc/pam.d/tac_plus` add the following at start and enter the parameters in the braces.

```
auth        sufficient    /usr/local/lib/security/pam_tacplus.so debug
server=<TACACS Server IP> secret=<TACACS Server secret key>

account     sufficient    /usr/local/lib/security/pam_tacplus.so debug
server=<TACACS Server IP here> secret=<TACACS Server secret key here>
service=shell protocol=ssh

session     sufficient    /usr/local/lib/security/pam_tacplus.so debug
server=<TACACS Server IP here> secret=<TACACS Server secret key here>
service=shell protocol=ssh
```

Step 2 `vi /etc/pam.d/sshd` add the following line at the start.

```
auth        include       tac_plus
```

Step 3 Restart the `service sshd restart`

ESXi 7.0 Patch Installation

ESXi 7.0 version less than to build-21930508 then upgrade to 7.0 latest version by using following steps:

1. To download ESXi 7.0 latest build locally by click on below url:

   URL: ESXi 7.0-2193058
2. Follow steps in the document “Release Notes for ESXI_7.0_21930508”.

CSPC NAT OVA Installation

You require all these noted below before you start deploying.

- ESXI Login IP and credentials
- Existing NAT router / CSRV1000VVM login IP and credentials
- Copy of NAT rules and other customized configuration on old NAT router VM that required to be replaced
- VSphere client to connect to ESXI
- CSPC NAT OVA available locally or on network to deploy. Default credentials of the OVA

This section describes steps to deploy CSPC NAT OVA using VMWare vSphere Client:

Step 1 Get the xxx.ova file either to a web server or local file system where vSphere client is available

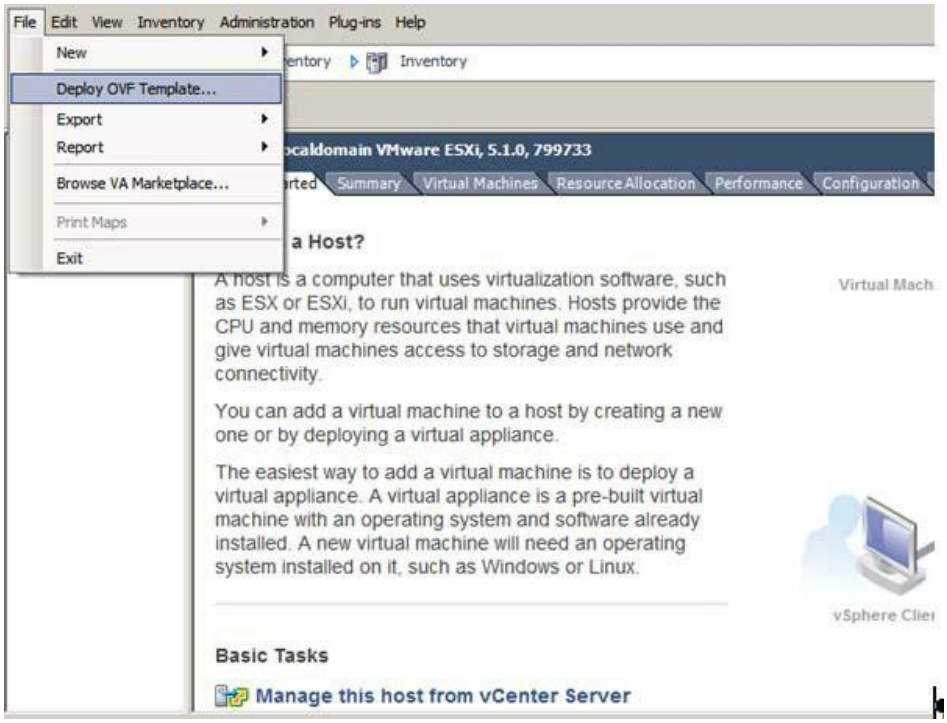
Step 2 Launch vSphere client and login using credentials with the privilege to deploy an OVA file

Step 3 Use vSphere client and select the ESXi host or IP address that manages NAT virtual machine

Step 4 Use vSphere client and select the File menu and then select the **Deploy OVF Template…** menu item shown in the file menu

