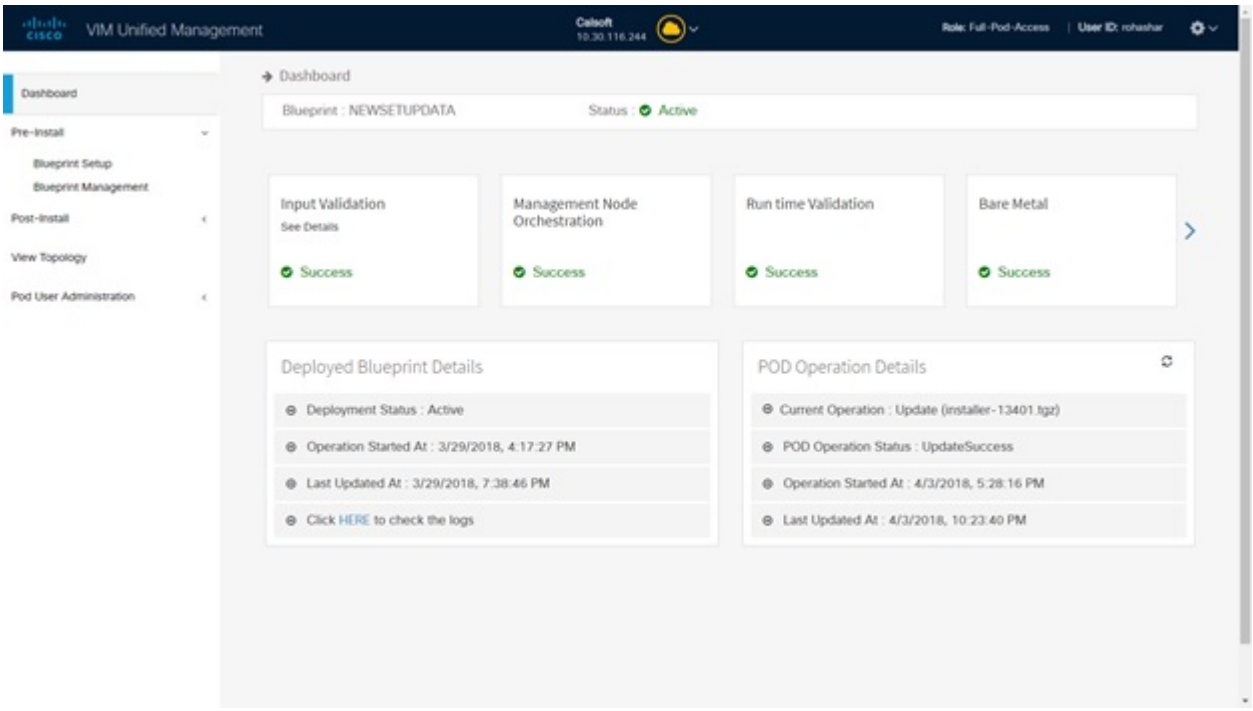
Installing Cisco VIM through Cisco VIM Unified Management

The VIM UM 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:

Unified Management Dashboard

When you login as UM admin, you will be redirected to the UM admin Dashboard.



The UM dashboard displays the following information about the pods it is currently managing:

Pod Status

- Active - Number of Pods which has health status OK (Example: Mgmt Node health of the pod is good).
- Inactive - Number of Pods whose health status is not good (Example:. Mgmt Node health of the pod is not good).
- Total number of Pods - Number of Pods registered in the system.

Pod Users

- Total – Total number of users registered who are associated with at-least one Pod.
- Registered – Number of users who have completed the registration process and are associated with at-least one Pod.
- Active – Number of Online users who are associated with at-least one Pod.

You can see the list of Pod with its Pod name, description, IP address, location, Pod status along with the Total users and Active users of each pod. You can search for a Pod using Name, IP and location in the search option.

If you click **Get health of current nodes icon (spin)** it does the health check of the Pod.

Pods

Pods allows you to check the health status (indicated through green and red dot) of the pod respectively.

To fetch the latest health status, click **Refresh** which is at the upper right corner.

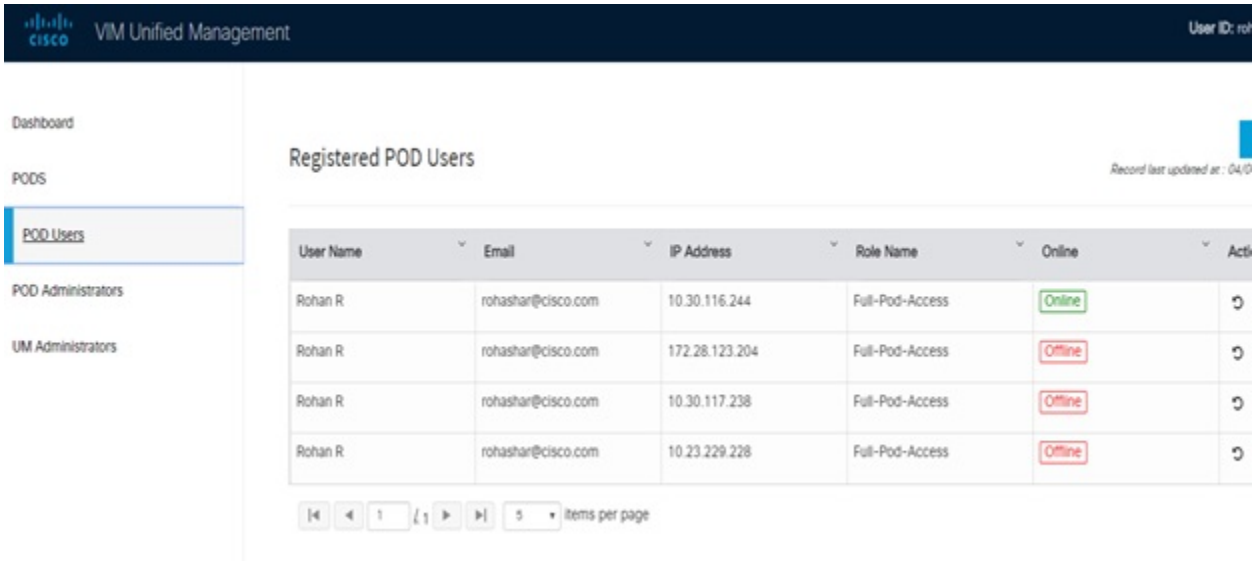
- Green dot – Pod is reachable and health is good.
- Red dot – Pod is not reachable.

Pod Users

The Pod Users page, gives you the details associated the pod, status (Online or Offline) and their Roles.

UM admin has the right to manage all Pod users in the system. The user with UM admin access can manage the following actions:

- Revoke User's permission from a specific Pod.
- Delete User from the system.



Revoking User

UM admin revokes the user's permission from a Pod by clicking **(undo)** icon. If the user is the only user with a Full-Pod-Access role for that particular Pod, then the revoke operation is not permitted. In this case, another user is granted with a Full-Pod-Access role for that Pod and then proceeds with revoking the old user.

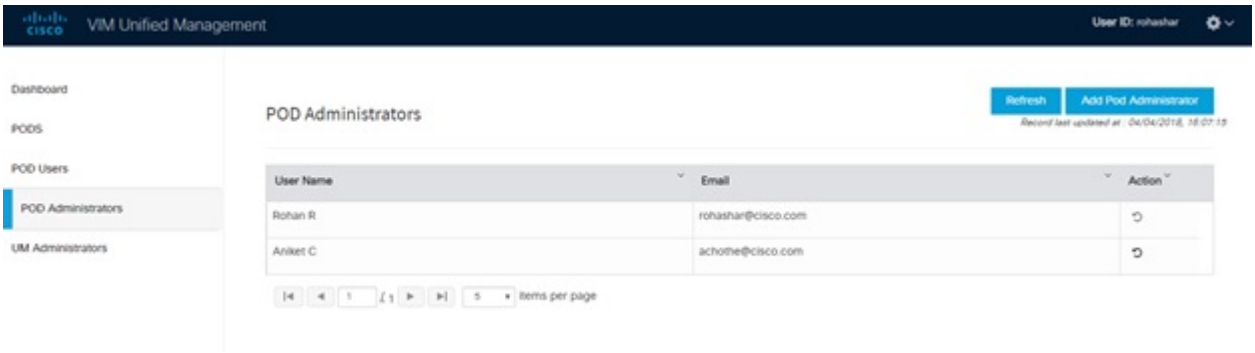
Note If the user is revoked from the last associated Pod, then the user is deleted from the system.

Deleting Users

UM admin can delete any user from the system by clicking **X** from an Action column. The delete operation is not permitted if the user has Full-Pod-Access. In, such case another user is granted with *Full-Pod-Access* role for that Pod and then proceed with deleting the old user. UM admin must revoke respective permission first and then proceed further.

Pod Administrator

Pod admins are the users who has the permission to register new Pods in the system. UM admin can add any number of Pod admins in the system.



Adding Pod Admin

Step 1 Log in as **UI Admin** and navigate to POD Administrator page.

Step 2 Click **Add Pod Administrator** .

Step 3 Enter the Email ID of the user.

- If email is already registered, then Username gets populated automatically.
- If not registered, an email is sent to the user email ID.

Step 4 Select User auth for the new user. This option is enabled only if Ldap mode is true.

- If email is already registered, then Username gets populated automatically.
- If not registered, an email is sent to the user email ID with the verification token. If User auth is set as LDAP, no verification token email is sent.

Step 5 Navigate to https://br_api :9000.

Step 6 Enter the Email ID and the Password of the Pod Admin and click **Login as Pod User**, it redirects to the landing page. Now the Pod admin can register a new Pod.

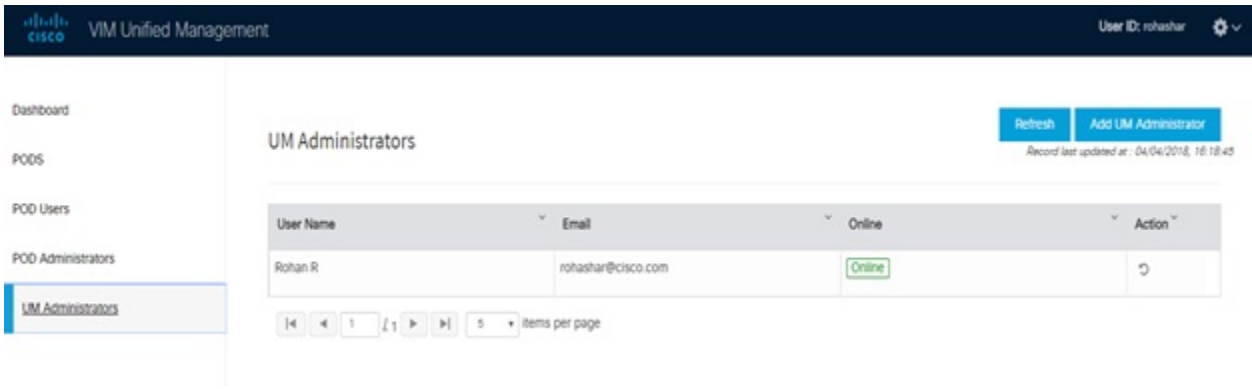
Revoking Pod Admin

UM admin can revoke Pod admin's permission anytime. To revoke Pod admin permission for the user, click **undo** icon.

Note You cannot revoke self permission.

Unified Management (UM) Administrator

UM admins have the access to the UM profile. Only a UM admin can add another UM admin in the system. There should be at least one UM admin in the system.



Adding UM Admin

To add a UM admin perform the following steps.

Step 1 Log in as **UI Admin** and navigate to UM Administrator page.

Step 2 Click **Add UM Administrator**.

Step 3 Enter the Email ID of the user.

Step 4 Select User auth for the new user. This option is enabled only if Ldap mode is true.

- If email is already registered, then Username gets populated automatically.
- If email is not registered, an email is sent to the user email ID with the verification token. If User auth is set as LDAP, no verification token email is sent.

Step 5 Navigate to https://br_api: 9000.

Step 6 Enter the Email ID and the Password of the UM Admin and click **Log in as UM admin** it will redirect to UM dashboard.

Revoking UM Admin

UM admin can revoke another UM admin's permission. To revoke UM Admin permission for any user, click **undo** icon.

Note You cannot revoke a self's permission. You can revoke a user if the user is not associated with any pod. After, revoking the user is deleted from the system.

Registering New Pod to Insight

Following are the steps that are required for UI Admin to register a Pod Admin:

Before you begin

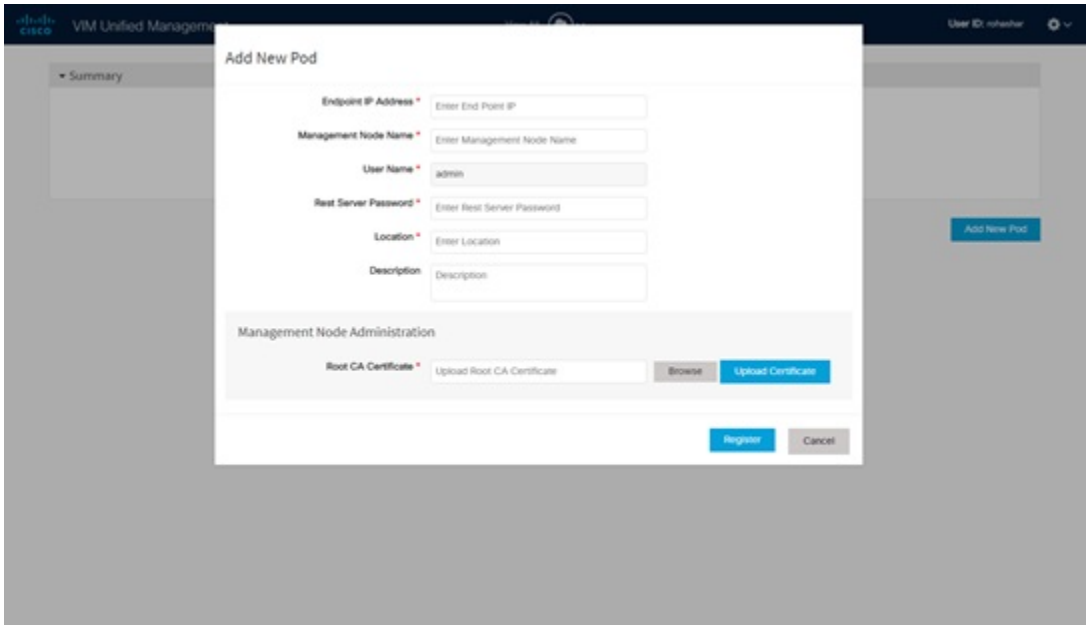
UI Admin has to register a Pod Admin to allow the user to access a pod.

Step 1 Log in as **UM Administrator**, you will be redirected to UM Admin section.

Step 2 Navigate to Pod Administrator and click **Add Pod Admin**.

Step 3 Enter the Email ID and the Password of the Pod Admin and click **Login as Pod User,** it will redirect to landing page.

Step 4 Click **Add New Pod** to register a Pod. Add New Pod popup window appears on the screen.



Step 5 Enter the Add New Pod field values, and click **Browse** to browse the Root CA certificate and **Upload** it.

Step 6 Click **Register** to start the Pod registration process starts.

The newly created Pod appears on the Landing Page.

