Installing Prime Service Catalog

Installing Prime Service Catalog Virtual Appliance

The OVA installation will install all the Virtual Appliance components on different nodes. The nodes should be deployed in the same order as shown in the Virtual Appliance prompt. You can also add additional Prime Service Catalog nodes to set up a cluster for failover.

Installing the Database Node

Open the VM's Console in your vSphere Client. The VM console will display the following prompts:

Before You Begin

Prepare the Virtual Appliance for deployment. For more information, see Preparing the Virtual Appliance for Deployment..

Step 1 Login as 'shelladmin' in to the database node using the default password **Cisco1234**.

Step 2 **Do you want to reconfigure network settings?** By default the node boots up with DHCP, to continue select **n**. This skips the next prompt.

Step 3 **Do you want to configure DHCP or Static IP?** Enter either the value **dhcp** or **static**.
If you select DHCP address, make sure that your VM is using a VMware network portgroup that is connected to a DHCP server.

If you select Static IP address, you are prompted to enter the values for Static IP Address, Subnet Mask, Default Gateway, Primary DNS Address, and (optionally) Secondary DNS Address.

You are prompted to confirm the values that you have entered before continuing.

Step 4 **Appliance Hostname:** Enter the hostname for your VM. You can enter a Fully Qualified Domain Name such as **pscdb.mydomain.com**, or a short hostname such as **pscdb**. Hostname value must begin with an alphabetic character, and must contain only alphabetic characters, digits, hyphen, and period.

Step 5 **Password for System Components:** Enter a common password that will be used for the following user(s):

- Shelladmin user
- root user
- Oracle **system** and **sys** users
- Prime Service Catalog Database user

A valid password must conform to the following rule:

- Is between 8 to 16 character long
- Begins with an alphabetic character
- Contains at least one upper-case character
- Contains at least one lower-case character
- Contains at least one digit
- Contains at least one special character from the following list: ^ * - _

After the value for the last prompt is entered, the VM will perform a series of tasks to install and configure the Oracle database server. This process will take a few minutes to complete. Wait until you see the message on the screen, which says that the Database Node has been successfully initialized. The message will contain the details to access Prime Service Catalog database.

The system will also show the details such as Host IP address, DB Port, DB Service Name, and User Name for connecting to Prime Service Catalog Database.

Installing the Prime Service Catalog Node

Use this procedure to set up a Prime Service Catalog node.

Before You Begin

- Prepare the Virtual Appliance for deployment. For more information, see Preparing the Virtual Appliance for Deployment..
- Set up the database node and ensure that it is up and running. For information on setting up a database node, see Installing the Database Node .

Step 1 Open the VM's Console in your vSphere Client.

Step 2 Login as 'shelladmin' in to the prime service catalog node using the default password **Cisco1234**. The VM console will display the following prompts:

a) **Do you want to reconfigure network settings?** By default the node boots up with DHCP, to continue select **n**. This skips the next prompt.

b) **Do you want to configure DHCP or Static IP?** Enter either the value **dhcp** or **static**.
If you select DHCP address, make sure that your VM is using a VMware network portgroup that is connected to a DHCP server.

If you select Static IP address, you are prompted to enter the values for Static IP Address, Subnet Mask, Default Gateway, Primary DNS Address, and (optionally) Secondary DNS Address.

You are prompted to confirm the values that you have entered before continuing.

c) **Appliance Hostname:** Enter the hostname for your VM. You can enter a Fully Qualified Domain Name such as **psc.mydomain.com**, or a short hostname such as **psc**. Hostname value must begin with an alphabetic character, and must contain only alphabetic characters, digits, hyphen, and period.

d) **Appliance Node Type:** Choose option **1 - Prime Service Catalog Node** to install Prime Service Catalog using an external database on a VM.

e) **Password for System Components:** Enter a common password that will be used for the following user(s):

- Shelladmin user
- root user
- Prime Service Catalog Site Administrator user
- Prime Service Catalog JMS user
- RabbitMQ user

A valid password must conform to the following rule:

- Is between 8 to 16 character long
- Begins with an alphabetic character
- Contains at least one upper-case character
- Contains at least one lower-case character
- Contains at least one digit

- Contains at least one special character from the following list: ^ * - _

f) **Multicast IP Address:** Enter a unique multicast IP address in your network environment, for use by Prime Service Catalog server.

g) **Multicast Port number:** Enter a unique multicast port number in your network environment, for use by the Prime Service Catalog server.