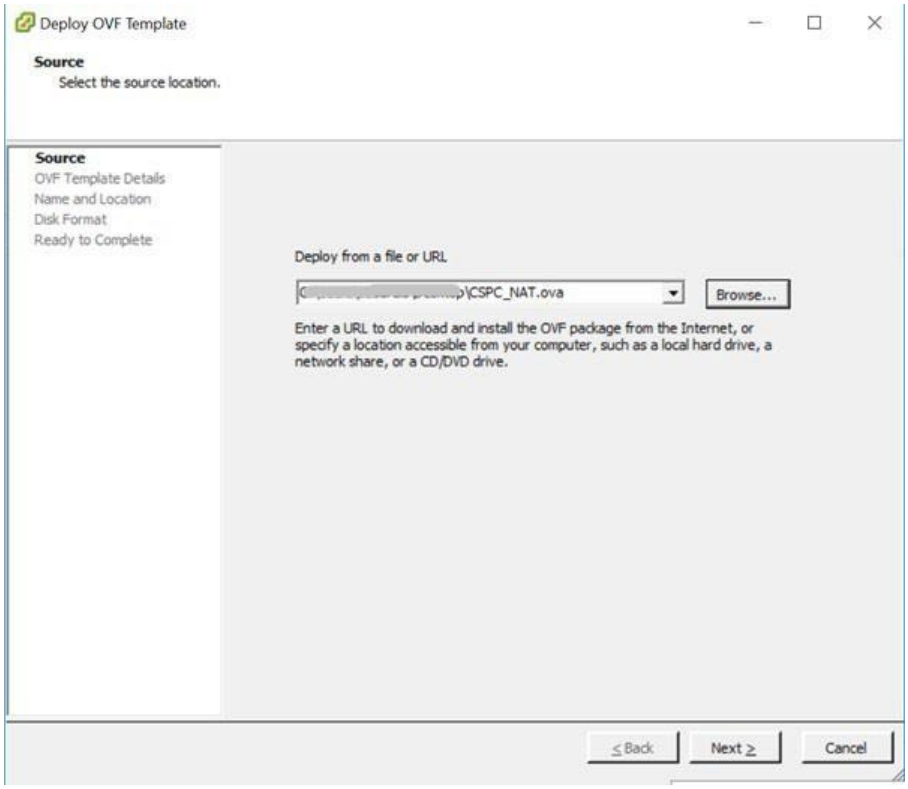
Step 5 Select the OVA file residing locally using the file explorer. If this option is used, click **Browse…** and navigate the file explorer to locate the file *xxx.ova*, then click **Next**

Figure 2-20 Deploy OVF Template



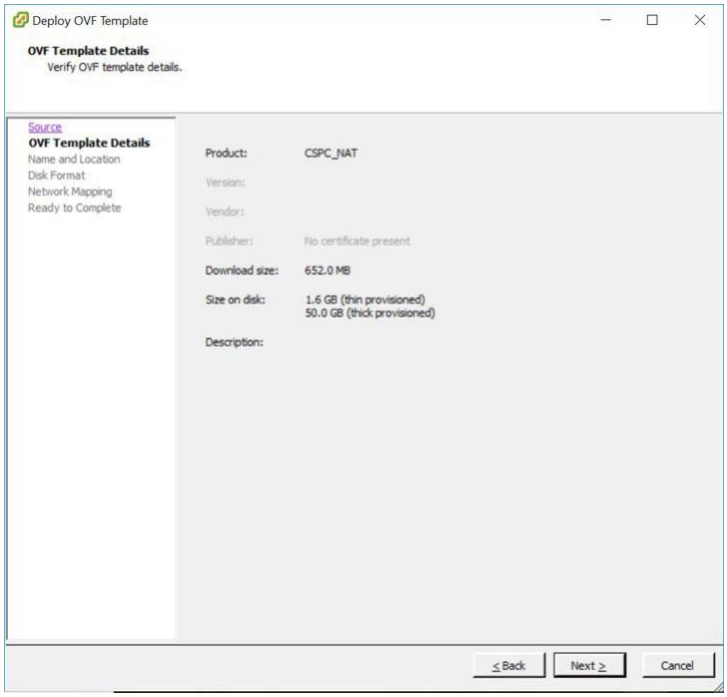
Step 6 Enter the path or Browse to select the CSPC NAT OVA and click **Next** to proceed