Configuring OpenStack Installation

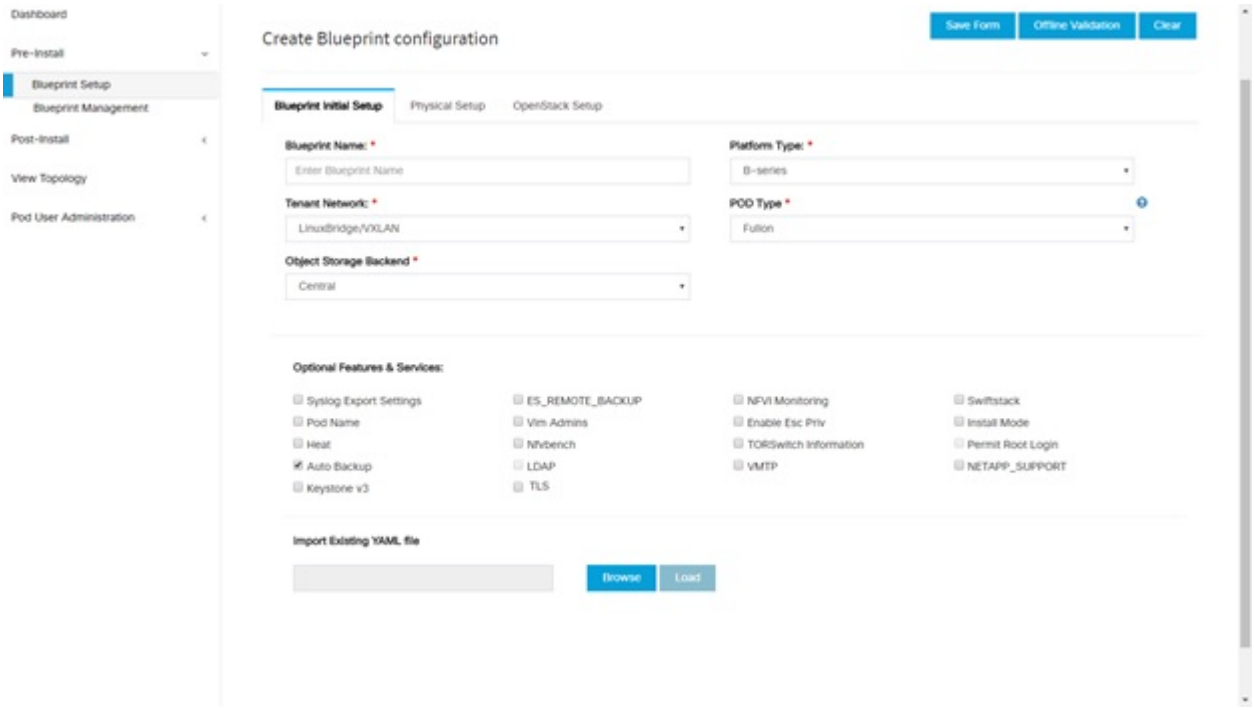
Before you begin

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**:

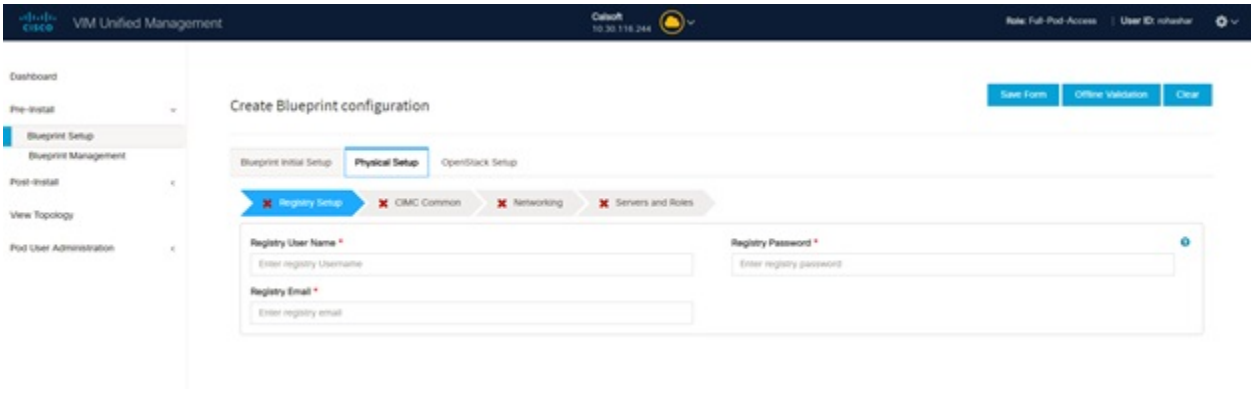
1. On the **Blueprint Initial Setup** pane of the Cisco VIM Insight, complete the following fields:



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)

Name	Description
Ceph Mode drop-down list	Choose one of the following Ceph types: • Dedicated • Central (By Default) - Not supported in Production
Optional Features and Services Checkbox	Swiftstack, LDAP, Syslog Export Settings, Install Mode, ToR Switch Information, TLS, NFVMON, Pod Name, VMTP, NFV Bench, Auto-backup, Heat, Keystone v3, Enable Esc Priv, Enable TTY logging, SNMP, ManagementNode_CloudAPI_Reachability. If any one is selected, the corresponding section is visible in various Blueprint sections. SNMP requires CVIMMON to be enabled. By default, all features are disabled except Auto-backup and Management Node_CloudAPI_Reachability.
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. Unified Management automatically fill in the fields and if any mandatory field is missed then it gets highlighted in the respective section.

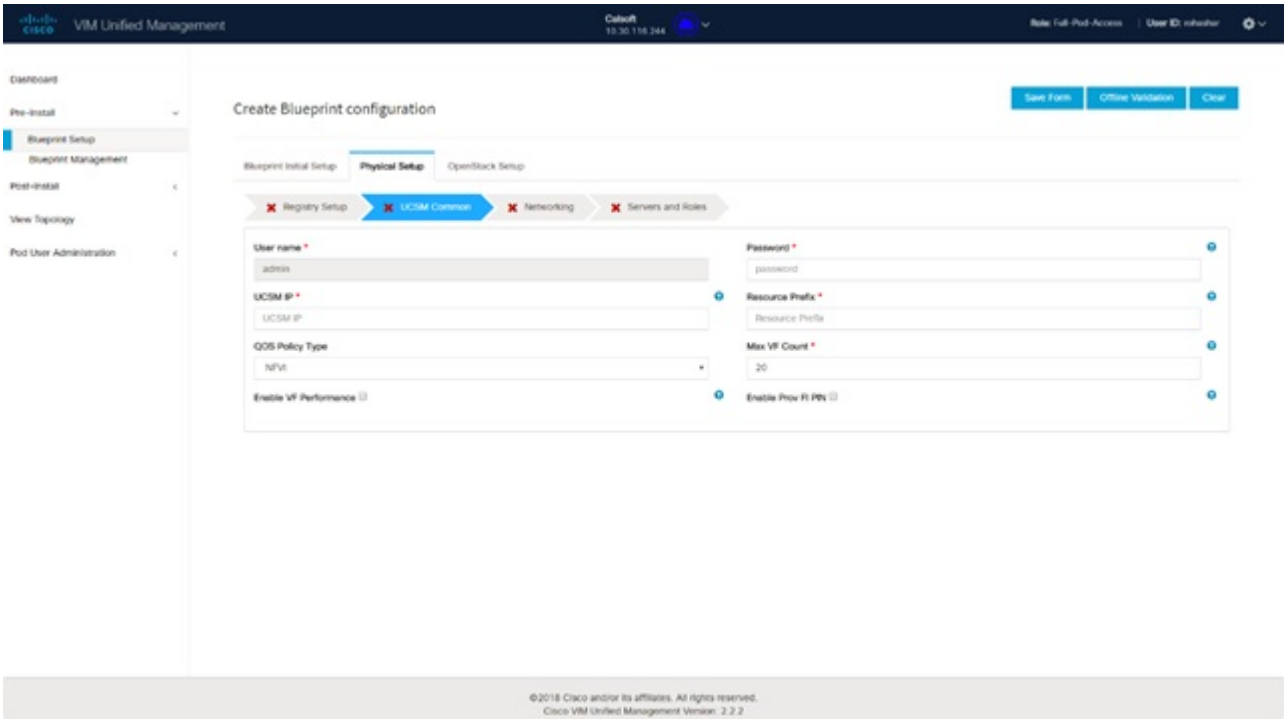
2. Click **Physical Setup** to navigate to the **Registry Setup** configuration page. Fill in the following details for Registry Setup:



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

Once all mandatory fields are filled the **Validation Check Registry Pane** shows a Green Tick.

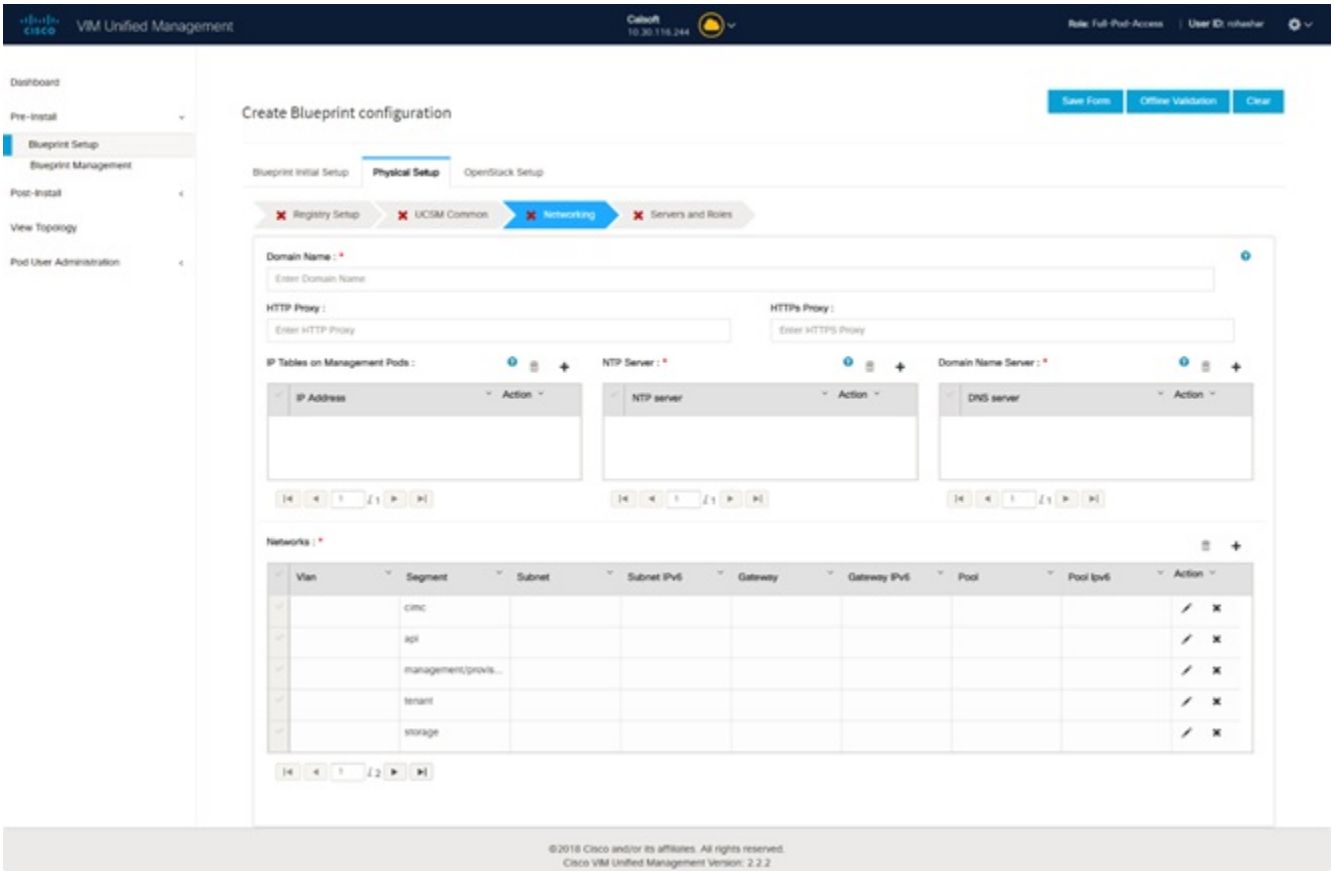
3. Click **UCSM Common Tab** and complete the following fields:



Name	Description
User name disabled field	By default the 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
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.

Name	Description
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 such as Add, Delete, Edit and, Multiple Delete.

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



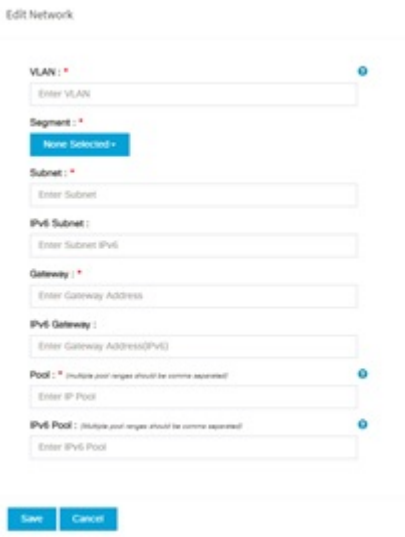
Name	Description
Domain Name field	Enter the domain name **(Mandatory)**.

Name	Description
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:

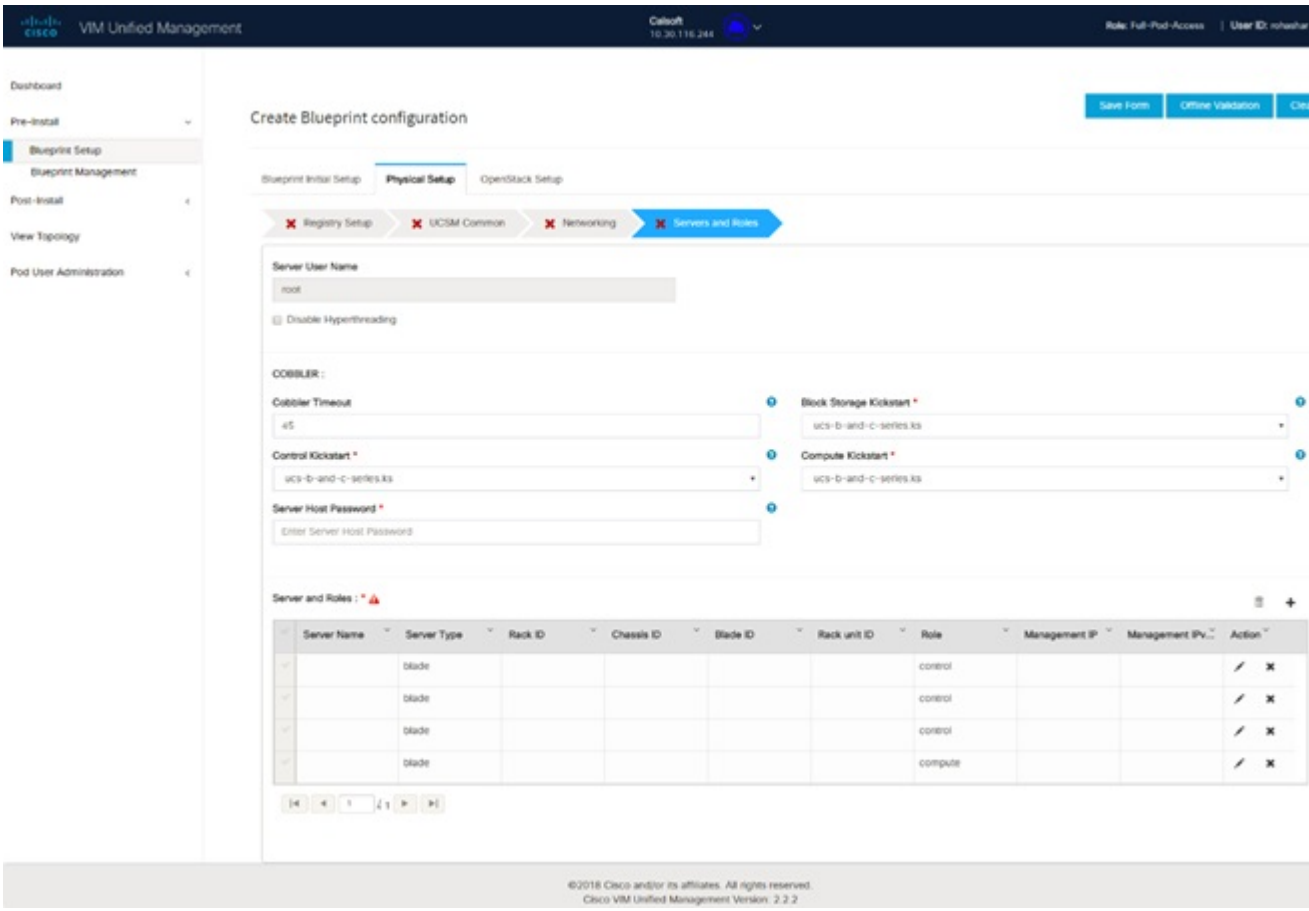


• Click + to enter new entries (networks) to the table.
• Specify the following fields in the Edit Entry to Networks dialog box.
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>VLAN field</td><td>Enter the VLAN ID.

