Installing Cisco VIM through Cisco VIM Insight

The VIM Insight has an UI admin, who has the privilege to manage the UI offering. The Insight UI admin, has the rights to add the right users as Pod administrators. Post bootstrap, the URL for the UI will be: https://br_api:9000.

The following topics helps you to install and configure Cisco Virtual Infrastructure Manager with VIM Insight:

- Registering New Pod to Insight , on page 1
- Configuring OpenStack Installation, on page 10
- Post Installation Features for Active Blueprint, on page 44

Registering New Pod to Insight

In this step the user registers a new pod.

Before you begin

UI Admin has to register a Pod Admin to allow the user to access a pod. Following are the steps required for UI Admin to register a Pod Admin:

Step 1 Login as UI Admin and navigate to **Manage Pod Admin(s)** page.

Step 2 Click **Add Pod Admin**.

Step 3 Enter the Email ID of the user.

a) If email is already registered then Username will be populated automatically.

b) If not registered, an email would be sent to the user Email ID.

Step 4 Navigate to https://br_api:9000.

Step 5 Click the Register Management Node Link

- Enter the Endpoint IP for the management node. Run time validation will check if the endpoint is already registered.
- Give the name or tag for the particular management node
- Enter the REST API Password (REST Password is present on the Pod at "/opt/cisco/ui_config.json")
- Provide the Location and the brief description about the management node (Max 200 characters are allowed).
- Enter the Pod Admin's Email ID. Run time validation will check if the entered Email ID belong to the Pod Admin.

1. Run time validation will check if the entered Email ID belong to the Pod Admin.
2. If entered Email ID is not the Pod Admin's ID, then User is not registered as Pod Admin error is displayed.
3. If entered Email ID is the Pod Admin's ID, then User-Name is auto-populated.
4. Section to upload Management Node CA
   - Server certificate is located on management node at /var/www/mercury/mercury-ca.crt.
   - Validation to check the cert file size and extensions are handled.
   - Click on Upload and Update button.
   - If certificate file passes all the validation then a message would be visible "Uploaded Root CA Certificate).

- Click **Register** and management node health validation would take place.
  - If Management Node Validation fails due to invalid certificate, then Insight will delete the certificate from the uploaded path.
  - If Management Node Validation fails due to Password mismatch, then proper message for password mismatch would be visible but certificate won't be deleted hence you can fix the password then go ahead with the Registration.
  - If Rest API service is down on the Management Node then error message "Installer REST API Service is not available" message would be visible.

Login to Insight as Pod Admin

To login to Insight as Pod Admin, follow these steps:

Step 1 Enter the registered Email ID.

Step 2 Enter the valid password.

Step 3 Click **Login as POD**.

Note After successful Sign in user will be redirected to the Dashboard.

The VIM Insight UI

The VIM Insight UI is divided into four parts:

1. **Dashboard**

   Dashboard of the VIM Installer provides the user an intuitive view of monitoring deployment. Dashboard provides a 3D view of 8 stages, which are present in the Installer CLI. The Carrousel displays the real-time status of the install steps, and it rotates automatically once an install stage is completed and a new install stage is started or scheduled. Dashboard maintains the pod state even when the User logs out. It will show the most recent data available via the VIM REST API on the management node. Dashboard provides the following rights to the administrator:

   1. **Deployed Blueprint Details**: Shows information about the current Blueprint (Active/In-Progress). In case of an Inactive Blueprint, the table will be blank.

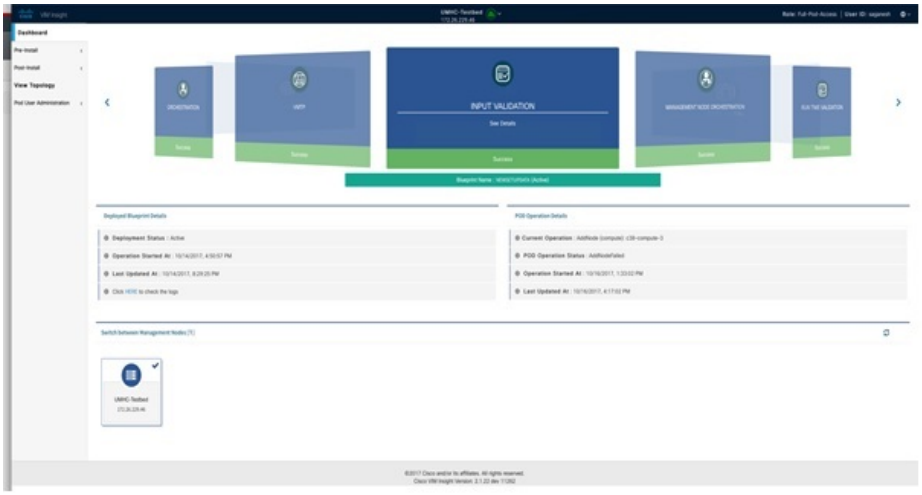
      1. Deployment Status: This tells the status of the Blueprint. There are 3 stages of a Blueprint : Active, in-progress and Failed. Incase of in-progress and Failed states, the stage name would be mentioned in Deployment Status which is a hyperlink. If you click on the stage name, the carrousel will directly jump to that particular stage.
      2. Deployment Started at: This tells the time when the installation was started.
      3. Last Updated at: This tells the last updated time of the installation.
      4. Click Here to check logs: If you click **Here** you will be redirected to the logs page in a new tab for which you will have to enter the REST Username and Password located at /opt/cisco/ui_config.json on the node. By default REST Username is "admin".

   2. **POD Operation Details**: Displays the status regarding all the POD Activities done POST Installation like POD Management, Re-generate Secrets, etc. Following are the information shared in POD Operation Details table:

      1. Current Operation: Name of the Operation Running.
      2. POD Operation Status: Status of the Operation.
      3. Operation Started at: Operation Start time.
      4. Last Updated at: Operation last update time.

   3. **Blueprint Deployment Progress bar for a given POD**: Shows the Blueprint success or failure state in percentage.
   4. **Switch Between Management Nodes**: Will be covered later in this chapter.

Figure 1: VIM Insight Dashboard



2. **Pre-install**

   This section has two menus:

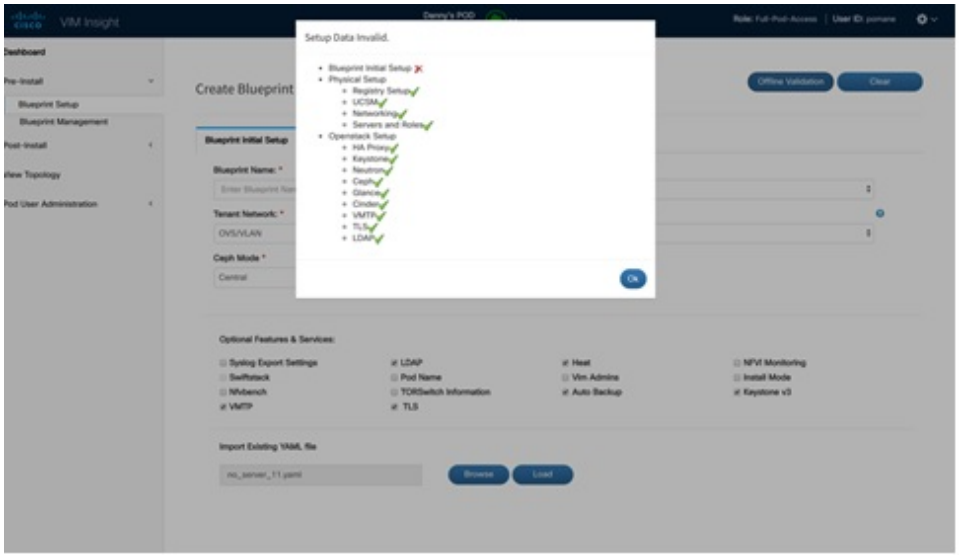
   1. **Blueprint Setup**: Blueprint is the YAML (setupdata) present in the Management node. There are two ways to create a Blueprint:

      1. Form based through the UI.
      2. Upload an existing YAML.

      In case of manual creation the user has to fill in details for Initial setup, physical setup and OpenStack, which covers core and optional features like VMTP, NFVI Monitoring, Auto configuration of ToR, Optional services like Heat, Keystonev3 and so on. In case of upload of an existing YAML, the user can just upload the file and click **Upload** to automatically populate all the corresponding fields in the UI. At any given point, one can initiate the offline validation of the entry, by clicking the **Offline Validate** button, on the upper right hand corner in the **Blueprint Setup** menu.

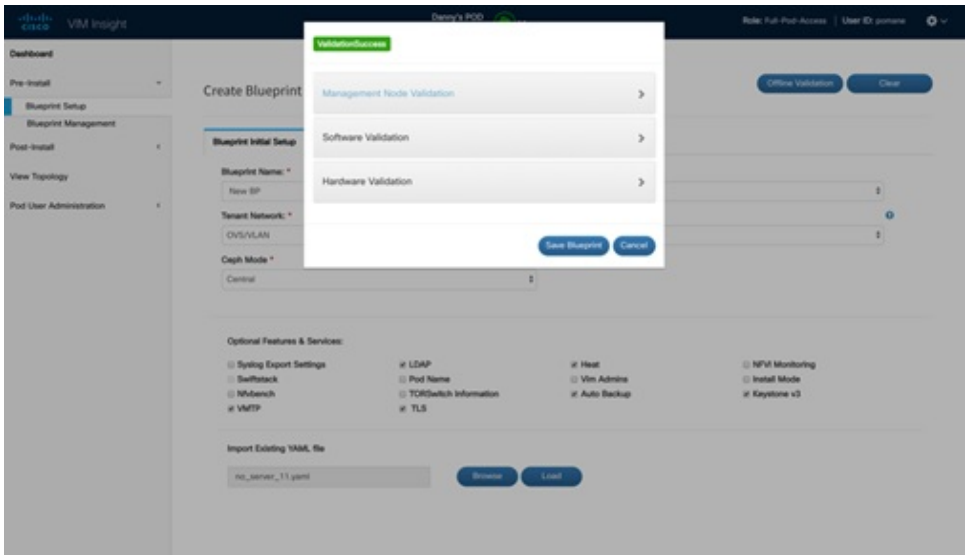
      Offline Validation will only take place if all the fields marked in Blueprint are filled and there are no client side validations remaining. Even if they are the Offline Validation, pop up will show which field is missing.