Figure 2-21 Source



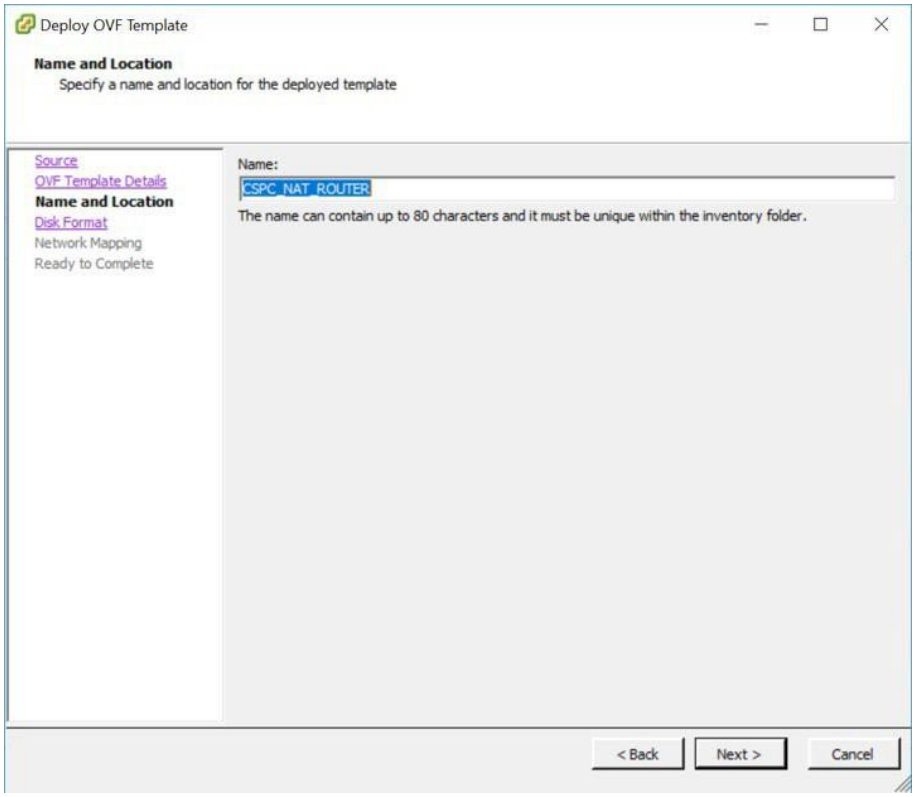
Step 7 Click **Next** to proceed

Figure 2-22 Verify OVF Template Details



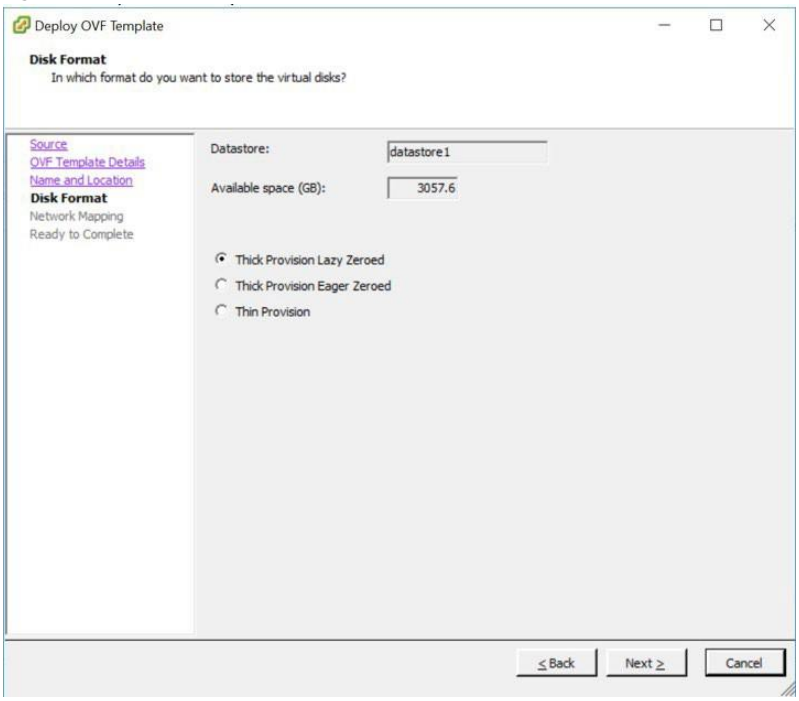
Step 8 Select the appropriate storage to store the virtual machine then click **Next** to proceed