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 drop-down list.
• API
• Management/Provision
• Tenant
• CIMC
• Storage
• External</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>• 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 is available only for Management provision and API.</td></tr>
<tr><td>Gateway field</td><td>Enter the IPv4 address for the Gateway.</td></tr>
<tr><td>IPv6 Gateway field</td><td>Enter IPv6 gateway. This field is available only for Management provision and API network.</td></tr>
<tr><td>Pool field</td><td>Enter the pool information in the following 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 following 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>

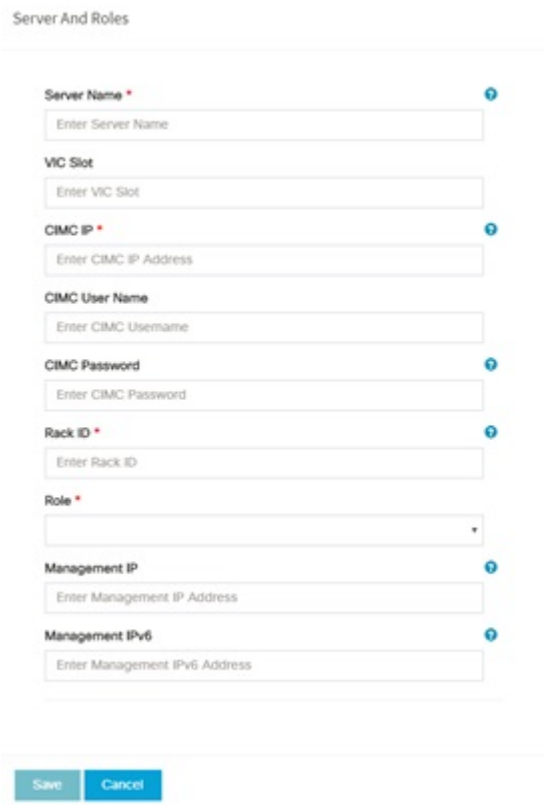
5. On the **Servers and Roles** page of the Cisco VIM Suite wizard, you see a pre-populated table filled with Roles: Control, Compute and Block Storage (Only if CEPH Dedicated is selected in Blueprint Initial Setup.



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 must 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>

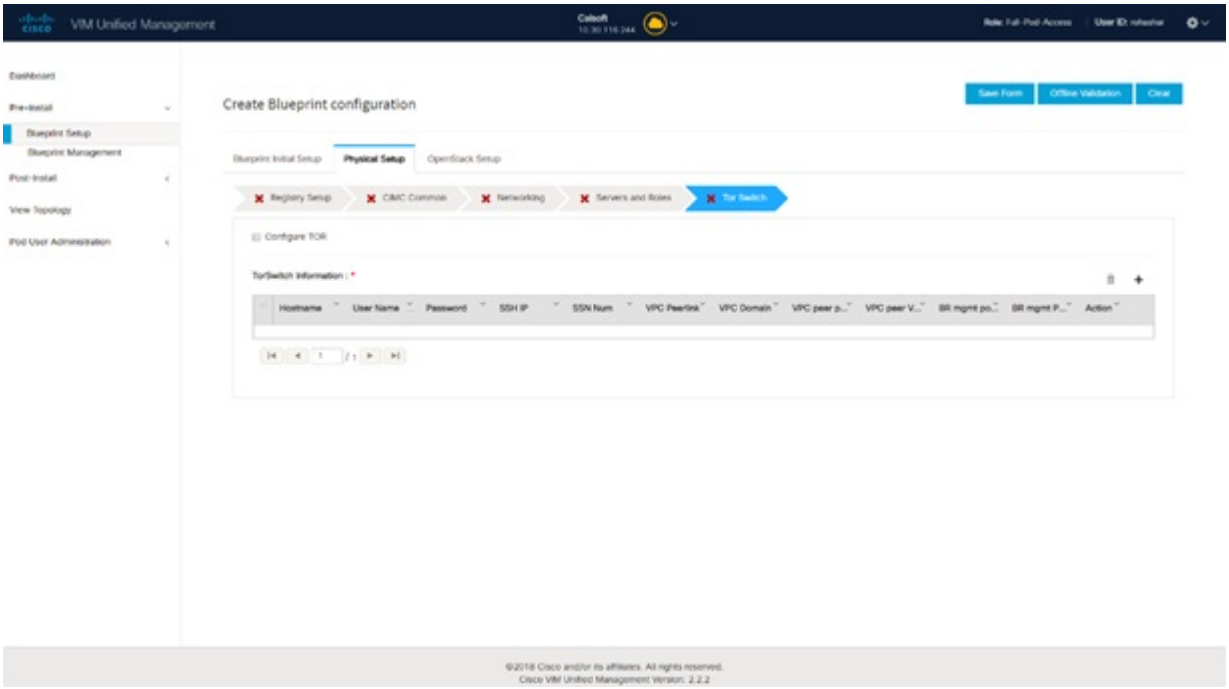
Name	Description
Add Entry to Servers and Roles	

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></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</td></tr>
</table>
</td></tr>
</table>

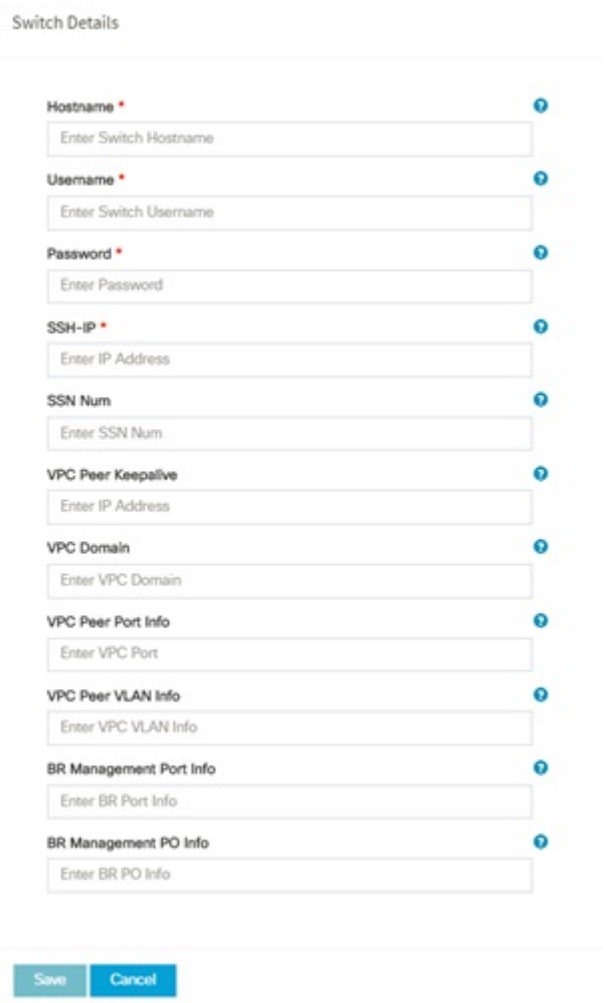
Name	Description
	provided for one server then it is mandatory to provide details for other Servers as well.
	Management IPv6 — Enter the Management IPv6 Address.
	Click **Save**.

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 when 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.

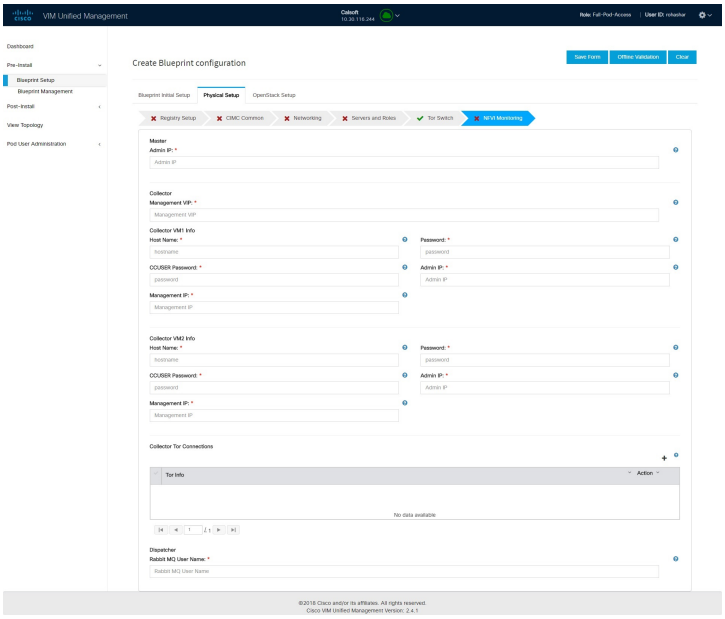
Name	Description
ToR Switch Information mandatory table.	

Name	Description
	Click **(+)** to add information for ToR Switch. 

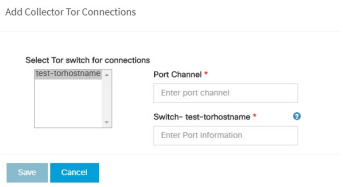
Name	Description
Hostname	ToR switch hostname.
Username	ToR switch username.
Password	ToR switch password.
SSH IP	ToR switch SSH IP Address.
SSN Num	ToR switch ssn num.
VPC Peer Keepalive	Peer Management IP. You do not define if there is no peer.
VPC Domain	Do not define if peer is absent.

Name	Description	
	VPC Peer Port Info	Interface for vpc peer ports.
	BR Management Port Info	Management interface of the management node.
	BR Management PO Info	Port channel number for management interface of the management node.
	Click**Save**.	
On clicking save button, **Add ToR Info Connected to Fabric** field is visible.	**Port Channel** field.	Enter the Port Channel input.
	Switch Name field.	Enter the name of the Switch.

7. Click **NFVI Monitoring** checkbox in Blueprint Initial Setup to enable the NFVI Monitoring configuration tab.

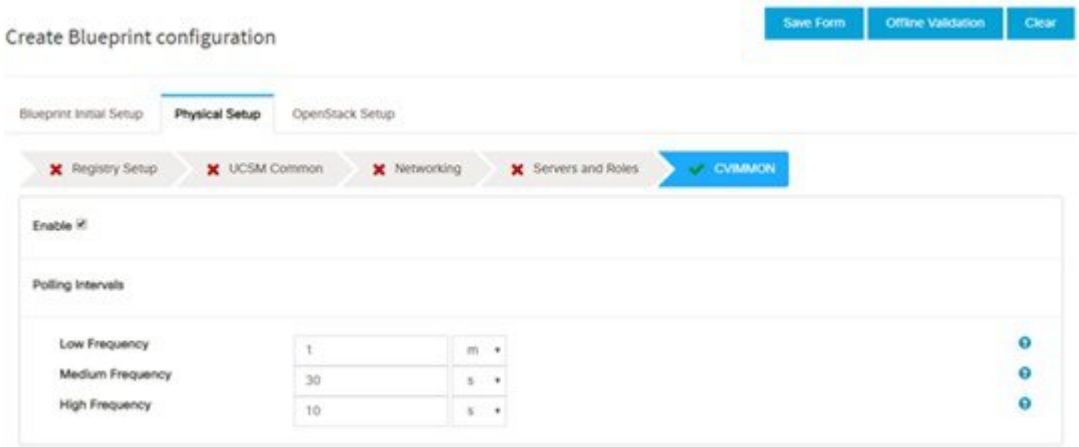


Name	Description
Admin IP	IP Address of Control Center VM
Management VIP	VIP for ceilometer/dispatcher to use, must be unique across VIM Pod
Host Name	Hostname of Collector VM
Password	Password of Collector VM
CCUSER Password	Password of CCUSER

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Admin IP</td><td>SSH IP of Collector VM</td></tr>
<tr><td>Management IP</td><td>Management IP of Collector VM</td></tr>
<tr><td>Collector ToR Connections</td><td>1. Click on (+) icon to Add Collector ToR Connections.
2. Select the ToR switches from list to add the information.
3. It is optional and available for ToR type NCS-5500
4. For now, it supports adding only one Collector ToR Connection
 

<table>
<tr><td>Port Channel</td><td>Enter port channel.</td></tr>
<tr><td>Switch - {torSwitch-hostname}</td><td>Enter port number, E.g:eth1/15.</td></tr>
</table>
Click Save</td></tr>
<tr><td>Rabbit MQ User Name</td><td>Enter Rabbit MQ username.</td></tr>
</table>

8. Click **CVIMMON** option in Blueprint Initial Setup to enable the CVIMMON configuration tab.



CVIM-MON is a built-in infrastructure monitoring service based on telegraf/prometheus/grafana.

When enabled, the telegraf service will be deployed on every node on the pod to capture infrastructure level stats (CPU, memory, network, containers, and so on) and a Prometheus server will be installed on the management node

to poll for these stats and store them in its time series database. The statistics can then be viewed using the grafana server that is accessible on the management node at port 3000 (password protected).

There are three levels of polling intervals which are used by different telegraf plugins:

- Low frequency interval is used to collect system level metrics like cpu, memory
- Medium frequency interval is used to collect docker metrics
- High frequency interval is used to collect rabbitmq metrics

Defining polling intervals in setup data is optional, if not defined the default values will be used

CVIM-MON is mutually exclusive to NFVIMON

PODNAME is required when CVIM-MON is enabled

Name	Description
Enable	Default is False
Polling Intervals	
Low frequency	<Integer following with time sign (s/m/h)> # min of 1 minute (1m) if not defined defaults to 1m, also it needs to be higher than medium interval.
Medium frequency	<Integer following with time sign (s/m/h)> # min of 30 seconds (30s) if not defined defaults to 30s, also it needs to be higher than high interval.
High frequency	<Integer following with time sign (s/m/h)> # min of 10 seconds (10s) if not defined defaults to 10s.

While CVIMMON checkbox is checked in Blueprint Initial setup, there is a checkbox provided in the CVIMMON tab area for enabling the SNMP feature. When user check this enable SNMP checkbox, Add a Manager button appears in the right area.

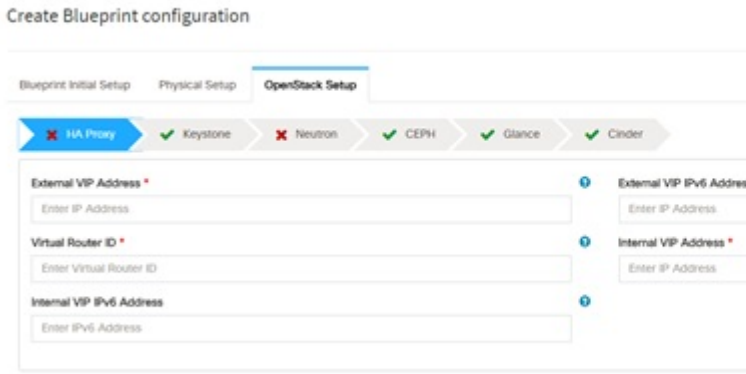
Clicking on this button shows various fields related to that manager. User can add up to three SNMP managers.

