Managing Blueprints

The following topics tell you how to manage Cisco NFVI Blueprints.

- Blueprints, page 1
- Creating a Blueprint for B-Series Server Platform, page 2
- Creating a Blueprint for C-Series Server Platform, page 17
- Creating a Blueprint using Upload Functionality , page 32
- Managing Post Install Features , page 35

Blueprints

Blueprints contain the configuration metadata required to deploy an OpenStack system through a Cisco VIM pod in Cisco VIM Insight. You can create a blueprint in Cisco Insight or you can upload a yaml file that contains the metadata for a blueprint. You can also create a blueprint from an existing OpenStack system that you are configuring as a Cisco VIM pod.

The configuration in the blueprint is specific to the type of Cisco UCS server that is in the OpenStack system. A blueprint for a C-Series server-based OpenStack system cannot be used to configure a B-Series server-based OpenStack system. Cisco Insight will display an error if the blueprint does not match the configuration of the OpenStack system.

The blueprint enables you to quickly change the configuration of an OpenStack system. While only one blueprint can be active, you can create or upload multiple blueprints for a Cisco VIM pod. If you change the active blueprint for a pod, you update the configuration of the OpenStack system to match the new blueprint.

You can modify and validate an existing blueprint, or delete a blueprint. However, you cannot modify any of the configuration metadata in the active blueprint for a Cisco VIM pod.

Blueprint Activation

A blueprint becomes active when you use it in a successful installation for a Cisco VIM pod. Any other blueprints that you created or uploaded to that pod are in non-active state.

Uploading or creating a blueprint does not activate that blueprint for the pod. You need to install a blueprint through the **Cisco VIM Suite** wizard. If the installation is successful, the selected blueprint becomes active.

Note If you want to activate a new blueprint in an existing pod, you need to delete certain accounts and the credential policies for that pod before you activate the blueprint. See Activating a Blueprint in an Existing Pod with OpenStack Installed, on page 33.

Viewing Blueprint Details

You can view the details of an OpenStack installation blueprint. To view blueprint details:

Step 1 Log in to Cisco VIM Insight as pod User.
Step 2 In the Dashboard's Switch between Management Nodes, select the Cisco VIM pod with the blueprint that you want to view.
Step 3 Click **Menu** button at the top left corner to expand the navigation pane.
Step 4 Choose **Pre-Install** > **Blueprint Management.**
Step 5 Choose a blueprint from the list.
Step 6 Click **Preview & Download YAML.**

Creating a Blueprint for B-Series Server Platform

Typically, you create the blueprint when you create the Cisco VIM pod. Follow the instructions below to create an additional blueprint for a pod that uses B-Series servers.

Before You Begin

Create a Cisco VIM Insight User Account and Register the respective Pod.

Step 1 Log-in to Cisco VIM Insight.
Step 2 In the **Navigation** pane, expand the **Pre-Install Section**.
Step 3 Click **Blueprint Setup**.
Step 4 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	• B-Series (By Default) • C-Series

Name	Description
Tenant Network drop-down list	Choose one of the following tenant network types: • Linux Bridge/VXLAN • OVS/VLAN
Ceph Mode drop-down list	Choose one of the following Ceph types: • Dedicated • Central (By Default) (not supported in production)
Pod Type drop-down list	Fullon (By default).
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, etc. If any one is selected, the corresponding section is visible in various Blueprint sections. By default all options are disabled.
Import Existing YAML field	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 fields are missed then the respective section will be highlighted.

Step 5 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 mandatory fields are filled the **Validation Check Registry** page will be changed to a Green Tick.

Step 6 Click **UCSM Common** tab and fill the following fields:

Name	Description
User name disabled field	By default value is admin.

Name	Description
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 list	Choose one of the following types: • NFVI (Default) • Media
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/VLA.
Enable QoS Policy optional checkbox	Visible only when UCSM Plugin is enabled. If UCSM Plugin is disabled then this option will be set to False.
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.

Step 7 Click **Networking** to advance to the networking section of the Blueprint.

Name	Description
Domain Name field	Enter the domain name (Mandatory).
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.
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.