Note If you plan to deploy multiple Prime Service Catalog nodes in a clustered configuration, ensure that you use the same Multicast Address and Port number for all the nodes.

h) Choose the node type for the location of your Prime Service Catalog database, you will be prompted with the following values:

- Enter **1** to proceed with **Prime Service Catalog Virtual Appliance Database Node**, you will be prompted with the following values:
  - Enter the Hostname or IP address of the machine where database node was installed.
  - Enter the database node password.
  - Enter the root password for Prime Service Catalog database node.
- Enter **2** to proceed with **Externally-Managed Oracle Database 12c**, you will be prompted with the following values:
  - Enter the Hostname or IP address of the machine where database node was installed.
  - Enter other database details such as the database port, Oracle service name or Oracle SID, database user name, and the Oracle database user password.

After the value for the last prompt is entered, the VM will perform a series of tasks to boot up the CentOS, and configure the Prime Service Catalog services. This process may take up to 10 minutes to complete. Wait until you see the message on the screen, which says that the Cisco Prime Service Catalog Virtual Appliance initialization completed successfully. The message will also contain the URL for Cisco Prime Service Catalog.

Step 3 Open a supported web browser and connect to the Prime Service Catalog URL. You should see the Login screen.

Step 4 To login as the Site Administrator user of Prime Service Catalog, type **admin** in the User Name field, type the password value that you provided in *Step 1 d* in the Password field, and then click the **Log In** button. Once logged in, you should see the Service Catalog home page.

The installation of the Prime Service Catalog Virtual Appliance is completed.

After the installation is complete, RabbitMQ Cluster connection is added automatically. This configuration can be verified in **Integrations > Internal > RabbitMQ Server**. For more information on RabbitMQ server see section Accessing RabbitMQ Server, on page 14.

What to Do Next

Proceed to the **Installing Prime Service Catalog Cluster Node**.

Installing Prime Service Catalog Cluster Node

Use the procedure detailed here only if you want to configure a clustered environment for Prime Service Catalog. In this section, you will deploy the OVA file for a second Prime Service Catalog Node, that will act as a secondary cluster node. The first Prime Service Catalog Node that you already have will act as the primary cluster node.

Before You Begin

- Prepare the Virtual Appliance for deployment. For more information, see Preparing the Virtual Appliance for Deployment.
- Set up the database node and ensure that it is up and running. For information on setting up a database node, see Installing the Database Node .
- Install the Prime service Catalog node and ensure that it is up and running. For more on installing a Prime Service Catalog node, see Installing the Prime Service Catalog Node .
- Make sure that root login is enabled on the Prime Service Catalog Primary node. You can enable the root login through shell admin menu. For more information, see Launching Shell Menu.
- Make sure that all the Firewall ports for services such as Service Link, Domain Controller, and Prime Service Catalog Application Management Port are open. You can enable these ports through shell admin menu. For more information on Shell Menu, see Launching Shell Menu.

Step 1 Open the VM's Console in your vSphere Client.

Step 2 Login as 'shelladmin' in to the Prime Service Catalog cluster node using the default password **Cisco1234**. The VM console will display the following prompts:

a) **Do you want to reconfigure network settings?** By default the node boots up with DHCP, to continue select **n**. This skips the next prompt.

b) **Do you want to configure DHCP or Static IP?** Enter either the value **dhcp** or **static**.
If you select DHCP address, make sure that your VM is using a VMware network portgroup that is connected to a DHCP server.

If you select Static IP address, you are prompted to enter the values for Static IP Address, Subnet Mask, Default Gateway, Primary DNS Address, and (optionally) Secondary DNS Address.

You are prompted to confirm the values that you have entered before continuing.

c) **Appliance Hostname:** Enter the hostname for your VM. You can enter a Fully Qualified Domain Name such as **psc.mydomain.com**, or a short hostname such as **psc**. Hostname value must begin with an alphabetic character, and must contain only alphabetic characters, digits, hyphen, and period.

d) **Appliance Node Type:** Choose option **1 - Prime Service Catalog Node** to install the Prime Service Catalog components on a VM.

e) **Prime Service Catalog Cluster Node:**Choose option **2 - PSC Cluster Node 2** to set up a two node cluster. If you want to set up a three node cluster, then execute the option **3 - PSC Cluster Node 3**.
Similarly, you can add up to 6 modes in a cluster.

f) **Domain Controller Hostname or IP address:** Enter the IP address of the machine where domain controller is installed.

g) **Domain Controller Password:** Enter the password to access the domain controller node.

h) Enter the root password for Prime Service Catalog Domain Controller node.