Name	Description
Address	Ipv4 address of the remote SNMP manager, unique across all managers
Port	Port (1-65535) to sent the traps; default 162, unique across all managers
Version	SNMP version of the manager; default 'v2c'
Community	For SNMPv2c. Community name; default 'public'
Engine_Id	For SNMPv3. ContextEngineId, min length of 5, max length of 32, unique across all managers; cannot we all 00s or FFs
Users	List of users; maximum: 3

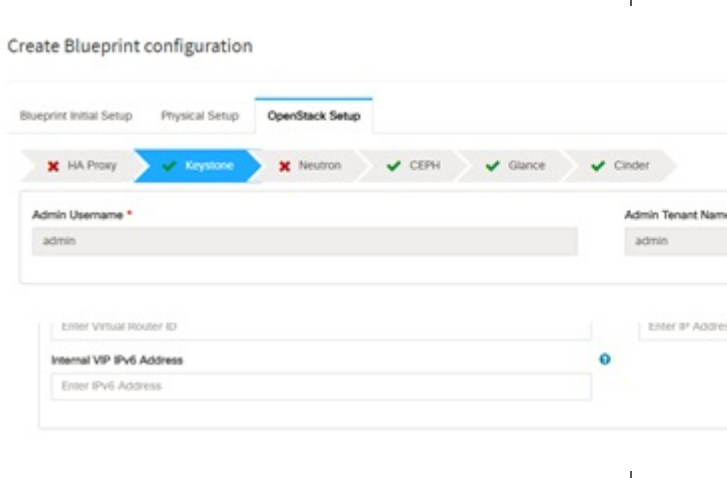
Name	Description
Name	Username has to be unique across users for the same manager
auth_key	Need to be min of 8 chars
authentication	Authentication protocol; default: 'SHA'
privacy_key	Encryption password; by default uses the same as the authentication
encryption	Encryption protocol ; default: 'AES128'

If CVIMMON is enabled and Platform type is C, then an optional feature to get SNMP traps from Cisco CIMC is available in the CVIMMON tab area. With this new feature SERVER_MON, there is a checkbox to enable or disable this feature and an input field to provide host information. User can either add comma separated server information or can have ALL to include all the servers.

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

Name	Description
HA Proxy	Fill in the following details: 

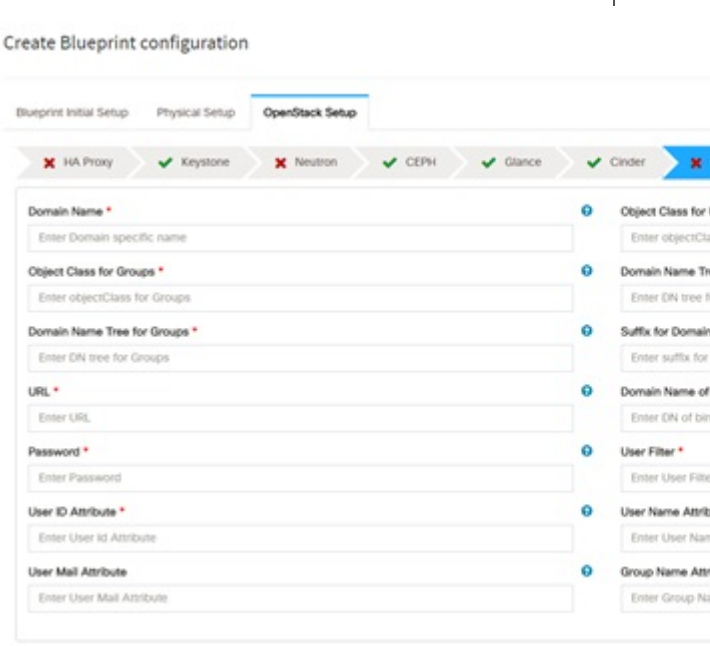
External VIP Address field	Enter the IP address of the External VIP.
External VIP Address IPv6 field	Enter the IPv6 address of the External VIP.
Virtual Router ID field	Enter the Router ID for the HA.
Internal VIP Address IPv6 field	Enter the IPv6 address of the Internal IP.
Internal VIP Address field	Enter the IP address of the Internal VIP.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Keystone</td><td>The following are the Pre-populated field values. This option is always set to be true.
 

<table>
<tr><td>Admin Username field</td><td>admin</td></tr>
<tr><td>Admin Tenant Name field</td><td>admin</td></tr>
</table></td></tr>
</table>

Name	Description
LDAP (Only if Keystonev3 is enabled) **Note** This option is only available with Keystone v3	

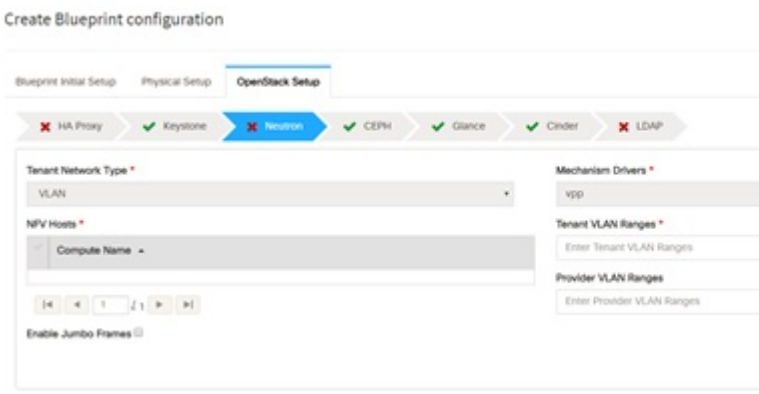
Name	Description
	This is available only when Keystone v3 and LDAP both are enabled under *Optional Features and Services* in Blueprint Initial Setup.



Domain Name field	Enter the Domain name.
Object Class for Users field	Enter a string as input.
Object Class for Groupsfield	Enter a string.
Domain Name Tree for Users field	Enter a string.
Domain Name Tree for Groups field	Enter a string.
Suffix for Domain Name field	Enter a string.
URL field	Enter a URL with ending port number.
Domain Name of bind user field	Enter a string.
Password field	Enter Password as string format.
User Filter field	Enter filter name as string.

Name	Description	
	User ID Attribute field	Enter a string.
	User Name Attribute field	Enter a string.
	User Mail Attribute field	Enter a string.
	Group Name Attribute field	Enter a string.

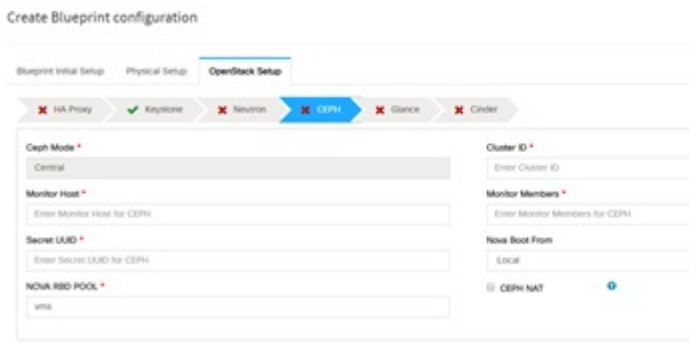
Name	Description
Neutron	

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>Neutron fields 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>It is Auto-filled based on the Tenant Network Typeselected in the Blueprint Initial Setup page.</td></tr>
<tr><td>Mechanism Drivers field</td><td>It is Auto-filled based on the Tenant Network Type selected in Blueprint Initial Setup page.</td></tr>
<tr><td>NFV Hosts field</td><td>It is Auto-filled with the Compute you added in Server and Roles.
If you select All in this section NFV_HOSTS: ALL is added to the Blueprint or you can select one particular compute. For Example:
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>
</table></td></tr>
</table>

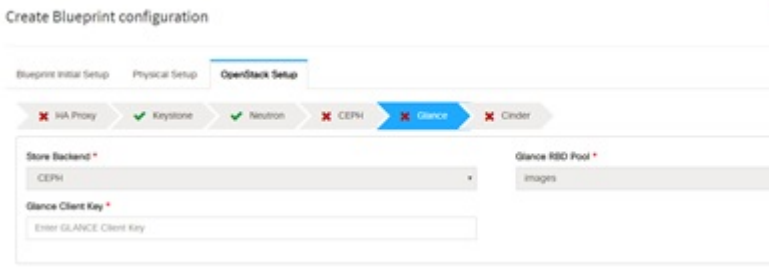
Name	Description
	Enable Jumbo Frames field: Enable the checkbox. For Tenant Network Type, Linux Bridge everything remains the same but **Tenant VLAN Ranges** is removed.

Name	Description
CEPH	

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>
1. 1. When Object Storage Backend is selected as Central in the blueprint initial setup.


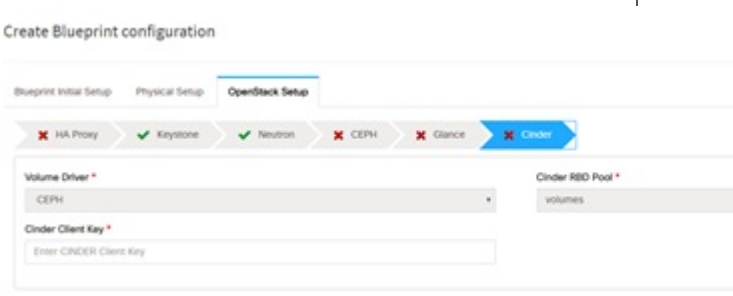
<table>
<tr><td>CEPH Mode</td><td>By default Ceph Mode is Central.</td></tr>
<tr><td>Cluster ID</td><td>Enter the Cluster ID.</td></tr>
<tr><td>Monitor Host</td><td>Enter the Monitor Host for CEPH</td></tr>
<tr><td>Monitor Members</td><td>Enter the Monitor Members for CEPH</td></tr>
<tr><td>Secret UUID</td><td>Enter the Secret UUID for CEPH</td></tr>
<tr><td>NOVA Boot from</td><td>You can choose CEPH or local from the drop-down list.</td></tr>
<tr><td>NOVA RBD POOL</td><td>Enter the NOVA RBD Pool (default's to vms)</td></tr>
<tr><td>CEPH NAT</td><td>CEPH NAT is required for Central Ceph and when mgmt network is not routable.</td></tr>
</table>
2. When Object Storage Backend is selected as Dedicated in the blueprint initial setup.

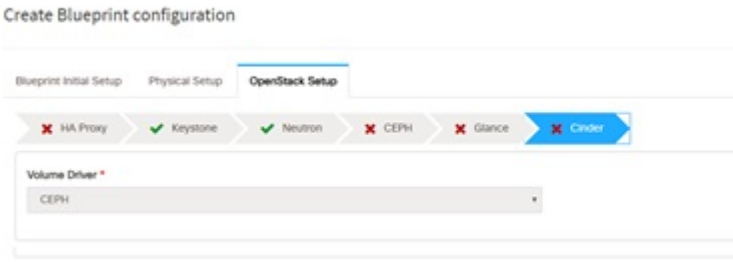

• CEPH Mode: By default Dedicated.
• NOVA Boot: From drop-down selection you can choose CEPH or local.
3. When Object Storage Backend is selected as NetApp in
</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>the blueprint initial setup.
 
</td></tr>
<tr><td>GLANCE</td><td>1. When Object Storage Backend is selected as Central in the blueprint initial setup.
 

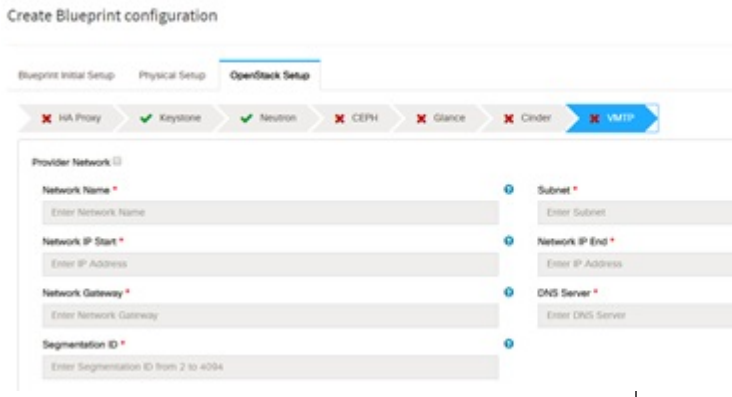
<table>
<tr><td>Store Backend</td><td>By default CEPH.</td></tr>
<tr><td>Glance RBD Pool field</td><td>By default images.</td></tr>
<tr><td>Glance Client Key</td><td>Enter GLANCE Client Key</td></tr>
</table>
2. When Object Storage Backend is selected as Dedicated in the blueprint initial setup.
 

By default Populated for CEPH Dedicated with Store Backend value as CEPH.</td></tr>
</table>

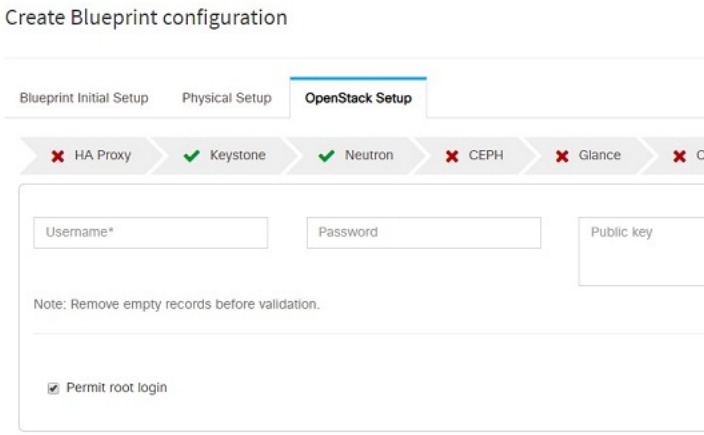
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>CINDER</td><td>By default Populated for CEPH Dedicated with Volume Driver value as CEPH.
 

<table>
<tr><td>Volume Driver</td><td>By default CEPH.</td></tr>
<tr><td>Cinder RBD Pool field</td><td>By default volumes.</td></tr>
<tr><td>Cinder Client Key</td><td>Enter Cinder Client Key</td></tr>
</table>

</td></tr>
</table>

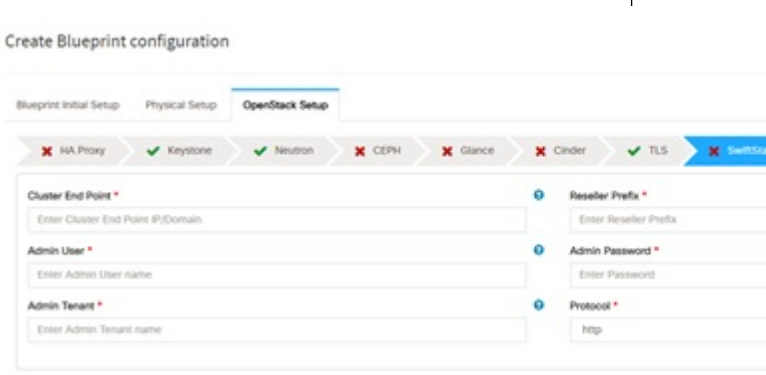
Name	Description
VMTP VMTP optional section will only be visible once VMTP is selected from Blueprint Initial Setup.	