Figure 2-23 Name and Location



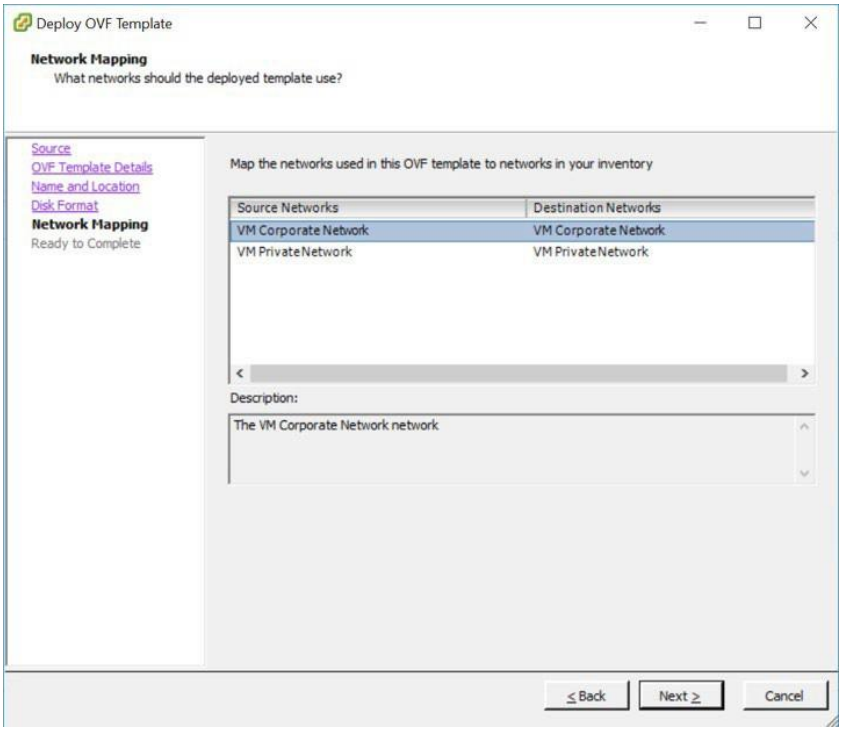
Step 9 "Thick provision Lazy Zeroed" is selected by default, click **Next** to proceed

Figure 2-24 Disk Format



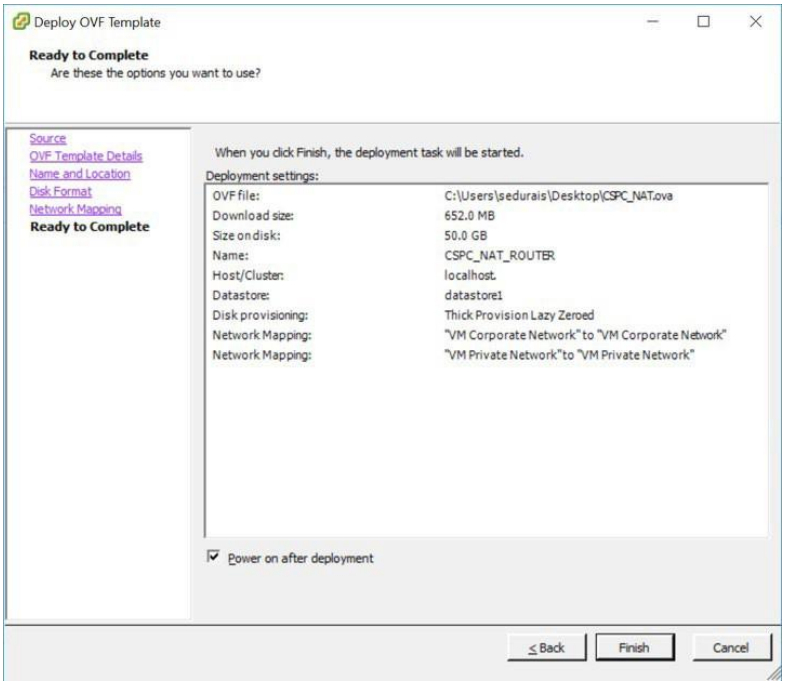
Step 10 Select Destination Networks, as "VM Corporate Network" to "VM Corporate Network" and "VM Private Network" to "VM Private Network" and click **Next**