Figure 2: Blueprint Creation



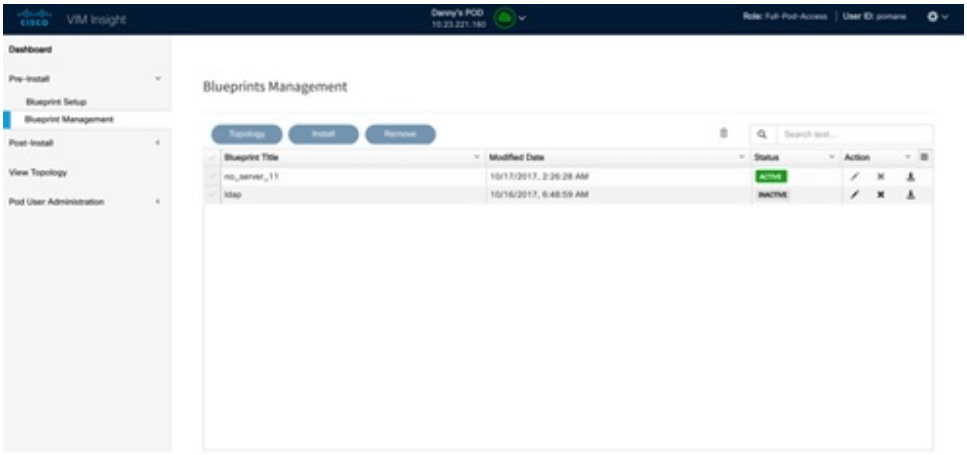
After filling all the details offline validation will take place, if successful, **Save Blueprint** option will be enabled, else user will not be allowed to save the Blueprint. Click **Save blueprint** to be redirected to Blueprint Management.

Figure 3: Blueprint Successful



2. **Blueprint Management**:Blueprint Management gives CRUD access to users for Blueprints in the System. A user can use following features in Blueprint Management:

Figure 4: Blueprint Management



1. Delete Single or Multiple Blueprints which are in Inactive State.
2. Edit Blueprint which are in Inactive State.
3. Deploy Blueprint.
4. Uninstall or Abort Blueprint.
5. Preview and Download created Blueprint on local machine.
6. Search Blueprint from created Blueprints.

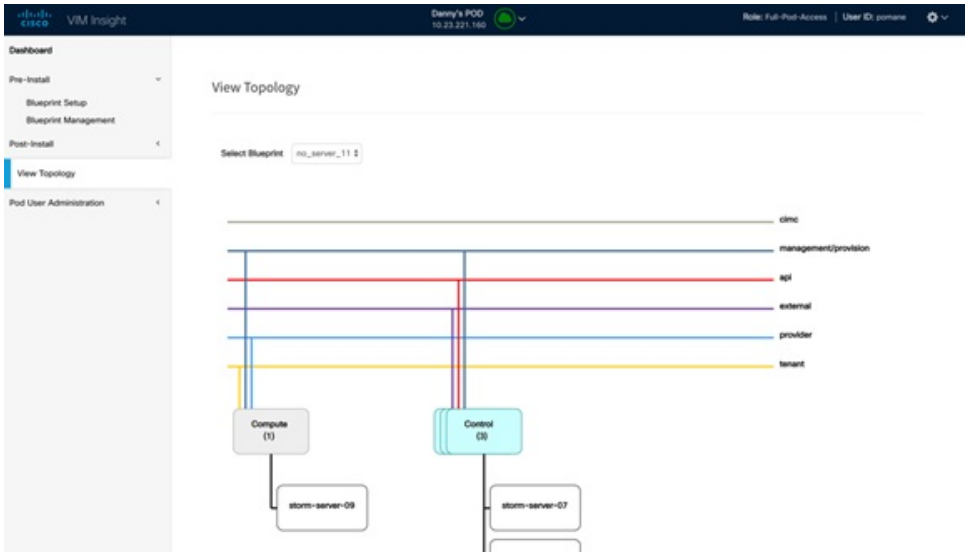
3. **Post-install**.

   This section is active only when a Blueprint is in active state; that is if the install is successful, hence day-n operations are allowed.

4. **Topology**.

   Topology is a logical representation of the Blueprint where it tells the user about the nodes connectivity with the respective networks and hardware information. Topology shows the active blueprints and user can select one among them.

Figure 5: Topology

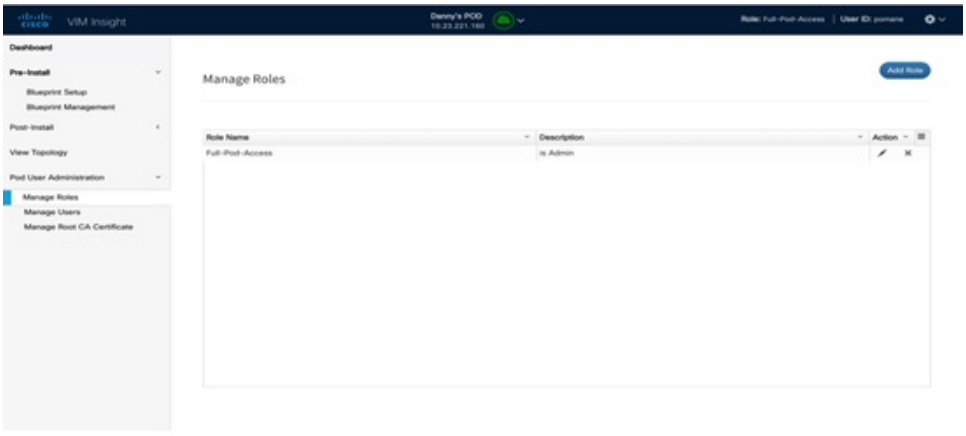


5. **Pod User Administration**

   Pod User Administration menu is available only to admin of the Management Node. This admin can be default admin of the pod or users assigned with Pod Admin role by the default admin. It has two additional sub-panel options:

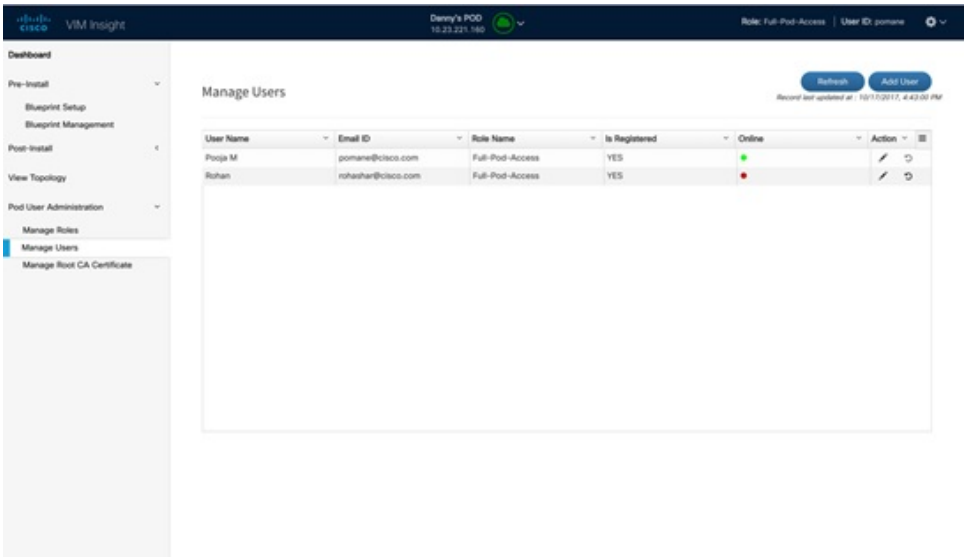
   1. **Manage Roles**:
      1. Add/Edit/Delete Roles.
      2. Permissions to restrict the user access.
      3. Roles provide the granular access to a specific user.
      4. A role cannot be deleted directly if it is associated to an user.

      Figure 6: Manage roles



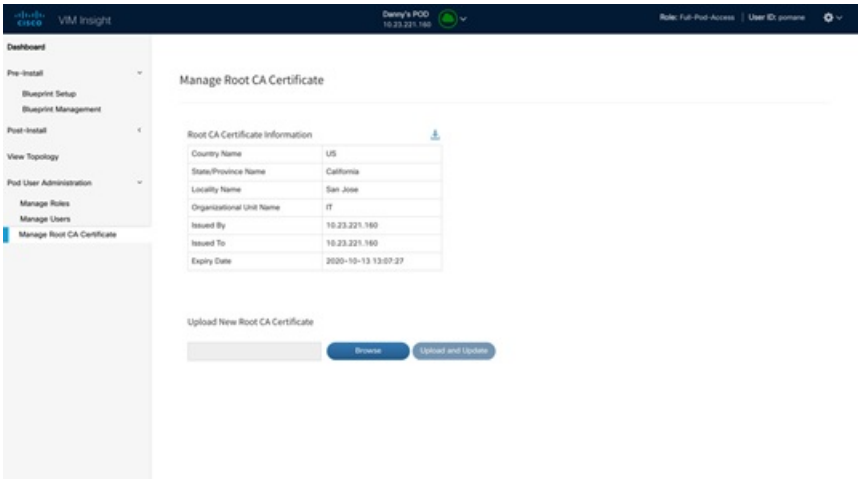
2. **Manage Users**:
   1. Add/Edit/Delete Users.
   2. List User name and Email ID for the users registered in the system.
   3. Roles associated to users.
   4. The current status of the user (Online and Offline user with Green and Red dot respectively).
   5. User registration status.
   6. Refresh button to get latest information about the users status.