Name	Description
	Check one of the check boxes to specify a VMTP network: • Provider Network • External Network For the **Provider Network** complete the following:  **Network Name** field — Enter the name for the external network. **Subnet** field — Enter the Subnet for Provider Network. **Network IP Start** field — Enter the start of the floating IPv4 address. **Network IP End** field — Enter the end of the floating IPv4 address. **Network Gateway**field — Enter the IPv4 address for the Gateway. **DNS Server** field — Enter the DNS server IPv4 address. **Segmentation ID** field — Enter the segmentation ID. For **External Network** fill in the following details: 

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>
<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 the external Network.</td></tr>
<tr><td>Network IP Start field</td><td>Enter the start of the floating IPv4 address.</td></tr>
<tr><td>Network IP End field</td><td>Enter the endof the 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>
<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>
</table>

<table>
<tr><th>Name</th><th>Description</th></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:
Add Username, Password, Public key or both for the non-root login.
At least one Vim Admin must be configured when Permit root login is false. 

<table>
<tr><td>User Name</td><td>Enter username for Vim Admin.</td></tr>
<tr><td>Password</td><td>Password field. Admin hash password should always start with $6.</td></tr>
<tr><td>Public Key</td><td>Public key for vim admin should always start with ‘ssh-rsa AAAA….’</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></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 the Swiftstack.</td></tr>
<tr><td>Reseller Prefix field</td><td>Reseller_prefix as configured for Keysone Auth,AuthToken support in Swiftstack. Example: 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>

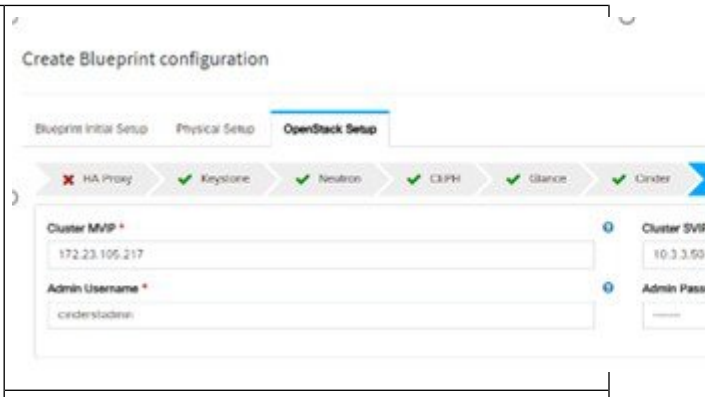
10. For SolidFire, enter the following:

Name	Description

SolidFire is visible for configuration on day0

SolidFire is not allowed as a day-2 deployment option

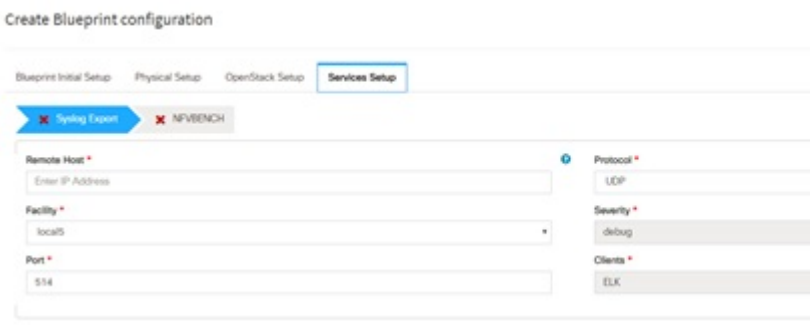
SolidFire is always available with CEPH.



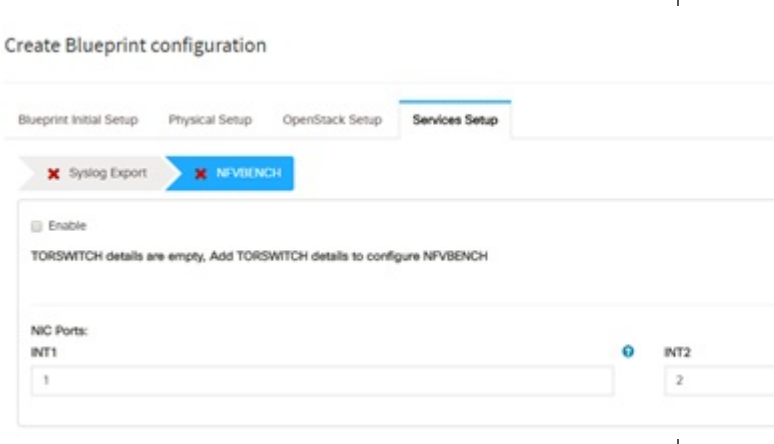
Cluster MVIP field	Management IP of SolidFire cluster.
Cluster SVIP field	Storage VIP of SolidFire cluster.
Admin Username	Admin user on SolidFire cluster
Admin Password	Admin password on SolidFire cluster.

11. If **Syslog Export** or **NFVBENCH** is selected in **Blueprint Initial Setup**, the **Services Setup** pane is enabled for the user to view.

    Following are the options under **Services Setup** tab:

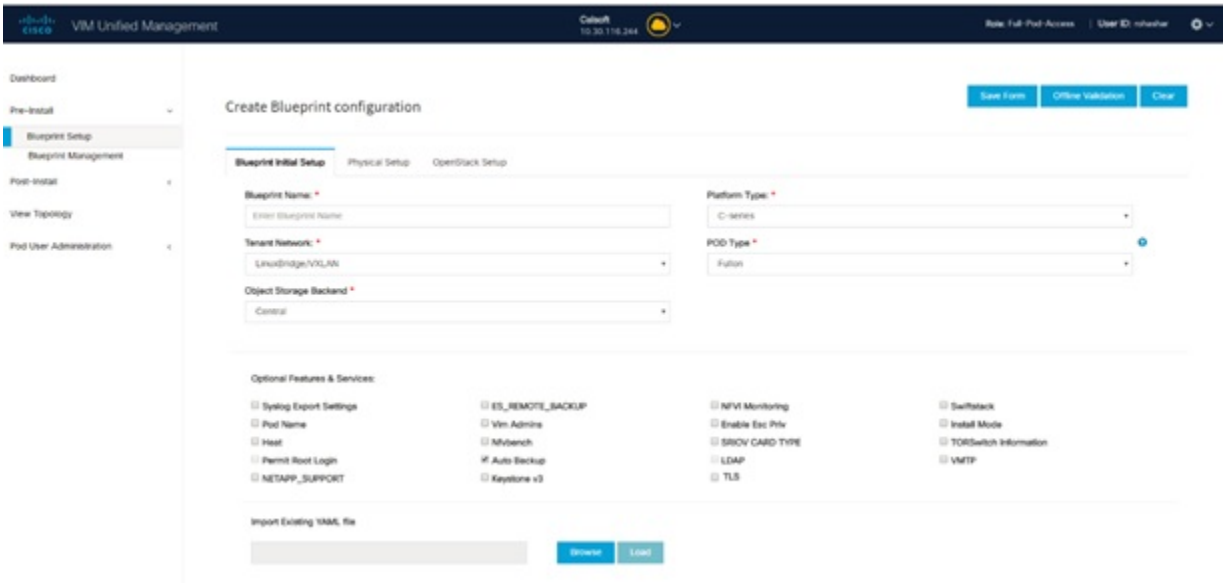
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Syslog Export</td><td>Following are the options for Syslog Settings:
 

<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>
</table>

Name	Description
NFVBENCH	**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 the NFVBench.
ENABLE_ESC_PRIV	Enable the checkbox to set it as True. By default it is *False*.

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

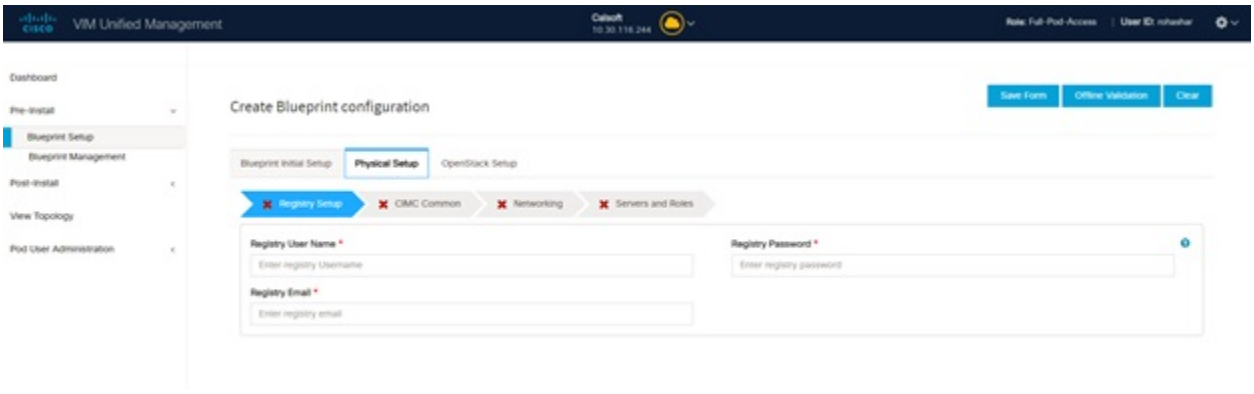
1. On the **Blueprint Initial Setup** page of the Cisco VIM Insight, complete the following fields:



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)
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. When Mechanism driver OVS or ACI is selected, VM_HUGEPAGE_PERCENTAGE field is enabled for all standalone compute nodes, when NFV_HOSTS is enabled.

Name	Description
Pod Type drop-down list	Choose one of the following pod type : • Fullon(By Default) • Micro • UMHC • NGENAHC **Note** • UMHC pod type is only supported for OVS/VLAN tenant type. • NGENAHC is supported for VPP/VLAN tenant type with no SRIOV • 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.

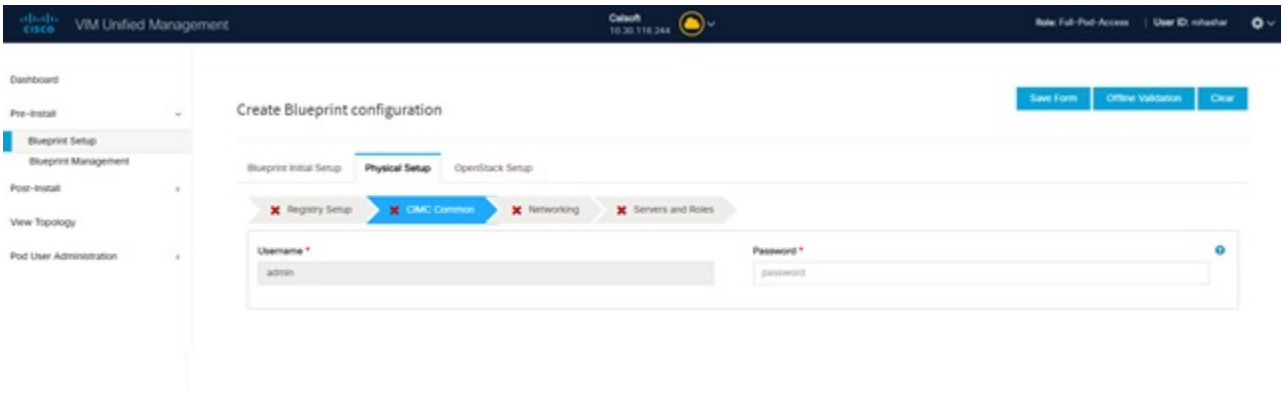
2. Click **Physical Setup** to advance to the **Registry Setup** configuration page. Fill in the following details for Registry Setup:



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)**.

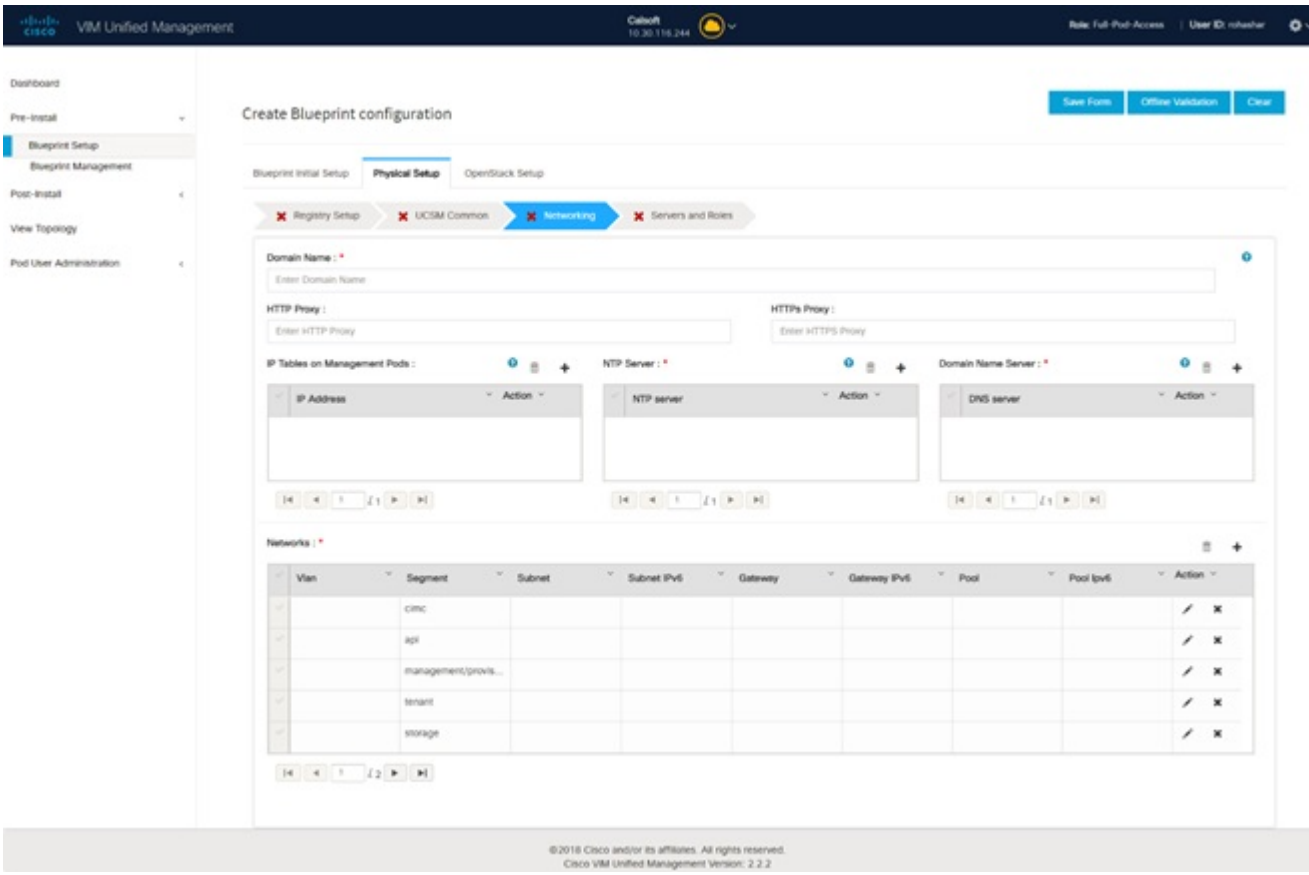
Once all the mandatory fields are filled the **Validation Check Registry Page** will be changed to a Green Tick.

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.