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 Edit to enter new entries (networks) to the table.
• Specify the following fields in the Edit Entry to Networks dialog:
<table><tr><td>Segment drop-down list</td><td>You can select any of one segment from dropdown list
• API
• Management Provision
• Tenant
• CIMC
• Storage
• External
• Provider (optional)
Note Depending upon the segment not all entries listed below are needed</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>VALN field</td><td>Enter the VLAN ID. For Segment - Provider, the VLAN ID value is always none.</td></tr><tr><td>Subnet ID field.</td><td>Enter the IPv4 address for the subnet.</td></tr><tr><td>Gateway field</td><td>Enter the IPv4 address for the Gateway.</td></tr></table></td></tr>
</table>

Name	Description
	IPv6 Gateway field: Enter IPv6 gateway. This field is only available for the Mgmt Provision and API Segments. **Pool** field: Enter the pool information in the required format: Example: 10.30.1.1 or 10.30.1.1 to 10.30.1.12 **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 This field is only available only for Management/provision.
Click **Save**.	

Step 8 On the **Servers and Roles** page of the **Cisco VIM Suite** wizard, click **Add (+)** to add a new entry in the table, and complete the following fields:

<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 field.</td><td>The Rack ID for the server.</td></tr>
<tr><td>Chassis ID field</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 Control and Compute. If Rack is selected then Block Storage.</td></tr>
<tr><td>Management IP field.</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 field.</td><td>Enter Management Ipv6 address.</td></tr>
</table></td></tr>
<tr><td>Click Save or Add.</td><td>Clicking Save or Add, adds all information for Servers and Roles.</td></tr>
<tr><td>Disable Hyperthreading</td><td>True or False. Default is false.</td></tr>
</table>

Step 9 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 .	If you enable this checkbox, the Configure ToR section will change from false to true.

<table>
<tr><th>Name</th><th colspan="2">Description</th></tr>
<tr><td>ToR Switch Information mandatory table if you want to enter ToR information.</td><td colspan="2">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 Address.</td></tr>
<tr><td>SSN Num</td><td>ToR switch ssn num. output of show license host-id.</td></tr>
<tr><td>VPC Peer Keepalive</td><td>Peer Management IP. You need not define if there is no peer as it is optional but it will become mandatory when the ToR is in VPC.</td></tr>
<tr><td>VPC Domain</td><td>Need not define if there is no peer.</td></tr>
<tr><td>VPC Peer port</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>
</table></td></tr>
<tr><td>On clicking Save, Add ToR Info connected to Fabric field will be visible.</td><td>Port Channel field.</td><td>Enter the port channel input.</td></tr>
<tr><td></td><td>Switch Name field.</td><td>Enter the switch name.</td></tr>
</table>

Step 10 Click **OpenStack Setup** tab to advance to the **OpenStack Setup** Configuration page.

Step 11 On the **OpenStack Setup** page of the Cisco VIM Insight wizard, complete the following fields:

Name	Description
HA Proxy	Fill in the mandatory fields: **External VIP Address**: Enter IP address of External VIP. **External VIP Address IPv6**: Enter IPv6 address of External VIP. **Virtual Router ID**: Enter the Router ID for HA. **Internal VIP Address IPv6**: Enter IPv6 address. **Internal VIP Address**: Enter IP address of Internal VIP.
Keystone	Mandatory fields are pre-populated. This option is always true. **Admin Username**: admin. **Admin Tenant Name**: admin.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>LDAP on Keystone.
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 Groups</td><td>Enter a string.</td></tr>
<tr><td>Domain Name Tree for Users</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 for 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 Attributefield</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 change on the basis of Tenant Network Type Selection from Blueprint Initial Setup page.
Following are the options available for Neutron for OVS/VLAN:
<table>
<tr><td>Tenant Network Type</td><td>Auto Filled based on the Tenant Network Type selected in the Blueprint Initial Setup page.</td></tr>
<tr><td>Mechanism Drivers</td><td>Auto Filled based on the Tenant Network Type selected in Blueprint Initial Setup page.</td></tr>
<tr><td>NFV Hosts</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</td><td>List of ranges separated by comma of form start:end.</td></tr>
<tr><td>Provider VLAN Ranges</td><td>List of ranges separated by comma of form start:end.</td></tr>
<tr><td>VM Hugh Page Size (available for NFV_HOSTS option)</td><td>2M or 1G</td></tr>
<tr><td>Enable Jumbo Frames</td><td>Check Box</td></tr>
</table>
For Tenant Network Type Linux Bridge, everything will remain the same except Tenant VLAN Ranges which will be removed.</td></tr>
</table>

Name	Description
CEPH	Ceph has two pre-populated fields • **CEPH Mode**: By default **Dedicated**. • **NOVA Boot from:** From the drop-down, choose **Ceph or local**.
GLANCE	By default Populated for **CEPH Dedicated** with **Store Backend** value as **CEPH**.
CINDER	By default Populated for **CEPH Dedicated** with **Volume Driver** value as **CEPH**.