   Figure 7: Manage users



3. **Manage Root CA Certificate:**
   1. Edit existing Root CA Certificate of the Management Node (Location: /var/www/mercury/mercury-ca.crt)
   2. You can also download existing certificate from Insight.
   3. If invalid Certificate is uploaded through Insight then previous working state will be recovered after clicking the **Upload** button.
   4. If Certificate is valid Management Node HEALTH check will be executed.

Figure 8: Manage Root CA Certificate



VIM Insight also have some extra features in the header:

1. User ID and Role - Indicates the User ID and Role of the current user.
2. Management Node Context Switching - User can switch between two or more nodes. (Right in the middle for the header).
3. Management Node Name and IP Address: Indicates the name and IP address of the management node.
4. User Profile - User can change the Password or Logout or change log level between Info and Debug.

Context Switching within Insight

One of the key features in VIM Insight, is that if you have permission for the node you can switch between two or more pods. You can be a Admin for one or more pods, and a normal user for some other pod, simultaneously. Ability to access multiple pods, provides the user to maintain context and yet scale from a pod management.

There are two ways that you can switch to another pod:

1. **Context Switching Icon**: Context Switching Icon is located at the middle of the UI header. Click **Management Node Context Switching** to access all available pods.
2. **Switch Between Management Nodes**: Switch Between Management Nodes is situated in the Dashboard. You can navigate to any pod by a single click. If the REST password provided during registration of the Management node does not match the current REST Password for that particular node, the cloud icon at the middle of the UI header will turn red instead of green. The Pod Admin/User can reach out to UI Admin and ask them to update the password for that node from Manage Nodes in Insight UI Admin Portal.

Configuring OpenStack Installation

Before you begin

You need to create a Blueprint (B or C Series) to initiate OpenStack Installation through the VIM.

Step 1 In the **Navigation** pane, choose **Pre-Install** > **Blueprint Setup**.

Step 2 To create a **B Series Blueprint**:

1. On the **Blueprint Initial Setup** page of the Cisco VIM Insight , complete the following fields:

Name	Description
Blueprint Name field	Enter blueprint configuration name.
Platform Type drop-down list	Choose one of the following platform types: • B-Series (By default) choose B series for this section. • C-Series
Tenant Network drop-down list	Choose one of the following tenant network types: • Linuxbridge/VXLAN • OVS/VLAN
Pod Type drop-down list	Choose one of the following pod types: • Fullon(By Default) • Micro • UMHC **Note** UMHC pod type is only supported for OVS/VLAN tenant type. **Note** Pod type micro is supported for OVS/VLAN, ACI/VLAN,VPP/VLAN.
Ceph Mode drop-down list	Choose one of the following Ceph types: • Dedicated • Central (By Default) - Not supported in Production

Name	Description
Optional Features and Services Checkbox	Swiftstack, LDAP, Syslog Export Settings, Install Mode, TorSwitch Information, TLS, Nfvmon, Pod Name, VMTP, Nfvbench, Auto Backup, Heat, Keystone v3, Enable Esc Priv. If any one is selected, the corresponding section is visible in various Blueprint sections. By default all features are disabled except Auto Backup.
Import Existing YAML file	Click **Browse** button to import the existing yaml file. If you have an existing B Series YAML file you can use this feature to upload the file. Insight will automatically fill in the fields and if any mandatory field is missed then it will be highlight it in the respective section.

2. Click **Physical Setup** to navigate to the **Registry Setup configuration** page. Fill in the following details for Registry Setup:

Name	Description
Registry User Name text field	User-Name for Registry **(Mandatory)**.
Registry Password text field	Password for Registry **(Mandatory)**.
Registry Email text field	Email ID for Registry **(Mandatory)**.

Once all mandatory fields are filled the **Validation Check Registry Page** will show a Green Tick.

3. Click **UCSM Common Tab** and complete the following fields:

Name	Description
User name disabled field	By default value is Admin.
Password text field	Enter Password for UCSM Common **(Mandatory)**.
UCSM IP text field	Enter IP Address for UCSM Common(Mandatory).
Resource Prefix text field	Enter the resource prefix**(Mandatory)**.
QOS Policy Type drop-down	Choose one of the following types: • NFVI (Default) • Media

Name	Description
Max VF Count text field	Select the Max VF Count. <1-54> Maximum VF count 54, default is 20. If VF performance is enabled we recommend you to keep MAX_VF_COUNT to 20 else may fail on some VICs like 1240.
Enable VF Performance optional checkbox	Default is false. Set to true to apply adaptor policy at VF level.
Enable Prov FI PIN optional checkbox	Default is false.
MRAID-CARD optional checkbox	Enables JBOD mode to be set on disks. Applicable only if you have RAID controller configured on Storage C240 Rack servers.
Enable UCSM Plugin optional checkbox	Visible when Tenant Network type is OVS/VLAN
Enable QoS Policy optional checkbox	Visible only when UCSM Plugin is enabled. If UCSM Plugin is disabled then this option is set to False.
Enable QOS for Port Profile optional checkbox	Visible only when UCSM Plugin is enabled.
SRIOV Multi VLAN Trunk optional grid	Visible when UCSM Plugin is enabled. Enter the values for network and vlans ranges. Grid can handle all CRUD operations like Add, Delete, Edit and, Multiple Delete.

4. Click **Networking** to advance to the networking section of the Blueprint:

Name	Description
Domain Name field	Enter the domain name **(Mandatory)**.
HTTP Proxy Server field	If your configuration uses an HTTP proxy server, enter the IP address of the server.
HTTPS Proxy Server field	If your configuration uses an HTTPS proxy server, enter the IP address of the server.
IP Tables on Management Pods	Specifies the list of IP Address with Mask.
NTP Server	Enter a maximum of four and minimum of one IPv4 and /or IPv6 addresses in the table.
Domain Name Server	Enter a maximum of three and minimum of one IPv4 and/or IPv6 addresses.

Name	Description
Network table	

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>Network table is pre-populated with segments. To add Networks you can either clear all the table using Delete All or click Edit icon for each segment and fill in the details.

You can add, edit, or delete network information in the table:

• Click + to enter new entries (networks) to the table.

• Specify the following fields in the Edit Entry to Networks dialog box.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>VLAN field</td><td>Enter the VLAN ID.

For Segment - Provider, the VLAN ID value is always "none".</td></tr>
<tr><td>Segment drop-down list</td><td>You can select any one segment from the dropdown list.

• API

• Management/Provision

• Tenant

• CIMC

• Storage

• External

• Provider (optional)

Note Some segments do not need some of the values listed in the preceding points.</td></tr>
<tr><td>Subnet field</td><td>Enter the IPv4 address for the subnet.</td></tr>
<tr><td>IPv6 Subnet field</td><td>Enter IPv6 address. This field will be available only for Management provision and API.</td></tr>
<tr><td>Gateway field</td><td>Enter the IPv4 address for</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>the Gateway.</td></tr>
<tr><td>IPv6 Gateway field</td><td>Enter IPv6 gateway. This field will only available only for Management provision and API network.</td></tr>
<tr><td>Pool field</td><td>Enter the pool information in the required format, for example: 10.30.1.1 or 10.30.1.1 to 10.30.1.12</td></tr>
<tr><td>IPv6 Pool field</td><td>Enter the pool information in the required format, for example: 10.1.1.5-10.1.1.10,10.2.1.5-10.2.1.10
This field is only available for the Mgmt/Provision.</td></tr>
</table>
Click Save.
</td></tr>
</table>

5. On the **Servers and Roles** page of the Cisco VIM Suite wizard, you will see a pre-populated table filled with Roles: Control, Compute and Block Storage (Only if CEPH Dedicated is selected in Blueprint Initial Setup.

Name	Description
Server User Name field	Enter the username of the server.
Disable Hyperthreading	Default value is false. You can set it as true or false.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Cobbler</td><td>Enter the Cobbler details in the following fields:
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Cobbler Timeout field</td><td>The default value is 45 min.
This is an optional parameter. Timeout is displayed in minutes, and its value ranges from 30 to 120.</td></tr>
<tr><td>Block Storage Kickstart field</td><td>Kickstart file for Storage Node.</td></tr>
<tr><td>Admin Password Hash field</td><td>Enter the Admin Password. Password should be Alphanumeric. Password should contain minimum 8 characters and maximum of 32 characters.</td></tr>
<tr><td>Cobbler Username field</td><td>Enter the cobbler username to access the cobbler server.</td></tr>
<tr><td>Control Kickstart field</td><td>Kickstart file for Control Node.</td></tr>
<tr><td>Compute Kickstart field</td><td>Kickstart file for Compute Node.</td></tr>
<tr><td>Cobbler Admin Username field</td><td>Enter the admin username of the Cobbler.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Add Entry to Servers and Roles</td><td>Click Edit or + to add a new server and role to the table.
<table>
<tr><td>Server Name</td><td>Enter a server name</td></tr>
<tr><td>Server Type drop-down list</td><td>Choose Blade or Rack from the drop-down list.</td></tr>
<tr><td>Rack ID</td><td>The Rack ID for the server.</td></tr>
<tr><td>Chassis ID</td><td>Enter a Chassis ID.</td></tr>
<tr><td>If Rack is chosen, the Rack Unit ID field is displayed.</td><td>Enter a Rack Unit ID.</td></tr>
<tr><td>If Blade is chosen, the Blade ID field is displayed.</td><td>Enter a Blade ID.</td></tr>
<tr><td>Select the Role from the drop-down list.</td><td>If Server type is Blade then select Control and Compute. If server is Rack then select Block Storage.</td></tr>
<tr><td>Management IP</td><td>It is an optional field but if provided for one server then it is mandatory to provide details for other Servers as well.</td></tr>
<tr><td>Management IPv6</td><td>Enter the Management IPv6 Address.</td></tr>
</table>
Click Save.</td></tr>
</table>

6. Click **ToR Switch** checkbox in **Blueprint Initial Setup** to enable the **TOR SWITCH** configuration page. It is an **Optional** section in Blueprint Setup but once all the fields are filled it is a part of the Blueprint.