The installation of the Prime Service Catalog Virtual Appliance Cluster is completed.

What to Do Next

Proceed to the **Installing the Guacamole Node**.

Installing the Guacamole Node

This is an optional node in case you want to integrate Guacamole server with Prime Service Catalog. For detailed information see section *Integrating Guacamole Server with Prime Service Catalog* in Cisco Prime Service Catalog Administration and Operation Guide.

Step 1 Open the VM's Console in your vSphere Client.

Step 2 Login as 'shelladmin' in to the Guacamole node using the default password **Cisco1234**. The VM console will display the following prompts:

Step 3 **Do you want to reconfigure network settings?** By default the node boots up with DHCP, to continue select **n**. This skips the next prompt.

a) **Do you want to configure DHCP or Static IP?** Enter either the value **dhcp** or **static**.
If you select DHCP address, make sure that your VM is using a VMware network portgroup that is connected to a DHCP server.

If you select Static IP address, you are prompted to enter the values for Static IP Address, Subnet Mask, Default Gateway, Primary DNS Address, and (optionally) Secondary DNS Address.

You are prompted to confirm the values that you have entered before continuing.

b) **Appliance Hostname:** Enter the hostname for your VM. You can enter a Fully Qualified Domain Name such as **guac.mydomain.com**, or a short hostname such as **guac**. Hostname value must begin with an alphabetic character, and must contain only alphabetic characters, digits, hyphen, and period.

c) **Enter new password for System Components:** Enter a common password that will be used for the following user(s):

- shelladmin user
- root user
- MaridDB root user
- MariaDB guacamole user
- guacadmin

A valid password must conform to the following rule:

- Is between 8 to 16 character long
- Begins with an alphabetic character
- Contains at least one upper-case character

- Contains at least one lower-case character
- Contains at least one digit
- Contains at least one special character from the following list: ^ * - _

d) **Enter PSC Domain Controller host name or IP address:** Enter the IP address of the machine where domain controller is installed.
e) **Enter Prime Service Catalog Admin Password:** Enter the password for Prime Service Catalog admin.
f) **Enter root password for Prime Service Catalog Domain Controller:** Enter the root password for Prime Service Catalog Domain Controller node.
After the value for the last prompt is entered, the VM performs a series of tasks to configure the Guacamole server. This process may take up to 10 minutes to complete. Wait until you see the message on the screen, which says that the Cisco Prime Service Catalog Virtual Appliance Guacamole node has been successfully initialized.

Step 4 Open a supported web browser and connect to the Guacamole URL *http://<ip-address>:8080/guacamole*. You should see the Guacamole Login screen. Enter "guacadmin" in the User Name field and enter the password value that you provided in *Step 3 c* in the Password field.

The installation of the Guacamole server is completed.

After the installation is complete, Guacamole server connection is added automatically. This configuration can be verified in **Integrations > Internal > Guacamole Server**.

What to Do Next

Proceed to **Post Installation Tasks** section to perform the additional configuration tasks, which are required if you plan to use more advanced features of Prime Service Catalog .

Performing Post Installation Tasks

This section consists of the following sub-sections:

- Launching Shell Menu
- Configuring SMTP
- Configuring Proxy Server Settings
- Manage Packages and Patches

Launching Shell Menu

The Shell Menu allows you to perform various administrative tasks for the Virtual Appliance such as configuring SMTP setting, configuring Proxy server, changing passwords, starting and stopping services on the Linux operating system, etc.

Login to the Virtual Appliance as the **shelladmin** user. You can do this via the VM Console in your vSphere Client, or via an SSH connection to the IP address of the VM. On the Login Prompt, type **shelladmin** for the user name, and type the password value that you provided in *Step 2 e* of the Installing the Prime Service

Catalog Node section. Once logged in, you will see the Shell Menu depending upon the type of installation. Following is the list of commands that appears in a Shell Menu for different types of installation. For details on these prompts, see the table below.

Database and Guacamole Node Shell Menu Options

- Manage Users
- View Service Status
- Stop Services
- Start Services
- Manage Database
- Manage Network Interface
- Manage SMTP
- View Logs
- System Information & Cisco Support
- Manage Docker Applications (available only for Guacamole node)
- Manage Packages and Patches
- Login as Root
- Shutdown Appliance
- Reboot Appliance
- Quit

Prime Service Catalog Node Shell Menu Options

- Manage Users
- View Service Status
- Stop Services
- Start Services
- Manage Firewall
- Manage Network Interface
- Manage SMTP
- Manage Cluster
- View Logs
- System Information & Cisco Support
- Manage Packages and Patches
- Manage Docker Applications
- Login as Root
- Shutdown Appliance

- Reboot Appliance
- Quit

The following table contains the descriptions of all the menu items available on the Shell Menu:

Note For some of the menu items, you may be presented with a list of choices to select. If you don't see any choices that you want and you want to get back to the previous menu, press Control-C (Ctrl+C).