Name	Description
VMTP optional section will only be visible once VMTP is selected from Blueprint Initial Setup.	

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></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>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>Segmentation ID field.</td><td>Enter the segmentation ID.</td></tr><tr><td>Subnet</td><td>Enter the Subnet for Provider Network.</td></tr><tr><td></td><td></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>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><tr><td>Subnet</td><td>Enter the Subnet for External</td></tr></table></td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td><table><tr><td></td><td>Network.</td></tr></table></td></tr>
<tr><td>TLS section will be visible 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 if SwiftStack is selected from Blueprint Initial Setup Page. SwiftStack is only supported with KeyStonev2 . If you select Keystonev3, swiftstack cannot be configured.</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>
<tr><td>Under the openstack setup tab, the Vim_admins tab will only be visible once Vim_admins is selected from the Optional Features & Services under the Blueprint InitialSetup tab.</td><td>Following are the options that needs to be filled for Vim Admins:
Username - Text Field
Password - Password field. Admin hash password should always start with $6</td></tr>
</table>

Step 12 If **Syslog Export** or **NFVBENCH** is selected in **Blueprint Initial Setup** Page, then **Services Setup** page would be **enabled** for 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>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>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>
</table>

Step 13 Click **Offline validation** to initiate an offline Blueprint validation.

Step 14 Once the **Offline validation** is successful, **Save** option will be enabled which will redirect you to the **Blueprint Management** page.

Creating a Blueprint for C-Series Server Platform

Create a Cisco VIM Insight User Account and register the respective Pod.

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

Step 2 In the **Navigation** pane, expand the **Pre-Install Section**.

Step 3 Click **Blueprint Setup**.

Step 4 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	• B-Series (By Default) • C-Series (Select C Series)
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 (Is not supported in production)
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, etc. If any one is selected, the corresponding section is visible in various Blueprint sections. By default all options are disabled.
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 if any mandatory field is missed then would highlight it in the respective section.

Step 5 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 Mandatory fields are filled, the **Validation Check Registry** page will indicate a green tick.

Step 6 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).

Step 7 Click **Networking** to advance to the networking section of the Blueprint.

Name	Description
Domain Name field.	Enter the domain name **(Mandatory).**
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
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.
Networks table	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.

Step 8 Click **Edit** to enter new entries (networks) to the table. Specify the following fields in the **Edit Entry** to Networks dialog:

Name	Description
Segment drop-down list	Default is already selected. When you add/edit the segment then the following are the segment types available and you can select only one from dropdown list. • 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 openstack-configs dir for details.
VLAN field	Enter the VLAN ID. For Segment - Provider , the VLAN ID value is always **none**.
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.
IPv6 Gateway 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 only available 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 This field is only available only for Management provision
Click **Save**.	

Step 9 On the **Servers and Roles** page of the **Cisco VIM Suite** wizard, click **Add (+)** to add a new entry in the table, and complete the following fields:
You can edit or delete existing entries in the **Server and Roles** table.

<table>
<tr><th>Name</th><th colspan="2">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 colspan="2">Click Edit or + to add a new server and role to the table.<table><tr><td>Server Name</td><td>Entry the server 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>Management IPv6field</td><td>This is optional field. Enter Ipv6 format address</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.</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><td></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** .	On clicking **Save or Add** all information related to Servers and Roles gets saved.	
Disable Hyper threading	Default value is false. You can set it as true or false.	
Click **Save or Add** button.	If all mandatory fields are filled, click **Save or Add** button information for Servers and Roles.	

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.