Name	Description
Configure ToR optional checkbox.	Enabling this checkbox, changes the configure ToR section from false to true.

<table>
<tr><th>Name</th><th colspan="3">Description</th></tr>
<tr><td>ToR Switch Information mandatory table.</td><td colspan="3">Click (+) to add information for ToR Switch.<table><tr><th>Name</th><th>Description</th></tr><tr><td>Hostname</td><td>ToR switch hostname.</td></tr><tr><td>Username</td><td>ToR switch username.</td></tr><tr><td>Password</td><td>Tor switch password.</td></tr><tr><td>SSH IP</td><td>ToR switch SSH IP Address.</td></tr><tr><td>SSN Num</td><td>ToR switch ssn num.</td></tr><tr><td>VPC Peer Keepalive</td><td>Peer Management IP. You do not define if there is no peer.</td></tr><tr><td>VPC Domain</td><td>Do not define if peer is absent.</td></tr><tr><td>VPC Peer Port Info</td><td>Interface for vpc peer ports.</td></tr><tr><td>BR Management Port Info</td><td>Management interface of management node.</td></tr><tr><td>BR Management PO Info</td><td>Port channel number for management interface of management node.</td></tr></table>ClickSave.</td></tr>
<tr><td>On clicking save button, Add ToR Info Connected to Fabric field will be visible.</td><td>Port Channel field.</td><td colspan="2">Enter the Port Channel input.</td></tr>
<tr><td></td><td>Switch Name field.</td><td colspan="2">Enter the Port number.</td></tr>
</table>

7. Click **OpenStack Setup** tab to advance to the OpenStack Setup Configuration page.
8. On the **OpenStack Setup** page of the Cisco VIM Insight wizard, complete the following fields:

Name	Description	
HA Proxy	Fill in the following details:	
	External VIP Address field	Enter IP address of External VIP.
	External VIP Address IPv6 field	Enter IPv6 address of External VIP.
	Virtual Router ID field	Enter the Router ID for HA.
	Internal VIP Address IPv6 field	Enter IPv6 address of Internal IP.
	Internal VIP Address field	Enter IP address of Internal VIP.
Keystone	Pre-populated field values. This option would always be true.	
	Admin Username field	admin
	Admin Tenant Name field	admin

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>LDAP (Only if Keystonev3 is enabled)
Note This option is only available with Keystone v3</td><td>This is available only when Keystone v3 and LDAP both are enabled under Optional Features and Services in Blueprint Initial Setup.<table>
<tr><td>Domain Name field</td><td>Enter name for Domain name.</td></tr>
<tr><td>Object Class for Users field</td><td>Enter a string as input.</td></tr>
<tr><td>Object Class for Groupsfield</td><td>Enter a string.</td></tr>
<tr><td>Domain Name Tree for Users field</td><td>Enter a string.</td></tr>
<tr><td>Domain Name Tree for Groups field</td><td>Enter a string.</td></tr>
<tr><td>Suffix for Domain Name field</td><td>Enter a string.</td></tr>
<tr><td>URL field</td><td>Enter a URL with ending port number.</td></tr>
<tr><td>Domain Name of bind user field</td><td>Enter a string.</td></tr>
<tr><td>Password field</td><td>Enter Password as string format.</td></tr>
<tr><td>User Filter field</td><td>Enter filter name as string.</td></tr>
<tr><td>User ID Attribute field</td><td>Enter a string.</td></tr>
<tr><td>User Name Attribute field</td><td>Enter a string.</td></tr>
<tr><td>User Mail Attribute field</td><td>Enter a string.</td></tr>
<tr><td>Group Name Attribute field</td><td>Enter a string.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Neutron</td><td>Neutron fields would change on the basis of Tenant Network Type Selection from Blueprint Initial Setup. Following are the options available for Neutron for OVS/VLAN:
<table>
<tr><td>Tenant Network Type field</td><td>Auto Filled based on the Tenant Network Type selected in the Blueprint Initial Setup page.</td></tr>
<tr><td>Mechanism Drivers field</td><td>Auto Filled based on the Tenant Network Type selected in Blueprint Initial Setup page.</td></tr>
<tr><td>NFV Hosts field</td><td>Auto filled with the Compute you added in Server and Roles.
If you select All in this section NFV_HOSTS: ALL will be added to the Blueprint or you can select one particular compute. For Eg:
NFV_HOSTS: compute-server-1, compute-server-2.</td></tr>
<tr><td>Tenant VLAN Ranges field</td><td>List of ranges separated by comma form start:end.</td></tr>
<tr><td>Provider VLAN Ranges field</td><td>List of ranges separated by comma form start:end.</td></tr>
<tr><td>VM Hugh Page Size (available for NFV_HOSTS option) field</td><td>2M or 1G</td></tr>
<tr><td>Enable Jumbo Frames field</td><td>Enable the checkbox</td></tr>
</table>
For Tenant Network Type Linux Bridge everything remains the same but Tenant VLAN Ranges will be removed.</td></tr>
<tr><td>CEPH</td><td>Ceph has two pre-populated fields
CEPH Mode : By default Dedicated.
NOVA Boot from: Drop Down selection. You can choose Ceph or local.</td></tr>
<tr><td>GLANCE</td><td>By default populated for CEPH Dedicated with Store Backend value as CEPH.</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>CINDER</td><td>By default Populated for CEPH Dedicated with Volume Driver value as CEPH.</td></tr>
<tr><td>VMTP
VMTP optional section will only be visible once VMTP is selected from Blueprint Initial Setup.</td><td>Check one of the check boxes to specify a VMTP network:
• Provider Network
• External Network
For the Provider Network complete the following:
<table>
<tr><td>Network Name field</td><td>Enter the name for the external network.</td></tr>
<tr><td>Subnet field</td><td>Enter the Subnet for Provider Network.</td></tr>
<tr><td>Network IP Start field</td><td>Enter the starting floating IPv4 address.</td></tr>
<tr><td>Network IP End field</td><td>Enter the ending floating IPv4 address.</td></tr>
<tr><td>Network Gatewayfield</td><td>Enter the IPv4 address for the Gateway.</td></tr>
<tr><td>DNS Server field</td><td>Enter the DNS server IPv4 address.</td></tr>
<tr><td>Segmentation ID field</td><td>Enter the segmentation ID.</td></tr>
</table>
For External Network fill in the following details:
<table>
<tr><td>Network Name field</td><td>Enter the name for the external network.</td></tr>
<tr><td>Subnet field</td><td>Enter the Subnet for External Network.</td></tr>
<tr><td>Network IP Start field</td><td>Enter the starting floating IPv4 address.</td></tr>
<tr><td>Network IP End field</td><td>Enter the ending floating IPv4 address.</td></tr>
<tr><td>Network Gateway field</td><td>Enter the IPv4 address for the Gateway.</td></tr>
<tr><td>DNS Server field</td><td>Enter the DNS server IPv4 address.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>TLS This optional section will only be visible once TLS is selected from Blueprint Initial Setup Page.</td><td>TLS has two options:
External LB VIP FQDN - -Text field.
External LB VIP TLS True/False. By default this option is false.</td></tr>
<tr><td>Under the OpenStack setup tab, Vim_admins tab will be visible only when Vim_admins is selected from the Optional Features & Services under the Blueprint Initial setup tab</td><td>Following are the field descriptions for VIM Admins:
User Name - Text field.
Password -Password field. Admin hash password should always start with $6.</td></tr>
<tr><td>SwiftStack optional section will be visible once SwiftStack is selected from Blueprint Initial Setup Page. SwiftStack is only supported with KeyStonev2 . If you select Keystonev3, swiftstack will not be available for configuration.</td><td>Following are the options that needs to be filled for SwiftStack:<table>
<tr><td>Cluster End Point field</td><td>IP address of PAC (proxy-account-container) endpoint.</td></tr>
<tr><td>Admin User field</td><td>Admin user for swift to authenticate in keystone.</td></tr>
<tr><td>Admin Tenant field</td><td>The service tenant corresponding to the Account-Container used by Swiftstack.</td></tr>
<tr><td>Reseller Prefix field</td><td>Reseller_prefix as configured for Keysone Auth,AuthToken support in Swiftstack E.g KEY_</td></tr>
<tr><td>Admin Password field</td><td>swiftstack_admin_password</td></tr>
<tr><td>Protocol</td><td>http or https</td></tr>
</table></td></tr>
</table>

9. If **Syslog Export** or **NFVBENCH** is selected in **Blueprint Initial Setup** Page, the **Services Setup** page will be enabled for the user to view. Following are the options under **Services Setup** Tab:

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Syslog Export</td><td>Following are the options for Syslog Settings:<table>
<tr><td>Remote Host</td><td>Enter Syslog IP address.</td></tr>
<tr><td>Protocol</td><td>Only UDP is supported.</td></tr>
<tr><td>Facility</td><td>Defaults to local5.</td></tr>
<tr><td>Severity</td><td>Defaults to debug.</td></tr>
<tr><td>Clients</td><td>Defaults to ELK.</td></tr>
<tr><td>Port</td><td>Defaults to 514 but can be modified by the User.</td></tr>
</table></td></tr>
<tr><td>NFVBENCH</td><td>NFVBENCH enable checkbox which by default is false.
Add ToR information connected to switch:
Select a TOR Switch and enter the Switch name.
Enter the port number. For example:eth1/5. VTEP VLANS (mandatory and needed only for VXLAN): Enter 2 different VLANs for VLAN1 and VLAN2
NIC Ports: INT1 and INT2 optional input. Enter the 2 port numbers of the 4-port 10G Intel NIC at the management node used for NFVBench.</td></tr>
<tr><td>ENABLE_ESC_PRIV</td><td>Enable the checkbox to set it as True. By default it is False.</td></tr>
</table>