Menu	Description
Manage Users	This menu option allows you to enable or disable root access to CentOS, and to set the password for the root user. It also allows you to change the System Passwords for the Virtual Appliance, shelladmin, Cisco Prime Service Catalog Admin and RabbitMQ User.
View Services Status	This menu option displays the status (running or stopped) of all services on the VM that are related to the Prime Service Catalog.
Stop Services	This menu option allows you stop individual services on the VM, such as, Service Catalog, Service Link, Httpd, RabbitMQ, and Docker.
Start Services	This menu option allows you to start individual services on the VM.
Manage Databases	This menu option allows you to perform database backup, restore, upgrade previous version of Prime Service Catalog database, execute custom SQL on database, and update the data source. It also allows you change Oracle system password and Cisco Prime Service Catalog database user password.
Manage Firewall	This menu option allows you to open or close the TCP port numbers for certain services.
Manage Network Interface	This menu option allows you to view the existing network information and to configure the proxy server settings. **Note:** The Virtual Appliance is not required to have Internet access. If you want to have Internet access for the Virtual Appliance, and your network requires your VM to go through a proxy server to connect to the internet, use this menu to configure the proxy settings on your VM.
Manage SMTP	This menu option allows you to configure the SMTP server setting.
Manage Cluster	This menu option allows you to configure the Prime Service Catalog Cluster settings.
View Logs	This menu option allows you to view the runtime logs of various services on the VM.

Menu	Description
System Information & Cisco Support	This menu option allows you to view the system information and send system information to Cisco Support by selecting appropriate sub-menu options: • Display System Information • Send System Information to Cisco Support
Manage Packages and Patches	This menu option allows you to install a patch for the appliance, should there be a patch released by Cisco in the future for this version of the Virtual Appliance.
Manage Docker Applications	This menu application allows you to view Guacamole containers status and start/stop Guacamole containers.
Login as Root	This menu option allows you to login to Linux as the **root** user. You must first enable the root access via Shell Menu **Manage Users** option.
Shutdown Appliance	This menu option shuts down the Linux operating system and power off the VM.
Reboot Appliance	This menu option reboots the Linux operating system.
Quit	This menu option logs you out of Linux and returns you to the Linux Login Prompt.

Configuring SMTP

The Prime Service Catalog service needs to connect to an SMTP server for all outbound emails. To configure the SMTP server:

Step 1 From the Shell Menu, select option **Manage SMTP**.

Step 2 Select the sub-menu option **Configure SMTP**. You will be prompted to enter the Fully Qualified Domain Name (or the IP address) of the SMTP server, and a valid Support Email Address. Press **Enter** to continue to configure the SMTP.

Configuring Proxy Server Settings

If your VM must go through a proxy server to connect to the internet, do the following on the Shell Menu:

Step 1 Select the option **Manage Network Interface**.

Step 2 Select the sub-menu option **Configure Proxy Settings**. You will be prompted with several questions regarding your proxy server. The system will reconfigure the appliance to use the proxy settings that you have entered.

Step 3 To verify the proxy settings, select the sub-menu option **View Proxy Settings**. Otherwise, select the sub-menu option **Return to Previous Menu** to get back to the main Shell Menu screen.

Manage Packages and Patches

Manage Packages and Patches has the following sub-menu options:

- Send Request for Repository Access
- Enable/Update Cisco Package repository
- Refresh Package repository cache
- Update Outdated System packages
- Update Prime Service catalog Packages
- Install New System Packages

Requesting Access to Repository

To be able to download the Cisco VA patch files from cisco.com you would need to request access to the repository. The sub menu *Send Request for Repository Access* sends an email requesting access for the required user.

Step 1 Select the option **Manage Packages and Patches** from the shell menu.

Step 2 Select the sub-menu option **Send Request for repository Access**.

Step 3 Enter the cisco account **username** who would need access and email address.
An email notification is sent once the access is granted.

Configuring Cisco Package Repository

If your Prime Service catalog VA must be updated with patches, you must enable the cisco repository that contains the latest packages.

Before You Begin

- You must have valid Cisco account.
- You must have access to package repository. For more information on requesting access, see section Requesting Access to Repository.
- You must configure proxy server settings.
- To configure proxy settings, select Manage Network Interface from the main menu and select the Configure Proxy Settings option.