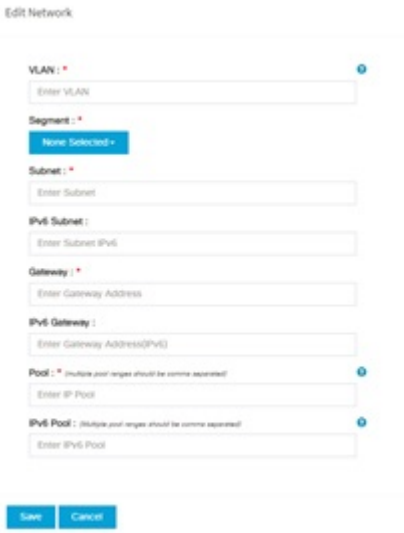


Name	Description
Domain Name field	Enter the domain name. **(Mandatory)**
HTTP Proxy Server field	If your configuration uses an HTTP proxy server, enter the IP address of the server.
HTTPS Proxy Server field	If your configuration uses an HTTPS proxy server, enter the IP address of the server.
IP Tables 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

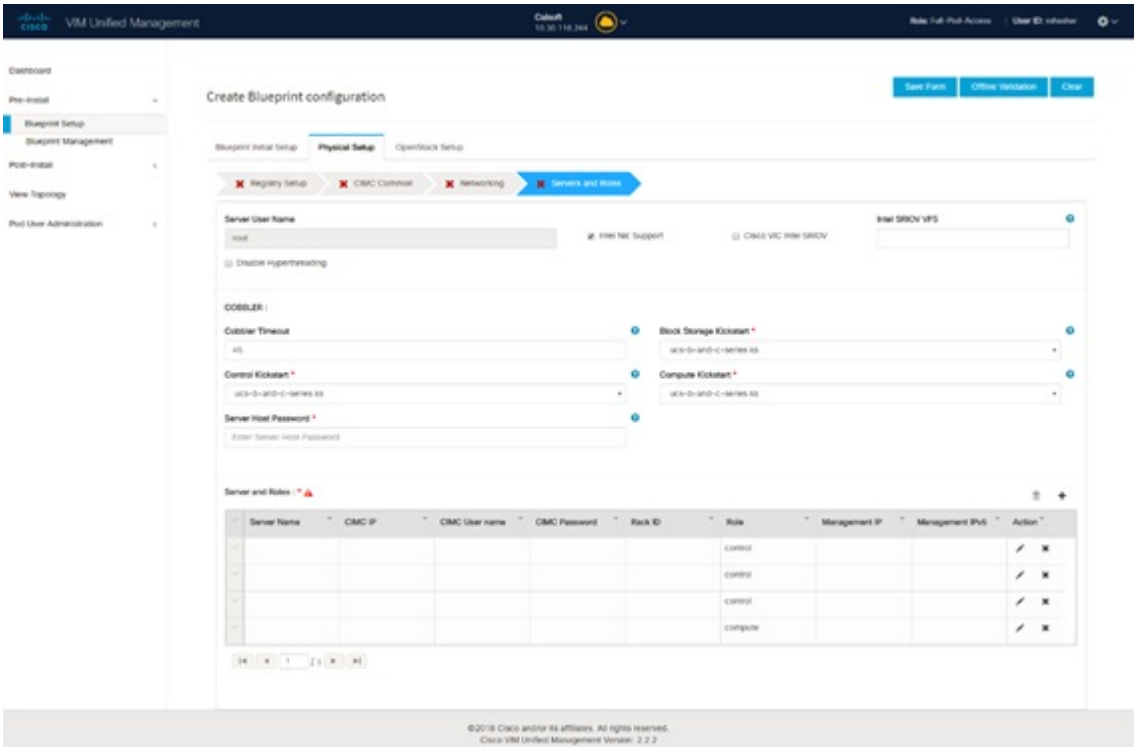
• Management/provision

• Tenant</td></tr>
</table>
</td></tr>
</table>

Name	Description	
		• 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.
	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	

Name	Description
	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.



Note If you choose mechanism driver as OVS or ACI, VM_HUGEPAGE_PERCENTAGE field column is available for compute nodes, where you can fill values from 0 to 100%, when NFV_HOSTS: ALL is chosen. Also, option of NIC Level Redundancy appears only when Intel Nic Support is set to true. This is applicable only in the case of M5 based pods.

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.

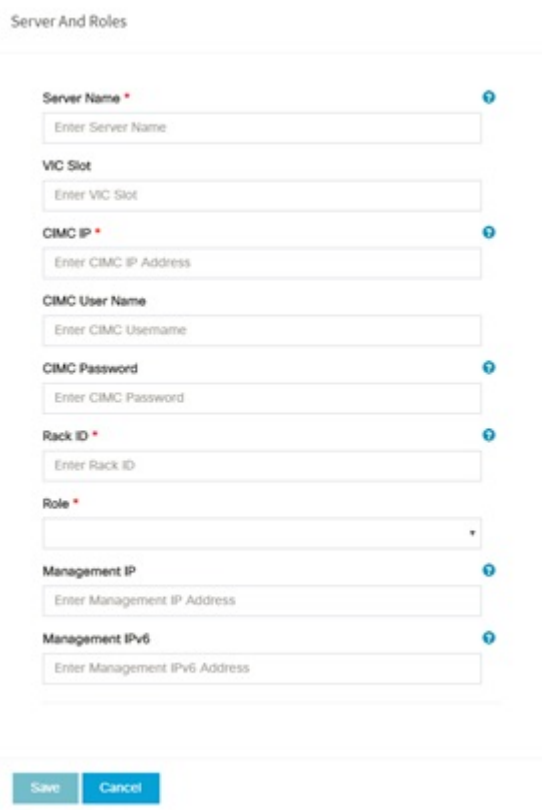
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Cobbler</td><td>Enter the Cobbler details in the following fields:
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Cobbler Timeout field</td><td>The default value is 45 min.
This is an optional parameter. Timeout is displayed in minutes, 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>

Name	Description

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.	

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>Click Edit or + to add a new server and role to the table.

If mechanism driver is either OVS or ACI, an additional optional field VM_HUGEPAGE_PERCENTAGE is shown when compute role is chosen; This option is only valid when NFV_HOSTS is set to ALL; If no value is entered then the global value of VM_HUGEPAGE_PERCENTAGE is used.

<table>
<tr><td>Server Name</td><td>Entry the name of the server.</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</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th></th></tr>
<tr><td></td><td colspan="2"><table>
<tr><td></td><td>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>
<tr><td>BGP speaker addressees</td><td>Optional, only when NETWORK_OPTIONS is vxlan network, for controller node only, IP belongs to the vxlan-tenant network but not part of the pool.</td></tr>
</table></td></tr>
<tr><td>Click Save or Add .</td><td colspan="2">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>
<tr><td>DP ToR (Only for Control and Compute) : Mandatory if Intel NIC and 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>
<tr><td>SRIOV TOR INFO (Only for Compute Nodes). It is mandatory in server and roles if Intel NIC and Configure TOR is True. with TOR TYPE Nexus. For TOR TYPE NCS-5500 these fields are optional 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</td><td>• Switch Name field
• Switch Port Info field</td><td>• Enter the switch name.
• Enter the switch port information.</td></tr>
<tr><td>Intel SRIOV VFS (valid for Intel NIC testbeds) and can be integer.</td><td colspan="2">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)</td></tr>
</table>

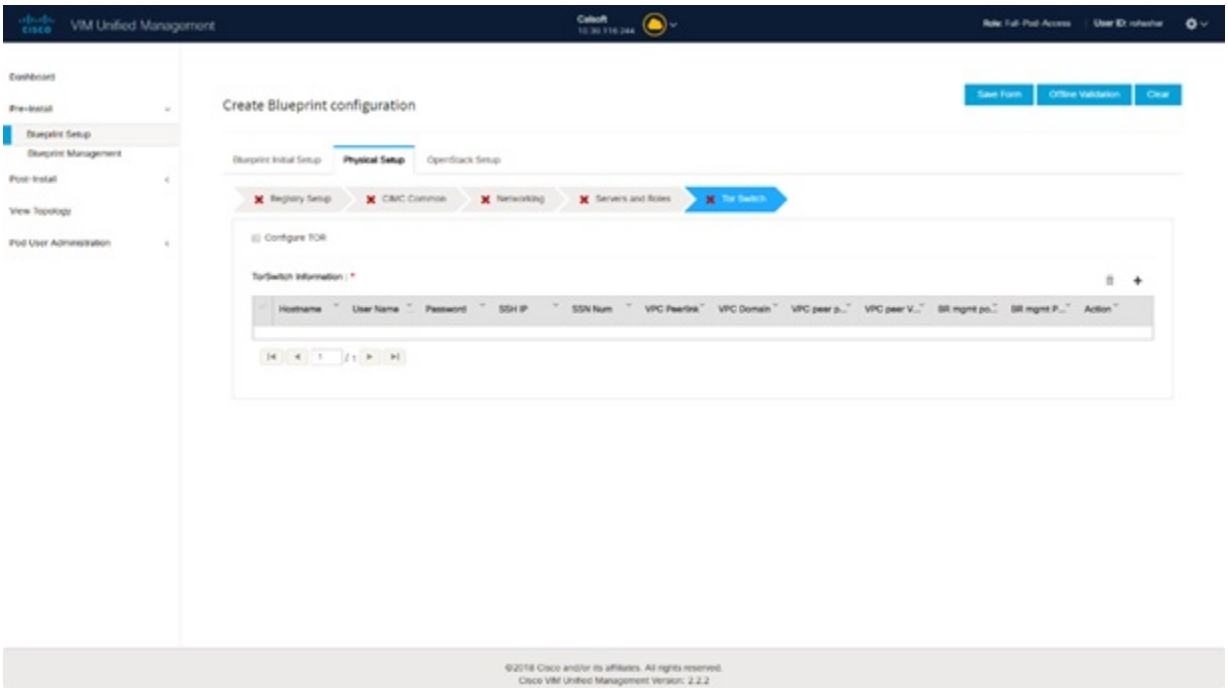
Name	Description
INTEL_SRIOV_PHYS_PORTS (valid for Intel NIC test beds) and can be of value 2 or 4 (default is 2)	In some cases the # of Physical SRIOV port needed is 4; to meet that requirement, define the following: # this is optional, if nothing is defined code will assume it to be 2; the only 2 integer values this parameter # takes is 2 or 4 and is true when INTEL_NIC_SUPPORT is True and INTEL_SRIOV_VFS is valid.. For NCS-5500 this value is set to 4 and is non-editable.
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. CISCO_VIC_INTEL_SRIOV is also supported on Micro pod with expanded computes

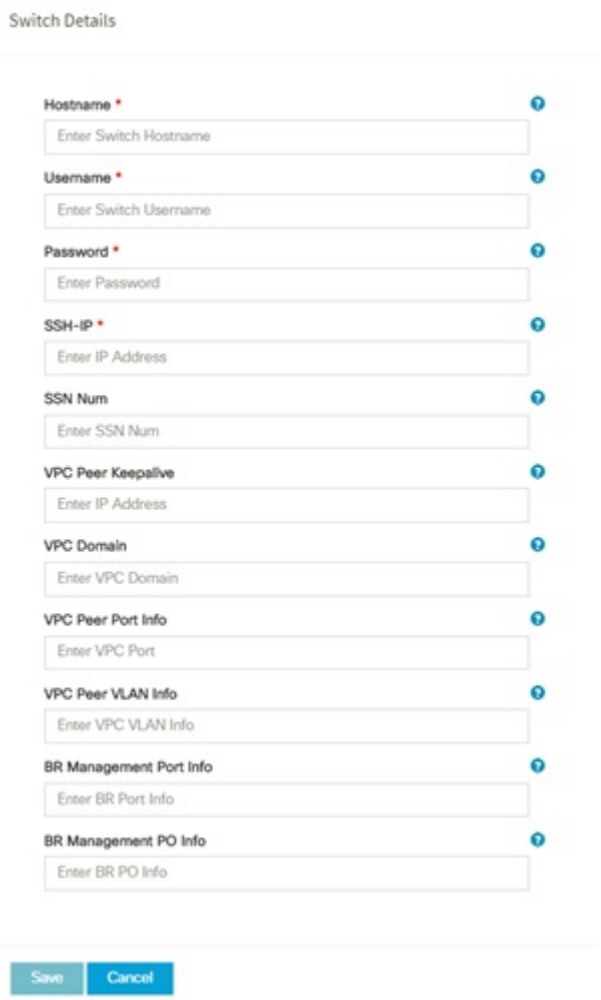
Note For Tenant type **ACI/VLAN,** port channel for each ToR port will not be available in servers and roles, as APIC will automatically assign port-channel numbers. Also, for ACI in full on mode you can select Intel NIC Support in the “Servers and Roles” section.

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

Name	Description
ToR Switch Information mandatory table if you want to enter ToR information.	

Name	Description
	Click **(+)** to add information for ToR Switch. 

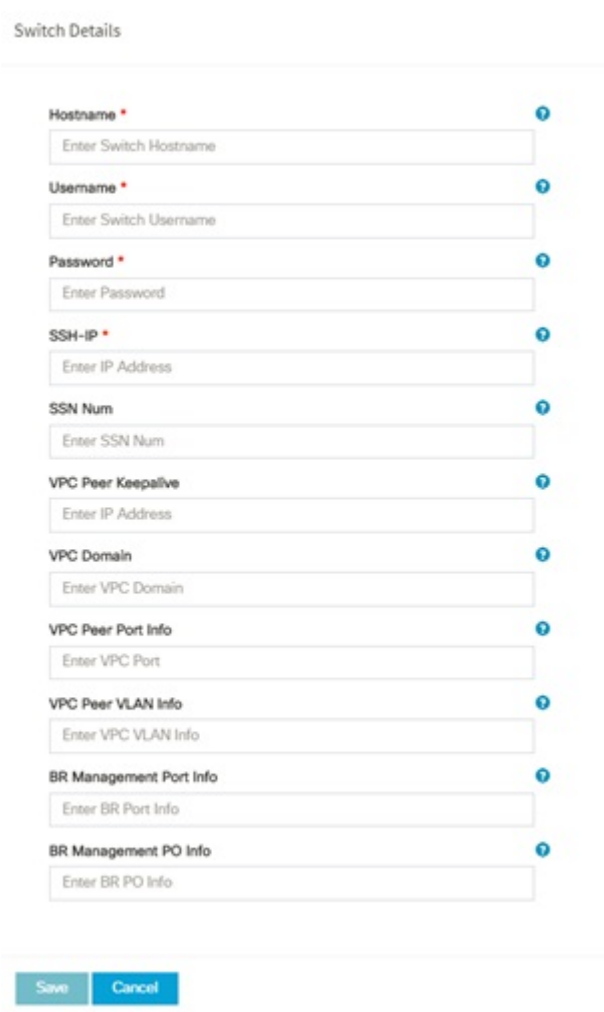
Name	Description
Name	ToR switch name.
Username	ToR switch username.
Password	ToR switch password.
SSH IP	ToR switch SSH IP.
SSN Num	ToR switch ssn num.
VPC Peer Keepalive	Peer Management IP. You cannot define if there is no peer.

Name	Description	
	VPC Domain	Cannot define if there is no peer.
	VPC Peer Port Info	Interface for vpc peer ports.
	VPC Peer VLAN Info	VLAN ids for vpc peer ports (optional).
	BR Management Port Info	Management interface of build node.
	BR Management PO Info	Port channel number for management interface of build node.
	BR Management VLAN info	VLAN ID for management interface of build node (access).
Splitter Optic 4x10	For C Series platform type, Tenant Type is VPP/VLAN and Pod Type is either fullon or Micro, an additional choice will be provided to select the TOR Type. If selected TOR type is NCS-5500, then user can configure splitter cable parameters.	
Click **Save**.		