Step 3 To create a **C Series Blueprint**:

1. On the **Blueprint Initial Setup** page of the Cisco VIM Insight, complete the following fields:

Name	Description
Blueprint Name field.	Enter the name for the blueprint configuration.
Platform Type drop-down list	Choose one of the following platform types: • B-Series (By default) • C-Series (Select C Series)

Name	Description
Tenant Network drop-down list	Choose one of the following tenant network types: • Linux Bridge/VXLAN • OVS/VLAN • VTS/VLAN • VPP/VLAN • ACI/VLAN **Note** when VTS/VLAN or ACI/VLAN is selected then respective tabs are available on Blueprint setup.
Pod Type drop-down list	Choose one of the following pod type : • Fullon(By Default) • Micro • UMHC **Note** UMHC pod type is only supported for OVS/VLAN tenant type. **Note** Pod type micro is supported for OVS/VLAN, ACI/VLAN,VPP/VLAN.
Ceph Mode drop-down list	Choose one of the following Ceph types: • Dedicated (By Default) • Central. Central is not supported in Production
Optional and Services Features checkbox	Swiftstack, LDAP, Syslog Export Settings, Install Mode, TorSwitch Information, TLS, NFVMON, Pod Name, VMTP, NFVBench, Autbackup, Heat, Keystone v3, Enable Esc Priv. If any one is selected, the corresponding section is visible in various Blueprint sections. By default all features are disabled except Auto Backup.
Import Existing YAML file	If you have an existing C Series YAML file you can use this feature to upload the file. Insight will automatically fill in the fields and any missed mandatory field will be highlighted in the respective section.

2. Click **Physical Setup** to advance to the **Registry Setup** configuration page. Fill in the following details for Registry Setup:

Name	Description

Registry User Name text field	User-Name for Registry **(Mandatory)**.
Registry Password text field	Password for Registry **(Mandatory)**.
Registry Email text field	Email ID for Registry **(Mandatory)**.

Once all the mandatory fields are filled the **Validation Check Registry Page** will be changed to a Green Tick.

3. Click **CIMC Common Tab** and complete the following fields:

Name	Description
User Name disabled field	By default value is Admin.
Password text field	Enter Password for UCSM Common **(Mandatory)**.

4. Click Networking to advance to the networking section of the Blueprint.

Name	Description
Domain Name field	Enter the domain name. **(Mandatory)**
HTTP Proxy Server field	If your configuration uses an HTTP proxy server, enter the IP address of the server.
HTTPS Proxy Server field	If your configuration uses an HTTPS proxy server, enter the IP address of the server.
IP Tables on Management Pods	Specifies the list of IP Address with Mask.
NTP Servers field	Enter a maximum of four and minimum of one IPv4 and/or IPv6 addresses in the table.
Domain Name Servers field	Enter a maximum of three and minimum of one IPv4 and/or IPV6 addresses.

Name	Description
Networks table	

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>Network table is pre-populated with Segments. To add Networks you can either clear all the table with Delete all or click edit icon for each segment and fill in the details.

You can add, edit, or delete network information in the table.

• Click Add (+) to add new entries (networks) to the table.

• Specify the following fields in the Edit Entry to Networks dialog:

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>VLAN field</td><td>Enter the VLAN ID.

For Segment - Provider, the VLAN ID value is 'none'.</td></tr>
<tr><td>Segment drop-down list</td><td>When you add/edit new segment then following segments types are available in the form of dropdown list and you can select only one.

• API

• Management/provision

• Tenant

• Storage

• External

• Provider

• ACIINFRA

Note Aciinfra segment is available only when ACI/VLAN tenant type is selected) Depending upon the segment some of the entries below are not needed. Please refer to the example file in</td></tr>
</table>
</td></tr>
</table>

Name	Description	
		openstack-configs dir for details.
	Subnet field	Enter the IPv4 address for the subnet.
	IPv6 Subnet field	Enter IPv6 Address. This field will be available only for Management provision and API
	Gateway field	Enter the IPv4 address for the Gateway.
	Gateway IPv6 field	Enter the IPv6 address for the gateway. This will support for API and management provision.
	Pool field	Enter the pool information in the required format, for example: 10.1.1.5-10.1.1.10,10.2.1.5-10.2.1.10 This field is available only for the Mgmt/Provision, Storage, and Tenant segments.
	IPv6 Pool field	Enter the pool information in the required format. For example: 10.1.1.5-10.1.1.10,10.2.1.5-10.2.1.10
	Click **Save**.	

5. On the **Servers and Roles** page of the Cisco VIM Suite wizard, a pre-populated table filled with Roles : Control, Compute and Block Storage (Only if CEPH Dedicated is selected in Blueprint Initial Setup is available.

Name	Description
Server User Name field	Enter the username of the Server.
Disable Hyperthreading	Default value is false. You can set it as true or false.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Cobbler</td><td>Enter the Cobbler details in the following fields:
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Cobbler Timeout field</td><td>The default value is 45 min.
This is an optional parameter. Timeout is displayed in minutes, and its value ranges from 30 to 120.</td></tr>
<tr><td>Block Storage Kickstart field</td><td>Kickstart file for Storage Node.</td></tr>
<tr><td>Admin Password Hash field</td><td>Enter the Admin Password. Password should be Alphanumeric. Password should contain minimum 8 characters and maximum of 32 characters.</td></tr>
<tr><td>Cobbler Username field</td><td>Enter the cobbler username to access the cobbler server.</td></tr>
<tr><td>Control Kickstart field</td><td>Kickstart file for Control Node.</td></tr>
<tr><td>Compute Kickstart field</td><td>Kickstart file for Compute Node.</td></tr>
<tr><td>Cobbler Admin Username field</td><td>Enter the admin username of the Cobbler.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Add Entry to Servers and Roles
Note when Pod type micro is selected then all the three servers will be associated with control, compute and block storage role.
For Example:
Roles
• Block Storage
• -Server 1
• -Server 2
• -Server 3
• Control
• -Server 1
• -Server 2
• -Server 3
• Compute
• -Server 1
• -Server 2
• -Server 3
Note When Pod type UMHC is selected then auto ToR configuration is not supported and the ToR info at server and roles level is not allowed to be entered.</td><td>Click Edit or + to add a new server and role to the table.<table><tr><td>Server Name</td><td>Entry a friendly name.</td></tr><tr><td>Rack ID field</td><td>The rack ID for the server.</td></tr><tr><td>VIC Slot field</td><td>Enter a VIC Slot.</td></tr><tr><td>CIMC IP field</td><td>Enter a IP address.</td></tr><tr><td>CIMC Username field</td><td>Enter a Username.</td></tr><tr><td>CIMC Password field</td><td>Enter a Password for CIMC.</td></tr><tr><td>Select the Role from the drop down list</td><td>Choose Control or Compute or Block Storage from the drop-down list.</td></tr><tr><td>Management IP</td><td>It is an optional field but if provided for one Server then it is mandatory to provide it for other Servers as well.</td></tr><tr><td>Management IPv6</td><td>Routable and valid IPv6 address. It is an optional field but if provided for one server then it is mandatory for all other servers as well.</td></tr></table></td></tr>
<tr><td>Click Save or Add .</td><td>On clicking Save or Add all information related to Servers and Roles gets saved.</td></tr>
<tr><td>If Configure ToR checkbox is Truewith at-least one switch detail, these fields will be displayed for each server and this is similar to DP Tor: Port Channel and Switch Name (Mandatory if Configure ToR is true)</td><td>• Port Channel field
• Switch Name field
• Switch Port Info field</td><td>• Enter the port channel input.
• Enter the switch name.
• Enter the switch port information.</td></tr>
</table>

Name	Description	
DP ToR (Only for Control and Compute) : Mandatory if Intel NIC and Configure TOR is True.	• **Port Channel** field • **Switch Name** field • **Switch Port Info** field	• Enter the port channel input. • Enter the switch name. • Enter the switch port information.
SRIOV TOR INFO (Only for Compute Nodes). It is mandatory in server and roles if Intel NIC and Configure TOR is True. **Switch Name (Mandatory if Configure ToR is true).** This field appears only when Intel NIC support is true, as Auto TOR config is not supported in VIC_NIC combo	• **Switch Name** field • **Switch Port Info** field	• Enter the switch name. • Enter the switch port information.
Intel SRIOV VFS (valid for Intel NIC testbeds) and can be integer.	For SRIOV support for Intel NIC. By Default, SRIOV support is disabled. To enable, define a value in the range # * 1-32 when INTEL_NIC_SUPPORT is set True (X710 Max VFs = 32) # * 1-63 when CISCO_VIC_INTEL_SRIOV is set True (X520 Max VFs = 63)	
INTEL_SRIOV_PHYS_PORTS (valid for Intel NIC test beds) and can be of value 2 or 4 (default is 2)	In some cases the # of Physical SRIOV port needed is 4; to meet that requirement, define the following: # this is optional, if nothing is defined code will assume it to be 2; the only 2 integer values this parameter # takes is 2 or 4 and is true when INTEL_NIC_SUPPORT is True and INTEL_SRIOV_VFS is valid	
Click **Save or Add** .	If all mandatory fields are filled click **Save or Add** to add information on Servers and Roles.	
Disable Hyperthreading	Default value is false. You can set it as true or false.	
Click **Save**		

Note Maximum two ToR info needs to be configured for each connection type on each node (control, compute and block_storage node).