Step 1 Select the option **Manage Packages and Patches**.

Step 2 Select the sub-menu option **Enable/Update Cisco Package Repository**.

Step 3 Enter the SSO **Username** and paste the **API Key** information from the clipboard. For information on Generating API Key, see Generate API Key Using SSO Login.

Step 4 Your repository is now enabled.

Generate API Key Using SSO Login

To generate the API Key using the SSO login, perform the following:

Step 1 Go to **JFrog Artifactory** using the link **https://devhub.cisco.com**.

Step 2 Click **Log In**, in the top right hand corner of the home page.

Step 3 Skip the credentials in this pop-up and Click **SSO Login** in the login page.

Step 4 Enter **User Name** and **Password** in the Cisco.com login page, you will be redirected back to the JFrog Artifactory home page.

Step 5 Click **Profile Name** on the top right hand side of the home page.

Step 6 Click **Generate** to create API Key.

Updating System Packages or Prime Service Catalog VA Patches

Once you have access to the repository and downloaded the packages, you can update the System Packages or Prime Service Catalog Patches from the shell menu.

Before You Begin

Ensure the database files are backed up. For more information on backing the old database, see Backing up the Database on Cisco Prime Service Catalog Virtual Appliance 11.0, 11.1, or 11.1.1.

Step 1 Select the option **Manage Packages and Patches** from the shell menu.

Step 2 Select the sub-menu option **Update Prime Service catalog Packages** to update Prime Service Catalog Patches or **Update Outdated System packages** to update system packages.

Step 3 Enter **Y** to continue, select the package to be updated from the list and enter **Y** again.

Configuring Prime Service Catalog Virtual Appliance With Cisco ONE Enterprise Cloud Suite

Step 1 Log in to Prime Service Catalog as Site Administrator.

Step 2 Go to the **Service Link** module and ensure that the UCSD Agent is up and running.

Step 3 Go to **Service Designer** > **Services**.

Step 4 Expand the **Reserved Services** folder, and then click the **UCSD Application Template Service** template.

Step 5 Choose **Plan**, and then click the **Publish HeatTemplate** task.
The task details appear in the lower pane.

Step 6 In the **General** tab, choose the workflow type, and then click the … button.
A dialog box appears.

Step 7 Choose a public key, and then click **Save**.

Step 8 Go to **Administration** > **Settings**.

Step 9 Enable the **UCSD Scheduler** option, and then click **Update**.

Replacing the Self-Signed Certificate

This is an optional procedure, perform these steps only if you wish to replace the Self-Signed certificate with a new one.

Step 1 Log into the Virtual Appliance system as root.

Step 2 If you have generated a new private key when creating your CSR, backup the original private key and replace it with the new private key:

```
# mv /etc/pki/tls/private/localhost.key /etc/pki/tls/private/localhost.key.orig
```

Step 3 Copy the new private key to /etc/pki/tls/private/localhost.key:

```
# cp {new.key} /etc/pki/tls/private/localhost.key
      # chown root:root /etc/pki/tls/private/localhost.key
      # chmod 400 /etc/pki/tls/private/localhost.key
```

Step 4 Back up the original cert:

```
# mv /etc/pki/tls/certs/localhost.crt /etc/pki/tls/certs/localhost.crt.orig
```

Step 5 Copy the new cert to /etc/pki/tls/certs/localhost.crt:

```
# cp {new.cert}  /etc/pki/tls/certs/localhost.crt
      # chown root:root /etc/pki/tls/certs/localhost.crt
      # chmod 400 /etc/pki/tls/certs/localhost.crt
```

Step 6 Restart the webserver:

```
# systemctl restart httpd
```

Step 7 Verify the new certificate is in place by browsing to https://{ip} and examine the certificate.

Accessing RabbitMQ Server

The rabbitmq-management plugin is installed on each Prime Service Catalog (RabbitMQ) node during installation. This provides an HTTP-based API for management and monitoring of your RabbitMQ server, along with a browser-based UI and a command line tool, rabbitmqadmin.

The RabbitMQ web UI can be accessed using the URL: *http://<serveIPaddress>:15672*. Enter *CPSCUSER* in the User Name field, type the password value that you provided in *Step 2e* of section Installing the Prime Service Catalog Node , on page 3.

Important The port 15672 is closed by default . You must manually open the port using the shelladmin menu: **Manage Firewall** > **Open/Close RabbitMQ Management Port**.