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

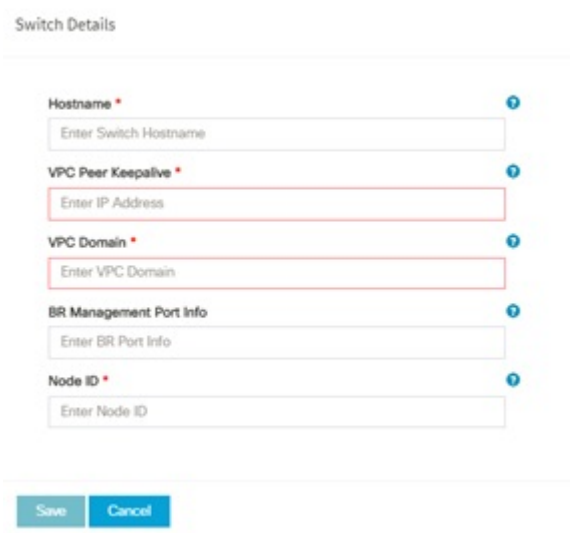
Name	Description
ToR Switch Information mandatory table if you want to enter ToR information.	

Name	Description
	Click **(+)** to add information for ToR Switch. 

Name	Description
Name	ToR switch name.
Username	ToR switch username.
Password	ToR switch password.
SSH IP	ToR switch SSH IP.
SSN Num	ToR switch ssn num.
VPC Peer Keepalive	Peer Management IP. You cannot define if there is no peer.

Name	Description	
	VPC Domain	Cannot define if there is no peer.
	VPC Peer Port Info	Interface for vpc peer ports.
	VPC Peer VLAN Info	VLAN ids for vpc peer ports (optional).
	BR Management Port Info	Management interface of build node.
	BR Management PO Info	Port channel number for management interface of build node.
	BR Management VLAN info	VLAN id for management interface of build node (access).
Click **Save**.		

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

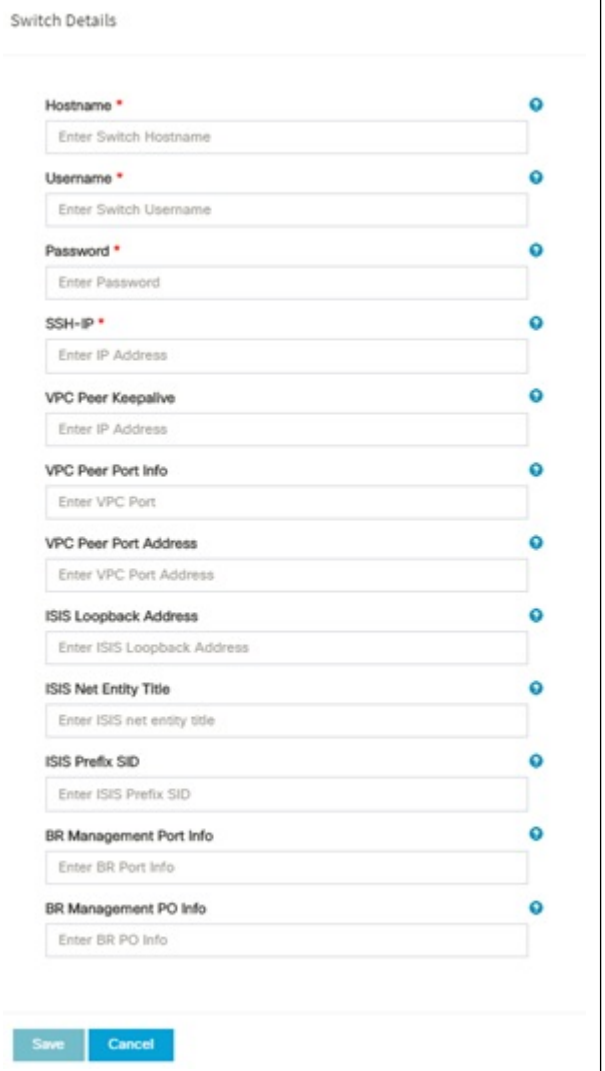
Name	Description
Configure ToR	Is not checked, as by default ACI will configure the ToRs 

Host Name	ToR switch name.
VPC Peer keep alive	Enter Peer must be exist pair.
VPC Domain	Enter an integer.
BR management port info	Enter BR management port info eg. Eth1/19 ,atleast one pair to be exist.
Enter Node ID	Entered integer must be unique.

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.

Name	Description
If you want to enter NCS details fill in the **NCS-5500 Information** table.	

Name	Description
	Click (+) to add information for NCS-5500 Switch. 

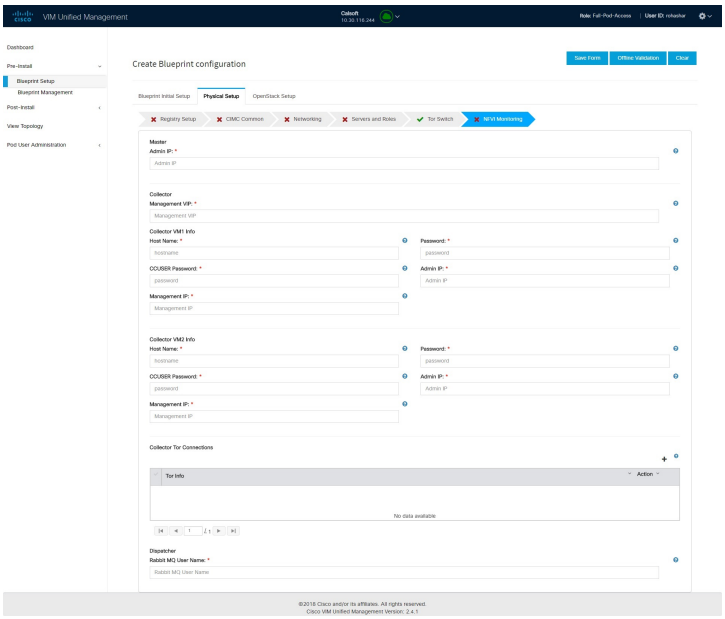
Name	Description
Name	Enter the NCS-5500 hostname.
User Name	Enter the NCS-5500 username.
Password	Enter the NCS-5500 password.
SSH IP	Enter the NCS-5500 ssh IP Address.
VPC Peer Link	Peer management IP.

Name	Description
	<table><tr><th>Name</th><th>Description</th></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>

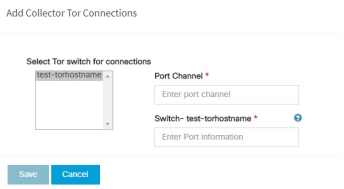
When TOR-TYPE selected as NCS-5500 and 2 NCS-5500 are configured it is mandatory to configure MULTI_SEGMENT_ROUTING_INFO

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.
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 **NFVI Monitoring** checkbox in Blueprint Initial Setup to enable the NFVI Monitoring configuration tab.

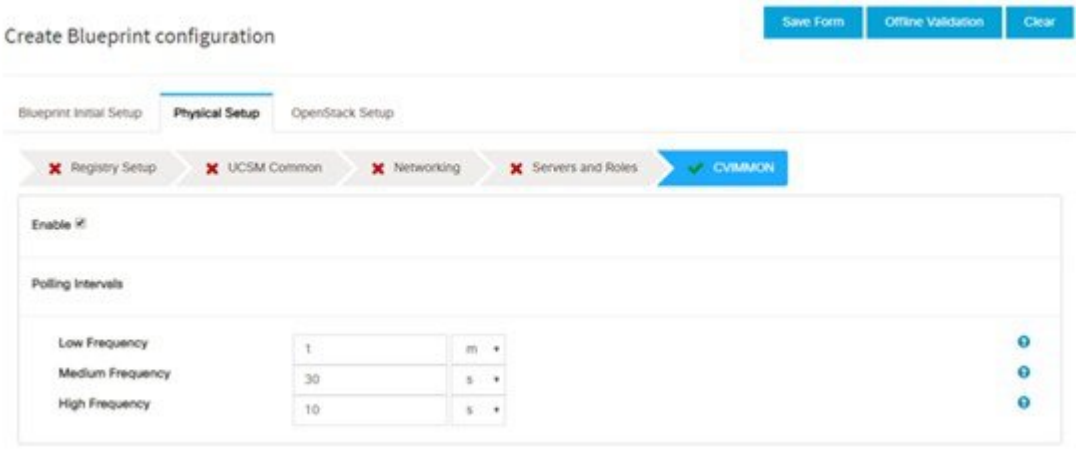


Name	Description
Admin IP	IP Address of Control Center VM
Management VIP	VIP for ceilometer/dispatcher to use, must be unique across VIM Pod
Host Name	Hostname of Collector VM
Password	Password of Collector VM
CCUSER Password	Password of CCUSER
Admin IP	SSH IP of Collector VM
Management IP	Management IP of Collector VM

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Collector ToR Connections</td><td>1. Click on (+) icon to Add Collector ToR Connections.
2. Select the ToR switches from list to add the information.
3. It is optional and available for ToR type NCS-5500
4. For now, it supports adding only one Collector ToR Connection
 

<table>
<tr><td>Port Channel</td><td>Enter port channel.</td></tr>
<tr><td>Switch - {torSwitch-hostname}</td><td>Enter port number, For example, eth1/15.</td></tr>
</table>
Click Save</td></tr>
<tr><td>Rabbit MQ User Name</td><td>Enter Rabbit MQ username.</td></tr>
</table>

8. Click **CVIMMON** checkbox in Blueprint Initial Setup to enable the CVIMMON configuration tab.



CVIM-MON is a built-in infrastructure monitoring service based on telegraf/prometheus/grafana.

When enabled, the telegraf service will be deployed on every node on the pod to capture infrastructure level stats (CPU, memory, network, containers, and so on.) and a Prometheus server will be installed on the management node to poll for these stats and store them in its time series database. The statistics can then be viewed using the grafana server that is accessible on the management node at port 3000 (password protected).

There are three levels of polling intervals which are used by different telegraf plugins:

- Low frequency interval is used to collect system level metrics like cpu, memory.

- Medium frequency interval is used to collect docker metrics.
- High frequency interval is used to collect rabbitmq metrics.

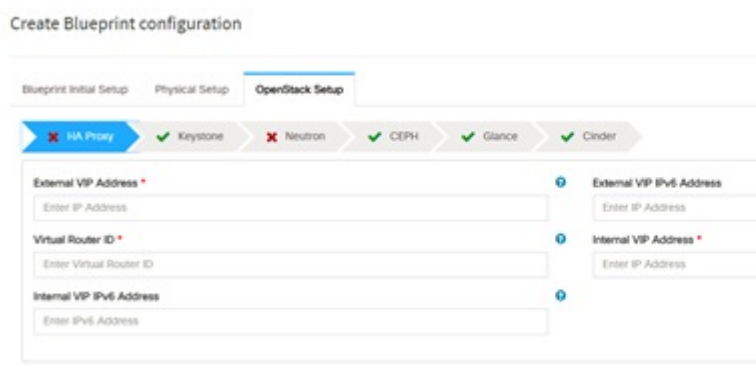
Defining polling intervals in setup data is optional. If not defined, the default values are used.

CVIM-MON is mutually exclusive to NFVIMON.

PODNAME is required, when CVIM-MON is enabled.

Name	Description
Enable	Default is False
Polling Intervals	
Low frequency	<Integer following with time sign (s/m/h)> # min of 1 minute (1m) if not defined defaults to 1m, also it needs to be higher than medium interval.
Medium frequency	<Integer following with time sign (s/m/h)> # min of 30 seconds (30s) if not defined defaults to 30s, also it needs to be higher than high interval.
High frequency	<Integer following with time sign (s/m/h)> # min of 10 seconds (10s) if not defined defaults to 10s.

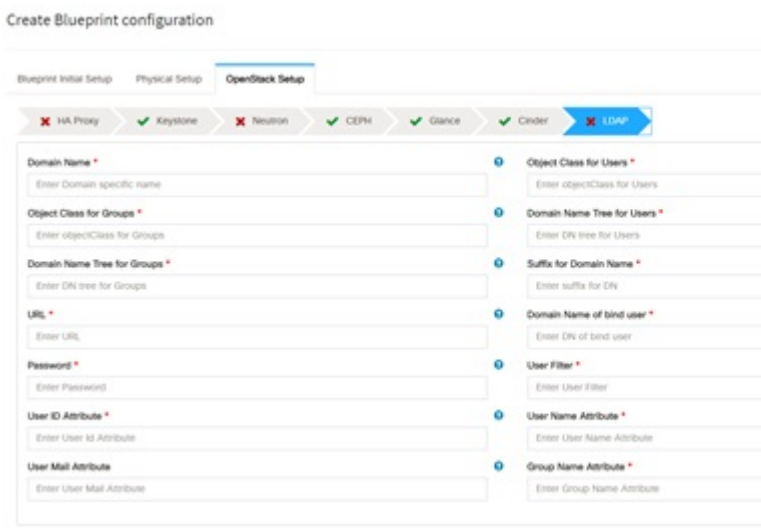
9. Click **OpenStack Setup** Tab to advance to the **OpenStack Setup** Configuration page. On the **OpenStack Setup** Configuration page of the Cisco VIM Insight wizard, complete the following fields:

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>HA Proxy</td><td>Fill in the following details:
 

<table>
<tr><td>External VIP Address field</td><td>Enter IP address of External VIP.</td></tr>
<tr><td>External VIP Address IPv6 field</td><td>Enter IPv6 address of External VIP.</td></tr>
<tr><td>Virtual Router ID field</td><td>Enter the Router ID for HA.</td></tr>
<tr><td>Internal VIP Address IPv6 field</td><td>Enter IPv6 address of Internal IP.</td></tr>
<tr><td>Internal VIP Address field</td><td>Enter IP address of Internal VIP.</td></tr>
</table></td></tr>
<tr><td>Keystone</td><td>Mandatory fields are pre-populated.
 

<table>
<tr><td>Admin User Name</td><td>admin.</td></tr>
<tr><td>Admin Tenant Name</td><td>admin.</td></tr>
</table></td></tr>
</table>

Name	Description
LDAP	

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>
LDAP enable checkboxwhich 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>
</table>
</td></tr>
</table>

Name	Description	
	Group Name Attribute field	Enter a string.