Note If pod type UMHC is selected then CISCO_VIC_INTEL_SRIOV is enabled to be TRUE.

Note For Tenant type **ACI/VLAN,** port channel for each ToR port will not be available in servers and roles, as APIC will automatically assign port-channel numbers.

6. Click **ToR Switch** checkbox in **Blueprint Initial Setup** to enable the **TOR SWITCH** configuration page. It is an **Optional** section in Blueprint Setup but once all the fields are filled in then it will become a part of the Blueprint.

Name	Description
Configure ToR optional checkbox. **Note** If **UMHC** is selected as podtype, configure TOR is not allowed.	Enabling this checkbox, changes the configure ToR section from false to true. **Note** Configure tor is true then ToR switch info maps in servers

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>ToR Switch Information mandatory table if you want to enter ToR information.</td><td>Click (+) to add information for ToR Switch.<table><tr><th>Name</th><th>Description</th></tr><tr><td>Name</td><td>ToR switch name.</td></tr><tr><td>Username</td><td>ToR switch username.</td></tr><tr><td>Password</td><td>ToR switch password.</td></tr><tr><td>SSH IP</td><td>ToR switch SSH IP.</td></tr><tr><td>SSN Num</td><td>ToR switch ssn num.</td></tr><tr><td>VPC Peer Keepalive</td><td>Peer Management IP. You cannot define if there is no peer.</td></tr><tr><td>VPC Domain</td><td>Cannot define if there is no peer.</td></tr><tr><td>VPC Peer Port Info</td><td>Interface for vpc peer ports.</td></tr><tr><td>VPC Peer VLAN Info</td><td>VLAN ids for vpc peer ports (optional).</td></tr><tr><td>BR Management Port Info</td><td>Management interface of build node.</td></tr><tr><td>BR Management PO Info</td><td>Port channel number for management interface of build node.</td></tr><tr><td>BR Management VLAN info</td><td>VLAN id for management interface of build node (access).</td></tr></table></td></tr>
<tr><td colspan="2">Click Save.</td></tr>
</table>

Note When tenant type ACI/VLAN is selected, the TOR switch information table differs and is mandatory.

Name	Description
Configure ToR optional checkbox. **Note** If **UMHC** is selected as podtype, configure TOR is not allowed.	Enabling this checkbox, changes the configure ToR section from false to true. **Note** Configure tor is true then ToR switch info maps in servers

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>ToR Switch Information mandatory table if you want to enter ToR information.</td><td>Click (+) to add information for ToR Switch.<table>
<tr><td>Name</td><td>Description</td></tr>
<tr><td>Name</td><td>ToR switch name.</td></tr>
<tr><td>Username</td><td>ToR switch username.</td></tr>
<tr><td>Password</td><td>ToR switch password.</td></tr>
<tr><td>SSH IP</td><td>ToR switch SSH IP.</td></tr>
<tr><td>SSN Num</td><td>ToR switch ssn num.</td></tr>
<tr><td>VPC Peer Keepalive</td><td>Peer Management IP. You cannot define if there is no peer.</td></tr>
<tr><td>VPC Domain</td><td>Cannot define if there is no peer.</td></tr>
<tr><td>VPC Peer Port Info</td><td>Interface for vpc peer ports.</td></tr>
<tr><td>VPC Peer VLAN Info</td><td>VLAN ids for vpc peer ports (optional).</td></tr>
<tr><td>BR Management Port Info</td><td>Management interface of build node.</td></tr>
<tr><td>BR Management PO Info</td><td>Port channel number for management interface of build node.</td></tr>
<tr><td>BR Management VLAN info</td><td>VLAN id for management interface of build node (access).</td></tr>
</table></td></tr>
<tr><td colspan="2">Click Save.</td></tr>
</table>

Note When the Tenant type ACI/VLAN is selected, the ToR switch information table differs and is mandatory.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Configure ToR</td><td>Is not checked, as by default ACI will configure the ToRs
<table>
<tr><td>Host Name</td><td>ToR switch name.</td></tr>
<tr><td>VPC Peer keep alive</td><td>Enter Peer must be exist pair.</td></tr>
<tr><td>VPC Domain</td><td>Enter an integer.</td></tr>
<tr><td>BR management port info</td><td>Enter BR management port info eg. Eth1/19 ,atleast one pair to be exist.</td></tr>
<tr><td>Enter Node ID</td><td>Entered integer must be unique.</td></tr>
</table></td></tr>
</table>

Note If TOR_TYPE is selected as NCS-5500, the TOR switch information table differs and is mandatory.

Name	Description
Configure ToR optional checkbox **Note** If **NSC-5500** is selected as TOR_TYPE, configure TOR is set as mandatory.	Enabling this checkbox, changes the configure ToR section from false to true. **Note** Configure TOR is true then ToR switchinfo maps in servers.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>If you want to enter Fretta details fill in the NCS-5500 Information table.</td><td>Click (+) to add information for Fretta Switch.
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Name</td><td>Enter the NCS-5500 hostname.</td></tr>
<tr><td>User Name</td><td>Enter the NCS-5500 username.</td></tr>
<tr><td>Password</td><td>Enter the NCS-5500 password.</td></tr>
<tr><td>SSH IP</td><td>Enter the NCS-5500 ssh IP Address.</td></tr>
<tr><td>VPC Peer Link</td><td>Peer management IP.</td></tr>
<tr><td>BR Management PO Info</td><td>Port channel number for management interface of build node.</td></tr>
<tr><td>BR Management VLAN info</td><td>VLAN id for management interface of build node (access).</td></tr>
<tr><td>VPC Peer Port Info</td><td>Interface for vpc peer ports.</td></tr>
<tr><td>VPC Peer Port Address</td><td>Address for ISIS exchange.</td></tr>
<tr><td>ISIS Loopback Interface address</td><td>ISIS loopack IP Address.</td></tr>
<tr><td>ISIS net entity title</td><td>Enter a String.</td></tr>
<tr><td>ISIS prefix SID</td><td>Integer between 16000 to 1048575.</td></tr>
</table></td></tr>
</table>

When TOR-TYPE selected as NCS-5500 and 2 NCS-5500 are configured it is mandatory to configure MULTI_SEGMENT_ROUTING_INFO

Name	Description
BGP AS Number field	Integer between 1 to 65535.
ISIS Area Tagfield	A valid string.
Loopback Interface namefield	Loopback Interface name.
API bundle IDfield	Integer between 1 to 65535.

Name	Description
API bridge domain field	String (Optional, only needed when br_api of mgmt node is also going through NCS-5500; this item and api_bundle_id are mutually exclusive).
EXT bridge domain field	A valid string (user pre-provisions physical, bundle interface, sub-interface and external BD for external uplink and provides external BD info setup_data).

7. Click **OpenStack Setup** Tab to advance to the **OpenStack Setup** Configuration page.
8. On the **OpenStack Setup** Configuration page of the Cisco VIM Insight wizard, complete the following fields:

Name	Description	
HA Proxy	Fill in the following details:	
	External VIP Address field	Enter IP address of External VIP.
	External VIP Address IPv6 field	Enter IPv6 address of External VIP.
	Virtual Router ID field	Enter the Router ID for HA.
	Internal VIP Address IPv6 field	Enter IPv6 address of Internal IP.
	Internal VIP Address field	Enter IP address of Internal VIP.
Keystone	Mandatory fields are pre-populated.	
	Admin User Name	admin.
	Admin Tenant Name	admin.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>LDAP</td><td>LDAP enable checkbox which by default is false, if LDAP is enabled on keystone.
<table>
<tr><td>Domain Name field</td><td>Enter name for Domain name.</td></tr>
<tr><td>Object Class for Users field</td><td>Enter a string as input.</td></tr>
<tr><td>Object Class for Groupsfield</td><td>Enter a string.</td></tr>
<tr><td>Domain Name Tree for Users field</td><td>Enter a string.</td></tr>
<tr><td>Domain Name Tree for Groups field</td><td>Enter a string.</td></tr>
<tr><td>Suffix for Domain Name field</td><td>Enter a string.</td></tr>
<tr><td>URL field</td><td>Enter a URL with ending port number.</td></tr>
<tr><td>Domain Name of Bind User field</td><td>Enter a string.</td></tr>
<tr><td>Password field</td><td>Enter Password as string format.</td></tr>
<tr><td>User Filter field</td><td>Enter filter name as string.</td></tr>
<tr><td>User ID Attribute field</td><td>Enter a string.</td></tr>
<tr><td>User Name Attribute field</td><td>Enter a string.</td></tr>
<tr><td>User Mail Attribute field</td><td>Enter a string.</td></tr>
<tr><td>Group Name Attribute field</td><td>Enter a string.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Neutron</td><td>Neutron fields would change on the basis of Tenant Network Type Selection from Blueprint Initial Setup. Following are the options available for Neutron for OVS/VLAN:
<table>
<tr><td>Tenant Network Type field</td><td>Auto Filled based on the Tenant Network Type selected in the Blueprint Initial Setup page.</td></tr>
<tr><td>Mechanism Drivers field</td><td>Auto Filled based on the Tenant Network Type selected in Blueprint Initial Setup page.</td></tr>
<tr><td>NFV Hosts field</td><td>Auto filled with the Compute you added in Server and Roles.
If you select All in this section NFV_HOSTS: ALL will be added to the Blueprint or you can select one particular compute. For Eg:
NFV_HOSTS: compute-server-1, compute-server-2.</td></tr>
<tr><td>Tenant VLAN Ranges field</td><td>List of ranges separated by comma form start:end.</td></tr>
<tr><td>Provider VLAN Ranges field</td><td>List of ranges separated by comma form start:end.</td></tr>
<tr><td>VM Hugh Page Size (available for NFV_HOSTS option) field</td><td>2M or 1G</td></tr>
<tr><td>Enable Jumbo Frames field</td><td>Enable the checkbox</td></tr>
</table>
For Tenant Network Type Linux Bridge everything remains the same but Tenant VLAN Ranges will be removed.</td></tr>
<tr><td>CEPH</td><td>Ceph has two pre-populated fields:
• CEPH Mode : By default Dedicated.
• NOVA Boot: From drop down selection you can choose Ceph or local.</td></tr>
<tr><td>GLANCE</td><td>By default Populated for CEPH Dedicated with Store Backend value as CEPH.</td></tr>
<tr><td>CINDER</td><td>By default Populated for CEPH Dedicated with Volume Driver value as CEPH.</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>VMTP optional section, this will be visible only if VMTP is selected from Blueprint Initial Setup. For VTS tenant type Provider network is only supported.</td><td>Check one of the check boxes to specify a VMTP network:
• Provider Network
• External Network