Figure 2-25 Network Mapping



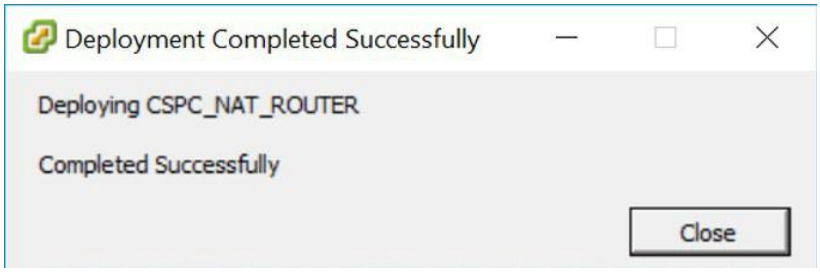
Step 11 Choose the **Power on after deployment**, then click **Finish**

Figure 2-26 Ready to Complete



Step 12 Deployment is completed. Click **Close**

Figure 2-27 Deployment progress

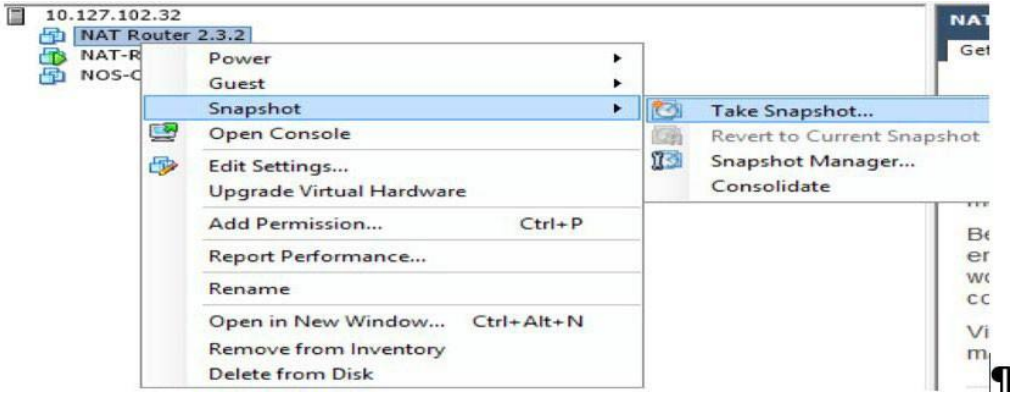


After Successful installation of OVA, you have to configure CSPC NAT OVA.

To configure CSPC NAT OVA, perform the following:

Step 1 Take Snapshot of old CSRV1000 and Power OFF old CSRV1000 VM

Figure 2-28 Old CSRV1000

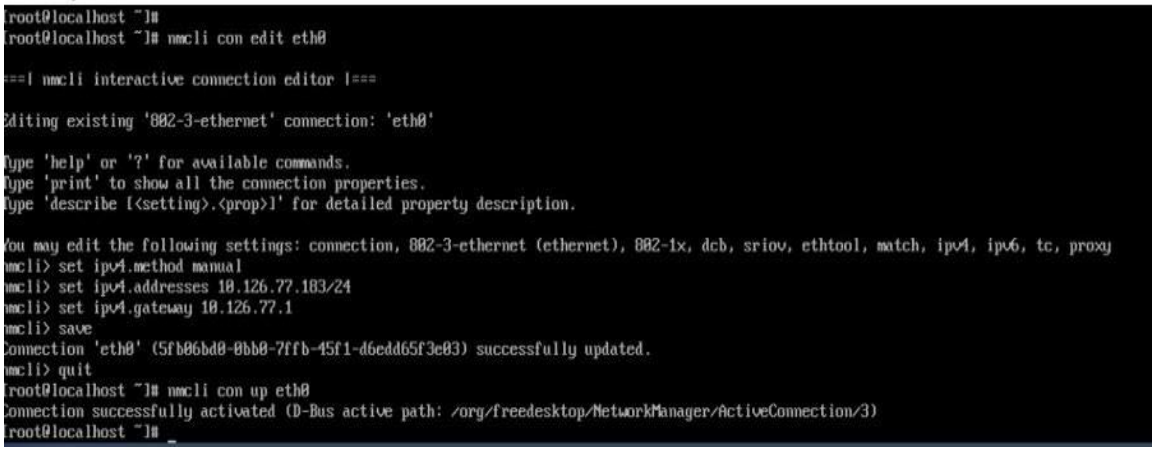


Step 2 Right click on new CSPC NAT VM, and select **Open Console**. Once Router up and running, Login as root user and provide default password "XXxxXX$" (contact CSPC support for default password)