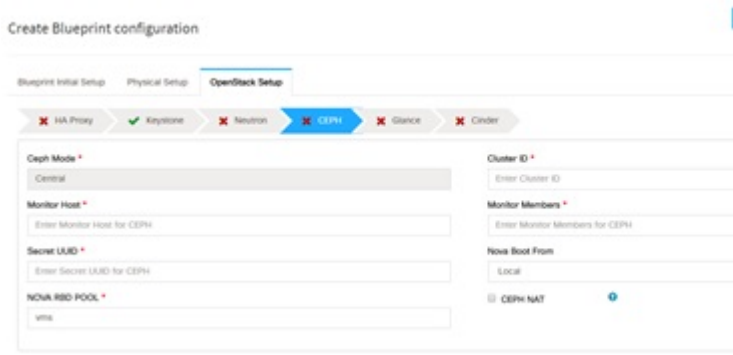
Name	Description
Neutron	

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></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 example:
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 (optional, defaults to 2M)</td></tr>
<tr><td>VM_HUGHPAGE_PERCENTAGE</td><td>Optional, defaults to 100%; can range between 0 and 100</td></tr>
</table></td></tr>
</table>

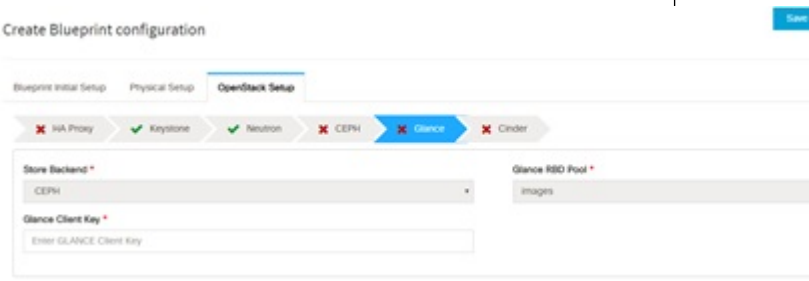
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>NR_RESERVED_VSWITCH_PCORES</td><td>Allowed only for VPP
Number of cores associated to VPP, defaults to 2. Takes value of 2 through 6.</td></tr>
<tr><td>Enable Jumbo Frames field</td><td>Enable the checkbox</td></tr>
</table>
For Tenant Network Type Linux Bridge everything remains the same but Tenant VLAN Ranges will be removed.
</td></tr>
</table>

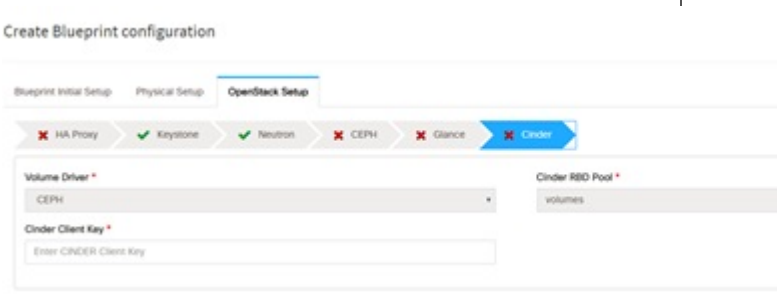
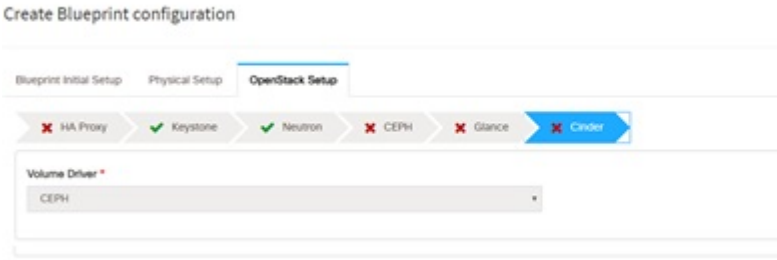
Name	Description
CEPH	

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>
1. 1. When Object Storage Backend is selected Central in blueprint initial setup.


<table>
<tr><td>CEPH Mode</td><td>By default Central.</td></tr>
<tr><td>Cluster ID</td><td>Enter Cluster ID.</td></tr>
<tr><td>Monitor Host</td><td>Enter Monitor Host for CEPH</td></tr>
<tr><td>Monitor Members</td><td>Enter Monitor Members for CEPH</td></tr>
<tr><td>Secret UUID</td><td>Enter Secret UUID for CEPH</td></tr>
<tr><td>NOVA Boot from</td><td>Drop down selection. You can choose CEPH or local.</td></tr>
<tr><td>NOVA RBD POOL</td><td>Enter NOVA RBD Pool (default's to vms)</td></tr>
<tr><td>CEPH NAT</td><td>Optional, needed for Central Ceph and when mgmt network is not routable</td></tr>
</table>
2. When Object Storage Backend is selected Dedicated in blueprint initial setup.

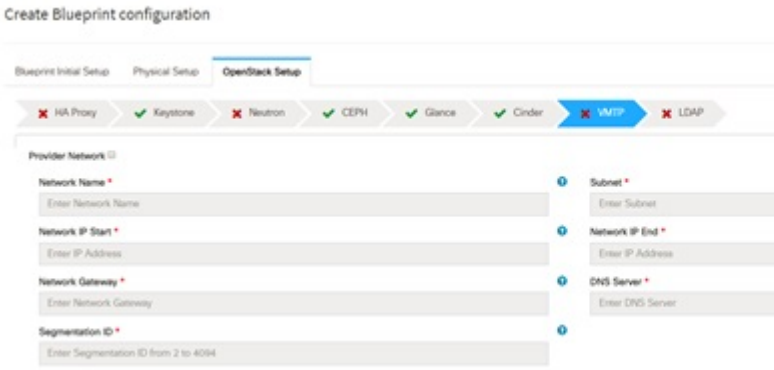

• CEPH Mode: By default Dedicated.
• NOVA Boot: From drop down selection you can choose CEPH or local.
3. When Object Storage Backend is selected NetApp in blueprint initial setup.
</td></tr>
</table>

Name	Description
	
GLANCE	1. When Object Storage Backend is selected Central in blueprint initial setup.  When Object Storage Backend is selected Dedicated in blueprint initial setup.  **Note** By default Populated for CEPH Dedicated with Store Backend value as CEPH.

Name	Description
CINDER	By default Populated for **CEPH Dedicated** with Volume Driver value as **CEPH**.  2. When Object Storage Backend is selected Dedicated in blueprint initial setup.  **Note** By default Populated for CEPH Dedicated with Volume Driver value as CEPH.

Name	Description
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.	

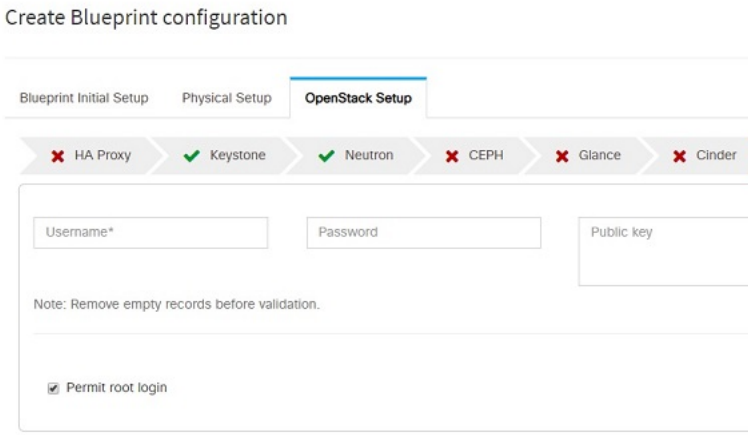
Name	Description
	Check one of the check boxes to specify a VMTP network: • Provider Network • External Network For the **Provider Network** complete the following:



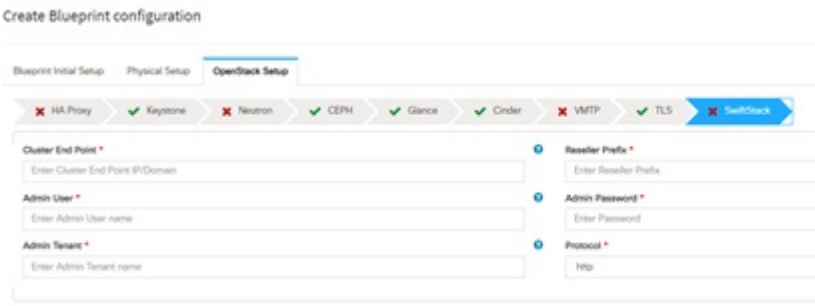
Network Name field	Enter the name for the external network.
Subnet field	Enter the Subnet for Provider Network.
Network IP Start field	Enter the starting floating IPv4 address.
Network IP End field	Enter the ending floating IPv4 address.
Network Gatewayfield	Enter the IPv4 address for the Gateway.
DNS Server field	Enter the DNS server IPv4 address.
Segmentation ID field	Enter the segmentation ID.

For **External Network** fill in the following details:

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>
<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>
<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>
</table>

<table>
<tr><th>Name</th><th>Description</th></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:
Add Username, Password, Public key or both for the non-root login.
At least one Vim Admin must be configured when Permit root login is false. 

<table>
<tr><td>User Name</td><td>Enter username for Vim Admin.</td></tr>
<tr><td>Password</td><td>Password field. Admin hash password should always start with $6.</td></tr>
<tr><td>Public Key</td><td>Public key for vim admin should always start with ‘ssh-rsa AAAA….’</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></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>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>APICINFO tab is available in Openstack setup, when the Tenant type ACI/VLAN is selected in blueprint initial setup.
Note When ACI/VLAN is selected then ToR switch from initial setup is mandatory.</td><td>
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>APIC Hosts field</td><td>Enter host input. Example: <ip1|host1>:[port] . max of 3, min of 1, not 2;</td></tr>
<tr><td>apic_username field</td><td>Enter a string format.</td></tr>
<tr><td>apic_password filed</td><td>Enter Password.</td></tr>
<tr><td>apic_system_id field</td><td>Enter input as string. Max length 8.</td></tr>
<tr><td>apic_resource_prefix field</td><td>Enter string max length 6.</td></tr>
<tr><td>apic_tep_address_ pool field</td><td>Allowed only 10.0.0.0/16</td></tr>
<tr><td>multiclass_address_pool field</td><td>Allowed only 225.0.0.0/15</td></tr>
<tr><td>apic_pod_id field</td><td>Enter integer(1- 65535)</td></tr>
<tr><td>apic_installer_tenant field</td><td>Enter String, max length 32</td></tr>
<tr><td>apic_installer_vrf field</td><td>Enter String, max length 32</td></tr>
<tr><td>api_l3out_network field</td><td>Enter String, max length 32</td></tr>
</table>
</td></tr>
<tr><td>VTS tab is available in Openstack setup, when Tenant Type is VTS/VLAN selected.
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</td><td>
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>VTS Day0 (checkbox)</td><td>True or false default is false.</td></tr>
<tr><td>VTS User name</td><td>Enter as string does not contain special characters.</td></tr>
<tr><td>VTS Password</td><td>Enter password</td></tr>
<tr><td>VTS NCS IP</td><td>Enter IP Address format.</td></tr>
<tr><td>VTC SSH Username</td><td>Enter a string</td></tr>
<tr><td>VTC SHH Password</td><td>Enter password</td></tr>
</table>
</td></tr>
</table>

10. For SolidFire, enter the following:

Name	Description

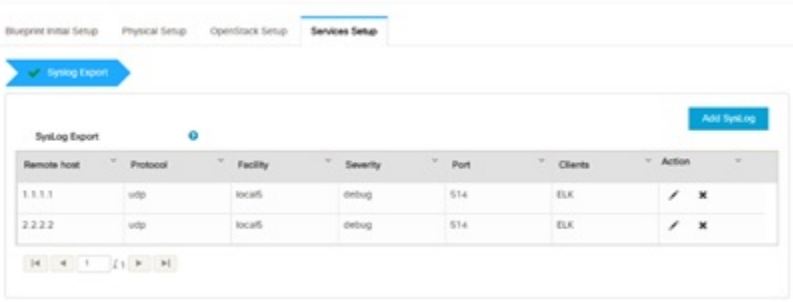
SolidFire is visible for configuration on day0

SolidFire is not allowed as a day-2 deployment option

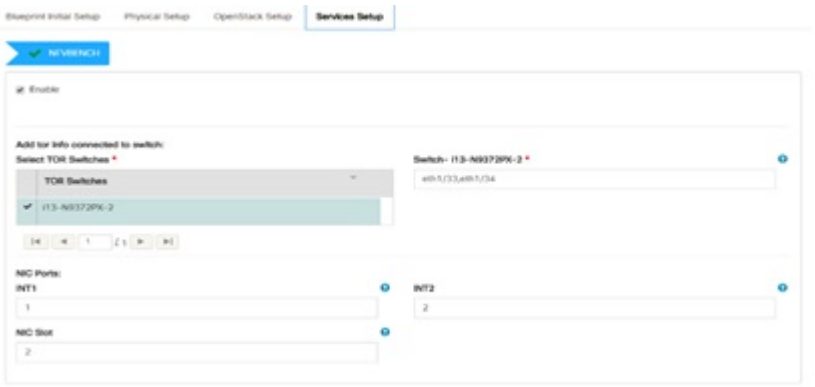
SolidFire is always available with CEPH.

Cluster MVIP field	Management IP of SolidFire cluster.
Cluster SVIP field	Storage VIP of SolidFire cluster.
Admin Username	Admin user on SolidFire cluster
Admin Password	Admin password on SolidFire cluster.

11. 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:
User can add maximum of three entries.
To add new SysLog information, click on Add SysLog button, fill all the required information listed below and hit Save button.
 

<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>
</table>

Name	Description
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. NIC Slot: Optional input, should be in the range of 1-6, indicates which NIC to use in case there are multiple NICs. If nic_slot is defined, then nic_port has to be defined and vice-versa.
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 valid 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 sublinks available to manage the day-n operation of the pod. However, often Insight cross-launches the relevant services, through delegating the actual rendering to the individual services.

Monitoring the Pod

Cisco VIM 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 Login as **POD User.**

Step 2 Naviagte to **POD.**

Step 3 Navigate to **Post-install**

Step 4 Click **Monitoring**
The **Authentication Required** browser pop up is displayed.

Step 5 Enter the **username** as admin.

Step 6 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 Login as **POD User.**

Step 2 Naviagte to **POD.**

Step 3 Navigate to **Post-install**

Step 4 Click **Reconfigure**.

Step 5 Click **NFVI Monitoring**

Step 6 Click the link **Click here to view NFVI monitoring.**.

You will be redirected to NFVI monitoring page

Run VMTP

VIM 2.0, provides an integrated data and control plan test tool (called VMTP).VMTP helps you to test the cloud at any given time.

Run VMTP is divided in two sections:

- **Results for Auto Run**: Auto run shows the results of VMTP which was run during the cloud deployment (Blueprint Installation).
- **Results for Manual Run**: To run VMTP on demand click **Run VMTP**.

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

Run CloudPulse

In VIM, we provide an integrated tool, called Cloud Pulse, that periodically checks the cloud services endpoint. The results of these tests are reflected under the Cloud Pulse link. You can also run these API endpoint tests on demand, and fetch the result of these tests by refreshing the table.

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 , 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

Name	Description
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 as **POD User.**

Step 2 Navigate to **POD.**

Step 3 Navigate to **Postinstall.**

Step 4 Click **Run NFV Bench**.

Step 5 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 **Run Fixed Rate Test.** Once Fixed rate test is finished, it displays 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 Login as **POD User.**

Step 2 Naviagte to **POD.**

Step 3 Navigate to **Post-install**

Step 4 Click **System Update**.

Step 5 Click **Openstack Password**

Step 6 Click **Browse** button.

Step 7 Select the valid tar file.

Step 8 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 Login as **POD User.**

Step 2 Naviagte to **POD.**

Step 3 Navigate to **Post-install**

Step 4 Click **Reconfigure**.

Step 5 Click **Openstack Password**

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 users password policy.

There are two options to regenerate the Password:

1. **Regenerate all passwords**: Check the **Regenerate all passwords** checkbox and click **Set Password**. This automatically regenerates all passwords in alphanumeric format.
2. **Regenerate single or more password**: If you want to set a specific password for any service like Horizon's ADMIN_USER_PASSWORD you can add it by doing an inline edit. Double click field under Password and then enter the password which enables **Set Password**.

Note During the reconfiguration of password, all other pod management activities are disabled. Postupdate, normal cloud management commences.

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 Login as **POD User.**

Step 2 Naviagte to **POD.**

Step 3 Navigate to **Post-install**

Step 4 Click **Reconfigure OpenStack Config**.

Step 5 Click on the specific item to be changed and updated; For TLS certificate it is the path to certificate location.

Step 6 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 Cisco VIM feature set. These services can be enabled in one-shot or selectively. Listed below are the steps to enable optional services:

Step 1 Login as **POD User.**

Step 2 Naviagte to **POD.**

Step 3 Navigate to **Post-install**

Step 4 Click **Reconfigure Optional Services**.

Step 5 Choose the right service and update the fields with the right values.

Step 6 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

Optional Features	Repeated re-deployment Options
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
HTTPS Proxy Server	True
Enable TTY LOGGING	False
MGMTNODE_EXTAPI_REACH	False

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 **Log in as POD User.**

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

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

Step 4 Complete the following fields on 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.
Permission	Check the **Permission** checkbox to select the permission.

Step 5 Click **Save**. Once, the Blueprint is in an 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 the granular level where viewing *Dashboard* is the default role that is 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.