For the Provider Network complete the following:
<table><tr><td>Network Name field</td><td>Enter the name for the external network.</td></tr><tr><td>Subnet field</td><td>Enter the Subnet for Provider Network.</td></tr><tr><td>Network IP Start field</td><td>Enter the starting floating IPv4 address.</td></tr><tr><td>Network IP End field</td><td>Enter the ending floating IPv4 address.</td></tr><tr><td>Network Gatewayfield</td><td>Enter the IPv4 address for the Gateway.</td></tr><tr><td>DNS Server field</td><td>Enter the DNS server IPv4 address.</td></tr><tr><td>Segmentation ID field</td><td>Enter the segmentation ID.</td></tr></table>For External Network fill in the following details:
<table><tr><td>Network Name field</td><td>Enter the name for the external network.</td></tr><tr><td>IP Start field</td><td>Enter the starting floating IPv4 address.</td></tr><tr><td>IP End field</td><td>Enter the ending floating IPv4 address.</td></tr><tr><td>Gateway field</td><td>Enter the IPv4 address for the Gateway.</td></tr><tr><td>DNS Server field</td><td>Enter the DNS server IPv4 address.</td></tr><tr><td>Subnet field</td><td>Enter the Subnet for External Network.</td></tr></table></td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>TLS optional section, this will be visible only if TLS is selected from Blueprint Initial Setup Page.</td><td>TLS has two options:
External LB VIP FQDN - Text Field.
External LB VIP TLS - True/False. By default this option is false.</td></tr>
<tr><td>SwiftStack optional section will be visible only if SwiftStack is selected from Blueprint Initial Setup Page. SwiftStack is only supported with KeyStonev2. If you select Keystonev3, swiftstack will not be available to configure.</td><td>Following are the options that needs to be filled for SwiftStack:<table>
<tr><td>Cluster End Point</td><td>IP address of PAC (proxy-account-container) endpoint.</td></tr>
<tr><td>Admin User</td><td>Admin user for swift to authenticate in keystone.</td></tr>
<tr><td>Admin Tenant</td><td>The service tenant corresponding to the Account-Container used by Swiftstack.</td></tr>
<tr><td>Reseller Prefix</td><td>Reseller_prefix as configured for Keysone Auth,AuthToken support in Swiftstack E.g KEY_</td></tr>
<tr><td>Admin Password</td><td>swiftstack_admin_password</td></tr>
<tr><td>Protocol</td><td>http or https</td></tr>
</table></td></tr>
</table>

Note When the Tenant type ACI/VLAN is selected then ACIINFO tab is available in blueprint setup.

Note When ACI/VLAN is selected then ToR switch from initial setup is mandatory.

Name	Description
APIC Hosts field	Enter host input. Example: <ip1|host1>:[port] . max of 3, min of 1, not 2;
apic_username field	Enter a string format.
apic_password filed	Enter Password.
apic_system_id field	Enter input as string. Max length 8.
apic_resource_prefix field	Enter string max length 6.
apic_tep_address_ pool field	Allowed only 10.0.0.0/16
multiclass_address_pool field	Allowed only 225.0.0.0/15
apic_pod_id field	Enter integer(1- 65535)
apic_installer_tenant field	Enter String, max length 32
apic_installer_vrf field	Enter String, max length 32
api_l3out_network field	Enter String, max length 32

Note

Name	Description
VTS Day0 (checkbox)	True or false default is false.
VTS User name	Enter as string does not contain special characters.
VTS Password	Enter password
VTS NCS IP	Enter IP Address format.
VTC SSH Username	Enter a string
VTC SHH Password	Enter password

When Tenant Type is VTS/VLAN then VTS tab is available in blueprint setup.

Note If vts day0 is enabled then SSH username and SSH password is mandatory.

If SSH_username is input present then SSH password is mandatory vice-versa

9. If **Syslog Export** or **NFVBENCH** is selected in **Blueprint Initial Setup** Page, then **Services Setup** page will be enabled for user to view. Following are the options under **Services Setup** Tab:

Name	Description
Syslog Export	Following are the options for Syslog Settings: **Remote Host**: Enter Syslog IP Address. **Protocol**: Supports only UDP. **Facility**: Defaults to local5. **Severity**: Defaults to debug. **Clients**: Defaults to ELK. **Port**: Defaults to 514 but can be modified by the User.
NFVBENCH	**NFVBENCH enable checkbox** by default is**false**. Add ToR information connect to Switch: • Select a TOR Switch and enter the Switch name. • Enter the port number. For Example: eth1/5 . VTEP VLANS (mandatory and needed only for VTS/VXLAN,): Enter 2 different VLANs for VLAN1 and VLAN2. • NIC Ports: INT1 and INT2 optional input. Enter the 2 port numbers of the 4-port 10G Intel NIC at the management node used for NFVBench.
ENABLE_ESC_PRIV	Enable the checkbox to set it as True. By default it is **False**.

Step 4 Click **Offlinevalidation**, to initiate an offline validation of the Blueprint.

Step 5 Blueprint can also be created using an **Upload functionality**:

- In Blueprint Initial Setup.
- Click **Browse** in the blueprint initial setup.
- Select the YAML file you want to upload.
- Click **Select** button.
- Clicking on load button in the Insight UI Application. All the fields present in the YAML file would be uploaded to the respective fields in UI.
- Enter the name of the Blueprint (Make sure you enter unique name while saving Blueprints. There would be no two Blueprints with same name.)
- Click **Offline Validation**.
- If all the mandatory fields in the UI are populated, then Offline Validation of the Blueprint will start else a pop up would be visible which will inform which section of Blueprint Creation has a missing information error.
- On Validation Success of Blueprint **Save Blueprint** button will be enabled with **Cancel** button
- A pop up will be generated asking to initiate the deployment with **Blueprint Name** and the stages you need to run.

On Validation Failure of Blueprint **Cancel** button will be enabled.

Once the **Offlinevalidation** is successful, **Save** option will be enabled which will redirect you to the Blueprint Management Page.

The wizard advances to the Blueprint Management page. On the Blueprint Management page you can select the recently added Inactive Blueprint and click **Install** button which is disabled by default.

A pop up will be generated asking to initiate the deployment with **Blueprint Name** and the stages you need to run.

By default all stages are selected but you can also do an incremented install.

In case of Incremented Install you should select stages in the order. For Example: If you select **Validation Stage** then the 2nd stage Management Node Orchestration will be enabled. You cannot skip stages and run a deployment.

Once you click **Proceed** the Cloud Deployment would be initiated and the progress can be viewed from "Dashboard".

Note Once the Blueprint is in **Active** State, the **Post-Install** features listed in Navigation Bar will changed to **Active** stage.

Post Installation Features for Active Blueprint

This option is only available to a pod, which is successfully deployed. There are multiple sub-links available to manage the day-n operation of the pod. However, in many cases, Insight cross-launches the relevant services, thereby delegating the actual rendering to the individual services.

Monitoring the Pod

VIM 2.2 uses ELK (elasticsearch, logstash and Kibana) to monitor the OpenStack services, by cross-launching the Kibana dashboard.

To cross launch Kibana, complete the following instructions:

Step 1 In the **Navigation** pane, click **POST-Install** > **Monitoring**.
The **Authentication Required** browser pop up is displayed.

Step 2 Enter the **username** as admin.

Step 3 Enter the ELK_PASSWORD password obtained from /root/installer-<tagid>/openstack-configs/secrets.yaml in the management node.
Kibana is launched in an I-Frame

Note Click **Click here to view Kibana logs in new tab** link to view Kibana Logs in a new tab.

Cross Launching Horizon

Horizon is the canonical implementation of Openstack's Dashboard, which provides a web based user interface to OpenStack services including Nova, Swift and, Keystone.

Step 1 In the Navigation pane, click **Post-Install** > **Horizon**.

Step 2 Click **Click here to view Horizon logs in new tab**.
You will be redirected to Horizon landing page in a new tab.

NFVI Monitoring

NFVI monitoring is a Cross launch browser same as Horizon. NFVI monitoring link is available in the post install only if the setupdata has NFVI Monitoring configuration during the cloud deployment which basically pings the monitoring and checks status of **Collector VM1 Info** and **Collector VM2 Info**.

Step 1 In the **Navigation**pane, click **Post-Install** >**NFVI monitoring**.

Step 2 Click the link **Click here to view NFVI monitoring.**.

You will be redirected to NFVI monitoring page

Run VMTP

Run VMTP is divided in two sections:

- **Results for Auto Run**: This will show the results of VMTP which was run during cloud deployment (Blueprint Installation).
- **Results for Manual Run**: Here you have an option to run the VMTP on demand. To run VMTP on demand just click **Run VMTP** button.

Note If VMTP stage was skipped/not-run during Blueprint Installation, this section of POST Install would be disabled for the user.