Step 10 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 becomes a part of the Blueprint.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Configure TOR optional checkbox.
Note If UMHC is selected as podtype, configure TOR is not allowed.</td><td>If you enable this checkbox configure tor section would be changed from false to true.
Note Configure tor is true then ToR switch info maps in servers</td></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. Do not define if there is no peer</td></tr>
<tr><td>VPC Domain</td><td>Do not 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>
</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	Is not checked, as by default ACI will configure the ToRs

	Click + to add information for ToR Switch **Name** / **Description** **Host Name** — ToR switch name. **VPC Peerkeep alive** — Peer info must exist in pair. **VPC Domain** — Enter an Integer. **BR Management Port Info** — Enter Br management port info eg. Eth1/19, must have a pair in the peer switch. **Enter Node ID** — Entered Integer must be unique.

Step 11 Click **OpenStack Setup** Tab to advance to the **OpenStack Setup** page.

Step 12 In the **OpenStack Setup** page of the Cisco VIM Insight wizard, complete the following fields:

<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:
<table>
<tr><td>Tenant Network Type</td><td>Auto Filled based on the Tenant Network Type selection in Blueprint Initial Setup page.</td></tr>
<tr><td>Mechanism Drivers</td><td>Auto Filled based on the Tenant Network Type selection in Blueprint Initial Setup page.</td></tr>
<tr><td>NFV Hosts</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 else you can select particular computes as well for eg: NFV_HOSTS: "compute-server-1, compute-server-2"</td></tr>
<tr><td>Tenant VLAN Ranges</td><td>Allowed with VTS/VLAN VPP/VLAN, OVS/VLAN, ACI/VLAN</td></tr>
<tr><td>Enable Jumbo Frames</td><td>Check Box default is false.</td></tr>
<tr><td>Huge page size Note : . This is available only when Compute node is present in NFV host</td><td>The following are the drop-downs:
2M
1G</td></tr>
</table>
For Tenant Network Type Linux Bridge everything will remain 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>HA Proxy</td><td>Enter the Mandatory fields:
<table><tr><td>External VIP Address</td><td>Enter IP Address of External VIP.</td></tr><tr><td>External VIP Address IPv6</td><td>Enter IP v6 Address of External VIP .</td></tr><tr><td>Virtual Router ID</td><td>Enter the Router ID for HA.</td></tr><tr><td>Internal VIP Address</td><td>Enter IP Address of Internal VIP.</td></tr><tr><td>Internal VIP Address IPv6</td><td>Enter IP v6 Address for Internal VIP.</td></tr></table></td></tr>
<tr><td>Keystone</td><td><table><tr><td>Admin Username</td><td>admin</td></tr><tr><td>Admin Tenant Name</td><td>admin</td></tr></table></td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>LDAP</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 Groups</td><td>Enter a string.</td></tr>
<tr><td>Domain Name Tree for Users</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 for 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</td><td>Enter filter name as string.</td></tr>
<tr><td>User ID Attribute</td><td>Enter a string.</td></tr>
<tr><td>User Name Attribute</td><td>Enter a string.</td></tr>
<tr><td>User Mail Attribute</td><td>Enter a string.</td></tr>
<tr><td>Group Name Attribute</td><td>Enter a string.</td></tr>
</table></td></tr>
</table>

Name	Description
VMTP optional section will only be visible once VMTP is selected from Blueprint Initial Setup. **Note** For VTS, Provider network is only supported	

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></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>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>Segmentation ID field</td><td>Enter the segmentation ID.</td></tr><tr><td>Subnet</td><td>Enter the Subnet for Provider Network.</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>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><tr><td>Subnet</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></td><td></td></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>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</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. Protocol that swiftstack is running on top</td></tr>
</table></td></tr>
</table>

Note When tenant type ACI/VLAN is selected then ACI INFO 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.

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

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

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

Under the **openstack setup** tab, the **Vim_admins** tab will only be visible once Vim_admins is selected from the **Optional Features & Services** under the **Blueprint InitialSetup** tab.	Following are the options that needs to be filled for Vim Admins: • **Username** - Text Field • **Password** - Password field. Admin hash password should always start with $6

Step 13 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:

<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>Enable checkbox which by default is false.
Add ToR info connected to switch:
Select a TOR Switch. Switch- (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 & INT2 Optional input, enter the 2 port numbers of the 4-port 10G Intel NIC at the management node used for NFVBench.</td></tr>
</table>

Step 14 Click **Offline validation** button to initiate an offline validation of the Blueprint.

Step 15 Once the **Offline validation** is successful, **Save** option will be enabled for you which when clicked would redirect you to the **Blueprint Management** Page.