Step 3 You need to provide IP address and Netmask for eth0 external interface

```
# nmcli con edit eth0
> set ipv4.method manual
> set ipv4.addresses <ip_address/prefix>
> set ipv4.gateway <gateway IP>
> save
> quit
        # nmcli con up eth0
```

Figure 2-29 Console



Step 4 CENTS OS7 NAT Router

"Reload Firewall rules firewall-cmd-reload"

Step 5 NAT Rules

Firewall-cmd –list-all –zone=cspszone

Note This CenOS7 Nat routeNote: This CenOS7 Nat router OVA can be accessed from ESXI console or CLI using ssh as 'admin' user from port 1022 then switch to root.r OVA can be accessed from ESXI console or CLI using ssh as 'admin' user from port 1022 then switch to root"

Now you will be able to login to CSPC UI and other VMs UI successfully.

CIMC Patch Installation

Step 1 Login to collector appliance as admin

Step 2 To check updates for CIMC execute below command:

```
#check update cimc
```

Step 3 To download the CIMC patch execute below command (M3 server):

```
#download jeos-101.0.3-0-lnx64
```

Step 4 To download the CIMC patch execute below command (M4 server):

```
#download jeos-101.0.4-0-lnx64
```

Step 5 To check download status execute below command:

```
#show download
```

Step 6 Once the patch is downloaded to `/opt/LCM/tmp`, unzip the patch and follow the instructions from Read_me_CIMC_3.0(4i).docx

NOS Configurer

Installation Sequence For nos_configurer

Note This is only for NOS.

This section shows the instructions on how to install nos_configurer_2.11 on CSPC 2.11, and to configure CSPC for NOS specific functionalities.

Note
- The NOS Configurer, RI Addons should be installed manually which are present in the $CSPCHOME/installer/manual folder.
- There is no updates on nos configurer in CSPC 2.11. So, you can follow the same steps below.

Note This only for fresh nos installation.

It performs the following tasks:

1. Schedule jobs to carry out NOS functionalities

   Following jobs are scheduled:

   a. Weekly Inventory Job
   b. Daily Upload Job
   c. Daily DAV Job
   d. Daily Health Upload Job
2. Adds dependency rules to maintain data consistency

Follow the steps given below to install nos_configure_2.11 on CSPC 2.11:

Step 1 Terminal login to CSPC appliance

Step 2 Navigate to path `$CSPCHOME/installs/manual`

Step 3 Unzip the file `nos_configurer_2.11.zip`

Step 4 On unzipping, a folder named nos_configurer_2.11 is created

Step 5 Enter the command:

a. **`cd nos_configurer_2.11`**

b. **`sh nos_cspc_2.11_patch.sh <username> <pwd> <fullInventoryDay> <hourOfFullInventory> <hourOfUpload>`**

   Example: **`sh nos_cspc_2.11_patch.sh <username> <pwd> 1 22 23`**

Note You can install the installer without giving above three optional arguments. This will install support installer with default values as 1, 23 and 23.

In the above example:

1..7 = Sunday to Saturday

1…23 = hours in a day.

Step 6 On triggering the above command, it will prompt for user confirmations. Provide them accordingly

a. Do you want to cancel installation and rerun with additional arguments? Enter Y or N: (y/n)? **N**

b. Do you want to cancel installation and rerun with different scheduling day and hours ? Enter Y or N: (y/n)? **N**

c. Do you want to schedule health job immediately Enter Y or N: (y/n)? **Y**

d. Do you want to schedule inventory/DAV/Upload job immediately Enter Y or N: (y/n)? **Y**

e. Restarting the server to make sure inventory is not running. Do you want to continue? Enter Y or N: (y/n)? **N**

Note You have option to schedule the job now or later.