Run CloudPulse

Endpoints Tests:

1. cinder_endpoint
2. glace_endpoint
3. keystone_endpoint
4. nova_endpoint
5. neutron_endpoint
6. all_endpoint_tests

Operator Tests:

1. rabbitmq_check
2. galera_check
3. ceph_check
4. node_check
5. docker_check
6. all_operator_tests

Run NFV Bench

One can **Run NFV Bench** for **B**and**C** series Pod, through Cisco VIM Insight. On a pod running with CVIM 2.2, click on the NFVBench link on the NAV-Menu.

You can run either fixed rate test or NDR/PDR test. As the settings and results for the test types differ, the options to run these tests are presented in two tabs, with its own settings and results .

NDR/PDR Test

Step 1 Log-in to **CISCO VIM Insight**.

Step 2 In the **Navigation** pane, click **Post-Install** >**Run NFV Bench.**

Step 3 Click on NDR/PDR test and complete the following fields

Name	Description
Iteration Duration	Select duration from 10 to 60 sec. Default is 20 sec
Frame Size	Select the correct frame size to run
Run NDR/PDR test	Click on Run NDR/PDR test. Once NDR/PDR test is finished it will display each type of test with its own settings and results.

Fixed Rate Test

Step 1 Log-in to **CISCO VIM Insight**.

Step 2 In the **Navigation** pane, click **Post-Install >Run NFV Bench.**

Step 3 Click Fixed rate test and complete the following fields.

Name	Description
Rate	Rate: Select right configuration pps or bps from drop down-list and enter values : For pps: minimum: 2500pps; maximum: 14500000pps (=14.5Mpps); default: 1000000pps (=1Mpps) For bps: minimum: 1400000bps; maximum: 10000000000bps (=10Gbps); default: 1000000000 (=1Gbps)
Iteration Duration	Select duration from 10-60Sec. Default is 20sec.
Frame Size	Select the right frame size(64,IMIX,1518) to run.
Run Fixed rate test	Click on Run Fixed rate test. Once Fixed rate test is finished it will display each type of test with its own settings and results.

POD Management

One of the key aspects of Cisco VIM is that it provides the ability for the admin to perform pod life-cycle management from a hardware and software perspective. Nodes of a given pod corrupts at times and VIM provides the ability to add, remove or replace nodes, based on the respective roles with some restrictions. Details of pod management will be listed in the admin guide, however as a summary the following operations are allowed on a running pod:

Step 1 **Add or Remove Storage Nodes**: You can add one node at a time, given that we run Ceph as a distributed storage offering.

Step 2 **Add or Remove Computes Nodes**: N-computes nodes can be replaced simultaneously; however at any given point, at least one compute node should be active.

Step 3 **Replace Control Nodes**: We do not support double fault scenarios, replacement of one controller at a time is supported.

System Update

As part of the lifecycle management of the cloud, VIM has the ability to bring in patches (bug fixes related to code, security, etc.), thereby providing the additional value of seamless cloud management from software perspective. Software update of the cloud is achieved by uploading a valid tar file following initiation of a System Update from the Insight as follows:

Step 1 In the Navigation pane, click **Post-Install** > **System Update**.

Step 2 Click **Browse** button.

Step 3 Select the valid tar file.

Step 4 Click **Open** > **Upload and Update** .

Message stating System Update has been initiated will be displayed. Logs front-ended by hyperlink would be visible in the section below before Update Logs to help see the progress of the update. During the software update, all other pod management activities will be disabled. Post-update, normal cloud management will commence.

Reconfiguring CIMC Password through Insight

Update the cimc_password in the CIMC-COMMON section, and/or the individual cimc_password for each server and then run the update password option.

To update a password, you need to follow the password rules:

- Must contain at least one lower case letter.
- Must contain at least one upper case letter.
- Must contain at least one digit between 0 to 9.
- One of these special characters !$#@%^-_+=*&
- Your password has to be 8 to 14 characters long.

Before you begin

You must have a C-series pod up and running with Cisco VIM to reconfigure CIMC password.

Note Reconfigure CIMC password section would be disabled if the pod is in failed state as indicated by ciscovim install-status.

Step 1 Log-in to **CISCO VIM Insight**.

Step 2 In the navigation pane, select **Post-Install**

Step 3 Click **Reconfigure CIMC Password**.

Step 4 On the Reconfigure CIMC Password page of the Cisco VIM Insight, complete the following fields:

Name	Description
CIMC_COMMON old Password	**CIMC_COMMON** old password field cannot be edited.
CIMC-COMMON new Password	Enter new **CIMC-COMMON** password. Password should be alphanumeric according to the password rule.
Click **Update Password**	Old **CIMC-COMMON** password will be updated with new **CIMC-COMMON** password.

Reconfiguring OpenStack Password

Cisco VIM has been designed with security to accommodate customers' password policy.

There are two options to regenerate the Password:

1. **Regenerate all passwords**: Click the checkbox of **Regenerate all passwords** and click **Set Password**. This will automatically regenerate all passwords in alphanumeric format.
2. **Regenerate single or more password**: If user wants to set a specific password for any service like Horizon's ADMIN_USER_PASSWORD they can add it by doing an inline edit. Double click on the filed under Password and then enter the password which will enable **Set Password** button.

Note During the reconfiguration of password, all other pod management activities will be disabled. Post-update, normal cloud management will commence.

Reconfiguring OpenStack Services, TLS certs and ELK configurations

Cisco VIM supports the reconfiguration of OpenStack log level services, TLS certificates, and ELK configuration. Listed below are the steps to reconfigure the OpenStack and other services:

Step 1 In the **Navigation** pane, click **Post-Install** > **Reconfigure OpenStack Config**.

Step 2 Click on the specific item to be changed and updated; For TLS certificate it is the path to certificate location.

Step 3 Enter **Set Config** and the process will commence.

During the reconfiguration process, all other pod management activities will be disabled. Post-update, normal cloud management will commence.

Reconfiguring Optional Services

Cisco VIM offers optional services such as heat, migration to Keystone v3, NFVBench, NFVIMON and so on, that can be enabled as post-pod deployment. Optional services can be un-configured as post-deployment in 2.2 feature. These services can be enabled in one-shot or selectively. Listed below are the steps to enable optional services:

Step 1 In the **Navigation** pane, click **Post-Install** > **Reconfigure Optional Services**.

Step 2 Choose the right service and update the fields with the right values.

Step 3 Enter **Reconfigure** to commence the process.

During the reconfiguration process, all other pod management activities will be disabled. Post-update, normal cloud management will commence. Once reconfigure is initiated than optional feature would be updated in active blueprint. If reconfigure of Optional Services fail in the time of reconfigure process then it is advised to contact CiscoTAC to resolve the situation through CLI.

Note All reconfigure operation feature contains repeated deployment true or false.

- Repeated re-deployment true - Feature can be re-deployed again.
- Repeated re-deployment false- Deployment of feature allowed only once.

Deployment Status :

Optional Features	Repeated re-deployment Options
APICINFO	True
EXTERNAL_LB_VIP_FQDN	False
EXTERNAL_LB_VIP_TLS	False
INSTALL_MODE	True
LDAP	True
NETWORKING	True
NFVBENCH	False
NFVIMON	False
PODNAME	False
PROVIDER_VLAN_RANGES	True
SWIFTSTACK	True
SYSLOG_EXPORT_SETTINGS	False
TENANT_VLAN_RANGES	True
TORSWITCHINFO	False
VIM _ ADMINS	True
VMTP	False
VTS_PARAMETERS	False
AUTOBACKUP	` True
Heat	False
Keystone v3	False
HTTP Proxy Server	True

Optional Features	Repeated re-deployment Options
HTTPS Proxy Server	True

Pod User Administration

Cisco VIM Insight offers Users (Pod Admin(s) or Pod Users) to manage Users and roles associated with them.

Managing Users

To add new User

Step 1 Click **Login as POD User**.

Step 2 Navigate to **POD User Administration**.

Step 3 Click **Manage Users**.

Step 4 Click **Add Users** to add a new user.

Step 5 Complete the following fields in the **Add Users** page of the Cisco VIM Insight:

Field Name	Field Description
Email ID	Enter the Email ID of the User.
User Name	Enter the User Name if the User is new. If the User is already registered to the Insight the User-Name gets auto-populated.
Role	Select the Role from the drop-down list.

Step 6 Click **Save**.

Managing Roles

To create a new Role

Step 1 Click **Login as POD User.**

Step 2 Navigate to **Pod User Administration** and click **Manage Roles**. By default you will see full-pod-access role in the table.

Step 3 Click **Add Role** to create a new role.

Step 4 Complete the following fields in the **Add Roles** page in Cisco VIM Insight:

Field Name	Field Description
Role	Enter the name of the role.
Description	Enter the description of the role.

Field Name	Field Description
Permission	Check the **Permission** checkbox to select the permission.

Step 5 Click **Save**. Once the Blueprint is in Active state all the permissions are same for C-series and B-series Pods other than Reconfigure CIMC Password which is missing for B-series Pod.

Note Permissions are divided in granular level where viewing **Dashboard** is the default role that is implicitly added while creating a role.

Managing Root CA Certificate

You can update the CA Certificate during the registration of the POD. Once, logged in as POD User and if you have the permission to update the certificate you can view under POD User Administration>> Manage Root CA Certificate.

To update the Certificate:

Step 1 Click **Login as POD User**

Step 2 Navigate to **POD User Administration>>Manage Root CA certificate**.

Step 3 Click **Browse** and select the certificate that you want to upload.

Step 4 Click **Upload.**

- If the certificate is Invalid, and does not matches with the certificate on the management node located at (var/www/mercury/mercury-ca.crt) then Insight will revert the certificate which was working previously.
- If the Certificate is valid, Insight will run a management node health check and then update the certificate with the latest one.

Note The CA Certificate which is uploaded should be same as the one which is in the management node.