Creating a Blueprint using Upload Functionality

Before You Begin

- You should have a YAML file (B series or C Series) on your system.
- Only one blueprint can be uploaded at a time. To create a blueprint off-line, please refer to the setup_data.yaml.B_Series_EXAMPLE or setup_data.yaml.C_Series_EXAMPLE.

- The respective keys in the sample YALM should match or the corresponding section will not be populated during upload.

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

Step 2 In the **Navigation** pane, expand the **Pre-Install** Section.

Step 3 Click **Blueprint** Setup.

Step 4 Click the **Browse** button in the **Blueprint Initial Setup** page.

Step 5 Click **Select**.

Step 6 Click on **Load** button in the **Insight UI Application**.
All the fields present in the YAML file will be uploaded to the respective fields in the UI.

Step 7 Provide a **Name for the Blueprint**.
Make sure the blueprint name is unique while saving it.

Step 8 Click **Offline Validation**.

- If all the mandatory fields in the UI are populated, then Offline Validation of the Blueprint will commence, or else a pop up message indicating the section of Blueprint Creation that has missing information error shows up.

Step 9 On Offline Blueprint Validation being successful , **Save Blueprint** and **Cancel** button will be enabled.
Note If the Blueprint Validation Fails, only the **Cancel** button will be enabled.

Activating a Blueprint in an Existing Pod with OpenStack Installed

Before You Begin

You must have a POD which has an active Installation of OpenStack. If the OpenStack installation is in Failed State, then Insight UI will not be able to fetch the Blueprint.

Step 1 Go to the **landing page** of the Insight Login.

Step 2 Click **Register Management Node**.

Step 3 Enter the following details:

- Management Node IP Address.
- Management Node Name (Any friendly Name).
- REST API Password (/opt/cisco/ui_config.json).
- Description about the Management Node.
- POD Admin's Email ID.

A notification email will be sent to the email id entered during registration.

Step 4 Login using the same email id and password.

Step 5 In the Navigation pane, click **Pre-Install** > **Blueprint Management**.
In the **Blueprint Management** Page you will see **NEWSETUPDATA**.

This is the same setup data which was used by ciscovimclient to run the installation on the Management Node.

Downloading Blueprint

Before You Begin

You must have atleast one blueprint (In any state Active/In-Active or In-progress), in the **Blueprint Management Page**.

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

Step 2 In the **Navigation** pane, expand the **Pre-Install Section**.

Step 3 Click **Blueprint Management**.

Step 4 Go-to **Download** button for any Blueprint under Action title. (**Download Button** > **Downward Arrow** (with tooltip Preview & Download YAML).

Step 5 Click the **Download** icon.
A pop to view the Blueprint in the YAML format will be displayed.

Step 6 Click the **Download** button at the bottom left of the pop-up window.
YAML will be saved locally with the same name of the Blueprint.

Validating Blueprint

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

Step 2 In the **Navigation** pane, expand the **Pre-Install Section**.

Step 3 Click **Blueprint Creation**.

Step 4 Upload an existing YAML, or create a **New Blueprint**.
Fill all the mandatory fields so that all Red Cross changes to **Green Tick**.

Step 5 Enter the name of the Blueprint.

Step 6 Click the **Offline Validation** button.
Only if the Validation is successful, the Insight will allow the user to save the blueprint.

What to Do Next

If you see any errors, then hyperlink will be created for those errors. Click on the link to be navigated to the page where error has been encountered.

Managing Post Install Features

Cisco VIM provides an orchestration that helps in lifecycle management of a cloud. VIM is responsible for pod management activities which includes fixing both hardware and software issues with one-touch automation. VIM Insight provides the visualization of the stated goal. As a result, it integrates with POST install features that Cisco VIM offers through its Rest API. These features are enabled only if there is an active Blueprint deployment on the pod.

Monitoring the Pod

In VIM 2.2, we use EFK (Elasticsearch, Fluentd 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 You can also view Kibana Logs in a new tab by clicking the **View Kibana logs** link.

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

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

Following are the tests supported in CloudPulse:

1. cinder_endpoint
2. glace_endpoint
3. keystone_endpoint
4. nova_endpoint
5. neutron_endpoint
6. rabbitmq_check
7. galera_check
8. ceph_check

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

Name	Description
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.

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.

Name	Description
Click **Update**	Old **CIMC-COMMON** password will be updated with new **CIMC-COMMON** password.